Reaktionsplan bei Cybervorfällen

Vorlage

# Verwendung dieses Dokuments

* Dieses Dokument enthält Leitlinien und Beispiele, an denen sich Organisationen orientieren können, um die Entwicklung ihres eigenen Cyber Incident Response Plan (CIRP) zu unterstützen. Die Vorlage ist nicht erschöpfend. Der CIRP jeder Organisation sollte auf ihr einzigartiges Betriebsumfeld, ihre Prioritäten, Ressourcen und Verpflichtungen zugeschnitten sein. Einige Felder enthalten **Mustertext in grün**. Dieser Text dient nur als Beispiel und sollte nicht als Grundlage für Ihren CIRP verwendet werden.
* Eine zusätzliche CIRP-Toolbox mit Checklisten und Vorlagen, die während der Entwicklung Ihres CIRP verwendet werden können, ist ebenfalls verfügbar.

Inhalt

[Verwendung dieses Dokuments 2](#_Toc170201026)

[Behörde und Überprüfung 3](#_Toc170201027)

[Dokumentenkontrolle und -prüfung 3](#_Toc170201028)

[Versionsverwaltung 3](#_Toc170201029)

[Zielsetzungen und Ziele 4](#_Toc170201030)

[Normen und Rahmenwerke 4](#_Toc170201031)

[Definitionen und Akronyme 4](#_Toc170201032)

[Ablauf der Reaktion auf einen Vorfall 5](#_Toc170201033)

[Häufige Sicherheitsvorfälle und Reaktionen 6](#_Toc170201034)

[Terminologie und Definitionen 6](#_Toc170201035)

[Gemeinsame Bedrohungsvektoren 7](#_Toc170201036)

[Häufige Cyber-Vorfälle 8](#_Toc170201037)

[Rollen und Verantwortlichkeiten 8](#_Toc170201038)

[Kontaktstellen für die Meldung von Cyber-Vorfällen 9](#_Toc170201039)

[Reaktionsteam für Cybervorfälle (CIRT) 9](#_Toc170201040)

[Leitungsteam (MT) 9](#_Toc170201041)

[Rollen und Beziehungen 10](#_Toc170201042)

[Kommunikation 11](#_Toc170201043)

[Interne Kommunikation 11](#_Toc170201044)

[Externe Kommunikation 11](#_Toc170201045)

[Meldepflicht für NIS2 12](#_Toc170201046)

[Unterstützende Verfahren und Fahrpläne 13](#_Toc170201047)

[Unterstützende Standardarbeitsanweisungen (SOPs) 13](#_Toc170201048)

[Unterstützende Playbooks 13](#_Toc170201049)

[Benachrichtigung von Interessengruppen und Meldung von Vorfällen 13](#_Toc170201050)

[Prozess der Reaktion auf Vorfälle 14](#_Toc170201051)

[Erkennung, Forschung, Analyse und Aktivierung 14](#_Toc170201052)

[Klassifizierung der Vorfälle 14](#_Toc170201053)

[Fragen zur Untersuchung von Vorfällen 15](#_Toc170201054)

[Eskalation und De-Eskalation 15](#_Toc170201055)

[Eindämmung, Beweissicherung und Beseitigung 16](#_Toc170201056)

[Eindämmung 16](#_Toc170201057)

[Dokumentation 16](#_Toc170201058)

[Erhebung und Sicherung von Beweismitteln 17](#_Toc170201059)

[Aktionsplan zur Beseitigung von Mängeln 17](#_Toc170201060)

[Erholung 18](#_Toc170201061)

[Lektionen gelernt. 18](#_Toc170201062)

# Behörde und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung** |  |
| Autor |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von |  |
| Datum der letzten Überarbeitung |  |

.

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum der Genehmigung** | **Genehmigt durch** | **Beschreibung der Änderung** |
|  |  |  |  |

# Ziele und Aufgaben

Beschreiben Sie hier den Zweck Ihres Cyber Incident Response Plan (CIRP).

*Zum Beispiel:*

*Ziel dieses CIRP ist es, eine schnelle und wirksame Reaktion auf Cyber-Vorfälle zu unterstützen, die mit den Sicherheits- und Geschäftszielen der Organisation in Einklang steht*.

*Zielsetzungen des CIRP*

* *Bereitstellung von Leitlinien für die erforderlichen Schritte zur Reaktion auf Cyber-Vorfälle.*
* *Beschreibung der Aufgaben, Zuständigkeiten, Verantwortlichkeiten und Befugnisse der Mitarbeiter und Teams, die für die Bewältigung von Cyber-Vorfällen erforderlich sind.*
* *Skizzieren Sie die Anforderungen an die Einhaltung von Vorschriften bei Cybervorfällen.*
* *Skizzieren Sie interne und externe Kommunikationsprozesse bei der Reaktion auf Cybervorfälle.*
* *Bereitstellung von Leitlinien für Aktivitäten nach einem Vorfall zur Unterstützung der kontinuierlichen Verbesserung.*

# Normen und Rahmenwerke

Die folgenden Dokumente dienten als Anregung für die Erstellung dieser Vorlage. Die Verweise sind nicht datiert. Hier gilt immer die letzte Ausgabe des referenzierten Dokuments (einschließlich aller Änderungen).

* [CyberFundamentals Framework](https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework) (www.cyfun.be)
* [NIST SP 800-61](https://csrc.nist.gov/pubs/sp/800/61/r2/final)Handbuch für den Umgang mit Computersicherheitsvorfällen
* ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3 Verwaltung von Informationssicherheitsvorfällen.
* ISO/IEC 27001, Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Managementsysteme für Informationssicherheit - Anforderungen
* ISO/IEC 27002, Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre

Managementsysteme für die Informationssicherheit - Maßnahmen zur Verwaltung der Informationssicherheit.

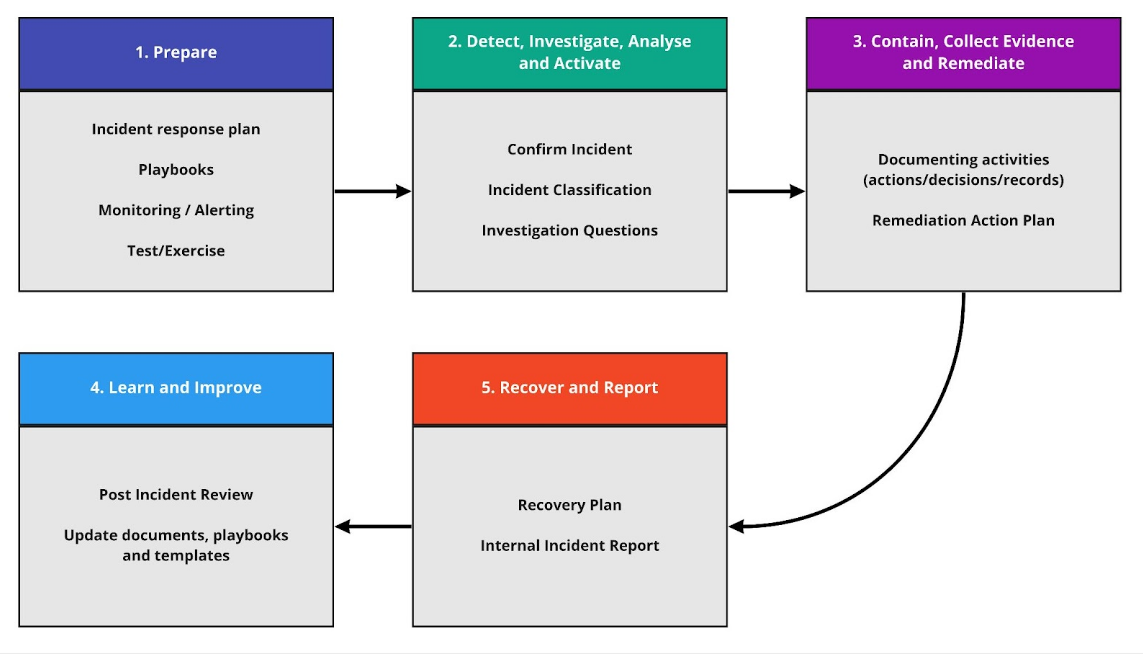
* Australisches Zentrum für Cybersicherheit, Cyber Incident Response Plan.

# Definitionen und Akronyme

In diesem Dokument gelten die Begriffe und Definitionen aus ISO/IEC 17000, ISO/IEC 27000 und die folgenden Abkürzungen.

|  |  |
| --- | --- |
| **CEO** | Geschäftsführender Direktor |
| **CFO** | Direktor Finanzen |
| **CIO** | Chief Information Officer |
| **CIRP** | Reaktionsplan auf Cybervorfälle |
| **CIRT** | Team für die Reaktion auf Cybervorfälle |
| **CISO** | Chief Information Security Officer |
| **COO** | Chief Operating Officer |
| **DDoS** | Verteiltes Denial-of-Service |
| **DoS** | Denial-of-Service |
| **DSB** | Datenschutzbeauftragter |
| **GBA** | Datenschutzbehörde |
| **ICS** | Industrielles Steuerungssystem |
| **MT** | Management-Team |
| **RPO** | Wiederherstellungspunkt Zielsetzung |
| **RTO** | Angestrebte Wiederherstellungszeit |
| **SN** | Seriennummer |
| **SPOC** | Zentrale Anlaufstelle |

# Ablauf der Reaktion auf Vorfälle



# Häufige Sicherheitsvorfälle und Reaktionen

## Terminologie und Definitionen

Die Verwendung einer einheitlichen und vordefinierten Terminologie zur Beschreibung von Vorfällen und deren Folgen kann bei einer Reaktion hilfreich sein. Nehmen Sie in Ihren Reaktionsplan für Cyber-Vorfälle (CIRP) gängige Begriffe auf, die in Ihrer Organisation verwendet werden. Cyber-Bedrohungen, -Ereignisse, -Warnungen und -Vorfälle werden wie folgt definiert:

|  |  |
| --- | --- |
| **bedeutendes Ereignis** | jedes Ereignis, das die Erbringung einer der Dienstleistungen in den in den Anhängen I und II des Gesetzes aufgeführten Sektoren oder Teilsektoren erheblich beeinträchtigt und das:   * eine schwerwiegende betriebliche Störung bei einem der Dienste in den in den Anhängen I und II aufgeführten Sektoren oder Teilsektoren oder finanzielle Verluste für die betreffende Stelle verursacht hat oder verursachen kann, oder * andere natürliche oder juristische Personen geschädigt haben oder schädigen können, indem sie einen erheblichen materiellen oder immateriellen Schaden verursachen. |
| **Beinahe-Zwischenfälle** | ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der von Netz- und Informationssystemen angebotenen oder über sie zugänglichen Dienste hätte beeinträchtigen können, das aber erfolgreich verhindert wurde oder nicht eingetreten ist; |
| **Cyber-Bedrohung** | Eine Cyber-Bedrohung ist jeder Umstand oder jedes Ereignis, das Systeme oder Informationen beschädigen kann. Die folgende Liste zeigt das Bedrohungsumfeld und die wichtigsten Trends im Bereich der Cybersicherheit:   * Phishing-E-Mails und Betrügereien * Ransomware * Ausnutzung von Sicherheitslücken * Kompromiss bei der Software-Lieferkette * Gefährdung von Geschäfts-E-Mails * Cyberkriminalität |
| **Cybersecurity-Veranstaltung** | Ein Cybersicherheitsereignis ist ein Ereignis in einem System, Dienst oder Netzzustand, das auf eine mögliche Verletzung der Sicherheitsrichtlinien, ein Sicherheitsversagen oder eine bisher unbekannte Situation hinweist, die für die Sicherheit relevant sein könnte. Ein Cybersicherheitsereignis kann sich zu einem Cybervorfall entwickeln, ist aber noch kein solcher.  Beispiele für Cybersicherheitsereignisse sind (unter anderem)   * Ein Benutzer hat das Antivirusprogramm auf seinem Computer deaktiviert * Ein Benutzer hat Systemdateien gelöscht oder verändert * Ein Benutzer hat einen Server neu gestartet * Unbefugter Zugriff auf einen Server oder ein System. |
| **Cybersecurity-Warnung** | Eine Cybersicherheitswarnung ist eine Benachrichtigung, die als Reaktion auf eine Abweichung vom normalen Verhalten generiert wird. Cybersicherheitswarnungen werden verwendet, um auf Cybersicherheitsereignisse hinzuweisen. |
| **Cyber-Vorfall** | Ein Cybervorfall ist ein unerwünschtes oder unerwartetes Cybersicherheitsereignis oder eine Reihe solcher Ereignisse, die mit hoher Wahrscheinlichkeit den Geschäftsbetrieb beeinträchtigen können. Ein Cybervorfall erfordert Abhilfemaßnahmen.  Beispiele für Cybersicherheitsvorfälle sind unter anderem:   * Denial-of-Service-Angriffe (DoS) * Unerlaubter Zugang oder versuchter Zugang zu einem System * Kompromittierung sensibler Informationen * Ausbruch von Viren oder Malware (einschließlich Ransomware). |

### Gemeinsame Bedrohungsvektoren

Die folgende Tabelle enthält häufige Bedrohungsvektoren aus dem NIST Computer Security Incident Handling Guide.

|  |  |
| --- | --- |
| **Typ** | **Beschreibung** |
| **Externe/entnehmbare Medien** | Ein Angriff, der von einem Wechseldatenträger oder einem Peripheriegerät ausgeht (z. B. bösartiger Code, der sich über ein infiziertes USB-Flash-Laufwerk auf einem System verbreitet). |
| **Versagen** | Ein Angriff, bei dem Brute-Force-Methoden eingesetzt werden, um Systeme, Netze oder Dienste zu beeinträchtigen, zu kompromittieren oder zu zerstören (z. B. ein DDoS, der darauf abzielt, den Zugang zu einem Dienst oder einer Anwendung zu behindern oder zu verweigern, oder ein Brute-Force-Angriff auf einen Authentifizierungsmechanismus wie Passwörter). |
| **Web** | Ein Angriff, der von einer Website oder einer webbasierten Anwendung aus durchgeführt wird (z. B. ein Cross-Site-Scripting-Angriff zum Diebstahl von Anmeldedaten oder eine Umleitung zu einer Website, die eine Schwachstelle im Browser ausnutzt und Malware installiert). |
| **E-Mail** | Ein Angriff, der über eine E-Mail-Nachricht oder einen Anhang ausgeführt wird (z. B. als angehängtes Dokument getarnter Exploit-Code oder ein Link zu einer bösartigen Website im Hauptteil einer E-Mail). |
| **Verbot in der Lieferkette** | Ein antagonistischer Angriff auf Hardware oder Software, bei dem physische Implantate, Trojaner oder Hintertüren verwendet werden, um Waren abzufangen und zu verändern, die sich auf dem Weg vom Hersteller oder Verkäufer befinden. |
| **Nachahmung** | Ein Angriff, bei dem etwas Gutartiges durch etwas Bösartiges ersetzt wird (z. B. Spoofing, Man-in-the-Middle-Angriffe, betrügerische drahtlose Zugangspunkte und SQL-Injection-Angriffe sind alle mit Impersonation verbunden). |
| **Unsachgemäße Verwendung** | Jeder Vorfall, der auf einen Verstoß gegen die Nutzungsrichtlinien einer Organisation durch einen autorisierten Benutzer zurückzuführen ist, mit Ausnahme der oben genannten Kategorien (z. B. ein Benutzer installiert eine File-Sharing-Software, was zu einem Verlust sensibler Daten führt). |
| **Verlust oder Diebstahl von Ausrüstung** | Verlust oder Diebstahl eines von einer Organisation verwendeten Computergeräts oder -mediums (z. B. eines Laptops, Smartphones oder Verifizierungstokens). |

### Häufige Cyber-Vorfälle

In der folgenden Tabelle sind gängige Arten von Cyber-Vorfällen und die entsprechenden ersten Reaktionsmaßnahmen aufgeführt.  
 Beschreiben Sie kurz die erste Reaktion auf den Vorfall. Zum Beispiel: Benachrichtigung der betroffenen Personen, Isolierung der betroffenen Geräte, Befolgung der relevanten Playbooks und Verfahren.

|  |  |
| --- | --- |
| **Typ/Beschreibung** | **Antwort** |
| **Denial of Service (DoS) und Distributed Denial of Service (DDoS):** Überflutung eines Dienstes mit Datenverkehr, was manchmal die Verfügbarkeit beeinträchtigt. | *Wie in Spielbuch X und Verfahren..... beschrieben, ergreifen Sie zunächst lokale Maßnahmen, um das Problem zu lösen.*  *Wenn dies nicht funktioniert, bitten Sie laut XYZ um die Erlaubnis, zur zweiten Leitung zu eskalieren, usw.* |
| **Phishing:** Irreführende Nachrichten, um Benutzern sensible Informationen zu entlocken (z. B. Bank- oder Geschäftsanmeldedaten) oder um bösartigen Code auszuführen, der einen Fernzugriff ermöglicht. | *Wenn vom Personal durch erfolgreiche schädliche Inhalte identifiziert*  *Schulung, Warnung und Übergabe einer Kopie an den Sicherheitsbeauftragten. Nächster Entwurf*  *Aktionen und andere externe und interne Benachrichtigungsaktionen, usw*. |
| **Ransomware:** ein Programm, das die Dateien der Opfer sperrt oder verschlüsselt, bis ein Lösegeld gezahlt wird. |  |
| **Malware:** ein Trojanisches Pferd, ein Virus, ein Wurm oder eine andere bösartige Software, die ein Computersystem oder ein Netzwerk beschädigen kann. |  |
| **Datenschutzverletzung:** unbefugter Zugriff auf und Offenlegung von Informationen. |  |
| **Kompromittierung eines industriellen Kontrollsystems:** Unbefugter Zugriff auf ICS. |  |

# Rollen und Verantwortlichkeiten

In diesem Abschnitt werden die Aufgaben und Zuständigkeiten der wichtigsten Personen und Teams erläutert, die für die Reaktion auf Vorfälle und die Entscheidungsfindung zuständig sind, darunter das Cyber Incident Response Team (CIRT) auf der operativen Ebene und das Management Team (MT) auf der strategischen Ebene.

Alle hier aufgeführten Mitarbeiter sollten mit ihren Zuständigkeiten im Rahmen dieses Plans vertraut sein und ihre Reaktion üben.

### Kontaktstellen für die Meldung von Cyber-Vorfällen

Primäre und sekundäre (Backup-) interne Kontaktstellen für die Meldung von Cyber-Vorfällen während eines 24/7-Zeitraums.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Die Öffnungszeiten** | **Kontaktangaben** | **Titel** | **Zuständigkeiten** |
| *Unbekannter* | *09:00-18:00* | *Mobiltelefonnummer,* | *Hauptansprechpartner im Falle eines Vorfalls* | *SPOC* |

### Reaktionsteam für Cybervorfälle (CIRT)

Geben Sie Einzelheiten über das CIRT an, das für die Reaktion auf Cybervorfälle zuständig ist. Die Zusammensetzung Ihres CIRT hängt von der Größe Ihrer Organisation und den verfügbaren Fähigkeiten und Ressourcen ab. Geben Sie Einzelheiten zu externen Lieferanten an, die Ihre IKT-Systeme/Anwendungen bereitstellen oder verwalten. Geben Sie gegebenenfalls Einzelheiten zu Ihren externen Anbietern von Notfallmaßnahmen und den von ihnen angebotenen Dienstleistungen an.

CIRT-Mitglieder, die für die Bewältigung von Cyber-Vorfällen zuständig sind:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation Rolle** | **Kontaktangaben** | **CIRT-Rolle Titel** | Zuständigkeiten CIRT |
|  |  |  | *Cyber Incident Manager* | *Terminierung der Antworten*  *CIRT-Einsätze* |
|  |  |  | *Netzwerktechniker,* |  |
|  |  |  | *Systemadministratoren,* |  |
|  |  |  |  |  |
|  |  |  |  |  |

Bei größeren Cybersicherheitsvorfällen kann das CIRT erweitert werden:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organisation Rolle** | **Kontaktangaben** | **CIRT-Rolle Titel** | **Zuständigkeiten CIRT** |
|  |  |  | *Managerin für Kommunikation* | *Informationen und Warnungen*  *Interne Kommunikation* |
|  |  |  | *Rechtsberater* | *Rechtsberatung*  *(einschließlich der Einhaltung gesetzlicher Vorschriften)* |
|  |  |  |  |  |

### Management-Team (MT)

Bei schwerwiegenden Cybervorfällen kann es erforderlich sein, eine MT zu bilden, die das CIRT strategisch beaufsichtigt, leitet und unterstützt und sich dabei auf Folgendes konzentriert

* Strategische Probleme erkennen und bewältigen
* Einbindung von Interessenvertretern und Kommunikation (einschließlich Kontakt mit Verwaltung und Ministerien, falls zutreffend)
* Bedarf an Ressourcen und Fähigkeiten (einschließlich dringender logistischer oder finanzieller Anforderungen und Überlegungen zur Personalbesetzung während des Einsatzes).

MT-Mitglieder, die für die Bewältigung von Cyber-Vorfällen zuständig sind:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Kontaktangaben** | **Titel** | **MT-Rolle** |
|  |  | *CEO* | *Stuhl* |
|  |  | *CIO* | *Stellvertretender Vorsitzender* |
|  |  | *CISO* | *Sicherheitswarnung und Überwachung der CIA.* |
|  |  | *COO* | *Operative Funktionen des Unternehmens* |
|  |  | *CFO* | *Notkäufe und Überwachung der Ausgaben* |
|  |  | *Juristischer Rat* | *Einhaltung von Vorschriften, Cyber-Versicherung* |
|  |  | *Managerin für Kommunikation* | *Öffentlichkeitsarbeit und Einbeziehung von Interessengruppen* |
|  |  |  |  |

### Rollen und Beziehungen

Das folgende Diagramm zeigt die Beziehungen zwischen den wichtigsten Mitarbeitern und Teams, die an der Reaktion beteiligt sind.



# Kommunikation

Bei der Reaktion auf einen Vorfall besteht ein ständiger Bedarf an Informationen von vielen verschiedenen Beteiligten. Jeder von ihnen wird eine andere Art von Informationen benötigen. Erstellen Sie Ihre eigene Liste potenzieller Beteiligter und stellen Sie sicher, dass die richtigen Kontaktinformationen verfügbar sind! Beachten Sie, dass die Organisation diese Kontaktinformationen zur Verfügung haben sollte, aber nicht immer mit allen Beteiligten kommunizieren muss.

Die Organisationen sollten bedenken, dass sie, sobald eine Partei benachrichtigt wurde, um regelmäßige Aktualisierungen bezüglich des betreffenden Vorfalls bitten werden. In der Regel gibt es keine einmalige Mitteilung, und der Kommunikationsplan sollte diese regelmäßigen Aktualisierungen berücksichtigen.

Der erste Schritt in Ihrem vorfallspezifischen Kommunikationsplan besteht darin, zu bestimmen, mit wem Sie kommunizieren werden. Dazu müssen Sie ermitteln, welche potenziellen Interessengruppen von dem Cyber-Sicherheitsvorfall, mit dem Sie konfrontiert sind, (nachteilig) betroffen sein könnten und ob Sie gesetzlich verpflichtet sind, bestimmte Stellen zu benachrichtigen.

* Interne Stakeholder: Top-Management, betroffene Manager, Mitarbeiter
* Externe Stakeholder: Medien, Kunden, Lieferanten, andere Partner usw.
* Offizielle Akteure: GBA, Sektoraufsichtsbehörde, Polizei, ....

Bei der Entscheidung darüber, was und mit wem kommuniziert werden soll, gilt die Faustregel, dass nur das kommuniziert werden soll, was man wissen muss. Es wird Beteiligte geben, mit denen Sie kommunizieren wollen, um den Cyber-Sicherheitsvorfall einzudämmen, und es wird Beteiligte geben, mit denen Sie kommunizieren müssen, weil sie Sie um Informationen bitten (z. B. die Medien) oder weil Sie gesetzlich verpflichtet sind, sie zu informieren.

### Interne Kommunikation

*Anleitung:*

Zusätzlich zu den regelmäßigen Lageberichten kann es erforderlich sein, die Mitarbeiter Ihrer Organisation über einen Cybervorfall zu informieren. Dies ist wichtig, wenn die IT-Netzwerke, Betriebssysteme oder Anwendungen der Organisation nicht mehr wie erwartet funktionieren oder wenn die Situation das Interesse der Medien oder der Öffentlichkeit wecken könnte.

Die wichtigsten Botschaften für die Mitarbeiter sind

* Was ist passiert und warum?
* Was wird in naher Zukunft geschehen?
* Was wird von den Mitarbeitern erwartet?
* An wen können sich die Mitarbeiter wenden, wenn sie Fragen haben?

### Externe Kommunikation

*Anleitung:*

Je nach Auswirkung und Schwere eines Cybervorfalls kann es erforderlich sein, mit externen Beteiligten (einschließlich Minister, Medien und Öffentlichkeit) zu kommunizieren. Dies ist besonders wichtig, wenn der Vorfall IT-Netze, Kontrollsysteme oder Anwendungen betrifft, auf die Dritte angewiesen sind, wie Websites oder Dienste für die Öffentlichkeit.

Zu den wichtigen Botschaften, die bei der Kommunikation mit externen Stakeholdern zu beachten sind, gehören:

* Was ist passiert und warum?
* Welche Systeme/Dienste sind betroffen?
* Welche Schritte werden unternommen, um die Situation zu klären?
* Kann man sagen, wann die Situation geklärt sein wird?
* Was wird von externen Stakeholdern erwartet?
* An wen können sich externe Beteiligte wenden, wenn sie Fragen/Bedenken haben?

**Alle Mitteilungen müssen vor ihrer Freigabe vom *Kommunikationsmanager und dem Incident Manager* geprüft und genehmigt werden.**

### Meldepflicht für NIS2

Wesentliche und wichtige Einrichtungen gemäß der Definition in Kapitel 4 (Artikel 11 und 12) der belgischen [NIS2](https://www.ejustice.just.fgov.be/cgi/article.pl?language=nl&sum_date=2024-05-17&lg_txt=n&pd_search=2024-05-17&s_editie=1&numac_search=2024202344&caller=sum&2024202344=4&view_numac=2024202344f) Gesetzgebung definiert sind, sind **verpflichtet**, eine Reihe von Anforderungen zu erfüllen, um Frühwarnungen oder **bedeutende Vorfälle\*** an das nationale CSIRT zu melden ([CERT.be](https://ccb.belgium.be/nl/cert)).

Diese Warnungen oder bedeutenden Vorfälle sollten dem CERT innerhalb von **vierundzwanzig Stunden** nach ihrer Entdeckung gemeldet werden. Diese Meldung muss unter anderem die folgenden Informationen enthalten:

* Ist der Vorfall das Ergebnis einer unrechtmäßigen oder böswilligen Handlung?
* Hat der heiße Vorfall grenzüberschreitende Auswirkungen?

**Innerhalb von zweiundsiebzig Stunden** nach der Meldung des Ereignisses muss die Organisation - falls zutreffend - ein:

* Aktualisierung der obigen Informationen
* Eine erste Bewertung des bedeutenden Vorfalls, einschließlich der Schwere und der Folgen.
* Indikatoren der Verschlechterung.

**Spätestens einen Monat** nach der Meldung des bedeutenden Vorfalls wird ein Abschlussbericht erstellt und an das CERT weitergeleitet, der Folgendes enthält

* Detaillierte Beschreibung des Vorfalls, einschließlich des Schweregrads und seiner Folgen.
* Die Art der Bedrohung oder die Ursache, die wahrscheinlich zu dem Vorfall geführt hat.
* Angewandte und laufende Maßnahmen zur Risikominderung (sowohl technisch als auch organisatorisch).
* Falls zutreffend, die grenzüberschreitenden Auswirkungen des Vorfalls.

Ist der Vorfall nach diesen 30 Tagen noch nicht behoben, wird ein Fortschrittsbericht erstellt und an das CERT weitergeleitet. Ein Abschlussbericht wird innerhalb eines Monats nach Beendigung des Vorfalls erstellt und übermittelt.

Zusätzlich zu der oben genannten Meldepflicht können **freiwillige** Meldungen an das CERT gemacht werden:

* *Für wesentliche und wichtige Einrichtungen*: Zwischenfälle, Cyber-Bedrohungen, Beinahe-Zwischenfälle.
* *Andere Organisationen, unabhängig davon, ob sie in den Anwendungsbereich der NIS2 fallen*: erhebliche Vorfälle, Cyber-Bedrohungen und Beinahe-Vorfälle

# Unterstützende Verfahren und Fahrpläne

### Unterstützende Standardarbeitsanweisungen (SOPs)

Die Standardarbeitsanweisungen (SOPs), die zur Unterstützung der Reaktion auf Vorfälle zur Verfügung stehen:

* *Erkennung, Triage und Analyse von Ereignissen*
* *Plan zur Aufrechterhaltung des Geschäftsbetriebs*
* *Plan zur Wiederherstellung im Katastrophenfall.*

### Unterstützende Playbooks

Die verfügbaren Playbooks bieten Schritt-für-Schritt-Leitlinien für Reaktionen auf häufige Vorfälle:

* *Reaktionsplan für Cybersicherheitsvorfälle -* ***Phishing***
* *Reaktionsplan für Cybersicherheitsvorfälle* ***- Eindringen in Daten/Diebstahl***
* *Reaktionsplan für Cybersicherheitsvorfälle* ***- Malware***
* *Reaktionsplan für Cybersicherheitsvorfälle* ***- Ransomware***
* *Cyber Security Incident Response Playbook* ***- Denial of Service.***

# Stakeholder Benachrichtigung und Meldung von Vorfällen

Zu den Verfahren für die interne und externe Benachrichtigung und Meldung von Vorfällen gehören:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Art des Vorfalls/**  **Schwellenwert** | **Organisation , die eine Meldung  oder einen Bericht  erhalten  möchte** | **Kontaktangaben  der meldenden Organisation.** | **Wichtige Melde- und Berichtspflichten und Verbindung zu organisatorischen Informationen** | **Verantwortliches Personal** |
| Ransomware | Zentrum für Cybersicherheit Belgien. CERT.BE | info@ccb.belgium.be | https://www.cert.be/en/report-incident-0 | Cyber Incident Manager |
| Verletzung von personenbezogenen Daten | Datenschutzbehörde | +32 (0)2 274 48 00  +32 (0)2 274 48 35  contact@apd-gba.be | https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens | Rechtsbeistand oder DSB |

* **die rechtlichen und regulatorischen Anforderungen für Ihr Unternehmen auflisten.**
* **Wenn es eine Cyber-Versicherungspolice gibt, prüfen Sie die darin enthaltenen Anforderungen, um sicherzustellen, dass Sie sie erfüllen.**

# Prozess der Reaktion auf Vorfälle

# Aufdeckung, Forschung, Analyse und Aktivierung

Verweisen Sie auf Ihre eigenen Standardarbeitsanweisungen zur Erkennung, Untersuchung und Analyse von Vorfällen. Dazu kann gehören, wie Sie auf ein Ereignis oder einen Vorfall aufmerksam werden und wie Sie sofort darauf reagieren.

Vorfälle können auf verschiedene Weise aufgedeckt werden, unter anderem durch:

* Selbst erkannte Vorfälle (z.B. Intrusion Detection and Prevention Systeme)
* Empfang von Benachrichtigungen von Dienstleistern oder Anbietern
* Benachrichtigungen von vertrauenswürdigen Dritten wie dem Centre for Cyber Security Belgium, MITRE ATT&CK, ENISA....

### Klassifizierung von Vorfällen

Dies kann helfen, Prioritäten bei den Ressourcen zu setzen. Klassifizierungsfaktoren können sein:

* Folgen des Vorfalls (Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen)
* Beteiligte Stakeholder (intern und extern)
* Art des Vorfalls
* Auswirkungen auf Wirtschaft und Gesellschaft.

|  |  |
| --- | --- |
| **Klassifizierung von Vorfällen** | **Beschreibungen** |
| **Kritisch** | *Ein kritischer Vorfall mit sehr starken Auswirkungen. Häufig handelt es sich um einen vollständigen Systemausfall, den Verlust von Kundendaten, größere Sicherheitsverletzungen oder kritische Infrastrukturausfälle.* |
| **Hoch** | *Ein schwerwiegender Vorfall mit erheblichen Auswirkungen. Er kann partielle Systemausfälle beinhalten oder kritische Funktionen betreffen.* |
| **Mittel** | *Ein Vorfall mit mäßiger Auswirkung, der nicht kritische Funktionen beeinträchtigen oder Unannehmlichkeiten für die Benutzer verursachen kann.* |
| **Niedrig** | *Ein kleiner Vorfall mit geringer Auswirkung, der aus unkritischen Funktionsausfällen oder Benutzerbeschwerden von geringer Priorität bestehen kann.* |

### Fragen zur Untersuchung von Vorfällen

Eine Liste mit Untersuchungsfragen kann Ihnen bei Ihren Bemühungen helfen, auf einen Vorfall zu reagieren und den Umfang und die Auswirkungen des Vorfalls zu verstehen. Nicht alle Fragen können mit den verfügbaren Daten beantwortet werden, und die Fragen können sich im Verlauf der Untersuchung ändern.

* *Wer hat den Vorfall entdeckt oder gemeldet?*
* *Wann wurde der Vorfall entdeckt oder gemeldet?*
* *Wo wurde der Vorfall entdeckt oder lokalisiert?*
* *Welche Auswirkungen hat der Vorfall auf den Betrieb?*
* *Welches Ausmaß hat der Vorfall im Netzwerk und bei den Anwendungen?*

### Eskalation und Deeskalation

Cyber-Vorfälle können eskaliert oder deeskaliert werden. Die Rollen, die eskalieren oder deeskalieren können, sollten tabellarisch aufgeführt werden.

|  |  |  |  |
| --- | --- | --- | --- |
| **Klassifizierung von Vorfällen** | **Aktion** | **Grund für die Eskalation/Deeskalation** | **Entscheider** |
|  |
| **Kritisch** | Deeskalation auf hoch |  |  |  |
| **Hoch** | Eskalation bis zur Kritik |  |  |  |
| Deeskalation zum Durchschnitt |  |  |  |
| **Mittel** | Eskalierend bis hoch |  |  |  |
| Deeskalierend auf niedrig |  |  |  |
| **Niedrig** | Eskalierend zum Durchschnitt |  |  |  |

# Eingrenzung, Beweissicherung und Beseitigung

### Eindämmung

Die Eindämmung ist wichtig, bevor ein Vorfall die Ressourcen überfordert oder den Schaden vergrößert. Die meisten Vorfälle müssen eingedämmt werden, daher ist dies eine wichtige Überlegung zu einem frühen Zeitpunkt bei der Bewältigung eines Vorfalls. Die Eindämmung verschafft Zeit für die Entwicklung einer maßgeschneiderten Wiederherstellungsstrategie. Ein wesentlicher Bestandteil der Eindämmung ist die Entscheidungsfindung (z. B. Herunterfahren eines Systems, Trennen von einem Netzwerk, Deaktivieren bestimmter Funktionen). Solche Entscheidungen sind viel leichter zu treffen, wenn es vorher festgelegte Strategien und Verfahren zur Eindämmung des Vorfalls gibt. Organisationen sollten akzeptable Risiken im Umgang mit Zwischenfällen definieren und entsprechende Strategien entwickeln.

Die Eindämmungsstrategien variieren je nach Art des Vorfalls. So unterscheidet sich beispielsweise die Strategie zur Eindämmung einer Malware-Infektion per E-Mail stark von der für einen DDoS-Angriff über ein Netzwerk. Unternehmen sollten für jeden wichtigen Vorfallstyp separate Eindämmungsstrategien mit klar dokumentierten Kriterien ausarbeiten, um die Entscheidungsfindung zu erleichtern. Zu den Kriterien für die Bestimmung der richtigen Strategie gehören:

* Mögliche Beschädigung und Diebstahl von Ressourcen
* Aufbewahrung von Beweismitteln
* Verfügbarkeit von Diensten (z. B. Netzanbindung, Dienste für externe Parteien)
* Zeit und Ressourcen, die für die Umsetzung der Strategie erforderlich sind
* Wirksamkeit der Strategie (z. B. teilweise Eindämmung, vollständige Eindämmung)
* Dauer der Lösung (z. B. Notlösung, die innerhalb von vier Stunden zu entfernen ist, vorübergehende Lösung, die innerhalb von zwei Wochen zu entfernen ist, Dauerlösung).

In einigen Fällen leiten einige Unternehmen den Angreifer in eine Sandbox (eine Art Eindämmung) um, damit sie die Aktivitäten des Angreifers überwachen können, in der Regel um zusätzliche Beweise zu sammeln. Das Incident Response Team sollte diese Strategie mit der Rechtsabteilung besprechen, um festzustellen, ob sie durchführbar ist. Wenn eine Organisation weiß, dass ein System kompromittiert wurde, und es zulässt, dass die Kompromittierung fortgesetzt wird, kann sie haftbar gemacht werden, wenn der Angreifer das kompromittierte System nutzt, um andere Systeme anzugreifen. Die Strategie der verzögerten Eindämmung ist gefährlich, da ein Angreifer den unbefugten Zugriff ausweiten oder andere Systeme kompromittieren kann.

Ein weiteres potenzielles Problem im Zusammenhang mit der Eindämmung ist, dass einige Angriffe zusätzlichen Schaden verursachen können, wenn sie eingedämmt werden. So kann beispielsweise ein kompromittierter Host einen bösartigen Prozess ausführen, der regelmäßig Pings an einen anderen Host sendet. Wenn der Incident Handler versucht, den Vorfall einzudämmen, indem er den kompromittierten Host vom Netzwerk trennt, schlagen die nachfolgenden Pings fehl. Als Folge dieses Fehlschlags kann der bösartige Prozess alle Daten auf der Festplatte des Hosts überschreiben oder verschlüsseln. Die Verantwortlichen sollten nicht davon ausgehen, dass, nur weil ein Host vom Netz getrennt wurde, weitere Schäden an dem Host verhindert wurden.

### Dokumentation

Die Dokumentation aller relevanten Informationen über den Vorfall ist von wesentlicher Bedeutung. Die folgende Liste ist ein Hinweis auf relevante Informationen, die dokumentiert werden sollten. Wenn Berichte für das Management oder andere Beteiligte erstellt werden, sollten diese Informationen im Bericht enthalten sein.

* Datum und Uhrzeit des Vorfalls
* Aktueller Stand des Vorfalls
* Kontaktdaten der zuständigen Personen (Incident Manager, CISO, CEO, ....)
* Umfang und Auswirkungen
* Ernst
* Art des Vorfalls und Klassifizierung
* Benötigen Sie externe Hilfe? JA / NEIN. Bitte geben Sie Ihre Kontaktinformationen an.
* Maßnahmen zur Eindämmung und Behebung des Vorfalls.
* Informationen über die nächste Aktualisierung des Vorfalls (Datum, Uhrzeit, wer wird informiert)

### Sammlung und Sicherung von Beweismitteln

Führen Sie bei der Sammlung von Beweismitteln ein detailliertes Protokoll, das eindeutig dokumentiert, wie alle Beweismittel gesammelt wurden. Darin sollte festgehalten werden, wer die Beweise gesammelt oder gehandhabt hat, wann die Beweise gesammelt und gehandhabt wurden und welche Details zu jedem gesammelten Objekt gehören (einschließlich physischer Standort, Seriennummer, Modellnummer, Hostname, Protokolldateien, IP-Adresse, Betriebssystem, ....).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum, Uhrzeit der Abholung** | **Gesammelt von** | **Beweise Details** | **Ort des Nachweises** | **Zugang** |
| *01/01/2024* | *Herr Janssens* | *Laptop-Festplatte mit SN, Modell-Nr.* | *Scheibe mit SN....*  *Im Tresor im Serverraum aufbewahrt* | *ICT-Manager, CIRT-Team* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Aktionsplan für die Sanierung

Erstellen Sie einen Aktionsplan, um den Vorfall nach erfolgreicher Eindämmung und Beweissammlung zu klären.

Bei der Ausarbeitung des Sanierungsplans sollten Sie die folgenden Fragen berücksichtigen. Diese Fragen sind begrenzt und dienen nur zur Orientierung.

* Welche Maßnahmen sind erforderlich, um den Vorfall zu klären?
* Welche (internen und externen) Ressourcen werden benötigt, um den Vorfall zu beheben?
* Wer ist Eigentümer des zu lösenden Problems?
* Gibt es eine Priorität von Systemen oder Diensten, die zur Behebung des Vorfalls benötigt werden?
* Wer und was ist von der Entschließung betroffen?
* Wie sieht der Zeitplan für den Abschluss des Vorfalls aus?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum, Uhrzeit des Vorfalls** | **Kategorie**  **(Kontrolle, Wiederherstellung,...)** | **Aktion** | **Aktion Eigentümer** | **Status**  **(nicht vergeben, in Arbeit, abgeschlossen)** |
| *01/01/2024* | *Enthält* | *Trennen Sie den infizierten Host vom Netzwerk.* | *Systemadministrator (einschließlich Name)* | *In Arbeit* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Erholung

Erstellen Sie Wiederherstellungspläne für verschiedene Szenarien. Der Wiederherstellungsplan sollte den Ansatz für die Wiederherstellung von IT- und/oder OT-Netzwerken, -Systemen und -Anwendungen nach Abschluss der Eindämmung und Sanierung detailliert beschreiben.

Bei der Ausarbeitung eines Wiederherstellungsplans sollten Sie Folgendes beachten:

* Das Ziel der Wiederherstellungszeit (RTO) und das Ziel des Wiederherstellungspunkts (RPO).
* Erstellen Sie ein Verfahren zur Überwachung der Systeme, um sicherzustellen, dass sie nicht mehr gefährdet sind und wie erwartet funktionieren.
* Was kann getan werden, um ähnliche Vorfälle zu verhindern?

# Lektionen gelernt.

Einer der wichtigsten Teile der Reaktion auf Zwischenfälle wird auch am häufigsten übersprungen: Lernen und Verbesserung. Jedes Notfallteam muss sich weiterentwickeln, um neuen Bedrohungen, verbesserten Technologien und gewonnenen Erkenntnissen Rechnung zu tragen. Die Abhaltung eines Treffens mit allen Beteiligten nach einem größeren Vorfall und möglicherweise in regelmäßigen Abständen nach kleineren Vorfällen, wenn die Ressourcen dies zulassen, kann sehr hilfreich sein, um die Sicherheitsmaßnahmen und den Reaktionsprozess selbst zu verbessern. In einer solchen Sitzung können mehrere Vorfälle besprochen werden. Diese Sitzung bietet die Gelegenheit, einen Vorfall abzuschließen, indem erörtert wird, was passiert ist, was unternommen wurde, um einzugreifen, und wie gut der Eingriff funktioniert hat. Die Sitzung sollte innerhalb weniger Tage nach Beendigung des Vorfalls stattfinden.

Während des Treffens sollen unter anderem folgende Fragen beantwortet werden:

* Was genau ist passiert und zu welchen Zeiten?
* Wie gut sind Personal und Management mit dem Vorfall umgegangen? Wurden die dokumentierten Verfahren befolgt? Waren sie angemessen?
* Welche Informationen wurden früher benötigt?
* Wurden Schritte oder Maßnahmen ergriffen, die die Einziehung behindert haben könnten?
* Was würden Mitarbeiter und Management anders machen, wenn ein ähnlicher Vorfall das nächste Mal eintreten würde?
* Wie hätte der Informationsaustausch mit anderen Organisationen verbessert werden können?
* Welche Abhilfemaßnahmen können ähnliche Vorfälle in Zukunft verhindern?
* Auf welche Vorläufer oder Indikatoren sollte in Zukunft geachtet werden, um ähnliche Vorfälle zu erkennen?

Besprechungen über die gewonnenen Erkenntnisse haben weitere Vorteile. Die Aufzeichnungen dieser Treffen sind ein gutes Material für die Schulung neuer Teammitglieder, indem sie ihnen zeigen, wie erfahrene Teammitglieder auf Vorfälle reagieren. Die Aktualisierung von Richtlinien und Verfahren zur Reaktion auf Vorfälle ist ein weiterer wichtiger Teil des Lernprozesses. Eine Post-Mortem-Analyse des Umgangs mit einem Vorfall offenbart oft einen fehlenden Schritt oder eine Ungenauigkeit in einem Verfahren, was zu einer Änderung führt. Aufgrund der sich wandelnden Informationstechnologie und der personellen Veränderungen sollte das Incident-Response-Team in regelmäßigen Abständen alle damit zusammenhängenden Unterlagen und Verfahren für die Behandlung von Vorfällen überprüfen.

**Regelmäßige Tests des Reaktionsplans auf Cyber-Vorfälle sind wichtig, um sicherzustellen, dass diese Dokumente aktuell bleiben und den zuständigen Mitarbeitern bekannt sind. Zu den Testmethoden könnten Diskussionen oder funktionale Übungen gehören.**

**Übungen zu verschiedenen Szenarien des Cyber Incident Response Plans sind von großem Wert, um mehr und mehr Informationen aus den gewonnenen Erkenntnissen zu gewinnen. Während dieser Testszenarien können viele Informationen fehlen oder Prozesse werden nicht wie definiert ausgeführt. Dies sind großartige Ergebnisse, damit Sie Verfahren und Prozesse für den Fall anpassen können, dass Sie den Reaktionsplan für Cybervorfälle wirklich benötigen!**