SOPHOS

# Sophos-Leitfaden für die Erstellung eines Incident-Response-Plans

# Inhalte

# Einführung

Der vorliegende Leitfaden liefert einen umfassenden Überblick über bewährte Verfahren zur Reaktion auf Sicherheitsvorfälle. Dabei werden sowohl technische als auch organisatorische Aspekte beleuchtet, die beim Umgang mit Cyberbedrohungen beachtet werden sollten. Ziel des Leitfadens ist es, Unternehmen bei der Entwicklung wirksamer Incident-Response-Prozesse zu unterstützen.

Zielgruppe sind IT-Security-Experten in technischen oder organisatorischen Funktionen sowie Einsteiger ohne Vorkenntnisse zu Cybersicherheit, denen dieser Leitfaden als Einführung in das Thema dienen kann. Bitte beachten Sie, dass der Leitfaden nicht den Anspruch erhebt, alle Gesetzes- und Verordnungsvorschriften für das Informationssicherheits-Management abzudecken. Er ist als Ergänzung zu den für Ihr Unternehmen geltenden Richtlinien bezüglich Datenschutzverletzungen und der zu ergreifenden Maßnahmen anzusehen. Cyber-Versicherungen sind in diesem Zusammenhang gesondert zu betrachten, da ihre Policen Richtlinien enthalten können, die von den in diesem Leitfaden zusammengestellten Empfehlungen abweichen können.

Eine sorgfältige Vorbereitung auf Cybersicherheitsvorfälle stellt sicher, dass Unternehmen auf standardisierte Protokolle und bewährte Verfahren zurückgreifen können, um Risiken schneller erkennen, zuordnen und eindämmen zu können. Ziel dieses Dokuments ist es, Unternehmen bei der Vorbereitung eines effektiven Vorfallsmanagements zu unterstützen. Es werden Prozesse aufgezeigt, die eine schnellere Eindämmung der Cybervorfälle ermöglichen, um finanzielle und betriebliche Auswirkungen auf Unternehmen zu minimieren.

Sicherheitsexperten wird empfohlen, die dargelegten Konzepte und Analysemethoden in ihre eigenen Incident-Response-Pläne und -Prozesse nach Bedarf einzubinden. Sie können diesen Leitfaden komplett durcharbeiten oder sich auf einzelne Kapitel konzentrieren, die für Sie am wichtigsten sind. Er enthält keine Schritt-für-Schritt-Anweisungen für den Umgang mit Cybersicherheitsvorfällen, aber unterstützt die verantwortlichen Sicherheitsteams bei der Vorbereitung und Implementierung ihrer eigenen Prozesse.

Die in diesem Leitfaden beschriebenen Phasen des Vorfallsmanagements stimmen mit dem vom SANS Institute empfohlenen Incident Response Framework mit sechs Phasen überein. In diesem Rahmenwerk werden die einzelnen Phasen des Vorfallsmanagements erläutert, um Sicherheitsexperten darin zu unterstützen, wirksame Prozesse zur Reaktion auf Vorfälle zu entwickeln. Es handelt sich dabei jedoch um kein Playbook. Cybersicherheitsvorfälle sind dynamisch. So gibt das Rahmenwerk zwar die notwendige Struktur für einen allgemeinen Ansatz vor, doch das professionelle Urteilsvermögen erfahrener Sicherheitsexperten und sicherheitsbewusster Mitarbeiter ist nach wie vor entscheidend, um Bedrohungen wirksam zu bekämpfen.

# Preparation (Vorbereitung)

Die Vorbereitung ist die erste Phase des Incident-Response-Prozesses. Die Maßnahmen der Vorbereitungsphase wirken sich maßgeblich auf die Effizienz und Effektivität der nachfolgenden Phasen aus. Aus diesem Grund sollte diese zentrale Phase regelmäßig überprüft und aktualisiert werden. Die Vorbereitungsphase umfasst sowohl nicht-technische Aspekte, wie Prozesse und Verfahren, als auch technische Komponenten wie Systemhärtung, Erfassung von Telemetriedaten und Training. Eine sorgfältige Vorbereitung ist daher die Voraussetzung für die Entwicklung einer robusten und resilienten Incident-Response-Strategie.

## Prozesse und Verfahren

Gut dokumentierte Prozesse und Verfahren sind für das einwandfreie Funktionieren eines Incident-Response-Teams unerlässlich. Übermitteln Sie diese Leitlinien allen Mitarbeitern, die in die Bearbeitung von Vorfällen involviert sind, um sicherzustellen, dass alle Beteiligten dieselben Informationen haben und dieselben Ziele verfolgen. Klar definierte Prozesse und Verfahren unterstützen das Team bei einem einheitlichen Vorgehen. Sie erleichtern zudem die Kommunikation, sodass alle Beteiligten effizient und koordiniert auf Cybersicherheitsvorfälle reagieren können.

### Incident-Handling-Plan

Ein wirksamer Plan für den Umgang mit Vorfällen (Incident Handling) legt klare Verfahren fest und bietet allen Beteiligten die notwendige Richtschnur. Die folgenden Punkte sollten Sie in Ihren Incident-Handling-Plan aufnehmen, damit ein umfassender Ansatz bei der Reaktion auf Vorfälle gewährleistet ist:

- **Beteiligte Personen festlegen:** Ermitteln Sie, welche Personen in den Incident-Handling-Prozess involviert sind, und weisen Sie konkrete Rollen zu. Hierzu gehören zum Beispiel Incident Leads, ein IT-Zusatzteam, die Verwaltung und das Führungsteam sowie externe Akteure wie IT-Dienstleister, Behörden und Anbieter von Incident-Response-Diensten.
- **Klassifizierung von Vorfällen und Schweregrade:** Führen Sie Kriterien für die Klassifizierung von Vorfällen ein, die auf Faktoren wie mögliche Auswirkungen, betroffene Systeme und Bedrohungstyp basieren. Legen Sie Schweregrade fest, um Prioritäten setzen und die Reaktion auf Vorfälle entsprechend steuern zu können.
- **Eskalationsplan:** Entwickeln Sie einen klaren Eskalationsplan für Vorfälle, die über die Kompetenzen oder Befugnisse der Incident Responder hinausgehen. Beziehen Sie dabei höhere Managementebenen oder externe Experten ein.
- **Kommunikation:** Sorgen Sie während einer Krise mit Vorlagen für eine stringente Kommunikation mit Mitarbeitern, Kunden und Partnern. Bewerten Sie anhand der Vorgehensweisen aus Ihren Plänen für Disaster Recovery und Geschäftskontinuität, welche alternativen Kommunikationskanäle zu E-Mail, Messaging-Dienst und Videokonferenzen verwendet werden können.
- **Asset Inventory:** Halten Sie Ihr Asset Inventory stets auf dem neuesten Stand, um die im Unternehmen verwendete Hardware und Software nachverfolgen und verwalten zu können. Diese Informationen sind entscheidend, um die Verbreitung und Auswirkung einer Bedrohung analysieren und entsprechende Reaktionsmaßnahmen festlegen zu können.
- **Zeitplan für die Reaktion auf Vorfälle:** Erstellen Sie einen Zeitplan für jede Incident-Response-Phase und legen Sie Fristen für die wichtigsten Meilensteine fest, um schnell und koordiniert reagieren zu können.
- **Dokumentation und Berichterstellung bei Vorfällen:** Sorgen Sie für einen standardisierten Prozess zur Dokumentation aller Aspekte eines Vorfalls, einschließlich der ergriffenen Maßnahmen, getroffenen Entscheidungen und erzielten Ergebnisse. Diese Dokumentation ist wichtig für die weitere Analyse nach einem Vorfall sowie für mögliche rechtliche oder behördliche Untersuchungen.
- **Prüfung nach einem Vorfall und kontinuierliche Verbesserung:** Implementieren Sie ein Verfahren zur Prüfung der Reaktion nach einem Vorfall, um die Wirksamkeit der Maßnahmen zu bewerten und verbesserungsbedürftige Bereiche zu ermitteln. Nutzen Sie diese Erkenntnisse, um Ihren Incident-Handling-Plan bei Bedarf zu aktualisieren und nachzubessern.

Wenn Sie diese Aspekte in Ihren Incident-Handling-Plan integrieren, ist Ihr Unternehmen für den Ernstfall und eine schnelle und wirkungsvolle Reaktion auf Cybersicherheitsvorfälle besser gerüstet.

## Rechtliche Dokumentation

Während der Vorbereitungsphase sollten sich Unternehmen auch mit den rechtlichen Pflichten hinsichtlich der Offenlegung, des Umgangs mit Vorfällen und anderen relevanten Aspekten der Cybersicherheit befassen. Die folgenden Abschnitte geben einen allgemeinen Einblick in die notwendigen rechtlichen Überlegungen. Jedes Unternehmen ist angehalten, darüber hinaus die branchen- und standortspezifischen gesetzlichen Anforderungen zu berücksichtigen. Überlegen Sie, welche Personen in Ihrem Unternehmen für die Themen Reporting und Legal Compliance verantwortlich sind und beziehen Sie sie mit klar definierten Rollen in die Entwicklung des Incident-Response-Plans ein.

- **Gesetzliche und regulatorische Pflichten bei Sicherheitsverletzungen:** Manche Unternehmen können aufgrund ihrer Branche oder ihres Status gesetzlich dazu verpflichtet sein, alle Vorfälle zu melden.
  - Unternehmen im Bereich Kritische Infrastrukturen
  - Staatliche Einrichtungen
  - Börsennotierte Unternehmen
- **Datenschutz:** Halten Sie sich an die Datenschutzgesetze, die eine verantwortungsvolle Offenlegung von Datenschutzverletzungen bei den jeweiligen Behörden und den betroffenen Kunden oder Personen vorschreiben.
- **Aufbewahrung und Vernichtung von Daten:** Legen Sie Richtlinien und Verfahren für die Aufbewahrung, Speicherung und sichere Vernichtung von Daten fest, die im Rahmen der Incident Response erfasst wurden, und halten Sie dabei die geltenden Gesetze und Vorschriften ein.
- **Vereinbarungen und Verträge mit Dritten:** Prüfen Sie Ihre Verträge und Vereinbarungen mit Anbietern, Lieferanten und Partnern in Bezug auf deren Pflichten im Fall einer Sicherheitsverletzung oder eines Vorfalls.
- **Schutz geistigen Eigentums:** Denken Sie auch an die rechtlichen Aspekte, die während und nach einem Cybervorfall zum Schutz des geistigen Eigentums Ihres Unternehmens gelten, wie Geschäftsgeheimnisse, Patente, Urheberrechte und Marken.
- **Länderübergreifende Datenübertragung und Berichterstattung:** Wenn Ihr Unternehmen international tätig ist, müssen Sie die rechtlichen Bedingungen und Anforderungen an die Übertragung und Meldung von Daten in den verschiedenen Rechtsgebieten berücksichtigen.
- **Rechte und Pflichten der Mitarbeiter:** Erläutern Sie die gesetzlichen Rechte und Pflichten von Mitarbeitern im Zusammenhang mit Cybersicherheitsvorfällen, einschließlich ihrer Verpflichtung, Vorfälle zu melden und sensible Daten zu schützen.
- **Dokumentation der Versicherungspolice:** Sie müssen den Prozess und die Anforderungen für die Geltendmachung eines Versicherungsanspruchs bei einem Cybersicherheitsvorfall kennen und verstehen.
  - Prüfen Sie den Geltungsbereich und die Ausnahmen Ihrer Versicherungspolice.
  - Beraten Sie sich mit den internen Versicherungsnehmern, um den bestehenden Versicherungsschutz vollumfänglich nachzuvollziehen.

## Incident-Response-Playbooks

Incident-Response-Playbooks beschreiben Schritt für Schritt, welche Maßnahmen bei spezifischen Bedrohungen ergriffen werden sollten. Diese Leitfäden sollten auf einem risikobasierten Ansatz basieren, der die Wahrscheinlichkeit und die potenziellen Auswirkungen verschiedener Angriffsszenarien berücksichtigt. Die folgenden Aspekte sollten Sie beim Erstellen Ihrer Incident-Response-Playbooks berücksichtigen:

- **Auf Ihr Unternehmen zugeschnitten:** Stellen Sie sicher, dass Ihre Playbooks auf die einzigartige Umgebung, die Ressourcen und die Kompetenzen Ihres Unternehmens zugeschnitten sind. Dazu gehören Ihre Unternehmensgröße, Branche und spezifische Risiken.
- **Spezifische Bedrohungen und Szenarien:** In größeren Unternehmen empfiehlt es sich, eigene Playbooks für bestimmte Bedrohungen zu entwickeln, z. B. für bestimmte Arten von Malware oder gezielte Angriffe. Bestehen in Unternehmen nur begrenzte Ressourcen, sollten diese Leitfäden umfassender sein und so viele Bedrohungen wie möglich abdecken, damit sie für unterschiedliche Szenarien verwendet werden können.
- **Klare und präzise Anweisungen:** Die Playbooks müssen klare und präzise Anweisungen für jeden Schritt des Reaktions-Prozesses enthalten. Dadurch können die Beteiligten die bei einem Vorfall erforderlichen Schritte schneller erfassen und ausführen.

- **Rollen und Verantwortlichkeiten:** Definieren Sie für jedes Teammitglied, das am Reaktions-Prozess beteiligt ist, die Rolle und Verantwortlichkeiten. So wissen alle, was von ihnen erwartet wird, was wiederum eine effektive Zusammenarbeit ermöglicht.
- **Kommunikation und Eskalation:** Erstellen Sie Richtlinien für die Kommunikation und Eskalation eines Vorfalls, z. B. wann das Management benachrichtigt oder externe Unterstützung angefordert werden muss.
- **Integration in den Incident-Handling-Plan:** Die Playbooks müssen mit Ihrem Gesamtplan für den Umgang mit Vorfällen abgestimmt sein und diesen unterstützen. Dies trägt dazu bei, dass Ihre Reaktionsmaßnahmen einheitlich und kohärent sind.
- Regelmäßige Updates und Überprüfungen: Die Playbooks müssen regelmäßig geprüft und aktualisiert werden, damit sie auch bei neuen Bedrohungen und veränderten organisatorischen Rahmenbedingungen relevant und wirksam bleiben.

Durch das Einbinden dieser Aspekte in Ihre Incident-Response-Playbooks ist Ihr Unternehmen besser auf eine Vielzahl von Cybersicherheitsvorfällen vorbereitet, kann schneller reagieren und mögliche Auswirkungen gezielt minimieren.

## Backups

Backups sind unerlässlich, um Geschäftskontinuität zu gewährleisten und die Auswirkungen von Datenverlusten aufgrund von Unfällen, Systemausfällen oder Cyberangriffen zu minimieren. Eine robuste Backup-Strategie umfasst das regelmäßige Erstellen und Validieren von Backups. Auch verschiedene Speicheroptionen sollten zur Maximierung der Datenverfügbarkeit bereitgestellt werden. Folgende Aspekte sollten Sie bei der Entwicklung Ihrer Backup-Strategie berücksichtigen:

- **Sicherungshäufigkeit:** Legen Sie fest, wie häufig Backups unter Berücksichtigung der Sensibilität der Daten und des vertretbaren Risikoniveaus erstellt werden müssen. Durch regelmäßige Backups können die möglichen Auswirkungen eines Datenverlusts minimiert werden.
- **Sicherungstypen:** Verwenden Sie eine Kombination aus vollständigen, inkrementellen und differenziellen Backups, um den verwendeten Speicherplatz zu optimieren und eine effiziente Datenwiederherstellung zu ermöglichen.
- **Speicheroptionen:** Nutzen Sie mehrere Speicheroptionen, wie lokal, in der Cloud oder auf externen Festplatten. Dies trägt dazu bei, die Datenverfügbarkeit zu gewährleisten und das Risiko des Datenverlusts aufgrund nur eines einzigen Ausfallpunkts (Single Point of Failure) zu verringern.
- **Priorisierung von geschäftskritischen Daten:** Sichern Sie geschäftskritische Daten und Systeme, die für die Aufrechterhaltung des Betriebs und wichtiger Geschäftsprozesse unerlässlich sind.
- **Verschlüsselte Backups:** Verschlüsseln Sie Ihre Backups, um sensible Daten zu schützen und unbefugte Zugriffe während der Speicherung und Übertragung zu unterbinden.
- **Backups überprüfen:** Überprüfen Sie Ihre Backups regelmäßig daraufhin, ob sie zuverlässig erstellt werden und bei Bedarf erfolgreich wiederhergestellt werden können. Testen Sie gegebenenfalls auch den Wiederherstellungsprozess und prüfen Sie die Integrität Ihrer gesicherten Daten.
- **Aufbewahrungsrichtlinien:** Implementieren Sie Richtlinien zur Datenaufbewahrung, um für eine Aufbewahrung und Löschung von Backups in Übereinstimmung mit den rechtlichen, regulatorischen und geschäftlichen Anforderungen zu sorgen.
- **Disaster-Recovery-Planung:** Integrieren Sie Ihre Backup-Strategie in Ihren Notfallplan zur Wiederherstellung der Daten und Systeme, um im Falle eines Datenverlusts koordiniert und effektiv vorgehen zu können.

Wenn Sie diese Punkte in Ihre Backup-Strategie einbeziehen, ist Ihr Unternehmen schneller in der Lage, seine Daten wiederherzustellen.

## System- und Netzwerkhärtung

Die System- und Netzwerkhärtung trägt dazu bei, die Angriffsfläche zu reduzieren, indem unnötige Funktionen eliminiert und die Zugriffe auf Systeme und Netzwerkverbindungen minimiert werden. Durch wirksame Härtungsmaßnahmen verringert Ihr Unternehmen die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs. Berücksichtigen Sie folgende Aspekte bei Ihrer Strategie zur Härtung Ihres Systems und Netzwerks:

### Patching

- **Patch-Management-Programm:** Richten Sie ein Programm ein, das die zeitnahe und einheitliche Installation von Patches in Ihrem Netzwerk mit automatischen oder halbautomatischen Patching-Tools sicherstellt.
- **Dokumentation:** Dokumentieren Sie, welche Patches installiert werden sowie eventuelle Ausnahmen.
- **Priorisierung:** Priorisieren Sie die Patches auf Basis einer Risikoanalyse und konzentrieren Sie sich auf die Schwachstellen, die sich potenziell am stärksten auf Ihr Unternehmen auswirken würden.

### Konfiguration

- **Security Compliance Auditing:** Führen Sie fortlaufend interne und externe Prüfungen durch, um die Konfiguration und Einstellungen Ihrer Sicherheitstools zu überprüfen und eventuelle Fehlkonfigurationen oder Ausschlüsse zu identifizieren und zu beheben.
- **Application Control:** Richten Sie Listen ein, um bestimmte Anwendungen zuzulassen oder zu blockieren. Begrenzen Sie zudem die Anzahl und Versionen von Anwendungen, die auf den Hosts ausgeführt werden können. So verringern Sie das Risiko , dass nicht autorisierte oder anfällige Software ausgenutzt wird.
- **Network Access Control:** Konfigurieren Sie Netzwerk-Tools, um den IP- und Port-Zugriff auf die erforderlichen internen und externen Hosts zu beschränken. So minimieren Sie die Wahrscheinlichkeit eines unbefugten Zugriffs oder einer Datenexfiltration.
- **Principle of Least Privilege:** Die Zugriffsrechte der Benutzer in Ihrem Unternehmen sollten auf das Minimum beschränkt sein, das sie für die Erfüllung ihrer Aufgaben benötigen. So verringern Sie das Risiko eines unbefugten Zugriffs und der Datenkompromittierung.

### Netzwerksicherheit

- **Netzwerksegmentierung:** Teilen Sie Ihr Netzwerk in kleinere, isolierte Segmente auf, um die potenziellen Auswirkungen einer Sicherheitsverletzung zu begrenzen. Zudem wird es Angreifern erschwert, sich in Ihrem Netzwerk lateral zu bewegen.
- **Firewall-Konfiguration:** Konfigurieren Sie Firewalls, um allen unnötigen ein- und ausgehenden Datenverkehr zu blockieren. Überprüfen und aktualisieren Sie die Vorschriften regelmäßig, um stets einen optimalen Sicherheitsstatus zu gewährleisten.
- **Intrusion-Detection- und Intrusion-Prevention-Systeme (IDPS):** Durch die Einrichtung von IDPS können Sie den Netzwerkverkehr auf schädliche Aktivitäten hin überwachen und entsprechende Gegenmaßnahmen ergreifen.

## Überwachung und Telemetrie

Überwachung und Telemetrie sind essenzielle Mechanismen für eine wirksame Reaktion auf Vorfälle, da sie wertvolle Einblicke in die Umgebung eines Unternehmens geben und somit potenzielle Bedrohungen frühzeitig erkannt werden. Wenn Sie Ihre Umgebung kennen und geeignete Schutzebenen zur Erkennung und Abwehr von Angriffen implementieren, verbessert sich die Reaktionsfähigkeit Ihres Unternehmens bei einem Vorfall.

### Ihre Umgebung

Ein umfassendes Bild Ihrer Umgebung bildet die Grundlage für eine effektive Überwachung und Telemetrie. Hierzu zählen:

- Asset Inventory: Führen Sie ein Verzeichnis aller aktuellen Endpoints und Server und wie diese durch die relevanten Sicherheitsplattformen geschützt werden.
- Netzwerktopologie: Verschaffen Sie sich einen klaren Überblick über Ihr Netzwerk mit allen Zugangs- und Ausgangspunkten, Segmentierung und Kontrollpunkten, vorzugsweise mithilfe eines aktuellen Diagramms.

### Schutzebenen zur Erkennung und Abwehr

Ein mehrschichtiger Schutz zur Erkennung und Abwehr von Bedrohungen ist essenziell für eine umfassende Sicherheitsstrategie. Ziehen Sie die folgenden Telemetriequellen in Betracht und sorgen Sie für einheitliche Zeitstempel in allen Quellen, wobei UTC als Standard empfohlen wird:

- **Peripheriegeräte:** Firewalls, Intrusion-Prevention-Systeme (IPS), Intrusion-Detection-Systeme (IDS), VPNs und Proxys.
- **Endpoint-Sicherheit:** Anti-Virus (AV), Next-Gen Anti-Virus (NGAV), Endpoint/Extended Detection and Response (E/XDR).
- **Zentrale Protokollierung:** Tools für das Sicherheitsinformations- und Ereignis-Management (SIEM), Syslog-Server und Cloud-basierte Datenspeicherung.
- **Authentifizierung:** Multi-Faktor-Authentifizierungsdienste und Identitäts- und Zugriffsverwaltungsdienste (IAM).
- **Threat Intelligence:** Taktische Beobachtungsdaten zur Korrelation und Überwachung verdeutlichen externe Risiken.

### Überwachungs-Tools und -Methoden

Mit den richtigen Überwachungs-Tools und -Methoden können Vorfälle zuverlässig identifiziert und Reaktionen angemessen koordiniert werden. Die folgenden Ansätze sind möglich:

- **Kontinuierliche Überwachung:** Eine Kombination aus Echtzeit- und periodischer Überwachung, um einen umfassenden Überblick über Ihre Umgebung zu erhalten.
- **Erkennung von Anomalien:** Fortschrittliche Analysen und maschinelles Lernen erkennen ungewöhnliche Verhaltensmuster, die auf eine potenzielle Bedrohung hinweisen.
- **Korrelation von Protokolldaten:** Aggregieren und Korrelieren der Protokolldaten aus verschiedenen Quellen, um Muster und Trends zu erkennen, die auf einen Angriff hindeuten können.
- **Priorisierung von Warnhinweisen:** Ein Prozess zur Priorisierung von Warnhinweisen auf Basis von Faktoren wie Schweregrad, mögliche Auswirkungen und Bedrohungsstufe.

Indem Sie sich auf Ihre Umgebung konzentrieren, robuste Schutzebenen zur Erkennung und Abwehr von Vorfällen implementieren und effektive Überwachungs-Tools und -Methoden einsetzen, sind Sie besser in der Lage, Sicherheitsvorfälle zu erkennen und auf diese rechtzeitig und effizient zu reagieren.

## Kommunikation

Bei der Reaktion auf einen Vorfall ist eine effektive Kommunikation entscheidend, da sie eine rechtzeitige Koordination und Zusammenarbeit zwischen allen Beteiligten ermöglicht. In diesem Abschnitt erfahren Sie, welche zentralen Punkte bei der internen und externen Kommunikation eines Vorfalls unter Einhaltung der rechtlichen Anforderungen zu berücksichtigen sind.

### Interne Kommunikation

- **Kommunikationsplan:** Erstellen Sie einen umfassenden Kommunikationsplan, in dem die Eskalationswege, Kommunikationskanäle und wichtigsten Kontaktpersonen aufgeführt sind. Dieser Plan sollte regelmäßig überprüft und aktualisiert werden, sodass er bei einem Vorfall zielgerichtet umgesetzt werden kann.
- **Incident-Response-Team:** Stellen Sie ein Incident-Response-Team (ITR) zusammen und benennen Sie einen Teamleiter, der für die Koordinierung der Maßnahmen verantwortlich ist. Die Rollen und Verantwortlichkeiten müssen für alle Teammitglieder nachvollziehbar sein. Sorgen Sie für eine reibungslose Kommunikation während des gesamten Vorfalls.
- **Sichere Kanäle:** Nutzen Sie sichere, zuverlässige Kommunikationskanäle, um einen unbefugten Zugriff auf sensible Informationen zu verhindern. Ziehen Sie Anwendungen für verschlüsseltes Messaging, sichere E-Mails oder spezielle Kommunikationsplattformen in Betracht.
- **Reaktionsvorlagen:** Erstellen Sie eine Bibliothek mit Incident-Response-Vorlagen für verschiedene Szenarien, um schneller und einheitlicher kommunizieren zu können. Diese Vorlagen sollten leicht zugänglich und einfach anzupassen sein und mit den Kommunikationsrichtlinien des Unternehmens übereinstimmen.
- **Updates an die Beteiligten:** Informieren Sie im Rahmen des Vorfallsmanagements alle Beteiligten über die aktuelle Situation, die ergriffenen Maßnahmen und die zu erwartenden Ergebnisse. Eine solche Transparenz trägt dazu bei, das Vertrauen darin zu stärken, dass das Unternehmen auf einen Vorfall angemessen und zuverlässig reagiert.

### Externe Kommunikation

- **Benachrichtigungsstrategie:** Entwickeln Sie eine Strategie zur Benachrichtigung von Kunden, Lieferanten, Partnern und Strafverfolgungsbehörden im Falle einer Sicherheitsverletzung oder anderen Vorfällen, die externe Beteiligte betreffen könnten. In dieser Strategie sollten die Meldekriterien, die geeigneten Kanäle und die für die Kommunikation verantwortlichen Personen festgelegt werden.
- **Einhaltung von Richtlinien und Vorschriften:** Die externe Kommunikation muss den rechtlichen und regulatorischen Richtlinien entsprechen, wie Datenschutzgesetze, Leitlinien zur verantwortungsvollen Offenlegung und branchenspezifische Vorschriften. Wenden Sie sich an Ihren Rechtsbeistand, um sicherzustellen, dass die Kommunikation allen relevanten Vorschriften entspricht.
- **Zuständige/r Sprecher/in:** Ernennen Sie eine/n Sprecher/in oder ein Team für die Öffentlichkeitsarbeit, das für Medienanfragen und öffentliche Stellungnahmen verantwortlich ist und sicherstellt, dass Ihre Botschaft korrekt und einheitlich vermittelt wird. Diese Ansprechpartner müssen in der Krisenkommunikation und Medienarbeit geschult sein.
- **Vorbereitungen für die externe Kommunikation:** Erstellen Sie Kommunikationsvorlagen für verschiedene Vorfallszenarien, um externe Parteien schnell und klar zu informieren. Diese Vorlagen müssen an die spezifischen Bedürfnisse verschiedener Interessengruppen, wie Kunden, Partner und Regulierungsbehörden, angepasst sein.
- **Zusammenarbeit mit anderen Abteilungen:** Arbeiten Sie eng mit der Rechts-, PR- und anderen relevanten Abteilungen zusammen, um sicherzustellen, dass die externe Kommunikation mit den Vorschriften übereinstimmt, der Ruf des Unternehmens geschützt wird und gegenüber den betroffenen Parteien transparent kommuniziert wird.

Durch Implementierung solcher Kommunikationsstrategien kann Ihr Unternehmen koordiniert auf Cybersicherheitsvorfälle reagieren und das Vertrauen in den korrekten Umgang Ihres Unternehmens mit solchen Vorfällen stärken.

## Bewusstsein für Cybersicherheit fördern und schulen

Die Mitarbeiter zu Cybersicherheit, Bedrohungen und Verhaltensweisen zu schulen, ist entscheidend für den allgemeinen Sicherheitsstatus des Unternehmens. In diesem Abschnitt wird dargelegt, welche Komponenten ein solches umfassendes Programm zur Sensibilisierung für Sicherheitsfragen und zur Schulung enthalten sollte, wie Security-Awareness-Trainings, Trainingsinhalte und -häufigkeit sowie Simulation von Vorfällen und Übungen.

### Security-Awareness-Programme

- **Programmziele:** Definieren Sie klare Ziele für Ihr Security-Awareness-Programm. Konzentrieren Sie sich darauf, die Kenntnisse der Mitarbeiter zu erweitern und ihre Verhaltensweisen auf den Schutz von Assets und Informationen des Unternehmens auszurichten.
- **Zielgerichtetes Training:** Entwickeln Sie maßgeschneiderte Trainingsmaterialien für die verschiedenen Rollen und Abteilungen innerhalb Ihres Unternehmens und berücksichtigen Sie dabei die jeweiligen Verantwortlichkeiten und den Zugang zu sensiblen Informationen.
- **Kontinuierliche Aktualisierungen:** Aktualisieren Sie Ihr Security-Awareness-Programm regelmäßig, um der sich verändernden Bedrohungslandschaft Rechnung zu tragen und die neuesten Entwicklungen und bewährten Verfahren einzubinden.
- **Kennzahlen und Auswertung:** Die Effektivität des Security-Awareness-Programms sollte anhand von Leistungsindikatoren (KPIs), wie Mitarbeiterengagement, Abschlussquote der Trainings und Verbesserung des Verhaltens in Sicherheitsfragen, gemessen und nachverfolgt werden.

### Trainingsinhalte und -häufigkeit

- **Entwicklung der Inhalte:** Erstellen Sie ansprechende und informative Trainingsinhalte, die ein breites Spektrum an Themen abdecken, zum Beispiel Passwortverwaltung, Phishing, Social Engineering und sicheres Surfen im Internet.
- **Durchführung der Trainings:** Bieten Sie verschiedene Trainingsformate an, wie zum Beispiel Online-Kurse, Präsenz-Workshops und interaktive Webinare, um den unterschiedlichen Präferenzen und Zeitplänen gerecht zu werden.

- **Häufigkeit:** Planen Sie das gesamte Jahr über Zeit für Trainings ein. Empfohlen wird mindestens einmal pro Quartal. Bieten Sie zeitnah zusätzliche Trainings an, wenn bestimmte Vorfälle eingetreten sind oder neue Bedrohungen aufkommen.
- **Kontinuierliche Fortbildung:** Fördern Sie eine Kultur der kontinuierlichen Fortbildung, indem Sie Ihren Mitarbeitern Zugang zu weiterführenden Ressourcen wie Artikeln, Videos und Podcasts ermöglichen, mit denen sie ihr Wissen über Cybersicherheit erweitern können.

### Simulation von Vorfällen und Übungen

- **Realistische Szenarien:** Entwickeln Sie eine Simulation von Vorfällen und Übungen auf Basis realistischer Szenarien, wie sie bei der täglichen Arbeit Ihrer Mitarbeiter auftreten können. Solche Szenarien können Ihren Mitarbeitern helfen, die möglichen Auswirkungen einer Sicherheitsverletzung besser nachzuvollziehen und Reaktionsmuster zu üben.
- **Funktionsübergreifende Zusammenarbeit:** Binden Sie mehrere Abteilungen in die Simulation ein und fördern Sie die Zusammenarbeit und Kommunikation zwischen den Teams aus unterschiedlichen Fachbereichen.
- **Auswertung und Feedback:** Führen Sie eine sorgfältige Auswertung der Leistung Ihrer Mitarbeiter bei den simulierten Vorfällen und Übungen durch, geben Sie konstruktives Feedback und identifizieren Sie Bereiche mit Verbesserungspotenzial.
- **Gewonnene Erkenntnisse:** Teilen Sie die aus den Simulationsübungen gewonnenen Erkenntnisse mit dem gesamten Unternehmen, um auf die wichtigsten Konzepte und bewährten Verfahren hinzuweisen.

Durch die Einführung eines effektiven Cybersecurity-Awareness-Programms können Unternehmen ihren Mitarbeitern die erforderlichen Kenntnisse und Kompetenzen vermitteln, um Bedrohungen zu erkennen und auf diese zu reagieren. Diese Maßnahme ist eine weitere wichtige Komponente bei der erfolgreichen Abwehr von Cyberangriffen.

## Incident-Response-Team

Ein eigens ernanntes Incident-Response-Team ist wichtig, um rechtzeitig und koordiniert auf Cybersicherheitsvorfälle reagieren zu können. In diesem Abschnitt erläutern wir die Rollen und Verantwortlichkeiten, die Zusammensetzung des Teams und die Bedeutung von Support und Expertenwissen von Dritten bei der Reaktion auf Vorfälle.

### Rollen und Verantwortlichkeiten

- **Incident Response Manager:** Überwachen den Incident-Response-Prozess, koordinieren die Aktivitäten des Teams und sorgen für eine effektive Kommunikation zwischen den Teammitgliedern und mit externen Beteiligten.
- **Sicherheitsanalysten:** Untersuchen und analysieren Sicherheitsvorfälle und bieten technische Expertise, um die Ursachen, den Umfang und die Auswirkungen des Vorfalls zu ermitteln.
- **Forensische Analysten:** Führen Aufgaben der digitalen Forensik durch, einschließlich Erfassung, Analyse und Sicherung von Beweisen, um diese bei weiterführenden Untersuchungen und Rechtsverfahren zur Verfügung zu stellen.
- **IT Operations:** Hilft bei der Eindämmung, Bereinigung und Wiederherstellung. Dieser Bereich ist für die Systeminfrastruktur verantwortlich und implementiert die notwendigen Änderungen, um künftige Vorfälle zu verhindern.
- **Legal und Compliance:** Berät zu allen geltenden Vorschriften im Zusammenhang mit der Reaktion auf Vorfälle und gewährleistet eine ordnungsgemäße Offenlegung und Berichterstattung.
- **Öffentlichkeitsarbeit und Kommunikation:** Steuert die interne und externe Kommunikation und erstellt Meldungen an die betroffenen Parteien, wie Mitarbeiter, Kunden, Partner und Aufsichtsbehörden.

## Zusammensetzung des Incident-Response-Teams

- **Funktionsübergreifende Vertreter/innen:** Stellen Sie ein multidisziplinäres Team zusammen, in dem verschiedene Abteilungen vertreten sind, darunter IT, Sicherheit, Recht, Personal und Kommunikation, um den vielfältigen Anforderungen bei der Reaktion auf Vorfälle Rechnung zu tragen.
- **Fähigkeiten und Kenntnisse:** Stellen Sie sicher, dass die Teammitglieder über das erforderliche Fachwissen verfügen, um die ihnen zugewiesenen Aufgaben zu erfüllen, und bieten Sie ihnen fortlaufende Schulungs- und Entwicklungsmöglichkeiten.
- **Verfügbarkeit und Rotation:** Das Team muss rund um die Uhr erreichbar sein. Nutzen Sie hierfür ein entsprechendes Schichtsystem.

## Support und Expertise von Dritten

- **Drittanbieter:** Engagieren Sie externe Experten, wie Cybersecurity-Berater oder Managed Security Service Provider (MSSP), um Ihre internen Kompetenzen zu ergänzen und Spezialwissen in Bereichen wie digitale Forensik oder Threat Intelligence bereitzustellen.
- **Rechtsbeistand:** Beauftragen Sie einen externen Rechtsbeistand mit Fachgebiet Cybersicherheit und Datenschutz, der Sie bei der Einhaltung der Vorschriften und Offenlegungspflichten berät und das Unternehmen bei allen Rechtsangelegenheiten im Zusammenhang mit einem Sicherheitsvorfall vertritt.
- **Strafverfolgungs- und Aufsichtsbehörden:** Knüpfen Sie Beziehungen zu den zuständigen Strafverfolgungs- und Aufsichtsbehörden, um die Zusammenarbeit und den Informationsaustausch bei etwaigen Untersuchungen von Vorfällen zu erleichtern.
- **Branchenweite Zusammenarbeit:** Nehmen Sie an branchenspezifischen Veranstaltungen und Expertengruppen zu Cybersicherheit teil und tauschen Sie Bedrohungsdaten sowie bewährte Praktiken mit anderen Unternehmen aus, um über neue Bedrohungen und Trends stets auf dem neuesten Stand zu bleiben.

Unternehmen, die über ein komplementäres Incident-Response-Team verfügen und auf externe Unterstützung und Expertise zurückgreifen, können Cybersicherheitsvorfälle besser bewältigen und mögliche Auswirkungen minimieren.

# Identification (Identifizierung)

Die Phase der Identifizierung ist entscheidend, um einen Angriff in einem Netzwerk oder System zu erkennen. Die kontinuierliche Überwachung der Telemetriedaten ist essenziell, um die Zeit zwischen Eindringen und Erkennen einer Bedrohung zu minimieren. Je schneller das Team reagiert, desto geringer sind die Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Systemen und Netzwerken. Lösungen für Managed Detection and Response (MDR) können bei diesem Prozess wertvolle Dienste leisten, da sie eine professionelle Erkennung von Bedrohungen und angemessene Reaktion darauf bieten.

## Zentrale Komponenten der Identifizierung

- **Netzwerk- und Geräte-Telemetrie:** Die umfassende Überwachung verschiedener potenzieller Quellen von Bedrohungen, wie sie im Abschnitt Telemetrie vorgestellt wird, ist für die Erkennung von Bedrohungen in Echtzeit und die Reaktion darauf unerlässlich. Die Implementierung einer MDR-Lösung kann die Effektivität der Maßnahmen verstärken.
- **Informationen von externen Partnern:** Die Zusammenarbeit mit Strafverfolgungsbehörden und anderen externen Partnern bei der Erfassung und Analyse von Bedrohungsdaten ermöglicht eine schnellere Identifizierung potenzieller Eindringlinge.
- **Threat Intelligence:** Die Überwachung von Dark-Web- und Untergrund-Websites hinsichtlich potenziell kompromittierter Unternehmensdaten, die zum Verkauf angeboten werden, unterstützt den Identifizierungsprozess.
- **Benutzermeldungen:** Die Benutzer sollten dazu ermutigt werden, verdächtige E-Mails oder Links zu melden und schnell auf diese potenziellen Bedrohungen zu reagieren, damit wichtige Informationen zuverlässig an die zuständigen Personen weitergeleitet werden.

Führen Sie robuste Verfahren zur Kategorisierung des Schweregrads eines Vorfalls anhand der folgenden Kriterien ein:

- **Vertrauenswürdigkeit:** Bezieht sich auf die Vertrauenswürdigkeit der Quelle (z. B. IPS, FW, AV, XDR).
- **Kritikalität:** Die Bedeutung des betroffenen Systems.
- **Schadenspotenzial:** Bewertet verdächtiges Verhalten und kann Hinweise auf eine möglicherweise unbekannte Sicherheitsverletzung liefern.
- **Vorfallstyp:** Klassifizierung von Vorfällen gemäß Rahmenwerken wie Cyber Kill Chain und MITRE ATT&CK.
- **Zeitstempel:** Einheitliche Zeitstempel unter Verwendung von UTC, NTP und gemeinsamen Standards zur Normierung der Daten.

## Vorfallstypen

Das NIST (National Institute of Standards and Technology Cybersecurity Framework) definiert zwei Kategorien von Vorfällen:

- **Vorläufer:** Erkennung von Anzeichen des Ausspionierens, wie z. B. Scan-Aktivitäten, die darauf abzielen, offene Ports und Softwareschwachstellen zu identifizieren. MDR-Lösungen können in diesem Zusammenhang besonders hilfreich sein. Erkennung von bekannten Remote-Code-Schwachstellen in der Infrastruktur des Unternehmens.
- **Indikator:** Identifizierung verschiedener Vorfälle des Typs Indikator, wie z. B. Malware-Warnungen, Änderungen an Dateien oder am Active Directory, ungewöhnliches Benutzerverhalten, wie z. B. Anmeldungen über einen RDP zu ungewöhnlichen Zeiten, inklusive Einleitung angemessener Reaktionsmaßnahmen. MDR bietet zusätzliche Unterstützung bei der Erkennung und Reaktion auf solche Vorfälle.

Unternehmen können ihren allgemeinen Sicherheitsstatus verbessern, indem sie eine umfassende Überwachungsstrategie implementieren und dabei Informationen externer Partner, Bedrohungsdaten, Benutzerberichte und klar definierte Kriterien für die Kategorisierung von Vorfällen einbeziehen. Des Weiteren bietet die Einbindung von MDR-Lösungen zusätzliche Unterstützung für die Erkennung und Reaktion auf solche Vorfälle. Eine starke Performance in der Identifizierungsphase reduziert nicht nur die Auswirkungen von Sicherheitsvorfällen, sondern fördert auch eine proaktive Sicherheitskultur innerhalb des Unternehmens, was letztendlich für Geschäftskontinuität sorgt und wertvolle Assets schützt.

## Potenziell verdächtige Dateien, Verzeichnisse, Prozesse und Persistenz

Potenziell verdächtige Dateien, Verzeichnisse, Prozesse und Persistenzmechanismen zu verstehen und zu identifizieren ist wichtig, um Vorfälle früh zu erkennen.

- **Dateien und Verzeichnisse:** Ungewöhnliche oder unerwartete Dateien und Verzeichnisse können auf einen Sicherheitsvorfall hinweisen. Beispiele:
  - Dateien mit ungewöhnlichen Erweiterungen oder Namen
  - Dateien an unerwarteten Orten
  - Verzeichnisse mit sensiblen Daten, die nicht zugänglich sein sollten
- **Prozesse:** Verdächtige Prozesse können ein Zeichen für schädliche Aktivitäten in einem System sein. Beispiele:
  - Prozesse mit hoher CPU- oder Speichernutzung
  - Prozesse, die von unerwarteten Orten ausgeführt werden
  - Prozesse, die versuchen, auf sensible Daten oder Ressourcen zuzugreifen
- **Persistenz:** Angreifer nutzen oft Persistenzmechanismen, um den Zugriff auf ein kompromittiertes System aufrechtzuerhalten. Beispiele für Persistenztechniken sind:
  - Geplante Aufgaben oder Cron-Jobs, die schädliche Skripte ausführen
  - Malware, die sich nach Entfernung oder einem Neustart erneut selbst installiert
  - Registrierungsschlüssel oder Autostartelemente, die schädliche Prozesse starten
- **Zugriff auf Anmeldeinformationen:** Der unbefugte Zugriff auf Anmeldeinformationen kann zu einer weiteren Gefährdung von Systemen und sensiblen Daten führen. Beispiele:
  - Brute-Force-Angriffe auf Benutzerkonten
  - Phishing-Kampagnen, die auf die Anmeldeinformationen der Mitarbeiter abzielen
  - Credential Dumping von kompromittierten Systemen
- **Zusätzliche Einfallstore/Zugriffspunkte:** Dabei versuchen die Angreifer, sich über zusätzliche Einfallstore in der Umgebung des Unternehmens einen erweiterten Zugriff und mehr Kontrolle zu schaffen. Beispiele:
  - Kompromittierte Benutzerkonten mit erweiterten Berechtigungen
  - Ausnutzung von ungepatchten Sicherheitslücken in Systemen oder Anwendungen
  - Laterale Bewegung innerhalb des Netzwerks, um auf zusätzliche Ressourcen zuzugreifen

Wenn Unternehmen diese Vorfallstypen erkennen, können sie potenzielle Bedrohungen effektiver identifizieren und entsprechend reagieren. Das Bewusstsein für diese verschiedenen Vorfallstypen ist entscheidend, um als Unternehmen Sicherheitsvorfälle rechtzeitig erkennen und die Auswirkungen schnell eindämmen zu können.

## Forensische Analyse

Forensische Analysen sind ein wichtiger Aspekt der Incident Response, da sie Unternehmen helfen, die Ursache eines Vorfalls zu ermitteln, seine Auswirkungen nachzuvollziehen und Beweise für weiterführende Untersuchungen oder rechtliche Schritte zu sammeln. Im Folgenden sind einige wichtige Elemente der forensischen Analyse aufgeführt:

### Forensische Tools und Methoden

Mithilfe verschiedener forensischer Tools und Methoden kann die Analyse von Systemen und Netzwerken während einer Reaktion auf einen Vorfall unterstützt werden. Diese Tools unterstützen die IT-Teams bei der Erfassung, Analyse und Speicherung von Daten. Beispiele für forensische Tools und Methoden sind:

- Disk-Imaging- und Klon-Programme, um den Status des kompromittierten Systems abzubilden
- Tools zur Speicheranalyse, um flüchtige Daten zu untersuchen und schädliche Prozesse zu identifizieren
- Tools zur Analyse des Netzwerkverkehrs, um die Netzwerkaktivität zu untersuchen und potenzielle Anzeichen für eine Gefährdung zu erkennen
- Protokollanalyse-Tools zur Überprüfung von System- und Anwendungsprotokollen auf Anzeichen verdächtiger Aktivitäten

### Sammeln und Aufbewahren von Beweismitteln

Ein korrektes Vorgehen beim Sammeln und Aufbewahren von Beweismitteln ist für die forensische Analyse wichtig, da so die Datenintegrität und die Zulässigkeit der Mittel bei Rechtsverfahren gesichert wird. Zu den bewährten Verfahren für das Sammeln und Aufbewahren von Beweisen gehört:

- Jeden Schritt der Beweiserhebung dokumentieren, einschließlich aller verwendeten Werkzeuge und Techniken.
- Eine detaillierte Zeitleiste der Ereignisse im Zusammenhang mit dem Vorfall erstellen.
- Mit Writeblockern und anderen forensischen Tools verhindern, dass die Beweise während der Erhebung verändert werden.
- Die erfassten Daten in manipulationssicheren Containern oder auf verschlüsselten Speichermedien speichern.
- Alle erfassten Daten in einer sicheren und überwachten Umgebung speichern.

### Beweiskette

Eine sachgerechte Nachweisführung ist entscheidend, um für die Unversehrtheit der Beweiskette zu sorgen und ihre Zulässigkeit in Gerichtsverfahren zu bewahren. Mit Beweiskette ist die Dokumentation und Nachverfolgung von Beweisen sowie deren Handhabung, Speicherung und Übermittlung während der gesamten Untersuchung gemeint. Um eine sachgerechte Nachweisführung zu erbringen, müssen Unternehmen:

- Angaben zu den Personen, die für die Beweismittel zuständig sind, dokumentieren, wie Name, Funktion und Kontaktdaten.
- Datum, Uhrzeit und Ort der Übermittlung oder Handhabung von Beweisen aufzeichnen.
- Alle Aktivitäten im Zusammenhang mit den Beweismitteln aufzeichnen, wie Kopieren, Analysieren oder Speichern.
- Die Beweismittel müssen stets sicher aufbewahrt und transportiert werden, bei Bedarf mit manipulationssicheren Siegeln versehen oder auf verschlüsselten Speichermedien.

Wenn forensische Analysen in den Incident-Response-Prozess eingebunden werden, können Unternehmen wertvolle Einblicke in die Art und den Umfang der Sicherheitsvorfälle gewinnen und wichtige Beweise erfassen, um diese für weiterführende Untersuchungen oder Rechtsverfahren zu verwenden. Für eine gründliche und effektive Analyse ist es wichtig, die forensischen Tools, Techniken und Praktiken zu kennen und korrekt anzuwenden.

## Datenexfiltration

Bei der Datenexfiltration handelt es sich um die unbefugte Übermittlung von sensiblen Informationen oder Daten aus den Systemen oder dem Netzwerk eines Unternehmens an einen externen Ort, der normalerweise von einem Angreifer kontrolliert wird. Datenexfiltration zu erkennen und zu verhindern ist entscheidend, um die Auswirkungen einer Sicherheitsverletzung zu minimieren und Assets zu schützen. Um sich wirksam gegen Datenexfiltration zu schützen, sollten Unternehmen Folgendes beachten:

- **Überwachung und Warnmeldung:** Implementieren Sie ein umfassendes Überwachungssystem, das ungewöhnliche Datenübertragungen oder anormale Muster im Netzwerkverkehr erkennt, wie zum Beispiel die Übertragung größerer Dateien, Kommunikation mit verdächtigen IP-Adressen oder mehrfach fehlgeschlagene Anmeldeversuche. Richten Sie angemessene Warnmechanismen ein, um die zuständigen Mitarbeiter über mögliche Vorfälle der Datenexfiltration zu informieren.
- **Data-Loss-Prevention(DLP)-Lösungen:** DLP-Lösungen verhindern, dass sensible Daten an einen Ort außerhalb des Unternehmensnetzwerks übertragen werden. DLP-Lösungen können zudem helfen, unbefugte Übertragungen sensibler Daten anhand von Richtlinien und Regeln zu erkennen und zu blockieren.
- **Verschlüsselung:** Verschlüsseln Sie sensible Daten, unabhängig davon, ob sie gerade gespeichert oder übermittelt werden. So verringern Sie den Wert Ihrer Daten für Cyberkriminelle im Falle eines erfolgreichen Exfiltrationsversuchs.
- **Training und Bewusstseinsstärkung der Mitarbeiter:** Klären Sie Ihre Mitarbeiter über die Risiken der Datenexfiltration auf und heben Sie hervor, wie wichtig es ist, sich an die Sicherheitsrichtlinien zu halten und sensible Daten zum Beispiel nicht über ungesicherte Kanäle zu übertragen oder mit nicht berechtigten Personen zu teilen.

## Validierung und Priorisierung

Sobald ein potenzieller Sicherheitsvorfall identifiziert wird, muss dieser validiert und die Reaktionsmaßnahmen auf Grundlage des Schweregrads und der möglichen Auswirkungen auf das Unternehmen priorisiert werden. Die Validierung und Priorisierung umfasst folgende Schritte:

- **Validierung des Vorfalls:** Überprüfen Sie, ob es sich bei dem identifizierten Vorfall wirklich um einen Sicherheitsvorfall und um keinen Fehlalarm handelt. Analysieren Sie hierfür die verfügbaren Daten unter Bezugnahme bekannter Bedrohungsdaten und den Kontext des Ereignisses.
- **Priorisierung des Vorfalls:** Beurteilen Sie die möglichen Auswirkungen des Vorfalls auf die Assets, den Betriebsablauf und den Ruf des Unternehmens. Berücksichtigen Sie dabei Faktoren wie Typ der betroffenen Daten oder Systeme, Ausmaß der Kompromittierung und mögliche Folgen des Vorfalls.
- **Schweregrad:** Weisen Sie dem Vorfall einen Schweregrad auf Basis der Priorisierung zu. Der Schweregrad kann anhand einer vordefinierten Skala definiert werden (z. B. mit niedrig, mittel, hoch oder kritisch). Diese Einstufung unterstützt das Incident-Response-Team beim Ermitteln der geeigneten Ressourcen und der Dringlichkeit der Reaktionsmaßnahmen.
- **Reaktionsplan:** Auf Grundlage des Schweregrads und der Art des Vorfalls wählen Sie den geeigneten Reaktionsplan aus dem Incident-Response-Playbook für Ihr Unternehmen aus. In diesem Plan müssen die notwendigen Schritte zur Eindämmung, Untersuchung und Behebung des Vorfalls sowie alle erforderlichen Kommunikations- und Berichterstattungsverfahren aufgeführt sein.

Eine effektive Identifizierung, Validierung und Priorisierung von Sicherheitsvorfällen stellt sicher, dass Unternehmen ihre Ressourcen effizient nutzen und ihre Reaktionsmaßnahmen auf die kritischsten Vorfälle ausrichten, um die Auswirkungen auf das Unternehmen insgesamt zu minimieren.

# Containment (Eindämmung)

Das oberste Ziel der Eindämmung besteht darin, weitere Schäden zu verhindern. Hierzu werden Systeme isoliert, die als kompromittiert identifiziert wurden oder bei denen der Verdacht einer Kompromittierung besteht. Dieser Schritt hilft, die weitere Ausbreitung von Vorfällen, wie z. B. die Verbreitung von Malware oder die fortlaufende Datenexfiltration, zu verhindern. Zudem befindet sich das System vorübergehend in einem Zustand, in dem zusätzliche Beweise gesammelt werden können. Funktionierende Eindämmungsstrategien können sich als wertvoll für weitere Untersuchungen erweisen. Zu diesen Strategien gehören das Sammeln von Indikatoren für eine Kompromittierung (Indicators of Compromise, IOCs), deren Dokumentation und weitere Analyse.

## Kurzfristige Eindämmung

Bei der kurzfristigen Eindämmung werden Sofortmaßnahmen ergriffen, um die Auswirkungen eines Vorfalls umgehend zu begrenzen. Diese erfolgen daher in der Regel nach der Identifizierung des kompromittierten Computers. Beispiele für kurzfristige Eindämmungsmaßnahmen sind:

- **Host-basierte Isolierung:** Mithilfe der Funktionen von Sicherheitsplattformen, wie z. B. Sophos Intercept X Advanced, können kompromittierte Hosts isoliert werden, während für weitere Untersuchungen eine aktive Verbindung aufrechterhalten werden kann.
- **Blockieren von SHA256-Hashes:** Mit Sophos Intercept X Advanced können schädliche Dateien anhand ihrer SHA256-Hashes blockiert werden, was ihre Ausführung verhindert.
- **Isoliertes Netzwerk:** Ändern Sie die Routing-Richtlinien von Switch, Router oder Firewall, um zu verhindern, dass das Netzwerksegment, in dem sich der identifizierte Rechner befindet, mit anderen Rechnern kommuniziert und der Schaden sich verbreitet.
- **Manuelle Isolierung:** Trennen Sie das Netzwerk-Ethernetkabel oder deaktivieren Sie die WLAN-Netzwerkkarte des Geräts, sobald eine Kompromittierung festgestellt wird.
- **Konto zurücksetzen:** Setzen Sie alle Benutzerkonten zurück, die nachweislich oder mutmaßlich kompromittiert wurden.

## Langfristige Eindämmung

Bei der langfristigen Eindämmung wird die Ausbreitung eines Angriffs auf andere Rechner und Assets im Netzwerk verhindert, sobald die ersten Untersuchungen abgeschlossen sind. Beispiele für langfristige Eindämmungsmaßnahmen sind:

- Blockieren von Netzwerkverbindungen zu bedenklichen Websites und Command-and-Control(C2)-Servern, die im Rahmen der Untersuchung identifiziert wurden.
- Sperren von kompromittierten Domänenkonten, Zurücksetzen/Sperren von Passwörtern für Domänen/lokale Administratorkonten und Durchführen einer domänenweiten Passwortzurücksetzung, falls das volle Ausmaß des Vorfalls nicht festgestellt werden kann.
- Automatisches Isolieren von Geräten, sobald die Mindestanforderungen an den Sicherheitsstatus des Geräts nicht mehr erfüllt sind.
- Installieren von Sicherheitsprogrammen auf ungeschützten oder zurückgesetzten Rechnern, um für Transparenz und Schutz zu sorgen.

## Best Practices

Für eine effektive Eindämmung sollte Folgendes beachtet werden:

### DOs

- Das Gerät mithilfe einer der oben genannten Optionen isolieren.
- Alle getätigten Schritte dokumentieren inklusive der benötigten Zeit, der Aktion und der durchführenden Person.
- Die Incident-Response-Pläne und die Eindämmungsstrategie beachten, insbesondere wenn Sie rechtliche Schritte einleiten möchten. Exakte Kopien (forensic image) anfertigen und die Cyberversicherung einbeziehen.
- Bedrohungen nach Bedrohungsstufe kategorisieren und das Management benachrichtigen, wenn es sich um einen Vorfall mit hohem Schweregrad handelt.
- IOCs bestimmen, die für Untersuchungszwecke und als Beweismittel dienen.
- Je nach Schweregrad und möglichen Auswirkungen des Vorfalls mit den entsprechenden Stakeholdern, wie Management, Rechts- und Presseabteilung, kommunizieren.

- Während des Eindämmungsprozesses auf jegliche Anzeichen eines Gegenschlags oder einer Eskalation seitens der Angreifer achten, da diese versuchen könnten, weiteren Schaden zu verursachen, nachdem ihre Aktivitäten entdeckt wurden.
- Sicherstellen, dass die Eindämmungsmaßnahmen bei Bedarf rückgängig gemacht werden können, falls es sich um False Positives handelt oder es zu ungewollten Folgen kommt.
- Eine gründliche Analyse des Vorfalls durchführen, um die Grundursachen zu ermitteln und aus den Erfahrungen zu lernen, damit Ihre Sicherheitsvorkehrungen und Ihr Incident-Response-Prozess optimiert werden können.

## DON'Ts

- Den kompromittierten Rechner herunterfahren oder neu starten.
- Überstürzte Aktionen ohne Rücksprache mit dem Incident Manager gemäß Ihrem Incident-Response-Plan.
- Sofortige Installation einer Sicherungskopie, ohne die anfängliche Erfassung der IOC und der ersten Untersuchungen abzuwarten.
- Den Vorfall veröffentlichen oder sensible Informationen an Unbefugte weitergeben, da dies die Angreifer alarmieren und den Eindämmungsprozess möglicherweise gefährden könnte.
- Allein auf automatisierte Tools oder Prozesse für die Eindämmung vertrauen, ohne das Know-how und Urteilsvermögen von Cyberexperten für fundierte Entscheidungen einzubeziehen.
- Die potenziellen geschäftlichen Auswirkungen von Eindämmungsmaßnahmen wie Ausfallzeiten oder Funktionsverluste nicht berücksichtigen und diese Faktoren gegen die Risiken des Nichthandelns nicht abzuwägen.
- Ihren Incident-Response-Plan und Ihre Verfahren nicht auf Grundlage der aus dem Eindämmungsprozess gewonnenen Erkenntnisse zu aktualisieren, um besser auf künftige Vorfälle vorbereitet zu sein.

Bedenken Sie, dass eine Einheitslösung nicht sinnvoll ist und dass bei den ergriffenen Maßnahmen der Vorfallstyp, die Netzwerklandschaft und die Zugänglichkeit des Netzwerks berücksichtigt werden müssen. Obwohl die Eindämmung die unmittelbare Bedrohung stoppt und dabei Raum für weitere Maßnahmen lässt, ist sie meist nicht der letzte Schritt bei der Bewältigung eines Vorfalls. Unternehmen sollten das Risiko, das von einem Cybersicherheitsvorfall ausgeht, stets im Auge behalten, da Angriffe eskalieren können, wenn die Angreifer merken, dass sie entdeckt wurden.

# Eradication (Bereinigung)

Bei der Bereinigung wird die Bedrohung bzw. der Angreifer vollständig aus der Umgebung beseitigt. Dieser Prozess umfasst oft mehrere Stufen. Ziel ist es, alle Aktivitäten von Angreifern, Systemänderungen, Malware und unbefugte Ausführungen im Netzwerk und auf den Rechnern zu identifizieren, zu dokumentieren und zu beseitigen. Da die meisten schwerwiegenden Cyberangriffe mehrere Einfallstore haben und Angreifer manuell eingreifen, ist es wichtig, auch jene Unregelmäßigkeiten zu erkennen, die von Scans möglicherweise nicht entdeckt werden. Bei der Bereinigung einer Bedrohung ist es zudem wichtig, alle potenziellen Folgewirkungen zu berücksichtigen.

Dabei gibt zwei Hauptstrategien: das erneute Aufsetzen oder Reimaging von Rechnern und die gezielte Entfernung. Beide haben ihre Stärken und Schwächen. Sie werden oft in Kombination durchgeführt, um maximale Wirksamkeit zu erzielen.

## Erneutes Aufsetzen oder Reimaging von Rechnern

Ein erneutes Aufsetzen oder Reimaging der Hosts mit einem vollständigen Rollback auf einen nicht kompromittierten Zustand ist am sinnvollsten, um kompromittierte Assets zuverlässig zu bereinigen. Für diesen Prozess empfiehlt es sich, auf den Hosts Standard-Software-Images einzusetzen und für die Wiederherstellung Zugriff auf das Master-Image zu haben. Das Master-Image sollte vor der Produktivschaltung erstellt werden. So ist sichergestellt, dass keine Kompromittierung vorliegt.

Bei kritischen Servern wie ERP-Systemen, Mail-Servern und Dateiservern ist die Wiederherstellung von einem alten Master-Image wegen des möglichen Datenverlusts und der damit verbundenen Kosten unüblich. Stattdessen können Unternehmen ihre Systeme von einer sauberen Sicherungsdatei (z. B. auf einem Backup-Server, Tape, in der Cloud oder auf einem Wechselmedium) wiederherstellen. Für diesen Prozess ist es erforderlich, die Verfügbarkeit und Integrität der Backup-Dateien zu überprüfen und den Zustand vor der Infektion wiederherzustellen. Um ihre Wiederherstellungs- und Reimage-Strategie möglichst effektiv umzusetzen, müssen Unternehmen das gesamte Netzwerk auf IOCs sowie Taktiken, Techniken und Prozesse (TTPs) der Cyberkriminellen prüfen und dabei besonders auf anfällige Rechner achten.

## Gezielte Entfernung

Bei der gezielten Entfernung werden sämtliche Malware und Artefakte identifiziert und die schwerwiegendsten vom Angreifer vorgenommenen Systemänderungen ermittelt, um diese zu entfernen oder die Systeme auf den Status vor der Kompromittierung zurückzuversetzen. Dieser Ansatz muss für Geräte, Produktionssysteme, Industrie-Kontrollsysteme oder andere kritische Geschäftsfunktionen verfolgt werden, bei denen ein Datenverlust oder eine Ausfallzeit besonders schwerwiegend wäre.

Dabei kommt oft eine Kombination aus Tools und geschulten Incident Respondern zum Einsatz, die auf Grundlage der zu Beginn beobachteten IOCs, der damit verbundenen Threat Intelligence und ihrer Erfahrung mit schädlichen TTPs nach Bedrohungen suchen. Die aus der gezielten Entfernung gewonnenen Erkenntnisse können genutzt werden, um einen tieferen Einblick in die Angriffsmethode zu erhalten und daraus langfristige Verbesserungsmaßnahmen abzuleiten, die das Risiko künftiger Cyberangriffe reduzieren.

Wenn ein Angreifer einen Host zum Beispiel über bestehende Schwachstellen, Fehlkonfigurationen oder eine frühere, schlafende Kompromittierung erfolgreich attackiert, müssen bei der Bereinigung auch diese Schwachstellen behoben werden, um zu verhindern, dass der Host zu einem Vektor für eine erneute Infektion oder einen neuen Angriff wird. Anhand einer Ursachenanalyse können Unternehmen ermitteln, welche Schritte die Angreifer bis zum Zeitpunkt der Erkennung unternommen haben. Das hilft, die Erstinfektion zu finden und künftige Angriffe zu verhindern.

Es wird empfohlen, dass Unternehmen ihre Erkenntnisse fortlaufend dokumentieren und Rahmenwerke wie das MITRE ATT&CK Framework nutzen, um die Vorgehensweise der Angreifer nachzuvollziehen. Dieser strukturierte Ansatz trägt dazu bei, die Ursache eines Vorfalls zu ermitteln und den allgemeinen Sicherheitsstatus zu optimieren.

# Recovery (Wiederherstellung)

Das Ziel der Wiederherstellungsphase ist die schrittweise Rückführung betroffener Geräte und Systeme zu einem normalen Geschäftsbetrieb. Dabei wird die volle Funktionsfähigkeit wie vor dem Angriff wiederhergestellt. Die Wiederherstellungsstrategie richtet sich nach der Art des Vorfalls. Bei manchen Vorfällen ist nur die Isolierung einiger weniger Rechner mit minimalen Auswirkungen auf den Betrieb notwendig. Bei größeren Angriffen, wie Ransomware, sind oft mehrere Rechner betroffen, was wiederum erhebliche betriebliche Folgen und Ausfallzeiten nach sich ziehen kann. Darum sollten sich die Wiederherstellungspläne nach der Art der Angriffe richten.

- Wenn ein einzelner Host von einer Phishing-E-Mail betroffen ist und dies vom Endpoint-Schutz entdeckt und bereinigt wurde, kann eine Isolierung des Rechners sinnvoll sein, um ihn von Sicherheitsanalysten untersuchen und bereinigen zu lassen – bei minimalen Auswirkungen auf den Gesamtbetrieb.
- Bei einer frühzeitigen Entdeckung eines Botnet im Netzwerk, der zwei Rechner mit installierten Persistenzmechanismen betrifft, können diese sofort isoliert und neu aufgesetzt werden, was zwar zu Ausfallzeiten der betroffenen Mitarbeiter führen kann, aber nur minimale betriebliche Auswirkungen hat.
- Im Fall eines netzwerkweiten Ransomware-Angriffs über mehrere Wochen mit identifizierter Ursache ist es möglich, dass nicht nur die Endpoints und Server isoliert werden, sondern auch E-Mails, VPNs, Active Directory-Konten und andere Dienste. Des Weiteren sollten in diesem Fall so lange Maßnahmen zur Eindämmung ergriffen werden, bis der Angriff unter Kontrolle ist. Hierzu müssen die Einfallstore identifiziert, Patches eingespielt und die Rechner neu aufgesetzt werden. Auch die Erstellung eines alternativen „sauberen" Netzwerks, der Wiederaufbau des Netzwerks ohne die betroffenen Rechner und die schrittweise Wiedereingliederung der Rechner nacheinander können Teil der Strategie sein. Die Wiedereingliederung von zuvor isolierten Rechnern sollte erst nach Abwägung des Risikos eines erneuten Eindringens oder einer erneuten Infektion erfolgen und nachdem dieses Risiko der Geschäftsleitung mitgeteilt wurde, um einen angemessenen und risikobasierten Zeitplan und Ansatz zu ermöglichen.

## Ein umsichtiger Ansatz

Bei der Wiederherstellung von Rechnern müssen alle kritischen systembezogenen Einzelheiten sorgfältig betrachtet werden. Denn ein zu großes Vertrauen in die Beseitigung der Bedrohung und Ermüdung aufgrund der intensiven Bearbeitung des Vorfalls können sich nachteilig auswirken. Es ist wichtig, wachsam zu bleiben und auf Folgendes zu achten:

- Gesamtstatus eines betroffenen Rechners bei der Wiedereingliederung in das Netzwerk durch Prüfen der Datenintegrität und Systemstabilität.
- Patches für Sicherheitslücken, insbesondere nach der Wiederherstellung eines Rechners auf eine frühere Version, die für einen erneuten Angriff anfällig sein könnte.
- Überprüfen der richtigen Anwendung von Sicherheitsrichtlinien und -kontrollen auf jedem Rechner:
  - Die Sicherheitsprogramme müssen auf allen Rechnern, die erneut eingegliedert werden, installiert sein.
  - Es dürfen nur minimale Scan-Ausschlüsse bestehen, mit Ausschlüssen und Anwendungen, die für die ausgeschlossenen Geräte, Rechner oder Benutzergruppen spezifisch sind.
- Suche nach identifizierten IOCs aus dem Angriff und jeglichen Einfallstoren, die der Bedrohungsakteur geschaffen haben könnte.

Außerdem müssen die Incident Responder und Sicherheitsanalysten die Umgebung weiterhin auf Bedrohungsaktivitäten überwachen und proaktiv nach typischen Aktivitäten von Bedrohungsakteuren suchen, um sich vorbeugend gegen Bedrohungen zu wehren und darauf zu reagieren, sobald sie auftreten.

Die Wiederherstellungsphase muss nicht zwingend auf die Bereinigungsphase folgen. Die Reihenfolge kann auch geändert werden, da Rechner, deren Sicherheitsstatus wiederhergestellt wurde, in die Produktivumgebung integriert werden können.

# Lessons Learned (Gewonnene Erkenntnisse)

Nach der erfolgreichen Wiederherstellung der Geräte und Systeme ist es wichtig, den Cybersicherheitsvorfall zu analysieren. Die Analyse gibt Aufschluss darüber, wie effektiv Ihre Incident Response ist und welche Bereiche optimiert werden müssten. Diese Erkenntnisse fließen anschließend in Ihren Incident-Response-Plan ein. Auf diese Weise ist Ihr Unternehmen besser auf künftige Vorfälle vorbereitet und das Risiko ähnlicher Sicherheitsverletzungen wird minimiert.

## Analyse nach dem Vorfall

### Wirksamkeit des Incident-Response-Plans analysieren

Überprüfen Sie die vom Incident-Response-Team ergriffenen Maßnahmen und messen deren Ergebnisse, um die Wirksamkeit Ihrer Reaktionsmaßnahmen bei einem Vorfall zu bewerten. Die folgenden Aspekte sind dabei zu berücksichtigen:

- Zeitspanne bis Vorfall erkannt, eingedämmt und behoben wurde
- Die Kommunikation und Abstimmung innerhalb des Teams und mit externen Stakeholdern (z. B. Strafverfolgungsbehörden, Lieferanten)
- Angemessenheit der Strategien zur Eindämmung, Bereinigung und Wiederherstellung
- Die Genauigkeit und Nützlichkeit der von den Überwachungs- und Erkennungstools gelieferten Informationen

### Bereiche mit Verbesserungspotenzial ermitteln

Nachdem Sie die Effektivität Ihrer Reaktionsmaßnahmen auf einen Vorfall analysiert haben, ermitteln Sie jene Bereiche, in denen Ihr Unternehmen seine Prozesse und Verfahren verbessern kann. Mögliche Bereiche wären:

- Programme zur Mitarbeiterschulung und Förderung des Sicherheitsbewusstseins
- Kapazitäten zur Erkennung und Überwachung von Vorfällen
- Aktualisierung des Incident-Response-Plans
- Technische Kontrollen und Sicherheitsmaßnahmen
- Rollen und Verantwortlichkeiten des Incident-Response-Teams
- Externe Kommunikation und Zusammenarbeit mit Stakeholdern

### Änderungen und Aktualisierungen des Incident-Response-Plans implementieren

Wenn Sie Bereiche mit Verbesserungspotenzial identifiziert haben, aktualisieren Sie Ihren Incident-Response-Plan entsprechend. Stellen Sie dabei Folgendes sicher:

- Aktualisieren Sie den Plan bei Bedarf mit neuen Verfahren, Richtlinien oder technischen Maßnahmen.
- Kommunizieren Sie die Änderungen an alle Beteiligten, wie Mitarbeiter, das Management und externe Stakeholder.
- Führen Sie regelmäßig Schulungen und Übungen durch, um sicherzustellen, dass der aktualisierte Plan nachvollziehbar ist und effektiv ausgeführt werden kann.
- Überwachen und bewerten Sie die Wirksamkeit der Änderungen und nehmen Sie bei Bedarf weitere Anpassungen vor.

Durch eine gründliche Überprüfung nach einem Vorfall und der daraus gewonnenen Erkenntnisse kann Ihr Unternehmen seine Cybersicherheit verbessern und sich besser auf künftige Vorfälle vorbereiten. Denken Sie daran, dass die Reaktion auf Vorfälle ein kontinuierlicher Prozess ist. Die regelmäßige Überprüfung und Aktualisierung Ihres Plans wird dazu beitragen, dass Ihr Unternehmen angesichts der sich stets weiter entwickelnden Cyberbedrohungen resilient bleibt.

## Gewonnene Erkenntnisse

Die gewonnenen Erkenntnisse hängen vom Vorfallstyp und dem Prozess ab, sie zeigen die zu optimierenden Bereiche auf. Erkenntnisse und Lehren aus dem Vorfall zu ziehen, wird als wichtiger Schritt des Prozesses oft übersehen, da der Alltag sofort wieder einkehrt, wenn der Ausnahmezustand vorbei ist. Darum ist es so wichtig, dass diese Phase direkt nach der Wiederherstellung stattfindet und auch die Geschäftsleitung eingebunden wird, damit der Vorfall sorgfältig untersucht und Verbesserungen vereinbart werden können, um künftige Risiken zu mindern.

Dies kann anhand eines schriftlichen Berichts über den Vorfall inklusive Kurzfassung erfolgen. Dieser sollte so formuliert sein, dass er auch von Stakeholdern ohne technisches Know-how verstanden wird. Dabei ist darauf zu achten, dass der Bericht kollaborativ erarbeitet wird, sodass mehrere Personen ihre Kommentare und Bearbeitungen einfügen können. Der Abschlussbericht sollte ein gemeinsames Fazit enthalten, einschließlich der technischen Details und der gewonnenen Erkenntnisse.

Angesichts des breiten Spektrums an Verbesserungsmöglichkeiten umfasst die folgende Liste nur eine Auswahl möglicher Bereiche.

### Empfohlene bewährte Sicherheitspraktiken:

- Veraltete Software, Anwendungen und Hardware innerhalb des Unternehmens stilllegen, um das Risiko einer Sicherheitslücke zu minimieren.
- Ein robustes Patch-Management für Software und Hardware einführen, das auf die Bedürfnisse des Unternehmens abgestimmt ist und regelmäßige Patch-Updates gewährleistet.
- Einen Cloud-basierten Endpoint-Schutz auf allen Computern innerhalb des Unternehmens installieren, um Bedrohungen zu erkennen und zu beseitigen.
- Multi-Faktor-Authentifizierung (MFA) für VPN, RDP und andere Services einführen, die eine Authentifizierung erfordern, um die Sicherheit zu erhöhen.
- Infrastruktur mittels zentraler Sicherheitskontrollmechanismen schützen, damit auf internetbasierte Dienste nicht unberechtigt zugegriffen werden kann.
- Berechtigungsmanagement stärker sichern, indem die Komplexitätsanforderungen erhöht, Passwortmanager verwendet und die Anmeldedaten regelmäßig geändert werden.
- E-Mail-Authentifizierungsprotokolle wie DMARC, DKIM und SPF zum Schutz vor Phishing-E-Mails und Spoofing implementieren.

### Netzwerkeinrichtung:

- Network Access Control (NAC) für eine zusätzliche Schutzebene einrichten, um sich gegen nicht autorisierte Geräte und Cyberbedrohungen zu schützen.
- Netzwerke mithilfe von VLANs voneinander trennen, damit kritische Systeme und sensible Daten geschützt sind. Internetbasierte Plattformen und Dienste in einer DMZ isolieren.

### Härtung:

- Geoblocking für Firewalls nutzen, um unerwünschten Netzwerkverkehr aufgrund seiner geografischen Herkunft zu verhindern.
- Lösungen zur Anwendungskontrolle wie AppLocker einsetzen, um zu verhindern, dass nicht autorisierte Anwendungen und Dateien im Unternehmen installiert oder ausgeführt werden.
- Domänencontroller härten, indem unnötige Dienste, nicht unterstützte Software und veraltete Protokolle, die ein Sicherheitsrisiko darstellen können, überprüft und entfernt werden.

### Proaktives Management und effektive Sicherheitsmaßnahmen:

- **Prüfung der Infrastruktur:** Die Port-Konfigurationen der gesamten internetbasierten Infrastruktur innerhalb des Unternehmens regelmäßig prüfen, damit nur erforderliche Protokolldienste zugelassen sind und die Ports für den Netzwerkfluss richtig konfiguriert sind.
  - Zum Beispiel: eth0 ist mit dem Internet verbunden und eth1 nur intern zu erreichen.
- **Web Control Auditing:** Regelmäßig die Konfiguration des Internetverkehrs auf Proxy-Servern und ähnlichen Plattformen für den Web-Datenverkehr prüfen. Sicherheitskontrollen, wo nötig, verschärfen und sich dabei an das Least-Privilege-Prinzip halten. Implementierung einer Verweigerungs- oder Blockierungsrichtlinie als Standard. Zum Beispiel:
  - Dateitypen blockieren, die ein unnötiges Risiko für das Unternehmen darstellen.
  - Die Standard-Kategorisierungsrichtlinien für nicht kategorisierte URLs und Domains prüfen.
  - Statistische Daten exportieren, um Anomalien, Muster oder wiederkehrende verdächtige und schädliche Ereignisse zu identifizieren.
  - Sicherstellen, dass Sicherheitsgruppen und -richtlinien im Einklang mit dem RBAC-Prinzip (rollenbasierte Zugriffskontrolle) aktualisiert werden.
- **Kontoprüfung:** Regelmäßig auf nicht standardmäßige und nicht genehmigte lokale Administratorkonten oder ähnliche Konten im Unternehmen prüfen und solche Konten entfernen.
- **Windows-Ereignisprotokolle:** Windows-Ereignisprotokolle so konfigurieren, dass die Daten archiviert werden, zum Beispiel indem Sie den Speicher für zentrale Windows-Ereignisprotokolle über die Gruppenrichtlinie erweitern oder neue Ereignisprotokolle erstellen, wenn die Größenbeschränkung erreicht ist. Windows-Ereignisprotokolle bieten wertvolle forensische Informationen.
- **Incident-Response-Plan:** Einen Plan für die Reaktion auf Cybersicherheitsvorfälle im Unternehmen entwickeln, implementieren, testen und pflegen. Den Plan regelmäßig überprüfen und testen, den Inhalt nach Bedarf aktualisieren und verfeinern.

- **Hardware- und Software-Asset-Management:** Ein Asset-Management für Hardware und Software im gesamten Unternehmen einrichten. Die Bewertung der Priorität/Kritikalität in die Asset-Management-Lösung integrieren, um wichtige Assets schnell zu identifizieren. Ein aktuelles Bestandsverzeichnis über Ihre Hardware und Software führen, um potenzielle Risiken zu erkennen und strategische Pläne zur Bewältigung dieser Risiken zu entwickeln.
- **Netzwerktopologie:** Ein aktuelles Diagramm der Netzwerktopologie des Unternehmens führen. Dieses soll als Referenz für die Überprüfung bestehender Konfigurationen und Infrastrukturtypen dienen und Unternehmen bei der Erstellung strategischer Pläne für Änderungen und Implementierungen im Netzwerk unterstützen. Während eines Cybersicherheitsangriffs kann ein solches Diagramm dabei helfen, die Struktur des Unternehmensnetzwerks schnell zu erfassen und gezielt und präzise zu reagieren.

## Datenintegrität

### Backups:

- Schützen Sie Ihre Sicherungsdateien, indem Sie verschiedene Backup-Lösungen nutzen, die Sicherungsdateien an vollständig voneinander getrennten Netzwerkstandorten oder auf Wechselmedien außerhalb der Unternehmensumgebung speichern und den Zugriff mit geeigneten Sicherheitskontrollen verwalten.
  - Konzipieren Sie eine Backup-Redundanzlösung anhand der 3-2-1-Regel und führen Sie während der Speicherung eine adäquate Verschlüsselung der Sicherungsdateien durch: Erstellen Sie 3 Kopien der Daten, speichern Sie die Daten auf mindestens 2 verschiedenen Medientypen, speichern Sie mindestens 1 Kopie der Daten außerhalb des Unternehmens (offsite).

### Verschlüsselung:

- Führen Sie eine vollständige Festplattenverschlüsselung auf Computern, mobilen Geräten und USB-Laufwerken durch, um die Daten bei Verlust oder Diebstahl des Geräts vor unbefugtem Zugriff zu schützen.
- Schützen Sie ruhende Daten (data at rest) durch Data At Rest Encryption (DARE), der Verschlüsselung von Daten, die auf einem physischen Speichermedium gespeichert sind. Dabei wird hochsensiblen Daten Priorität eingeräumt. Richten Sie adäquate Verschlüsselungsmechanismen für Netzwerkdaten bei deren Übertragung ein, z. B. durch Verwendung der aktuellsten TLS-Version (Transport Layer Security) für den verschlüsselten Kommunikationsaustausch mit digitaler Zertifizierung, und verhindern Sie, dass Server Cipher Suites herabstufen, um nicht unterstützte Browsertypen zu unterstützen.

## Investitionen in die Sicherheit

Setzen Sie sich mithilfe der aus früheren Sicherheitsvorfällen gewonnenen Erkenntnissen für eine bessere Finanzierung der Sicherheit des Unternehmens ein.

- Investieren Sie in Security-Awareness-Trainings Ihrer Mitarbeiter. Oft ist der Mensch selbst die Schwachstelle und Einfallstor für einen Angriff. Darum sollten Sie investieren in:
  - Phishing-Awareness-Trainings oder -Lösungen, um die Mitarbeiter über gängige Phishing-Techniken aufzuklären. Diese Trainings sind als fortlaufende Übung mit geplanten Trainingseinheiten oder automatisierten Angriffssimulationen in den Betriebsablauf zu integrieren. Anhand von Berichten kann das IT-Team anschließend prüfen, wer häufig Opfer wird, und zusätzliche Unterstützung bieten.
  - Weiterbildung der Mitarbeiter im Bereich IT-Sicherheit, insbesondere in den Bereichen Sicherheitsanalyse, Suche nach Bedrohungen und Reaktion auf Vorfälle.

### Managed Cybersecurity Services

- Stellen Sie Cybersicherheitsexperten ein, die auf die Sicherheitsanalyse, Suche nach Bedrohungen und Reaktion auf Vorfälle, Entwicklung von Sicherheitstools zur Erkennung von Bedrohungen usw. spezialisiert sind. Mit der Einrichtung eines Cybersecurity Operation Center können Unternehmen Bedrohungen überwachen und rund um die Uhr reagieren.
- Investieren Sie in eine Managed-Cybersecurity-Lösung wie Sophos Managed Detection and Response (MDR). MDR-Services sind Sicherheitsmaßnahmen, die von einem externen Spezialistenteam als Erweiterung des internen Sicherheitsteams des Kunden durchgeführt werden.

## Investitionen in Tools

- Sophos XDR – Extended Detection and Response – ist eine Lösung, die wichtige Informationen von Endpoints, Servern, Firewalls, E-Mails und anderen XDR-fähigen Produkten abfragt und speichert, und so Prozesse zur Erkennung und Abwehr von Bedrohungen optimiert.
- Die SIEM-Technologie (Security Information and Event Management) bietet Funktionen zur Erkennung von Bedrohungen, zur Einhaltung von Vorschriften und für das Vorfallsmanagement. Ereignisse und Informationen aus verschiedenen Datenquellen werden in einem zentralen Repository für Bedrohungsdaten gesammelt und gespeichert.
- Anhand der gewonnenen Erkenntnisse können zusätzliche Investitionen getätigt werden, die dazu betragen, die Sicherheitslage insgesamt zu verbessern. Dabei sollten Lücken beim Schutz oder der Filterung, der Erkennung und Überwachung geschlossen werden. Beispiele für solche Tools sind AV, Intrusion Prevention/Detection-Systeme (IPS/IDS), Firewalls usw.

Indem Sie diese typischen Bereiche mit Verbesserungsbedarf angehen, kann Ihr Unternehmen seinen Sicherheitsstatus bereits erheblich verbessern und sich gegen künftige Cybersicherheitsvorfälle besser schützen. Denken Sie daran, dass neue Erkenntnisse fortlaufend ermittelt werden müssen. Die regelmäßige Überprüfung und Aktualisierung Ihrer Sicherheitsverfahren stärkt die Resilienz Ihres Unternehmens angesichts der sich stets weiter entwickelnden Cyberbedrohungen.

# Vorfallsmeldung

Nach einem Cybersicherheitsvorfall ist es wichtig, alle Informationen, Ergebnisse und Bereinigungsmaßnahmen an die verschiedenen Stakeholder zu kommunizieren. Dazu gehört die interne Meldung des Vorfalls sowie die Meldung an die Aufsichts- und Strafverfolgungsbehörden, damit die Transparenz aufrechterhalten, Vorschriften eingehalten und eventuelle Ermittlungen unterstützt werden können.

## Interne Vorfallsmeldung

Zur Förderung einer Kultur der kontinuierlichen Optimierung und Kompetenzerweiterung sollten Unternehmen einen klaren Prozess für die interne Berichterstattung festlegen. Dieser Prozess sollte Folgendes umfassen:

- Dokumentation des Vorfalls mit zeitlichem Ablauf der Ereignisse, der betroffenen Systeme und des Angriffstyps.
- Zusammenfassung der Auswirkungen des Vorfalls auf den Betriebsablauf, die Finanzen und die Reputation des Unternehmens.
- Erläuterung, welche Schritte zur Eindämmung, Bereinigung und Wiederherstellung unternommen wurden.
- Darlegung der gewonnenen Erkenntnisse und Empfehlungen für künftige Verbesserungen des Sicherheitsstatus des Unternehmens.
- Verteilung des Vorfallsberichts an die relevanten Stakeholder, wie Geschäftsleitung, IT-Teams und betroffene Mitarbeiter oder Abteilungen.

## Meldung an Aufsichtsbehörden

Je nach Rechtsprechung und Branche sind Unternehmen möglicherweise verpflichtet, Cybersicherheitsvorfälle an Aufsichtsbehörden zu melden. Wer sich nicht an diese Vorschrift hält, muss mit Geldbußen, Strafen und Schädigung des Rufs des Unternehmens rechnen. Um den Vorfall den Aufsichtsbehörden zu melden, müssen Unternehmen:

- Ermitteln, welche zuständige(n) Behörde(n) zu benachrichtigen ist/sind, was vom Vorfallstyp, der Branche und dem Standort des Unternehmens abhängt.
- Die geltenden Meldeanforderungen, einschließlich der erforderlichen Informationen und des Zeitrahmens für die Meldung, prüfen.
- Einen detaillierten Meldebericht vorbereiten, der dem von der Aufsichtsbehörde vorgegebenen Format und Inhalt entspricht.
- Den Bericht innerhalb der vorgegebenen Frist einreichen und während des gesamten Untersuchungs- und Lösungsprozesses offen mit der Aufsichtsbehörde kommunizieren.

## Meldung an Strafverfolgungsbehörden

Handelt es sich um kriminelle Aktivitäten oder Cyberangriffe mit schwerwiegenden Auswirkungen, sollten Unternehmen in Erwägung ziehen, den Vorfall den Strafverfolgungsbehörden zu melden. Dies kann bei Ermittlungen helfen und möglicherweise dazu führen, dass die Angreifer gefasst werden. Um den Vorfall den Strafverfolgungsbehörden zu melden, müssen Unternehmen:

- Die zuständige(n) Strafverfolgungsbehörde(n) ermitteln, zum Beispiel die örtliche Polizei, spezielle Dienststellen zur Bekämpfung der Cyberkriminalität oder Behörden (zum Beispiel die Bundespolizei).
- Relevante Beweise sammeln, einschließlich Protokolle, System-Images und Aufzeichnungen des Netzwerkverkehrs. Dabei gilt es, Beweise für eine schlüssige Beweiskette zu sichern und alle geltenden rechtlichen Anforderungen einzuhalten.
- Einen detaillierten Bericht zum Vorfall erstellen, einschließlich Angriffstyp, betroffene Systeme und Daten, zeitlicher Ablauf der Ereignisse und alle bekannten Informationen über den/die Angreifer.
- Während der gesamten Ermittlungen mit den Strafverfolgungsbehörden kooperieren und bei Bedarf zusätzliche Informationen und Unterstützung bieten.

Wenn diese Punkte im Falle einer Vorfallsmeldung befolgt werden, ist sichergestellt, dass Unternehmen die erforderliche Transparenz aufrechterhalten, die gesetzlichen Anforderungen erfüllen und die allgemeinen Bemühungen zur Bekämpfung der Cyberkriminalität unterstützen.

## Fazit

Dieser Leitfaden bietet Unternehmen umfassende Informationen zur Ausarbeitung eines Incident-Response-Plans. Dieser ermöglicht es ihnen, sich effektiv auf Cybersicherheitsvorfälle vorzubereiten, angemessen auf Angriffe zu reagieren und sich wieder schnell davon zu erholen. Durch die Einführung eines proaktiven Managements und wirksamer Sicherheitsmaßnahmen, durch die Sicherstellung von Datenintegrität, Investitionen in Mitarbeiterschulungen und Sicherheitstools sowie Einrichtung klarer Reporting-Verfahren können Unternehmen ihre Resilienz gegenüber Cyberbedrohungen erheblich verbessern.

Eine effektive Incident-Response-Planung hilft Unternehmen nicht nur dabei, den durch Cyberangriffe verursachten Schaden zu minimieren, sondern fördert auch eine Kultur der kontinuierlichen Verbesserung und Kompentenzerweiterung. Da sich die Landschaft der Cyberbedrohungen ständig verändert, müssen Unternehmen ihre Incident-Response-Pläne zudem regelmäßig überprüfen und aktualisieren, damit sie neuen Bedrohungen immer einen Schritt voraus sind.

Die in diesem Leitfaden aufgeführten Hinweise unterstützen Sie dabei, Ihr Unternehmen besser auf Cybersicherheitsvorfälle vorzubereiten. So können Sie Bedrohungen besser erkennen, effektiv eindämmen und beseitigen, Ihre Daten und Assets wirksam schützen, die Einhaltung gesetzlicher Vorschriften sicherstellen und den Ruf Ihres Unternehmens in einer zunehmend vernetzten Welt besser schützen.

Für weitere Informationen zum Sophos Incident Response Service klicken Sie hier.

## Bei Ihnen findet gerade ein Angriff statt?

Kontaktieren Sie unsere Incident-Response-Experten über die untenstehende E-Mail-Adresse oder die Rufnummer für Ihre Region.

**E-Mail:** RapidResponse@Sophos.com

**Deutschland:** +49 611 711 867 66

**Österreich:** +43 732 655 755 20

**Schweiz:** +41 44 51 52 286

**Frankreich:** +33 186539880

**Italien:** +39 0294752897

**Niederlande:** +31 162708600

**Großbritannien und Nordirland:** +44 1235635329

**Schweden:** +46 858400610

**USA:** +1 4087461064

**Kanada:** +1 7785897255

**Australien:** +61 272084454



2023-08-23 (IRG-MP)

SOPHOS