Spezialisierte Institutionen im Kanton Freiburg Leitfaden für bewährte Verfahrensweisen zur Cybersicherheit

infri

Version Datum
30/01/2025

Kontakt:
immunIT sàrl
44-46 Chemin des Plantaz
1260 Nyon - Switzerland

Kontaktperson:
Alain Sullam
asullam@immunit.ch
+41 76 488 00 28

Inhaltsverzeichnis

Einführung

Ziele des Leitfadens

Dieser Leitfaden stellt den spezialisierten Institutionen des Kantons Freiburg eine Reihe von Empfehlungen und bewährten Verfahrensweisen im Bereich der Cybersicherheit zur Verfügung. Angesichts der sich ständig verändernden Bedrohungen und Risiken, die mit der Nutzung von Informationssystemen verbunden sind, ist es entscheidend, dass diese Institutionen robuste Sicherheitsmassnahmen ergreifen, die auf ihre spezifischen Bedürfnisse zugeschnitten sind. Der Leitfaden soll IT-Verantwortliche, Systemadministratoren, externe Dienstleister, sowie Führungskräfte bei der Entwicklung und Umsetzung einer kohärenten, effizienten und nachhaltigen Cybersicherheitsstrategie unterstützen.

Die Hauptziele dieses Leitfadens sind:

- Sensibilisierung der Institutionen für die Herausforderungen der Cybersicherheit.
- Bereitstellung von zweckvollen Richtlinien, die auf die Grösse und Komplexität der Infrastruktur zugeschnitten sind.
- Hilfe bei der Einführung von Schutzmassnahmen gegen aktuelle Cyberbedrohungen.
- Förderung einer Sicherheitskultur bei allen Mitarbeitende, von den Benutzern bis zu den technischen Teams.

Dieser Leitfaden für bewährte Verfahrensweisen soll auch den Abschluss eines umfassenden Projekts zur Cybersicherheit bilden, das bei den Sonderinstitutionen des Kantons Freiburg durchgeführt wurde. Im Rahmen dieses Projekts wurden Tätigkeiten wie die Sensibilisierung der Benutzer, eine Phishing-Kampagne, sowie individuelle Audits der Institutionen durchgeführt, um sowohl eine Bestandsaufnahme der Situation zu erhalten als auch Verbesserungsmassnahmen vorzuschlagen, die die Sicherheitshaltung aller INFRI-Mitglieder stärken sollen.

Kontext der spezialisierten Institutionen im Kanton Freiburg

Die spezialisierten Institutionen im Kanton Freiburg zeichnen sich durch eine grosse Vielfalt in Bezug auf Grösse, Aufgaben und IT-Mittel aus. Einige haben nur wenige Angestellte, während andere Hunderte von Mitarbeitenden mit unterschiedlichen Anforderungen an die IT-Infrastruktur verwalten. Ausserdem sind diese Organisationen häufig dezentralisiert und können das IT-Management an Drittanbieter auslagern, ihre Daten intern hosten oder Cloud-Lösungen wie Microsoft Office 365 nutzen.

Diese Vielfalt spiegelt sich auch in der Art der genutzten IT-Dienstleistungen wider: einige kritische Systeme werden intern verwaltet, andere vollständig an externe Anbieter ausgelagert und in vielen Fällen gibt es eine Hybridisierung zwischen diesen beiden Ansätzen. Die Heterogenität der Systeme und Prozesse verursacht manchmal ein komplexes Management der Cybersicherheit und erfordert Massnahmen, die auf den besonderen Kontext der jeweiligen Institution zugeschnitten sind.

Ziel dieses Leitfadens ist es diese Institutionen unabhängig von ihrer Grösse und ihrer IT-Konfiguration mit konkreten und modularen Empfehlungen zu unterstützen, um den heutigen Anforderungen an die Cybersicherheit gerecht zu werden.

Herausforderungen der Cybersicherheit in den Institutionen

Die spezialisierten Institutionen des Kantons Freiburg verwalten häufig sensible Daten, seien es persönliche Daten, Gesundheitsdaten oder geschäftskritische Informationen. Diese Daten müssen vor immer häufigeren und raffinierteren Cyberangriffen geschützt werden, seien es Datendiebstähle, Ransomware-Angriffe oder auch Systemzugeständnisse über nicht behobene Schwachstellen.

Die wichtigsten Herausforderungen der Cybersicherheit für diese Institutionen sind:

- **Sensible Daten schützen:** Institutionen sind oft für eine grosse Menge kritischer Daten verantwortlich, darunter medizinische, soziale oder administrative Daten. Der Schutz dieser Daten ist entscheidend, um die Kontinuität ihrer Dienstleistungen zu gewährleisten und die Privatsphäre der betroffenen Personen zu bewahren.
- **Gewährleistung der Weiterführung der Dienstleistungen:** Cyberangriffe können die von diesen Institutionen bereitgestellten Dienstleistungen unterbrechen, was schwerwiegende Auswirkungen auf den täglichen Betrieb verursachen kann. Daher müssen Strategien für die Weiterführung der Aktivitäten und die Wiederaufnahme nach dem Schaden eingeführt werden, um die potenziellen Auswirkungen zu minimieren.
- **Gesetzliche und vorschriftsmässige Verpflichtungen einhalten:** Die Institutionen unterliegen verschiedenen gesetzlichen und vorschriftsmässigen Rahmenbedingungen, insbesondere in Bezug auf das Datenschutzgesetz (DSG) und das Risikomanagement bei der Nutzung von Informationstechnologien. Die Nichteinhaltung dieser Verpflichtungen kann zu finanziellen oder rechtlichen Sanktionen oder zu einem Vertrauensverlust seitens der Benutzer und Partner führen.
- **Cyberbedrohungen antizipieren und darauf reagieren:** Cyberangriffe entwickeln sich schnell weiter, sowohl in Bezug auf die Häufigkeit als auch auf die Komplexität. Es ist wesentlich, dass spezialisierte Institutionen proaktive Verteidigungssysteme einrichten, aber auch in der Lage sind, schnell auf einen Vorfall zu reagieren.

Zusammenfassend lässt sich sagen, dass dieser Leitfaden einen umfassenden Rahmen bietet, der es den spezialisierten Institutionen im Kanton Freiburg ermöglicht, auf diese Herausforderungen zu reagieren und eine proaktive und widerstandsfähige Haltung in Bezug auf die Internetsicherheit einzunehmen.

Bewertung der Reife und Priorisierung von Empfehlungen

Um die Umsetzung der Empfehlungen dieses Leitfadens zu erleichtern, wurde jeder Cybersicherheitsmassnahme ein Reifegrad von 1 bis 3 zugeordnet. Diese Einstufung ermöglicht es spezialisierten Institutionen, ihre Bemühungen entsprechend ihrer aktuellen Situation, ihren verfügbaren Ressourcen und dem Grad ihrer Risikoausmass zu priorisieren.

Ziel dieser Einteilung ist es, einen progressiven Fahrplan anzubieten, der es Organisationen ermöglicht, ihre Cybersicherheitshaltung schrittweise zu stärken und dabei ihre betrieblichen und finanziellen Beschränkungen zu berücksichtigen.

Definition von Reifegraden

Stufe 1 - Niedriger Reifegrad (Prioritäre und wesentliche Massnahmen)

Diese Stufe entspricht den grundlegenden und kritischen Cybersicherheitsmassnahmen, die vorrangig umgesetzt werden müssen, um die Organisation vor den häufigsten und einschneidendsten Risiken zu schützen.

Ziel: Minimale Einhaltung der Vorschriften und Verringerung der grössten Risiken.

Eigenschaften:

- Fehlende oder schwache Formalisierung von Verfahren zur Cybersicherheit.
- Ungenügender Schutz vor den am weitesten verbreiteten Bedrohungen (Beispiel: Phishing, Ransomware).
- Reaktives Management von Sicherheitsvorfällen.
- Geringes Bewusstsein und geringe Ausbildung der Mitarbeitenden.
- Wenig oder keine Überwachungs- und Prüfungsinstrumente.

Stufe 2 - Mittlere Reife (Optimierung und Stärkung)

Diese Stufe stellt eine deutliche Verstärkung der Cybersicherheitsmassnahmen dar und zielt auf die Einführung eines proaktiven Bedrohungs- und Schwachstellenmanagements ab.

Ziel: Übergang von einer reaktiven Haltung zu einem präventiven Vorgehen.

Eigenschaften:

- Formalisierte und dokumentierte Cybersicherheitsprozesse.
- Einführung fortgeschrittener Tools zur Überwachung und Verwaltung von Zugängen.
- Sensibilisierung und regelmässige Schulung der Mitarbeitende in Bezug auf Cyberbedrohungen.

- Systematische Anwendung von Sicherheits-Patches und -Updates.
- Proaktive Überwachung der Infrastruktur und der Sicherheitslogs.

Stufe 3 - Hohe Reife (fortgeschrittene Cybersicherheit und Governance)

Diese Stufe spiegelt eine fortgeschrittene Reife im Bereich der Internetsicherheit wider, die sich durch ein strategisches und integriertes Sicherheitsmanagement sowie fortgeschrittene Fähigkeiten zur Erkennung und Reaktion auf Bedrohungen auszeichnet.

Ziel: Bedrohungen voraussehen und optimale Widerstandsfähigkeit gegen Cyberangriffe gewährleisten.

Eigenschaften:

- Cybersecurity Governance, die in die Gesamtstrategie der Organisation integriert ist.
- Fortschrittliche Automatisierung von Sicherheitsprozessen.
- Regelmässige Intrusionstests und Simulationen von Cyberangriffen.
- Echtzeitüberwachung mit Erkennung von anormalem Verhalten.
- Einrichtung eines internen oder ausgelagerten SOC (Security Operations Center).

Strategie für die Umsetzung

Der Übergang von einer Reifegradstufe zur nächsten sollte schrittweise erfolgen und den Ressourcen der Institution angepasst sein. Hier einige Tipps, wie Sie diesen Reifegrad strukturieren können:

1. **Priorisierung von Massnahmen der Stufe 1:** Diese Massnahmen bilden die Grundlage für die Sicherheit und sollten in erster Linie umgesetzt werden.
2. **Die Entwicklung regelmässig bewerten:** Führen Sie interne Audits durch, um den erreichten Reifegrad zu messen.
3. **Planen Sie die notwendigen Investitionen:** Die Stufen 2 und 3 erfordern oft zusätzliche Tools und Fachkenntnisse.
4. **Management und Mitarbeitende einbeziehen:** Cybersicherheit ist eine kollektive Verantwortung und muss durch eine effektive Unternehmensführung unterstützt werden.

Bestandsaufnahme von Systemen und Diensten

Der erste grundlegende Schritt zur Gewährleistung der Cybersicherheit einer Organisation ist die Erstellung eines vollständigen und aktuellen Inventars der von ihren verwalteten Computersystemen, Dienste und Daten. Dieses Inventar dient als Grundlage für die Risikobewertung, die Planung von Schutzmassnahmen und die Gewährleistung eines fortlaufendes Sicherheitsmanagements. Es erlaubt auch mögliche Abhängigkeiten zwischen internen Diensten und Diensten externer Anbieter zu sehen, die direkt auf die Gesamtsicherheit eine Auswirkung haben können.

Kartierung der internen und externen IT-Systeme

Jede Institution verfügt über eine spezifische IT-Infrastruktur, die eine Mischung aus intern verwalteten Systemen, Dienstleistungen von externen Dienstleistern oder Cloud-Lösungen umfassen kann. Eine umfassende Kartierung der vorhandenen Systeme ist relevant. Dazu gehören:

- Physische und virtuelle Server: identifizieren Sie alle Server, ihre Funktion (Dateiserver, Anwendungsserver, Datenbanken usw.) und ihren physischen oder virtuellen Standort (Datencenter, Cloud, vor Ort).
- Systeme zur Verwaltung von Datenbanken: listen Sie alle verwendeten Datenbanken, die Versionen der Verwaltungssoftware, ihren Standort (vor Ort oder Cloud) und die für ihre Verwaltung zuständigen Personen oder Abteilungen auf.
- Arbeitsplätze und Peripheriegeräte: schliessen Sie Desktops, Laptops, mobile Geräte, Drucker und andere Peripheriegeräte ein, die an das Netzwerk der Institution angeschlossen sind.
- Interne Netzwerke: beschreiben Sie die innerhalb der Institution verwendeten Netzwerksegmente (Verwaltungsnetzwerke, Gastnetzwerke, Produktionsnetzwerke usw.) sowie deren Verbindungen.
- Externe Netzwerke und Dienste: ermitteln Sie VPN-Verbindungen, Netzwerke, die von Partnern oder Dienstleister genutzt werden, sowie Dienste, die ausserhalb der Institution gehostet werden.

Klassifizierung von Daten und Systemen

Nicht alle Daten besitzen die gleiche Sensibilität oder den gleichen Wert für die Institution. Eine gute Klassifizierung der Daten ist ausschlaggebend, um die Prioritäten für den Schutz und das Risikomanagement festzulegen. Diese Klassifizierung enthält:

- Vertraulichkeitsstufen: sortieren Sie die Daten, ob sie öffentlich, privat oder vertraulich sind. Sensible Daten (persönliche Daten von Begünstigten, finanzielle Informationen usw.) sollten beispielsweise so eingestuft werden, dass ihr verstärkter Schutz gewährleistet ist.

- Systemkritikalität: identifizieren Sie kritische Systeme, deren Nichtverfügbarkeit die Vorgänge der Institution ernsthaft beeinträchtigen könnte (z. B. die Systeme zur Verwaltung von Leistungsempfängern in einer Institution).
- Regulierte Daten: heben Sie Daten hervor, die bestimmten Regulierungen unterliegen, z. B. dem DSG (personenbezogene Daten) oder lokalen Vorschriften (Gesundheitsdaten).

Eine gute Klassifizierung ermöglicht es, bei der Behandlung von Vorfällen Prioritäten zu setzen und je nach Sensibilitätsgrad geeignete Sicherheitsmassnahmen anzuwenden.

Identifikation externer Anbieter (Hosting, Cloud, Dienstleistungen)

Spezialisierte Institutionen können für das Hosting ihrer Systeme, die Verwaltung bestimmter IT-Dienstleistungen oder den Zugang zu Cloud-Lösungen von externen Dienstleistern abhängig sein. Die Bestandsaufnahme der externen Dienstleister muss exakt sein, um sicherzustellen, dass die von diesen Dienstleistern angewandten Sicherheitsmassnahmen den Anforderungen der Institution entsprechen.

- Anbieter von Hosting-Diensten: erfassen Sie Angaben von Unternehmen, die physische oder Cloud-Hosting-Dienste anbieten. Überprüfen Sie die sicherheitsrelevanten Vertragsbedingungen, einschliesslich der Service Level Agreements (SLAs), und die Richtlinien für Datensicherung, Verschlüsselung und Zugangsverwaltung.
- Anbieter von Software-as-a-Service (SaaS)-Lösungen: erfassen Sie die Anwendungen von Drittanbietern, die im Rahmen von Cloud-Diensten genutzt werden (z. B. Microsoft Office 365, Google Workspace). Stellen Sie sicher, dass diese Dienste die erforderlichen Sicherheitsstandards erfüllen (Identitätsmanagement, Zugangssicherheit, Daten-verschlüsselung usw.).
- Wartungs- und Supportanbieter: erstellen Sie eine Liste der externen Anbieter, die für die Wartung, den Support oder die Verwaltung auf Ihre Systeme zugreifen. Legen Sie fest, wie der Zugriff auf Ihre Systeme erfolgen soll und welche Sonderrechtestufen gewährt werden.

Verbindungen und Abhängigkeiten zwischen Diensten

IT-Systeme funktionieren in der Regel nicht isoliert. Häufig nutzt eine Institution miteinander verbundene Dienste oder Teile ihrer Infrastruktur sind von externen Ressourcen abhängig. Es ist entscheidend, diese Abhängigkeiten zu verstehen, um Schwachstellen in der Sicherheitskette zu vermeiden. Zu den üblichen Beispielen gehören:

- Verbindungen zu Cloud-Diensten: zum Beispiel eine in der Cloud gehostete E-Mail- oder Dokumentenverwaltungslösung, bei der die Daten lokal synchronisiert werden.
- Verbindungen mit Diensten von Drittanbietern: zum Beispiel Zahlungssysteme, Dienste zur Kommunikation mit anderen Organisationen (Partner, Regierungen, Dienstleister).
- API-Abhängigkeiten und Software-Integrationen: erfassen Sie die Schnittstellen, die verwendet werden, um Anwendungen miteinander zu verbinden (zum Beispiel APIs zum Austausch von Daten zwischen Ihrem ERP-System und einer Drittanbieteranwendung).

Dieser Überblick über die gegenseitigen Abhängigkeiten wird es ermöglichen, potenzielle Fehlerquellen zu antizipieren und Sicherheitsmassnahmen auf allen betroffenen Ebenen einzuführen.

Aktualisierung und Pflege des Inventars

Das Inventar der Systeme und Dienste muss ständig auf dem neuesten Stand gehalten werden. Änderungen an der Infrastruktur, das Hinzufügen oder Entfernen neuer Dienste sowie Änderungen der Abhängigkeiten von externen Dienstleistern müssen regelmässig dokumentiert werden. Ein automatisierter oder halbautomatischer Aktualisierungsprozess (zum Beispiel mittels Inventarverwaltungssoftware) wird empfohlen, um sicherzustellen, dass das Inventar jederzeit korrekt ist. Folgende Punkte müssen besonders beachtet werden:

- Aktualisierungen bei Änderungen der Infrastruktur (neue Server, Migration in die Cloud, Entfernen veralteter Systeme).
- Überwachung des externen Zugriffs, insbesondere für Anbieter, die sich in den Systemen der Einrichtung einloggen können.
- Dokumentation von neuen Geräten und Endgeräten, die dem Netzwerk hinzugefügt wurden (Computer, Handys usw.).

Netzwerksicherheit und Segmentierung

Einführung

Die Netzwerksicherheit ist ein wesentlicher Pfeiler zum Schutz der Informationssysteme von Institutionen, insbesondere in einem Umfeld, in dem sensible Systeme und Daten zunehmend Cyberbedrohungen ausgesetzt sind. Die Netzwerksegmentierung, bei der das Netzwerk in logische Subnetze unterteilt wird, ist eine Schlüsselstrategie, um die Ausbreitung von Bedrohungen zu begrenzen, wenn ein Segment gefährdet wird. Sie ermöglicht es auch, den Zugriff auf kritische Ressourcen nach Bedarf zu beschränken, indem das Prinzip der geringsten Privilegien angewandt wird.

Dieser Abschnitt beschreibt bewährte Verfahrensweisen zur Sicherung der internen Netzwerke von spezialisierten Institutionen und gibt Empfehlungen für die Segmentierung, wobei die unterschiedlichen Umgebungen der einzelnen Institutionen (Grösse, interne Mitarbeitende, externe Dienstleister) berücksichtigt werden.

Prinzipien der Netzwerksegmentierung

NIVEAU 1

Die Segmentierung des Netzwerks ermöglicht die Unterteilung von Systemen und Daten und verringert so das Risiko, dass ein Angreifer das gesamte Netzwerk gefährdet. Eine effiziente Segmentierung beruht auf folgenden Grundsätzen:

- **Isolierung kritischer Segmente:** kritische Systeme, wie Datenbankserver und Systeme zur Verwaltung sensibler Informationen, sollten in zweckgebundenen Segmenten isoliert werden. Dadurch wird der Zugriff nur auf berechtigte Benutzer und Abteilungen beschränkt.
- **Prinzip des geringsten Privilegs:** nur Benutzer und Abteilungen, die betriebliche Bedürfnisse haben, sollten auf kritische Segmente zugreifen können. Die Zugriffsregeln sollten auf der Grundlage der Benutzerrollen und der Sensibilität der Systeme festgelegt werden.
- **Begrenzung der Angriffsfläche:** indem die Verbindungen zwischen den einzelnen Segmenten eingeschränkt werden, werden die potenziellen Verbreitungsvektoren für Angriffe reduziert. Beispielsweise sollte das Verwaltungsnetzwerk vom Produktions-netzwerk getrennt sein, um das Risiko von Seitenangriffen zu begrenzen.

Bewährte Verfahrensweisen für die Segmentierung und Trennung interner Netzwerke

Um eine effektive Netzwerksegmentierung zu implementieren, finden Sie hier einige praktische Empfehlungen:

Klassifizierung von Ressourcen

- Identifizieren Sie kritische Ressourcen, sensible Anwendungen und vertrauliche Daten.
- Erstellen Sie eine Karte der Netzwerkressourcen in der Sie die Klassifizierung der einzelnen Systeme (vertraulich, sensibel, öffentlich usw.) bezeichnen, um die Segmentierungs-bedürfnisse besser definieren zu können.

Einrichtung von Sicherheitszonen

- Öffentlicher Bereich: umfasst über Internet zugängliche Dienste und Anwendungen, wie öffentliche Websites und E-Mail-Server. Diese Dienste sollten isoliert werden, um ihre Exposition gegenüber anderen Teilen des Netzwerks zu begrenzen.
- DMZ-Zone (demilitarisierte Zone): diese Zwischenzone wird verwendet, um Dienste, auf die von aussen zugegriffen wird, zu isolieren und gleichzeitig ein zusätzliches Schutzniveau aufrechtzuerhalten. Sie schränkt den direkten Zugriff auf interne Systeme ein, indem sie Logins zwingt, über Firewalls und Proxys zu gehen.
- Interner Bereich: umfasst die internen Systeme der Organisation, z. B. Dateiserver und Benutzerarbeitsplätze. Dieser Bereich sollte nicht direkt über Internet erreichbar sein.
- Sensibler Bereich: dieser Bereich ist kritischen Ressourcen gewidmet (sensible Datenbanken, Anwendungen für die interne Verwaltung usw.). Er ist stark eingeschränkt und sein Zugang muss streng kontrolliert werden.

Kontrolle des Zugangs zwischen den Bereichen

- Implementieren Sie strenge Zugriffskontrollen zwischen den verschiedenen Bereichen des Netzwerks. Beispielsweise sollten Benutzer des internen Bereichs nicht ohne Begründung auf den sensiblen Bereich zugreifen können.
- Verwenden Sie interne Firewalls, um die Richtlinien für die Kontrolle zwischen den einzelnen Bereichen festzulegen. Verbindungen zwischen Bereichen sollten auf die notwendigsten Protokolle beschränkt werden (zum Beispiel FTP- oder RDP-Verbindungen zu sensiblen Bereichen blockieren).
- Verfolgen Sie eine "deny-by-default"-Vorgehensweise, indem Sie nur explizit benötigte Kommunikationsflüsse zulassen.

Logische Segmentierung mit VLANs

- Verwenden Sie VLANs (Virtual Local Area Networks), um logische Subnetze zu erstellen. Beispielsweise ein VLAN für die Verwaltung, eines für die Produktion und eines für Besucher.
- Stellen Sie sicher, dass die VLANs richtig konfiguriert sind, mit strengen Routing-Regeln, um unberechtigte Zugriffe zwischen ihnen zu verhindern.
- Beschränken Sie den Zugriff auf VLANs auf berechtigte Benutzer und wenden Sie für jedes VLAN spezifische Sicherheitsrichtlinien an.

Sicherung von Zugangspunkten und VPN-Verbindungen

- VPN-Zugänge (Virtual Private Network) sollten in einer DMZ-Zone platziert werden und nicht direkt mit sensiblen internen Bereichen verbunden sein.

- Richten Sie eine Multi-Faktor-Authentifizierung (MFA) für den VPN-Zugang ein und beschränken Sie die Zugriffsrechte von VPN-Benutzern auf die unbedingt erforderlichen Ressourcen.
- Überwachen und protokollieren Sie VPN-Verbindungen, um verdächtige Aktivitäten zu erkennen.

Verwendung interner Firewalls zur Filterung des Datenverkehrs

- Verwenden Sie Firewalls, um den Datenverkehr zwischen den verschiedenen Netzwerksegmenten zu filtern. Firewalls sollten so konfiguriert sein, dass sie nur den wichtigsten Datenverkehr zulassen.
- Erstellen Sie strenge Firewall-Regeln zwischen VLANs und Subnetzen, indem Sie granulare Filter nach IP-Adressen, Ports und Protokollen anwenden.

Überwachung und Wartung von Perimeter-Sicherheitseinrichtungen

Die Sicherheit der Segmentierung beruht auf der kontinuierlichen Überwachung und regelmässigen Wartung der Sicherheitsvorrichtungen des Netzwerks, einschliesslich Firewalls und Intrusion Detection Systems (IDS/IPS).

Aktive Überwachung des Netzwerks

- Implementieren Sie Überwachungssysteme, um Anomalien oder Eindringversuche zwischen den Netzwerksegmenten zu erkennen und zu alarmieren.
- Integrieren Sie ein SIEM (Security Information and Event Management), um die Protokolle von Firewalls und Netzwerksystemen zu analysieren und verdächtiges Verhalten zu erkennen.

Aktualisierungen und Sicherheitstests

- Stellen Sie sicher, dass alle Netzwerksicherheitsgeräte (Firewalls, Router usw.) regelmässig aktualisiert werden, um bekannte Schwachstellen zu schliessen.
- Führen Sie regelmässig Penetrationstests durch, um die Wirksamkeit der Segmentierung zu überprüfen und Schwachstellen zu identifizieren.

Prüfung der Segmentierungsregeln

- Führen Sie regelmässige Prüfungen der Segmentierungsregeln durch, um ihre Angemessenheit und die Einhaltung der Sicherheitsanforderungen zu überprüfen.
- Überprüfen und optimieren Sie regelmässig die Firewall- und Routing-Regeln, um eine optimale Segmentierung zu gewährleisten und die Zugriffskontrollen an ändernde Bedürfnisse anzupassen.

Schlussfolgerung

Die Segmentierung des Netzwerks ist eine wesentliche Massnahme, um die internen Ressourcen einer Institution vor externen und internen Bedrohungen zu schützen. Durch eine rigorose Segmentierung in Verbindung mit strengen Zugangskontrollen und einer kontinuierlichen Überwachung können Institutionen die Wahrscheinlichkeit grösserer Sicherheitsvorfälle stark reduzieren und ihre kritischen Daten und Systeme wirksam schützen.

Konfiguration und Verwaltung von Firewalls

Firewalls sind wichtige Sicherheitsvorrichtungen, um den Perimeter des Netzwerks von Institutionen zu schützen und unberechtigten Zugriff zu verhindern. Durch ihre korrekte Konfiguration kann das Eindringling Risiko begrenzt und gleichzeitig die Kontinuität der Dienste für berechtigte Benutzer gewährleistet werden. In diesem Abschnitt werden bewährte Verfahren für die Konfiguration, Verwaltung und Wartung von Firewalls vorgestellt.

Die Rolle von Firewalls beim Perimeterschutz verstehen

Firewalls fungieren als Barriere zwischen dem internen Netzwerk einer Institution und externen Netzwerken, einschliesslich des Internets. Sie filtern den ein- und ausgehenden Datenverkehr anhand festgelegter Regeln, um potenzielle Bedrohungen zu blockieren und nur legitime Kommunikation zuzulassen. Eine effiziente Konfiguration von Firewalls ist entscheidend um:

- kritische Daten und Systeme vor Angriffen von aussen zu schützen.
- die Exposition der internen Dienste im Internet zu begrenzen.
- die Segmentierung zwischen verschiedenen Subnetzen zur besseren Isolierung sensibler Systeme sicherzustellen.

Filterrichtlinien für ein- und ausgehenden Datenverkehr

Prinzip des geringsten Privilegs: Konfigurieren Sie die Firewall so, dass nur Datenverkehr zugelassen wird, der für den Betrieb der Institution unerlässlich ist. Alle anderen Verbindungen sollten standardmässig blockiert werden.

Port- und Dienstefilterung: Identifizieren Sie die notwendigen Ports und Dienste und lassen Sie nur die unbedingt notwendigen zu.

Geofencing-Regeln: Beschränken Sie die Verbindungen auf die notwendigen geografischen Bereiche. Wenn die Einrichtung beispielsweise nur mit lokalen Partnern zusammenarbeitet, beschränken Sie die Zugriffe auf die Schweiz und Europa.

Überwachung des ausgehenden Datenverkehrs: Überwachen Sie ausgehende Verbindungen, um Datenlecks oder unberechtigte Verbindungen zu bösartigen Websites zu verhindern.

Bewährte Verfahrensweisen für die Verwaltung von Firewall-Regeln

Alle Firewall-Regeln dokumentieren: Führen Sie eine klare und genaue Dokumentation jeder Firewall-Regel, einschliesslich ihres Zwecks, der geöffneten Ports, der betroffenen IPs und der Gründe für ihre Implementierung.

Minimierung der Komplexität von Regeln: Vermeiden Sie die Anhäufung redundanter oder veralteter Regeln, die zu Fehlern oder Sicherheitslücken führen könnten.

Regelgruppen nach Funktion einrichten: Ordnen Sie die Firewallregeln in Gruppen (z. B. Internetzugang, Zugang zu internen Diensten usw.), um sie übersichtlicher zu gestalten und die Verwaltung zu vereinfachen.

Regelmässige Überprüfung der Firewall-Regeln: Führen Sie regelmässige Überprüfungen durch, um die Relevanz jeder Regel zu bewerten. Löschen oder aktualisieren Sie Regeln, die nicht mehr notwendig sind.

Überwachung und Wartung von Perimeter-Sicherheitseinrichtungen

Kontinuierliche Überwachung: Richten Sie eine 24/7-Überwachung ein, um Eindringversuche oder Anomalien im Datenverkehr zu erkennen. Verwenden Sie zusätzlich zur Firewall Tools zur Erkennung von Eindringlingen (IDS/IPS).

Protokollierung und Prüfung: Aktivieren Sie die Protokolle (Logs) der Firewalls, um Verbindungen und Zugriffsversuche nachzuverfolgen. Diese Protokolle sollten für einen bestimmten Zeitraum aufbewahrt werden (oft zwischen 6 Monaten und 1 Jahr, je nach gesetzlichen Anforderungen) und regelmässig auf verdächtige Aktivitäten überprüft werden.

Updates und Patches: Stellen Sie sicher, dass die Firmware der Firewall regelmässig aktualisiert wird, um bekannte Sicherheitslücken zu schliessen. Aktivieren Sie die Update-Benachrichtigungen des Anbieters und legen Sie Zeitfenster für das Einspielen von Patches ohne Dienstunterbrechung fest.

Regelmässige Eindringlingstests: Führen Sie regelmässige Eindringlingstests durch, um die Robustheit der Firewallregeln zu bewerten. Diese Tests können intern oder von Dritten durchgeführt werden, um Konfigurationen zu validieren und potenzielle Schwachstellen zu identifizieren.

Erweiterte Konfiguration von Firewalls

Intrusion Detection and Prevention (IDS/IPS): Viele moderne Firewalls verfügen über integrierte IDS/IPS-Funktionen, um Angriffssignaturen zu erkennen und automatisch zu reagieren. Konfigurieren Sie IDS/IPS-Regeln, um gängige Bedrohungen zu blockieren und Warnungen zu erhalten, wenn verdächtiger Datenverkehr erkannt wird.

Deep Packet Inspection (DPI): Verwenden Sie die Deep Packet Inspection, um den Inhalt der Kommunikation detailliert zu analysieren und versteckte Angriffe, einschliesslich Malware, zu erkennen.

VPN und sicherer Fernzugriff: Bevorzugen Sie für den Fernzugriff Verbindungen über VPN mit starker Authentifizierung. Beschränken Sie den Fernzugriff nur auf Benutzer, die ihn benötigen, um die Gefährdung zu minimieren.

Anwendungsfilterung: Konfigurieren Sie die Firewall so, dass sie den Datenverkehr nicht nur auf Port-, sondern auch auf Anwendungsebene filtert. Dadurch kann der Zugriff nur auf genehmigte Anwendungen beschränkt werden.

Reaktion auf Vorfälle und Wiederherstellung

Plan zur Reaktion auf Vorfälle: Definieren Sie einen spezifischen Reaktionsplan für Vorfälle, die die Firewall betreffen, wie Brute-Force-Versuche oder Denial-of-Service (DoS). Dieser Plan sollte Verfahren zur schnellen Sperrung verdächtiger IP-Adressen und zur Wiederherstellung des Dienstes enthalten.

Sicherung und Wiederherstellung der Konfiguration: Sichern Sie die Konfiguration der Firewall regelmässig und stellen Sie sicher, dass eine Kopie für eine schnelle Wiederherstellung im Falle eines Ausfalls verfügbar ist. Testen Sie den Wiederherstellungsprozess regelmässig, um seine Effizienz zu überprüfen.

Koordination mit den Sicherheitsteams: Im Falle eines Vorfalls muss die Firewall in die Reaktionskette der Institution eingebunden sein, mit einer reibungslosen Kommunikation zwischen den Netzwerkadministratoren, den Sicherheitsteams und den Verantwortlichen der Institution.

Schlussfolgerung und Empfehlungen

Eine effiziente Verwaltung von Firewalls erfordert kontinuierliche Aufmerksamkeit und regelmässige Überprüfungen. Es wird empfohlen:

- Eine aktuelle und zugängliche Dokumentation für jede Regel und Konfiguration zu halten.
- Netzwerkadministratoren und Benutzer über bewährte Verfahrensweisen zur Cybersicherheit aufzuklären und zu sensibilisieren.
- In Überwachungs- und Erkennungstools zu investieren, um einen proaktiven Schutz vor Bedrohungen zu gewährleisten.

Die richtige Konfiguration und Verwaltung von Firewalls ist eine der Säulen der Cybersicherheit für Institutionen. Dadurch wird das Risiko eines Eindringlings erheblich verringert und die Verfügbarkeit und Integrität digitaler Dienste sichergestellt.

Datensicherung und -wiederherstellung

Die Einführung einer effizienten Backup-Politik ist ein Schlüsselelement der Cybersicherheitsstrategie. Die regelmässige Sicherung von Daten und die Fähigkeit, Systeme im Falle eines Schadens (Hardwareausfall, Cyberangriff, menschliches Versagen usw.) schnell wiederherzustellen, sind für die Betriebskontinuität von Fachinstitutionen unerlässlich. Dieser Abschnitt bietet einen Rahmen mit bewährten Verfahrensweisen zur Definition und Verwaltung von Datensicherungs- und Wiederherstellungsprozessen.

Strategien für die Datensicherung

Die Sicherungsstrategien müssen an die spezifischen Bedürfnisse jeder Institution angepasst werden, je nachdem, wie sensibel die Daten sind, wie oft die Informationen geändert werden und welche rechtlichen Anforderungen bestehen. Nachstehend die wichtigsten empfohlenen Arten von Datensicherungen:

Vollständige Backups: Eine vollständige Kopie aller Daten wird regelmässig erstellt. Obwohl dies die umfassendste Methode ist, kann sie viel Zeit und Speicherplatz erfordern.

Inkrementelle Sicherungen: Es werden nur die Daten gesichert, die seit der letzten Sicherung (vollständig oder inkrementell) geändert wurden. Diese Methode ist zügiger und spart Speicherplatz, kann aber den Wiederherstellungsprozess verlängern.

Differentielle Sicherungen: Es werden nur die Daten gesichert, die seit der letzten vollständigen Sicherung geändert wurden. Auch diese Methode verringert das Volumen der gesicherten Daten im Vergleich zu einer vollständigen Sicherung, aber die Wiederherstellung erfordert weniger Schritte als eine inkrementelle Sicherung.

Kontinuierliche Datensicherung (CDP - Continuous Data Protection): Bei dieser Methode werden die Daten in Echtzeit gesichert. Sie ist ideal für kritische Daten, da sie das Risiko eines Datenverlusts zwischen zwei Backups minimiert.

Wahl des Speicherortes für Backups

Der Standort der Backups ist ein entscheidender Faktor, um sicherzustellen, dass sie bei Bedarf verfügbar sind. Institutionen können sich für verschiedene Optionen entscheiden:

- **Lokale Backups:** Die Daten werden auf lokalen Festplatten oder Servern gespeichert. Diese Option ermöglicht eine schnelle Wiederherstellung, kann aber bei einem Vorfall wie Feuer oder Überschwemmung anfällig sein.
- **Externe Backups:** Die Daten werden bei einem externen Anbieter gesichert. Dies bietet Schutz vor lokalen Schaden, hängt aber von der Zuverlässigkeit und Sicherheit der Infrastruktur des Anbieters ab.

- **Cloud-Backups:** Die Daten werden auf einer Cloud-Plattform gespeichert, die Flexibilität und Redundanz bietet. Es muss jedoch unbedingt sichergestellt werden, dass der Cloud-Anbieter die Sicherheits- und Datenschutzstandards einhält.
- **Hybrider Ansatz:** Diese Strategie kombiniert lokale und cloudbasierte Datensicherungen, um die Vorteile beider Optionen zu nutzen. Eine lokale Kopie ermöglicht beispielsweise eine schnelle Wiederherstellung, während eine Kopie in der Cloud eine geografisch weit entfernte Redundanz gewährleistet.

Häufigkeit und Planung von Backups

Die Häufigkeit der Datensicherungen sollte sich nach den Bedürfnissen der Institution und der Kritikalität der Daten richten. Hier einige Empfehlungen:

- **Kritische Daten:** Bei sensiblen und regelmässig aktualisierten Daten ist eine tägliche (oder sogar eine kontinuierliche) Sicherung empfehlenswert.
- **Weniger kritische Daten:** Bei weniger strategischen Informationen kann eine wöchentliche oder monatliche Sicherung ausreichen.
- **Datensicherungstests:** Es ist wichtig, die Integrität von Datensicherungen regelmässig zu überprüfen und sicherzustellen, dass sie ordnungsgemäss funktionieren. Ein vierteljährlicher oder halbjährlicher Test wird empfohlen.

Wiederherstellungstests: Bewährte Verfahrensweisen und Häufigkeit

Die Fähigkeit, Daten aus einem Backup wiederherzustellen, ist genauso wichtig wie das Backup selbst. Ohne ein Testverfahren für die Wiederherstellung ist es unmöglich zu wissen, ob Backups im Schadenfall effizient eingesetzt werden können.

- **Wiederherstellungstest:** Planen Sie regelmässige Tests, um die Fähigkeit zur Datenwiederherstellung zu überprüfen. Dazu gehören partielle Wiederherstellungen (bestimmte Dateien oder Ordner) und vollständige Wiederherstellungen (ganze Systeme).
- **Frequenz der Tests:** Wiederherstellungstests sollten mindestens einmal pro Quartal und nach bedeutenden Änderungen an der Infrastruktur oder den Daten durchgeführt werden.
- **Dokumentation des Wiederherstellungsverfahrens:** Es ist wesentlich, das Wiederherstellungsverfahren zu dokumentieren, damit die Teams wissen, wie sie im Krisenfall vorgehen müssen. Diese Dokumentation sollte regelmässig aktualisiert werden und im Notfall zugänglich sein.

Zusätzliche Empfehlungen

Sicherheit von Backups: Gesicherte Daten müssen verschlüsselt werden, um einen unbefugten Zugriff zu verhindern. Ausserdem sollte der Zugang zu den Sicherungssystemen auf berechtigtes Personal beschränkt werden.

Richtlinie für die Aufbewahrung von Backups: Legen Sie Richtlinien für die Aufbewahrung von Backups fest, die den Bedürfnissen der Institution entsprechen. Gewisse Daten

müssen möglicherweise aus rechtlichen Gründen oder zur Einhaltung von Vorschriften langfristig aufbewahrt werden.

Backup-Audit: Führen Sie ein regelmässiges Audit der Backup-Verfahren und -Systeme ein, um sicherzustellen, dass sie den bewährten Verfahrensweisen entsprechen und ordnungsgemäss funktionieren.

Protokollverwaltung: Führen Sie Protokolle über alle Sicherungs- und Wiederherstellungsvorgänge, um die Prüfung und Lösung von Vorfällen zu erleichtern.

Benutzerschulung: Schulen Sie die technischen Teams in den Sicherungs- und Wiederherstellungsverfahren, um sicherzustellen, dass sie im Falle eines Problems effizient reagieren können.

Sicherung von im Internet offengelegte Dienste

Im Internet offengelegte Dienste sind ein beliebter Einstiegspunkt für Angreifer, die diese Dienste gezielt anvisieren können, um Schwachstellen auszunutzen oder auf interne Ressourcen einer Organisation zuzugreifen. Daher ist es entscheidend, geeignete Sicherheitsstrategien zu implementieren, um die mit der Exposition von Diensten im Internet verbundenen Risiken zu reduzieren. Dieser Abschnitt enthält Empfehlungen für die Identifizierung, den Schutz und die Verschärfung dieser Dienste.

Identifizierung der ausgestellten Dienste

Der erste Schritt zur Sicherung ist die Identifizierung aller Dienste, die dem Internet ausgesetzt sind. Diese Identifizierung sollte Folgendes umfassen:

- **Die Erfassung aller öffentlich zugänglichen Dienste:** u. a. Webserver, E-Mail-Dienste, VPNs, FTP-Server, Datenbanken, Verwaltungsschnittstellen usw.
- **Die Beurteilung der Notwendigkeit jedes ausgestellten Dienstes:** Jeder im Internet zugängliche Dienst sollte durch einen klaren Geschäftsbedarf gerechtfertigt sein. Ist dies nicht der Fall, wird empfohlen, ihn zu entfernen.
- **Dokumentation der Konfigurationen jedes ausgestellten Dienstes:** Dazu gehören Informationen über die offenen Ports, die verwendeten Protokolle und die angewandten Sicherheitskonfigurationen.

Diese Erhebungsphase kann durch Tools zur Netzwerkerkennung (z. B. Nmap) und Lösungen für die Vermögensverwaltung (Asset Management) erleichtert werden.

Reduzierung der Angriffsfläche

Sobald die Dienste identifiziert sind, sollte die Angriffsfläche möglichst reduziert werden, insbesondere durch:

- **Schliessung ungenutzter Ports:** Alle Ports, die nicht unbedingt erforderlich sind, sollten geschlossen werden, um eine unnötige Exposition zu vermeiden.
- **Beschränkung der zulässigen IP-Adressen:** Beschränken Sie den Zugang zu Diensten nach Möglichkeit auf bestimmte IP-Adressen oder IP-Adressbereiche, um die öffentliche Exposition zu begrenzen.
- **Verwendung von Proxys oder sichere Gateways:** um eine Sicherheitseinrichtung zwischen den ausgestellten Dienst und das Internet zu schalten, mit der der eingehende Datenverkehr gefiltert und überwacht werden kann.
- **Implementierung von Anwendungsfirewalls (WAF):** Bei Webanwendungen kann der Einsatz einer WAF (Web Application Firewall) bösartige Anfragen herausfiltern und vor gängigen Angriffen wie SQL-Injection, Cross-Site-Scripting (XSS) usw. schützen.

Sicherung von Kommunikationsdiensten (SSL/TLS)

Die Verwendung verschlüsselter Kommunikation ist entscheidend für den Schutz der Daten, die zwischen den Benutzern und den offengelegten Diensten ausgetauscht werden:

- Erzwingen Sie die Verwendung des HTTPS-Protokolls für alle offengelegte Webdienste.
- Verwenden Sie gültige SSL/TLS-Zertifikate, die von vertrauenswürdigen Zertifizierungsstellen ausgestellt wurden. Vermeiden Sie selbstsignierte Zertifikate für öffentlich zugängliche Dienste.
- Deaktivieren Sie veraltete Protokolle (wie SSL 2.0, SSL 3.0, TLS 1.0 und TLS 1.1) zugunsten von TLS 1.2 und TLS 1.3, die eine höhere Sicherheit bieten.
- Konfigurieren Sie robuste Verschlüsselungssuiten und vermeiden Sie schwache Verschlüsselungsalgorithmen (wie DES, RC4).
- HSTS (HTTP Strict Transport Security) einrichten, um Browser dazu zu zwingen, nur sichere Verbindungen zum Dienst zu akzeptieren.

Authentifizierungs- und Berechtigungskontrollen

Offengelegte Dienste müssen starke Authentifizierungs- und Berechtigungskontrollen integrieren, um den Zugriff nur auf bewilligte Benutzer zu beschränken:

- **Starke Authentifizierung verlangen:** Verwenden Sie für alle sensiblen Zugriffe Mechanismen zur Multifaktor-Authentifizierung (MFA).
- **Administrative Zugriffe einschränken:** Beschränken Sie administrative Sonderrechte auf Benutzer, die sie unbedingt benötigen und begrenzen Sie den administrativen Zugriff auf vertrauenswürdige Netzwerke.
- **Sichere Sessions einrichten:** Session Tokens verwenden und Beschränkungen für die Lebensdauer von Sessions und Inaktivität anwenden.
- **Aktivieren Sie die Protokollierung und Prüfung von Zugriffen:** Protokollieren Sie Zugriffe auf exponierte Dienste, einschliesslich erfolgreicher und fehlgeschlagener Versuche, um Prüfungen und die Erkennung verdächtiger Aktivitäten zu erleichtern.

Testen von Schwachstellen und Verwaltung von Patches

Die Sicherheit der offengelegten Dienste muss regelmässig durch Schwachstellentests und proaktives Patchmanagement überprüft werden:

- **Regelmässige Schwachstellen-Scans durchführen:** Verwenden Sie Scan-Tools (wie Nessus, OpenVAS), um potenzielle Sicherheitslücken zu identifizieren.
- **Kritische Schwachstellen schnell beheben:** Exponierte Schwachstellen in öffentlichen Diensten müssen umgehend behoben werden. Priorisierung von Sicherheitspatches nach Kritikalitätsgrad.
- **Patch-Management-Prozess umsetzen:** Ein regelmässiges Verfahren zum Einspielen von Sicherheitsaktualisierungen einrichten, das auch Betriebssysteme, Software von Drittanbietern und Netzwerkgeräte umfasst.

Verschärfung von Konfigurationen

Zusätzlich zu den Patches ist es entscheidend, die Konfigurationen zu verschärfen, um die Möglichkeiten der Ausnutzung einzuschränken:

- **Wenden Sie die dargelegten Leitfäden zur Dienstverschärfung an:** Verwenden Sie z. B. die CIS-Benchmarks (Center for Internet Security) für die Konfigurationen von Webservern, Datenbanken usw.
- **Nicht benötigte Funktionen deaktivieren:** Funktionen auf die strikten Bedürfnisse der ausgesetzten Dienste beschränken.
- **Berechtigungen stärken:** Sicherstellen, dass ausgesetzte Dienste nur über die minimalen Berechtigungen verfügen, die sie zum Funktionieren benötigen.

Überwachung und Erkennung von Eindringlingen

Durch die kontinuierliche Überwachung der exponierten Dienste können Eindring- und Missbrauchsversuche erkannt werden:

- **Einrichten einer Intrusion-Detection-Lösung (IDS/IPS):** Eine IDS- (Intrusion Detection System) oder IPS-Lösung (Intrusion Prevention System) ermöglicht es, den Datenverkehr zu überwachen und bei verdächtigem Verhalten zu alarmieren.
- **Sicherheitsprotokolle analysieren:** Überwachen Sie Zugriffs- und Fehlerprotokolle, um anormales Verhalten zu erkennen.
- **Warnmeldungen über verdächtige Aktivitäten einrichten:** Richten Sie Warnmeldungen ein, um über anormale Anmeldeversuche, Brute-Force-Methode usw. benachrichtigt zu werden.

Schlussfolgerung

Die Sicherung von offengelegten Diensten im Internet ist ein fortlaufender Prozess, der ständige Aufmerksamkeit erfordert, um die Sicherheitsmassnahmen an neue Bedrohungen anzupassen. Dank der in diesem Abschnitt beschriebenen bewährten Verfahrensweisen können Institutionen die Risiken, die mit der Exponierung ihrer Dienste im Internet verbunden sind, deutlich reduzieren. Es wird ausserdem empfohlen, die Sicherheit der offengelegten Dienste regelmässig zu überprüfen und die Kontrollen an die technologischen Entwicklungen und neu identifizierten Bedrohungen anzupassen.

Verwaltung von Schwachstellen und Updates

Das Management von Schwachstellen und Updates ist entscheidend, um Computersysteme vor wachsenden Bedrohungen und gezielten Angriffen zu schützen. Eine nicht behobene Schwachstelle kann von Cyberkriminellen ausgenutzt werden, um sich unberechtigten Zugriff auf Systeme zu verschaffen, bösartigen Code auszuführen oder den reibungslosen Betrieb der Infrastruktur zu stören. Dieser Abschnitt beschreibt bewährte Verfahrensweisen, um Schwachstellen proaktiv und kontinuierlich zu identifizieren, zu priorisieren und zu beheben.

Prozess des Schwachstellenmanagements

Schwachstellenmanagement ist ein kontinuierlicher Prozess mit mehreren Stufen:

1. **Identifikation von Schwachstellen:** Verwenden Sie Vulnerability-Scanner, um Schwachstellen in Systemen, Anwendungen und Netzwerken zu identifizieren. Zu den gängigen Tools gehören Nessus, Qualys und OpenVAS. Regelmässige, mindestens monatliche Scans werden empfohlen, um einen aktuellen Überblick über die Schwachstellen zu behalten.
2. **Bewertung der Auswirkungen und Kritikalität:** Jede Schwachstelle muss nach ihren potenziellen Auswirkungen und ihrer Kritikalität bewertet werden. Standards wie das Common Vulnerability Scoring System (CVSS) ermöglichen die Priorisierung von Schwachstellen anhand ihres Schweregradscores (kritisch, hoch, mittel, niedrig).
3. **Priorisierung der Korrekturen:** Kritische Schwachstellen müssen vorrangig behoben werden. Kriterien für die Priorisierung sind u. a. der Schweregrad, die öffentliche Exposition des Systems und die potenziellen Auswirkungen auf den Betrieb der Organisation.
4. **Planung von Korrekturmassnahmen:** Erstellen Sie einen Zeitplan für die Behebung von Schwachstellen, wobei Sie besonders auf Sicherheitspatches achten sollten, die von Softwareherstellern und Entwicklern von Betriebssystemen bereitgestellt werden. Wichtige Änderungen müssen möglicherweise getestet werden, um Betriebsunterbrechungen zu vermeiden.
5. **Validierung und Tests nach den Korrekturen:** Nach dem Einspielen eines Patches sollte ein Test durchgeführt werden, um sicherzustellen, dass die Schwachstelle behoben wurde, ohne zusätzliche Probleme zu verursachen. Schwachstellen-Scans sollten wiederholt werden, um die effektive Behebung zu überprüfen.
6. **Dokumentation und Nachverfolgung:** Führen Sie ein Verzeichnis der identifizierten Schwachstellen, der angewandten Patches und der Validierungstests. Eine Nachverfolgung ermöglicht es, die durchgeführten Massnahmen nachzuvollziehen und die Effizienz des Schwachstellenmanagementprozesses zu messen.

Richtlinien für die Aktualisierung von Software und Systemen

Eine strenge Update-Politik verringert die Gefährdung durch bekannte Schwachstellen. Schlüsselelemente für ein effizientes Update-Management:

- **Automatisierung kritischer Updates:** Aktivieren Sie möglichst die automatische Installation von Updates für kritische Komponenten, insbesondere von Sicherheitspatches für Betriebssysteme und wichtige Anwendungen.
- **Geplante Aktualisierungen für kritische Systeme:** Legen Sie eine Aktualisierungsroutine für kritische Systeme und Anwendungen fest, die nicht automatisch aktualisiert werden können. Beispielsweise können Updates ausserhalb der Produktionszeiten geplant werden, um die Auswirkungen auf die Benutzer zu minimieren.
- **Tests vor der Bereitstellung:** Testen Sie bei kritischen Systemen die Updates in einer Vorproduktionsumgebung, bevor Sie sie in der Produktion anwenden. So können mögliche Konflikte oder Kompatibilitätsprobleme identifiziert werden.
- **Verwaltung von Patches für veraltete Geräte:** Einige Systeme oder Software erhalten möglicherweise keine Sicherheitsupdates mehr von den Herstellern. Betrachten Sie in diesen Fällen alternative Massnahmen wie Netzwerksegmentierung, Zugriffsbeschränkungen oder die Isolierung veralteter Systeme, um deren Gefährdung zu verringern.
- **Überwachung von Sicherheitsupdates:** Achten Sie kontinuierlich auf Veröffentlichungen von Patches und Sicherheitsbulletins von Software- und Hardwareherstellern. Beispielsweise veröffentlichen Microsoft, Adobe, Cisco und andere Hersteller regelmässig Sicherheits-Patches, die es zu überwachen gilt.

Automatisierung von Aktualisierungen und kontinuierliche Überwachung

Um die Effizienz und Geschwindigkeit beim Einspielen von Patches zu erhöhen, empfiehlt es sich, Teile des Aktualisierungsprozesses zu automatisieren:

- **Patch-Management-Tools:** Verwenden Sie Patch-Management-Tools (z. B. WSUS oder SCCM für Windows, Chef, Ansible), um Updates zentral und automatisiert anzuwenden. Mit diesen Tools können Sie die Installation von Updates auf allen Geräten planen, verfolgen und überprüfen.
- **Überwachung der Einhaltung von Patches:** Richten Sie ein Dashboard zur Verfolgung von Updates ein, um Systeme, die nicht den Sicherheitsrichtlinien entsprechen, schnell zu identifizieren. Systeme, die nicht auf dem neuesten Stand sind, müssen schnell identifiziert und behoben werden.
- **Echtzeit-Warnungen:** Richten Sie Warnmeldungen ein, um Versuche, bekannte Schwachstellen auszunutzen, zu erkennen und kritische Systeme, die nicht auf dem neuesten Stand sind, zu melden. Dies ermöglicht eine schnelle Reaktion auf eine aktive Bedrohung, die eine Schwachstelle ausnutzt.

Bewährte Verfahrensweisen für die Verwaltung von Schwachstellen und Updates

- **Benutzer und Mitarbeitende aufklären:** Informieren Sie die Benutzer über die Risiken von nicht aktualisierter Software und über allgemeine Sicherheitspraktiken. Die Wachsamkeit aller kann dazu beitragen, menschliche Fehler zu vermeiden, die Schwachstellen offenlegen könnten.

- **Kontinuierliches Feedback und Prozessverbesserung:** Beurteilen Sie regelmässig die Effizienz des Schwachstellenmanagements und der Updates, um mögliche Verbesserungen zu identifizieren. Führen Sie regelmässige Audits durch, um die Einhaltung bewährter Verfahrensweisen und die Kohärenz des Prozesses zu gewährleisten.
- **Periodische Überprüfung der Patch-Management-Strategie:** Die Aktualisierungsstrategie sollte regelmässig überprüft werden, um sicherzustellen, dass sie weiterhin an neue Bedrohungen und Entwicklungen in den von der Organisation verwendeten Systemen und Anwendungen angepasst ist.

Schutz von Arbeitsplätzen und Servern

Arbeitsplätze und Server sind kritische Bestandteile der Infrastruktur einer Organisation und häufig das bevorzugte Ziel von Cyberangriffen. Der Schutz dieser Elemente ist entscheidend, um das Risiko von Kompromittierungen, Datenverlusten und Betriebsunterbrechungen zu minimieren. In diesem Abschnitt werden bewährte Verfahrensweisen zum Schutz von Arbeitsplätzen und Servern vorgestellt. Dazu gehören der Einsatz von Antiviren- und Endpoint Detection and Response (EDR)-Lösungen, die Konfiguration geeigneter Sicherheitsrichtlinien und die strikte Verwaltung lokaler Privilegien.

Antiviren- und EDR-Lösungen (Endpoint Detection and Response)

Antiviren

- **Einrichtung eines hochwertigen Antivirenprogramms:** Auf alle Arbeitsplätze und Servern muss ein Antivirenprogramm installiert sein. Wählen Sie eine anerkannte Lösung, die regelmässig aktualisiert wird, um von den neuesten Bedrohungsdefinitionen zu profitieren.
- **Häufige Aktualisierungen:** Richten Sie die Arbeitsplätze so ein, dass Antiviren-Aktualisierungen automatisch durchgeführt werden, wodurch sichergestellt wird, dass neue Virensignaturen schnell integriert werden.
- **Regelmässige Scans:** Planen Sie regelmässige Scans (mindestens wöchentlich) den Arbeitsplätzen und Servern, um Anomalien oder schlummernde Malware zu erkennen.

Endpoint Detection and Response (EDR)

Als Alternative zu "klassischen" Antivirenlösungen kann man sich für eine EDR-Technologie entscheiden, die in den meisten Fällen effizienter ist. Im Vergleich zu einem Antivirenprogramm bietet eine EDR-Lösung unter anderem folgende Vorteile:

- **Erweiterte Erkennung:** EDR bietet eine kontinuierliche Überwachung von Endpunkten, um anormales Verhalten und aufkommende Bedrohungen zu erkennen, die von herkömmlichen Antivirenlösungen nicht erkannt werden.
- **Automatisierte Reaktion:** EDR-Lösungen sind in der Lage, automatisch zu reagieren, indem sie einen kompromittierten Endpunkt isolieren, bösartige Aktivitäten unterbrechen oder Echtzeit-Warnungen für Sicherheitsteams auslösen.
- **Untersuchungen nach Vorfällen:** Im Falle einer Kompromittierung ermöglicht EDR die Rückverfolgung des Angriffsvektors, die Identifizierung potenzieller Schwachstellen und die Durchführung von Analysen nach dem Vorfall, um den künftigen Schutz zu verstärken.

Konfiguration von Sicherheitsrichtlinien für Endpunkte

Strategie zur Stärkung (Hardening) von Endpunkten

- **Deaktivierung unnötiger Dienste:** Um die Angriffsfläche zu minimieren, deaktivieren Sie alle unwesentlichen Dienste und Protokolle auf den Arbeitsplätzen und Servern.
- **Konfiguration von lokaler Firewall-Richtlinien:** Verwenden Sie die in den Betriebssystemen integrierten Firewalls, um nicht bewilligte Verbindungen zu blockieren. Konfigurieren Sie strenge Regeln, um den ein- und ausgehenden Datenverkehr auf jedem Endpunkt zu beschränken.
- **Port- und Gerätekontrolle:** Beschränken Sie den Zugriff auf USB-Ports, CD-ROMs und andere physische Geräte, die häufig als Angriffsvektoren zum Einschleusen von Malware genutzt werden.

Verwaltung von Sicherheitsaktualisierungen (Patch Management)

- **Regelmässige Systemaktualisierung:** Stellen Sie sicher, dass alle Betriebssysteme und die auf den Arbeitsplätzen und Servern installierte Software auf dem neuesten Stand sind. Planen Sie automatische Updates, um bekannte Schwachstellen zu vermeiden.
- **Testen kritischer Updates:** Bevor Sie grössere Updates bereitstellen, führen Sie Tests in einer Testumgebung durch, um die Kompatibilität zu überprüfen und Betriebsunterbrechungen zu vermeiden.

Verwendung einer Festplattenverschlüsselung

Bei Diebstahl oder Verlust der Geräte sorgt die Verschlüsselung der Laufwerke dafür, dass die Daten nicht von unbefugten Dritten gelesen werden können. Verwenden Sie Verschlüsselungslösungen wie BitLocker für Windows oder FileVault für macOS.

Bewährte Verfahrensweisen für die Verwaltung lokaler Privilegien

- **Principle of Least Privilege (POLP):** Die Benutzer sollten nur die Rechte haben, die sie zur Erfüllung ihrer Aufgaben benötigen. Beschränken Sie administrative Privilegien auf Benutzer mit besonderen Bedürfnissen, um das Risiko einer Verbreitung im Falle einer Kompromittierung zu verringern.
- **Trennung von administrativen und Standardkonten:** Verlangen Sie, dass Benutzer mit administrativen Rechten ein separates Konto für administrative Tätigkeiten und ein Standardkonto für alltägliche Aufgaben haben. Dies verringert das Risiko, dass Malware mit hohen Rechten ausgeführt wird.
- **Kontrolle des temporären Verwaltungszugriffs:** Wenn für eine bestimmte Aufgabe hohe Rechte erforderlich sind, gewähren Sie temporäre Rechte über einen Genehmigungsprozess. Verwenden Sie Lösungen zur Verwaltung von Privilegien, um diesen Prozess zu automatisieren, den temporären Zugriff zu beschränken und die durchgeführten Aktionen zu protokollieren.
- **Überwachung und Prüfung privilegierter Aktivitäten:** Richten Sie detaillierte Aktivitätsprotokolle ein, um die Handlungen von Benutzern mit hohen Rechten zu verfolgen. Analysieren Sie diese Protokolle regelmässig, um anormales Verhalten oder Kompromittierungsversuche zu erkennen.

Verstärkte Sicherheit von Benutzersitzungen

- **Automatische Sitzungssperre:** Konfigurieren Sie Arbeitsplätze und Server so, dass sie sich nach einer bestimmten Zeit der Inaktivität automatisch sperren. Dies verringert das Risiko eines unberechtigten Zugriffs, wenn die Benutzer ihre Arbeitsplätze verlassen.
- **Multi-Faktor-Authentifizierung (MFA):** Aktivieren Sie die MFA für alle Benutzer, insbesondere für solche mit hohen Rechten, um die Authentifizierung zu verstärken und das Risiko eines Zugriffs durch kompromittierte Passwörter zu minimieren.
- **Überwachung von Anmeldeversuchen:** Implementieren Sie Warnmeldungen und Sperren bei wiederholten fehlgeschlagenen Anmeldeversuchen, um Brute-Force-Angriffe zu erkennen und zu verhindern.

Verwaltung privilegierter Zugänge

Privileged Access Management (PAM) ist ein wichtiger Bereich der IT-Sicherheit und besonders kritisch für Institutionen, die ihre sensibelsten Bestände schützen wollen. Privilegierte Konten wie Administratorkonten, Dienstkonten und andere Benutzer mit weitreichenden Berechtigungen sind ein beliebter Angriffsvektor für Cyberkriminelle. Daher ist ein strukturierter und methodischer Ansatz für ihre Verwaltung unerlässlich, um die Sicherheit des Informationssystems zu gewährleisten.

Einführung in die Verwaltung privilegierter Konten

- **Definition:** Privilegierte Konten sind Konten mit erweiterten Zugriffsrechten auf Informationssysteme, die es ihnen ermöglichen, administrative Aufgaben wie die Installation von Software, die Verwaltung von Konfigurationen und die System-administration zu erledigen.
- **Sicherheitsaspekte:** Eine Kompromittierung dieser Konten kann weitreichende Folgen haben, die vom unberechtigten Zugriff auf sensible Daten bis hin zur Manipulation kritischer Konfigurationen oder der Verbreitung von Bedrohungen im gesamten Netzwerk reichen können.

Sicherheitsgrundsätze für Konten mit hohen Privilegien

- **Least-Privilege-Prinzip:** Jeder Benutzer oder jedes Konto sollte nur über minimalen Berechtigungen verfügen, die zur Erfüllung der Aufgaben benötigt sind. Dies verringert das Risiko im Falle einer Kompromittierung.

- **Aufgabentrennung:** Der Zugriff auf hohe Rechten sollte so verteilt werden, dass nicht eine einzige Person kritische Aktionen ohne Aufsicht oder Kontrolle durchführen kann.

- **Zentrale Verwaltung privilegierter Konten:** Der Einsatz von PAM-Lösungen ermöglicht eine zentrale Zugriffsverwaltung, eine Echtzeitüberwachung und eine Verringerung der Risiken, die mit hochprivilegierten Konten verbunden sind.

Identifizierung und Klassifizierung von privilegierten Konten

- **Kartierung der Konten:** Führen Sie eine umfassende Bestandsaufnahme der vorhandenen privilegierten Konten durch, einschliesslich lokaler Konten, Domänenkonten, Dienstkonten und von Anwendungen verwendete Konten.

- **Zugriffsklassifizierung:** Kategorisierung von Konten nach Zugriffsebene, Bedeutung und Verwendungszweck (Netzwerkverwaltungskonten, Anwendungskonten, Dienstkonten usw.).

- **Bewertung der damit verbundenen Risiken:** Analysieren Sie die potenziellen Auswirkungen einer Kompromittierung jedes Kontotyps, um die Sicherheitsmassnahmen zu priorisieren.

Implementierung einer PAM-Lösung (Privileged Access Management)

- **Verwaltung privilegierter Passwörter:** Nutzen Sie sichere Safe, um Passwörter privilegierter Konten zu speichern, zu verwalten und den Zugriff darauf zu kontrollieren. PAM-Lösungen ermöglichen auch die automatische Änderung von Passwörtern nach ihrer Verwendung, um die Sicherheit zu erhöhen.
- **Just-in-Time-Zugriffskontrolle (JIT):** Vorübergehende Zugriffsgewährung für die Ausführung bestimmter Aufgaben, wobei die Rechte nach der Nutzung automatisch entzogen werden.
- **Session Management:** Aufzeichnung und Überwachung von Sitzungen, die von privilegierten Konten initiiert werden, um eine bessere Nachvollziehbarkeit und Kontrolle der durchgeführten Aktionen zu ermöglichen.
- **Doppelte Authentifizierung:** Verlangen Sie eine starke Authentifizierung (z. B. Multi-Faktor-Authentifizierung) für den Zugriff auf privilegierte Konten.

Überwachung und Prüfung der Aktionen privilegierter Benutzer

- **Kontinuierliche Überwachung:** Richten Sie Echtzeit-Überwachungstools ein, um die Aktivitäten von privilegierten Benutzern zu verfolgen und aufzuzeichnen. So kann verdächtiges Verhalten schnell erkannt werden.
- **Regelmässige Audits:** Führen Sie regelmässige Sicherheitsaudits durch, um sicherzustellen, dass die Richtlinien für die Verwaltung privilegierter Zugriffe eingehalten werden und die Sicherheitskontrollen ordnungsgemäss funktionieren.
- **Logs und Berichte:** Bewahren Sie die Zugriffs- und Aktivitätsprotokolle der privilegierten Benutzer in einem sicheren und unveränderlichen Format auf, das bei Bedarf eine nachträgliche Analyse ermöglicht.

Richtlinien für die Überprüfung privilegierter Konten

- **Regelmässige Überprüfung:** Beurteilen Sie regelmässig die Zugriffsbedürfnisse der Benutzer und entfernen oder ändern Sie die Rechte von Konten, die nicht mehr benötigt werden.
- **Automatische Deaktivierung:** Führen Sie Richtlinien für die automatische Deaktivierung von Konten ein, die über einen bestimmten Zeitraum nicht genutzt werden.
- **Kontrolle verwaister Konten:** Stellen Sie sicher, dass Konten, die von ehemaligen Mitarbeitenden oder Auftragnehmern eingerichtet wurden, nicht aktiv bleiben, insbesondere Konten mit hohen Rechten.

Sicherheit von Dienst- und Anwendungskonten

- **Verwaltung von Dienst-IDs:** Ersetzen Sie statische Passwörter für Dienstkonten durch Kennungen, die dynamisch von einer PAM-Lösung verwaltet werden.
- **Sichere Authentifizierung:** Verwenden Sie starke Authentifizierungsmechanismen oder die Integration mit Zertifikaten und sicheren Schlüsseln für Anwendungskonten.

- **Aktualisierung der IDs:** Ändern Sie die IDs regelmässig und stellen Sie sicher, dass sie im Quellcode von Anwendungen nicht fest codiert sind.

Aufklärung und Sensibilisierung der privilegierten Benutzer

- **Spezifische Ausbildungen:** Bieten Sie spezifische Ausbildungen für Benutzer mit erweiterten Rechten an, wobei der Schwerpunkt auf der sicheren Verwaltung ihrer Zugänge und der Erkennung potenzieller Bedrohungen liegt.
- **Angemessene Sicherheitsrichtlinien:** Erstellen Sie klare Richtlinien über erwartetes Verhalten, Einschränkungen und bewährte Verfahrensweisen für Benutzer mit privilegiertem Zugriff.

Überwachung und Monitoring der Infrastruktur

Einführung in die Infrastrukturüberwachung

Die Überwachung der IT-Infrastruktur ist ein zentraler Pfeiler der Systemsicherheit. Das Ziel ist, kritische Ereignisse, die sich auf die Sicherheit oder Verfügbarkeit von IT-Diensten auswirken können, zu sammeln, zu analysieren und zu alarmieren. Durch die schnelle Erkennung von Sicherheitsvorfällen und Betriebsanomalien verkürzt die Überwachung die Reaktionszeit und begrenzt die Auswirkungen von Bedrohungen.

Ziele der Überwachung

Die Hauptziele der Infrastrukturüberwachung sind:

- Frühzeitige Erkennung von Bedrohungen und potenziellen Angriffen
- Analyse von Ereignissen, um verdächtige Aktivitäten zu identifizieren
- Verkürzung der Reaktionszeiten auf Vorfälle
- Überwachung der Leistung und Verfügbarkeit von Diensten
- Verstärkte Einhaltung der regulatorischen Anforderungen

Überwachungsarten

Bei der Überwachung der Infrastruktur sind mehrere Aspekte zu beachten:

Überwachung von Ereignisprotokollen (Logs)

Die Erhebung und die Analyse von Protokollen von Servern, Anwendungen, Netzwerkgeräten, Firewalls und anderen Systemen sind für einen vollständigen Einblick unerlässlich. Anhand der Protokolle lassen sich Anomalien, unberechtigte Zugriffe und andere verdächtige Verhaltensweisen erkennen.

Netzwerk-Monitoring

Die Überwachung des Netzwerkverkehrs hilft, Anomalien zu erkennen, z. B. ungewöhnliche Spitzen im Datenverkehr, Kommunikation mit bösartigen Websites oder Eindringversuche. Tools wie Intrusion Detection/Prevention Systems (IDS/IPS) können diese Überwachung verstärken.

Überwachung der Systemintegrität

Dazu gehört die Überprüfung kritischer Dateien auf Servern oder Anwendungen auf unbefugte Veränderungen, die auf eine Kompromittierung hindeuten können.

Leistungs- und Verfügbarkeitsüberwachung

Leistungsindikatoren (CPU, Speicher, Verfügbarkeit von Diensten, Reaktionszeit) müssen überwacht werden, um sicherzustellen, dass die Systeme reibungslos funktionieren. Ein plötzlicher Leistungsabfall kann auf einen bevorstehenden Angriff oder Ausfall hinweisen.

Überwachung der Aktivitäten privilegierter Benutzer

Die Handlungen von Benutzern mit hohen Rechten müssen kontinuierlich überwacht werden, um Missbrauch zu verhindern und verdächtige Verhaltensweisen zu erkennen. Dazu gehören kritische Konfigurationsänderungen, nicht autorisierte Zugriffe oder Versuche, die Sicherheitsrichtlinien zu umgehen.

Tools zur Überwachung

Um eine effektive Überwachung zu gewährleisten, können verschiedene Tools und Technologien eingesetzt werden:

Systeme zur Verwaltung von Sicherheitsereignissen und -informationen (SIEM)

Ein SIEM zentralisiert Logs aus mehreren Quellen, korreliert Ereignisse, alarmiert, wenn verdächtige Aktivitäten entdeckt werden und hilft bei der Analyse von Sicherheitsvorfällen. Diese Lösungen sind für einen einheitlichen Echtzeitüberblick über die Sicherheit der Infrastruktur unerlässlich.

Netzwerk- und System-Monitoring-Tools

Lösungen wie Nagios, Zabbix oder integrierte Cloud-Plattformen ermöglichen es, die Verfügbarkeit und Leistung von Diensten zu überwachen, Warnmeldungen bei Vorfällen zu generieren und Ausfälle zu antizipieren.

Systeme zur Erkennung von Eindringlingen (IDS/IPS)

Diese Systeme analysieren den Netzwerkverkehr und die Pakete in Echtzeit, identifizieren bekannte Angriffe (über Signaturen) oder anormales Verhalten (über heuristische Analysen).

Wichtigste Schritte zur Einrichtung einer effizienten Überwachung

Bewertung von Bedürfnissen und Risiken

Auffassung der Risiken und spezifischen Anforderungen der Systeme und Daten der Institution.

Definition von Schlüsselindikatoren (KPIs) und Warnschwellen

Bestimmung der Ereignisse, die eine Warnung auslösen sollen und ab welchen Schwellenwerten ein Eingreifen erforderlich ist.

Implementierung von Lösungen zur Sammlung von Logs

Zentralisierte Sammlung der Protokolle aller kritischen Quelle. Stellen Sie sicher, dass die Protokolle mit Zeitstempel versehen und gemäss den gesetzlichen Anforderungen aufbewahrt werden.

Implementierung einer Lösung zur Ereigniskorrelation (SIEM)

Korrelation der Daten aus verschiedenen Quellen, um bösartige Verhaltensweisen zu erkennen.

Kontinuierliche Überwachung und Aktualisierung von Richtlinien

Die Überwachungskonfigurationen müssen bei neuen Bedrohungen und Änderungen der Infrastruktur aktualisiert werden. Falsche Warnungen sollten reduziert werden, um sicherzustellen, dass nur relevante Warnungen untersucht werden.

Reaktion auf Vorfälle, die durch das Monitoring festgestellt wurden

Verwaltung von Warnungen

Alle Warnungen müssen bewertet, kategorisiert und untersucht werden, um festzustellen, ob sie eine echte Bedrohung darstellen.

Reaktionsverfahren für Vorfälle

Wenn ein Vorfall entdeckt wird, müssen Reaktionsverfahren schnell angewendet werden. Dazu gehören die Isolierung der kompromittierten Systeme, die Untersuchung, die Behebung der Schwachstelle und die Kommunikation mit den Beteiligten.

Überprüfung nach einem Vorfall

Jeder Vorfall sollte einer Post-Mortem-Analyse unterzogen werden, um die Ursachen zu verstehen, die Wirksamkeit der Reaktion zu bewerten und die Verfahren zu verbessern.

Bewährte Überwachungsverfahrensweisen

Automatisierung von wiederkehrenden Aufgaben

Verwenden Sie Skripte und Tools, um die Sammlung von Daten, die Korrelation von Ereignissen und die Reaktion auf bestimmte Warnungen zu automatisieren.

Regelmässige Überprüfung von Konfigurationen

Die Konfigurationen der Monitoringstools müssen regelmässig überprüft werden, um sicherzustellen, dass sie auch bei neuen Bedrohungen relevant und wirksam bleiben.

Weiterbildung der Betreiber

Die für die Überwachung zuständigen Personen müssen kontinuierlich ausgebildet werden, um neue Bedrohungen zu erkennen, Tools effektiv zu nutzen und bewährte Verfahrensweisen zur Reaktion auf Vorfälle einzuhalten.

Schlussfolgerung

Die Überwachung und das Monitoring der Infrastruktur sind dynamische Prozesse, die kontinuierliche Aufmerksamkeit erfordern, um einen wirksamen Schutz der Systeme und Daten zu gewährleisten. Durch die Kombination von Tools, Prozessen und menschlichem Fachwissen können Institutionen Risiken reduzieren, ihre Reaktionsfähigkeit verbessern und die Sicherheit ihrer Infrastruktur gewährleisten.

Ausbildung und Sensibilisierung der Benutzer

Die Sensibilisierung und die Ausbildung der Benutzer sind eine der wichtigsten Komponenten, um eine robuste Cybersicherheit in spezialisierten Institutionen zu gewährleisten. Ein Grossteil der erfolgreichen Cyberangriffe beruht auf menschlichen Fehlern, wie der Preisgabe sensibler Daten, dem Ausführen bösartiger Anhänge oder der Wiederverwendung schwacher Passwörter. Daher ist es wesentlich, durch regelmässige und gezielte Ausbildungen eine solide Cybersicherheitskultur zu schaffen. In diesem Abschnitt wird ein strukturierter Ansatz zur Entwicklung und Aufrechterhaltung eines Sensibilisierungsprogramms für Cybersicherheit in Institutionen vorgestellt.

Ziele der Sensibilisierung für Cybersicherheit

- **Stärkung des Bedrohungsbewusstseins:** Informieren Sie die Benutzer über aktuelle Cyberbedrohungen wie Phishing, Ransomware, Malware und gezielte Angriffe.
- **Praktische Fähigkeiten entwickeln:** Vermitteln Sie praktische Massnahmen und sichere Verhaltensweisen, die zur Risikominimierung angewendet werden können.
- **Förderung einer Sicherheitskultur:** Ermutigung zu ständiger Wachsamkeit und proaktivem Melden von Vorfällen.
- **Einhaltung gesetzlicher Vorschriften:** Sicherstellen, dass die Mitarbeitende die geltenden gesetzlichen Normen und Anforderungen einhalten.

Inhalt der Ausbildung

Die Ausbildung muss folgende Aspekte abdecken:

- Sicherheit von Passwörtern:
  - Erstellung starker Passwörter und Verwendung von Passwortmanagern
  - Richtlinien für die Änderung von Passwörtern und Sensibilisierung für die Nichtwiederverwendung
- Erkennen von Phishing- und Betrugsversuchen:
  - Identifikation verdächtiger E-Mails, SMS und Anrufe
  - Verfahren zur Überprüfung der Echtheit von Absendern und Nachrichten
- Sichere Nutzung von E-Mails und Nachrichten:
  - Guter Umgang mit Anhängen und Links in E-Mails
  - Verhinderung des Austauschs sensibler Daten
- Sicherheit von persönlichen und mobilen Geräten (BYOD):
  - Richtlinien für die sichere Nutzung von Mobilgeräten, die mit dem Netzwerk der Institution verbunden sind

  - Installation und Nutzung von Schutzlösungen wie Antivirenprogrammen oder EDR-Lösungen (Endpoint Detection and Response)
- Physischer Zugang zu Systemen:
  - Schutz von Arbeitsplätzen durch automatische Sperrbildschirme
  - Überwachung sensibler Bereiche und Einhaltung von Zugangsrichtlinien
- Sicherheit von Netzwerkverbindungen:
  - Best Practices für die Verbindung mit öffentlichen oder ungesicherten Wi-Fi-Netzwerken
  - Verwendung von VPNs beim Zugriff auf sensible Systeme
- Updates und Patchmanagement:
  - Relevanz, die Systeme mit Sicherheitspatches auf dem neuesten Stand zu halten
  - Prozess, um Aktualisierungen auf sichere Weise anzuwenden
- Verwendung von USB-Sticks und externen Geräten:
  - Sensibilisierung für die Gefahren unbekannter oder nicht zugelassener Geräte
  - Richtlinie zur Validierung von Geräten vor der Verwendung

Methoden zur Sensibilisierung

- **Regelmässige Sensibilisierungskampagnen:** Durchführung regelmässiger thematischer Kampagnen, um an Sicherheitsprinzipien zu erinnern (z. B. "Monat der Cybersicherheit").

- **Interaktive Ausbildungen:** Präsenz- oder Online-Schulungen mit praktischen Demonstrationen, Fallstudien, Fragen und Antworten und praktischen Workshops.

- **E-Learning-Module:** Zugang zu Online-Modulen, damit die Mitarbeitende in ihrem eigenen Tempo lernen können.

- **Simulierte Angriffe:** Organisation von Phishing-Simulationskampagnen, um die Wachsamkeit der Benutzer zu testen und zu erhöhen.

- **Sicherheitsbulletins:** Verbreitung regelmässiger Bulletins mit Informationen über aufkommende Bedrohungen, bewährte Verfahrensweisen und beobachtete Erfolge.

- **Schulungspakete für neue Mitarbeitende:** Integration der Sensibilisierung für Cybersicherheit, sobald neue Mitarbeitende in die Institution aufgenommen werden.

Überwachung und Bewertung der Wirksamkeit der Ausbildung

- **Fragebögen und Tests:** Regelmässige Bewertung der Kenntnis der Benutzer, um das Verständnis der Konzepte zu messen.
- **Verhaltensanalysen:** Überwachung des Benutzerverhaltens (z. B. Reaktionen auf Phishing-Tests), um die Übernahme der gelehrten Verfahren zu bewerten.
- **Lernberichte:** Verfolgen Sie die Teilnahmequoten an Ausbildungen, Testergebnisse und der Gesamtentwicklung.

- **Kontinuierliche Verbesserung:** Anpassung der Ausbildungsinhalte an neue Bedrohungen, vergangene Vorfälle und Benutzerfeedback.

Engagement der Geschäftsleitung

Um sicherzustellen, dass alle Benutzer mitmachen, ist es wichtig, dass sich die Leitung aktiv einbringt, indem sie Sensibilisierungsprogramme unterstützt und daran teilnimmt. Dies trägt dazu bei, eine Kultur der Cybersicherheit zu etablieren und zeigt, wie wichtig der Schutz der Systeme und Daten der Institution ist.

Verwaltung von externen IT-Anbietern

Die spezialisierten Institutionen des Kantons Freiburg beauftragen häufig externe IT-Dienstleister um einen Teil oder die gesamten IT-Infrastruktur, insbesondere mit dem Hosting der Systeme, der Verwaltung von Cloud-Diensten, der Netzwerkverwaltung und der Cybersicherheit, zu verwalten. Ein sorgfältiges Management dieser Dienstleister ist wesentlich, um die Sicherheit der Systeme und den Schutz sensibler Daten zu gewährleisten.

Identifizierung von Anbietern und ausgelagerten Diensten

Bevor Sie einen Dienstleister beauftragen, ist es entscheidend, die Bedürfnisse und Verantwortlichkeiten aller beteiligten Akteure genau zu definieren. Hier die wichtigsten Kategorien ausgelagerter Dienstleistungen:

- **Beherbergung und Speicherung von Daten:** Data centers, cloud providers (Microsoft 365, AWS, Google Cloud).
- **Verwaltung der IT-Infrastrukturen:** Serververwaltung, Virtualisierung, Netzwerkwartung.
- **IT-Sicherheit:** Security Operations Center (SOC), Verwaltung von Firewalls, Sicherheitsauditdienste.
- **Support und Benutzerunterstützung:** Helpdesk, technische Wartung.
- **Anwendungsentwicklung und -wartung:** Spezifische Softwaredienste, Aktualisierungen interner Anwendungen.

Jede Institution muss eine detaillierte Bestandsaufnahme der beteiligten Anbieter und der von ihnen erbrachten Dienstleistungen erstellen.

Auswahl und Bewertung von IT-Anbietern

Bevor Sie einen Anbieter beauftragen, sollte unbedingt eine strenge Auswertung durchgeführt werden, die auf folgenden Kriterien beruht:

- Erfahrung und Ruf: Überprüfung von Referenzen und Zertifizierungen im Bereich Cybersicherheit (ISO 27001, SOC 2 usw.).
- Einhaltung gesetzlicher Vorschriften: Einhaltung der in der Schweiz geltenden Normen (DSGVO, DSG, kantonale Regelungen).
- Angebotenes Sicherheitsniveau: Zugriffsverwaltung, Datenschutz, Sicherung von Umgebungen.
- Vertragliche Verpflichtungen und Sicherheitsklauseln:
    - Service Level Agreements (SLAs)
    - Verpflichtungen in Bezug auf Kontinuität und Notfallwiederherstellung (BCP/DRP)

- Prozess zur Bewältigung von Vorfällen und Datenlecks

Es kann ein vorgängiges Audit durchgeführt werden, um die Cybersicherheitsreife des Anbieters zu bewerten.

Verträge und Service Level Agreements (SLAs)

Die Verträge mit den Anbietern sollten spezifische Klauseln enthalten, die den Schutz der digitalen Vermögenswerte der Institution gewährleisten:

- Festlegung von Verantwortlichkeiten: Wer ist für was zuständig (Systemaktualisierung, Monitoring, Zugriffsverwaltung usw.)?
- Verfügbarkeit und Leistung: Verpflichtungen zu Reaktionszeiten und Lösungen bei Vorfällen.
- Sicherheit und Compliance:
  - Schutz sensibler Daten und Verschlüsselungsanforderungen.
  - Verpflichtungen zum Umgang mit Sicherheitsvorfällen.
  - Recht auf Prüfung und regelmässige Kontrolle durch die Kundeninstitution.
- Verwaltung von Zugriff und Vertraulichkeit:
  - Strenge Regeln für den Zugang zu kritischen Infrastrukturen.
  - Verpflichtung zur Einrichtung starker Authentifizierungsmechanismen (MFA).
  - Verfahren zum Widerruf von Zugriffen bei Vertragsende oder Zuweisungswechsel.
- Kontinuitäts- und Notfallwiederherstellungsplan (BCP/DRP):
  - Verpflichtungen des Auftragnehmers im Falle einer grösseren Panne.
  - Regelmässige Tests der Wiederherstellungspläne, um ihre Wirksamkeit zu gewährleisten.

Überwachung und Prüfung von Anbietern

Sobald Sie einen Anbieter ausgewählt haben, ist es unerlässlich, dessen Sicherheitsniveau und die Einhaltung der vertraglichen Verpflichtungen kontinuierlich zu überwachen:

- **Regelmässige Cybersicherheitsprüfung:** Überprüfung der Einhaltung von Sicherheitsrichtlinien.
- **Zugriffskontrolle und Logs:** Überwachung der Verbindungen und Aktionen, die von den Anbietern durchgeführt werden.
- **Kontinuierliche Leistungsauswertung:** Analyse von Schlüsselindikatoren (Reaktionszeit auf Vorfälle, Verfügbarkeit von Diensten usw.).
- **Einbruchstests und Schwachstellenscans:** Durchführung von technischen Bewertungen, um mögliche Schwachstellen zu identifizieren.

Vorfall-Management und Reversibilität der Leistungen

Wenn ein Auftragnehmer in einen Cybersicherheitsvorfall verwickelt ist, muss ein strukturierter Managementprozess eingerichtet werden:

Identifikation und Meldung:

- Fristen und Verfahren für die Meldung von Vorfällen.
- Koordination zwischen dem Anbieter und der Institution.

Analyse und Auflösung:

- Korrekturmassnahmen und Behebungsplan.
- Dokumentation der Ursachen und Erkenntnisse.

Kommunikation und Berichterstattung:

- Information von Beteiligten und zuständigen Behörden, falls erforderlich.
- Einhaltung der gesetzlichen Anforderungen im Falle eines Datenverlusts.

Schliesslich sollte im Vertrag ein Reversibilitätsplan vorgesehen werden, um bei strategischen Veränderungen einen reibungslosen Übergang zu einem anderen Anbieter oder eine interne Rückkehr zu gewährleisten.

Pläne für Kontinuität und Reaktion auf Vorfälle

Erstellung eines Incidents Response Plan (IRP)

Der Incidents Response Plan (IRP) ist ein strategisches Dokument, das sicherstellen soll, dass die Organisation Sicherheitsvorfälle schnell erkennen, bewerten und auf sie reagieren kann. Ein klarer IRP ist entscheidend, um den durch einen Vorfall verursachten Schaden zu begrenzen und den normalen Betrieb so schnell wie möglich wiederherzustellen.

Ziele des Incidents Response Plans

- **Frühzeitige Erkennung von Sicherheitsvorfällen:** Überwachung von Systemen, Protokollen und Datenströmen, um anormales Verhalten schnell zu erkennen.
- **Wirksame Koordination:** Führen Sie Verfahren ein, um sicherzustellen, dass jeder beteiligte Akteur seine Rolle und seine Verantwortlichkeiten kennt.
- **Folgenminderung:** Verhindern von Vorfällen, um Schäden für die Organisation, ihre Systeme und Daten zu begrenzen.
- **Schnelle Wiederherstellung:** Festlegen von Schritten, um den Betrieb so schnell wie möglich nach der Lösung des Vorfalls wieder auf den Normalzustand zurückzusetzen.
- **Kontinuierliche Verbesserung:** Bewerten Sie jeden Vorfall, um daraus zu lernen und die Präventivmassnahmen zu verstärken.

Wesentliche Elemente des Plans zur Reaktion auf Vorfälle

- **Incident Response Team (IRT):** Bildung eines Teams aus entscheidenden Mitgliedern, das je nach Situation, die Geschäftsleitung, IT-Manager, IT-Sicherheit und gesetzliche Vertreter umfasst.
- **Erkennungs- und Meldeprozess:** Verfahren, um Vorfälle zu erkennen und schnell zu melden.
- **Auswertung des Vorfalls:** Identifizieren Sie die Art, das Ausmass und die Schwere des Vorfalls.
- **Eindämmungsmassnahmen:** Ergreifen von Massnahmen, um die Ausbreitung des Vorfalls einzuschränken.
- **Analyse nach einem Vorfall:** gründliche Untersuchung der Ursachen des Vorfalls, seiner Auswirkungen und der möglicherweise ausgenutzten Schwachstellen.
- **Berichterstattung und Dokumentation:** Dokumentieren Sie jeden Schritt, jede Entscheidung und die Ergebnisse, um eine solide Grundlage für die Erkenntnisse und zukünftige Prüfungen zu schaffen.

Regelmässige Tests der Verfahren zur Reaktion auf Vorfälle

Die blosse Erstellung eines Plans reicht nicht aus; es ist entscheidend, ihn regelmässig zu testen, um seine Wirksamkeit sicherzustellen. Durch die Tests wird überprüft, ob die Teammitglieder ihre Rollen kennen, und es wird bewertet, wie robust die Prozesse sind.

Test-Methoden

- **Simulierte Vorfälle:** Durchführung von simulierten Übungen auf der Grundlage realistischer Szenarien.
- **Tabletop exercises:** Übungen, bei denen die IRT-Mitglieder theoretisch diskutieren und festlegen, welche Massnahmen als Reaktion auf ein bestimmtes Szenario zu ergreifen sind.
- **Regelmässige Tests:** Planen Sie Tests in regelmässigen Abständen (vierteljährlich oder jährlich).

Auswertung der Testergebnisse

- **Leistungsbericht:** Analyse der Geschwindigkeit der Erkennung und der Reaktion.
- **Erfahrungsaustausch (RETEX):** Organisieren Sie Sitzungen, um zu identifizieren, was funktioniert hat, was nicht funktioniert hat und welche Verbesserungen eingeführt werden können.
- **Aktualisierung des Plans:** Anpassung des Plans auf der Grundlage des erhaltenen Feedbacks, um erkannte Lücken oder Ineffizienzen zu beheben.

Strategien für Notfallwiederherstellung (DRP) und Geschäftskontinuität (BCP)

Die Geschäftskontinuität muss auch bei einem grösseren Zwischenfall gewährleistet sein. Dazu gehört die Planung von Disaster Recovery (DRP) und Business Continuity (BCP), beides massgebende Komponenten, um die Auswirkungen einer grösseren Unterbrechung auf den Geschäftsbetrieb zu minimieren.

Disaster Recovery Plan (DRP)

- **Ziel:** kritische Systeme so schnell wie möglich wieder in einen funktionsfähigen Zustand zu versetzen.
- **Business Impact Analysis (BIA):** Ermittlung der Kernprozesse der Institution und ihrer Abhängigkeit von Systemen und Daten.
- **Ausweichstandorte:** Planen Sie Backup- oder Ausweichstandorte, an denen kritische Aktivitäten untergebracht werden können, wenn die Haupteinrichtungen ausfallen.
- **Strategien für die Datensicherung:** Sicherstellen, dass die Datensicherungen aktualisiert, geschützt und schnell wiederherstellbar sind.

Business Continuity Plan (BCP)

- **Risikoauswertung:** Ermittlung der wahrscheinlichsten Risiken und ihrer potenziellen Auswirkungen.

- **Planung von Kontinuitätsszenarien:** Umsetzung von Strategien, um kritische Funktionen trotz Störungen in Betrieb zu halten.
- **Kommunikation in Krisenzeiten:** Einführung von Protokollen zur Information interner und externer Stakeholder (Kunden, Partner usw.).
- **Einarbeitung und Sensibilisierung:** Sicherstellen, dass alle Mitarbeitende das BCP kennen und wissen, wie sie bei einer grösseren Störung reagieren müssen.

Koordination mit Dritten

Die Institutionen müssen auch eng mit ihren Dienstleistern, Technologieanbietern und anderen externen Stakeholder zusammenarbeiten, um eine koordinierte und harmonisierte Reaktion auf Vorfälle zu gewährleisten, insbesondere in Fällen, in denen Systeme oder Daten ausgelagert werden.

Schlussfolgerung

Die Entwicklung und Aufrechterhaltung von Incident Response Plänen und Geschäftskontinuitätsplänen sind Grundpfeiler der organisatorischen Widerstandsfähigkeit im Bereich der Cybersicherheit. Kontinuierliche Wachsamkeit, regelmässiges Testen und die Verbesserung von Prozessen gewährleisten eine bessere Widerstandsfähigkeit gegenüber sich entwickelnden Bedrohungen. Dieser Prozess erfordert die Zusammenarbeit der gesamten Institutionen, um ein optimales Sicherheitsniveau aufrechtzuerhalten und die Kontinuität des Betriebs zu gewährleisten.

Einhaltung von Vorschriften und Prüfung

Die Einhaltung gesetzlicher Vorschriften und die Prüfung der IT-Sicherheit sind massgebende Komponenten, um sicherzustellen, dass die Institutionen die geltenden Gesetze, Regulierungen sowie die Industriestandards für den Schutz von Daten und IT-Systemen einhalten. Dieser Abschnitt bietet einen Rahmen, um sicherzustellen, dass die Sicherheitsmassnahmen konform sind, dokumentiert und regelmässig geprüft werden, um Abweichungen oder unerkannte Risiken zu verhindern.

Einhaltung von Gesetzen und Vorschriften

Die Einhaltung von Gesetzen und Vorschriften ist eine unumgängliche Verantwortung für jede Institution, die mit sensiblen Daten umgeht, seien es persönliche Daten, Finanzinformationen oder Gesundheitsdaten. Die Institutionen des Kantons Freiburg müssen insbesondere folgende Vorschriften einhalten:

Die Datenschutzgrundverordnung (DSGVO): Diese EU-Verordnung stellt strenge Anforderungen an die Erhebung, die Verarbeitung und den Schutz personenbezogener Daten. Die Institutionen müssen:

- Die Verarbeitung personenbezogener Daten urkundlich belegen.
- Sicherheitsmassnahmen einführen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten.
- Einen Datenschutzbeauftragten ernennen, falls erforderlich.
- Sicherstellen, dass Datenübertragungen ausserhalb der EU den Bestimmungen der DSGVO entsprechen.

Schweizer Datenschutzgesetze (DSG): Zusätzlich zur DSGVO müssen Institutionen auch lokale Gesetze wie das neue DSG einhalten, die ähnliche Verpflichtungen auferlegen, insbesondere:

- Transparenz und Information der betroffenen Personen.
- Die Einhaltung der Rechte von Personen (Zugang, Berichtigung, Löschung usw.).
- Die Pflicht, Verletzungen personenbezogener Daten der zuständigen Behörde zu melden.

Industriestandards und Normen: Je nach Tätigkeit der Institutionen können bestimmte Branchenstandards gelten (z. B. ISO/IEC 27001 für das Management der Informationssicherheit, PCI-DSS für Zahlungen mit Karten).

Entwicklung einer Compliance-Politik

Die Institutionen müssen eine klar definierte Compliance-Politik verabschieden, in der die spezifischen regulatorischen Verpflichtungen, die eingeführten Kontrollmassnahmen und

die für die Einhaltung der Vorschriften verantwortlichen Personen im Einzelnen aufgeführt sind. Diese Politik sollte folgende Elemente enthalten:

- **Datenkartierung:** Identifizieren Sie sensible Daten, ihren Standort und die damit verbundenen Datenflüsse.
- **Technische und organisatorische Kontrollen:** Einführung von Massnahmen wie Datenverschlüsselung, starke Authentifizierung, Zugriffsverwaltung usw.
- **Ausbildung der Mitarbeitenden:** Informieren Sie die Mitarbeitende regelmässig über gesetzliche Verpflichtungen und bewährte Verfahrensweisen zur Einhaltung von Vorschriften.
- **Verfahren zum Umgang mit Vorfällen:** Entwickeln Sie Protokolle, um schnell auf Datenverletzungen oder Abweichungen zu reagieren.

Interne und externe Prüfung der Computersicherheit

Um ein gleichbleibender Stand an Compliance und Sicherheit zu gewährleisten, ist es unerlässlich, regelmässig Audits durchzuführen. Diese Audits ermöglichen es, die Wirksamkeit der eingeführten Massnahmen zu bewerten, Abweichungen zu erkennen und die notwendigen Korrekturmassnahmen zu ergreifen.

NIVEAU 3

Interne Prüfung

- Durchführung durch ein zweckgebundenes internes Team oder einen Compliance-Beauftragten.
- Überprüfung der vorhandenen Richtlinien, Verfahren und Sicherheitseinrichtungen.
- Bewertung der Konformität von Prozessen im Hinblick auf die gesetzlichen Anforderungen.
- Erstellung interner Berichte mit Empfehlungen für Verbesserungen.

NIVEAU 2

Externe Prüfung

- Durchgeführt von einer unabhängigen dritten Partei oder einer spezialisierten Firma.
- Konformitätsprüfung nach anerkannten Standards (ISO 27001, DSGVO).
- Gründliche Überprüfung der Sicherheitskontrollen, vergangener Vorfälle und des Risikomanagements.
- Erstellung eines Prüfberichts, der die Beobachtungen, die identifizierten Risiken und die empfohlenen Aktionspläne enthält.

NIVEAU 2

Regelmässige Überprüfung der Sicherheitspolitik und -verfahren

Die Einhaltung von Vorschriften ist keine ausserordentliche Übung, sondern ein kontinuierlicher Prozess. Es ist entscheidend:

- Regelmässige Überprüfungen durchzuführen, um sicherzustellen, dass die Sicherheitsrichtlinien bei Änderungen der Vorschriften, neuen Bedrohungen oder Entwicklungen der institutionellen Aktivitäten aktualisiert werden.
- Die Wirksamkeit der Kontrollmassnahmen durch regelmässige Prüfungen zu bewerten.

- Krisentests und -simulationen zu planen, um zu überprüfen, ob die Verfahren zur Reaktion auf Vorfälle robust und wirksam sind.

Die Einführung einer strengen und gut dokumentierten Compliance-Strategie schützt Institutionen nicht nur vor rechtlichen Risiken, sondern stärkt auch ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen.

Checkliste bewährte Verfahrensweisen

Mithilfe dieser Checkliste wird die Umsetzung der im Leitfaden genannten bewährten Verfahren für die Cybersicherheit überprüft:

Inventar der Vermögenswerte

- ☐ Führen Sie eine Abbildung der Systeme und Dienste durch.
- ☐ Klassifizieren Sie sensible Daten.
- ☐ Identifizieren Sie externe Dienstleister.

Netzwerksicherheit und Segmentierung

- ☐ Wenden Sie Netzwerksegmentierung an (interne Netzwerke trennen, DMZ usw.).
- ☐ Konfigurieren Sie den Netzwerkzugang mit strengen Kontrollen.
- ☐ Verwenden Sie VPNs für Fernverbindungen mit Multi-Faktor-Authentifizierung (MFA).

Konfiguration und Verwaltung von Firewalls

- ☐ Legen Sie strenge Filterrichtlinien fest.
- ☐ Führen Sie eine regelmässige Überprüfung der Firewall-Regeln durch.
- ☐ Halten Sie Firewalls mit der neuesten verfügbaren Firmware-Version auf dem neuesten Stand.

Datensicherung und -wiederherstellung

- ☐ Planen Sie regelmässige Datensicherungen (täglich, wöchentlich, monatlich).
- ☐ Testen Sie regelmässig die Wiederherstellung von Datensicherungen.
- ☐ Verschlüsseln Sie sensible Datensicherungen.

Sicherung von im Internet ausgestellten Diensten

- ☐ Beschränken Sie die Anzahl der Dienste, die im Internet verfügbar sind.
- ☐ Beschränken Sie den Zugriff auf Dienste nur auf befugte Benutzer, mit Multi-Faktor-Authentifizierung (MFA).
- ☐ Führen Sie regelmässige Sicherheitstests der exponierten Dienste durch.

Verwaltung von Schwachstellen und Updates

- ☐ Führen Sie ein Inventar von Software und Systemen.
- ☐ Wenden Sie kritische Aktualisierungen schnell an.
- ☐ Implementieren Sie ein zentrales Patch-Management.

Schutz von Arbeitsplätzen und Servern

- ☐ Installieren und konfigurieren Sie mindestens Antivirenlösungen, idealerweise EDR.
- ☐ Setzen Sie Sicherheitsrichtlinien durch (lokale Firewall, Kontrolle von USB-Geräten).
- ☐ Legen Sie Mindestberechtigungen für Benutzer fest.

Verwaltung privilegierter Zugänge

- ☐ Setzen Sie strenge Richtlinien für die Verwaltung privilegierter Konten durch.
- ☐ Zeichnen Sie Aktivitäten von privilegierten Benutzern auf.
- ☐ Verwenden Sie Lösungen für die Verwaltung privilegierter Zugriffe (PAM).

Überwachung und Monitoring der Infrastruktur

- ☐ Implementieren Sie ein Überwachungssystem (SIEM).
- ☐ Legen Sie Regeln für die Erkennung von Anomalien fest.
- ☐ Richten Sie Warnmeldungen und Verfahren für schnelle Reaktionen ein.

Ausbildung und Sensibilisierung

- ☐ Organisieren Sie regelmässige Ausbildungsveranstaltungen für die Mitarbeitenden.
- ☐ Führen Sie Kampagnen zur Sensibilisierung für Cybersicherheit durch.
- ☐ Testen Sie regelmässig die Wachsamkeit der Mitarbeiter (z. B. Phishing-Tests).

Verwaltung von externen IT-Anbietern

- ☐ Sorgen Sie dafür, dass Sie alle IT-Anbieter und deren Verantwortungsbereiche genau kennen.
- ☐ Wählen Sie IT-Anbieter nach bestimmten und pragmatischen Kriterien aus.
- ☐ Schliessen Sie Verträge mit ihren IT-Dienstleistern ab, insbesondere unter Berücksichtigung des Service Level Agreement (SLA), eines Prüfungsrechts sowie einer Erleichterung der Reversibilität der Dienste.

Pläne für Kontinuität und Reaktion auf Vorfälle

- ☐ Entwickeln Sie einen Plan zur Reaktion auf Vorfälle (IRP).
- ☐ Testen Sie den Incident Response Plan (IRP) und den Disaster Recovery Plan (DRP).
- ☐ Dokumentieren Sie nach jedem Vorfall die Erkenntnisse.

immunIT sàrl

Chemin des Plantaz 44-46, 1260 Nyon

+41 22 565 33 71

info@immunit.ch

https://www.immunit.ch