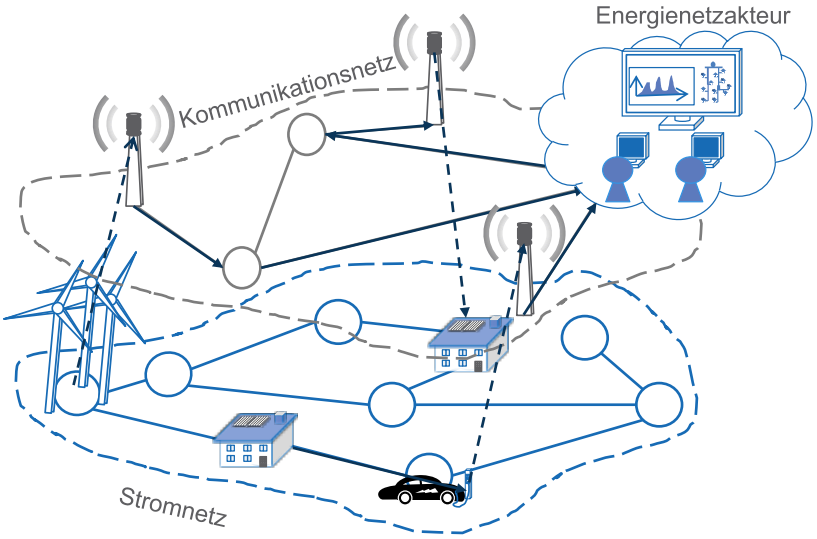
MÆDIT

Prävention, Detektion und Reaktion bei IT-Angriffen und -Ausfällen



Leitfaden für die Vorbereitung und Reaktion auf IT-Angriffe und -Ausfälle

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Version 2022-07

Inhalt

Kapitel 1

Einleitung

Themen:

Dieser Leitfaden unterstützt Betreiber kritischer Infrastrukturen im Energiesektor bei der Prävention, Detektion und Behandlung von IT-Sicherheitsvorfällen.

Im Gegensatz zu klassischen Fehlersituationen durch Defekte ist zu erwarten, dass Angreifer in vielen Fällen redundante Systeme ebenfalls kompromittiert haben und identische Backup-Systeme leicht mit den gleichen Mitteln angreifen können. Die Reaktion auf Cybervorfälle und IKT-Ausfälle erfordert daher operative Leitlinien mit klaren Handlungsempfehlungen.

Vorwort

Die Behandlung von IT-Sicherheitsvorfällen in kritischen Infrastrukturen (*KRITIS*) wie der Stromversorgung ist ein komplexes, mehrdimensionales Themenfeld. Im Gegensatz zu klassischen Fehlersituationen durch Defekte ist zu erwarten, dass Angreifer in vielen Fällen redundante Systeme ebenfalls kompromittiert haben und identische Backup-Systeme leicht mit den gleichen Mitteln angreifen können. Die Reaktion auf Cybervorfälle und IKT-Ausfälle erfordert daher operative Leitlinien mit klaren Handlungsempfehlungen.

In diesem Abschnitt werden zunächst Vorgaben und Richtlinien vorgestellt sowie die allgemeine Vorgehensweise für Beobachtungen und Handlungen eingeführt. Begriffliche und technische Grundlagen werden im anschließenden Grundlagen-Abschnitt diskutiert.

Vorgaben und Richtlinien

Die meisten existierenden relevanten Vorgaben und Richtlinien (insbesondere gesetzliche Vorgaben, Konzern- und Vorstandsvorgaben sowie technische Regelungen) befassen sich hauptsächlich mit organisatorischen Maßnahmen und legen fest, wer informiert werden muss und welche organisatorischen Prozesse durchgeführt werden sollen. Konkrete Handlungsempfehlungen für den Endanwender, der einen mögliches IT-Sicherheitsereignis entdeckt, fehlen zumeist. Diese Lücke will der hier vorliegende Maßnahmenkatalog schließen. Nachfolgen sind die wichtigsten regulatorischen Vorgaben aufgelistet. Im Anschluss daran sind mögliche unternehmensinterne Vorgaben aufgelistet. Diese sind bewusst generisch gehalten und geben nur eine Indikation, welche internen Dokumente zur Bearbeitung hinzugezogen werden könnten.

- Gesetzliche Vorgaben
  - EnWG §11 Abs. 1a
  - DIN ISO / IEC 27001:2015
  - DIN ISO / IEC 27019:2017
  - DIN ISO / IEC 27035
  - IT-Sicherheitsgesetzt *(Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme)*
  - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSIKritisV)
  - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
- Konzern- und Unternehmensvorgaben
  - interne Informations-Sicherheits-Standards
  - Mitarbeiter Guidelines
  - Netzrichtlinien
  - Konzernrichtlinien
  - Vorstandsvorgaben

Um eine breite Anwendbarkeit sicherzustellen, sind diese vielfältigen Vorgaben und Richtlinien typischerweise sehr generisch und abstrakt gehalten. Klare und konkrete Anweisungen auf technischer Ebene stehen in der Regel nicht im Fokus von aktuell im Einsatz befindlicher Vorgaben und Richtlinien. Das vorliegende Dokument soll diese Lücke durch die Bereitstellung von konkreten Maßnahmenlisten schließen und dabei insbesondere geeignete Sofortmaßnahmen bereitstellen. Ziel des Leitfadens, der den Kern dieses Dokuments bildet, ist es, allen Mitarbeiterinnen und Mitarbeitern, die potenziell mit einem IT-Ausfall oder Cyber-Angriff konfrontiert sind -- insbesondere jenen ohne vertieftem IT-Hintergrund, wie z.B. dem Leitstellenpersonal -- klare und präzise Anweisungen zur Verfügung zu stellen.

Grundlagen

Dieser Abschnitt beschreibt den grundlegenden Aufbau dieses Maßnahmenkatalogs sowie die Systeme und Szenarien, für die dieser Leitfaden genutzt werden kann. Zudem werden entsprechende Begriffe eingeführt und gegeneinander abgegrenzt.

Beobachtungs- und Aktionszyklus

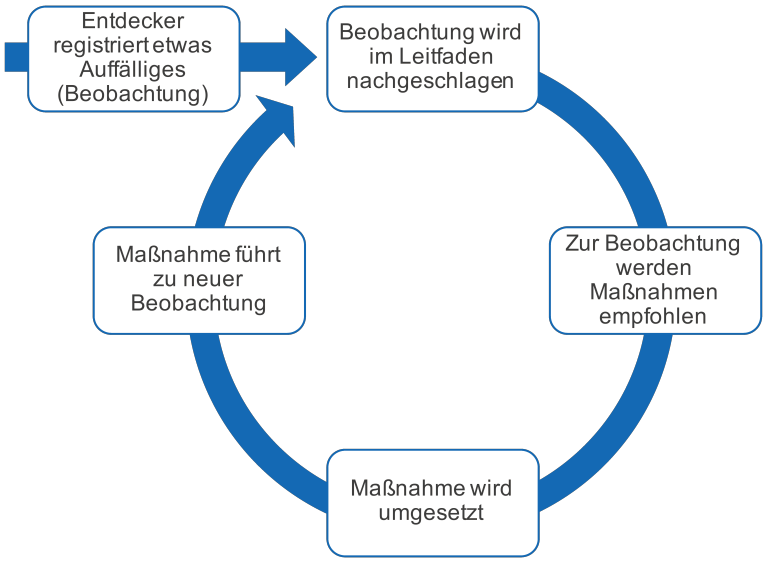


Abbildung 1: Der im Rahmen dieses Dokuments vorgestellte Leitfaden unterstützt Mitarbeiterinnen und Mitarbeiter bei der Reaktion auf IT-Sicherheitsvorfälle durch einen iterativen Beobachtungs-/Aktionszyklus mit klaren Handlungsempfehlungen.

Wie in Abbildung 1 auf Seite 10 dargestellt, ist der Kerngedanke des vorliegenden Leitfadens, Beobachtungen aus Sicht der Mitarbeiterinnen und Mitarbeiter zu beschreiben, die potentiell als erste mit der jeweiligen Beobachtung in Berührung kommen. Auf der Grundlage jeder Beobachtung werden verschiedene Maßnahmen vorgeschlagen, die dann zu neuen Beobachtungen führen können, die einen Ausgangspunkt für die nächste Iteration darstellen.

Im Detail liegt dem Leitfaden ein iterativer Beobachtungs-/Aktionszyklus mit fünf Schritten zugrunde:

1. Die Entdeckerin bzw. der Entdecker macht eine Beobachtung, z.B. wird eine etwas Auffälliges beobachtet,
2. die Beobachtung wird im Leitfaden nachgeschlagen,
3. zur Beobachtung werden eine oder mehrere Maßnahmen empfohlen,
4. die Maßnahme wird durchgeführt, so dass
5. eine neue Beobachtung gemacht wird.

Dieser Zyklus wird solange durchlaufen, bis keine weiteren Schritte von der Mitarbeiterin bzw. dem Mitarbeiter durchzuführen sind.

Begriffsbestimmungen

Die Abbildung 2 auf Seite 11 stellt die Systeme und Komponenten dar, die im Rahmen dieses Leitfadens adressiert werden. In der nachfolgenden Auflistung finden Sie Verweise auf die Definitionen bzw. Beschreibungen von diesen Systemen. Daneben sind auch weitere Begriffe, die in diesem Katalog genutzt werden und nicht unmittelbar einem konkreten Systems zuordenbar sind, aufgelistet.

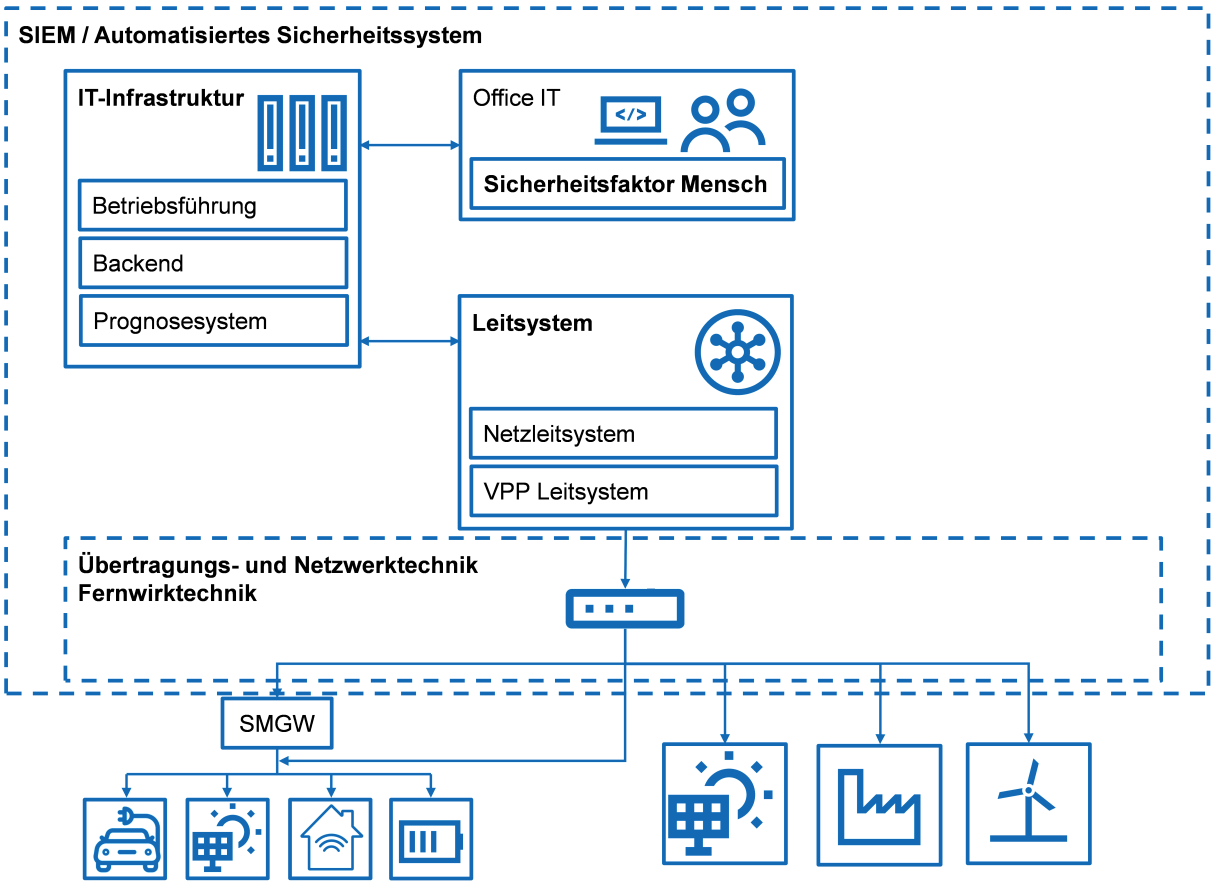


Abbildung 2: Überblick über Systeme und Komponenten, die in diesem Leitfaden adressiert werden.

- Backend
- Fernwirktechnik
- Leitsystem
- Sicherheitsfaktor Mensch
- Organisatorische Vorgaben
- SIEM
- Übertragungs- und Netzwerktechnik
- Zufallsbeobachtungen

Meldung an Behörden

Je nach der Schwere des Vorfalls muss eine Meldung an die Behörden erfolgen. In den meisten Fällen gehen diese Meldungen an das Bundesamt für Informationssicherheit *BSI* oder die Bundesnetz Agentur *BNetzA*. Eine Entscheidung, ob es sich um ein meldepflichtiges Ereignis handelt, muss von den Bearbeitern getroffen. Nachfolgende Grafik kann hierbei als Orientierung genutzt werden.

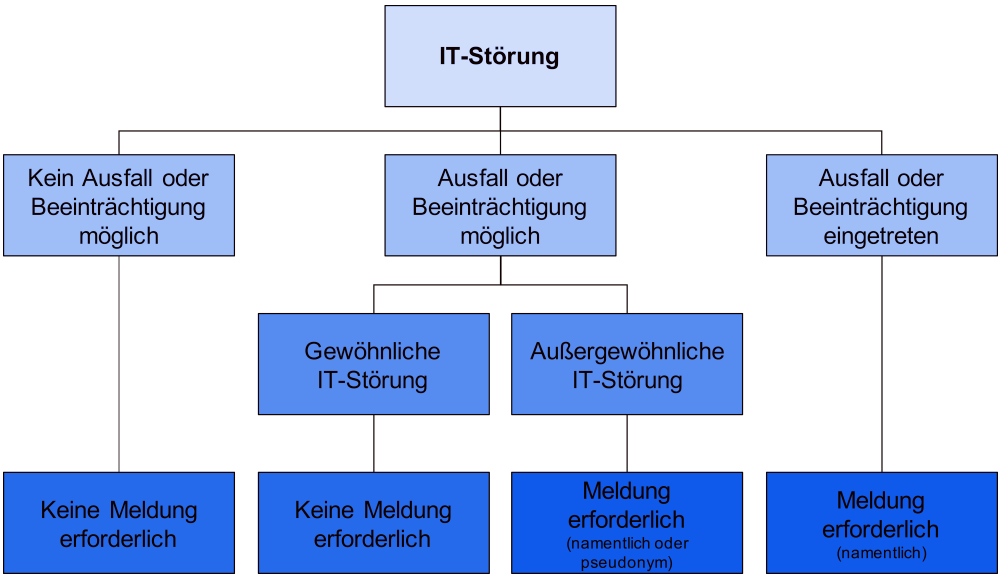


Abbildung 3: Entscheidungsbaum Meldung Vorfall

Die weitere Bearbeitung der Meldung orientiert sich an dem folgenden Schaubild:

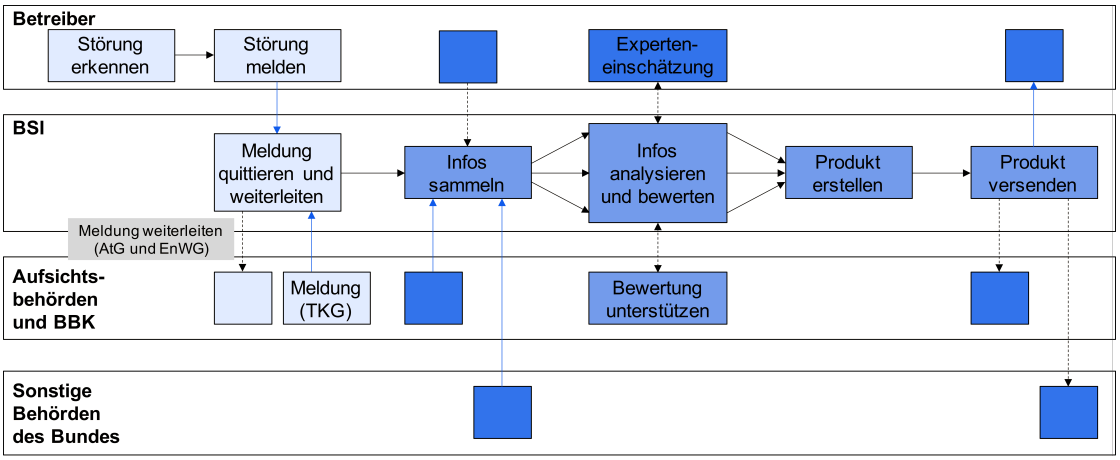


Abbildung 4: Schematische Darstellung Meldewege

Hinweise zur Nutzung

Dieser Abschnitt gibt Hinweise, wie dieser Maßnahmenkatalog zu nutzen ist.

Verknüpfungen

Wie im vorangegangenen Grundlagen-Abschnitt beschrieben wurde, basiert dieser Maßnahmenkatalog auf einem Beobachtungszyklus: Zu einer Beobachtung wird eine passende Maßnahme ausgewählt. Aus dieser Maßnahme werden in aller Regel neue Beobachtungen entstehen, die ihrerseits neue Maßnahmen nach sich ziehen können. Ein Schlüsselrolle spielen dabei die Verknüpfungen zwischen Beobachtungen und zugeordneten Maßnahmen. Allen Beobachtungen und Maßnahmen ist neben ihrem vollständigen Titel ein Kurztitel zugeordnet, welcher die Identifizierung von Themengebieten sowie den Lesefluss erleichtern. Im Leitfaden werden Verknüpfungen sowohl über die vollständigen Beschreibungen als auch über die Kurztitel kontextspezifisch genutzt.

Neben Verknüpfungen zu anderen Beobachtungen und Maßnahmen im Text finden Sie am Ende einer jeden Beobachtung oder Maßnahme zudem eine Zusammenstellung aller relevanten Verknüpfungen, ebenfalls unterteilt in Beobachtungen und Maßnahmen.

Die Kurztitel, wie z.B. **B.ORG.FDA** oder **M.INV.ÜT/NT-ÜSV** setzen sich nach einem festem Schema zusammen. Dabei gibt der erste Buchstabe an, ob es sich um eine Maßnahme **M** oder um eine Beobachtung **B** handelt. Der zweite Buchstabenblock nach dem Punkt steht für ein Kürzel der betroffenen Systeme oder die Art der Maßnahme. Der dritte Teil nach dem zweiten Punkt gibt eine Abkürzung der enthaltenen Beobachtung

oder Maßnahme an und ist somit spezifisch und wird vom jeweiligen Autor festgelegt. Für eine bessere Übersichtlichkeit ist in der folgenden Tabelle ein Auflistung aller genutzten Kürzel angegeben.

Erläuterung	
B	Kürzel für eine **Beobachtung**
AS	Kürzel für **Automatisiertes Sicherheitssystem** (SIEM)
BE	Kürzel für **Backend** Systeme und allgemeine **IT-Infrastruktur**
FWT	Kürzel für **Fernwirktechnik**
LS	Kürzel für **Leitsystemtechnik**
ORG	Kürzel für **Organisatorische Vorgaben**
SFM	Kürzel für **Sicherheitsfaktor Mensch**
ÜT/NT	Kürzel für **Übertragungs- und Netzwerktechnik**
ZB	Kürzel für **Zufallsbeobachtungen**

Erläuterung	
M	Kürzel für eine **Maßnahme**
KOM	Kürzel für **Kommunikation**
INV	Kürzel für **Investigation**
REA	Kürzel für **Reaktion**
NAB	Kürzel für **Nachbereitung**
DOK	Kürzel für **Dokumentation**

Hervorhebung von Beobachtungen

Beobachtungen, welche direkt von den Mitarbeitenden gemacht werden können, sind im Leitfaden besonders hervorgehoben.

Eine wichtige Beobachtung, welche einem Mitarbeitenden als Einstiegspunkt für die Bearbeitung eines Vorfalls bietet, ist besonders hervorgehoben.

Rechtshinweis und Lizenz

Kapitel 2

Leitsystem

Themen:

Das *Leitsystem* ist eine zentrale Komponente in der Steuerung von Energienetzen. Es ist dafür verantwortlich, alle angeschlossenen Teilsysteme wie z.B. Fernwirkgeräte oder Schaltanlagen zu koordinieren. Ein Ausfall des Leitsystems, würde daher zur Folge haben, dass das gesamte System nicht mehr gesteuert werden kann.

In diesem Abschnitt finden Sie alle Beobachtungen, die das Leitsystem betreffen. Unter dem Begriff Leitsystem werden im Rahmen dieses Maßnahmenkatalogs sämtliche zentralen Komponenten des *SCADA*, wie z.B. die Leitrechner inklusive Datenbanken sowie die zentralen Übergangspunkte zu den Prozessdatennetzen verstanden. Es stellt somit einen wesentlichen Teil der Prozess-IT *PIT* eines Netzbetreibers oder Einsatzverantwortlichen dar. Anstelle des Kürzels PIT wird oftmals auch oft der Begriff Operational Technology *OT* verwendet. Dies Bezeichnung wird als Abgrenzung zur normalen Office-IT verwendet, die meist nur mit (*IT*) oder (*CIT*) bezeichnet wird.

Es wird betrachtet, wie ein aktiver Angriff oder wie ein kompromittiertes System erkannt werden kann. Ein kompromittiertes Leitsystem frühzeitig zu erkennen ist enorm wichtig, da im Falle einer Kompromittierung des Systems eine uneingeschränkte Steuerung von angebundenen Systemen nicht mehr gewährleistet werden kann. Ein kompromittiertes System birgt ebenfalls die Gefahr, dass ein Angreifer in der Lage ist unautorisierte Steuerbefehle auszuführen, um Schaden anzurichten. Ebenfalls werden in diesem Kapitel Netzwerkangriffe betrachtet bzw. wie Netzwerkwerkangriffe auf das Leitsystem erkannt werden können, da diese zu einem kompromittierten System oder zu einem Ausfall des Systems führen können.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Fehlinformationen im Leitsystem entdeckt (B.LS.FE)

Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt

Ein Bediener hat im Leitsystem offensichtlich falsche oder unplausible Informationen entdeckt. Dabei kann es sich um einzelne Messwerte von Sensoren oder Fernwirkgeräten handeln. Ebenso können grafische Anzeigen auf der Nutzeroberfläche widersprüchliche oder falsche Informationen darstellen.

Da eine mögliche Fehlfunktion oder Manipulation des Leitsystems oder eines der angeschlossenen Fernwirkgeräte, Schaltanlagen oder Sensoren nicht ausgeschlossen werden kann, muss dieser Vorfall untersucht werden.

Zugehörige Beobachtungen

Diskrepanz zwischen Daten und Messwerten (B.BE.DDM) auf Seite 45

Diskrepanz zwischen Vorhersagen und Messwerten (B.BE.DVM) auf Seite 45

Zugehörige Maßnahmen

Leitsystemtechnik hinzuzuziehen (M.KOM.LSTH) auf Seite 72
Für die weitere Bearbeitung eines Vorfalls, ist die Fernwirktechnik hinzuzuziehen

Quelle von Fehlinformationen im Leitsystem untersuchen (M.INV.LS-FLSU) auf Seite 84
Die Quelle von Fehlinformationen oder unplausiblen Messwerten soll untersucht werden.

Fehlinformationen im Leitsystem ohne Quellzuordnung entdeckt (B.LS.FIKQ)

Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt, die keiner bestimmten Quelle zugeordnet werden können

Ein Bediener hat im Leitsystem offensichtlich falsche oder unplausible Informationen entdeckt. Dabei kann es sich um einzelne Messwerte von Sensoren oder Fernwirkgeräten handeln. Ebenso können grafische Anzeigen auf der Nutzeroberfläche widersprüchliche oder falsche Informationen darstellen. Bei der Untersuchung der falschen Informationen konnte entweder keine Quelle für die falschen Werte identifiziert werden, oder die Quelle sendet korrekte Informationen und auch der Übertragungsweg wurde bereits ergebnislos untersucht.

Da eine mögliche Fehlfunktion oder Manipulation des Leitsystems nicht ausgeschlossen werden kann, muss dieser Vorfall untersucht werden

Zugehörige Maßnahmen

Leitsystemtechnik hinzuzuziehen (M.KOM.LSTH) auf Seite 72
Für die weitere Bearbeitung eines Vorfalls, ist die Fernwirktechnik hinzuzuziehen

Software des Leitsystems überprüfen (M.INV.LS-SWU) auf Seite 88
Die Softwarestände des Leitsystems müssen überprüft werden.

Virenscan eines Systems (M.REA.CIT-VS) auf Seite 111
Überprüfung

Das Leitsystem oder die Software scheint kompromittiert zu sein. (B.LS.LSKo)

Ein Standort des Netzleitsystems zeigt Auffälligkeiten und ist gegebenenfalls kompromittiert.

Es wurde festgestellt, dass ein Standort des Netzleitsystems kompromittiert ist.

Solch eine Kompromittierung kann unterschiedliche Ursachen haben z.B.:

- lokale technische Störungen (z.B. Stromausfall)

- physikalische Abtrennung des Netzleitsystems von dem digitalen Übertragungsnetz
- Virenbefall oder Hackerangriffe

In diesem Szenario muss entschieden werden, ob der kompromittierte Standort weiter genutzt werden kann, oder ob der Standort als Ausfall zu bewerten ist. Hierbei werden folgende Vorfälle unterschieden:

- Malware/ Virenbefall eines Standorts
- Nicht registrierte Software an einem Standort entdeckt
- Software mit falscher Signatur, Checksumme oder Versionsstand an einem Standort
- Ein normaler Nutzer hat weiterreichende Rechte bekommen
- Ausfall Hauptstandort
- Ausfall Ersatzstandort
- Ausfall Kommunikationsstandort
- Komplettausfall des Netzleitsystems

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61
Hacking Tool detected
Unexpected Desktop Software (B.CIT.UDS) auf Seite 52
Keine Reaktion auf Steuerbefehle (B.LS.KRS) auf Seite 23
Hohe Latenz (B.LS.HL) auf Seite 23
Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23
Privilege Escalation (B.BE.PrEs) auf Seite 51

Ausfall eines Hauptstandorts des Netzleitsystems (B.LS.ASH) auf Seite 19
Ein Hauptstandort des Netzleitsystems ist ausgefallen.

Ausfall eines Ersatzstandorts des Netzleitsystems (B.LS.ASE) auf Seite 19
Ein Ersatzstandort des Netzleitsystems ist ausgefallen.

Ausfall eines Kommunikationsstandort des Netzleitsystems (B.LS.ASC) auf Seite 20
Ein Kommunikationsstandort des Netzleitsystems ist ausgefallen.

Ausfall aller Standorte des Netzleitsystems (B.LS.ASK) auf Seite 20
Sämtliche Standorte des Netzleitsystems sind komplett ausgefallen.

Ausfall eines Standortes des Netzleitsystems (B.LS.ASA)

Ein Standort des Netzleitsystems ist ausgefallen.

Es wurde festgestellt, dass ein Standort des Netzleitsystems nicht mehr verfügbar ist.

Der Ausfall eines Standortes des Netzleitsystems bezeichnet dabei die komplette Nichtverfügbarkeit der Technik eines Standortes. Diese Situation kann ausgelöst werden durch z.B.:

- lokale technische Störungen (z.B. Stromausfall)
- physikalische Abtrennung des Netzleitsystems von dem digitalen Übertragungsnetz
- Elementarereignisse (z.B. Brand)
- Räumung durch Behörden
- Virenbefall oder Hackerangriffe

In diesem Szenario wird die Betriebsführung durch die verbleibenden Standorte mit übernommen. Je nachdem welcher Standort betroffen ist, hat dieses Szenario mehr oder weniger starke Auswirkungen. Hierbei werden folgende Standorttypen und Vorfälle unterschieden:

- Hauptstandort
- Ersatzstandort
- Kommunikationsstandort
- Komplettausfall des Netzleitsystems

Zugehörige Beobachtungen

Ausfall eines Hauptstandorts des Netzleitsystems (B.LS.ASH) auf Seite 19
Ein Hauptstandort des Netzleitsystems ist ausgefallen.

Ausfall eines Ersatzstandorts des Netzleitsystems (B.LS.ASE) auf Seite 19
Ein Ersatzstandort des Netzleitsystems ist ausgefallen.

Ausfall eines Kommunikationsstandort des Netzleitsystems (B.LS.ASC) auf Seite 20
Ein Kommunikationsstandort des Netzleitsystems ist ausgefallen.

Ausfall aller Standorte des Netzleitsystems (B.LS.ASK) auf Seite 20
Sämtliche Standorte des Netzleitsystems sind komplett ausgefallen.

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23

Ausfall eines Hauptstandorts des Netzleitsystems (B.LS.ASH)

Ein Hauptstandort des Netzleitsystems ist ausgefallen.

Es wurde festgestellt, dass ein Hauptstandort des Netzleitsystems nicht mehr verfügbar ist.

Bei einem Ausfall des Hauptstandorts können die folgenden für die Betriebsführung relevanten Komponenten und Leitsystemarbeitsplätze betroffen sein:

- Wegfall
  - Redundanz der Leitsystemkomponenten
  - Mehrzahl der Leitsystemarbeitsplätze
- Ausfall
  - Backup-Systeme
  - An-/Abmeldesystem
  - Prozessdatenarchiv
  - Kommunikation
    - Leitstellen TK
    - Betriebsfunk (nur noch Direktkommunikation zwischen mobilen Geräten möglich, nicht jedoch über die Leitsystemarbeitsplätze)
  - Managementsysteme (*PDH*, *SDH*, *DWDM*)
  - *VNC* Anbindung für Kommunikation mit den Nahsteuerplätzen
  - *VNC* Aufschaltfunktion des Netzleitsystems
  - Installationsquelle PSI Leitsystem
  - Dateiaustausch-System für:
    - Screenshots
    - *Einsman*-Veröffentlichung,-Abrechnung,-Clearing
    - An-/Abmeldesystem Dateiaustausch
    - Störungs-/Tagesberichte
    - Mapviewer (aktuelle Versorgungsunterbrechungen)
- betriebswirtschaftliche Verluste durch nicht ausführbare Bau- und Instandhaltungs-Maßnahmen und nicht durchführbare EinsMan-Abrechnung

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Hauptstandorts (M.REA.LS-ALSH) auf Seite 108
Maßnahmen die bei Ausfall eines Hauptstandorts des Leitsystems getroffen werden müssen.

Ausfall eines Ersatzstandorts des Netzleitsystems (B.LS.ASE)

Ein Ersatzstandort des Netzleitsystems ist ausgefallen.

Es wurde festgestellt, dass ein Ersatzstandort des Netzleitsystems nicht mehr verfügbar ist.

Bei einem Ausfall eines Ersatzstandort können die folgenden für die Betriebsführung relevanten Komponenten und Leitsystemarbeitsplätze betroffen:

- Wegfall
  - Redundanz der Leitsystemkomponenten
  - Notarbeitsplätze
- Ausfall
  - Dateiaustausch-Systeme für:
    - Screenshots
    - *Einsman*-Berichte/Protokolle für den Kontext Clearing
    - Datenmodelleingabe Fernwirken
    - Störungs-/Tagesberichte
    - Wetterprognose
- betriebswirtschaftliche Verluste durch nicht ausführbare Bau- und Instandhaltungs-Maßnahmen und nicht durchführbare EisMan-Abrechnung

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.REA.LS-ALSE) auf Seite 108
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Ausfall eines Kommunikationsstandort des Netzleitsystems (B.LS.ASC)

Ein Kommunikationsstandort des Netzleitsystems ist ausgefallen.

Es wurde festgestellt, dass ein Kommunikationsstandort des Netzleitsystems nicht mehr verfügbar ist.

Bei einem Ausfall eines Kommunikationsstandort sind die folgenden für die Betriebsführung relevanten Komponenten und Leitsystemarbeitsplätze betroffen:

- Ausfall
  - Firewalls für Mobilfunk und *DSL*
  - Mobilfunkverbindungen/ *DSL*
    - Einspeisemanagement
    - Fernwirkanlagen in Ortsnetzstationen
    - Fernwirkanlagen in Schaltanlagen
    - Fernwirkanlagen in Umspannwerken
  - Anbindung Fernwartungszugänge
    - Intern
    - Dienstleister fürs Leitsystem
    - Dienstleister fürs Prozessdatennetz / Firewalls

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Kommunikationsstandorts (M.REA.LS-ALSK) auf Seite 108
Maßnahmen die bei Ausfall eines Kommunikationsstandorts des Leitsystems getroffen werden müssen.

Ausfall aller Standorte des Netzleitsystems (B.LS.ASK)

Sämtliche Standorte des Netzleitsystems sind komplett ausgefallen.

Es wurde festgestellt, dass alle Standorte des Netzleitsystems nicht mehr verfügbar sind.

Ein Komplettausfall des Netzbetriebsführungssystems tritt ein, wenn eine oder mehrere der nachstehenden Bedingungen erfüllt sind:

- schwerwiegende Fehlfunktionen (z.B. wiederholtes, unbeabsichtigtes, eigenständiges Steuern des Netzleitsystems)
- Nichtbedienbarkeit aller Leitsystemarbeitsplätze
- mangelnde Verlässlichkeit und Integrität des Prozessabbildes bzw. der Visualisierung
- Ausfall der kompletten Prozessanbindung für voraussichtlich 90 Minuten oder auf nicht absehbare Zeit

Solche Situationen können verschiedene Auslöser haben. Denkbar sind hier:

- Softwarefehler, die zu einem korrupten Netzabbild führen
- Fehler in der Datenbank Systemsoftware
- Virenbefall oder Hackerangriffe

Die für die physikalische Redundanz innerhalb des Netzleitsystems wichtige enge Kopplung aller Systemkomponenten wirkt sich für diese Szenarien insofern negativ aus, als dass auch Fehler sofort auf alle IT-Systeme übergreifen können. Im Rahmen der Ablaufpläne des Maßnahmenkatalogs ist es daher wichtig, auch einen Komplettausfall des Netzbetriebsführungssystems an allen Standorten zu betrachten.

Durch den in diesem Szenario angenommenen Ausfall des Netzbetriebsführungssystems ergeben sich die folgenden Auswirkungen auf den Geschäftsbetrieb:

- Mögliche Erdschlüsse können nicht erkannt werden und können erst nach Beginn des Notbetriebes bearbeitet werden.
- Betriebsmittelüberlastungen aufgrund dezentraler Einspeiser können nicht verhindert werden und müssen vorsorglich über die nachgelagerten Systeme manuell abgeschaltet werden.
- Störungen (inkl. Versorgungsunterbrechungen) werden erst nach Einrichtung des Notbetriebes, bzw. durch Kundenmeldung erkannt.
- Störungsbehebungszeit bei Netzstörungen ist deutlich verlängert.
- Abbruch aller Arbeiten im Netz und daraus resultierende betriebswirtschaftliche Verluste.
- Nichteinhaltung von Netzbetriebsführungsdienstleistungsverträgen und daraus resultierende Entschädigungszahlungen.

Stromversorgung der Leitstelle, Betriebsfunk und Telefonie, aktuelle Netzpläne, Alarmpläne und die nachgelagerten Systeme zur Umsetzung des Einspeisemanagements sind nicht Teil der betroffenen Infrastruktur und stehen in diesem Szenario weiterhin zur Verfügung.

Zugehörige Maßnahmen

Maßnahmen bei Komplettausfall des Leitsystems (M.REA.LS-KALS) auf Seite 109
Maßnahmen die bei einem Ausfall aller Standorte des Leitsystems getroffen werden müssen.

Ausfall Prozessdatennetze (B.LS.APN)

Die Prozessdatennetze zur Anbindung des Leitsystems sind ausgefallen.

Es wurde festgestellt, dass die Prozessdatennetze zur Anbindung des Netzleitsystems nicht mehr verfügbar sind.

Dieses Szenario behandelt den Ausfall des Prozessdatennetzes, sowie den Ausfall des Übergangs zu öffentlichen Kommunikationsnetzen, die für die Betriebsführung genutzt werden. Dadurch sind die Kommunikation der Leittechnik mit den Fernwirkanlagen in den Umspannwerken und die Kommunikation der Komponenten des Netzleitsystems nicht mehr gegeben. Außerdem ist die IP-basierte Kommunikation der Betriebsfunk Basisstationen mit der Betriebsfunk Zentrale unterbrochen. Die nachgelagerten Systeme zur Umsetzung des

Einspeisemanagements stehen in diesem Szenario nicht zur Verfügung. Dies kann zum Beispiel durch folgende Ereignisse ausgelöst werden:

- Fehlkonfigurationen von Netzwerkkomponenten
- Routing, Spanning-Tree oder sonstige Protokollfehler
- Schwerwiegende systematische Fehlfunktion von Netzwerkkomponenten (IOS Fehler)
- Virenbefall oder Hackerangriffe
- Fehler beim öffentlichen Kommunikationsnetz-Provider (z.B. S2M, APN)

Durch den in diesem Szenario angenommenen Ausfall des Betriebsdatennetzes ergeben sich die folgenden Auswirkungen auf den Geschäftsbetrieb:

- Mögliche Erdschlüsse können nicht erkannt werden und können erst nach Beginn des Notbetriebes bearbeitet werden.
- Betriebsmittelüberlastungen aufgrund dezentraler Einspeiser können nicht verhindert werden und müssen vorsorglich abgeregelt werden, falls dieses technisch noch möglich ist und wenn in Zusammenarbeit mit der Netzführung aus der Einspeiseprognose im Leitsystem noch ersichtlich ist, dass mit erhöhter EEG-Einspeisung zu rechnen ist. Im Zweifelsfall wird abgeregelt. Daraus könnten betriebswirtschaftliche Verluste durch Entschädigungszahlungen resultieren.
- Störungen (inkl. Versorgungsunterbrechungen) werden erst nach Einrichtung des Notbetriebes, bzw. durch Kundenmeldung erkannt.
- Störungsbehebungszeit bei Netzstörungen ist deutlich verlängert.
- Abbruch aller Arbeiten im Netz und daraus resultierende betriebswirtschaftliche Verluste.
- Nichteinhaltung von Netzbetriebsführungsdienstleistungsverträgen und daraus resultierende Entschädigungszahlungen.

Stromversorgung der Leitstelle, Telefonie, Netzpläne, Alarmpläne stehen über nicht betroffene Infrastruktur in diesem Szenario weiterhin zur Verfügung.

Zugehörige Beobachtungen

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23
Configuration Modification (B.BE.CoMo) auf Seite 48
Network Access Control Modification (B.BE.NACM) auf Seite 51
Malware Infection (B.AS.MIn) auf Seite 61

Zugehörige Maßnahmen

Maßnahmen bei Komplettausfall des Leitsystems (M.REA.LS-KALS) auf Seite 109
Maßnahmen die bei einem Ausfall aller Standorte des Leitsystems getroffen werden müssen.

Ausfall der Leitstellen-Telefonanlage (B.LS.AT)

Die für die Netzbetriebsführung genutzte Leistellen-Telefonanlage ist nicht mehr verfügbar.

Dieses Szenario behandelt den Ausfall der Leitstellen-Telefonanlage für die Netzbetriebsführung. Die Telefonanlage wird für die Kommunikation der Netzleitstelle mit dem Personal in den Anlagen/der Fläche zur Wahrnehmung der Aufgaben der Netzführung benötigt. Die Nutzung des Betriebsfunks über die Telefone der Netzleitstelle ist bei einem Ausfall der Leitstellen-Telefonanlage ebenfalls nicht mehr möglich.

Ein Ausfall der Leitstellen-Telefonanlage kann z.B. ausgelöst werden durch:

- Fehler seitens des Dienstleisters
- lokale technische Störungen (z.B. Stromausfall)
- Elementarereignisse (z.B. Brand)
- Virenbefall oder Hackerangriffe

Durch den in diesem Szenario angenommenen Ausfall der Leitstellen-Telefonanlage ergeben sich die folgenden Auswirkungen auf den Geschäftsbetrieb:

- Gefahrenmeldungen für laufende Arbeiten unter Spannung (>1kV) können nicht abgesetzt werden.
- Gefahrenmeldungen für laufende Arbeiten im Gas-Netz können nicht abgesetzt werden.
- Störungsbehebungszeit ist deutlich verlängert.

- Geplante Arbeiten im Netz können nicht durchgeführt werden und daraus resultierende betriebswirtschaftliche Verluste.
- Nichteinhaltung von Netzbetriebsführungsdienstleistungsverträgen und daraus resultierende Entschädigungszahlungen.
- Ausfall der Alarmierung zur Umsetzung der BDEW-Kaskade und dadurch Gefährdung der Systembilanz und Netzsicherheit.

Zugehörige Beobachtungen

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23

Malware Infection (B.AS.MIn) auf Seite 61

Zugehörige Maßnahmen

Maßnahmen bei Ausfall der Leitstellen-Telefonanlage (M.REA.LS-ALSTA) auf Seite 110
Maßnahmen die beim Ausfall der Leitstellen-Telefonanlage getroffen werden müssen.

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES)

Der Ausfall oder die Nichterreichbarkeit von Systemen kann neben Störungen in der Verbindung oder Fehlern im System selbst, auch durch einen Angriff auf das Leitsystem oder auf Systeme, die mit dem Leitsystem kommunizieren, verursacht werden.

Zugehörige Beobachtungen

Ausfall der Leitstellen-Telefonanlage (B.LS.AT) auf Seite 22
Die für die Netzbetriebsführung genutzte Leistellen-Telefonanlage ist nicht mehr verfügbar.

Ausfall Prozessdatennetze (B.LS.APN) auf Seite 21
Die Prozessdatennetze zur Anbindung des Leitsystems sind ausgefallen.

Verbindungsabbruch zu einem Fernwirkgerät (B.FWT.VAG) auf Seite 31
Zu einem einzelnen Fernwirkgerät besteht keine Verbindung mehr.

Verbindungsabbruch zu mehreren Fernwirkgeräten (B.FWT.MGKV) auf Seite 31
Zu mehreren Fernwirkgeräten besteht keine Verbindung mehr.

Zugehörige Maßnahmen

Keine oder verzögerte Reaktion von Steuerbefehlen untersuchen (M.INV.LS-KVRSU) auf Seite 87

Hohe Latenz (B.LS.HL)

Ein Nutzer stellt fest, dass ein System zwar korrekt reagiert, jedoch sehr stark verzögert. Während dies auch auf Verbindungsprobleme zurückzuführen sein kann ist es ebenfalls möglich, dass gerade ein Angriff in Gange ist, der die Kommunikationskanäle überlastet.

Zugehörige Beobachtungen

Erhöhte Systemauslastung (B.ZB.ESA) auf Seite 68

Denial of Service (B.ZB.DOS) auf Seite 67

Denial of Service (B.AS.DOS) auf Seite 61

Zugehörige Maßnahmen

Keine oder verzögerte Reaktion von Steuerbefehlen untersuchen (M.INV.LS-KVRSU) auf Seite 87

Keine Reaktion auf Steuerbefehle (B.LS.KRS)

Ein System, das nicht auf Steuerbefehle reagiert, kann neben Verbindungsproblemen oder Fehlern im System bzw. nicht definierte Steuerbefehle auch von einem Angreifer übernommen worden sein.

Zugehörige Beobachtungen

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23

Verbindungsabbruch zu einem Fernwirkgerät (B.FWT.VAG) auf Seite 31

Zu einem einzelnen Fernwirkgerät besteht keine Verbindung mehr.

Verbindungsabbruch zu mehreren Fernwirkgeräten (B.FWT.MGKV) auf Seite 31
Zu mehreren Fernwirkgeräten besteht keine Verbindung mehr.

Successful System Persistence (B.BE.SSP) auf Seite 52

System Persistence (B.BE.SyPe) auf Seite 52

Zugehörige Maßnahmen

Keine oder verzögerte Reaktion von Steuerbefehlen untersuchen (M.INV.LS-KVRSU) auf Seite 87

Nicht autorisierte Steuerbefehle (B.LS.NAS)

Ein System reagiert zwar auf Steuerbefehle, wird jedoch scheinbar von anderer Stelle auch gesteuert, da Operationen unautorisiert erkannt wurden. Dies kann neben einer Fehlfunktion des Systems auch durch einen Angriff hervorgerufen werden.

Zugehörige Beobachtungen

Command-and-Control Communication (B.AS.CCC) auf Seite 60

Reverse Shell (B.AS.RSh) auf Seite 62

System Persistence (B.BE.SyPe) auf Seite 52

Successful System Persistence (B.BE.SSP) auf Seite 52

Zugehörige Maßnahmen

Nicht autorisierte Steuerbefehle unterbinden (M.INV.LS-NASU) auf Seite 87

Automatisierte Beobachtungen

Network Anomaly (B.LS.NA)

Ein automatisiertes Sicherheitssystem meldet Netzwerk-Anomalien.

Hintergrund: Beispiele sind die Nutzung unerwarteter Ports für bestimmte Prozesse, unpassende Protokolle für bestimmte Ports, IP-Konflikte, oder Traffic, der anhand von vordefinierten Regeln als ungewöhnlich eingestuft wird. Auch Meldungen für die Nutzung von üblicherweise ungenutzten Switch-Ports oder Traffic von unbekannten IP-Adressen sind entsprechend zu bewerten. Da ein Angriff nicht ausgeschlossen werden kann, sind entsprechende Maßnahmen zu treffen.

Zugehörige Beobachtungen

Port Scan (B.AS.PSc) auf Seite 62

Denial of Service (B.AS.DOS) auf Seite 61

Zugehörige Maßnahmen

Ein- und Ausgehenden Traffic auf Anomalien untersuchen (M.INV.LS-NA-EATU) auf Seite 85

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Network Attack: ARP Spoofing (B.LS.ARP)

Ein automatisiertes Sicherheitssystem meldet, dass ein Gerät im Netzwerk ein (versuchter) ARP-Spoofing-Angriff ausgeführt wurde.

Hintergrund: Durch einen ARP-Spoofing-Angriff (Address Resolution Protocol) können Angreifende versuchen, ihre eigene Hardware-Adresse (MAC) mit einer IP-Adresse eines anderen Gerätes zu verknüpfen, um so die Kommunikation zu diesem Gerät zu unterbinden, zu manipulieren oder mitzuschneiden. Ein erkannter ARP-Spoofing-Versuch ist in den allermeisten Fällen als Angriff zu werten.

Zugehörige Beobachtungen

Denial of Service (B.AS.DOS) auf Seite 61
Lateral Movement (B.AS.LMo) auf Seite 61

Zugehörige Maßnahmen

ARP Spoofing überprüfen und unterbinden (M.INV.LS-NA-ARP) auf Seite 86
Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Network Attack: IP Spoofing (B.LS.IPS)

Ein automatisiertes Sicherheitssystem meldet, dass ein Gerät im Netzwerk eine gespoofte IP-Adresse hat.

Hintergrund: Durch vortäuschen einer anderen IP-Adresse kann ein Gerät Firewallregeln umgehen und geschützte Netzwerkbereiche erreichen.

Zugehörige Beobachtungen

Denial of Service (B.AS.DOS) auf Seite 61
Lateral Movement (B.AS.LMo) auf Seite 61

Zugehörige Maßnahmen

IP Spoofing überprüfen und unterbinden (M.INV.LS-NA-IPSU) auf Seite 86

Kapitel 3

Übertragungs- und Netzwerktechnik

Themen:

Alle Beobachtungen und Maßnahmen der Übertragungs- und Netzwerktechnik

In diesem Abschnitt finden Sie alle Beobachtungen und Maßnahmen, die die Übertragungs- und Netzwerktechnik betreffen.

Die Übertragungstechnik beinhaltet die Technologien des Kommunikationsnetzes im Prozessdatenbereich, die für die Weitverkehrsanbindung eingesetzt werden. Zu diesen zählen z. B.:

- TDM-basierende Technologien
  - PDH
  - SDH
- Packet-Dienste
  - Switche
  - Router
  - MPLS
- Wellenlängenmultiplexing
  - CWDM
  - DWDM

Zur Administration und Überwachung werden Managementsystem eingesetzt.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Das Übertragungstechnikgerät steht unter Spannung und ist betriebsbereit. (B.ÜT/NT.ÜsSb)

Das Gerät steht unter Spannung und zeigt den erwarteten Betriebszustand. Es wird mit der Überprüfung der Sendeeinheit fortgefahren.

Zugehörige Maßnahmen

Überprüfung der Sendeeinheit einer Übertragungstechnik (M.INV.ÜT/NT-ÜSÜ) auf Seite 94

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Fehler Spannungsversorgung (B.ÜT/NT.FSP)

Das Gerät ist spannungslos und nicht betriebsbereit. Es wird mit der Überprüfung der Spannungsversorgung fortgefahren.

Zugehörige Maßnahmen

Überprüfung der Spannungsversorgung (M.INV.ÜT/NT-ÜSV) auf Seite 93

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Ein Übertragungs- oder Netzwerkgerät wurde manipuliert (B.ÜT/NT.GMa)

Es wurde eine Manipulation eines oder mehrerer Geräte im Übertragungsnetz entdeckt.

Eine Manipulation kann

- Mechanische Eingriffe auf Komponenten des Netzes sowie
- Veränderungen der Konfiguration

umfassen. Hierbei kann es sich unter Umständen um einen Angriff handeln. Es sind sofortige Maßnahmen zum Schutz des Datennetzes zu treffen.

Zugehörige Beobachtungen

Configuration Modification (B.BE.CoMo) auf Seite 48

Network Access Control Modification (B.BE.NACM) auf Seite 51

Zugehörige Maßnahmen

Reaktion nach einer Manipulation in der Übertragungstechnik (M.REA.ÜT/NT-Ma) auf Seite 122

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Ein Übertragungs- oder Netzwerkgerät wurde entwendet (B.ÜT/NT.GEn)

Ein Gerät wurde entwendet und ist nicht mehr auffindbar.

Fehlt ein Gerät, ist von einem Diebstahl auszugehen. Es sind sofortige Maßnahmen zum Schutz des Datennetzes zu treffen. Es ist zu klären, ob das Gerät auf valide Weise, z.B. zu Wartungszwecken, entfernt wurde. Falls keine entsprechenden Informationen vorliegen, ist von einem Einbruch und einem potentiellen Angriff (M.INV.AGR (Seite 74)) auszugehen.

Zugehörige Maßnahmen

Reaktion nach einem Gerätediebstahl (M.REA.ÜT/NT-GDS) auf Seite 121

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Es wird ein Fremdgerät im Übertragungsnetz entdeckt (B.ÜT/NT.FGE)

Ein fremdes, nicht autorisiertes Gerät wird vor Ort oder über ein Managementsystem entdeckt.

Ein Fremdgerät kann auf eine valide, jedoch nicht dokumentierte Änderung zurückgehen oder Teil eines Angriffs auf das Netzwerk sein. Es sind sofortige Maßnahmen zum Schutz des Datennetzes zu treffen.

Zugehörige Maßnahmen

Reaktion auf die Entdeckung eines Fremdgerätes im Übertragungsnetz. (M.REA.ÜT/NT-EFG) auf Seite 122

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Die Übertragungseinheit sendet mit einem zulässigen Pegelwert, aber kein Empfangssignal (B.ÜT/NT.KES)

Da am Gerät ein Sendepegel vorhanden ist, muss der Übertragungsweg in Abschnitten überprüft werden. Die nächste Messung wäre am Kabelendverschluss und ggf. an der Gegenstelle, bis das Mess- oder Sendesignal nicht mehr messbar ist.

Zugehörige Maßnahmen

Überprüfung der Datenverkabelung (M.INV.ÜT/NT-ÜDV) auf Seite 95

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Automatisierte Beobachtungen

Bitfehler auf einer Verbindung (B.ÜT/NT.BFV)

Im Managementsystem wurden durch das Netzmanagement Bitfehler erkannt.

Im Netzmanagementcenter wurden Bitfehler erkannt. Dadurch ist die Kommunikation beeinträchtigt, aber es kommt noch nicht zu einem kompletten Ausfall.

Zugehörige Maßnahmen

Überprüfung des Zustandes des Kommunikationsnetzes (M.INV.ÜT/NT-ÜN) auf Seite 96

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS)

In Abhängigkeit von der Netztopologie muss das Fehlerbild bewertet werden:

- Standorte mit einer Anbindung (Stern- oder Baumtopologie)
  - Ein Signalverlust führt zu einem Komplettausfall des Standortes
  - Das Ausmaß des Fehlers wird durch die explizite Suche nach weiteren Ausfällen bestimmt (M.INV.WKA (Seite 92)).
  - Nach Überprüfung auf weitere Ausfälle und deren Behebung wird der lokale Ausfall durch weitere Bearbeitung durch einen Servicetechniker vor Ort behoben (M.INV.HVO (Seite 93)).

- Standorte mit mehreren Fernverbindungen (Ring- oder Maschentopologie)
  - Ein Komplettausfall deutet auf einen Geräteausfall hin. Dieser muss vor Ort untersucht werden.
    - Weitere Bearbeitung durch einen Servicetechniker
  - Teilausfall, die Übertragungsgeräte sind weiterhin managebar
    - Auswertung der Störungsinformationen.
    - Überprüfung weiterer Ausfälle. (M.INV.WKA (Seite 92))
    - Weitere Bearbeitung durch einen Servicetechniker vor Ort. (M.INV.HVO (Seite 93))

Zugehörige Maßnahmen

Überprüfung weiterer Kommunikationsausfälle im Störungszusammenhang (M.INV.WKA) auf Seite 92

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Störungsmeldungen aus dem Netzmanagementsystem (B.ÜT/NT.SNM)

Im Netzmanagementsystem werden Fehler auf WAN-Abschnitten angezeigt. Mögliche Fehlermeldungen sind:

- Eine erhöhte Fehlerrate
- Wiederholte Verbindungsabbrüche

Zugehörige Maßnahmen

Überprüfung des Zustandes des Kommunikationsnetzes (M.INV.ÜT/NT-ÜN) auf Seite 96

Kapitel 4

Fernwirktechnik

Themen:

Die Aufgabe der Fernwirktechnik besteht darin, die Netzinformationen zwischen den Schaltanlagen und einer Netzleitstelle zu übertragen. Darüber hinaus ist sie verantwortlich dafür, dass alle Anlagen aus der Distanz gesteuert werden können. Fernwirk- und Stationsleittechnik sitzt in der Regel an zentralen Punkten des Kommunikationsnetzwerkes. Die Geräte besitzen verschiedene Schnittstellen zu anderen Diensten und Herstellern, zu unterschiedlichen Komponenten sowie zum physikalischen Prozess. Die Übertragung findet häufig auch zu verschiedenen Leitstellen mehrerer Betreiber statt. Fernwirktechnik ist daher immer Teil eines Gesamtsystems. Ein IT-Angriff auf ein oder mehrere Fernwirkgeräte könnte zur Folge haben, dass falsche Messdaten übertragen werden, Anlagen ausfallen oder willkürlich angemeldet werden, wodurch ein enormer Schaden entstehen kann.

In diesem Abschnitt finden Sie alle Beobachtungen, die die Fernwirktechnik betreffen. Es wird betrachtet, wie ein kompromittiertes Fernwirkgerät erkannt werden kann, um zu verhindern, dass ein Angreifer unbemerkt vollen Zugriff auf das Fernwirkgerät hat, da dies zu Ausfällen von angeschlossenen Anlagen führen kann. Zusätzlich finden Sie in diesem Kapitel Beobachtungen, woran erkannt werden kann, dass ein Angreifer versucht, sich Zugang zu den Fernwirkgeräten zu verschaffen.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Verbindungsabbruch zu einem Fernwirkgerät (B.FWT.VAG)

Zu einem einzelnen Fernwirkgerät besteht keine Verbindung mehr.

Es wurde festgestellt, dass ein einzelnes Fernwirkgerät nicht mehr erreichbar ist.

Dies kann beispielsweise im Leitsystem festgestellt werden. Des Weiteren könnte dies ebenfalls durch Analysen innerhalb der Übertragungstechnik oder direkt vor Ort am Fernwirkgerät festgestellt worden sein.

Da eine mögliche Fehlfunktion oder Manipulation des Geräts oder der Übertragungstechnik naheliegend ist, muss dieser Vorfall weiter untersucht werden. Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Beobachtungen

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Zugehörige Maßnahmen

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU) auf Seite 82

Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Verbindungsabbruch zu mehreren Fernwirkgeräten (B.FWT.MGKV)

Zu mehreren Fernwirkgeräten besteht keine Verbindung mehr.

Es wird festgestellt, dass mehrere Fernwirkgeräte nicht mehr erreichbar sind. Dies kann beispielsweise im Leitsystem erkannt werden. Des Weiteren könnte dies ebenfalls durch Analysen innerhalb der Übertragungstechnik erkannt werden.

Da eine mögliche Fehlfunktion oder Manipulation des Geräts oder der Übertragungstechnik naheliegend ist, muss dieser Vorfall weiter untersucht werden. Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Beobachtungen

Ausfall oder Nichterreichbarkeit von Systemen (B.LS.NES) auf Seite 23

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Ein Gerät liefert unplausible Werte (B.FWT.EGUW)

Ein einzelnes Fernwirkgeräte liefert unplausible Werte

Es wird festgestellt, dass ein einzelnes Fernwirkgerät unplausible oder falsche Messwerte liefert. Dies kann beispielsweise im Leitsystem festgestellt werden. Des Weiteren könnte dies ebenfalls durch Analysen innerhalb der Leittechnik oder direkt vor Ort am Fernwirkgerät festgestellt werden.

Da eine mögliche Fehlfunktion oder Manipulation des Geräts naheliegend ist, muss dieser Vorfall weiter untersucht werden. Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Beobachtungen

Fehlinformationen im Leitsystem entdeckt (B.LS.FE) auf Seite 17

Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt

Zugehörige Maßnahmen

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU) auf Seite 82

Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Mehrere Geräte liefern unplausible Werte (B.FWT.MGUW)

Mehrere Fernwirkgeräte liefern unplausible oder falsche Werte

Es wird festgestellt, dass mehrere Fernwirkgeräte unplausible oder falsche Messwerte liefern. Dies kann durch Analysen innerhalb Leitsystems festgestellt werden.

Da eine mögliche Fehlfunktion oder Manipulation der Geräte naheliegend sind, muss dieser Vorfall weiter untersucht werden. Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Beobachtungen

Fehlinformationen im Leitsystem entdeckt (B.LS.FE) auf Seite 17
Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt

Zugehörige Maßnahmen

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU) auf Seite 82
Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Quelle von Fehlinformationen im Leitsystem untersuchen (M.INV.LS-FLSU) auf Seite 84
Die Quelle von Fehlinformationen oder unplausiblen Messwerten soll untersucht werden.

Ein Gerät ist defekt (B.FWT.EGD)

Ein einzelnes Fernwirkgerätes ist defekt

Es wird festgestellt, dass ein einzelnes Fernwirkgerät defekt ist.

Der Defekt kann verschiedene Ursache haben und durch die Fehlerdiagnosen von der Parametriersoftware erkannt werden.

Um den Fehler zu beheben sollte die entsprechende Baugruppe ausgetauscht werden. Darüber hinaus Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Maßnahmen

Reparatur eines defekten Fernwirkgeräts (M.REA.FWT-RDG) auf Seite 105
Ein einzelnes Fernwirkgerät meldet sich mit Fehlermeldung.

Die Konfiguration eines Fernwirkgerätes wurde manipuliert (B.FWT.KGM)

Unautorisierte Veränderung der Konfiguration.

Die Konfiguration eines Gerätes ist unautorisiert verändert worden. Das führt dazu, dass unplausible oder falsche Messwerte in das Leitsystem geliefert werden können. Dies kann in der Fernwirk-Leittechnik durch den Vergleich der Datenmodellstände festgestellt werden.

Da eine mögliche Fehlfunktion oder Manipulation des Gerätes naheliegend ist, nach der Feststellung einer Differenz in den Datenmodellen muss dieser Vorfall weiter untersucht werden. Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Beobachtungen

Configuration Modification (B.BE.CoMo) auf Seite 48

Zugehörige Maßnahmen

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU) auf Seite 82
Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Falsche Firmware-Prüfsumme (B.FWT.FFPS)

Die Prüfsumme der Firmware eines Systems entspricht nicht der erwarteten.

Hintergrund: Prüfsummen können verwendet werden, um die Integrität von Software zu verifizieren. Eine falsche Prüfsumme bedeutet, dass die Software fehlerhaft ist oder manipuliert wurde.

Zugehörige Maßnahmen

Verdächtige Firmware (M.REA.FWT-VFU) auf Seite 105

Falsche Firmware-Version (B.FWT.FFW)

Die Firmwareversion eines Systems entspricht nicht der erwarteten.

Hintergrund: Die Firmware ist entweder veraltet, oder wurde möglicherweise von einer nicht-autorisierten Person oder einem Angreifer installiert.

Zugehörige Maßnahmen

Firmware Version überprüfen (M.REA.FWT-FWU) auf Seite 107

Nicht-Plausible Anmeldung von Anlagen (B.FWT.NPAA)

Energieressourcen oder ähnliche Anlagen werden unter falschem Namen oder mit anderweitig unplausiblen Anmeldedaten angemeldet.

Hintergrund: Dies deutet darauf hin, dass ein Angreifer sich eine Testanlage aufbaut, um sie zu hacken und daraus Informationen über das Gesamtsystem zu erlangen. Um unerkannt zu bleiben, gibt er falsche Anmeldedaten an.

Zugehörige Maßnahmen

Nicht-Plausible Anmeldung von Anlagen untersuchen (M.INV.FWT-NPAAU) auf Seite 84

Unerwartete Neustarts (B.FWT.UNS)

Ein System wurde ungeplant neugestartet.

Hintergrund: Speziell bei eingebetteten Systemen ist für neue Firmware häufig ein Neustart notwendig. Ein unerwarteter Neustart kann demnach durch eine unautorisierte Softwareinstallation hervorgerufen werden. Ebenfalls kann ein unerwarteter Neustart auf einen MitM (Man in the Middle) Angriff hindeuten.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61

Hacking Tool detected

Zugehörige Maßnahmen

Unerwartete Neustarts untersuchen (M.INV.FWT-UNS) auf Seite 84

Ein Gerät liefert unplausible Werte, obwohl es keine Auffälligkeiten bei ihm gibt (B.FWT.EGUWKA)

Leitsystem empfängt unplausible Werte von einem Fernwirkgerät, welches bei der Überprüfung aber keine Fehler oder Manipulationen aufwies.

Das Leitsystem empfängt unplausible oder falsche Messwerte eines einzelnes Fernwirkgerät. Dieses wurde aber bereits überprüft und wies keine Auffälligkeiten oder Fehler auf. Da das Fernwirkgerät als Ursache ausgeschlossen worden ist, müssen die Messwerte entweder auf dem Übertragungsweg oder bei der Verarbeitung im Leitsystem verfälscht worden sein.

Da eine mögliche Fehlfunktion oder Manipulation des Leitsystems oder des Prozessdatennetzes naheliegend ist, muss dieser Vorfall weiter untersucht werden. Hierzu können die unten verlinkten Maßnahmen genutzt werden.

Zugehörige Beobachtungen

Fehlinformationen im Leitsystem entdeckt (B.LS.FE) auf Seite 17
Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt

Zugehörige Maßnahmen

Quelle von Fehlinformationen im Leitsystem untersuchen (M.INV.LS-FLSU) auf Seite 84
Die Quelle von Fehlinformationen oder unplausiblen Messwerten soll untersucht werden.

Automatisierte Beobachtungen

Default Credentials (B.FWT.DC)

Ein automatisiertes Sicherheitssystem meldet einen Loginversuch mit Default-Zugangsdaten.

Hintergrund: In der Regel sollten die Default-Credentials deaktiviert sein (und alle berechtigten Personen sollten dies auch wissen), für einen Angreifer ist es aber ein sehr einfacher Versuch, Zugang zu bekommen (und nicht alle Ziele haben sie tatsächlich deaktiviert).

Zugehörige Beobachtungen

Successful Brute Force Authentication (B.AS.SBFA) auf Seite 63

Zugehörige Maßnahmen

Login mit Default Credentials unterbinden (M.REA.FWT-LDCU) auf Seite 105

Kapitel 5

Sicherheitsfaktor Mensch

Themen:

Da das Fehlen von grundlegenden IT-Sicherheitskenntnissen bei Angestellten oftmals zu einem erfolgreichen IT-Angriffe führen kann, sollte der Mensch genauso wie die anderen Teilsysteme, als Sicherheitsrisiko eingestuft werden.

Daher finden Sie in diesem Abschnitt alle Beobachtungen, deren Angriffsziel die Angestellten sind. Dabei werden sowohl technische Angriffe auf die Angestellten betrachtet, als auch Angriffe im Kontext von Social Engineering. Bei den technischen Angriffen, werden Angriffe im Kontext von Phishing betrachtet, die bei einem Angestellten ohne grundlegende IT-Kenntnisse besonders gefährlich sind, da oftmals ahnungslos auf einen Phishing-Versuch eingegangen wird. Im nicht-technischen Kontext werden unterschiedliche Arten des Social Engineerings betrachtet, da dieser Angriff sich immer mehr einer Beliebtheit erfreut und bei stetig wachsenden Unternehmen schwer zu durchschauen ist.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Beobachten relevanter Orte oder Abläufe (B.SFM.BRO)

Eine Person, ein Fahrzeug oder eine Drohne erweckt den Eindruck, relevante Orte oder Abläufe zu beobachten.

Hintergrund: Das Beobachten von Abläufen und Sicherheitsvorkehrungen kann Vorbereitung auf ein physisches Eindringen sein, da vorab geplant werden kann, wie Sicherheitsvorkehrungen umgangen werden.

Zugehörige Beobachtungen

Physische Eindringversuche (B.SFM.PEV) auf Seite 37

Zugehörige Maßnahmen

Verdächtige Personen vor dem Firmen Gelände entdeckt (M.INV.SFM-VPVFGE) auf Seite 88

Physische Eindringversuche (B.SFM.PEV)

Ein Angreifer versucht, physisch in geschützte Bereiche einzudringen. Neben einem klassischen Einbruch wird auch häufig versucht, sich als Mitarbeiter oder Kontraktor (inkl. Reparaturkräfte oder Reinigungskräfte) auszugeben, um offen Zutritt gewährt zu bekommen, oder zumindest nicht aufgehalten zu werden.

Hintergrund: In vielen Situationen ist physischer Zugriff auf ein System der einfachste Weg, es zu manipulieren.

Zugehörige Beobachtungen

Physische Eindringversuche (B.SFM.PEV) auf Seite 37

Zugehörige Maßnahmen

Unautorisierte physische Eindringversuche (M.REA.SFM-UPEV) auf Seite 124

Physisches Eindringen (B.SFM.PE)

Eine unbekannte Person, und somit ein potentieller Angreifer, ist in geschützte Bereiche eingedrungen.

Hintergrund: In vielen Situationen ist physischer Zugriff auf ein System der einfachste Weg es zu manipulieren.

Zugehörige Beobachtungen

Schadsoftwarepayload durch Infizierte Peripherie (B.SFM.SSIP) auf Seite 38
Ein Übertragungs- oder Netzwerkgerät wurde entwendet (B.ÜT/NT.GEn) auf Seite 27

Zugehörige Maßnahmen

Unautorisierte physische Eindringversuche (M.REA.SFM-UPEV) auf Seite 124

Peripheriegerät mit ungeklärter Herkunft (B.SFM.GUH)

Im Arbeitsumfeld wurde ein Peripheriegerät (USB-Stick, Tastatur, etc.), dessen Herkunft nicht geklärt werden konnte.

Hintergrund: Allgemein sollten Peripheriegeräte mit ungeklärter Herkunft nicht an Arbeitsrechnern angesteckt werden, da diese Schadsoftware enthalten können oder auch dauerhaft das System physisch beschädigen können. Nutzer können allerdings in manchen Fällen bewegt werden, sich dieser Vorsichtsmaßnahme zu widersetzen, beispielsweise bei Geräten, die sie für die eigenen halten, oder hochwertigen Geschenken.

Zugehörige Maßnahmen

Ordnungsgemäße Handlung beim Fund von unbekannten Peripheriegeräten (M.INV.SFM-OHFVP) auf Seite 89

Phishing (B.SFM.Pi)

Ein Nutzer wird Ziel eines Phishing-Angriffs.

Hintergrund: Bei Phishing Angriffen wird versucht, einem Nutzer vertrauliche Informationen wie z.B. Zugangsdaten zu entlocken, oder ihn unbewusst Schadsoftware installieren zu lassen. Es gibt verschiedene Methoden, wie Phishing Angriffe stattfinden können. Die meisten Phishing Methoden haben aber gemeinsam, dass ein Systemnutzer entweder aufgefordert wird vertrauliche Informationen einzugeben oder eine bestimmte Datei bzw. einen bestimmten Link zu öffnen.

Zugehörige Beobachtungen

Unberechtigte Personen können vertrauliche oder interne Informationen einsehen (B.SFM.UPVI) auf Seite 40
Vertrauliche oder interne Informationen (auf dem Rechner, Schreibtisch oder Bildschirm / am Drucker, Flipchart oder Whiteboard / auf Reisen) sind für unberechtigte Personen im Zugriff oder unberechtigte Personen haben die Möglichkeit zur Einsicht auf vertrauliche oder interne Informationen.

Credentials Stolen and Leaked (B.SFM.ACSL) auf Seite 42

Links in E-Mails (B.SFM.UL) auf Seite 41
Links in E-Mails nur mit Sorgfalt öffnen

Schadsoftwarepayload durch Spear Phishing (B.SFM.SSSP) auf Seite 38

Credential Abuse (B.BE.CrAb) auf Seite 48

Zugehörige Maßnahmen

Phishing überprüfen und gegebenenfalls Auswirkung untersuchen (M.INV.SFM-PUAU) auf Seite 89

Schadsoftwarepayload durch Infizierte Peripherie (B.SFM.SSIP)

Im Arbeitsumfeld wurde ein Peripheriegerät (USB-Stick, Tastatur, etc.) entdeckt, dessen Herkunft nicht geklärt werden konnte und auf dem spezifische, auf das System zugeschnittene, Schadsoftware gefunden werden konnte.

Hintergrund: Allgemein sollten Peripheriegeräte mit ungeklärter Herkunft nicht an Arbeitsrechnern angesteckt werden, da diese Schadsoftware enthalten können oder auch dauerhaft das System physisch beschädigen können. Nutzer können allerdings in manchen Fällen bewegt werden, sich dieser Vorsichtsmaßnahme zu widersetzen, beispielsweise bei Geräten, die sie für die eigenen halten, oder bei hochwertigen Geschenken.

Zugehörige Maßnahmen

Ordnungsgemäße Handlung beim Fund von unbekannten Peripheriegeräten (M.INV.SFM-OHFVP) auf Seite 89

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Schadsoftwarepayload durch Spear Phishing (B.SFM.SSSP)

Ein Nutzer wird Ziel eines Phishing-Versuchs mit spezifischem, auf das System zugeschnittenem, Schadsoftwarepayload.

Hintergrund: Beim Spear Phishing handelt es sich um Phishing mit dem Zusatz, dass die Phishing Angriffe auf das Opfer zugeschnitten sind. Nachdem ein Angreifer also genug Informationen gesammelt hat, kann er Software

entwickeln, die genau auf sein Zielsystem zugeschnitten ist, und sie beispielsweise per Phishing-Nachricht auf das Zielsystem bringen.

Zugehörige Beobachtungen

Phishing (B.SFM.Pi) auf Seite 38

Zugehörige Maßnahmen

Phishing überprüfen und gegebenenfalls Auswirkung untersuchen (M.INV.SFM-PUAU) auf Seite 89

Rechner (PC oder Notebook) ist unbeaufsichtigt und/oder frei zugänglich (B.SFM.PCO)

Auf PC oder Notebook sind der Schreibtisch (Desktop) und die Ordner, Dokumente, Bilder u.s.w. zu sehen

Ein Bediener hat auf einem PC oder Notebook beobachtet, dass der Schreibtisch (Desktop) und die Ordner, Dokumente, Bilder u.s.w. zu sehen und somit frei zugänglich sind.

Diese Beobachtung kann sowohl auf einem fremden Computer als auch auf dem eigenen PC oder Notebook gemacht werden.

Zugehörige Beobachtungen

Unberechtigte Personen können vertrauliche oder interne Informationen einsehen (B.SFM.UPVI) auf Seite 40
Vertrauliche oder interne Informationen (auf dem Rechner, Schreibtisch oder Bildschirm / am Drucker, Flipchart oder Whiteboard / auf Reisen) sind für unberechtigte Personen im Zugriff oder unberechtigte Personen haben die Möglichkeit zur Einsicht auf vertrauliche oder interne Informationen.

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Rechner sperren (M.KOM.SFM-PCS) auf Seite 73
Rechner sind zu sperren, sobald der Arbeitsplatz verlassen wird, um einen unautorisierten Zugriff auf den Rechner und darin gespeicherte Informationen zu verhindern.

Es ist darauf zu achten, dass keine unberechtigten Personen Zugriff oder Einsicht in vertrauliche Informationen erhalten. (M.REA.ORG-SV) auf Seite 112
Überprüfung

Datenträger (Externe Festplatten, USB-Sticks, DVD, SSD) sind unbeaufsichtigt (B.SFM.DO)

Datenträger (Externe Festplatten, USB-Sticks, DVD, SSD) sind unbeaufsichtigt

Ein Bediener hat beobachtet, dass externe Festplatten, USB-Sticks, DVD, SSD oder sonstige Datenträger rumliegen und somit frei zugänglich sind.

Zugehörige Beobachtungen

Unberechtigte Personen können vertrauliche oder interne Informationen einsehen (B.SFM.UPVI) auf Seite 40
Vertrauliche oder interne Informationen (auf dem Rechner, Schreibtisch oder Bildschirm / am Drucker, Flipchart oder Whiteboard / auf Reisen) sind für unberechtigte Personen im Zugriff oder unberechtigte Personen haben die Möglichkeit zur Einsicht auf vertrauliche oder interne Informationen.

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Es ist darauf zu achten, dass keine unberechtigten Personen Zugriff oder Einsicht in vertrauliche Informationen erhalten. (M.REA.ORG-SV) auf Seite 112
Überprüfung

Verlust von Schlüsseln, Transpondern, Token oder Firmenausweisen (B.SFM.VST)

Ein Mitarbeiter stellt fest, dass er Zugangsmittel, wie bzw. Schlüsseln, Transpondern, etc. verloren hat.

Ein Mitarbeiter stellt fest, dass er seine Zugangsmittel für Unternehmens IT bzw. Unternehmens-Liegenschaften verloren hat. Dazu zählen z.B.:

- Token für den Fernzugang
- Schlüssel bzw. Transponder zum Zugang zu Liegenschaften des Unternehmens
- Firmenausweis

Zugehörige Maßnahmen

Vorgehen bei Verlust von Zugangsmitteln (M.REA.SFM-VVZ) auf Seite 125

Unberechtigte Personen können vertrauliche oder interne Informationen einsehen (B.SFM.UPVI)

Vertrauliche oder interne Informationen (auf dem Rechner, Schreibtisch oder Bildschirm / am Drucker, Flipchart oder Whiteboard / auf Reisen) sind für unberechtigte Personen im Zugriff oder unberechtigte Personen haben die Möglichkeit zur Einsicht auf vertrauliche oder interne Informationen.

Ein Bediener hat auf einem PC oder Notebook, auf einem Schreibtisch oder Bildschirm, am Drucker, Flipchart oder Whiteboard oder auf Reisen beobachtet das vertrauliche oder interne Informationen für unberechtigte Personen im Zugriff sind. Oder diese unberechtigten Personen haben die Möglichkeit zur Einsicht auf vertrauliche oder interne Informationen. Beispiele hierfür sind: Passwörter werden ausgespäht, z.B. durch Schulterblick, oder Pläne mit vertraulichen Informationen (z.B. IP-Adressen) liegen offen aus.

Zugehörige Beobachtungen

Phishing (B.SFM.Pi) auf Seite 38

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Es ist darauf zu achten, dass keine unberechtigten Personen Zugriff oder Einsicht in vertrauliche Informationen erhalten. (M.REA.ORG-SV) auf Seite 112
Überprüfung

Datenträger (Externe Festplatten, USB-Sticks, DVD, SSD) sind unbeaufsichtigt (B.SFM.DO)

Datenträger (Externe Festplatten, USB-Sticks, DVD, SSD) sind unbeaufsichtigt

Ein Bediener hat beobachtet, dass externe Festplatten, USB-Sticks, DVD, SSD oder sonstige Datenträger rumliegen und somit frei zugänglich sind.

Zugehörige Beobachtungen

Unberechtigte Personen können vertrauliche oder interne Informationen einsehen (B.SFM.UPVI) auf Seite 40
Vertrauliche oder interne Informationen (auf dem Rechner, Schreibtisch oder Bildschirm / am Drucker, Flipchart oder Whiteboard / auf Reisen) sind für unberechtigte Personen im Zugriff oder unberechtigte Personen haben die Möglichkeit zur Einsicht auf vertrauliche oder interne Informationen.

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Es ist darauf zu achten, dass keine unberechtigten Personen Zugriff oder Einsicht in vertrauliche Informationen erhalten. (M.REA.ORG-SV) auf Seite 112
Überprüfung

Links in E-Mails (B.SFM.UL)

Links in E-Mails nur mit Sorgfalt öffnen

Ein Mitarbeiter hat in einer EMail unbekannte oder merkwürdige Links erhalten.

Es darf nur auf bekannte Links geklickt werden. Im Zweifelsfall kontaktieren Sie Ihren zuständigen Sicherheitsansprechpartner oder Hotline.

Zugehörige Beobachtungen

Phishing (B.SFM.Pi) auf Seite 38

Räume sind unverschlossen (B.SFM.RNV)

Räume sind unverschlossen

Es wurde festgestellt, dass ein oder mehrere Räume, die verschlossen sein sollten, unverschlossen sind. Gegebenenfalls haben Sie sogar gesehen, welcher Kollege vergessen hat diesen Raum abzuschließen. In diesem Fall weisen Sie in analog zu unten verknüpfter Maßnahme auf sein Fehlverhalten hin. Falls der Verdacht besteht, dass die Tür bereits längere Zeit unverschlossen war, müssen Vorkehrungen getroffen werden, um einen physischen Eindringversuch auszuschließen.

Hintergrund: Für sensible Bereiche gilt eine Schlüsselordnung, die vorgibt welche Räume verschlossen sein müssen und wer Zugang zu diesen Räumlichkeiten hat.

Hintergrund: In vielen Situationen ist physischer Zugriff auf ein System der einfachste Weg, es zu manipulieren.

Zugehörige Beobachtungen

Physische Eindringversuche (B.SFM.PEV) auf Seite 37

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Vertrauliche E-Mails sind nicht verschlüsselt (B.SFM.VENV)

Vertrauliche E-Mails sind nicht verschlüsselt

Ein Bediener hat auf einem PC oder Notebook beobachtet, dass vertrauliche E-Mails nicht verschlüsselt wurden.

Diese Beobachtung kann sowohl auf einem fremden Computer als auch auf dem eigenen PC oder Notebook gemacht werden.

Zugehörige Beobachtungen

Klassifikationsstufen (B.ORG.KS) auf Seite 55
Klassifikationsstufen für die Einstufung der Vertraulichkeit von Unterlagen.

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Es ist darauf zu achten, dass keine unberechtigten Personen Zugriff oder Einsicht in vertrauliche Informationen erhalten. (M.REA.ORG-SV) auf Seite 112
Überprüfung

Unbekannte Personen/Besucher im Gebäude ohne Ausweis/Besucherausweis (B.SFM.UPE)

Unbekannte Personen/Besucher im Gebäude ohne Ausweis/Besucherausweis ansprechen

Eine unbekannte Person wurde auf dem Firmengelände entdeckt und angesprochen. Nach Aufforderung konnte sie sich nicht mit einem Firmen- oder Besucherausweis ausweisen.

Zugehörige Maßnahmen

Unautorisierte physische Eindringversuche (M.REA.SFM-UPEV) auf Seite 124

Automatisierte Beobachtungen

Credentials Stolen and Leaked (B.SFM.ACSL)

Ein automatisiertes Sicherheitssystem meldet *Credentials Stolen and Leaked*, das heißt im Internet wurden Zugangsdaten für eigene Systeme veröffentlicht.

Zugehörige Beobachtungen

Phishing (B.SFM.Pi) auf Seite 38

Schadsoftwarepayload durch Spear Phishing (B.SFM.SSSP) auf Seite 38

Zugehörige Maßnahmen

Accounts mit gestohlenen Zugangsdaten sperren (M.REA.SFM-AZS) auf Seite 124

Phishing: automatisierte Erkennung (B.SFM.PAE)

Ein automatisiertes Sicherheitssystem meldet einen Phishing-Versuch.

Hintergrund: Diese Meldung kann darauf hindeuten, dass ein Angreifer versucht unautorisierten Zugang zu einem System zu bekommen. Phishing ist eine der effektivsten Wege, den gewünschten Zugang zu einem System zu bekommen. Auf ein bestimmtes Ziel zugeschnittene Phishing-Versuche (inkl. Physischen, wie z.B. herumliegenden USB-Sticks) weisen auf einen gezielten Angriff hin.

Zugehörige Beobachtungen

Phishing (B.SFM.Pi) auf Seite 38

Schadsoftwarepayload durch Spear Phishing (B.SFM.SSSP) auf Seite 38

Links in E-Mails (B.SFM.UL) auf Seite 41

Links in E-Mails nur mit Sorgfalt öffnen

Zugehörige Maßnahmen

Phishing Versuche untersuchen und Mitarbeiter über die Gefahr informieren (M.REA.SFM-PVUMI) auf Seite 123

Successful Phishing: automatisierte Erkennung (B.SFM.SPAE)

Ein automatisiertes Sicherheitssystem meldet erfolgreiches Phishing, das heißt der Rechner eines Nutzers wurde erfolgreich von einem Angreifer infiziert.

Hintergrund: Phishing ist einer der effektivsten Wege, den gewünschten Zugang zu einem System zu bekommen. Auf ein bestimmtes Ziel zugeschnittene Phishing-Versuche (inkl. Physischen, wie z.B. herumliegenden USB-Sticks) weisen auf einen gezielten Angriff hin.

Zugehörige Maßnahmen

Vorgehen bei Successful Phishing: automatisierte Erkennung (M.REA.SFM-VSPAE) auf Seite 124

Kapitel 6

IT-Infrastruktur

Themen:

Das Backend umfasst alle Systeme, die nicht Teil des Leitsystems oder der Fernwirkgeräte sind, wie beispielsweise Prognose- oder Tradingmodule. Kurzgesagt stellt das Backend die serverseitige Implementierung des Systems, sowie die IT-Infrastruktur dar. Dadurch ist das Backend mit anderen Teilsystemen entweder direkt oder indirekt verbunden. Ein Beispiel für eine indirekte Verbindung, stellt die Verbindung zu den Fernwirkgeräten dar. Die Verbindung zu einem Leitsystem stellt dagegen eine direkte Verbindung dar. Durch die direkte Verbindung zu einem Leitsystem, ist es möglich mit Remote Zugriffen via SSH das System aktiv zu steuern oder auch zu verändern. Die IT-Infrastruktur bei Energienetzunternehmen stellt das Netzwerk dar, mit dem Office-Geräte oder Enterprise Resource Planing (ERP) Systeme verbunden sind. Durch die Verbindung zu einem zentralen Netzwerk, ist es möglich, mit den angebundenen Geräten, auf Firmen interne Daten zuzugreifen oder auch Daten unter den angebundenen Geräten auszutauschen. Ein Angreifer wäre durch ein Eindringen in das Backend somit in der Lage enormen Schaden anzurichten, da fast alle Teilsysteme Abhängigkeiten zum Backend haben und da IT-Angriffe auf die IT-Infrastruktur meistens zum Ziel haben Firmen interne Daten abzugreifen, wodurch die betroffenen Unternehmen sehr stark an Vertrauen verlieren.

In diesem Abschnitt finden Sie alle Beobachtungen, die das Backend betreffen. Es werden Beobachtungen zu unterschiedlichen Eindringversuchen eines Angreifers gemacht, um einen Großteil von Eindringversuchen frühzeitig erkennen zu können. Beispielsweise werden Brute-Force-Versuche oder die Ausnutzung einer SSH-Schwachstelle aufgeführt. Zudem wird betrachtet, wie ein aktiver Angriff und wie ein kompromittiertes System erkannt werden können. Dabei werden ebenfalls unterschiedliche Angriffsmethoden abgedeckt. So kann ein kompromittiertes System unter anderem daran erkannt werden, wenn Hacking-Tools von einem automatisierten Sicherheitssystem erkannt werden oder wenn Spuren von gelöschten Logs gefunden wurden.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Diskrepanz zwischen Daten und Messwerten (B.BE.DDM)

Eine Energieressource übermittelt andere Leistungsaufname-/abgabedaten als im System gemessen werden.

Hintergrund: Ein Angreifer könnte versuchen, mittels dieser Daten eine Reaktion hervorzurufen, die durch die falsifizierte Ausgangslage die Systemstabilität beeinträchtigt.

Zugehörige Beobachtungen

Fehlinformationen im Leitsystem entdeckt (B.LS.FE) auf Seite 17
Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt

Zugehörige Maßnahmen

Ursprung von Wiederkehrender Schadsoftware unterbinden (M.REA.BE-WSU) auf Seite 104

Diskrepanz zwischen Vorhersagen und Messwerten (B.BE.DVM)

Die aus vorherigen Nutzungsdaten und Wetterdaten errechneten Vorhersagen liegen signifikant über oder unter den tatsächlichen. Dies spricht für entweder einen Fehler im System oder eine Ausnahmesituation, die ein stark verändertes Nutzerverhalten bewirkt.

Zugehörige Beobachtungen

Fehlinformationen im Leitsystem entdeckt (B.LS.FE) auf Seite 17
Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt

Zugehörige Maßnahmen

Diskrepanz zwischen Vorhersagen und Messwerten untersuchen (M.INV.BE-DVMU) auf Seite 80

Unerwartete Benutzer (B.CIT.UB)

Beim Auflisten aller Nutzer auf dem System wird die Existenz eines unerwarteten Nutzers festgestellt.

Hintergrund: In Unix-Betriebssystemen werden beispielsweise alle Nutzer auch Systemnutzer in der passwd Datei unter /etc/passwd hinterlegt. Wenn ein unerwarteter Nutzer festgestellt wird, könnte das ein Indiz sein, dass ein Angreifer Zugriff auf das System hat.

Zugehörige Maßnahmen

Unerwartete Benutzer und dessen Aktivitäten überprüfen (M.INV.CIT-UBAU) auf Seite 81

Unerwartete Rechte bei einem Benutzer (B.CIT.URB)

Es werden unerwartete Rechte bei einem Nutzer oder eine Gruppe von Nutzern im System festgestellt.

Hintergrund: Anstatt bei einem Angriff neue Nutzer zu erstellen kann ein bestehender, unprivilegierter Nutzer übernommen werden, und ihm oder seiner Gruppe durch eine Sicherheitslücke Administratorrechte gegeben werden.

Zugehörige Beobachtungen

Brute Force Permission Enumeration (B.BE.BFPE) auf Seite 47

Privilege Escalation (B.BE.PrEs) auf Seite 51

Zugehörige Maßnahmen

Unerwartete Rechte bei einem Benutzer überprüfen (M.INV.CIT-URBU) auf Seite 81

Automatisierte Beobachtungen

Access Control Modification (B.BE.ACM)

Ein automatisiertes Sicherheitssystem meldet unerwartete Änderungen in Sicherheitseinstellungen (Access Control), speziell Abschwächungen.

Hintergrund: Diese Meldung kann auf einen Angreifer hindeuten, der sich das Eindringen erleichtern möchte. Beispiele sind die Deaktivierung von Zwei-Faktor-Authentifizierung, Änderungen der Passwortwiederherstellung oder das Freigeben von Daten für Benutzergruppen.

Zugehörige Beobachtungen

Security Tools Disabled (B.BE.STD) auf Seite 52

Configuration Modification (B.BE.CoMo) auf Seite 48

Zugehörige Maßnahmen

Unerwartete Änderungen der Sicherheitseinstellungen untersuchen (M.INV.BE-USEU) auf Seite 75

Account Manipulation (B.BE.AM)

Ein automatisiertes Sicherheitssystem meldet Account-Manipulationen wie das Erstellen/Löschen vieler Accounts oder Gruppen, insbesondere von Gästeaccounts.

Hintergrund: Ein Angreifer kann versuchen, durch diese großflächigen Änderungen Konstellationen zu finden, die ihm die benötigten Rechte geben, und gleichzeitig die Arbeit der Verteidigung zu erschweren.

Zugehörige Beobachtungen

Anomalous User Behavior: Account Deletion (B.BE.AUB-AD) auf Seite 46

Anomalous User Behavior: Account Manipulation (B.BE.AUB-AM) auf Seite 47

Zugehörige Maßnahmen

Account auf Manipulationen untersuchen (M.INV.BE-AMU) auf Seite 76

Anomalous User Behavior: Account Deletion (B.BE.AUB-AD)

Ein automatisiertes Sicherheitssystem meldet, dass ein neu erstellter Account ältere Accounts gelöscht hat.

Hintergrund: Ein Angreifer kann dadurch eine Reaktion erschweren, indem er den Administratoren den Zugriff auf das angegriffene System blockiert.

Zugehörige Maßnahmen

Reaktion auf anomale Account Löschungen (M.REA.CIT-AUB-ADU) auf Seite 99

Reaktion auf Anomales Login Verhalten (M.REA.BE-AUB-LVU) auf Seite 99

Anomalous User Behavior: Account Manipulation (B.BE.AUB-AM)

Ein automatisiertes Sicherheitssystem meldet anhand von vordefinierten Regeln anomales Nutzerverhalten. Dieses Verhalten bezieht sich vor allem auf sicherheitsrelevante Funktionen wie Nutzererstellung oder Nutzerlöschung oder mehrmalige Passwortresets.

Hintergrund: Aufgrund des untypischen Verhaltens besteht der Verdacht, dass der Account kompromittiert wurde.

Zugehörige Maßnahmen

Anomales Nutzerverhalten untersuchen (M.INV.BE-AUB-AMU) auf Seite 76

Anomalous User Behavior: Unexpected Login Behavior (B.BE.AUB-UL)

Ein automatisiertes Sicherheitssystem meldet anhand von vordefinierten Regeln Anomalien im Nutzerverhalten, wie z.B. Logins von unerwarteten Geolocations, mehrfach gescheiterte Logins, oder Loginversuche in nicht existierenden Accounts bzw. nicht vorhandenen Account-Namen.

Hintergrund: Die genannten Verhaltensweisen können auf eine erfolgreiche Kompromittierung eines Accounts hinweisen. Generell sind alle oben genannten Aktivitäten, potentielle Hinweise darauf, dass es sich hierbei nicht um eine echte Person handelt oder um einen Angreifer, der sich für eine Person ausgibt.

Zugehörige Beobachtungen

Credential Abuse (B.BE.CrAb) auf Seite 48
Successful Brute Force Authentication (B.AS.SBFA) auf Seite 63

Zugehörige Maßnahmen

Reaktion auf Anomales Login Verhalten (M.REA.BE-AUB-LVU) auf Seite 99

Anonymous Channel (B.BE.AC)

Ein automatisiertes Sicherheitssystem meldet die Verwendung von TOR (Anonymisierungsnetzwerk) oder Proxy-Diensten.

Hintergrund: Diese Dienste verschleiern den Webtraffic, wodurch ein Angreifer unerkannt bleiben kann. Nachdem die Nutzung dieser Dienste im Arbeitskontext eher unüblich ist, ist dies ein starkes Indiz für einen Angriff.

Zugehörige Maßnahmen

Aufbau eines Anonymous Channel überprüfen (M.REA.BE-AACU) auf Seite 100

Brute Force Permission Enumeration (B.BE.BFPE)

Ein automatisiertes Sicherheitssystem meldet eine Brute Force Permission Enumeration.

Hintergrund: Es wurde detektiert, dass ein Nutzer wiederholt zufällige Operationen ausführt, für die der Nutzer keine Berechtigungen hat. Dieses Verhalten kann darauf hindeuten, dass ein Angreifer versucht, herauszufinden, welcher Nutzer welche Berechtigungen hat.

Zugehörige Beobachtungen

Privilege Escalation (B.BE.PrEs) auf Seite 51
Unerwartete Rechte bei einem Benutzer (B.CIT.URB) auf Seite 45

Zugehörige Maßnahmen

Unautorisierte Versuche Systemrechte auszuweiten unterbinden (M.INV.BE-BF-USRAU) auf Seite 77

Bulk Data Replication (B.BE.BDR)

Ein automatisiertes Sicherheitssystem meldet (unerwartete) große Datenkopien oder Datenbank-Snapshots.

Hintergrund: Diese Meldung kann auf Datendiebstahl hindeuten, speziell, wenn sie von unerwarteten Personen oder zu unerwarteten Zeiten durchgeführt werden. Hierfür nutzt ein automatisiertes Sicherheitssystem neben einer Echtzeitanalyse zusätzlich vordefinierte Regeln, um während des Regelbetriebs Anomalien zu erkennen und diese zu melden.

Zugehörige Beobachtungen

Data Exfiltration (B.BE.DaEx) auf Seite 49

Zugehörige Maßnahmen

System auf Datendiebstahl überprüfen (M.INV.BE-KGDU) auf Seite 77

Code Execution (B.BE.CE)

Ein automatisiertes Sicherheitssystem meldet unerwartete, oder von unerwarteten Prozessen gestartete, Scripts und Prozesse.

Hintergrund: Diese Meldung kann darauf hindeuten, dass eine Schwachstelle, die das Ausführen von Code erlaubt, existiert und ausgenutzt wird.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61
Successful Code Injection/Execution (B.AS.SCI) auf Seite 63

Zugehörige Maßnahmen

Reaktion auf unerwartete Code Ausführungen (M.REA.BE-CASU) auf Seite 100

Configuration Modification (B.BE.CoMo)

Ein automatisiertes Sicherheitssystem meldet unerwartete Konfigurationsänderungen.

Hintergrund: Unerwartete Konfigurationsänderungen, beispielsweise bei der Firewall, bei Passwortvorgaben oder beim Logging, können darauf hindeuten, dass ein Angreifer sich neue Angriffsvektoren ermöglichen möchte.

Zugehörige Beobachtungen

Access Control Modification (B.BE.ACM) auf Seite 46

Zugehörige Maßnahmen

Reaktion auf Konfigurationsänderungen (M.REA.BE-KMU) auf Seite 101
Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Credential Abuse (B.BE.CrAb)

Ein automatisiertes Sicherheitssystem meldet einen potentiellen Credential Abuse.

Hintergrund: Grundlage für diese Meldung sind unerwartete Logins, speziell mit Root-Rechten.

Zugehörige Beobachtungen

Anomalous User Behavior: Unexpected Login Behavior (B.BE.AUB-UL) auf Seite 47

Zugehörige Maßnahmen

Vorgehen beim Missbrauch von Anmeldedaten (M.INV.BE-VMA) auf Seite 77

Data Exfiltration (B.BE.DaEx)

Ein automatisiertes Sicherheitssystem meldet Data Exfiltration, also dass wiederholt Daten beispielsweise mittels Komprimierung verschleiert und an einen Malicious Host verschickt wurden.

Hintergrund: Wiederholtes Senden von verschleierten Daten, insbesondere an bekannte Malicious Hosts, legt einen Datendiebstahl nahe.

Zugehörige Maßnahmen

Datendiebstahl unterbinden und Ursprung analysieren (M.REA.BE-DUUA) auf Seite 101

Known Attack Tool Detected (B.BE.KATD)

Ein automatisiertes Sicherheitssystem meldet, dass ein bekanntes Hacking-Tool detektiert wurde.

Hintergrund: Manche Tools haben charakteristisches Verhalten, oder verschleiern ihren Namen in den Prozessen des Zielsystems nicht.

Zugehörige Beobachtungen

Known Hacking Tool as Process Name (B.BE.KHTPN) auf Seite 49
Logs Cleared (B.BE.LoCl) auf Seite 49

Zugehörige Maßnahmen

Vorgehen bei detektierten Hacking-Tools (M.REA.AS-HTSU) auf Seite 112

Known Hacking Tool as Process Name (B.BE.KHTPN)

Ein automatisiertes Sicherheitssystem meldet, dass ein bekanntes Hacking-Tool ausgeführt wird.

Hintergrund: Manche Hacking-Tools tauchen unverschleiert in der Liste der Prozesse (Task Manager) auf.

Zugehörige Beobachtungen

Masquerading of Process (B.BE.MaPr) auf Seite 50

Zugehörige Maßnahmen

Vorgehen bei detektierten Hacking-Tools (M.REA.AS-HTSU) auf Seite 112

Logs Cleared (B.BE.LoCl)

Ein automatisiertes Sicherheitssystem meldet das manuelle Löschen von Log-Einträgen.

Hintergrund: Ein Angreifer kann versuchen seine Spuren verwischen, indem er die relevanten Einträge aus den Logs des angegriffenen Systems löscht. Gleichzeitig gibt es wenige Gründe für einen Administrator, manuell Logs zu löschen. Diese wenigen Ausnahmen sollten bekannt sein.

Zugehörige Maßnahmen

Gelöschten Log Einträgen untersuchen (M.INV.BE-GLEU) auf Seite 78

Malware File Detection (B.BE.MFD)

Ein automatisiertes Sicherheitssystem meldet, dass potentielle Schadsoftware durch einen Antivirus- bzw Malware-Scanner detektiert wurde.

Zugehörige Beobachtungen

Known Attack Tool Detected (B.BE.KATD) auf Seite 49

Known Hacking Tool as Process Name (B.BE.KHTPN) auf Seite 49

Logs Cleared (B.BE.LoCl) auf Seite 49

Malware Infection (B.AS.MIn) auf Seite 61

System Persistence (B.BE.SyPe) auf Seite 52

Zugehörige Maßnahmen

System auf Malware File Detection untersuchen und System auf Schwachstellen analysieren (M.REA.BE-MFDU) auf Seite 102

Masquerading of Process (B.BE.MaPr)

Ein automatisiertes Sicherheitssystem meldet, dass ein Prozess von einem unerwarteten Pfad ausgeführt wurde, bzw. dass der Prozessname nicht jenem entspricht, der von diesem Pfad erwartet wird.

Hintergrund: Schadsoftware kann verborgen werden, indem sie von Pfaden wie dem Windows-Papierkorb, tmp oder ähnlichen Ordnern ausgeführt wird. Eine weitere Möglichkeit ist, ihr Namen von bekannten Prozessen (z.B. Windows-Systemprozessen) zu geben.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61

Suspicious Code Execution (B.CIT.SCEx) auf Seite 50

Zugehörige Maßnahmen

Verschleierten Prozesse untersuchen (M.INV.BE-VPU) auf Seite 78

Suspicious Code Execution (B.CIT.SCEx)

Ein automatisiertes Sicherheitssystem meldet eine Suspicious Code Execution, also die Ausführung von verdächtigem Code.

Hintergrund: Unerwartete Kommandos oder speziell PowerShell-Prozesse, die von Programmen wie Office, Web-Browsern oder Windows-Anwendungen wie Notepad oder Calculator erzeugt wurden, können stark auf eine Kompromittierung und das Ausführen von Fremdcode hindeuten.

Zugehörige Beobachtungen

Code Execution (B.BE.CE) auf Seite 48

Malware File Detection (B.BE.MFD) auf Seite 50

Zugehörige Maßnahmen

Verdächtige Code Ausführung untersuchen (M.INV.CIT-VCAU) auf Seite 81

Network Access Control Modification (B.BE.NACM)

Ein automatisiertes Sicherheitssystem meldet, dass Änderungen an den Routing-Einstellungen vorgenommen wurden.

Hintergrund: Ein Angreifer kann hiermit abgeschirmte Systeme von außen zugänglich machen.

Zugehörige Beobachtungen

Configuration Modification (B.BE.CoMo) auf Seite 48

Zugehörige Maßnahmen

Manipulation von Netzwerk Einstellungen überprüfen (M.REA.BE-MNEU) auf Seite 102

Obfuscated Command (B.BE.ObCo)

Ein automatisiertes Sicherheitssystem meldet die Obfuskation von Commands oder Skripten.

Hintergrund: Bestimmte Skripte, z.B. Python oder Perl, können z.B. Base64-codiert ausgeführt werden, wodurch ihr Inhalt schlechter erkennbar ist. Auch Komprimierung und Verschlüsselung sind Möglichkeiten, um den Inhalt zu verschleiern.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61

Zugehörige Maßnahmen

Verschleierte/verdächtige Befehle untersuchen (M.INV.BE-VBU) auf Seite 79

Privilege Escalation (B.BE.PrEs)

Ein automatisiertes Sicherheitssystem meldet, dass ein Nutzer versucht, zusätzliche Berechtigungen zu erlangen.

Zugehörige Beobachtungen

Brute Force Permission Enumeration (B.BE.BFPE) auf Seite 47

Successful Privilege Escalation (B.AS.SPE) auf Seite 64

Zugehörige Maßnahmen

Unautorisierte Rechte Gewinnung rückgängig machen (M.REA.BE-URG) auf Seite 103

SSH Username Enumeration (B.BE.SSHUNE)

Ein automatisiertes Sicherheitssystem meldet eine SSH Username Enumeration.

Hintergrund: Diese Meldung bedeutet, dass versucht wurde, durch Login-Fehler in OpenSSH Nutzernamen auszuspähen. Auch andere Quellen, die eine Liste der Nutzernamen einsehbar machen, stellen potentiell ein Sicherheitsrisiko dar (siehe Password Spraying als Brute Force Authentication).

Zugehörige Beobachtungen

Successful Brute Force Authentication (B.AS.SBFA) auf Seite 63

Zugehörige Maßnahmen

Ausspähen von SSH-Nutzernamen unterbinden (M.REA.BE-ASSHNU) auf Seite 103

Security Tools Disabled (B.BE.STD)

Ein automatisiertes Sicherheitssystem meldet die unerwartete Deaktivierung von Sicherheitstools.

Hintergrund: Beispiele für Sicherheitstools Firewalls, Antivirus, AppArmor oder SELinux sein. Die Deaktivierung von Sicherheitstools erleichtert Angriffe und sollte normalerweise nicht vorkommen.

Zugehörige Maßnahmen

Deaktivierte Sicherheitseinstellungen untersuchen (M.INV.BE-DSTU) auf Seite 79

Successful System Persistence (B.BE.SSP)

Ein automatisiertes Sicherheitssystem meldet Successful System Persistence.

Hintergrund: Diese Meldung bedeutet, dass Schadsoftware trotz Löschen wiederholt wieder auf demselben Rechner auftaucht.

Zugehörige Maßnahmen

Vorgehen bei Successful System Persistence (M.REA.BE-VSSP) auf Seite 104

System Persistence (B.BE.SyPe)

Ein automatisiertes Sicherheitssystem meldet einen Versuch, System Persistence zu erlangen.

Hintergrund: Einträge in cronjobs, bashrc und ähnlichen Autorun-Funktionen erlauben es dem Angreifer, nach einem erfolgreichen Angriff auch über Neustarts hinweg die Kontrolle über das System zu behalten. Dementsprechend lohnt es sich, neue Einträge generell zu überprüfen.

Zugehörige Beobachtungen

Successful System Persistence (B.BE.SSP) auf Seite 52

Zugehörige Maßnahmen

Ursprung von Wiederkehrender Schadsoftware unterbinden (M.REA.BE-WSU) auf Seite 104

Unexpected Desktop Software (B.CIT.UDS)

Ein automatisiertes Sicherheitssystem meldet die Verwendung unerwarteter Software.

Hintergrund: Verschiedene Desktop-Programme, insbesondere Chat-Software, Torrent-Clients und Remote-Desktop-Anwendungen erlauben den unauffälligen Diebstahl von Daten, sowie einen Kanal für Kontrollbefehle.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61

Zugehörige Maßnahmen

Unerwartete Desktop Software untersuchen

Kapitel 7

Organisatorische Vorgaben

Themen:

Um die Informationssicherheit und Datenschutz in einer Organisation zu gewährleisten, werden interne Richtlinien und operative Vorgaben erlassen, an die sich die Mitarbeiter und Dienstleister zu halten haben.

Daher finden Sie in diesem Abschnitt alle Beobachtungen, die einen Verstoß gegen solcherlei interne organisatorische Maßnahmen darstellen. Die meisten dieser Maßnahmen haben ihre Wurzeln in öffentlichen Richtlinien und Normen. Daher werden im Rahmen dieses Maßnahmenkataloges solche generische organisatorische Vorgaben abgebildet. Auf unternehmensspezifische Vorgaben kann hier kein Bezug genommen werden. Grundlage der hier dargestellten Beobachtungen sind die Richtlinien und Normen aus dem einführenden Kapitel.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Klassifikationsstufen (B.ORG.KS)

Klassifikationsstufen für die Einstufung der Vertraulichkeit von Unterlagen.

Unterlagen, egal ob digital oder analog müssen entsprechend ihrer Vertraulichkeitsstufe gekennzeichnet werden. Hierfür existieren folgende Stufen:

Erläuterung	
ÖFFENTLICH	Informationen, die für die Allgemeinheit bestimmt sind und keinen besonderen Schutzbedarf haben. Vor Veröffentlichung, wie z.B. auf einer Website, *MUSS* aber das zuständige Public Relations Office eingebunden werden.
INTERN	Informationen, die während des normalen Arbeitsalltags erstellt werden und die nicht in eine der beiden nachfolgenden Kategorien fallen. Diese Informationen sind ausschließlich den Mitarbeitern des jeweiligen Unternehmens vorbehalten und *DÜRFEN* an Geschäftspartner weitergegeben werden, die eine Vertraulichkeitsvereinbarung (NDA) unterzeichnet haben.
VERTRAULICH	Informationen, deren Offenlegung an Unbefugte Dritte zu Schäden für das Unternehmen, Kunden oder Kollegen führen könnte. Diese Art der Information erfordert einen angemessenen Schutz der Vertraulichkeit und *MUSS* auf sichere Weise und *DARF* nur gemäß dem Prinzip "Kenntnis nur wenn nötig" (Need-To-Know-Prinzip) mit Mitarbeitern geteilt werden oder auch mit Geschäftspartnern, die eine Vertraulichkeitserklärung (NDA) unterzeichnet haben.
STRENG VERTRAULICH	Informationen, deren Offenlegung an Unbefugte Dritte zu extistenzbedrohenden Schäden für das Unternehmen oder Tochtergesellschaften führen könnte. Diese Art von Daten *MUSS* angemessen geschützt werden und *DARF* lediglich an benannte Mitarbeiter weitergegeben werden.

Zugehörige Maßnahmen

Papierunterlagen entsprechend ihrer „Klassifikation“ kennzeichnen (M.REA.ORG-PKK) auf Seite 126

Papierunterlagen entsprechend ihrer „Klassifikation“ entsorgen (B.ORG.PKE)

Papierunterlagen wurden nicht entsprechend ihrer „Klassifikation“ entsorgt

Es wurde entdeckt, dass Papierunterlagen nicht entsprechend ihrer Klassifikation entsorgt wurden.

Zugehörige Maßnahmen

Papierunterlagen entsprechend ihrer „Klassifikation“ kennzeichnen (M.REA.ORG-PKK) auf Seite 126

Umgang mit Gästen und Besuchern (B.ORG.UGB)

Wenn Gäste oder andere Besucher sich angekündigt haben, müssen bestimmte Vorgaben eingehalten werden, um die Sicherheit des Unternehmens nicht zu gefährden.

Für Mitarbeiter des Unternehmens haben sich Gäste angekündigt. Darunter fallen z.B. folgende Kategorien:

- private Kontakte
- Mitarbeiter anderer Unternehmen
- Dienstleister
- Lieferanten

Um beim Umgang mit Gästen oder Besuchern die Sicherheit nicht zu gefährden sind die unten gelisteten Maßnahmen auszuführen.

Zugehörige Maßnahmen

Maßnahmen zum Umgang mit Gästen und Besuchern (M.KOM.MGB) auf Seite 72

Konzernfremde Datenträger nicht an konzerneigene Hardware anschließen (B.ORG.FDA)

Konzernfremde Datenträger nicht an konzerneigene Hardware anschließen.
Ein Bediener hat beobachtet, dass konzernfremde externe Festplatten, USB-Sticks, DVD, SSD oder sonstige Datenträger an konzerneigene PCs, Notebooks, Multifunktionsgeräte oder sonstige konzerneigene Hardware angeschlossen wurde.

Zugehörige Maßnahmen

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH) auf Seite 73
Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

Virenscan eines Systems (M.REA.CIT-VS) auf Seite 111
Überprüfung

Meldung an ISMS (M.KOM.ISMS) auf Seite 73
Bei möglichen IT-Sicherheitsereignissen ist der ISMS-Ansprechpartner bzw. IT-Sicherheitsbeauftragte zu informieren.

Kapitel 8

Übergreifende Meldungen eines automatischen Sicherheitssystems (SIEM).

Themen:

Viele Beobachtungen und deren dazugehörigen Maßnahmen lassen sich oftmals in das gleiche Teilsystem einordnen. Um Redundanzen zu vermeiden und um das Dokument übersichtlicher zu gestalten, wurden die betroffenen Beobachtungen nicht zu den passenden Teilsystemen zugeordnet.

In diesem Abschnitt finden Sie alle Meldungen, die ein SIEM oder ähnliches automatisiertes Sicherheitssystem generieren könnte, die keinem bestimmten Bereich zugeordnet werden können. Daher finden Sie in diesem Kapitel IT-Angriffe mit unterschiedlichen Kontexten. Beispielsweise werden IT-Angriffe betrachtet, um ein System auszuspähen oder auch IT-Angriffe, die bei einem Erfolg dazu führen können, dass das angegriffene System ausfällt. Zusammengefasst werden in diesem Kapitel IT-Angriffe von der Anfangsphase eines Angriffs bis zur letzten Phase bzw. bis zu einem erfolgreichen Angriff betrachtet, wobei alle genannten Angriffsmethoden nicht auf ein spezifisches Teilsystem beschränkt sind.

zurück zur Begriffsbestimmung

Automatisierte Beobachtungen

Alarmanlage löst aus (B.AS.ALARM)

Eine Alarmanlage, welche Gebäude an externen Standorten oder auch Gebäudebereiche im Kontext der Leitwarte überwacht, meldet einen (Einbruchs-)Alarm.

Falls eine Alarmanlage den möglichen Einbruch bzw. unautorisierte Aktivität in einem Gebäude oder Gebäudeteil registriert, ist von einem Sicherheitsverstoß auszugehen.

Halten Sie Rücksprache mit für den Bereich Verantwortlichen (M.KOM.RSH (Seite 71)) und informieren Sie ggf. Ihren Vorgesetzten.

Der Vorfall muss unverzüglich durch einen Mitarbeiter vor Ort untersucht werden, um einen Fehlalarm auszuschließen und die Situation zu klären. Als Einstiegspunkt für mögliche Erkenntnisse ziehen Sie B.ZB.UEB (Seite 67) heran.

Attempt to Exploit Known Vulnerability (B.AS.AEKV)

Ein automatisiertes Sicherheitssystem meldet einen Attempt to Exploit Known Vulnerability, also dass Versuche unternommen wurden, bekannte Schwachstellen auszunutzen.

Hintergrund: Analog zu bekannten Hacking Tools haben auch viele bekannte Schwachstellen bestimmte Muster, nach denen sie ausgenutzt werden können. Die Ziele sind hierbei sehr vielfältig, von Acrobat Reader und Office-Programmen bis hin zu manchen Antivirusprogrammen.

Zugehörige Beobachtungen

Successful Exploit of Known Vulnerability (B.AS.SEKV) auf Seite 63

Zugehörige Maßnahmen

Angriffsversuche auf bekannte Schwachstellen unterbinden (M.REA.AS-ABSU) auf Seite 113

Brute Force Authentication (B.AS.BFA)

Ein automatisiertes Sicherheitssystem meldet einen Brute-Force-Versuch.

Hintergrund: Es wurden viele fehlgeschlagene Loginversuche, oder Loginversuche bei nicht existenten Benutzern detektiert. Das angegriffene System kann Aufschluss über die aktuellen Ziele des Angreifers geben. Brute Force Authentication kann z.B. dadurch verschleiert werden, dass ein einzelnes Passwort bei sehr vielen Nutzern verwendet wird, anstatt bei einem Nutzer viele Passwörter durchzuprobieren (Password Spraying, wird verwendet um Loginsperren nach einer bestimmten Anzahl Fehlversuchen zu umgehen).

Zugehörige Beobachtungen

Anomalous User Behavior: Unexpected Login Behavior (B.BE.AUB-UL) auf Seite 47

SSH Username Enumeration (B.BE.SSHUNE) auf Seite 51

Successful Brute Force Authentication (B.AS.SBFA) auf Seite 63

Zugehörige Maßnahmen

Verdächtige Anmeldeversuche unterbinden (M.INV.AS-BF-VAU) auf Seite 91

Code Injection/Execution (B.AS.CIE)

Ein automatisiertes Sicherheitssystem meldet Code-Injection oder -Execution.

Hintergrund: Code Injections nutzen aus, dass der Inhalt von Eingabemasken den Quellcode mancher Masken verändern kann. Gescheiterte Versuche sind in den entsprechenden Logs sichtbar.

Zugehörige Beobachtungen

DLL Injection (B.AS.VuSc) auf Seite 60

Malware Infection (B.AS.MIn) auf Seite 61

Successful Code Injection/Execution (B.AS.SCI) auf Seite 63

Zugehörige Maßnahmen

Code Injection und Schwachstellen untersuchen (M.REA.AS-CISU) auf Seite 113

Command-and-Control Communication (B.AS.CCC)

Ein automatisiertes Sicherheitssystem meldet Steuerungsbefehle von einem Kontrollserver (eines Angreifers).

Hintergrund: Diese Meldung kann darauf hindeuten, dass das System kompromittiert wurde und von einem Angreifer ferngesteuert wird. Auch die Verwendung eines unerwarteten SSL-Zertifikats kann auf einen Command-and-Control-Verbindungsaufbau hindeuten.

Zugehörige Beobachtungen

Lateral Movement (B.AS.LMo) auf Seite 61

Zugehörige Maßnahmen

Command-and-Control Communication untersuchen und unterbinden (M.REA.AS-CCCUU) auf Seite 113

Covert Channel established (B.AS.CCE)

Ein automatisiertes Sicherheitssystem meldet den Aufbau eines verdeckten Kommunikationskanals.

Hintergrund: Diese Meldung kann darauf hindeuten, dass ein System über diesen verdeckten Kanal ferngesteuert wird. Beispiele für verschleierte Kommunikationskanäle sind HTTP-Traffic über den DNS oder NTP Port oder in übergroßen ICMP-Paketen verborgener Traffic.

Zugehörige Beobachtungen

Reverse Shell (B.AS.RSh) auf Seite 62

Zugehörige Maßnahmen

Verdeckte Kommunikationskanäle untersuchen (M.INV.AS-VKKU) auf Seite 91

DLL Injection (B.AS.VuSc)

Ein automatisiertes Sicherheitssystem meldet eine DLL-Injection.

Hintergrund: DLL-Injections erlauben das Laden von Libraries in existierende Prozesse, um so Schadcode auszuführen.

Zugehörige Beobachtungen

Successful Code Injection/Execution (B.AS.SCI) auf Seite 63

Zugehörige Maßnahmen

Vorgehen bei einer DLL Injection (M.REA.AS-DLLISU) auf Seite 114

Denial of Service (B.AS.DOS)

Ein automatisiertes Sicherheitssystem meldet einen Denial of Service.

Hintergrund: Diverse Denial-of-Service-Methoden (z.B. UDP/SYN/ICMP-Floods) können verwendet werden, um Teile der Infrastruktur zu überlasten und so eventuell Sicherheitsvorkehrungen zu deaktivieren.

Zugehörige Beobachtungen

Network Attack: Replay Attack (B.AS.NA-RA) auf Seite 62

Zugehörige Maßnahmen

Denial of Service unterbinden (M.REA.AS-DOSU) auf Seite 114

File Download from poor reputation source (B.AS.FDPRS)

Ein automatisiertes Sicherheitssystem meldet einen Download von einer nicht vertrauenswürdigen Quelle.

Hintergrund: Downloads von bekannten Malicious Hosts können darauf hindeuten, dass Schadcode auf das System geladen wurde. Insbesondere der Download von ausführbaren Dateien ist ein starkes Indiz dafür.

Zugehörige Beobachtungen

Unexpected Desktop Software (B.CIT.UDS) auf Seite 52

Malware Infection (B.AS.MIn) auf Seite 61

Malware File Detection (B.BE.MFD) auf Seite 50

Zugehörige Maßnahmen

Download von nicht vertrauenswürdigen Quellen (M.REA.AS-DNVQ) auf Seite 115

Lateral Movement (B.AS.LMo)

Ein automatisiertes Sicherheitssystem meldet Lateral Movement, also die Bewegung des Angreifers zwischen Systemen im Netzwerk.

Hintergrund: Wiederholte Remote-Management Versuche können darauf hindeuten, dass sich ein Angreifer innerhalb des Netzwerkes bewegen möchte.

Zugehörige Beobachtungen

Successful Lateral Movement (B.AS.SLM) auf Seite 64

Zugehörige Maßnahmen

Reaktion auf Lateral Movement (M.REA.AS-LMVSU) auf Seite 116

Malware Infection (B.AS.MIn)

Ein automatisiertes Sicherheitssystem meldet eine Malware-Infektion.

Hintergrund: Diese Meldung deutet auf die Kompromittierung des Systems durch Malware oder Rootkits hin.

Zugehörige Beobachtungen

Command-and-Control Communication (B.AS.CCC) auf Seite 60
System Persistence (B.BE.SyPe) auf Seite 52

Zugehörige Maßnahmen

Reaktion auf Malware Infection (M.REA.AS-MWISU) auf Seite 116

Network Attack: Replay Attack (B.AS.NA-RA)

Ein automatisiertes Sicherheitssystem meldet einen Netzwerk-Angriff, wie z.B. eine Replay-Attack.

Hintergrund: Charakteristisch für diesen Angriff kann der Empfang von größeren Mengen an identischen oder leicht veränderten Paketen sein. Die Meldung kann darauf hindeuten, dass ein Angreifer probiert, mittels Kontrollnachrichten Systeme zu beeinflussen, indem er Pakete abfängt und zu beliebigen Zeiten an die jeweiligen Systeme sendet.

Zugehörige Beobachtungen

Successful Network Attack: Replay Attack (B.AS.SNA-RA) auf Seite 64

Zugehörige Maßnahmen

Netzwerk Replay Angriff unterbinden (M.REA.AS-NA-RPU) auf Seite 117

Port Scan (B.AS.PSc)

Ein automatisiertes Sicherheitssystem meldet einen Port Scan.

Hintergrund: Dies äußert sich in einer großen Menge an (in der Regel unvollständigen) Verbindungen zum Server, insbesondere zu unerwarteten (das heißt vom Server nicht verwendeten) Ports, die häufig vom selben Host ausgehen. Ein Port Scan kann dadurch verschleiert werden, dass er über längere Zeit ausgedehnt wird – ein Angreifer hat häufig relativ viel Zeit zur Beobachtung und eine verdächtige Verbindung pro Stunde ist weitaus weniger auffällig als mehrere tausend Verbindungen innerhalb weniger Minuten.

Zugehörige Beobachtungen

Network Attack: Replay Attack (B.AS.NA-RA) auf Seite 62

Zugehörige Maßnahmen

Port Scan unterbinden (M.REA.AS-PSU) auf Seite 117

Reverse Shell (B.AS.RSh)

Ein automatisiertes Sicherheitssystem meldet eine Reverse Shell.

Hintergrund: Kommandozeilenparameter, die auf eine Reverse Shell hindeuten, können in TCP- oder UDP-Verbindungen beobachtet werden.

Zugehörige Beobachtungen

Command-and-Control Communication (B.AS.CCC) auf Seite 60

Zugehörige Maßnahmen

Reverse Shell unterbinden (M.REA.AS-RSU) auf Seite 117

Service Discovery (B.AS.SDi)

Ein automatisiertes Sicherheitssystem detektiert ein bestehendes Scan-Tool zur Detektion verfügbarer Services.

Hintergrund: Viele fertige Hacking- und Scan-Tools haben charakteristische Verhaltensweisen, die identifiziert werden können.

Zugehörige Beobachtungen

Port Scan (B.AS.PSc) auf Seite 62

Zugehörige Maßnahmen

Service Discovery unterbinden (M.REA.AS-SDU) auf Seite 118

Successful Brute Force Authentication (B.AS.SBFA)

Ein automatisiertes Sicherheitssystem meldet eine erfolgreiche Brute Force Authentication.

Hintergrund: Durch wiederholte Loginversuche kann der Angreifer erfolgreich unautorisierten Zugang zum System erlangen. Diese Meldung deutet daher auf ein kompromittiertes System hin.

Zugehörige Beobachtungen

Privilege Escalation (B.BE.PrEs) auf Seite 51

Zugehörige Maßnahmen

Vorgehen bei Successful Brute Force Authentication (M.REA.AS-VSBFA) auf Seite 118

Successful Code Injection/Execution (B.AS.SCI)

Ein automatisiertes Sicherheitssystem meldet eine erfolgreiche Code-Injection oder -Execution.

Hintergrund: Code Injections nutzen aus, dass der Inhalt von Eingabemasken den Quellcode mancher Masken verändern kann.

Zugehörige Maßnahmen

Vorgehen bei Successful Code Injection/Execution (M.REA.AS-VSCI) auf Seite 119

Successful Exploit of Known Vulnerability (B.AS.SEKV)

Ein automatisiertes Sicherheitssystem meldet Successful Exploit of Known Vulnerability, also dass eine bekannte Schwachstelle in einer Anwendung erfolgreich ausgenutzt wurde.

Hintergrund: Analog zu bekannten Hacking Tools haben auch viele bekannte Schwachstellen bestimmte Muster, nach denen sie ausgenutzt werden können. Die Ziele sind hierbei sehr vielfältig, von Acrobat Reader und Office-Programmen bis hin zu manchen Antivirusprogrammen.

Zugehörige Maßnahmen

Vorgehen bei Successful Exploit of Known Vulnerability (M.REA.AS-VSEKV) auf Seite 119

Successful Lateral Movement (B.AS.SLM)

Ein automatisiertes Sicherheitssystem meldet erfolgreiches Lateral Movement, also dass ein Angreifer erfolgreich von einem System in ein anderes eindringen konnte und sich somit im Netzwerk bewegt hat.

Hintergrund: In manchen Fällen ist das Zielsystem nicht direkt erreichbar, sondern nur über mehrere Zwischenschritte.

Zugehörige Maßnahmen

Vorgehen bei Successful Lateral Movement (M.REA.AS-VSLM) auf Seite 120

Successful Network Attack: Replay Attack (B.AS.SNA-RA)

Ein automatisiertes Sicherheitssystem meldet eine erfolgreiche Replay-Attack.

Hintergrund: Bei einer Replay-Attack werden abgefangene Pakete (insb. zur Authentifizierung) genauso oder leicht verändert mehrmals gesendet, um ohne ihren genauen Inhalt zu kennen das System zu beeinflussen. Hier hat ein solches Paket eine valide Antwort erhalten.

Zugehörige Maßnahmen

Netzwerk Replay Angriff unterbinden (M.REA.AS-NA-RPU) auf Seite 117

Successful Privilege Escalation (B.AS.SPE)

Ein automatisiertes Sicherheitssystem meldet eine erfolgreiche Privilege Escalation.

Hintergrund: Diese Meldung kann darauf hindeuten, dass ein Angreifer erfolgreich mehr Rechte für einen Nutzer eingeräumt hat, als ein Administrator für diesen vorgesehen hatte.

Zugehörige Maßnahmen

Vorgehen bei Successful Privilege Escalation (M.REA.AS-VSPE) auf Seite 120

System Error (B.AS.VSc)

Ein automatisiertes Sicherheitssystem meldet Fehlermeldungen in sicherheitskritischen Anwendungen, wie z.B. Firewalls.

Zugehörige Maßnahmen

Vorgehen auf Fehlermeldungen (M.REA.AS-FU) auf Seite 121

Vulnerability Scanning (B.AS.VuSc)

Ein automatisiertes Sicherheitssystem detektiert Traffic eines Vulnerability Scanners.

Hintergrund: Ein Vulnerability Scanner wird verwendet um automatisiert nach Schwachstellen zu suchen. Der Traffic, der dabei hinterlassen wird, ist abhängig von Software und Zielgerät, aber häufig charakteristisch für einen bestimmten Scanner.

Zugehörige Beobachtungen

Attempt to Exploit Known Vulnerability (B.AS.AEKV) auf Seite 59

Zugehörige Maßnahmen

Scannen von etwaigen Schwachstellen unterbinden (M.REA.AS-SSCU) auf Seite 121

Kapitel 9

Übergreifende Zufallsbeobachtungen

Themen:

In diesem Abschnitt finden Sie alle Beobachtungen, die unter die Kategorie Zufallsbeobachtungen fallen und keinem bestimmten Bereich zugeordnet werden können.

zurück zur Begriffsbestimmung

Manuelle Beobachtungen

Überwachungskamera zeigt ungewöhnliches Ereignis (B.ZB.CAM)

Auf einer Überwachungskamera wurden unautorisierte Personen oder anormale Ereignisse beobachtet.

Fahren Sie entsprechend der Vorgehensweise bei Ein ungewöhnliches Ereignis wird beobachtet (B.ZB.UEB) auf Seite 67 fort.

Zugehörige Beobachtungen

Ein ungewöhnliches Ereignis wird beobachtet (B.ZB.UEB) auf Seite 67

Ein ungewöhnliches Ereignis wird beobachtet (B.ZB.UEB)

Es wurden unautorisierte Personen oder anormale Ereignisse - bspw. zerstörte Schlösser oder Zäune, unverschlossene Türen oder Fenster - beobachtet.

- Sollten unidentifizierte Personen in Bereichen gesichtet werden, in denen ihre Anwesenheit fragwürdig oder nicht autorisiert ist, halten Sie Rücksprache mit zuständigen Personen gemäß M.KOM.RSH (Seite 71) und fahren Sie entsprechend der Beobachtung B.SFM.UPE (Seite 41) fort.
- Werden beispielsweise geöffnete Türen oder sogar beschädigte Schlösser, Türen oder Fenster beobachtet, ist von nicht autorisiertem Eindringen auszugehen. Halten Sie Rücksprache mit für den Bereich zuständigen Personen gemäß M.KOM.RSH (Seite 71) und informieren Sie ggf. Ihren Vorgesetzten.

  Orientieren Sie Ihr Vorgehen am Vorgehen für Vorfälle physischen Eindringens gemäß B.SFM.PE (Seite 37) und untersuchen Sie die Räumlichkeiten hinsichtlich Veränderungen an Geräten (B.ÜT/NT.GMa (Seite 27)), beschädigter Technik (B.ÜT/NT.GEn (Seite 27)) oder unbekannten Geräten (B.ÜT/NT.FGE (Seite 28)).

  Stellen Sie sicher, dass beschädigte Schlösser, Türen, Fenster und Geräte repariert bzw. ersetzt werden.

  Sollte es sich um einen Einbruch handeln, informieren Sie Ermittlungsbehörden und halten Sie Rücksprache (M.KOM.RSH (Seite 71)) mit Verantwortlichen für betroffene Bereiche bezüglich der Vermeidung entsprechender Vorfälle.

Prüfen Sie abschließend gemäß M.DOK.MBP (Seite 127), ob eine Meldung des Vorfalls vorgeschrieben ist und führen Sie die Meldung entsprechend durch.

Denial of Service (B.ZB.DOS)

Das System weist erhöhte Ladezeiten auf.

Hintergrund: Erhöhte Ladezeiten können ein Indiz für einen Denial-of-Service-Angriff sein. Charakteristisch für einen Denial-of-Service-Angriff ist, dass Teile oder das ganze System überlastet sind. Im schlimmsten Fall führt dies zu einem Teil- oder Komplettausfall des Systems.

Zugehörige Beobachtungen

Erhöhte Systemauslastung (B.ZB.ESA) auf Seite 68

Network Attack: Replay Attack (B.AS.NA-RA) auf Seite 62

Zugehörige Maßnahmen

Denial of Service unterbinden (M.INV.ZB-DOSU) auf Seite 89

Erhöhte Systemauslastung (B.ZB.ESA)

Die Auslastung eines Systems ist unerwartet hoch.

Hintergrund: Eine unerwartet hohe Auslastung eines Systems kann durch Manipulationen wie unautorisierte Installationen, Brute-Force-Angriffe, Denial-of-Service-Angriffe oder nicht autorisierte, laufende Prozesse hervorgerufen werden.

Zugehörige Beobachtungen

Denial of Service (B.ZB.DOS) auf Seite 67
Denial of Service (B.AS.DOS) auf Seite 61

Zugehörige Maßnahmen

Erhöhte Systemauslastung senken (M.INV.ZB-ESAS) auf Seite 90

Unerwartete Log-Einträge (B.ZB.ULE)

In den Logs eines Systems oder Programms wurden verdächtige Einträge gefunden.

Hintergrund: Hacking-Tools oder Schadsoftware hinterlassen meistens verdächtige Log-Einträge, anhand derer ein Angriff nachverfolgt werden kann, sofern sie nicht gelöscht wurden.

Zugehörige Beobachtungen

Code Injection/Execution (B.AS.CIE) auf Seite 60

Zugehörige Maßnahmen

Unerwartete Log-Einträge behandeln (M.INV.ZB-ULEB) auf Seite 90

Kapitel 10

Maßnahmen

Themen:

- Kommunikation
- Investigation
- Reaktion
- Nachbereitung
- Dokumentation

Maßnahmen für getroffene Beobachtungen

Kommunikation

Rücksprache halten und Vorfall kommunizieren (M.KOM.RSH)

Abhängig von der konkreten Beobachtung ist mit zuständigen Ansprechpartnern Rücksprache zu halten, um Zwischenfälle zu beurteilen und zu kommunizieren.

> Es ist ein Ereignis eingetreten, welches noch nicht eindeutig eingeordnet wurde oder dessen Lösung weitere Informationen benötigt. Abhängig von der konkreten Situation werden die zuständigen Ansprechpartner identifiziert:

1. Identifizieren Sie den Kontext des Vorfalls und die zuständigen Mitarbeiter.
2. Kontaktieren Sie abhängig vom Kontext die Übertragungstechnik (M.KOM.ÜTH (Seite 71)), die Fernwirktechnik (M.KOM.FWTH (Seite 72)), die Leitsystemtechnik (M.KOM.LSTH (Seite 72)) und gegebenenfalls Ihren direkten Vorgesetzten über das Ereignis.
3. Halten Sie Rücksprache zu eventuell geplanten Ereignissen der festgestellten Art, um einen unangekündigtes, jedoch geplanten Vorfall auszuschließen.
4. Nutzen Sie die gewonnenen Erkenntnisse für die weitere Bearbeitung des Zwischenfalls und greifen Sie ggf. auf weitere Unterstützung durch die kontaktierten Personen zurück.
5. Dokumentieren Sie Ihr Vorgehen gemäß M.DOK.SDOK (Seite 127)

Übertragungstechnik hinzuzuziehen (M.KOM.ÜTH)

Für die weitere Bearbeitung eines Vorfalls, ist die Übertragungstechnik hinzuzuziehen

> Zuvor ist ein Vorfall eingetretten für dessen weitere Analyse Kollegen aus der Übertragungstechnik benötigt werden

1. Nehmen die den Alarmplan bzw. Adressbuch zur Hand
2. Suchen die die Hotline-nummer bzw. die Emailadresse des Funktionspostfachs der Übertragungstechnik heraus
3. Informieren Sie die Kollegen der Übertragungstechnik über den Vorfall und übergeben die notwendigen Informationen

   Falls es ein Ticketsystem gibt, notieren Sie sich die Ticketnummer, falls nein notieren Sie sich den Namen Ihres Gesprächspartners und -uhrzeit.
4. Stimmen Sie das weitere Vorgehen mit den Kollegen der Übertragungstechnik ab.
5. Dokumentieren Sie das weitere Vorgehen
6. Informieren Sie Ihren Schichtleiter bzw. direkten Vorgesetzten

Die fachliche Bearbeitung/ Analyse des Vorfalls wird mit Unterstützung bzw, unter Federführung der Übertragungstechniker vorgesetzt.

Fahren Sie mit der Bearbeitung des Vorfalls fort.

Erfassung und Übergabe der Fehlerinformation (M.KOM.INF)

> Für die Ermittlung der Fehlerstelle und Störungsbearbeitung sind Informationen zum Fehlerbild notwendig. Dazu werden die entsprechenden Fehlermeldungen aus den genutzten Managementsystemen herangezogen. Bei Verfügbarkeit sind folgende Informationen für die weitere Bearbeitung bereitzustellen.

1. Betroffene Standorte
2. Art und Inhalt der Fehlermeldung
3. Zeitliches Auftreten
4. Bisherige Erkenntnisse
5. Beteiligte und zu informierende Personen oder Fachbereiche

Die Erfassung und Bereitstellung der Informationen erfolgt nach den Unternehmensvorgaben, z. B. durch ein Ticketsystem.

Zugehörige Beobachtungen

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Zugehörige Maßnahmen

Überprüfung weiterer Kommunikationsausfälle im Störungszusammenhang (M.INV.WKA) auf Seite 92

Überprüfung der Dokumentation der gestörten Verbindung (M.INV.DOK) auf Seite 92

Fernwirktechnik hinzuzuziehen (M.KOM.FWTH)

Für die weitere Bearbeitung eines Vorfalls, ist die Fernwirktechnik hinzuzuziehen

> Zuvor ist ein Vorfall eingetreten für dessen weitere Analyse Kollegen aus der Fernwirktechnik benötigt werden

1. Nehmen die den Alarmplan bzw. Adressbuch zur Hand
2. Informieren Sie die Kollegen der Fernwirktechnik über den Vorfall und übergeben die notwendigen Informationen
3. Stimmen Sie das weitere Vorgehen mit den Kollegen der Fernwirktechnik ab.
4. Dokumentieren Sie das weitere Vorgehen

Die fachliche Bearbeitung/ Analyse des Vorfalls wird mit Unterstützung bzw., unter Federführung der Fernwirktechniker vorgesetzt.

Fahren Sie mit der Bearbeitung des Vorfalls fort.

Leitsystemtechnik hinzuzuziehen (M.KOM.LSTH)

Für die weitere Bearbeitung eines Vorfalls, ist die Fernwirktechnik hinzuzuziehen

> Zuvor ist ein Vorfall eingetreten für dessen weitere Analyse Kollegen aus der Leitsystemtechnik benötigt werden

1. Nehmen die den Alarmplan bzw. Adressbuch zur Hand
2. Informieren Sie die Kollegen der Leitsystemtechnik über den Vorfall und übergeben die notwendigen Informationen
3. Stimmen Sie das weitere Vorgehen mit den Kollegen der Leitsystemtechnik ab.
4. Dokumentieren Sie das weitere Vorgehen

Die fachliche Bearbeitung/ Analyse des Vorfalls wird mit Unterstützung bzw., unter Federführung der Leitsystemtechniker vorgesetzt.

Fahren Sie mit der Bearbeitung des Vorfalls fort.

Maßnahmen zum Umgang mit Gästen und Besuchern (M.KOM.MGB)

> Gäste oder andere Besucher haben sich angekündigt.

1. Unternehmensfremde Personen, die das Gelände betreten möchten *SOLLEN* im Vorfeld nach den Unternehmensvorgaben anzumelden. Auf ihre Legitimation zu überprüfen, und sofern möglich für die Dauer ihres Aufenthalts zu begleiten. Zur besseren Nachverfolgbarkeit sollte ihr Aufenthalt auch mit Anfangs- und Endzeit festgehalten werden.
2. Zur besseren Nachverfolgbarkeit *SOLL* ihr Aufenthalt auch mit Anfangs- und Endzeit festgehalten werden.
3. Gäste und Besucher *MÜSSEN* sich beim Eintreffen an der jeweiligen Stelle mit einem gültigen Lichtbildausweis, wie Mitarbeiter- oder Personalausweis, legitimieren.
4. Gäste und Besucher *MÜSSEN* von dem in der Anmeldung genannten Mitarbeiter abgeholt werden.
5. Sie *SOLLEN* sofern möglich für die Dauer ihres Aufenthalts ständig von einem Mitarbeiter begleitet werden, ggfs. ist für längere Arbeiten wie Wartung oder Installationstätigkeiten hierfür der Sicherheitsdienst hinzuziehen, um Fachpersonal nicht dauerhaft zu binden.

Mit der vollständigen Dokumentation des Besuchs kann die Bearbeitung abgeschlossen werden.

First-Level-Support kontaktieren (M.KOM.FLS)

Für die weitere Bearbeitung eines IT-Problems, ist der Support hinzuzuziehen

> Zuvor ist ein Problem mit einem Computer aufgetreten, das nicht durch den Nutzer behoben werden konnte.

1. Suchen Sie die Nummer bzw. Email-Adresse des First-Level-Supports, des Service-Desk oder des für Ihr System zuständigen Administrators heraus.
2. Kontaktieren Sie den Support und schildern das Problem möglichst genau
3. Folgen Sie den weiteren Anweisungen des Supports.

Die fachliche Bearbeitung/ Analyse des Problems wird mit Unterstützung bzw., unter Federführung des Supports vorgesetzt.

Rechner sperren (M.KOM.SFM-PCS)

Rechner sind zu sperren, sobald der Arbeitsplatz verlassen wird, um einen unautorisierten Zugriff auf den Rechner und darin gespeicherte Informationen zu verhindern.

> Zuvor wurde festgestellt, dass ein Rechner unbeaufsichtigt und nicht gesperrt ist.

1. Weisen Sie den Nutzer des Rechners darauf hin, dass Rechner zu sperren sind, sobald der Arbeitsplatz verlassen wird.
2. Der Nutzer sperrt den Rechner mit der Tastenkombination "Windows-Taste" + "L" oder über das Windowsmenü -> auf Name des Nutzers klicken und *Sperren* auswählen.

Der Rechner wurde gesperrt und ist somit von unbefugtem Zugriff geschützt.

Meldung an ISMS (M.KOM.ISMS)

Bei möglichen IT-Sicherheitsereignissen ist der ISMS-Ansprechpartner bzw. IT-Sicherheitsbeauftragte zu informieren.

> Zuvor wurde ein mögliches IT-Sicherheitsereignis festgestellt.

1. Suchen Sie sich aus Unternehmensadressbuch bzw. Meldeplan die Kontaktdaten Ihres zuständigen IT-Sicherheitsbeauftragten oder den ISMS-Ansprechpartner.
2. Melden Sie den Vorfall möglichst detailliert.
3. Folgen Sie den weiteren Anweisungen Ihres Ansprechpartners.
4. In den meisten Unternehemen *MUSS* ebenfalls der unmittelbare Linienvorgesetzte informiert werden.

Der Vorfall wurde gemeldet und die weitere Bearbeitung erfolgt unter der Koordination des ISMS-Ansprechpartner oder IT-Sicherheitsbeauftragten.

Fahren Sie mit der weiteren Bearbeitung nach Anweisung Ihres Ansprechpartners oder Vorgesetzte fort.

Mitarbeiter auf Fehler hinweisen (M.KOM.SFM-MH)

Wir achten aufeinander und weisen uns gegenseitig auf Fehler hin.

> Zuvor wurde festgestellt, dass ein Kollege vergessen hat, gewisse Unternehmensvorgaben zur Sicherheit zu beachten.

1. Weisen Sie Ihren Kollegen auf den Fehler hin. Achten Sie hierbei auf einen freundlichen und kollegialen Umgangston.
2. Falls der Kollege bereits mehrfach durch Fehlverhalten aufgefallen ist, weisen Sie ihn auf die entsprechenden Vorgaben hin und kontaktieren Sie im Notfall dessen Vorgesetzten.

Der Kollege wurde auf seinen Fehler aufmerksam gemacht.

Hersteller hinzuzuziehen (M.KOM.HSH)

Für die weitere Bearbeitung eines Vorfalls, ist der Hersteller der Software/ Komponente hinzuzuziehen.

Zuvor ist ein Vorfall eingetreten für dessen weitere Analyse der Hersteller des jeweiligen Systems, bzw. der jeweiligen Software benötigt wird.

1. Nehmen die den Alarmplan, Adressbuch, oder ggf. die Supportunterlagen des jeweiligen Systems zur Hand.
2. Suchen die die Hotline-Nummer bzw. die Emailadresse des Funktionspostfachs des Herstellers heraus.
3. Informieren Sie den Hersteller über den Vorfall und übergeben die notwendigen Informationen.

   Falls es ein Ticketsystem gibt, notieren Sie sich die Ticketnummer, falls nein notieren Sie sich den Namen Ihres Gesprächspartners und -uhrzeit.
4. Dokumentieren Sie das weitere Vorgehen.

Die fachliche Bearbeitung/ Analyse des Vorfalls wird mit Unterstützung bzw., unter Federführung des Herstellers vorgesetzt.

Fahren Sie mit der Bearbeitung des Vorfalls fort.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Investigation

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR)

In einem Teilbereich des Systems, einer Komponente oder eines Gebäudes wurde ein (potentieller) Angriff erkannt und untersucht. Zum Sichern der IT-Security im Gesamtsystem muss das System ganzheitlich auf weitere angegriffene oder angreifbare Komponenten untersucht werden, welche anschließend isoliert und instand gesetzt werden müssen.

Im Falle eines Angriffs ist es unter Umständen sinnvoll, externe Unterstützung zur forensischen Analyse und der Beseitigung der Angriffsauswirkungen heranzuziehen.

1. **Meldung.** Informieren Sie Ihren Vorgesetzten und prüfen Sie, ob der Vorfall meldepflichtig ist (M.DOK.MBP (Seite 127)).
2. **Physisches Eindringen.** Bei physischem Eindringen bzw. einem gescheiterten Versuch sind alle Räumlichkeiten der betroffenen Standorte zu überprüfen (B.SFM.PE (Seite 37)). Hierbei ist insbesondere auf beschädigte Türen, Fenster und Schlösser sowie Veränderungen an Geräten in Form von unbekannter (B.ÜT/NT.FGE (Seite 28)), entwendeter (B.ÜT/NT.GEn (Seite 27)), defekter (B.FWT.EGD (Seite 32)), oder manipulierter (B.FWT.KGM (Seite 32)) Hardware zu achten.
3. **Kommunikation.** Halten Sie Rücksprache mit anderen Mitarbeitenden, auch über die lokale Fehlerstelle hinaus, um so mögliche korrelierte Angriffsauswirkungen zu identifizieren und koordiniert zu bearbeiten (M.KOM.RSH (Seite 71)) Neben eindeutigen Angriffshinweisen sind auch Aspekte wie unerwartete Mailanfragen oder Geschwindigkeitseinbußen (B.ZB.ESA (Seite 68)) an Rechnern relevant.

   Sind in anderen Systembereichen ebenfalls ungewöhnliche Vorkommnisse gemeldet - auch solche, die nicht direkt auf einen Angriff zurückzuführen sind - ist von einem erfolgreichen Angriff auf das Gesamtsystem auszugehen. Alle Mitarbeitenden müssen informiert werden, um das Bewusstsein für einen vorliegenden Angriff zu schärfen und um die Meldung aller ungewöhnlichen Vorkommnisse einzufordern.
4. **SIEM prüfen.** Überprüfen Sie, ob Meldungen über unerwartete Logeinträge (M.INV.ZB-ULEB (Seite 90)), Logins oder ungewöhnliche Netzwerkaktivität (M.INV.LS-NA-EATU (Seite 85)) wie unter anderem hohe Latenz oder Denial of Service (M.INV.ZB-DOSU (Seite 89)), Netzwerkscans M.INV.LS-NA-EATU (Seite 85), Kommunikation zwischen Geräten, welche üblicherweise nicht oder anders kommunizieren oder unerwartete Kommunikationsprotokolle vom automatischen Sicherheitssystem gemeldet werden.
   Untersuchen Sie die Quelle und die Auswirkungen jeden Zwischenfalls, isolieren Sie betroffene Geräte und Netzsegmente, fahren Sie mit der Untersuchung des Vorfalls fort und beheben Sie die Verwundbarkeit durch Rückspielung von Backups, Änderung von Zugangsdaten, Rücksprache mit dem Hersteller (M.KOM.HSH (Seite 73)), Softwareaktualisierungen und die eventuelle Installation weiterer Sicherheitsmaßnahmen.

   Greifen Sie je nach Befund auf die entsprechenden Beobachtungen zurück.

5. **Manuelle Systeminvestigation.** Komponenten und Geräte, welche nicht (vollständig) über ein SIEM oder ein vergleichbares System überwacht werden, müssen manuell auf Auffälligkeiten wie im vorherigen Schritt überprüft werden. Hierbei ist insbesondere auf Logeinträge (B.ZB.ULE (Seite 68)), Loginverhalten, laufende Prozesse, ggf. geöffnete Remote-Verbindungen via SSH (B.BE.SSHUNE (Seite 51)) oder andere Software sowie ungewöhnliche Netzwerkaktivität zu achten.

   Greifen Sie je nach Befund auf die entsprechenden Beobachtungen zurück.

6. **Einfallstor identifizieren.** Sollte ein Angriff nicht durch physisches Eindringen erfolgt sein, sondern von einem infizierten Gerät oder von gestohlene Zugangsdaten ausgegangen sein, ist die genaue Ursache zu untersuchen. Nutzen Sie die Erkenntnisse aus den vorhergegangenen Schritten, um den Ablauf des Angriffs zu rekonstruieren und mögliche Ausgangsgeräte zu identifizieren. Prüfen Sie das Ausgangsgerät auf (bekannte) Schwachstellen in installierter Software, unerwartete Programme (B.CIT.UDS (Seite 52)) und beheben Sie diese Schwachstellen durch Softwareupdates oder die langfristige Isolation des Systems.
   Bei Missbrauch von Zugangsdaten sprechen Sie mit dem betroffenen Nutzer und prüfen Sie, ob ggf. ein Phishing-Angriff erfolgreich gewesen sein kann oder die Zugangsdaten anderweitig entwendet worden sein könnten. Prüfen Sie zudem, ob die Zugangsdaten durch einen Brute-Force-Angriff herausgefunden worden sein können.
   In jedem Fall sind betroffene Zugangsdaten, optimalerweise **alle** Zugangsdaten von Mitarbeitenden, welche potentiell Opfer des gleichen Angriffs geworden sein können, gemäß M.REA.ZDA (Seite 111) zu ändern. Die Durchsetzung einer Passwortrichtlinie sowie die Verwendung von bspw. Zweifaktorauthentifizierung kann helfen, Angriffe dieser Art zu erschweren und zu verhindern.

   Für forensisches Vorgehen ist es hilfreich, auf externe Expertise zurückzugreifen.

7. **Vor-Ort-Überprüfung.** Einzelne Standorte und Komponenten, für die nicht zweifelsfrei ausgeschlossen werden kann, dass sie vom Angriff betroffen sind, werden durch einen Techniker Ort überprüft (M.INV.HVO (Seite 93)).
8. **Dokumentation.** Dokumentieren Sie alle Erkenntnisse und durchgeführten Schritte gemäß M.DOK.SDOK (Seite 127).

Zugehörige Beobachtungen

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Unerwartete Änderungen der Sicherheitseinstellungen untersuchen (M.INV.BE-USEU)

> Zuvor hat ein automatisiertes Sicherheitssystem unerwartete Änderungen in Sicherheitseinstellungen detektiert.

1. Zeitpunkt und betroffene Systeme sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
2. Es sollte überprüft werden, ob ein Nutzer für die Änderungen verantwortlich war und ob die Änderungen berechtigt waren. Hierbei sollten alle Nutzer gefragt werden, die die benötigten Berechtigungen für die Änderung an Sicherheitseinstellungen haben.
3. Falls Ursache der Änderungen ein Angriff sein könnte, muss das System umgehend von anderen Systemen isoliert werden. Es muss untersucht werden, welche Änderungen vorgenommen worden sind, damit diese rückgängig gemacht werden können. Die Isolierung darf erst wieder aufgehoben werden, sobald die Änderung rückgängig gemacht worden bzw. sichergestellt ist, dass keine Kompromittierung des System mehr vorliegt, beispielsweise indem das System mit einem Backup wiederhergestellt wird. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
4. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
5. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
6. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.

7. Es sollte untersucht werden durch welche Schwachstelle der Angreifer die Möglichkeit hatte Änderungen vorzunehmen. Alle Befunde sollten behoben und dokumentiert werden. Anhand der dokumentierten Befunde sollten angrenzende Systeme ebenfalls auf ähnliche Schwachstellen untersucht werden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Account auf Manipulationen untersuchen (M.INV.BE-AMU)

Zuvor hat ein automatisiertes Sicherheitssystem Account-Manipulationen festgestellt.

1. Zuerst muss überprüft werden, ob es einen berechtigten Grund für das beobachtete Verhalten gibt.
2. Falls nicht, sind Zeitpunkt und betroffene/beteiligte Accounts zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
3. Alle unberechtigten Änderungen sind rückgängig zu machen, und die ausführenden Accounts sind zu sperren.
4. Weiterhin muss nach Sicherheitslücken gesucht werden, die Zugriff auf die Accounts, von denen die Änderungen ausgingen, ermöglicht hatten, und diese geschlossen werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Überprüfung von unautorisierten Account Löschungen (M.INV.BE-AUB-UAD)

Zuvor hat ein automatisiertes Sicherheitssystem anomales Nutzerverhalten detektiert.

1. Zuerst muss überprüft werden, ob es einen berechtigten Grund für das Verhalten gab, um einen Fehlalarm auszuschließen.
2. Falls sich herausstellt, dass die Kompromittierung eines Accounts dazu geführt hat, dass dieser andere Accounts gelöscht hat, muss dieser umgehend gesperrt werden.
3. Zeitpunkt und betroffene Accounts sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
4. Etwaige daraus entstandene Schäden sind zu beheben, und gegebenenfalls Sicherheitslücken, die die Kompromittierung ermöglicht haben, zu schließen.
5. Weiterhin ist das restliche System auf ähnliche Zugriffe zu überprüfen.
6. Danach kann der Account mit neuen Zugangsdaten (Neues Passwort) wieder freigegeben werden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Anomales Nutzerverhalten untersuchen (M.INV.BE-AUB-AMU)

Zuvor hat ein automatisiertes Sicherheitssystem anomales Nutzerverhalten detektiert.

1. Der Nutzer, der anomales Verhalten aufweist, sowie das Verhalten des Nutzers sollten dokumentiert werden.
2. Es ist zu überprüfen, ob der Nutzer tatsächlich selbst für die Beobachtung verantwortlich ist, und ob er evtl. eine neue Rolle hat, die sein Verhalten rechtfertigt.
3. Falls das Verhalten des Nutzers keinen validen Grund hatte, ist der Account mit hoher Wahrscheinlichkeit kompromittiert. Daher sollten dem Nutzer vorerst alle Rechte entzogen werden, damit kein weiterer Schaden angerichtet werden kann.

4. Daraufhin muss untersucht werden, wie der Account kompromittiert werden konnte, und gefundene Sicherheitslücken geschlossen werden. Weiterhin sind etwaige Schäden zu beheben.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Unautorisierte Versuche Systemrechte auszuweiten unterbinden (M.INV.BE-BF-USRAU)

> Zuvor hat ein automatisiertes Sicherheitssystem detektiert, dass per Brute Force Nutzerberechtigungen geprüft wurden.

1. Zuerst muss überprüft werden, ob der Nutzer selbst für die Aktivitäten verantwortlich war oder ob ein anderer valider Grund für die Ausführung von zufälligen Operationen vorliegt.
2. Sofern keine validen Gründe vorliegen, sollte der betroffene Nutzer vorerst gesperrt werden und diesbezüglich informiert werden. Die Sperrung darf erst wieder aufgehoben werden, nachdem sichergestellt ist, dass der betroffene Nutzeraccount nicht mehr kompromittiert ist, beispielweise können dem betroffenen Nutzer neue Zugangsdaten ausgestellt werden, um dem Angreifer den Zugang zu entziehen.
3. Weiterhin muss untersucht werden, wie ein Angreifer Zugang zu dem betroffenen Account erlangen konnte, und etwaige Sicherheitslücken müssen geschlossen werden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

System auf Datendiebstahl überprüfen (M.INV.BE-KGDU)

> Zuvor hat ein automatisiertes Sicherheitssystem Hinweise auf Datendiebstahl detektiert.

1. Das betroffene System sollte dokumentiert werden.
2. Es sollte überprüft werden, ob die Anfertigung der Datenkopien und Datenbank-Snapshots berechtigt war.
3. Falls kein valider Grund vorliegt, handelt es sich sehr wahrscheinlich um Datendiebstahl, weshalb die gestohlenen Daten darauf überprüft werden müssen, inwiefern sie kritische oder sensible Daten beinhalten. Ebenso sollten gegebenenfalls verantwortliche Personen in Kenntnis gesetzt werden.
4. Der Inhalt der gestohlenen Daten sollte dokumentiert werden, sowie eine Untersuchung eingeleitet werden, durch welche Schwachstelle der Datendiebstahl möglich war. Gefundene Schwachstellen müssen beseitigt werden.
5. Um zukünftigen Datendiebstahl durch Kopieren von großen Dateien zu erschweren sollte eine Richtlinie eingeführt werden, die besagt, dass das Kopieren von großen Dateien vorher beantragt werden muss und ein kopieren von Daten ohne einen entsprechenden Antrag zur Sperrung der Daten für den entsprechenden Nutzer führt.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen beim Missbrauch von Anmeldedaten (M.INV.BE-VMA)

> Zuvor hat ein automatisiertes Sicherheitssystem einen potentiellen Credential Abuse detektiert.

1. Zeitpunkt und betroffene Accounts sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.

2. Der entsprechende Nutzer umgehend gesperrt werden. Die Sperrung kann erst wieder aufgehoben werden, sobald der betroffene Account neue, sichere Zugangsdaten erhält oder falls sichergestellt wurde, dass es sich hierbei um einen Fehlalarm handelt.
3. Es sollte überprüft werden, ob es sich um einen Fehlalarm handelt, also ob ein berechtigter Nutzer für die Aktivität verantwortlich ist.
4. Falls Credential Abuse für den Alarm verantwortlich war, sollte untersucht werden, wodurch der Credential Abuse zustande kam. Weiterhin kann eine Mehr-Wege-Authentifizierung eingeführt werden, die einen Credential Abuse erheblich erschwert.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Gelöschten Log Einträgen untersuchen (M.INV.BE-GLEU)

Zuvor hat ein automatisiertes Sicherheitssystem die Löschung von Log-Einträgen detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt werden kann, sollte das System schnellstmöglich von anderen Systemen isoliert werden, da die Löschung von Log-Einträgen auf ein kompromittiertes System hindeuten kann. Die Isolierung darf erst wieder aufgehoben werden, nachdem sichergestellt ist, dass es sich hierbei um einen Fehlalarm handelt oder das System keine Kompromittierung mehr aufweist, beispielsweise indem das System mit einem Backup wiederhergestellt wird. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Die Art der Log-Einträge sowie der Zeitpunkt der Löschung sollten dokumentiert werden.
6. Es sollte überprüft werden, ob ein Administrator oder Nutzer selbst für die Löschung verantwortlich war.
7. Wenn eine Kompromittierung festgestellt wurde, sollte untersucht werden, durch welche Schwachstelle der Angreifer in das System eindringen konnte. Alle Befunde sollten behoben und dokumentiert werden. Ebenfalls sollten angrenzende Systeme auf ähnliche Schwachstellen untersucht werden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Verschleierten Prozesse untersuchen (M.INV.BE-VPU)

Zuvor hat ein automatisiertes Sicherheitssystem einen maskierten Prozess detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt werden kann, muss das System schnellstmöglich von anderen Systemen isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, nachdem das System mit einem Backup wiederhergestellt wurde. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.

3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Der Prozessname des unerwarteten Prozesses, sowie der Zeitpunkt der Feststellung sollten dokumentiert werden.
6. Es sollte überprüft werden, ob ein berechtigter Nutzer für die Ausführung des Skripts verantwortlich ist.
7. Sofern ein Angreifer verantwortlich sein sollte, muss untersucht werden, durch welche Schwachstelle der Angreifer die Möglichkeit hatte, das Skript auszuführen. Alle Befunde sollten behoben und dokumentiert werden. Ebenfalls sollten angrenzende Systeme auf ähnliche Schwachstellen untersucht werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Verschleierte/verdächtige Befehle untersuchen (M.INV.BE-VBU)

Zuvor hat ein automatisiertes Sicherheitssystem ein obfuskiertes Skript detektiert.

1. Sofern die Meldung nicht direkt als Fehlalarm erkannt werden kann, ist das System umgehend zu isolieren. Die Isolierung des Systems kann erst wieder aufgehoben werden, sobald das System sicher nicht mehr kompromittiert ist, beispielsweise wenn ein Backup wiederhergestellt wurde oder falls sich die detektierten Skripte und Kommandos im späteren Verlauf als harmlos herausstellen.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Nachdem das System isoliert ist, sollten die Skripte und Kommandos weiter überprüft werden, ob diese trotz Obfuskation einen vertrauenswürdigen Ursprung haben, um einen Fehlalarm auszuschließen.
6. Falls nach der Überprüfung die Skripte und Kommandos als schädlich eingestuft werden, sollte das System umgehend auf Schwachstellen analysiert werden.
7. Die Skripte und Kommandos sollten restlos aus dem System entfernt werden, beispielsweise indem das System mit einem Backup wiederhergestellt wird. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden. Ebenfalls sollten anschließend alle gefundenen Schwachstellen des Systems behoben werden.
8. Skripte ohne vertrauenswürdigen Herausgeber sollten im Normalfall immer erst ausgeführt werden dürfen, nachdem eine Prüfung des Herausgebers stattgefunden hat.
9. Skripte, die nach einer Prüfung des Herausgebers weiterhin verdächtig sind, sollten dokumentiert werden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Deaktivierte Sicherheitseinstellungen untersuchen (M.INV.BE-DSTU)

Zuvor hat ein automatisiertes Sicherheitssystem die Deaktivierung von Sicherheitstools detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt werden kann, muss das System schnellstmöglich von anderen Systemen isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, nachdem das System

mit einem Backup wiederhergestellt wurde. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.

2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Zeitpunkt und betroffene Systeme sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
6. Es sollte überprüft werden, ob die Deaktivierung legitim von einer berechtigten Person ausgeführt wurde.
7. Sofern keine berechtigte Person für die Deaktivierung verantwortlich war, sollte untersucht werden durch welche Schwachstelle ein Angreifer die Möglichkeit hatte die Sicherheitstools zu deaktivieren. Etwaige Sicherheitslücken sind umgehend zu beheben oder unzugänglich zu machen. Ebenfalls sollten angrenzende Systeme auf ähnliche Schwachstellen untersucht werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Diskrepanz zwischen Vorhersagen und Messwerten untersuchen (M.INV.BE-DVMU)

Eine Diskrepanz zwischen Vorhersagen und Messwerten wurde festgestellt.

1. Das System oder Teilsystem, dass unplausible Daten liefert, sollte dokumentiert werden.
2. Zuerst muss überprüft werden, ob ein Software- oder Hardwarefehler Ursache für die Diskrepanzen ist. In diesem Falle ist es hinreichend, das entsprechende Teilsystem zu reparieren. Ebenfalls sollte überprüft werden, ob die falschen Daten zu falschen Handlungen geführt haben.
3. Falls kein Software- oder Hardwarefehler vorliegt, muss das betroffene System auf Schadsoftware überprüft werden.
4. Sollte Schadsoftware gefunden werden, muss das System umgehend von angrenzenden Systemen isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, wenn das System in einen sicheren Zustand zurückgesetzt werden konnte, beispielsweise durch Wiederherstellung eines Backups. Darüber hinaus ist zu überprüfen, wie die Schadsoftware auf das System gelangen konnte, und etwaige Schwachstellen sind zu beheben.
5. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
6. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
7. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
8. Eine weitere mögliche Ursache sind gefälschte Datenpakete im Zuge eines IT-Angriffs. In diesem Falle muss untersucht werden, wie der Angreifer die Datenpakete des Systems spoofen konnte, und welche Sicherheitslücken dies ermöglicht haben. Etwaige Schwachstellen müssen schnellstmöglich behoben oder mindestens unzugänglich gemacht werden.
9. Falls Sicherheitslücken gefunden wurden, sind andere ähnliche Systeme auch auf diese zu überprüfen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Unerwartete Benutzer und dessen Aktivitäten überprüfen (M.INV.CIT-UBAU)

Beim Auflisten aller Nutzern auf dem System wurde die Existenz eines unerwarteten Nutzer festgestellt.

1. Im Falle eines unerwarteten Nutzers muss zuerst festgestellt werden, ob dieser von einem anderen, berechtigten Mitarbeiter erstellt wurde, und ob dieser die Erstellung sinnvoll begründen kann.
2. Falls der Nutzer nicht intern erstellt wurde, kann anhand von Logs verfolgt werden, von wem und wie er erstellt wurde, und welche Aktionen von ihm ausgeführt wurden.
3. Etwaige Aktivitäten des Nutzers sind rückgängig zu machen, gegebenenfalls durch das Wiederherstellen von Backups, und dem Account sind alle Rechte zu entziehen (Zur weiteren Analyse des Angreifers kann der Account aktiviert bleiben, um weitere Aktivitäten zu beobachten. Falls dies nicht gewünscht ist, sollte der Account gelöscht werden).
4. Weiterhin ist die Accounterstellung zu untersuchen, um die Sicherungslücke, die sie ermöglicht hat, zu identifizieren und zu beheben.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Unerwartete Rechte bei einem Benutzer überprüfen (M.INV.CIT-URBU)

Zuvor wurden unerwartete Rechte bei einem Nutzer oder eine Gruppe von Nutzern im System festgestellt.

1. Im Falle unerwarteter Rechte bei einem Nutzer ist zuerst zu überprüfen, ob diese durch eine berechtigte Person begründet gegeben wurden.
2. Sollte keine verantwortliche Person auffindbar sein, sind die Logs des Nutzers zu überprüfen, um herauszufinden, wie er an die zusätzlichen Rechte gelangen konnte (und welche Sicherheitslücken somit bestehen), und ob bzw. wie er sie genutzt hat.
3. Etwaige Aktivitäten des Nutzers sind rückgängig zu machen, gegebenenfalls durch das Wiederherstellen von Backups, und dem Account sind alle Rechte zu entziehen (Zur weiteren Analyse des Angreifers kann der Account aktiviert bleiben, um weitere Aktivitäten zu beobachten. Falls dies nicht gewünscht ist, sollte der Account gelöscht werden).
4. Für den wahrscheinlichen Fall, dass der Account übernommen wurde, ist der ursprüngliche Besitzer zu informieren.
5. Weiterhin sind etwaige Sicherheitslücken, die die Rechtevergabe ermöglicht haben, zu schließen.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Verdächtige Code Ausführung untersuchen (M.INV.CIT-VCAU)

Zuvor hat ein automatisiertes Sicherheitssystem die Ausführung von verdächtigem Code detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt werden kann, muss das System schnellstmöglich von anderen Systemen isoliert werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.

5. Um einen Fehlalarm auszuschließen, sollte danach überprüft werden, ob der unerwartete Code einen vertrauenswürdigen Herausgeber hat und ob die Ausführung berechtigt war.
6. Sollte die Ausführung nicht berechtigt sein und der Code keinen vertrauenswürdigen Herausgeber haben, sollte der unerwartete Code als Schadsoftware eingestuft werden.
7. Die Schadsoftware sollte analysiert werden, um Informationen über einerseits das genaue Angriffsziel, andererseits die ausgenutzten Sicherheitslücken zu erhalten.
8. Sobald alle Sicherheitslücken geschlossen oder unzugänglich gemacht wurden, und das System in einen sicheren Zustand zurückgesetzt wurde, kann es wieder ins Netzwerk eingebunden werden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU)

Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Zuvor wird die Störungsmeldung von Netzleitstelle weitergegeben.

1. Gespräch mit Schaltermeister über die Fehler und feiner differenzieren, was da passiert ist.
2. Verantwortlichen für die Störungsbehebung zuordnen.
   - Es sind andere Techniken betroffen, die die gleiche Technik benutzen. Übergabe an die

     -ÜT-Team. Wenn die Störung mehrere Geräte betroffen ist, dann kann man schon festgestellt, dass der Fehler bei Übertragungstechnik steckt. (s. Punkt 3)
   - Es sind keine weiteren Techniken betroffen. Weitere Untersuchungen bei Fernwirk-/Leittechnik finden nicht statt. (vgl. Punkt 4)
3. Fehlersuche bei ÜT-Team vertiefen. Durch Identifizierung der betroffenen Geräte werden die Verantwortlichen für die Störungsbehebung weiter unterteilt
   - Die Störung wird von fehlerhaften Fernmeldekabel verursacht. Störungsbehebung durch Kabel-Team.
   - Störungsbehebung durch ÜT-Team. (s. Kapitel Übertragungs- und Netzwerktechnik)
4. Fehleruntersuchung bei Fernwirk-/Leittechnik. Um den Überblick zu verschaffen, sind die folgenden Informationen zu verifizieren:
   - *1) Tag/Nacht;*
   - *2) ob Mann in Anlage war;*
   - *3) ob Datenmodell getauscht wurde;*
   - *4) Bereitschaftsrelevant;*
   - *5) Zeitpunkt.*
5. Durch Überprüfung der Informationen wird die Verantwortung der Störungsbehebung ferner identifiziert:
   - Ein Schutzgerät ist betroffen. -> Störungsbehebung durch Schutz-Team.
   - Elektrische Fehler in der Anlage. -> Störungsbehebung durch Sekundär-Team.
   - Man telefoniert mit den Kollegen im Umspannwerk (UW), um Informationen gegenseitig auszutauschen. Wenn der Fehler eindeutig vor Ort angezeigt wird. Störungsbehebung durch die UW-Kollegen.
   - Es sind keine anderen Techniken betroffen. Weitere Untersuchungen bei Fernwirk-/Leittechnik (s. Punkt 6)

6. Gemäß der Inhalt von Störungsmeldungen kann man beurteilen, ob der Fehler in eBASE oder in Fernwirk-/ Leittechnik liegt.
   a) Wenn es die Fehler in Leitsystem steckt, wird die Fehlersuche weiter an Datenaufbreitung(DAB) übergeben.
   b) Wenn es die Fehler in Fernwirk-/Leittechnik steckt, logt man in die Bedienoberfläche der Parametriersoftware setIT ein. Folgende Möglichkeiten kann man ausprobieren:
      - *1) Fehlerdiagnose genauer betrachten;*
      - *2) Datenmodell aktualisieren;*
      - *3) Zustände Schnittstelle/Eingänge aufpassen;*
      - *4) Anlage reset/neu laden*
7. Nach dem entsprechenden Maßnahmen, prüft der Schaltermeister in Leitsystem nach, ob die Störungsmeldung genau quittiert werden kann. Wenn nicht, folgt der weiteren Untersuchungen im nächsten Schritt.
8. Fernwirk-Team zur Anlage mit Ersatzteilen hinfahren. Um den Fehler weiter zu identifizieren, kann man vor Ort folgende Maßnahmen durchführen:
   - *1) Stationsbuch kontrollieren;*
   - *2) Spannung messen;*
   - *3) Optische Diagnose;*
9. Wenn man schon von außen feststellen kann, dass es ein Hardwarefehler ist. Je nach Umständen kann man
   a) entweder die Parametrierung durch FW-Team selbst anpassen,
   b) als auch diese Aufgabe an externen Dienstleister beauftragen
10. Wenn man den Fehler rein optisch nicht verifizieren kann, dann müsste die Abnormalität durch Softwarefehler verursacht werden. Es gibt wieder ein paar Möglichkeiten:
    - Baugruppentausch
    - Weitere Fehlersuche in der Anlage. Erfahrungsgemäß sind die folgenden Fehler möglich:

      -kabelfehler

      -Erdschluss
11. Man gleicht die Information mit Leitsystem ab. Die Störungsmeldung wurde erfolgreich quittiert

Bei der Suche nach der Ursache für die Anomalie sollte eine der unten aufgeführten Beobachtungen gemacht werden.

Fahren Sie mit der Bearbeitung des Vorfalls durch die unten verlinkten neuen Beobachtungen fort.

Zugehörige Beobachtungen

Ein Gerät ist defekt (B.FWT.EGD) auf Seite 32
Ein einzelnes Fernwirkgerätes ist defekt

Die Konfiguration eines Fernwirkgerätes wurde manipuliert (B.FWT.KGM) auf Seite 32
Unautorisierte Veränderung der Konfiguration.

Verbindungsabbruch zu einem Fernwirkgerät (B.FWT.VAG) auf Seite 31
Zu einem einzelnen Fernwirkgerät besteht keine Verbindung mehr.

Ein Gerät liefert unplausible Werte, obwohl es keine Auffälligkeiten bei ihm gibt (B.FWT.EGUWKA) auf Seite 34
Leitsystem empfängt unplausible Werte von einem Fernwirkgerät, welches bei der Überprüfung aber keine Fehler oder Manipulationen aufwies.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Test eines Fernwirkgeräts (M.INV.FWT-EGT)

Ein einzelnes Fernwirkgerät soll nach der Konfiguration getestet werden.

1. Bei der Erstinbetriebnahme wird im ersten Schritt die Verbindung zur NLST getestet, hier ist eine vollständige Generalabfrage „GA“ gefordert.

2. Dann erfolgt ein Datenpunkttest alles Informationen. Vor der Inbetriebnahme werden die Schaltgeräte von der NLST scharf geschaltet.
3. Im Fehlerfall wird eine GA seitens der NLST durchgeführt, dann werden Werte verglichen und zum Abschluss ein Befehl getestet. Meistens etwas unkritisches wie Automatik Ein/Aus.

Das Fernwirkgerät wird geprüft und in Betrieb genommen

Zugehörige Maßnahmen

Einbau eines Fernwirkgeräts (M.REA.FWT-GEB) auf Seite 106
Ein einzelnes Fernwirkgerät soll installiert werden.

Konfiguration eines Fernwirkgeräts (M.REA.FWT-KFW) auf Seite 106
Ein einzelnes Fernwirkgerät soll nach dem Einbau konfiguriert werden.

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Unerwartete Neustarts untersuchen (M.INV.FWT-UNS)

Ein System wurde unerwartet neugestartet.

1. Bei einem für den Beobachter unerwartet wirkenden Neustart ist anhand von Logs zu überprüfen, was ihn verursacht hat. Sollte keine sinnvolle Ursache gefunden werden, ist die Systemsoftware zu verifizieren, um Manipulationen auszuschließen. Hierzu nutzen Sie unten verknüpfte Beobachtung. Weiterhin ist zu überprüfen, ob der Neustart durch eine Sicherheitslücke ausgelöst werden konnte, und diese gegebenenfalls zu schließen, oder mindestens der Außenwelt unzugänglich zu machen.
2. Falls Manipulationen oder Sicherheitslücken entdeckt wurden, sind ähnliche Systeme auf dieselben zu überprüfen.

Falls die Ursache für die Neustarts gefunden werden konnte, kann mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen die Bearbeitung abgeschlossen werden.

Zugehörige Beobachtungen

Falsche Firmware-Version (B.FWT.FFW) auf Seite 33

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Nicht-Plausible Anmeldung von Anlagen untersuchen (M.INV.FWT-NPAAU)

Zuvor wurde eine Energieressource mit unplausiblen Daten angemeldet.

1. Die verwendeten Anmeldedaten sollten verifiziert werden, um einen Fehlalarm auszuschließen.
2. Sollten die Daten tatsächlich falsch sein, und sollte zudem kein normaler Bedienungsfehler seitens des Endnutzers vorliegen, ist davon auszugehen, dass es sich um ein unbekanntes Gerät handelt. Für die weitere Bearbeitung ist dann die untern verknüpfte Beobachtung zu nutzen. Alternativ kann auch erst versucht werden mittels Fingerprinting mehr über das auffällige Gerät herauszufinden.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Beobachtungen

Es wird ein Fremdgerät im Übertragungsnetz entdeckt (B.ÜT/NT.FGE) auf Seite 28

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Fingerprinting eines Systems an Hand seiner IP-Adresse (M.INV.ÜT/NT-FPIP) auf Seite 98

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Quelle von Fehlinformationen im Leitsystem untersuchen (M.INV.LS-FLSU)

Die Quelle von Fehlinformationen oder unplausiblen Messwerten soll untersucht werden.

Zuvor hat ein Bediener falsche, fragwürdige oder unplausbible Messwerte oder anderweitige Informationen im Leitsystem entdeckt.

1. Melden Sie dem Schichtleiter den Vorfall.

2. Klären Sie mit dem Schichtleiter, wer den Vorfall weiter untersuchen soll.
   - Der Schichtleiter bestimmt Sie zur weiteren Bearbeitung.
   - Der Schichtleiter bestimmt einen anderen Kollegen für die weitere Bearbeitung des Vorfalls.
   - Der Schichtleiter bestimmt, dass zu jetzigen Zeitpunkt keine weitere Bearbeitung möglich oder notwendig ist.
3. Falls ein anderer Kollege bestimmt wurde, übergeben Sie den Vorfall und weisen Sie Ihren Kollegen ein.
4. Falls zum jetzigen Zeitpunkt keine weitere Bearbeitung möglich ist, dokumentieren Sie den Vorfall, um eine spätere Analyse zu ermöglichen.
   a) Notieren Sie hierzu Ihre Beobachtung.
   b) Fertigen Sie nach Möglichkeit Sreenshots an, die die Beobachtung abbilden.
5. Falls Sie vom Schichtleiter bestimmt wurden, versuchen Sie die Quelle der falschen Informationen / Messwerte / Anzeigen herauszufinden.

Bei der Suche nach der Quelle sollte eine der unten verlinkten neuen Beobachtungen auftreten.

Fahren Sie mit der Bearbeitung des Vorfalls durch die unten verlinkten neuen Beobachtungen fort.

Zugehörige Beobachtungen

Ein Gerät liefert unplausible Werte (B.FWT.EGUW) auf Seite 31
Ein einzelnes Fernwirkgeräte liefert unplausible Werte

Mehrere Geräte liefern unplausible Werte (B.FWT.MGUW) auf Seite 32
Mehrere Fernwirkgeräte liefern unplausible oder falsche Werte

Fehlinformationen im Leitsystem ohne Quellzuordnung entdeckt (B.LS.FIKQ) auf Seite 17
Im Leitsystem wurden fehlerhafte / unplausible Informationen entdeckt, die keiner bestimmten Quelle zugeordnet werden können

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Ein- und Ausgehenden Traffic auf Anomalien untersuchen (M.INV.LS-NA-EATU)

Zuvor hat ein automatisiertes Sicherheitssystem Netzwerk-Anomalien detektiert.

1. Das betroffene System ist zunächst zu isolieren. Die Isolierung kann erst wieder aufgehoben werden, nachdem sichergestellt wurde, dass das System keine Kompromittierung aufweist oder ein valider Grund die Netzwerk Anomalie begründet.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Der eingehende und ausgehende Traffic, sowie alle offenen Ports des betroffenen Systems sollten überprüft werden, um einen Fehlalarm auszuschließen.
6. Falls im Traffic Anomalien zu finden sind, oder falls offene Ports eigentlich geschlossen sein sollten, ist von einer Kompromittierung des Systems auszugehen, weshalb das System auf Schwachstellen zu analysieren ist.
7. Das System sollte mit einem Backup wiederhergestellt werden und alle Schwachstellen beseitigt werden. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

ARP Spoofing überprüfen und unterbinden (M.INV.LS-NA-ARP)

Zuvor hat ein automatisiertes Sicherheitssystem einen ARP-Spoofing-Netzwerk-Angriff detektiert.

Der Angriff kann entweder von einem bekannten Gerät oder auch von einem Fremdgerät ausgegangen sein. In jedem Fall ist der Ursprung des Angriffs über mehrere Stufen hinweg zu prüfen.

1. Falls möglich, und nicht bereits automatisiert geschehen, muss der Host, von dem der Angriff ausging, umgehend gesperrt und das angegriffene System isoliert werden. Falls die Meldung des Sicherheitssystems den genauen Ursprung nicht beinhaltet, können die Logs von Switches und Routern nach neuen Geräten oder ARP-Nachrichten durchsucht werden. Sollte es sich **nicht** um ein Fremdgerät handeln, ist zu untersuchen, wie der Angreifende Zugriff erlangen konnte. Hierbei sollten Log-Dateien gemäß M.INV.ZB-ULEB (Seite 90) untersucht werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Erfolgreiches Spoofing deutet darauf hin, dass ein Switch oder Router nicht korrekt konfiguriert ist. Daher müssen alle entsprechenden Systeme auf Sicherheitslücken und Konfigurationsfehler untersucht und diese behoben werden.
6. Weiterhin muss das angegriffene System untersucht werden, um den Zweck des Angriffs herauszufinden und eventuelle Schäden rückgängig zu machen.
7. Nachdem alle Sicherheitslücken und Schäden nach M.INV.AGR (Seite 74) behoben wurden und das angegriffene System in einen sicheren Zustand zurückversetzt wurde, kann die Isolation aufgehoben werden. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatzsystems in Betracht gezogen werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

IP Spoofing überprüfen und unterbinden (M.INV.LS-NA-IPSU)

Zuvor hat ein automatisiertes Sicherheitssystem einen Netzwerk-Angriff detektiert.

1. Falls möglich, und nicht bereits automatisiert geschehen, muss der betroffene Host umgehend gesperrt und das angegriffene System isoliert werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Erfolgreiches Spoofing deutet darauf hin, dass eine Firewall bzw. ein Eingangsfilter falsch oder unzureichend konfiguriert wurde. Daher müssen alle entsprechenden Systeme auf Sicherheitslücken und Konfigurationsfehler untersucht und diese behoben werden.
6. Weiterhin muss das angegriffene System untersucht werden, um den Zweck des Angriffs herauszufinden und eventuelle Schäden rückgängig zu machen.
7. Nachdem alle Sicherheitslücken und Schäden behoben wurden und das angegriffene System in einen sicheren Zustand zurückversetzt wurde, kann die Isolation aufgehoben werden. Handelt es sich bei dem betroffenen

System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Keine oder verzögerte Reaktion von Steuerbefehlen untersuchen (M.INV.LS-KVRSU)

Ein System ist entweder nicht mehr erreichbar, oder zwar erreichbar, reagiert aber nicht oder nur stark verzögert auf Steuerbefehle.

1. Zuerst muss überprüft werden, ob die Ursache ein Verbindungsproblem ohne den Hintergrund eines IT-Angriffs ist, oder ob ein IT-Angriff als Ursache angenommen werden muss, und das betroffene System/Gerät möglicherweise kompromittiert wurde.
2. Sollte kein allgemeines Verbindungsproblem festgestellt werden können, muss das betroffene System/Gerät isoliert werden und auf Schadsoftware überprüft werden. Eine Neuinstallation der Firmware ist nicht hinreichend, da eine etwaige Sicherheitslücke bestehen bleibt, und das System wieder infiziert werden könnte.
3. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
4. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
5. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
6. Falls Schadsoftware gefunden werden konnte, müssen etwaige Schwachstellen, durch welche diese installiert werden konnte, behoben werden. Dies betrifft auch alle weiteren gleichartigen Fernwirkgeräte. Weiterhin müssen alle betroffenen Fernwirkgeräte in einen bekannt sicheren Zustand zurückversetzt werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Beobachtungen

Verbindungsabbruch zu einem Fernwirkgerät (B.FWT.VAG) auf Seite 31
Zu einem einzelnen Fernwirkgerät besteht keine Verbindung mehr.

Verbindungsabbruch zu mehreren Fernwirkgeräten (B.FWT.MGKV) auf Seite 31
Zu mehreren Fernwirkgeräten besteht keine Verbindung mehr.

Malware Infection (B.AS.MIn) auf Seite 61

Das Leitsystem oder die Software scheint kompromittiert zu sein. (B.LS.LSKo) auf Seite 17
Ein Standort des Netzleitsystems zeigt Auffälligkeiten und ist gegebenenfalls kompromittiert.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Nicht autorisierte Steuerbefehle unterbinden (M.INV.LS-NASU)

Zuvor wurde festgestellt, dass ein System Steuerbefehle unbekannter Herkunft erhält.

1. Um einen Fehlalarm auszuschließen muss zuerst überprüft werden, ob eventuell eine legitimierte Person für die Steuerbefehle verantwortlich sein könnte, beispielsweise im Zuge von Wartungsarbeiten.
2. Sollte dies nicht der Fall sein, muss von einem Angriff und somit einem kompromittierten System ausgegangen werden. Daher muss das System umgehend isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, wenn das System mittels eines Backups wiederhergestellt wurde. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.

3. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
4. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
5. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
6. Im Angriffsfall ist das System auf Schwachstellen zu untersuchen, die den Angriff möglich machten, und diese zu beseitigen oder unzugänglich zu machen. Weiterhin ist das System in einen bekannt sicheren Zustand zurückzusetzen.
7. Ähnliche Systeme müssen auf dieselben Schwachstellen untersucht werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Software des Leitsystems überprüfen (M.INV.LS-SWU)

Die Softwarestände des Leitsystems müssen überprüft werden.

> Zuvor hat ein Bediener falsche, fragwürdige oder unplausibile Messwerte oder anderweitige Informationen im Leitsystem entdeckt. Es konnte auch keine Quelle für die Fehlinformation außerhalb des Leitsystems ausgemacht werden.

1. Die Softwarestände aller Module des Leitsystems müssen überprüft werden.

   Gegebenenfalls müssen Sie hierzu den Softwarehersteller hinzuziehen.
2. Vergleichen Sie hierzu die dokumentierten Versionsnummern der Module mit den installierten.
3. In aller Regel sollten die Softwaremodule über eine Signatur oder Checksumme verfügen, die ebenfalls abgeglichen werden muss.

Bei der Überprüfung sollte eine der unten verlinkten neuen Beobachtungen auftreten.

Fahren Sie mit der Bearbeitung des Vorfalls durch die unten verlinkten neuen Beobachtungen fort.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61

Das Leitsystem oder die Software scheint kompromittiert zu sein. (B.LS.LSKo) auf Seite 17
Ein Standort des Netzleitsystems zeigt Auffälligkeiten und ist gegebenenfalls kompromittiert.

Falsche Firmware-Version (B.FWT.FFW) auf Seite 33

Falsche Firmware-Prüfsumme (B.FWT.FFPS) auf Seite 33

Zugehörige Maßnahmen

Hersteller hinzuzuziehen (M.KOM.HSH) auf Seite 73
Für die weitere Bearbeitung eines Vorfalls, ist der Hersteller der Software/ Komponente hinzuzuziehen.

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Verdächtige Personen vor dem Firmen Gelände entdeckt (M.INV.SFM-VPVFGE)

> Zuvor wurde entdeckt, dass relevante Orte beobachtet werden.

1. Die Beobachtung sollte zuerst nach Möglichkeit näher untersucht werden, um Verwechslungen auszuschließen.
2. Sofern der Verdacht bei näherer Untersuchung nicht ausgeschlossen werden konnte sind relevante Wachhabende zu informieren. Darüber hinaus sollten Eingangskontrollen von Fremden wie z.B. Kontraktoren verschärft werden, da durch die observierten Informationen bessere Vorwände oder Alibis ermöglicht werden.
3. In jedem Fall ist der Vorfall zu protokollieren, um Nachverfolgbarkeit zu sicherzustellen.

Mit der vollständigen Dokumentation von Beobachtung , erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Ordnungsgemäße Handlung beim Fund von unbekannten Peripheriegeräten (M.INV.SFM-OHFVP)

Zuvor wurde ein verdächtiges Peripheriegerät gefunden.

1. Sofern das betroffene Peripheriegerät noch nicht mit einem firmeneigenen System verbunden wurde, kann es hinreichend sein, das Gerät sicher zu verwahren, sodass es nicht verwendet wird, und den Vorfall zu protokollieren.
2. Sollten Zweifel bestehen, ob das Gerät vielleicht doch legitim sein könnte (und dadurch wichtige Daten enthalten könnte), oder sollten sich derartige Vorfälle häufen, ist ein IT-Experte hinzuzuziehen, der das Gerät in einer sicheren Umgebung auf Schadsoftware überprüfen kann.
3. Falls das Gerät bereits angeschlossen wurde, ist das betroffene System schnellstmöglich vom restlichen Netzwerk zu isolieren und auszuschalten. Die Analyse durch einen Experten ist in diesem Fall unabdinglich, je nach Ergebnis müssen eventuell andere Systeme im Netzwerk auch auf die Schadsoftware überprüft werden.
4. Wenn bei dieser Untersuchung Schadsoftware gefunden wird, kann das genaue Verhalten dieser Aufschluss über Zweck und Ziel des Angriffs geben.
5. Diese Informationen sind an die jeweiligen Verantwortlichen des Zielsystems weiterzuleiten.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Phishing überprüfen und gegebenenfalls Auswirkung untersuchen (M.INV.SFM-PUAU)

Ein Nutzer ist Ziel eines Phishingangriffs.

1. Zuerst muss überprüft werden, ob der betroffene Nutzer auf den Phishing-Versuch eingegangen ist, und um welche Art Phishing es sich handelt.
2. Sofern der Nutzer nicht darauf eingegangen ist, ist es hinreichend, andere Nutzer über die Herangehensweise des Phishing-Angriffs zu informieren, um sie vor ähnlichen Angriffen zu schützen. Zusätzlich kann eine Analyse des Angriffs genauere Informationen über sein Ziel geben.
3. Sollte der Nutzer auf den Phishing-Versuch eingegangen sein, sind alle Auswirkungen zu mitigieren (dabei kann es sich z.B. um veröffentlichte Zugangsdaten oder unberechtigt ausgeführte Schadsoftware handeln). Auch hier ist es sinnvoll, den Angriff zu analysieren, und andere Nutzer über die Umstände zu informieren, um sie vor weiteren Angriffen dieser Art zu schützen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Denial of Service unterbinden (M.INV.ZB-DOSU)

Ein System ist gerade von einem Denial-of-Service-Angriff betroffen.

1. Zunächst sollte überprüft werden, ob ein technischer Defekt die Ursache für die erhöhten Ladezeiten sein könnte. Falls kein technischer Defekt vorliegt, ist ein Angriff auf das Netzwerk naheliegend, weshalb

eingehender Traffic überprüft werden sollte. Falls verdächtiger Traffic gefunden wurde, sollten die IP-Adressen, von denen der Angriff ausgeht, gesperrt werden. Bei Distributed-Denial-of-Service-Attacken ist eventuell eine temporäre Sperrung sinnvoller, da große IP-Bereiche betroffen sein könnten.

2. Angegriffene Systeme sollten auf die Integrität ihrer Software untersucht werden, um die Verschleierung eines weiteren Angriffs auszuschließen.
3. Relevante Personen sollten darüber informiert werden, dass eventuell weitere Angriffe zu erwarten sind.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Erhöhte Systemauslastung senken (M.INV.ZB-ESAS)

> Zuvor wurde eine unerwartet hohe Auslastung bei einem System bemerkt.

1. Das betroffene System sollte dokumentiert werden.
2. Es muss überprüft werden, wodurch die Auslastung entsteht. Da Denial-of-Service-Angriffe häufige Gründe für eine Systemüberlastung sind, sollte insbesondere überprüft werden, ob Anfragen von einer nicht vertrauenswürdigen IP-Adresse gesendet werden.
3. Falls ein Denial-of-Service-Angriff vermutet wird, sollten die verantwortlichen IP-Adressen blockiert werden. Wenn unerwartete Prozesse der Grund für die Systemüberlastung sind, sollten die Prozesse auf ihre Herkunft überprüft werden. Sollten diese sich als Schadsoftware herausstellen, muss das System umgehend von angrenzenden Systemen isoliert werden. Die Isolation darf erst wieder aufgehoben werden, wenn das System in einen bekannt sicheren Zustand versetzt wurde, beispielsweise durch Wiederherstellung eines Backups.
4. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
5. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
6. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
7. Wenn Schadsoftware für die erhöhte Auslastung verantwortlich ist, sollte das System auf Schwachstellen überprüft werden, die das Ausführung der Schadsoftware möglich gemacht hat, und diese gegebenenfalls behoben werden. Um zukünftige Angriffe zu erschweren sollten zudem angrenzende Systeme auf ähnliche Schwachstellen überprüft werden.
8. Falls ein Denial-of-Service-Angriff die Ursache für die erhöhte Auslastung war, sollten die Einstellungen der Firewall angepasst werden, um zukünftige Angriffe zu erschweren.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Unerwartete Log-Einträge behandeln (M.INV.ZB-ULEB)

> In den Logs eines Systems wurden unerwartete Einträge gefunden oder es soll gezielt nach Anomalien gesucht werden.

1. Zuallererst sind die verdächtigen bzw. unerwarteten Logeinträge zu sichern, um ein nachträgliches Löschen durch einen Angreifer zu verhindern.
2. Im Folgenden werden die Logeinträge analysiert, wobei evtl. ein Experte für das betroffene Teilsystem hinzuzuziehen ist. Die erste Fragestellung hierbei ist, ob eine interne Ursache für die Einträge gefunden werden kann, oder ob von einer Manipulation bzw. einem Angriff ausgegangen werden muss. Besonders zu beachten sind Loginversuche bzw. durchgeführte Logins (B.BE.CrAb (Seite 48)).

3. Falls ein wahrscheinlicher Angriff vorliegt, ist nachzuvollziehen, durch welche Sicherheitslücke die Aktivitäten ausgeführt werden konnten, welche Wirkung erzielt wurde, und welchen Zweck der Angriff gehabt haben könnte.
4. Daraufhin ist die Sicherheitslücke nach Möglichkeit zu schließen, oder zumindest von außen unzugänglich zu machen. Weiterhin müssen alle betroffenen Systeme überprüft werden, und eventuelle Veränderungen zurückgesetzt werden. Je nach System können auch Backups wiederhergestellt werden, um die Effekte des Angriffs rückgängig zu machen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Verdächtige Anmeldeversuche unterbinden (M.INV.AS-BF-VAU)

Zuvor hat ein automatisiertes Sicherheitssystem einen Brute-Force-Versuch detektiert.

1. Falls die Meldung nicht sofort als Fehlalarm erkannt wird, sollten, sofern nicht bereits automatisiert geschehen, alle betroffenen Accounts temporär gesperrt werden, um den Angriff bzw. vermeintlichen Angriff vorsorglich zu unterbinden.
2. Zeitpunkt und betroffene Systeme sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
3. Es sollte überprüft werden, ob die betroffenen Nutzer selbst für die fehlgeschlagenen Loginversuche verantwortlich sind oder ob ein anderer valider Grund vorliegt.
4. Falls es sich hierbei tatsächlich um Bute-Force-Versuche handelt, dürfen die betroffenen Account erst wieder freigegeben werden, nachdem die IP-Adresse des Angreifers identifiziert und gesperrt wurde.
5. Um weitere Brute-Force-Angriffe zu erschweren, kann eine Mehr-Wege-Authentifizierung eingeführt werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Verdeckte Kommunikationskanäle untersuchen (M.INV.AS-VKKU)

Zuvor hat ein automatisiertes Sicherheitssystem einen verdeckten Kommunikationskanal detektiert.

1. Falls es sich nicht um einen offensichtlichen Fehlalarm handelt, ist das System umgehend von benachbarten Systemen zu isolieren.
2. Anschließend sollte überprüft werden, ob es sich um einen Fehlalarm handelt.
3. Je nach Kritikalität des Systems gibt es an dieser Stelle zwei Möglichkeiten: Entweder der Kommunikationskanal wird umgehend gesperrt, oder es werden kurzzeitig Pakete mitgeschnitten, um Aufschluss über die genauen Aktivitäten zu bekommen, und der Kommunikationskanal wird danach gesperrt.
4. In jedem Fall muss das System auf Folgen des Angriffs überprüft werden, um diese daraufhin gegebenenfalls zu beheben. Etwaige mitgeschnittene Pakete können zusätzlich Aufschluss über die Auswirkungen geben.
5. Weiterhin ist das System auf Sicherheitslücken zu untersuchen, die die Kompromittierung und den Aufbau des Kommunikationskanals erlaubt haben.
6. Nach Behebung aller Angriffsauswirkungen und Sicherheitslücken kann die Isolation wieder aufgehoben werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Überprüfung weiterer Kommunikationsausfälle im Störungszusammenhang (M.INV.WKA)

Im Rahmen eines erkannten lokalen Ausfalls ist das System auf Ausfälle und Störungen unabhängiger Dienste und Verbindungen zu prüfen. Entsprechende Vorfälle deuten auf eine zentrale Ursache für eine Störung oder einen Angriff hin.

1. Überprüfung der Fehlermeldungen der Managementsysteme. M.INV.MAN (Seite 92)
2. Überprüfen des Dokumentationssystems. M.INV.DOK (Seite 92)

   Eine von mehreren Techniken genutzte Infrastruktur (Kabel, Gebäude, Räume) grenzt bei einer gemeinsamen Störung die Fehlerstelle ein. Wenn keine gemeinsame Störung vorliegt, schließt dies einige Fehlermöglichkeiten weitestgehend aus.
3. Erkannte Kommunikationsausfälle mit einzelnen Standorten oder Komponenten werden durch einen Techniker vor Ort überprüft und behoben (M.INV.HVO (Seite 93)).
4. Alle Ausfälle und Störungen werden gemäß M.INV.AGR (Seite 74) hinsichtlich eines potentiellen Angriffs geprüft und aufbereitet.

Die Informationen zum Fehlerbild werden für die weitere Fehlersuche benötigt und entsprechend dokumentiert M.KOM.INF (Seite 71)

Zugehörige Beobachtungen

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung der Fehlermeldungen in Managementsystemen (M.INV.MAN) auf Seite 92

Überprüfung der Dokumentation der gestörten Verbindung (M.INV.DOK) auf Seite 92

Erfassung und Übergabe der Fehlerinformation (M.KOM.INF) auf Seite 71

Überprüfung der Fehlermeldungen in Managementsystemen (M.INV.MAN)

Bei der Nutzung eines oder unterschiedlicher Managementsysteme für die eingesetzten Übertragungstechniken werden die aktuellen und zeitnahen Meldungen überprüft.

1. Bei der Überprüfung der Fehlermeldungen wird ein zeitlicher Zusammenhang beim Auftreten untersucht. Ein annähernd zeitgleiches Auftreten deutet auf eine gemeinsame Ursache hin.
   Beim Vergleich der Zeitstempel ist darauf zu achten, welche Zeiteinstellung das jeweilige System nutzt!
2. Bei zeitgleichen Störungen ist auf einen geographischen Zusammenhang zu achten, um einen Fehlerort zu bestimmen.
   Bei Weitverkehrsanbindungen ist es möglich, dass betroffene Systeme einen deutlichen geographischen Abstand zur Fehlerstelle und ggf. zu anderen in dem Kontext gestörten Systemen haben!
3. Zusätzlich zu den Systemmeldungen sollte, soweit möglich, der aktuelle Zustand der betroffenen Techniken direkt auf den Geräten ermittelt werden.

Die Informationen zum Fehlerbild werden für die weitere Fehlersuche benötigt und entsprechend dokumentiert M.KOM.INF (Seite 71).

Zugehörige Beobachtungen

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Zugehörige Maßnahmen

Überprüfung weiterer Kommunikationsausfälle im Störungszusammenhang (M.INV.WKA) auf Seite 92

Überprüfung der Dokumentation der gestörten Verbindung (M.INV.DOK) auf Seite 92

Erfassung und Übergabe der Fehlerinformation (M.KOM.INF) auf Seite 71

Überprüfung der Dokumentation der gestörten Verbindung (M.INV.DOK)

In dem für die Technik genutzten Dokumentationssystem werden die geographischen, physikalischen und logischen Parameter der gestörten Verbindung überprüft und zur Fehlereingrenzung herangezogen.

Die gewonnenen Informationen werden für weitere Bearbeitung dokumentiert. M.KOM.INF (Seite 71)

Zugehörige Beobachtungen

Im Managementsystem wird ein Signalausfall gemeldet (B.ÜT/NT.MNS) auf Seite 28

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung der Fehlermeldungen in Managementsystemen (M.INV.MAN) auf Seite 92

Erfassung und Übergabe der Fehlerinformation (M.KOM.INF) auf Seite 71

Hardwareprüfung vor Ort (M.INV.HVO)

Die Fehlersuche vor Ort hängt vom Störungsbild ab. Folgende Bereiche werden nach Bedarf in die Fehlersuche einbezogen:

- Spannungsversorgung
- Gerätefunktion
- Verkabelung
- Fernkabel

1. Wenn das betroffene Gerät über optische Meldeelemente verfügt, kann dadurch der Status der Spannungsversorgung ermittelt werden. Wird ein Ausfall erkannt oder die Anzeigen fehlen, muss die Spannungsversorgung weitergehend überprüft werden (M.INV.ÜT/NT-ÜSV (Seite 93)).
2. Sobald die Spannungsversorgung gewährleistet ist, muss bei einem Gerät der Übertragungstechnik die Funktion der Sendeeinheit geprüft werden (M.INV.ÜT/NT-ÜSÜ (Seite 94))
3. Ist die Sendeeinheit funktionsfähig, ist die Verkabelung des Gerätes sowie der zugehörigen Netzwerkgeräte zu überprüfen (M.INV.ÜT/NT-ÜDV (Seite 95)).
   Bei der Verkabelung handelt es sich um die für die Übertragung des Datensignals notwendigen Patchkabel und Patchfelder von der Sendeeinheit der Übertragungstechnikgerätes bis zum Anschlusspunkt des Fernkabels.
4. Insbesondere ist das Fernkabel (Kupfer- oder Lichtwellenleiter), welches die Standorte einer Kommunikationsverbindung verbindet, auf Unversehrtheit und korrekten Anschluss zu prüfen (M.INV.ÜT/NT-ÜDV (Seite 95)).
5. Alle Ausfälle und Störungen werden gemäß M.INV.AGR (Seite 74) hinsichtlich eines potentiellen Angriffs geprüft und aufbereitet.

Nach Abschluss der Fehlersuche und der Behebung ist eine Funktionskontrolle durchzuführen. **TODO: Maßnahme?**

Zugehörige Beobachtungen

Fehler Spannungsversorgung (B.ÜT/NT.FSP) auf Seite 27

Das Übertragungstechnikgerät steht unter Spannung und ist betriebsbereit. (B.ÜT/NT.ÜsSb) auf Seite 27

Die Übertragungseinheit sendet mit einem zulässigen Pegelwert, aber kein Empfangssignal (B.ÜT/NT.KES) auf Seite 28

Zugehörige Maßnahmen

Überprüfung der Spannungsversorgung (M.INV.ÜT/NT-ÜSV) auf Seite 93

Überprüfung der Sendeeinheit einer Übertragungstechnik (M.INV.ÜT/NT-ÜSÜ) auf Seite 94

Überprüfung der Datenverkabelung (M.INV.ÜT/NT-ÜDV) auf Seite 95

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung der Spannungsversorgung (M.INV.ÜT/NT-ÜSV)

Ein kompletter Geräteausfall kann durch einen Gerätedefekt oder einen Ausfall der Versorgungsspannung verursacht werden. Die Spannungsversorgung einer Übertragungstechnik kann folgende Bereiche einschließen:

- Elektrische Verteilung mit der zugehörigen Sicherung
- Verkabelung und Anschlusskabel
- Externe Netzteile
- Interne Netzteile

Bei Arbeiten an elektrischen Anlagen sind die einschlägigen Sicherheitsvorschriften (DIN VDE 0105-100 VDE 0105-100:2015-10; Betrieb von elektrischen Anlagen – Teil 100: Allgemeine Festlegungen) und unternehmensspezifische Vorschriften zu beachten. Sollte eine Manipulation festgestellt werden, sind umgehend Maßnahmen entsprechend (M.REA.ÜT/NT-Ma (Seite 122)) zu ergreifen.

1. Elektrische Verteilung mit der zugehörigen Sicherung
   a) Identifikation und Überprüfung des Zustandes des zugehörigen Sicherungselements.
   b) Wenn die Sicherung ausgelöst hat, diese wieder einschalten. Sollte es erneut zu einer Auslösung kommen, sind die angeschlossenen Verbraucher vom diesem Stromkreis zu trennen und die Sicherung erneut einzuschalten.
   c) Wenn es ohne angeschlossene Verbraucher zu einer Sicherungsauslösung kommt, sind die Zuleitungen, Anschlusskabel und Klemmenverbindungen zu prüfen.
2. Verkabelung und Anschlusskabel.
   a) Die Zuleitung ist einer Sichtprüfung zu unterziehen. Dabei ist auf mechanische Schäden und Anzeichen einer thermischen Überlastung zu achten.
   b) Klemm- und Verteilungspunkte sind einer Sichtprüfung zu unterziehen. Dabei ist auf mechanische Schäden und Anzeichen einer thermischen Überlastung zu achten.
   c) Die Geräteanschlussleitung ist einer Sichtprüfung zu unterziehen. Dabei ist auf mechanische Schäden und Anzeichen einer thermischen Überlastung zu achten.
   d) Wenn bei der Sichtprüfung keine Schäden festgestellt werden können, ist die Zuleitung von der Sicherung zu trennen und der Sicherungsautomat einzuschalten. Kommt es weiterhin zu einer Auslösung ist das Sicherungselement zu tauschen. Andernfalls ist die Zuleitung inklusive aller Klemmpunkte mit einem geeigneten Messgerät (Isolationstester, Widerstandsmessgerät) zu überprüfen.
3. Externe Netzteile. Wenn in der Zuleitung keine Fehler vorliegen, sind, wenn vorhanden, die externen Netzteile zu überprüfen.
   a) Die Eingangs- und Ausgangsspannung werden mit einem geeigneten Messgerät überprüft.
   b) Wenn keine Eingangsspannung vorhanden ist, muss die Durchgängigkeit der Zuleitung messtechnisch überprüft werden.
   c) Wenn keine Ausgangsspannung vorhanden ist, wird das Netzteil getauscht. Sollten auf dem Netzteil Sicherungselemente für die Ausgangsspannung vorhanden sein, werden diese überprüft und bei einer Auslösung wiedwer eingeschaltet bzw. gewechselt.
   d) Wenn eine Ausgangsspannung vorhanden ist, muss das interne Netzteil des Übertragungstechnikgeräts überprüft werden.
4. Internes Netzteil
   a) Ist ein auswechselbares internes Netzteil vorhanden, wird diese ausgetauscht.
   b) Ist das interne Netzteil nicht tauschbar, muss das gesamte Gerät ausgetauscht werden.

Abschließend ist die korrekte Funktion zu überprüfen.

Zugehörige Maßnahmen

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung der Sendeeinheit einer Übertragungstechnik (M.INV.ÜT/NT-ÜSÜ)

Das Gerät ist betriebsbereit. Somit wird als nächstes die Funktion der Sendeeinheit überprüft. Dies umfasst:

- Messung der Sendeleistung
- Messung der Empfangsleistung
- Überprüfung der Konfiguration

- Austausch des Sendemoduls

1. Messung des Sendepegels und / oder Empfangspegel mit einem geeigneten Messgerät. Dabei ist auf die korrekt eingestellte Wellenlänge zu achten. Da Übertragungstechniken als Sicherheitsmaßnahme bei Signalverlust nur noch Sendeimpulse übertragen, muss ein solcher Impuls abgewartet werden.
   a) Messung über einen Zeitraum von 2 - 5 Minuten. In diesem Zeitraum sollte ein Sendeimpuls auftreten.
   b) Wenn vorhanden, manuelle Auslösung des Sendeimpulses.
   c) Es ist darauf zu achten, dass Sende- und Empfangspegel die Betriebsparameter der betroffenen Sendeeinheit einhalten.
2. Wenn kein Sendesignal vorhanden ist, kann die Konfiguration überprüft werden oder gleich präventiv das Sendemodul getauscht werden. Wenn kein Empfangssignal messbar ist, deutet das auf eine Unterbrechung des Kommunikationsweges oder einen Fehler am Gegengerät hin.
   a) Verbindung mit dem betroffenen Gerät herstellen.
   b) Überprüfung der Hardwarekonfiguration. Dabei wird kontrolliert, ob ein korrektes Sendemodul am Gerät angemeldet ist
   c) Überprüfung der Kommunikationkonfiguration. Dabei werden die Einstellungen der Sende- und Empfangsparameter kontrolliert.
3. Ein fehlendes Sendesignal kann auf ein defektes Sendemodul hinweisen. Durch einen Austausch kann dies überprüft werden.
   a) Bei einem Einsteckmodul, z. B. *SFP*, wird dieses gegen ein baugleiches getauscht.

Wenn bei der Überprüfung der Sendeeinheit kein Fehler feststellbar war, muss die Datenverkabelung überprüft werden.

Zugehörige Maßnahmen

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung der Datenverkabelung (M.INV.ÜT/NT-ÜDV)

Die Überprüfung der Datenverkabelung umfasst folgende Bereiche bis zum Anschlusspunkt der Datenkabel:

- Patchkabel
- Verbindungskabel
- Patchpunkte und Steckverbindungen
- Dämpfungsglieder
- Fernkabel

Für die Überprüfung der Datenverkabelung sind Sende- mit passenden Empfangsgeräten einzusetzen.

1. Überprüfung der Gesamtverkabelung
   a) Die Verbindung wird am Anschluss des Gerätes und des Fernkabels getrennt und alle Fasern bzw. Adern gemessen. Diese müssen durchgängig sein. Wenn eine Durchgängigkeit ermittelt wurde, ist eine Überprüfung in der Gegenstation und / oder des Fernkabels notwendig.
2. Wenn die Gesamtverbindung nicht durchgängig ist, muss die Verkabelung in Messabschnitte unterteilt werden. Dadurch kann der fehlerbehaftete Abschnitt eingegrenzt werden.
   a) Wenn zwischen Gerät und Fernkabel eine direkte Verbindung besteht, ist dieses Patchkabel auszutauschen. Danach ist die Funktion zu überprüfen.
   b) Durch an Patchpunkten werden Abschnitte gebildet: Gerät - Trennpunkt und Trennpunkt - Fernkabel. Diese werden gemessen, wodurch der Fehlerabschnitt identifiziert werden kann. Dieses Vorgehen wird so lange wiederholt, bis auf dem fehlerhaften Bereich keine Patchmöglichkeit besteht. Dieser Teilabschnitt wird ausgewechselt und danach die Funktion überprüft.
3. Wenn Dämpfungsglieder eingesetzt werden, sind diese mit einem geeigneten Messgerät zu überprüfen.
4. Fernkabel
   a) Das Fernkabel wird nach dem gleichen Muster, wie die Anschlusskabel überprüft. Dabei wird auch das Fernkabel in Abschnitte unterteilt. Nach Identifikation eines Fehlers, wird dieser repariert.

Je nach Fehlerlage muss die lokale Verkabelung an beiden Standorten überprüft werden.

Zugehörige Maßnahmen

Hardwareprüfung vor Ort (M.INV.HVO) auf Seite 93

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung des Zustandes des Kommunikationsnetzes (M.INV.ÜT/NT-ÜN)

Ist eine WAN-Verbindung gestört ist die Art der Datenverbindung zu unterscheiden:

- Direkte Nutzung eigener Fasern ohne Abhängigkeit einer Transporttechnik
- Nutzung einer untergelagerten Transporttechnik (*DWDM*, *MPLS*, *DSL*, ...)

1. Die Technik ist auf eigene Fasern geschaltet und nicht von anderen Techniken beeinflusst. Daher muss auch nur die betroffene Technik überprüft werden.
2. Wenn Transporttechniken genutzt werden, müssen auch diese in die Fehlersuche mit eingebunden werden.

Zugehörige Maßnahmen

Überprüfung einer WAN-Störung beim Betrieb über eigene Fasern (M.INV.ÜT/NT-ÜWEF) auf Seite 96

Überprüfung einer WAN-Störung beim Betrieb über eine Transporttechnik (M.INV.ÜWST) auf Seite 96

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung einer WAN-Störung beim Betrieb über eigene Fasern (M.INV.ÜT/NT-ÜWEF)

Die Technik ist auf eigene Fasern geschaltet und nicht von anderen Techniken beeinflusst. Als Ursache für eine Fehlerbitrate oder Verbindungsabbrüche ist eine schlechte Signalqualität oder ein technischer Defekt zu überprüfen.

Überprüfung der Empfangs- und Sendepegel in der Geräteanzeige. Dies kann mit Hilfe des Managementsystems oder vor Ort direkt geschehen.

a) Ist der Empfangspegel zu gering, muss die Verbindung getrennt werden und der Wert mit geeigneten Messgeräten überprüft werden. Wenn dadurch ein unzureichender Pegel bestätigt wird, muss die Dämpfung der Verbindungsstrecke überprüft werden.
b) Ist der Empfangspegel in einem zulässigen und plausiblen Bereich, ist von einem Defekt des Empfangs- oder Sendemoduls auszugehen. Dazu wird beim fehlerbehafteten Gerät das Sende- / Empfangsmodul ausgetauscht. Sollte bei der anschließenden Funktionskontrolle weiterhin ein Fehler vorhanden sein, ist der Tausch an der Gegenstelle zu wiederholen.

Durch eine abschließende Funktionskontrolle wird ein fehlerfreier Betrieb überprüft.

Zugehörige Maßnahmen

Überprüfung der Datenverkabelung (M.INV.ÜT/NT-ÜDV) auf Seite 95

Überprüfung des Zustandes des Kommunikationsnetzes (M.INV.ÜT/NT-ÜN) auf Seite 96

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung einer WAN-Störung beim Betrieb über eine Transporttechnik (M.INV.ÜWST)

Die Technik nutzt eine Transporttechnik zur Datenübertragung. Fehler auf diesen Systemen haben Auswirkungen auf die transportierten Techniken. Als Ursache für eine Fehlerbitrate oder Verbindungsabbrüche ist eine schlechte Signalqualität oder ein technischer Defekt zu überprüfen.

1. Die Technik nutzt andere Übertragungstechnik (*DWDM*, *MPLS*, *DSL*, ...)
   a) Überprüfung der Empfangs- und Sendepegel und Fehlermeldungen aller beteiligten Techniken entsprechend einem Betrieb auf eigenen Fasern M.INV.ÜT/NT-ÜWEF (Seite 96)

2. Ist die Transportschicht fehlerfrei, wird die Verbindung zwischen Transport- und Clientschicht kontrolliert.
   a) Die Auslastung der WAN-Verbindung wird über eine Performanceanzeige der Technik oder einer Messung ermittelt und mit der Datenrate des Transportkanals abgeglichen. Bei einem Bandbreitenengpass auf dem Transportkanal ist Maßnahme M.INV.ÜT/NT-BEW (Seite 97) durchzuführen.
   b) Überprüfung der Datenverkabelung zwischen den Geräten.
   c) Bei korrekter Datenverkabelung folgt eine Messung der Clientverbindung über das Transportnetz mit geeigneten Messgeräten.
   d) Wird bei der durchgeführten Messung ein Fehler detektiert, erfolgt ein Austausch der Module, ggf. an beiden Standorten
   e) Ist auf der Transportstrecke kein Fehler erkennbar, wird am Clientsystem das entsprechende Kommunikationsmodul getauscht oder ein alternativer Anschlusspunkt genutzt.

Durch eine abschließende Funktionskontrolle wird ein fehlerfreier Betrieb überprüft.

Zugehörige Maßnahmen

Überprüfung einer WAN-Störung beim Betrieb über eigene Fasern (M.INV.ÜT/NT-ÜWEF) auf Seite 96

Überprüfung der Datenverkabelung (M.INV.ÜT/NT-ÜDV) auf Seite 95

Überprüfung des Zustandes des Kommunikationsnetzes (M.INV.ÜT/NT-ÜN) auf Seite 96

Bandbreitenengpass einer WAN-Verbindung (M.INV.ÜT/NT-BEW) auf Seite 97

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Bandbreitenengpass einer WAN-Verbindung (M.INV.ÜT/NT-BEW)

Die Performance einer WAN-Verbindung ist beeinträchtigt oder sogar gestört. Bei der Überprüfung wurde festgestellt, dass die Datenrate des Transportkanals nicht ausreicht. Die Ursache des erhöhten Datenaufkommens durch eine Analyse der Kommunikation ermittelt und kategorisiert werden.

- Zulässige bzw. plausible Verbindungen
- Unzulässige bzw. unplausible Verbindungen

1. Wird eine unzulässige oder unplausible Kommunikation ermittelt, sind unverzüglich weitere Maßnahmen einzuleiten.
   a) Meldung eines möglichen IT-Sicherheitsvorfalls an die zuständige Stelle (ISMS, Fachabteilung, Alarmplan)
   b) Meldung eines möglichen IT-Sicherheitsvorfalls an den Vorgesetzten
   c) Weiteres Vorgehen anhand der Vorgaben der Fachabteilung und / oder der zuständigen IT-Sicherheitsinstanz zur Erstsicherung (Trennen der Verbindung, Deaktivierung von Geräten, Sicherstellung, von Komponenten und Aufzeichnungen).
   d) Weitere Analyse des Vorfalls und des Netzwerkes entsprechend M...
2. Bei einem zulässigen Kommunikationsaufkommen, sind die Parameter und die Konfiguration der Verbindung zu prüfen.
   a) Überprüfung der konfigurierten Datenrate des Transportkanals
   b) Ermittlung der technisch möglichen Datenrate auf dem Transportmedium und der eingesetzten Technik.
   c) Ist eine Anpassung möglich, wird diese durchgeführt.
   d) Wenn keine Anpassung möglich ist oder diese weiterhin keine ausreichende Übertragungskapazität ermöglicht, sind Optimierungen der Konfiguration, der Qualitätsparameter oder eine Erweiterung / Austausch im Transportnetz notwendig. Dies ist mit einer entsprechenden Priorität an die zuständigen Stellen als Bedarf zu melden.

Fahren Sie mit der Bearbeitung nach den unten verlinkten Beobachtungen und Maßnahmen fort.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Überprüfung des Zustandes des Kommunikationsnetzes (M.INV.ÜT/NT-ÜN) auf Seite 96

Überprüfung einer WAN-Störung beim Betrieb über eine Transporttechnik (M.INV.ÜWST) auf Seite 96

IP-Adressen in einem Netzwerk werden untersucht (M.INV.ÜT/NT-IPC)

Es wurden Unregelmäßigkeiten im Übertragungsnetz festgestellt. Um auszuschließen, dass Fremdgeräte hierfür verantwortlich sind, sind die angeschlossenen Geräte in dem betreffenden Netzwerk oder Netzwerksegment zu untersuchen.

1. Das entsprechende Netzwerk oder Netzwerksegment ist zu identifizieren.
2. Es ist eine Liste mit allen erlaubten IP-Adressen dieses Netzwerk bzw. Netzwerksegments zu erstellen oder heranzuziehen.
3. Es ist ein Netzwerksniffer einzusetzen, der die IPs aller angeschlossener Geräte auslesen kann.
   Ein bekannter Netwzerksniffer für Windows ist beispielsweise Wireshark. Bei Linux-Systemen kann beispielsweise tcpdump verwendet werden.
4. Es muss überprüft werden, ob unbekannte IP-Adressen im Netzwerk genutzt werden.
   Falls hierbei unbekannte IP-Adressen gefunden wurden, ist davon auszugehen, dass ein Fremdgerät entdeckt wurde oder ein Gerät falsch parametriert wurde. Um dies weiter einzugrenzen, muss das entsprechende Gerät untersucht werden. Falls keine unbekannten IPs detektiert wurde, muss nun untersucht werden, ob die Systeme zu den IP-Adressen passen
5. Es sind weitere Tools zu nutzen, um weitere Informationen wie z.B. das Betriebssystem zu den IP-Adressen abzufragen.
   Z.B. kann ein versuchter telnet-login auf einer der IPs, als Antwort den Namen und das Betriebssystems des jeweiligen Geräts enthalten. Eine weitere Möglichkeit für die Beschaffung von Informationen über das Zielsystem ist snmp. Hierbei können oftmals die Befehle *snmpget* und/oder *snmpwalk* mit der community *public* genutzt werden. Die ausgefeilteste Möglichkeit weitere Informationen zu den angeschlossenen Systemen heraus zu finden, ist der Einsatz eines Fiungerprinting-Programms wie z.B. nmap bei Linux.

Zugehörige Beobachtungen

Es wird ein Fremdgerät im Übertragungsnetz entdeckt (B.ÜT/NT.FGE) auf Seite 28

Zugehörige Maßnahmen

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU) auf Seite 82
Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Fingerprinting eines Systems an Hand seiner IP-Adresse (M.INV.ÜT/NT-FPIP)

Es wurden Unregelmäßigkeiten im Übertragungsnetz festgestellt. Um auszuschließen, dass Fremdgeräte hierfür verantwortlich sind, sind die angeschlossenen Geräte in dem betreffenden Netzwerk oder Netzwerksegment zu untersuchen. Im Vorfeld wurde bereits ausgeschlossen, dass unbekannte IP-Adressen im Netzwerk verwendet werden.

1. Das entsprechende Netzwerk oder Netzwerksegment ist zu identifizieren.
2. Es ist eine Liste mit allen erlaubten IP-Adressen dieses Netzwerk bzw. Netzwerksegments zu erstellen oder heranzuziehen.
3. Es ist ein Netzwerksniffer einzusetzen, der die IPs aller angeschlossener Geräte auslesen kann.
   Ein bekannter Netwzerksniffer für Windows ist beispielsweise Wireshark. Bei Linux-Systemen kann beispielsweise tcpdump verwendet werden.
4. Es sind Tools zu nutzen, um einen Fingerprint von der verdächtigen IP anzulegen.
   Z.B. kann ein versuchter telnet-login auf einer der IPs, als Antwort den Namen und das Betriebssystems des jeweiligen Geräts enthalten. Eine weitere Möglichkeit für die Beschaffung von Informationen über das Zielsystem ist snmp. Hierbei können oftmals die Befehle *snmpget* und/oder *snmpwalk* mit der community *public* genutzt werden. Die ausgefeilteste Möglichkeit weitere Informationen zu den angeschlossenen Systemen heraus zu finden, ist der Einsatz eines Fingerprinting-Programms wie z.B. nmap bei Linux.
5. Der Fingerprint der untersuchten IP ist mit vorhanden Informationen abzugleichen.
   Beispielsweise sind die Daten eines snmpget-Befehls mit der Dokumentation anzugleichen. Daneben können weitere Informationen, wie z.B. das genutzte Betriebssystem und -Version, abgeglichen werden.

Für eine zu untersuchende IP ist ein Fingerprint angelegt worden und mit dokumentierten Informationen abgeglichen worden. Falls dabei Diskrepanzen festgestellt wurden, muss das angeschlossene Gerät weiter

untersucht werden. Falls es als wahrscheinlich gilt, dass es sich um ein Fremdgerät handelt, kann direkt mit der entsprechenden Beobachtung weitergearbeitet werden.

Zugehörige Beobachtungen

Es wird ein Fremdgerät im Übertragungsnetz entdeckt (B.ÜT/NT.FGE) auf Seite 28

Zugehörige Maßnahmen

Untersuchung fehlerbetroffener Fernwirkgeräte (M.INV.FWT-EGU) auf Seite 82
Ein einzelnes oder mehrere Fernwirkgerät(e) wird als Ursache für einen Vorfall identifiziert. Daher muss dieses Gerät nun untersucht werden.

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Reaktion

Reaktion auf Anomales Login Verhalten (M.REA.BE-AUB-LVU)

> Zuvor hat ein automatisiertes Sicherheitssystem anomales Nutzerverhalten detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt werden kann, sollten die Nutzer Accounts, deren Verhalten auffällig war vorsorglich gesperrt werden.
2. Zeitpunkt und betroffene Accounts sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
3. Die Nutzer, deren Verhalten auffällig war, sollten kontaktiert werden, um einen potentiellen Fehlalarm auszuschließen.
4. Falls sich herausstellt, dass ein Account kompromittiert wurde, darf dieser erst wieder freigegeben werden, nachdem etwaige daraus entstandene Schäden behoben worden sind und die Sicherheitslücken, die die Kompromittierung ermöglicht haben geschlossen wurden.
5. Danach kann der Account mit neuen Zugangsdaten (Neues Passwort) wieder freigegeben werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion auf anomale Account Löschungen (M.REA.CIT-AUB-ADU)

> Zuvor hat ein automatisiertes Sicherheitssystem anomales Nutzerverhalten detektiert.

1. Zuerst muss überprüft werden, ob es einen berechtigten Grund für das Verhalten gab, um einen Fehlalarm auszuschließen.
2. Falls sich herausstellt, dass die Kompromittierung eines Accounts dazu geführt hat, dass dieser andere Accounts gelöscht hat, muss dieser umgehend gesperrt werden.
3. Zeitpunkt und betroffene Accounts sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
4. Etwaige daraus entstandene Schäden sind zu beheben, und gegebenenfalls Sicherheitslücken, die die Kompromittierung ermöglicht haben, zu schließen.
5. Weiterhin ist das restliche System auf ähnliche Zugriffe zu überprüfen.
6. Danach kann der Account mit neuen Zugangsdaten (Neues Passwort) wieder freigegeben werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Aufbau eines Anonymous Channel überprüfen (M.REA.BE-AACU)

Zuvor hat ein automatisiertes Sicherheitssystem die Verwendung von TOR oder eines Proxy-Dienstes detektiert.

1. Zuerst sollte das betroffenen System isoliert werden, da die Nutzung von TOR oder Proxydiensten auf dem Backend von Energiesystemen unüblich sind und deshalb eine Kompromittierung angenommen werden sollte.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Anschließend sind betroffene Nutzer bzw. Verantwortliche zu kontaktieren, um einen Fehlalarm auszuschließen.
6. Sollten die Umstände eine Kompromittierung eines Systems wahrscheinlich machen, darf die Isolation erst wieder aufgehoben werden, nachdem alle Sicherheitslücken geschlossen und das System wieder in einen sicheren Zustand überführt wurde.
7. Zeitpunkt und betroffene Accounts sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
8. Falls möglich sollte der Traffic analysiert werden, um Hinweise zu seinem Inhalt oder Zweck zu bekommen.
9. Sollte dies nicht möglich sein, muss die Verbindung gesperrt werden.
10. Etwaige Schadsoftware auf dem System ist zu entfernen, und das System ist in einen sicheren Zustand zurückzusetzen, beispielsweise durch Einspielen eines Backups. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
11. Weiterhin ist das System auf Sicherheitslücken zu überprüfen, die eine Kompromittierung ermöglicht haben könnten, und diese sind zu beheben.
12. Danach kann die Isolation wieder aufgehoben werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion auf unerwartete Code Ausführungen (M.REA.BE-CASU)

Zuvor hat ein automatisiertes Sicherheitssystem unerwartete Prozesse detektiert.

1. Das System sollte umgehend vorsorglich von anderen Systemen isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, nachdem sichergestellt wurde, dass es sich bei der Meldung um einen Fehlalarm handelt oder das System keine Kompromittierung mehr aufweist, beispielsweise indem das System mit einem Backup wiederhergestellt wird. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Das betroffene System, sowie der Prozessname des Skripts sollten dokumentiert werden.
6. Es sollte überprüft werden, ob ein Nutzer für die Ausführung des Skripts verantwortlich ist.

7. Sollte ein Angreifer für die Meldung verantwortlich sein, sollte untersucht werden, durch welche Schwachstelle der Angreifer die Möglichkeit hatte ein Skript auszuführen. Alle Befunde sollten behoben und dokumentiert werden. Ebenfalls sollten angrenzende Systeme auf ähnliche Schwachstellen untersucht werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion auf Konfigurationsänderungen (M.REA.BE-KMU)

> Zuvor hat ein automatisiertes Sicherheitssystem unerwartete Konfigurationsänderungen detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt wurde, muss ein Angriff als wahrscheinliche Ursache angenommen werden, daher muss das System umgehend von anderen Systemen isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, sobald sichergestellt wurde, dass es sich um einen Fehlalarm handelt oder das System mit einem Backup wiederhergestellt wurde. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Das betroffene System sollte dokumentiert werden.
6. Es sollte überprüft werden, ob ein berechtigter Nutzer für die Änderungen verantwortlich war, um einen Fehlalarm auszuschließen.
7. Falls kein Fehlalarm festgestellt werden kann, muss untersucht werden, welche Änderungen vorgenommen wurden, damit diese rückgängig gemacht werden können.
8. Es sollte untersucht werden durch welche Schwachstelle der Angreifer die Möglichkeit hatte Änderungen vorzunehmen. Alle Befunde sollten behoben und dokumentiert werden. Ebenfalls sollten angrenzende Systeme auf ähnliche Schwachstellen untersucht werden.

Gemäß M.DOK.MBP (Seite 127) ist zu prüfen, ob der Vorfall weitergehende Meldung erfordert. Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Zugehörige Beobachtungen

Configuration Modification (B.BE.CoMo) auf Seite 48

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Datendiebstahl unterbinden und Ursprung analysieren (M.REA.BE-DUUA)

> Zuvor hat ein automatisiertes Sicherheitssystem eine Datenexfiltrierung detektiert.

1. Sofern die Meldung nicht sofort als Fehlalarm erkannt werden kann, ist die Verbindung umgehend zu sperren, um weitere Datenverluste zu vermeiden.
2. Weiterhin muss das System isoliert werden, da es offensichtlich kompromittiert wurde.
3. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.

4. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
5. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
6. Eine Analyse der gestohlenen Daten kann Aufschluss über das genaue Ziel des Angriffs geben. Weiterhin muss untersucht werden, durch welche Sicherheitslücken das System kompromittiert wurde, um die Datenexfiltration zu ermöglichen. Die gefundenen Sicherheitslücken sollten dokumentiert werden.
7. Sobald das System in einen sicheren Zustand zurückgesetzt wurde, beispielsweise durch Einspielen eines Backups, kann die Isolation wieder aufgehoben werden. Zusätzlich sollten alle dokumentierten Sicherheitslücken beseitigt werden. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
8. Darüber hinaus sind relevante Personen über den Datendiebstahl in Kenntnis zu setzen, um darauf reagieren zu können.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

System auf Malware File Detection untersuchen und System auf Schwachstellen analysieren (M.REA.BE-MFDU)

> Zuvor hat ein automatisiertes Sicherheitssystem Schadsoftware detektiert.

1. Sofern die Meldung nicht direkt als Fehlalarm erkannt werden kann, ist das System umgehend zu isolieren. Die Isolierung des Systems kann erst wieder aufgehoben werden, sobald das System sicher nicht mehr kompromittiert ist, beispielsweise wenn ein Backup wiederhergestellt wurde, oder falls sich die detektierte Software im späteren Verlauf als harmlos herausstellt.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Nachdem das System jetzt isoliert ist, sollte die gemeldete Software genauer überprüft werden, um Fehlalarme auszuschließen.
6. Sofern es sich tatsächlich um Malware handelt, ist eine genauere Analyse hilfreich, um Informationen über das Angriffsziel sowie über verwendete Schwachstellen zu erlangen.
7. Hiernach ist die Malware und ihre Auswirkungen rückstandsfrei zu entfernen, je nach System kann auch ein Backup wiederhergestellt werden. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
8. Weiterhin sind etwaige Sicherheitslücken oder Schwachstellen zu beheben oder unzugänglich zu machen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Manipulation von Netzwerk Einstellungen überprüfen (M.REA.BE-MNEU)

> Zuvor hat ein automatisiertes Sicherheitssystem Änderungen an den Routing-Einstellungen detektiert.

1. Zuerst ist das betroffene System zu isolieren, sofern kein Fehlalarm erkannt werden kann. Die Isolierung des Systems kann erst wieder aufgehoben werden, wenn sichergestellt ist, dass das System keine

Kompromittierung mehr aufweist, beispielsweise indem ein Backup wiederhergestellt wird, oder falls ein valider Grund für die Änderungen gefunden werden konnte.

2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Es sollte überprüft werden, ob ein berechtigter Administrator die Änderungen vorgenommen hat, um eine Kompromittierung auszuschließen.
6. Sollte dies nicht der Fall sein, sollte das System auf Schwachstellen analysiert werden.
7. Nun sollte das System mit einem Backup wiederhergestellt werden. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
8. Anschließend sind alle Sicherheitslücken und Schwachstellen zu beheben oder unzugänglich zu machen

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Unautorisierte Rechte Gewinnung rückgängig machen (M.REA.BE-URG)

> Zuvor hat ein automatisiertes Sicherheitssystem, dass ein Nutzer versucht, zusätzliche Berechtigungen zu erlangen.

1. Alle betroffenen Accounts sind umgehend zu sperren, um weitere unerlaubte Zugriffe zu verhindern.
2. Betroffene Nutzer sind schnellstmöglich zu informieren, und es muss überprüft werden, ob ein valider Grund für den Versuch, zusätzliche Rechte zu erlangen, vorliegt, um einen Fehlalarm auszuschließen.
3. Wenn sichergestellt wurde, dass es sich um einen Fehlalarm handelt, ist es hinreichend, die Accounts wieder zu entsperren, andernfalls muss der Vorfall weiter untersucht werden.
4. Nachdem sichergestellt ist, dass die Accounts nicht weiter missbraucht werden können, muss überprüft werden, welche weiteren Aktivitäten von den betroffenen Accounts ausgingen, und welche Schäden verursacht werden konnten. Wichtig ist außerdem, herauszufinden, welche Sicherheitslücke oder Schwachstelle den Zugriff auf die Accounts ermöglicht hat, von denen der Versuch ausging. Diese ist umgehend zu beheben oder unzugänglich zu machen.
5. Alle Operationen, die während der Privilege Escalation entstanden sind und alle betroffene Systeme sind zu dokumentieren, zu überprüfen und gegebenenfalls rückgängig zu machen, zum Beispiel durch Wiederherstellung eines Backups. Weiterhin sind die Privilegien der Accounts (falls erfolgreich Änderungen durchgeführt wurden) wieder auf die Ursprünglichen zu begrenzen.
6. Sobald alle Schäden, die direkt die Accounts betreffen, behoben sind, können die Accounts (nach Änderung der Zugangsdaten) wieder für die Nutzer geöffnet werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Ausspähen von SSH-Nutzernamen unterbinden (M.REA.BE-ASSHNU)

> Zuvor hat ein automatisiertes Sicherheitssystem detektiert, dass SSH-Nutzernamen ausgespäht wurden.

1. Zuerst ist (sofern noch nicht automatisiert geschehen) die IP-Adresse des Angreifers zu blockieren.

2. Accounts, deren Nutzername erfolgreich herausgefunden werden konnte, sollten auf Folgeangriffe überprüft werden.
3. Falls möglich kann die Firewall modifiziert werden, sodass der betroffene SSH-Zugang nur noch aus dem internen Netz möglich ist. Allgemein sollten alles Systeme, die keine externen Zugriffe benötigen, nur aus dem internen Netz erreichbar sein.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful System Persistence (M.REA.BE-VSSP)

> Zuvor hat ein automatisiertes Sicherheitssystem eine erfolgreiche System Persistence detektiert.

1. Das System muss bei dieser Meldung umgehend isoliert werden. Die Isolierung darf erst wieder aufgelöst werden, wenn die Schadsoftware und alle Auswirkungen dieser sicher beseitigt wurden, beispielsweise durch Wiederherstellung eines Backups von vor der Infektion. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Anschließend ist das betroffene System sowie alle weiteren Informationen des automatisierten Sicherheitssystems zu dokumentieren.
6. Folglich besteht der nächste Schritt darin, die Schadsoftware auf Funktion und Auswirkungen zu untersuchen, um Einblicke in das Ziel des Angriffs zu bekommen.
7. Das System sollte weiterhin auf Schwachstellen überprüft werden, die sowohl das erstmalige Eindringen als auch die Persistenz der Software ermöglicht haben.
8. Nach erfolgter Analyse ist die Schadsoftware vollständig zu entfernen und das System in einen sicheren Zustand zurückzusetzen.
9. Alle gefundenen Sicherheitslücken oder Schwachstellen müssen behoben oder zumindest unzugänglich gemacht werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Ursprung von Wiederkehrender Schadsoftware unterbinden (M.REA.BE-WSU)

> Zuvor hat ein automatisiertes Sicherheitssystem einen Versuch, System Persistence zu erlangen, detektiert.

1. Das System muss bei dieser Meldung umgehend isoliert werden. Die Isolierung darf erst wieder aufgehoben werden, wenn sichergestellt ist, dass das System wieder in einem unkompromittierten Zustand ist, beispielsweise durch Wiederherstellung eines Backups von vor der möglichen Infektion. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.

3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Anschließend ist das betroffene System, sowie alle weiteren Informationen des automatisierten Sicherheitssystems zu dokumentieren.
6. Um eine Fehlmeldung auszuschließen sind alle relevanten Dienste und Skripte, die bei einem Systemstart ausgeführt werden, wie cronjobs, bashrc etc. auf unerwartete Einträge zu überprüfen.
7. Wenn verdächtige Einträge gefunden wurden, sollte das System auf Schwachstellen überprüft werden, die sowohl das erstmalige Eindringen als auch die Persistenz der Schadsoftware ermöglicht haben.
8. Nach erfolgter Analyse ist das System in einen sicheren Zustand zurückzusetzen. Anschließend müssen alle gefundenen Sicherheitslücken oder Schwachstellen behoben oder zumindest unzugänglich gemacht werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Login mit Default Credentials unterbinden (M.REA.FWT-LDCU)

Zuvor hat ein automatisiertes Sicherheitssystem einen Loginversuch mit Default-Zugangsdaten gemeldet.

1. Falls der Loginversuch erfolgreich war, ist das System umgehend zu isolieren und auf Veränderungen zu untersuchen, sowie in einen sicheren Zustand zurückversetzt werden.
2. Die Default-Zugangsdaten müssen deaktiviert und durch sichere ersetzt werden.
3. Sicherheitshalber sollten alle Systeme, bei denen dies vorkommen könnte, darauf überprüft werden, dass auch dort die Default-Logindaten deaktiviert sind.
4. Falls der Loginversuch nicht erfolgreich war, weist er trotzdem auf einen laufenden Angriff hin. Relevante Personen wie z.B. Administratoren sollten darüber informiert werden, dass mit vermehrten Angriffen zu rechnen ist. Ebenfalls sollten alle erkannten Angriffe untersucht werden, damit die Herkunft des Angriffs festgestellt werden kann, um gegebenfalls die IP-Adresse des Angreifers zu sperren.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reparatur eines defekten Fernwirkgeräts (M.REA.FWT-RDG)

Ein einzelnes Fernwirkgerät meldet sich mit Fehlermeldung.

Es wird festgestellt, dass ein einzelnes Fernwirkgerät defekt ist.

1. Man schaut konkret in die Bedienoberfläche der Parametriersoftware setIT an, was für eine Fehlerdiagnose es hinweist.
2. Je nach Fehlerart wird das Fernwirkgerät vor Ort direkt repariert.

Das Fernwirkgerät wird erfolgreich repariert

Verdächtige Firmware (M.REA.FWT-VFU)

Ein System hat eine unerwartete Firmware-Version, oder die Firmware hat keine valide Prüfsumme.

1. Sofern diese Meldung nicht sofort als Fehlalarm erkannt wurde, ist das betroffene System umgehend zu isolieren.

2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Es sollte beim Administrator oder Hersteller des Systems geklärt werden, ob es sich um eine valide Firmware handelt.
6. Sollte dies nicht der Fall sein, ist die Firmware zu untersuchen. Eventuell können hierbei Spuren des Angreifers gefunden werden, insbesondere solche, die auf ausgenutzte Sicherheitslücken hinweisen. Um Sicherheitslücken in der Firmware zu finden, kann hierzu ein Vulnerability-Scanner herangezogen werden.
7. Nach abgeschlossener Spurensuche ist das System mit einer validen Firmware zu bespielen, und erkannte Sicherheitslücken zu beheben oder mindestens unzugänglich zu machen. Dies gilt auch für weitere Geräte, die die gleiche Software verwenden.
8. Sobald alle Auswirkungen beseitigt sind, kann das System wieder ins Netzwerk aufgenommen werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Einbau eines Fernwirkgeräts (M.REA.FWT-GEB)

Ein einzelnes Fernwirkgerät soll installiert werden.

es handelt sich um eine Neuinstallation

1. Entnehmen Sie das Gerät aus der Packung. Es wird mit den Lieferanten vereinbart, dass alle Geräte von den Außenpackungen immer mit Siegelband abgesichert.
2. Untersuchen Sie, ob das Fernwirkgerät intakt erscheint.
   Falls das Gerät unbeschädigt wirkt, fahren Sie mit der Installation fort. Falls das Gerät Beschädigungen aufweist, kontaktieren Sie Ihren Vorgesetzten.
3. Bringen Sie das Gerät an die gewünschte Position.
4. Ziehen Sie die Halteschrauben an, bzw. lassen Sie die Halteklammer einrasten.
5. Schließen sie die Anschlusskabel, wie z.B. Netzwerkkabel an.
6. Als letztes schließen Sie das Stromkabel an.
7. Schalten Sie das Gerät ein.

Das Fernwirkgerät wird erfolgreich eingebaut.

Fahren Sie mit dem Test und der Konfiguration des Geräts fort.

Zugehörige Maßnahmen

Test eines Fernwirkgeräts (M.INV.FWT-EGT) auf Seite 83
Ein einzelnes Fernwirkgerät soll nach der Konfiguration getestet werden.

Konfiguration eines Fernwirkgeräts (M.REA.FWT-KFW) auf Seite 106
Ein einzelnes Fernwirkgerät soll nach dem Einbau konfiguriert werden.

Konfiguration eines Fernwirkgeräts (M.REA.FWT-KFW)

Ein einzelnes Fernwirkgerät soll nach dem Einbau konfiguriert werden.

> Die Fernwirkanlage wird je nach Umfang der Anlagenkomponenten konfiguriert.

1. Anzahl Transformatoren, Schaltfelder verifizieren
2. Im Detail haben der Typ der Schaltfelder und die Auslegung der Einfluss auf die Konfiguration. Hierbei geht es um Einfach oder Duplexfelder, Spannung der Netzebene, Ströme.
3. Für die Anbindung der Geräte in der Anlage zur Übertragung zum Netzleitsystem sind Protokolle auszuwählen und zu konfigurieren.

Das Fernwirkgerät wird erfolgreich konfiguriert.

Fahren Sie mit dem Test des Geräts fort.

Zugehörige Maßnahmen

Einbau eines Fernwirkgeräts (M.REA.FWT-GEB) auf Seite 106
Ein einzelnes Fernwirkgerät soll installiert werden.

Test eines Fernwirkgeräts (M.INV.FWT-EGT) auf Seite 83
Ein einzelnes Fernwirkgerät soll nach der Konfiguration getestet werden.

Einbau eines Fernwirkgeräts (M.REA.FWT-EGE)

Ein einzelnes Fernwirkgerät soll installiert werden.

Zuvor wurde ein defektes Gerät ausgebaut oder es handelt sich um eine Neuinstallation

1. Entnehmen Sie das Gerät aus der Packung.
2. Untersuchen Sie, ob das Fernwirkgerät inatkt erscheint.
   Falls das Gerät unbeschädigt wirkt, fahren Sie mit der Installation fort. Falls das Gerät Beschädigungen aufweist, kontaktieren Sie Ihren Vorgesetzten.
3. Bringen Sie das Gerät an die gewünschte Postion.
4. Ziehen Sie die Halteschrauben an, bzw. lassen Sie die Halteklammer einrasten.
5. Schließen sie die Anschlusskabel, wie z.b. Netzwerkkabel an.
6. Als letztes schließen Sie das Stromkabel an.
7. Schalten Sie das Gerät ein.

Das Fernwirkgerät wurde erfolgreich eingebaut.

Fahren Sie mit dem Test und der Konfiguration des Geräts fort.

Zugehörige Maßnahmen

Einbau eines Fernwirkgeräts (M.REA.FWT-GEB) auf Seite 106
Ein einzelnes Fernwirkgerät soll installiert werden.

Firmware Version überprüfen (M.REA.FWT-FWU)

> Ein System hat eine unerwartete Firmware-Version, oder die Firmware hat keine valide Prüfsumme.

1. Sofern diese Meldung nicht sofort als Fehlalarm erkannt wurde, ist das betroffene System umgehend zu isolieren.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Nachdem das System nun isoliert ist, muss beim Administrator oder Hersteller des Systems geklärt werden, ob es sich um eine valide Firmware handelt.
6. Sollte dies nicht der Fall sein, ist die Firmware zu untersuchen. Eventuell können hierbei Spuren des Angreifers gefunden werden, insbesondere solche, die auf ausgenutzte Sicherheitslücken hinweisen.
7. Nach abgeschlossener Spurensuche ist das System mit einer validen Firmware zu bespielen, und erkannte Sicherheitslücken zu beheben oder mindestens unzugänglich zu machen. Dies gilt auch für weitere Geräte ähnlicher Bauart.
8. Sobald alle Auswirkungen somit beseitigt sind, kann das System wieder ins Netzwerk aufgenommen werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.REA.LS-ALSE)

Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Zuvor wurde festgestellt, dass ein Ersatzstandort des Leitsystems nicht mehr verfügbar ist.

Wiederherstellung der Redundanz der Leitsystemkomponenten

a) Wiederinbetriebnahme / Neustart der Leitrechner
b) Wiederinbetriebnahme / Neustart der Datenbankrechner und Prozessanschlussrechner
c) Wiederherstellung der Notarbeitsplätze

Die Redundanz der Leitsystemkomponenten konnte erfolgreich wiederhergestellt werden.

Wiederherstellung des Dateiaustausch-Systems. Bis dahin erfolgen Ex-und Import Funktionalitäten manuell.

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL) auf Seite 125
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Maßnahmen bei Ausfall eines Leitsystem-Hauptstandorts (M.REA.LS-ALSH)

Maßnahmen die bei Ausfall eines Hauptstandorts des Leitsystems getroffen werden müssen.

Zuvor wurde festgestellt, dass ein Hauptstandort des Leitsystems nicht mehr verfügbar ist.

1. Die Schaltmeister besetzen die Notfallarbeitsplätze am Ersatzstandort.
   a) Hierzu sind mindestens 2xMS, 1xHS, 1x Dispatching Arbeitsplätze benötigt.
   b) Nach spätestens zwei Stunden sind diese 5 Arbeitsplätze mit eingeschränkter Telefonie betriebsbereit.
   c) Das An-/Abmeldesystem ist durch manuelle Erfassung der Kollegen in den Stationen zu ersetzen.
   d) Der Ausfall des Betriebsfunks ist durch die Telefonie der Notfallarbeitsplätze und die Mobiltelefone der Außenmitarbeiter zu ersetzen.
2. Anschließend erfolgt die Wiederherstellung eines eingeschränkten und zeitlich nicht beschränkten Netzführungsbetriebes.
   a) Besetzung von insgesamt 9 Arbeitsplätzen 4xMS, 2xHS, 2x Dispatching, 1xDAB
   b) Ausstattung aller Leitsystemarbeitsplätze mit Telefon
   c) Verbindung zum Prozessdatenarchiv (PDA) herstellen
   d) Verbindung zum Datenmodellserver (DMS) herstellen

   Alle weiteren ausgefallenen Systeme beeinträchtigen nicht direkt die Aufgaben der Netzbetriebsführung, werden jedoch für den regulären Betrieb des Netzes (Neubau, Umbau, Störungssuche, Wartungsarbeiten, etc.) erforderlich.

Ein eingeschränkter aber zeitlich nicht beschränkter Netzführungsbetrieb am Ersatzstandort wurde wiederhergestellt.

Wiederherstellung des Dateiaustausch-Systems. Bis dahin erfolgen Ex-und Import Funktionalitäten manuell.

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL) auf Seite 125
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Maßnahmen bei Ausfall eines Leitsystem-Kommunikationsstandorts (M.REA.LS-ALSK)

Maßnahmen die bei Ausfall eines Kommunikationsstandorts des Leitsystems getroffen werden müssen.

Zuvor wurde festgestellt, dass ein Kommunikationsstandort des Leitsystems nicht mehr verfügbar ist.

1. Bei einem längeren Ausfall dieses Kommunikationsstandorts ist der Neuaufbau eines GPRS/DSL-Knotens am Hauptstandort zu erwägen.

2. Die Geräte des Einspeisemanagements werden in der Zeit des Ausfalls direkt über GSM vom Hauptstandort aus angerufen.
   a) Starten sie die zugehörige Konfigurationssoftware der betroffenen Geräte die pro Gerät etwa zwei Minuten in Anspruch nimmt
   b) Ändern Sie die Konfiguration der betroffenen Geräte von der IP zu GSM Kommunikation

      Dies benötigt ca. 2 Minuten pro Gerät.
3. Die Fernwirkanlagen können erst nach einem Wiederaufbau des GPRS/DSL-Knotens wieder erreicht werden.
4. Der interne Bereitschaftsdienst ist eingeschränkt (fehlende Wartungszugänge).
   a) Wiederherstellung des Fernwartungszugang innerhalb einer Woche.
   b) Solange der Wartungszugang nicht verfügbar ist, erfolgt der Betrieb ersatzweise von jedem beliebigen Büronetz-Standort aus
5. Externe Wartungszugänge sind während der Störung nicht möglich.
   a) Einrichten von alternativen Kommunikationswegen für die Fernwartung, wie z.B Telefon/ Bildschirmfreigabe über Internet (z.B. MS-Teams oder Skype).

Ein zeitlich nicht eingeschränkter Notbetrieb wurde erfolgreich wiederhergestellt.

Der Kommunikationsstandort sollte zeitnah wieder in Betrieb genommen werden und falls dies nicht möglich ist, muss wie oben beschrieben ein neuer GPRS/DSL-Knoten aufzubauen.

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL) auf Seite 125
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Maßnahmen bei Komplettausfall des Leitsystems (M.REA.LS-KALS)

Maßnahmen die bei einem Ausfall aller Standorte des Leitsystems getroffen werden müssen.

Zuvor wurde festgestellt, dass sämtliche Standorte des Leitsystems nicht mehr verfügbar sind.

1. Besetzung wichtiger Anlagen mit geeignetem Personal vor Ort. Hierzu zählen:
   a) Umspannwerke
   b) Gasübergabestationen mit Versorgungsaufgaben
   c) netzrelevante Gas-Stationen
   d) Erdgasspeicher
2. Einspeiser werden für den Zeitraum des Notfalls dauerhaft abgeregelt, wenn mit erhöhter EEG-Einspeisung zu rechnen ist. Im Zweifelsfall wird abgeregelt.
3. Weitere Schritte Priorität 1:
   a) Remoteaufschaltung der Nahsteuerplätze in den Umspannwerken per VNC über einen separaten Server (SPLIT-Rechner oder neu aufzusetzenden Server)
   b) Wiederherstellen eines ersten Leitsystemarbeitsplatzes
   c) Herstellen eines isolierten Netzwerkes
   d) Einbinden Prozesskoppler und IEC 104 Unterstationen in isoliertes Netzwerk

   Ein eingeschränkter Schaltbetrieb ist mit Inbetriebnahme des ersten Leitsystemarbeitsplatzes möglich (keine Störungserfassung/-bearbeitung, kein Netzsicherheitsmanagement, keine Abschaltplanung, kein Datenmodelländerungsdienst).
4. Weitere Schritte Priorität 2:
   a) Wieder-/ Neuinbetriebnahme Leitrechner
   b) Wieder-/ Neuinbetriebnahme Prozesskoppelsysteme (PKS und TCG)
   c) Wieder-/ Neuinbetriebnahme TASE.2 Rechner
   d) Wieder-/ Neuinbetriebnahme weiterer Leitsystemarbeitsplätze 3xMS 1xHS 1xDispatching

   Mit Abschluss dieser Maßnahmen ist ein regulärer Schaltbetrieb wieder möglich.
5. Weitere Schritte Priorität 3:
   a) Schrittweiser Wiederaufbau restlicher Funktionen (z.B. zusätzliche Leitsystemarbeitsplätze für Abschaltplanung, DME, Prüfung, etc.)

Mit Abschluss dieser Maßnahmen ist ein eingeschränkter aber zeitlich nicht befristeter Notbetrieb wieder möglich.

Wiederinbetriebnahme der übrigen Standorte und Systeme.

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL) auf Seite 125
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Maßnahmen bei Ausfall der Prozessdatennetze (M.REA.LS-APDN)

Notfallmaßnahmen die bei Ausfall der Prozessdatennetze zur Anbindung des Leitsystems getroffen werden müssen.

Zuvor wurde festgestellt, dass die Prozessdatennetze zur Anbindung des Leitsystems nicht mehr verfügbar sind.

1. Besetzung wichtiger Anlagen mit geeignetem Personal vor Ort. Hierzu zählen:
   a) Umspannwerke mit Versorgungsaufgaben
   b) Netzkuppler
2. Einspeiser werden für den Zeitraum des Notfalls dauerhaft abgeregelt, wenn mit erhöhter EEG-Einspeisung zu rechnen ist. Im Zweifelsfall wird abgeregelt.
3. Weitere Schritte Priorität 1 bei Routing- oder ähnlichen Protokollfehlern: :
   a) Behebung des Netzwerkfehlers.

   Nach Behebung des Fehlers ist der reguläre Betrieb wieder erreicht.
4. Weitere Schritte Priorität 1 bei Provider-Fehlern:
   a) Beauftragung des Dienstleisters mit Störungsbehebung gemäß SLA

   Nach Behebung des Fehlers ist der reguläre Betrieb wieder erreicht.
5. Weitere Schritte Priorität 1 bei anderen Fehlern:
   a) Remoteaufschaltung der Nahsteuerplätze in den Umspannwerken per VNC über einen separaten Server (SPLIT-Rechner oder neu aufzusetzenden Server), wenn möglich
   b) Abtrennen des beschädigten Netzes, Wiederaufbau erfolgt ausgehend vom Hauptstandort
   c) Herstellung Backbone an zentralen Prozesskoppel-Standorten
6. Weitere Schritte Priorität 2:
   a) Herstellung vollständiges Backbone Netz

   Nach Abschluss der Priorität 2 Maßnahmen ist ein Schaltbetrieb wieder möglich.
7. Weitere Schritte Priorität 3:
   a) Schrittweiser Wiederaufbau der restlichen Funktionen.

Nach Abschluss der Priorität 3 Maßnahmen sollten die Prozessdatennetze wiederhergestellt sein.

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL) auf Seite 125
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Maßnahmen bei Ausfall der Leitstellen-Telefonanlage (M.REA.LS-ALSTA)

Maßnahmen die beim Ausfall der Leitstellen-Telefonanlage getroffen werden müssen.

Zuvor wurde festgestellt, dass die Leitstellen-Telefonanlage nicht mehr verfügbar ist. Am Hauptstandort des Leitsystems stehen unabhängig von der Leitstellen-Telefonanlage Satellitentelefone, Betriebsfunkgeräte und ein Amtstelefon zur Verfügung. Das Personal in den Stationen/Fläche ist weiterhin über Betriebsfunk normal erreichbar.

Schritte Priorität 1:

a) Beauftragung des Dienstleisters mit Störungsbehebung gemäß SLA

Mit Abschluss dieser Maßnahmen sollte die Leitstellen-Telefonanlage wieder normal verfügbar sein.

Gegebenenfalls Fehlersuche und Analyse, um zukünftigen Ausfällen vorzubeugen. Ebenfalls muss bei meldepflichtigen Vorfällen der Abschlussbericht für die Behörden erstellt werden.

Zugehörige Maßnahmen

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL) auf Seite 125
Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Neustart PC oder Notebook (M.REA.CIT-NSPC)

Überprüfung

> Es wurde vorher ein Problem mit diesem Gerät festgestellt.

Um Auszuschließen, dass es sich um ein temporäres softwarebedingtes Problem handelt ist ein Neustart auszuführen.
Um einen Neustart durchzuführen, führen Sie die für dieses System notwendigen Schritte aus.
Bei Windows-Rechner drücken Sie beispielsweise auf das Windows-Logo in der Taskleiste und anschließend auf das Ein-Aus-Symbol und wählen im Kontextmenü den Eintrag "Neu starten" aus.
Falls der Rechner nicht reagieren sollte, können Sie meist durch längeres Drücken des Anschaltknopfs ein "hartes" Herunterfahren erzwingen. Hierbei können nicht gespeicherte Daten verloren gehen.

Der Rechner wurde neu gestartet. Falls das Problem weiterhin besteht muss dieses zur weiteren Bearbeitung an den zuständigen Administrator oder Service-Desk gemeldet werden.

Zugehörige Maßnahmen

First-Level-Support kontaktieren (M.KOM.FLS) auf Seite 73
Für die weitere Bearbeitung eines IT-Problems, ist der Support hinzuzuziehen

Virenscan eines Systems (M.REA.CIT-VS)

Überprüfung

> Es wurde vorher ein Problem mit diesem Gerät/ System festgestellt.

Um Auszuschließen, dass es sich Schadsoftware auf dem System befindet ist ein Virenscan durchzuführen.
Suchen Sie die auf dem Gerät installierte Antivirensoftware und starten eine manuelle Prüfung.

Eine Antivirenprüfung wurde durchgeführt.

Falls Schadsoftware gefunden wurde, fahren Sie bitte mit den untenstehenden Maßnahmen fort.

Zugehörige Beobachtungen

Malware Infection (B.AS.MIn) auf Seite 61

Zugehörige Maßnahmen

First-Level-Support kontaktieren (M.KOM.FLS) auf Seite 73
Für die weitere Bearbeitung eines IT-Problems, ist der Support hinzuzuziehen

Zugangsdaten ändern (M.REA.ZDA)

> Es wurde festgestellt, dass Zugangsdaten eines oder mehrerer Nutzer gestohlen oder anderweitig kompromittiert wurden. Die Ursache wurde identifiziert und behoben.

1. Die Zugangsdaten werden durch die Vergabe eines neuen Passworts, das Erstellen eines neuen Zertifikats oder die Vergabe einer neuen Hardwareauthentifizierungsmethode ersetzt.

   Die Nutzung einer Passwortrichtlinie und die Verwendung von Zweifaktorauthentifizierung erhöht die Sicherheit und die Resilienz gegen Folgeangriffe.

2. Alle aktiven Logins des Nutzers, gespeicherte Passwörter, aktive Sitzungen und ggf. installierte Zertifikatsauthentifizierungen werden gelöscht.
3. Dokumentieren Sie die das Vorgehen (M.DOK.SDOK (Seite 127)) und informieren Sie die betroffenen Nutzer.

Es ist darauf zu achten, dass keine unberechtigten Personen Zugriff oder Einsicht in vertrauliche Informationen erhalten. (M.REA.ORG-SV)

Überprüfung

> Zuvor wurde bemerkt, dass vertrauliche Informationen frei zugänglich sind. Dies kann z.B. durch das offene Liegenlassen auf dem Schreibtisch oder das nicht-Sperren des Bildschirms eintreten.

1. Lassen Sie keine vertraulichen Informationen offen herumliegen, wenn Sie nicht mehr damit arbeiten, damit keine Unbefugten Zugriff oder Einsicht erhalten.
2. Sperren Sie immer Ihren Bildschirm, wenn Sie nicht am Arbeitsplatz sind.
3. Achten Sie darauf, dass vertrauliche Informationen nur durch berechtigte Personen eingesehen werden dürfen. Dies gilt insbesondere für Gäste und Dienstleister.
4. Falls eine Person unbefugter Einsicht in vertrauliche Informationen erhalten hat, weisen Sie sie daraufhin, dass diese nicht weitergeben werden dürfen.

Je nach Sensibilität der Informationen sind ggfs. weitere Schritte einzuleiten, wie z.B. das Ändern von Zugangsdaten.

Zugehörige Beobachtungen

Klassifikationsstufen (B.ORG.KS) auf Seite 55
Klassifikationsstufen für die Einstufung der Vertraulichkeit von Unterlagen.

Zugehörige Maßnahmen

Accounts mit gestohlenen Zugangsdaten sperren (M.REA.SFM-AZS) auf Seite 124

Vorgehen bei detektierten Hacking-Tools (M.REA.AS-HTSU)

> Zuvor hat ein automatisiertes Sicherheitssystem ein bekanntes Hacking-Tool detektiert.

1. Das genaue Verhalten hängt von der Art des Hacking-Tools ab. Insbesondere ist festzustellen, ob das Hacking-Tool auf dem System selbst ausgeführt wird, oder ob es von außen angreift.
2. Sofern es auf dem System selbst ausgeführt wird, ist das System umgehend zu isolieren, auf Schwachstellen zu untersuchen, die das Eindringen des Hacking-Tools ermöglicht haben, und in einen sicheren Zustand zurückzusetzen. Weiterhin sind etwaige Sicherheitslücken zu schließen.
3. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
4. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
5. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
6. Je nach Art und Funktionsumfang des Hacking-Tools muss dasselbe für angrenzende Systeme wiederholt werden.
7. Sollte das Hacking-Tool von außen angreifen, sollte die Verbindung gesperrt werden und überprüft werden durch welche Sicherheitslücke eine Verbindung zustande kam. Alle gefundenen Sicherheitslücken sind zu schließen.
8. Sicherheitshalber sollte ein interner Test mit demselben Tool gemacht werden, um sicherzustellen, dass es nicht erfolgreich war.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Angriffsversuche auf bekannte Schwachstellen unterbinden (M.REA.AS-ABSU)

Zuvor hat ein automatisiertes Sicherheitssystem die versuchte Ausnutzung einer bekannten Schwachstelle detektiert.

1. Da der Angreifer bisher noch nicht erfolgreich war, ist seine Verbindung umgehend zu sperren.
2. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. Weiterhin sollte durch einen internen Penetration Test überprüft werden, ob sein Angriff Erfolg hätte haben können. Gefundene Sicherheitslücken sind gegebenenfalls zu schließen.
5. Relevante Personen wie zum Beispiel Administratoren sollten informiert werden, dass eventuell weitere Angriffe zu erwarten sind.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Code Injection und Schwachstellen untersuchen (M.REA.AS-CISU)

Zuvor hat ein automatisiertes Sicherheitssystem eine Code-Injection oder -Execution detektiert.

1. Das betroffene System ist zunächst umgehend zu isolieren. Die Isolierung kann erst wieder aufgehoben werden, nachdem sichergestellt wurde, dass das System keine Kompromittierung aufweist, beispielsweise indem ein Backup wiederhergestellt wird. Handelt es sich bei dem betroffenen System um eine KRITIS, dann sollte eine Neuinstallation des Systems oder das Verwenden eines Ersatz Systems in Betracht gezogen werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Es sollte überprüft werden, ob die Code-Injection, bzw. -Execution erfolgreich war, um einen Fehlalarm auszuschließen. In diesem Fall ist von einer Kompromittierung des Systems auszugehen, weshalb das System auf Schwachstellen zu analysieren ist.
6. Das System sollte mit einem Backup wiederhergestellt werden und alle Schwachstellen beseitigt werden.
7. Ebenfalls sollten andere ähnliche Systeme auf dieselben Schwachstellen überprüft werden

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Command-and-Control Communication untersuchen und unterbinden (M.REA.AS-CCCUU)

Zuvor hat ein automatisiertes Sicherheitssystem Steuerungsbefehle (Command-and-Control Communication) detektiert.

1. Das System ist umgehend vom restlichen Netzwerk zu isolieren. Die Verbindung zum C&C-Server kann entweder sofort gekappt werden, oder für Analysezwecke kurz offengehalten und mitgeschnitten werden.

2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Nachdem Steuerbefehle einen Client im System benötigen, der sie interpretieren kann, muss hier von einer sehr starken Kompromittierung des Systems ausgegangen werden.
6. Das System sollte daher vollständig auf Schadsoftware untersucht werden, sowie auf mögliche Sicherheitslücken, durch welche diese Schadsoftware installiert werden konnte. Auch benachbarte Systeme müssen auf Hinweise zu Schadsoftware untersucht werden. Gegebenenfalls sollte während der Überprüfung das gesamte Netzwerk abgeschaltet werden.
7. Das System ist auf einen sicher unkompromittierten Zustand zurückzusetzen, und alle gefundenen Sicherheitslücken zu schließen.
8. Danach kann es wieder ins Netzwerk eingebunden werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Denial of Service unterbinden (M.REA.AS-DOSU)

> Zuvor hat ein automatisiertes Sicherheitssystem einen Denial-of-Service-Angriff detektiert.

1. Falls nicht bereits geschehen, sollten die IP-Adressen, von denen der Angriff ausgeht, gesperrt werden. Bei Distributed-Denial-of-Service-Attacken ist eventuell eine temporäre Sperrung sinnvoller, da große IP-Bereiche betroffen sein könnten.
2. Angegriffene Systeme sollten auf die Integrität ihrer Software untersucht werden, um die Verschleierung eines weiteren Angriffs auszuschließen.
3. Relevante Personen wie zum Beispiel Administratoren sollten informiert werden, dass eventuell weitere Angriffe zu erwarten sind bzw. dass parallel eventuell Angriffe schon laufen, da Denial-of-Service-Angriffe häufig als Ablenkungsmanöver genutzt werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei einer DLL Injection (M.REA.AS-DLLISU)

> Zuvor hat ein automatisiertes Sicherheitssystem eine DLL-Injection detektiert.

1. Falls nicht bereits geschehen, ist das System umgehend zu isolieren. Die Isolation kann erst wieder aufgehoben werden, nachdem sichergestellt wurde, dass das System keine Kompromittierung mehr aufweist, beispielsweise indem ein Backup wiederhergestellt wird.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.

5. Um einen Fehlalarm auszuschließen sollte überprüft werden, ob die DLL-Injection erfolgreich war und bereits Schadcode ausgeführt wurde.
6. Sofern die DLL-Injection erfolgreich war und bereits Schadcode ausgeführt wurde, ist das System als kompromittiert einzustufen. Das System sollte daher auf Schwachstellen analysiert werden.
7. Anschließend sollte das System mit einem Backup wiederhergestellt werden, um die Integrität des Systems wiederherzustellen.
8. Weiterhin sind etwaige Sicherheitslücken oder Schwachstellen zu beheben oder unzugänglich zu machen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Download von nicht vertrauenswürdigen Quellen (M.REA.AS-DNVQ)

> Zuvor hat ein automatisiertes Sicherheitssystem einen Download von einer nicht vertrauenswürdigen Quelle detektiert.

1. Zuerst sollte der betroffene Nutzer, bzw. der Verantwortliche für das System, kontaktiert werden, um einen Fehlalarm auszuschließen.
2. Sofern es keinen legitimen Grund für den Download gibt, muss ein Ausführen der Datei, sofern noch nicht geschehen, verhindert werden.
3. Weiterhin muss das System isoliert werden, um einerseits alle Auswirkungen der heruntergeladenen Schadsoftware rückgängig zu machen, und um andererseits die Sicherheitslücke zu finden, die den Download ermöglicht hat.
4. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
5. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
6. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
7. Nach Möglichkeit sollte die Quelle des Downloads in der Firewall gesperrt werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Vorgehen bei detektierten Hacking-Tools (M.REA.AS-HTSU)

> Zuvor hat ein automatisiertes Sicherheitssystem ein bekanntes Hacking-Tool detektiert.

1. Das genaue Verhalten hängt von der Art des Hacking-Tools ab. Insbesondere ist festzustellen, ob das Hacking-Tool auf dem System selbst ausgeführt wird, oder ob es von außen angreift.
2. Sofern es auf dem System selbst ausgeführt wird, ist das System umgehend zu isolieren, auf Schwachstellen zu untersuchen, die das Eindringen des Hacking-Tools ermöglicht haben, und in einen sicheren Zustand zurückzusetzen. Weiterhin sind etwaige Sicherheitslücken zu schließen.
3. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
4. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
5. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.

6. Je nach Art und Funktionsumfang des Hacking-Tools muss dasselbe für angrenzende Systeme wiederholt werden.
7. Sollte das Hacking-Tool von außen angreifen, sollte die Verbindung gesperrt werden und überprüft werden durch welche Sicherheitslücke eine Verbindung zustande kam. Alle gefundenen Sicherheitslücken sind zu schließen.
8. Sicherheitshalber sollte ein interner Test mit demselben Tool gemacht werden, um sicherzustellen, dass es nicht erfolgreich war.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion auf Lateral Movement (M.REA.AS-LMVSU)

> Zuvor hat ein automatisiertes Sicherheitssystem detektiert, dass ein Angreifer versucht, sich zwischen Systemen zu bewegen.

1. Sofern diese Meldung nicht sofort als Fehlalarm erkannt werden konnte, muss das gesamte System umgehend isoliert werden und auf Notbetrieb gewechselt werden, um vorsorglich zu verhindern, dass ein Angreifer sich erfolgreich auf weitere Systeme ausbreitet.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Anschließend sollte überprüft werden, ob ein Fehlalarm, also eine valide Remote-Management-Administration zu Grunde liegt.
6. Sollte kein valider Grund zugrunde liegen, muss auf dem Ursprungssystem nach Sicherheitslücken gesucht werden, die die Kompromittierung möglich machte, und diese behoben oder unzugänglich gemacht werden. Ebenfalls sollte anschließend das gesamte System auf Sicherheitslücken und Schadsoftware überprüft werden.
7. Nachdem alle Sicherheitslücken behoben wurden, muss das gesamte System in einen sicheren Zustand zurückversetzt werden, indem eine komplette Neuinstallation durchgeführt wird, um ein unkompromittiertes System gewährleisten zu können.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion auf Malware Infection (M.REA.AS-MWISU)

> Zuvor hat ein automatisiertes Sicherheitssystem die Infektion eines Systems mit Malware detektiert.

1. Sofern die Meldung nicht direkt als Fehlalarm erkannt werden kann, ist das System umgehend zu isolieren. Die Isolierung des Systems kann erst wieder aufgehoben werden, sobald das System sicher nicht mehr kompromittiert ist, beispielsweise wenn ein Backup wiederhergestellt wurde oder falls sich die detektierte Software im späteren Verlauf als harmlos herausstellt.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.

4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Nachdem das System jetzt isoliert ist, sollte die gemeldete Software genauer überprüft werden, um Fehlalarme auszuschließen.
6. Sofern es sich tatsächlich um Malware handelt, ist eine genauere Analyse hilfreich, um Informationen über das Angriffsziel sowie über verwendete Schwachstellen zu erlangen.
7. Hiernach ist die Malware und ihre Auswirkungen rückstandsfrei zu entfernen, je nach System kann auch ein Backup wiederhergestellt werden.
8. Weiterhin sind etwaige Sicherheitslücken oder Schwachstellen zu beheben oder unzugänglich zu machen.
9. Alle anderen ähnlichen Systeme sind ebenfalls auf dieselbe Sicherheitslücke zu überprüfen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Netzwerk Replay Angriff unterbinden (M.REA.AS-NA-RPU)

Zuvor hat ein automatisiertes Sicherheitssystem eine Replay-Attack detektiert.

1. Falls nicht bereits automatisiert geschehen, müssen die IP-Adressen, von denen der Angriff ausging, gesperrt werden, um weitere Schäden zu vermeiden.
2. Es muss überprüft werden, ob der Angriff erfolgreich war, also ob ein gefälschtes Paket einen Effekt auf das System hatte.
3. Relevante Personen wie zum Beispiel Administratoren sollten informiert werden, dass eventuell weitere Angriffe zu erwarten sind.
4. Im Falle wiederholter Angriffe können zusätzliche Sicherheitsmaßnahmen in Erwägung gezogen werden, um Netzwerk-Angriffe zu erschweren, beispielsweise kann die Einführung von Nonces oder Zeitstempeln Replay-Attacks erheblich erschweren.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Port Scan unterbinden (M.REA.AS-PSU)

Zuvor hat ein automatisiertes Sicherheitssystem einen Port Scan detektiert.

1. Die IP-Adresse, von der der Port Scan ausgeht, sollte gesperrt werden.
2. Es kann sinnvoll sein, selbst einen gleichartigen Port Scan durchzuführen, um auszuschließen, dass der Angreifer eine offensichtliche Sicherheitslücke entdecken konnte.
3. Weiterhin sollten alle relevanten Personen wie zum Beispiel Administratoren über die Aktivitäten informiert werden, da weitere Angriffe in nächster Zeit zu erwarten sind.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reverse Shell unterbinden (M.REA.AS-RSU)

Zuvor hat ein automatisiertes Sicherheitssystem eine Reverse Shell detektiert.

1. Sofern die Meldung nicht direkt als Fehlalarm erkannt werden kann, ist das System umgehend zu isolieren. Die Isolierung des Systems kann erst wieder aufgehoben werden, sobald das System sicher nicht mehr kompromittiert ist, beispielsweise wenn ein Backup wiederhergestellt wurde.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Das System ist auf Spuren zu untersuchen, die Aufschluss über das Verhalten und Ziel des Angriffs, sowie über ausgenutzte Schwachstellen geben.
6. Alle gefundenen Schwachstellen sind zu beheben, und das System in einen sicheren Zustand zu bringen.
7. Alle Systeme, die mit dem infizierten System kommuniziert haben, müssen auf dieselben Schwachstellen untersucht werden, um gleichartige Angriffe zu verhindern.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Service Discovery unterbinden (M.REA.AS-SDU)

> Zuvor hat ein automatisiertes Sicherheitssystem ein bestehendes Scan-Tool detektiert.

1. Zeitpunkt und betroffene Systeme sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
2. Falls möglich ist die IP-Adresse des Angreifers zu sperren, um den Scan zu unterbinden.
3. Die gescannten Systeme können intern auf die gleiche Weise gescannt werden, um etwaige Sicherheitslücken, die der Scan gefunden haben könnte, aufzudecken.
4. Alle gefundenen Schwachstellen sind zu beheben.
5. Weiterhin sind alle relevanten Personen zum Beispiel Administratoren darüber zu informieren, dass in nächster Zeit weitere Angriffe wahrscheinlicher sein könnten.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful Brute Force Authentication (M.REA.AS-VSBFA)

> Zuvor hat ein automatisiertes Sicherheitssystem einen erfolgreichen Brute-Force-Angriff detektiert.

1. Falls es sich nicht um einen offensichtlichen Fehlalarm handelt, muss der betroffene Account umgehend gesperrt werden.
2. Der betroffene Nutzer sollte kontaktiert werden, um auszuschließen, dass dieser durch wiederholte Loginversuche selbst für die Meldung verantwortlich ist (Ein erfolgreicher Login nach einigen Fehlversuchen kann zu einem falschen Alarm führen).
3. Sollte dies nicht der Fall sein, muss der Account auf Aktivitäten des Angreifers überprüft werden und gegebenenfalls muss das System mit einem Backup wiederhergestellt werden, um im Zweifel alle Änderungen rückgängig zu machen.
4. Alle Schäden sind zu beheben, bevor der Account (mit neuen sichereren Zugangsdaten) wieder freigegeben werden kann.
5. Nachdem der Account erfolgreich brute-forced werden konnte, ist eine strengere Passwortrichtlinie und/oder eine Mehr-Wege-Authentifizierung empfehlenswert.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful Code Injection/Execution (M.REA.AS-VSCI)

Zuvor hat ein automatisiertes Sicherheitssystem eine erfolgreiche Code-Injection oder -Execution detektiert.

1. Nachdem unbekannter Fremdcode auf dem System ausgeführt werden konnte, muss das System als kompromittiert angenommen werden, was eine umgehende Isolation erfordert.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Die Schwachstelle, welche die Code Injection erlaubt hat, ist zu schließen, und das System muss in einen sicheren Zustand zurückgesetzt werden, bevor die Isolation aufgehoben werden darf.
6. Darüber hinaus müssen ähnliche Systeme auf dieselbe Schwachstelle überprüft werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful Exploit of Known Vulnerability (M.REA.AS-VSEKV)

Zuvor hat ein automatisiertes Sicherheitssystem die erfolgreiche Ausnutzung einer bekannten Schwachstelle detektiert.

1. Nachdem die Schwachstelle bereits erfolgreich ausgenutzt wurde, ist das System mit Sicherheit kompromittiert, und muss daher umgehend isoliert werden.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Die Schwachstelle ist zu schließen, und das System muss in einen sicheren Zustand zurückgesetzt werden, bevor die Isolation aufgehoben werden darf.
6. Darüber hinaus müssen ähnliche Systeme auf dieselbe Schwachstelle überprüft werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful Lateral Movement (M.REA.AS-VSLM)

Zuvor hat ein automatisiertes Sicherheitssystem detektiert, dass ein Angreifer sich erfolgreich zwischen Systemen bewegen konnte.

1. Sofern diese Meldung nicht sofort als Fehlalarm erkannt werden konnte, muss das gesamte System umgehend isoliert werden und auf Notbetrieb gewechselt werden, um vorsorglich zu verhindern, dass ein Angreifer sich erfolgreich auf weitere Systeme ausbreitet.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Anschließend sollte überprüft werden, ob ein Fehlalarm, also eine valide Remote-Management-Administration zu Grunde liegt.
6. Sollte kein valider Grund zugrunde liegen, muss auf dem Ursprungssystem nach Sicherheitslücken gesucht werden, die die Kompromittierung möglich machte, und diese behoben oder unzugänglich gemacht werden. Ebenfalls sollte anschließend das gesamte System auf Sicherheitslücken und Schadsoftware überprüft werden.
7. Nachdem alle Sicherheitslücken behoben wurden, muss das gesamte System in einen sicheren Zustand zurückversetzt werden, indem eine komplette Neuinstallation durchgeführt wird, um ein unkompromittiertes System gewährleisten zu können.
8. Als zusätzliche Sicherheitsmaßnahme kann erwägt werden, die verwendeten Zugänge schwerer erreichbar zu machen, z.B. ausschließlich per VPN, um unabhängig von Sicherheitslücken den Zugriff zu erschweren.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful Privilege Escalation (M.REA.AS-VSPE)

Zuvor hat ein automatisiertes Sicherheitssystem eine erfolgreiche Privilege Escalation detektiert.

1. Alle betroffenen Accounts sind umgehend zu sperren, um weitere unerlaubte Zugriffe zu verhindern.
2. Betroffene Nutzer sind schnellstmöglich zu informieren, und es muss überprüft werden, ob ein valider Grund für die zusätzlichen Rechte vorliegt, um einen Fehlalarm auszuschließen.
3. Im Falle eines Fehlalarms ist es hinreichend, die Accounts wieder zu entsperren, andernfalls muss der Vorfall weiter untersucht werden:
4. Nachdem sichergestellt ist, dass die Accounts nicht weiter missbraucht werden können, muss überprüft werden, welche Aktivitäten von den betroffenen Accounts ausgingen, und welche weiteren Schäden verursacht werden konnten. Wichtig ist außerdem, herauszufinden, welche Sicherheitslücke oder Schwachstelle die Privilege Escalation ermöglicht hat. Diese ist umgehend zu beheben oder unzugänglich zu machen.
5. Relevante Aktivitäten und betroffene Systeme sind zu dokumentieren, zu überprüfen und gegebenenfalls rückgängig zu machen, zum Beispiel durch Wiederherstellung eines Backups. Weiterhin sind die Privilegien der Accounts wieder auf die Ursprünglichen zu begrenzen.
6. Sobald alle Schäden, die direkt die Accounts betreffen, behoben sind, können die Accounts (nach Änderung der Zugangsdaten) wieder für die Nutzer geöffnet werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen auf Fehlermeldungen (M.REA.AS-FU)

Zuvor hat ein automatisiertes Sicherheitssystem einen Fehler in einer sicherheitskritischen Anwendung detektiert.

1. Sofern die Meldung nicht direkt als Fehlalarm erkannt werden kann, ist das System umgehend zu isolieren. Die Isolierung des Systems kann erst wieder aufgehoben werden, sobald das System sicher nicht mehr kompromittiert ist, beispielsweise wenn ein Backup wiederhergestellt wurde.
2. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
3. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
4. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
5. Die Fehlermeldungen sind genauer zu analysieren, sowohl auf Manipulationen durch einen potentiellen Angriff als auch auf Sicherheitslücken infolge des Fehlers.
6. In beiden Fällen ist das dahintergelegene System auf Spuren einer Kompromittierung zu untersuchen. Gegebenenfalls ist das System in einen bekannt sicheren Zustand zurückzusetzen, beispielsweise durch Wiederherstellen eines Backups.
7. Zusätzlich muss im Falle eines Angriffs auf die Sicherheitsanwendung analysiert werden, welche Sicherheitslücke verwendet wurde, um diese zu schließen oder unzugänglich zu machen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Scannen von etwaigen Schwachstellen unterbinden (M.REA.AS-SSCU)

Zuvor hat ein automatisiertes Sicherheitssystem charakteristischen Traffic eines fertigen Vulnerability Scanners detektiert.

1. Zeitpunkt und betroffene Systeme sind zu dokumentieren, um in Kombination mit anderen Beobachtungen gegebenenfalls den Ablauf eines größeren Angriffs nachvollziehen zu können.
2. Falls möglich ist die IP-Adresse des Angreifers zu sperren, um den Scan zu unterbinden.
3. Die gescannten Systeme können intern auf die gleiche Weise gescannt werden, um etwaige Sicherheitslücken, die der Scan gefunden haben könnte, aufzudecken.
4. Alle gefundenen Schwachstellen sind zu beheben oder unzugänglich zu machen.
5. Weiterhin sind alle relevanten Personen darüber zu informieren, dass in nächster Zeit weitere Angriffe wahrscheinlicher sein könnten.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion nach einem Gerätediebstahl (M.REA.ÜT/NT-GDS)

Wird ein Gerätediebstahl entdeckt, müssen Maßnahmen ergriffen werden, um

- Die Sicherheit des Kommunikationsnetzes wiederherzustellen
- Die Funktion wiederherzustellen und aufrechtzuerhalten

1. Identifikation der betroffenen Geräte, Anlagen und Netzbereiche
   a) Meldung eines möglichen IT-Sicherheitsvorfalls an die zuständige Stelle (ISMS, Fachabteilung, Alarmplan)
   b) Meldung eines möglichen IT-Sicherheitsvorfalls an den Vorgesetzten
   c) Weiteres Vorgehen anhand der Vorgaben der Fachabteilung und / oder der zuständigen IT-Sicherheitsinstanz zur Erstsicherung (Trennen der Verbindung, Deaktivierung von Geräten, Sicherstellung, von Komponenten und Aufzeichnungen).
   d) Weitere Analyse des Vorfalls und des Netzwerkes entsprechend M...
2. Wiederherstellung der Funktion
3. Gemäß M.DOK.MBP (Seite 127) ist zu prüfen, ob der Vorfall weitergehende Meldung erfordert. Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Weitere Maßnahmen entsprechend der Vorgaben aus dem Bereich Informationssicherheit.

Zugehörige Beobachtungen

Ein Übertragungs- oder Netzwerkgerät wurde entwendet (B.ÜT/NT.GEn) auf Seite 27

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Reaktion auf die Entdeckung eines Fremdgerätes im Übertragungsnetz. (M.REA.ÜT/NT-EFG)

Wird ein Fremdgerät im Übertragungsnetz entdeckt, müssen Maßnahmen ergriffen werden, um

- Die Sicherheit des Kommunikationsnetzes wiederherzustellen
- Die Funktion wiederherzustellen und aufrechtzuerhalten

1. Identifikation der betroffenen Geräte, Anlagen und Netzbereiche
   a) Meldung eines möglichen IT-Sicherheitsvorfalls an die zuständige Stelle (ISMS, Fachabteilung, Alarmplan)
   b) Meldung eines möglichen IT-Sicherheitsvorfalls an den Vorgesetzten
   c) Weiteres Vorgehen anhand der Vorgaben der Fachabteilung und / oder der zuständigen IT-Sicherheitsinstanz zur Erstsicherung (Trennen der Verbindung, Deaktivierung von Geräten, Sicherstellung, von Komponenten und Aufzeichnungen).
   d) Weitere Analyse des Vorfalls und des Netzwerkes entsprechend M.INV.AGR (Seite 74)
   e) Entfernung des Fremdgerätes
   f) Überprüfung, ob weitere Fremdgeräte installiert worden.
2. Wiederherstellung der Funktion
3. Gemäß M.DOK.MBP (Seite 127) ist zu prüfen, ob der Vorfall weitergehende Meldung erfordert. Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Weitere Maßnahmen entsprechend der Vorgaben aus dem Bereich Informationssicherheit.

Zugehörige Beobachtungen

Es wird ein Fremdgerät im Übertragungsnetz entdeckt (B.ÜT/NT.FGE) auf Seite 28

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

IP-Adressen in einem Netzwerk werden untersucht (M.INV.ÜT/NT-IPC) auf Seite 97

Reaktion nach einer Manipulation in der Übertragungstechnik (M.REA.ÜT/NT-Ma)

Wird ein Fremdgerät im Übertragungsnetz entdeckt, müssen Maßnahmen ergriffen werden, um

- Die Sicherheit des Kommunikationsnetzes wiederherzustellen
- Die Funktion wiederherzustellen und aufrechtzuerhalten

1. Manipulation der Konfiguration
   a) Identifikation der betroffenen Geräte, Anlagen und Netzbereiche
   b) Meldung eines möglichen IT-Sicherheitsvorfalls an die zuständige Stelle (ISMS, Fachabteilung, Alarmplan)
   c) Meldung eines möglichen IT-Sicherheitsvorfalls an den Vorgesetzten
   d) Weiteres Vorgehen anhand der Vorgaben der Fachabteilung und / oder der zuständigen IT-Sicherheitsinstanz zur Erstsicherung (Trennen der Verbindung, Deaktivierung von Geräten, Sicherstellung, von Komponenten und Aufzeichnungen).
   e) Weitere Analyse des Vorfalls und des Netzwerkes entsprechend M...
   f) Entfernung der betroffenen Geräte
   g) Identifikation und Überprüfung gleichartiger Geräte
2. Mechanische Manipulation des Übertragungsnetzes
   a) Meldung eines möglichen IT-Sicherheitsvorfalls an die zuständige Stelle (ISMS, Fachabteilung, Alarmplan)
   b) Meldung eines möglichen IT-Sicherheitsvorfalls an den Vorgesetzten
   c) Weiteres Vorgehen anhand der Vorgaben der Fachabteilung und / oder der zuständigen IT-Sicherheitsinstanz zur Erstsicherung (Trennen der Verbindung, Deaktivierung von Geräten, Sicherstellung, von Komponenten und Aufzeichnungen).
   d) Feststellen mechanischer Veränderungen und Schäden
   e) Austausch beschädigter Geräte
   f) Wiederherstellung der korrekten Hardwarekonfiguration
   g) Wiederinbetriebnahme und Funktionskontrolle
3. Überprüfung der Anlage auf weitere Veränderungen.
4. Gemäß M.DOK.MBP (Seite 127) ist zu prüfen, ob der Vorfall weitergehende Meldung erfordert. Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen nach M.DOK.SDOK (Seite 127) kann die Bearbeitung abgeschlossen werden.

Weitere Maßnahmen entsprechend der Vorgaben aus dem Bereich Informationssicherheit.

Zugehörige Beobachtungen

Ein Übertragungs- oder Netzwerkgerät wurde manipuliert (B.ÜT/NT.GMa) auf Seite 27

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Phishing Versuche untersuchen und Mitarbeiter über die Gefahr informieren (M.REA.SFM-PVUMI)

Zuvor hat ein automatisiertes Sicherheitssystem einen Phishing-Versuch detektiert.

1. Da diese Meldung bedeutet, dass der Phishing-Versuch noch nicht erfolgreich war, sind daher alle betroffenen Nutzer umgehend zu informieren, und betreffende Phishing-Nachrichten gegebenenfalls zu kennzeichnen oder zu löschen.
2. Der Angriff, insbesondere eventuelle Schadsoftware-Payloads, sollten analysiert werden, um Informationen über das genaue Ziel zu erlangen.
3. Weiterhin sollten alle Nutzer über die Herangehensweise des Angriffs informiert werden, um besser auf zukünftige Angriffe vorbereitet zu sein.
4. Falls ein Nutzer bereits Opfer des Phishing-Angriffs wurde, sind entsprechende Maßnahmen unter "Successful Phishing" zu finden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Successful Phishing: automatisierte Erkennung (M.REA.SFM-VSPAE)

Zuvor hat ein automatisiertes Sicherheitssystem einen erfolgreichen Phishing-Versuch detektiert.

1. Der betroffene Nutzer sollte kontaktiert werden, um einen Fehlalarm auszuschließen.
2. Sollte ein Angriff nicht ausgeschlossen werden können, ist das betroffene System umgehend zu isolieren.
3. Bei der Isolierung ist es wichtig zu gewährleisten, dass keine Verbindung mehr nach außen oder zu anderen angrenzenden Systemen besteht. Bei entsprechenden Kenntnissen sollte die Firewall so konfiguriert werden, dass das kompromittierte System keinen Ein-/Ausgehenden Traffic mehr zulässt.
4. Sollte dies nicht möglich oder ausreichend sein, können alternativ auch die Netzwerkschnittstellen abgeschaltet werden, die Netzwerkkabel entfernt werden oder auch das kompromittierte System heruntergefahren werden.
5. In jedem Fall sollte bei Bedarf ein Ersatzsystem herangezogen werden.
6. Nach Behebung etwaiger Schäden (abhängig von der Art des Phishings) und gegebenenfalls Änderung der Zugangsdaten kann das System wieder freigegeben werden.
7. Eine Analyse der verwendeten Phishing-Software und des genauen Ziels kann Aufschluss über die Absichten des Angreifers geben.
8. Weiterhin könnte dies ein Anlass für eine vertiefende Schulung zu Phishing sein. In jedem Fall sollten andere Nutzer über die Art und Weise des Angriffs informiert werden, um sich vor zukünftigen ähnlichen Angriffen schützen zu können.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Accounts mit gestohlenen Zugangsdaten sperren (M.REA.SFM-AZS)

Zuvor hat ein automatisiertes Sicherheitssystem gestohlene Zugangsdaten detektiert.

1. Alle betroffenen Accounts sind umgehend zu sperren, um weitere unerlaubte Zugriffe zu verhindern. Betroffene Nutzer sind zu informieren.
2. Nachdem sichergestellt ist, dass die Accounts nicht weiter missbraucht werden können, muss überprüft werden, welche Aktivitäten von den betroffenen Accounts ausgingen, und welche weiteren Schäden verursacht werden konnten.
3. Relevante Aktivitäten und betroffene Systeme sind zu dokumentieren, zu überprüfen und gegebenenfalls rückgängig zu machen.
4. Sobald alle Schäden, die direkt die Accounts betreffen, behoben sind, können die Accounts (nach Änderung der Zugangsdaten) wieder für die Nutzer geöffnet werden.
5. Schlussendlich muss untersucht werden, wie das Datenleck verursacht worden sein könnte, damit erforderliche Maßnahmen gegebenenfalls getroffen werden können.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127
Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Unautorisierte physische Eindringversuche (M.REA.SFM-UPEV)

Ein potentieller Angreifer versucht, in geschützte Bereiche einzudringen.

1. Prinzipiell sind alle Fremden, die das Gelände betreten möchten, auf ihre Legitimation zu überprüfen, und sofern möglich für die Dauer ihres Aufenthalts zu begleiten. Zur besseren Nachverfolgbarkeit sollte ihr Aufenthalt auch mit Anfangs- und Endzeit festgehalten werden.
2. Im Falle eines unautorisierten Eindringens sind neben den üblichen Maßnahmen (Polizei informieren, überprüfen, ob etwas gestohlen wurde) auch alle potenziell innerhalb der Eindringdauer erreichbaren Systeme auf Schadsoftware und Manipulationen zu untersuchen.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Überprüfung des Systems auf vom Angriff betroffene Komponenten (M.INV.AGR) auf Seite 74

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Vorgehen bei Verlust von Zugangsmitteln (M.REA.SFM-VVZ)

Zuvor hat ein Mitarbeiter festgestellt, dass er Zugangsmittel, wie z.B. Schlüssel, Transponder, etc. verloren hat.

1. Alle betroffenen Transponder, Token, etc. sind umgehend zu sperren, um weitere unerlaubte Zugriffe zu verhindern.
2. Nachdem sichergestellt ist, dass die Zugangsmittel nicht missbraucht werden können, muss überprüft werden, ob Aktivitäten mit den Zugangsdaten nach Verlust durch den Mitarbeiter stattgefunden haben.
3. Relevante Aktivitäten und betroffene Systeme sind zu dokumentieren, zu überprüfen und gegebenenfalls rückgängig zu machen.
4. Falls Aktivitäten bekannt geworden sind, sind diese an den Sicherheitsbeauftragten zu melden und ggfs. müssen Behörden eingeschaltet werden.

Mit der vollständigen Dokumentation von Beobachtung, erfolgten Arbeitsschritten und gewonnen Erkenntnissen kann die Bearbeitung abgeschlossen werden.

Zugehörige Maßnahmen

Arbeitsschritt dokumentieren (M.DOK.SDOK) auf Seite 127

Meldung an Behörden prüfen (M.DOK.MBP) auf Seite 127

Nachbereitung

Maßnahmen bei Ausfall eines Leitsystem-Ersatzstandorts (M.NAB.LL)

Maßnahmen die bei Ausfall eines Ersatzstandorts des Leitsystems getroffen werden müssen.

Zuvor wurde ein IT-Ereignis, IT-Sicherheitsereignis oder ein anderer Vorfall entdeckt und erfolgreich bearbeitet. Gerade bei schwerwiegenden Vorfällen mit starken Auswirkungen auf den Geschäftsbetrieb, müssen im Nachgang "Lessons Leraned" erstellt werden. Bei meldepflichtigen Ereignissen sind diese meist als Teil der Berichte gefordert.

1. Tragen Sie alle Dokumentationen von den beteiligten Akteuren zusammen.
2. Versuchen Sie Maßnahmen oder Erkenntnisse abzuleiten. Dabei sollen folgende drei Schwerpunkte berücksichtigt werden:

Erläuterung	
Prävention	*Vorbeugung bzw. Senkung der Eintrittswahrscheinlichkeit eines Ereignisses. Hierunter fassen sie alle Maßnahmen und Erkenntnisse zusammen, die ein erneutes Eintreten solch eines Vorfalls verhindern oder zumindest unwahrscheinlicher machen. Die Leitfrage, nach der Sie sich richten sollten, lautet: Wie kann das Eintreten eines solchen Vorfalls in Zukunft verhindert werden?*

Erläuterung	
Detektion	*Erkennung eines Ereignisses. Hierunter fassen sie alle Maßnahmen und Erkenntnisse zusammen, die das Entdeckung bzw. Detektion eines solchen Vorfalls erleichtern oder zumindest wahrscheinlicher machen. Die Leitfrage, nach der Sie sich richten sollten, lautet: Wie kann ein solcher Vorfall in Zukunft schneller und besser entdeckt werden?*
Reaktion	*Reaktion auf ein Ereignis. Hierunter fassen sie alle Maßnahmen und Erkenntnisse zusammen, die sich auf die Reaktion auf das Eintreten eines solchen Ereignisses beziehen. Die Leitfrage, nach der Sie sich richten sollten, lautet: Wie kann in Zukunft besser auf solch einen Vorfall reagiert werden?*

3. Stellen Sie die dokumentierten Lessons Learned den beteiligten Akteuren und weiteren Experten zur Verfügung und diskutieren sie mit ihnen. Nehmen Sie Änderungen und Anmerkungen auf.
4. Fügen Sie die gewonnenen Erkenntnisse zu der firmeninternen Dokumentation zu. Falls es in Ihrem Unternehmen bislang keine Dokumentation für Lesson Learned oder Ähnliches gibt, stoßen Sie die Erstellung an.

Die gewonnenen Erkenntnisse wurden systematisch erfasst und an zentraler Stelle dokumentiert.

Zugehörige Maßnahmen

Abschlussdokumentation erstellen (M.DOK.ADE) auf Seite 127

Dokumentation

Papierunterlagen entsprechend ihrer „Klassifikation“ kennzeichnen (M.REA.ORG-PKK)

Unterlagen, sowohl in Papierform als auch digital, müssen entsprechend ihrer Klassifikation gekennzeichnet werden.

1. Unterlagen mit der Klassifikation **STRENG VERTRAULICH**
   MÜSSEN ausdrücklich als solche gekennzeichnet werden! Autorisierte Empfänger *MÜSSEN* benannt/ dokumentiert werden! Diese Vertraulichkeitsstufe *MUSS* ausschließlich durch autorisiertes Personal z.B. Unternehmensvorstand klassifiziert werden! Ausgedruckte Infomationen *MÜSSEN* geschreddert werden! Digitale Datenträger *MÜSSEN* durch zertifizierte Verfahren vernichtet werden!
2. Unterlagen mit der Klassifikation **VERTRAULICH**
   SOLLEN ausdrücklich als solche gekennzeichnet werden! *DARF* nur gemäß dem Prinzip "Kenntnis nur wenn nötig" (Need-To-Know-Prinzip) mit Mitarbeitern geteilt werden oder auch mit Geschäftspartnern, die eine Vertraulichkeitserklärung (NDA) unterzeichnet haben. Ausgedruckte Infomationen *MÜSSEN* geschreddert werden
3. Unterlagen mit der Klassifikation **INTERN** und **ÖFFENTLICH**
   DÜRFEN ausdrücklich als solche gekennzeichnet werden. *DÜRFEN* im Papierkorb entsorgt werden.
4. Die Kennzeichnung *SOLL* - unabhängig von der verwendeten Methode - leicht erkennbar sein.

   In einem digitalen Format gespeicherte Informationen können entweder durch elektronische Wasserzeichen, Beschriftung von Kopf- und Fußzeilen, Einbettung von Kennzeichnungen in Metadaten, durch Verwendung von Dateinamenskonventionen oder durch Auswahl entsprechenden Vertraulichkeitsstufen aus einem Menü des verwendeten Tools / der verwendeten Anwendung gekennzeichnet werden (falls zutreffend). In einem physischen Format gespeicherte Informationen (z.B. handschriftliche Dokumente) können mit Stempeln oder ähnlichem gekennzeichnet werden. Informationen, die in gesprochener Form durch menschliche Interaktion ausgetauscht werden, können einen verbalen Hinweis bezüglich der Vertraulichkeitsstufe enthalten.

Die Information wurde erfolgreich an Hand ihrer Vertraulichkeitsstufe gekennzeichnet.

Arbeitsschritt dokumentieren (M.DOK.SDOK)

Bei der Untersuchung eines möglichen IT-Ereignisses, müssen alle Arbeitsschritte dokumentiert werden.

1. Dokumentieren Sie jeden ihrer Arbeitsschritte.
2. Notieren Sie hierzu jede ihrer Tätigkeiten wenigsten in Form einer Stichpunktaufzählung.
3. Falls es ein Ticketsystem gibt, notieren Sie sich die Ticketnummer.
4. Falls sie mit jemanden telefonieren oder reden, notieren Sie sich den Namen Ihres Gesprächspartners und die Uhrzeit

   Beachten Sie hierbei die Vertraulichkeitsstufen und geben nur die Informationen weiter, die für Ihren Gesprächspartner freigegeben sind.
5. Speichern Sie die dokumentierten Arbeitsschritte.

   Beachten Sie hierbei die Vertraulichkeitsstufen und kennzeichnen Sie die Datei entsprechend.
6. Wenn Sie die Bearbeitung des Vorfalls an jemanden abgeben, stellen Sie ihm eine Kopie der Dokumentation zur Verfügung.

   Nur wenn Ihr Kollege im Bilde ist, was bereits unternommen wurde, kann er effizient weiterarbeiten.

Der Arbeitsschritt wurde erfolgreich dokumentiert.

Zugehörige Maßnahmen

Papierunterlagen entsprechend ihrer „Klassifikation“ kennzeichnen (M.REA.ORG-PKK) auf Seite 126

Meldung an Behörden prüfen (M.DOK.MBP)

Bei der Untersuchung eines möglichen IT-Ereignisses, muss geprüft werden, ob eine Meldung an die Behörden notwendig ist.

1. Entscheiden Sie an Hand der folgenden Übersicht, ob das zu bearbeitende IT-Ereignis meldepflichtig ist:

   Meldepflichtige Ereignisse
2. Die Meldung wird dann nach folgendem Schema abgearbeitet:

   Meldewege

Der Arbeitsschritt wurde erfolgreich dokumentiert.

Zugehörige Maßnahmen

Papierunterlagen entsprechend ihrer „Klassifikation“ kennzeichnen (M.REA.ORG-PKK) auf Seite 126

Abschlussdokumentation erstellen (M.DOK.ADE)

Bei meldepflichtigen Ereignissen, muss eine Abschlussdokumentation für die Behörden erstellt werden

1. Sammeln Sie alle Dokumentationen zu den Teilschritten.
2. Erstellen sie die Abschlussmeldung in der Vorlage, bzw. nach den Vorgaben der jeweiligen Behörde.

Der Arbeitsschritt wurde erfolgreich dokumentiert.

Glossar

BNetzA

Bundesnetzagentur

BSI

Bundesamt für Sicherheit in der Informationstechnik

CIT

Commercial Information Technology - Oberbegriff für normale kommerzielle IT-Komponenten. Synonym für Office-IT.

DSL

Digital Subscriber Line (DSL) - Übertragungsstandard der Bitübertragungsschicht.

DWDM

Dense Wavelength Division Multiplex - Derzeit leistungsstärkstes optisches Multiplex-Verfahren für Glasfasertechnik.

eBASE

eBASE ist ein modernes Netzleitsystem, das zur Steuerung von Strom- und Gasnetzen im e.on-Konzern eingesetzt wird. Es stammt vom Hersteller PSI und basiert auf der PSI-Control Familie.

Einsman

Einspeisemanagment - Beschreibt den Prozess die Erzeugungsleistung von Anlagen zur Aufhebung von Netzengpässen zu reduzieren. Wird perspektivisch vom Redipatch-Prozess abgelöst werden.

IT

Information Technology - Oberbegriff für elektronische Datenverarbeitungstechnologie. Im Rahmen dieses Maßnahmenkatalogs wird mit IT auf normale kommerzielle Office-IT verwiesen.

KRITIS

Kritische Infrastrukturen

Leitsystem

Das Leitsystem ist eine zentrale Komponente in der Steuerung von Energienetzen. Es ist dafür verantwortlich, alle angeschlossenen Teilsysteme wie z.B. Fernwirkgeräte oder Schaltanlagen zu koordinieren. Ein Ausfall des Leitsystems, würde daher zur Folge haben, dass das gesamte System nicht mehr gesteuert werden kann.

MPLS

Multiprotocol Label Switching (MPLS) - verbindungsorientierte Übertragung von Datenpaketen.

NLST

Netzleitstelle

OT

Operational Technology - Oberbegriff für IT Komponenten, an die besondere Anforderungen in Bezug auf Sicherheit, Verfügbarkeit, Vertraulichkeit gestellt werden. Bezeichnet IT-Komponenten im industriellen Umfeld, wie z.B. Fabbrikautomatisierungstechnik oder Steuerungstechnik von Energienetzen.

PDH

Plesiochrone Digitale Hierarchie - (griech. plesio „fast, beinahe“; chronos „Zeit“) ist eine international standardisierte Technik zum Multiplexen digitaler Datenströme, die über Weitverkehrsstrecken übertragen werden.

PIT

Prozess-IT - Gesamtheit aller IT-Komponenten, die für die Steuerung von Energienetzen benötigt werden. Synonym für OT

SCADA

Supervisory Control and Data Acquisition - Zentrale Steuerungsinstanz in der Prozesstechnik. Oft als Leitsystem bezeichnet.

Schaltmeister

- Der Schaltmeister bzw. die Schaltmeisterin hat bei seiner bzw. ihrer Arbeit die Aufgabe, alle Abläufe, die sich im Zusammenhang mit der Stromversorgung und elektrischen Anlagen ergeben, fachlich zu kontrollieren und zu überwachen.

SDH

Die Synchrone Digitale Hierarchie (SDH) ist eine der Multiplextechniken im Bereich der Telekommunikation, die das Zusammenfassen von niederratigen Datenströmen zu einem hochratigen Datenstrom erlaubt. Das gesamte Netz ist dabei synchron.

Sekundäre-Team

Sekundärtechnik-Team Das Team, das für die Gesamtheit aller steuerungs-, regelungs- und schutztechnischen Komponenten im Umspannwerk oder Schaltstationen zuständig ist.

setIT

setIT ist ein vom Fernwirkgerätehersteller SAE entwickeltes multifunktionales Parametrier- und Diagnosewerkezeug. Diese Paramitiersoftware stellt SAE ihren Kunden bei Nutzung ihrer Fernwirkgeräte zur Verfügung.

SFP

Small Form-factor Pluggable (SFP) - standardisierte Module für Netzwerkverbindungen.

ÜT

Übertragungstechnik

VNC

Virtual Network Computing - plattformunabhängige Fernwartungssoftware, die den Bildschirminhalt eines entfernten Rechners auf einem lokalen Rechner anzeigt und im Gegenzug Tastatur- und Mausbewegungen sendet.

Index

R

S

T

U

V

Z