Bayerisches Landesamt für
Datenschutzaufsicht

Checkliste Cyberfestung

10 Punkte für mehr Datensicherheit

Aktuelle Prüfkriterien nach Art. 32 DS-GVO

Mehr Sicherheit durch Datenschutz

Geht es um Ihre Sicherheit, haben Sie einen bedeutenden Vorsprung: Niemand kennt Ihre Organisation so gut wie Sie selbst. Sorgen Sie dafür, dass dies so bleibt. Nutzen Sie Ihr exklusives Wissen, um Ihre verwundbaren Punkte aktiv zu schützen. Folgen Sie wie bei dem Bau einer Festung einfach dem Gedanken, möglichst effektive Hindernisse aufzubauen – sei es ein unüberwindbarer Burggraben, meterhohe Steinmauern oder auch Wachtürme, die rund um die Uhr besetzt sind. Stimmen Sie Maßnahmen aufeinander ab und sorgen Sie dafür, dass beim Ausfall einzelner Schutzmaßnahmen weiterhin eine ausreichende Sicherheit gewährleistet ist. Mit einem durchgängigen Konzept und einer regelmäßigen Überprüfung Ihrer Bausteine wird es gelingen, bekannte Angriffsmuster zu entschärfen und Cyberakteure weiter in Schach zu halten. Auch im Zeitalter moderner Angriffe mit künstlicher Intelligenz (KI) bleiben klassische technische und organisatorische Maßnahmen entscheidend, um überhaupt verteidungsfähig zu sein.

Machen Sie Ihre Organisation zu einer eigenen Cyberfestung.
Bauen auch Sie effektiv vor.

Defense in Depth – die „mehrschichtige Verteidigung" oder auch „Verteidigung in der Tiefe" – ist eine bekannte Strategie der Cybersicherheit, die auf Redundanz setzt. Dabei wird ein System durch die Kombination von mehreren, unabhängigen Schutzmechanismen wie Firewalls, Verschlüsselung und Zugriffskontrollen abgesichert. Falls eine Sicherheitsebene versagt, können die nachfolgenden Schichten den Angriff abfangen und so eine vollständige Kompromittierung verhindern. Da kein einzelner Schutzmechanismus als unfehlbar gilt, stellt dieser Ansatz also sicher, dass der Ausfall einer oder weniger Ebenen durch andere kompensiert wird, wodurch die Widerstandsfähigkeit des Gesamtsystems effektiv erhöht wird. Da der englische Begriff etwas sperrig klingt, fassen wir die zehn Punkte für mehr Datensicherheit unter unserer Analogie der **Cyberfestung** zusammen.

Die aufgeführten Themen und darin enthaltenen Punkte sind nicht als abschließend zu betrachten, sondern stellen einen Good-Practice-Ansatz dar, der im Sinne einer Soll-Ist-Überprüfung verwendet werden kann. Welche Maßnahmen in welchem Umfang angewendet werden können bzw. sollten und sich letztendlich als wirksam erweisen, hängt von den individuellen Rahmenbedingungen jeder Organisation ab.

Checkliste – Themenüberblick:

1. Netzwerkperimeter samt Angriffsmöglichkeiten ermitteln

Unter Netzwerkperimeter versteht man die Sicherheitsbarriere, die ein internes Netzwerk von der Außenwelt – wie dem Internet – abgrenzt. Er schützt das Netzwerk vor unbefugtem Zugriff sowie Angriffen und umfasst in der Regel Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systeme (IDS), Gateways für virtuelle Private Netzwerke (VPN) und andere Schutzmechanismen, die den Datenverkehr kontrollieren und überwachen. Zur Ermittlung des Netzwerkperimeters und der möglichen Angriffspunkte ist eine umfassende Sicherheitsanalyse unerlässlich. Dabei sollten sowohl die physische Infrastruktur als auch die virtuelle Netzwerkarchitektur genau untersucht werden. Durch die Identifikation von Schwachstellen in Firewalls, Router-Konfigurationen und Zugriffskontrollen lassen sich potentielle Einfallstore für Angreifer erkennen. Zudem ist es wichtig, die Nutzung von Cloud-Diensten und externen Schnittstellen zu analysieren, da diese zusätzliche Angriffsflächen bieten. Cyberkriminelle führen vor einem Angriff oftmals eine sogenannte Reconnaissance-Phase durch, bei der sie das Netzwerk systematisch ausforschen, um Schwachstellen zu identifizieren. Durch eigene Penetrationstests und Schwachstellen-Scans kann die eigene Sicherheitslage geprüft und verbessert werden. Es empfiehlt sich außerdem, regelmäßig Log-Daten auszuwerten, um ungewöhnliche Aktivitäten frühzeitig zu erkennen. Ein proaktives Monitoring des Netzwerkverkehrs sowie die Implementierung von Intrusion Detection und Prevention Systemen (IDS/IPS) tragen dazu bei, potenzielle Angriffe frühzeitig zu erkennen und abzuwehren. Insgesamt ist die kontinuierliche Überprüfung und Aktualisierung der Sicherheitsmaßnahmen entscheidend, um den Schutz des Netzwerkperimeters aufrechtzuerhalten und Angriffsmöglichkeiten zu minimieren.

Netzwerk-Bausteine:

- ☐ Interne Übersicht: Eine aktuelle und vollständige Liste aller IT-Komponenten im internen Netzwerk ist vorhanden. Dabei sind insbesondere alle über das Internet erreichbaren Komponenten (z. B. Firewalls, VPN-Endpunkte, Mailserver) deutlich gekennzeichnet.
  - ✓ Grund: Die Übersicht ist Voraussetzung für die effektive Ermittlung möglicher Angriffspunkte.

- ☐ Externe Übersicht: Eine aktuelle und vollständige Liste aller extern betriebenen IT-Komponenten ist vorhanden (z. B. externe Server, externe Security-Dienste, externe Mailserver, Cloud Infrastructure as a Service (IaaS), Cloud Platform as a Service (PaaS)).
  - ✓ Grund: Extern verwendete Komponenten sind als potentielle Einfallstore nicht zu vergessen.

- ☐ Cloud-Übersicht: Eine aktuelle und vollständige Liste aller Cloud-Anwendungen (z. B. MS 365, Google Workspace, Salesforce, SAP) ist vorhanden.
  - ✓ Grund: Mögliche Angriffspunkte über Cloud-Anwendungen müssen berücksichtigt werden.

- ☐ IT-Richtlinie: In der Organisation existiert eine Richtlinie, die die In- und Außerbetriebnahme von IT-Komponenten und Cloud-Diensten verbindlich regelt.
  - ✓ Grund: Verhinderung sog. Schatten-IT – also IT-Systemen, deren Einsatzzweck, Konfiguration und Softwarestand außerhalb der Kontrollmöglichkeiten der Organisation liegen.

- ☐ Portscans: Es werden regelmäßig eigene Port-/Netzwerkscans der externen IP-Adressen des Unternehmensnetzes sowie der extern betriebenen IT-Komponenten durchgeführt (ggf. beauftragt).
  - ✓ Grund: Erkennung von Schatten-IT, unzulässig betriebener Dienste sowie möglicher Fehlkonfigurationen von aktiven Sicherheitskomponenten (z. B. Portfilter bei Firewalls).

- ☐ Cloud-Scans: Es werden regelmäßig Port-/Netzwerkscans bei der eigenen Cloud-Umgebung (sog. Virtual Private Cloud (VPC)-Netzwerk) durchgeführt und – sofern vorhanden – sog. cloud-native Monitoring-Tools mit Scanfunktion der Cloudanbieter verwendet.
  - ✓ Grund: Dient der Erkennung möglicher Fehlkonfigurationen von Cloud-Diensten.

- ☐ Scan-Routine: Die durchzuführenden Port-/Netzwerkscans werden automatisiert in regelmäßigen Abständen durchgeführt und die Ergebnisse automatisiert mit Soll-Vorgaben (laut spezifiziertem Netzplan) verglichen. Soll-Ist-Abweichungen werden automatisiert an interne Stellen eskaliert.
  - ✓ Grund: Eine automatisierte und regelmäßige Überprüfung beugt Verzögerungen der Scans aufgrund höherer Arbeitslast und-/oder Urlaub/Krankheit der IT-Mitarbeitenden vor.

- ☐ Firewall-Regeln: Restriktive Firewall-Policies werden auf allen von extern erreichbaren Systemen (internes Netzwerk, extern betriebene Komponenten, Cloud-Dienste) angewendet. Dabei gilt eine „Deny-All"-Policy, bei der nur die unbedingt notwendigen Ausnahmen im Rahmen eines geregelten Antragsverfahrens zugelassen werden.
  - ✓ Grund: Je weniger Dienste über das Internet erreichbar sind, desto geringer ist die Angriffsfläche.

- ☐ Dokumentation: Eine aktuelle und vollständige Dokumentation externer Schnittstellen zu (Web-)Services und API-Endpunkten ist vorhanden.
  - ✓ Grund: Voraussetzung für die Kontrolle und Sicherheitsüberprüfung von Datenendpunkten auf Anwendungsebene.

2. Multi-Faktor-Authentifizierung einsetzen

Starke Passwörter stellen weiterhin einen Basisschutz bei der Anmeldung an IT-Systemen und Diensten dar. Zugleich versuchen Angreifer immer wieder, diese Passwörter in die eigenen Hände zu bekommen (z. B. durch Phishing oder Social Engineering). Durch die Ergänzung eines weiteren Zugangfaktors, der nicht so leicht zu erlangen ist, wird die Sicherheit deutlich erhöht. Eine Anmeldung, bei der mehr als nur das klassische Passwort abgefragt wird, heißt Multi-Faktor-Authentifizierung (MFA). MFA kann verschiedene Formen annehmen, beispielsweise Hardware-Token, die Einmalpasswörter generieren oder Softwarelösungen wie Authenticator-Apps, die zeitbasierte Einmalpasswörter (Time-Based One-Time Password, kurz: TOTP) bereitstellen. Auch biometrische Verfahren, wie Fingerabdruck- oder Gesichtserkennung, bieten eine komfortable und sichere Alternative – vorausgesetzt, sie werden datenschutzkonform eingesetzt. Der Einsatz von Multi-Faktor-Authentifizierung (MFA) erhöht die Sicherheit bei der Anmeldung an IT-Systemen und Diensten erheblich, da er die Abhängigkeit von lediglich einem Passwort reduziert. Der Einsatz von MFA ist daher nicht nur bei sensiblen Daten oder kritischen Infrastrukturen empfehlenswert, sondern auch bei der Absicherung täglich genutzter Systeme wie z. B. die Zugänge zu E-Mail- und Office-Accounts, da dort eine Vielzahl an wertvollen Daten liegen. MFA schützt auch vor unbefugtem Zugriff, selbst wenn Passwörter kompromittiert wurden. Neben der technischen Umsetzung ist es wichtig, die Nutzerinnen und Nutzer entsprechend zu schulen und die Handhabung der MFA-Lösungen benutzerfreundlich zu gestalten. So kann die Akzeptanz erhöht und die Sicherheitslücke durch menschliches Versagen minimiert werden. Insgesamt trägt MFA wesentlich dazu bei, die Cybersicherheit nachhaltig zu stärken und das Risiko von unbefugten Systemeingriffen zu verringern.

Authentifizierung-Bausteine:

- ☐ Password Policy: Es werden ausschließlich starke Passwörter verwendet (Mindestlänge zwölf Zeichen, hohe Komplexität), die, sofern möglich, auch über technische Vorgaben erzwungen werden.
  - ✓ Grund: Zu kurze oder triviale Passwörter können erraten oder von Angreifern mittels Ausprobierens (sog. Wörterbuchangriffe) erlangt werden. Gerade durch Data Leaks, gesteigerter Rechenleistungen sowie KI-Techniken reichen einfache Passwörter längst nicht mehr aus.

- ☐ MFA für Administratoren: Alle administrativen Konten sind ausschließlich mittels MFA zugänglich.
  - ✓ Grund: Administrative Konten müssen aufgrund ihres Schadenspotentials im Falle einer Übernahme durch Angreifer besonders abgesichert werden.

- ☐ MFA-Einsatz: Benutzerkonten in besonders exponierten Bereichen (z. B. Leitungsebene, Forschungsabteilung, Sekretariat, Personalstelle, Personalrat) sind ausschließlich mittels MFA zugänglich.
  - ✓ Grund: Konten mit erhöhtem Angriffsrisiko oder Zugang zu besonders schützenswerten Informationen müssen auch besonders abgesichert werden.

- ☐ MFA für Cloud: Cloud-Dienste (z. B. MS 365) werden durchgängig mittels MFA abgesichert. Dies gilt nicht nur für besondere Nutzergruppen, sondern für alle Benutzerkonten (z. B. auch für Marketing, Vertrieb, Praktikanten).
  - ✓ Grund: Angriffe auf Cloud-Dienste mit entwendeten Zugangsdaten (z. B. Phishing) ist eine der häufigsten vorkommenden Cyberangriffe. Ein einzelner aufgrund eines schwachen Passworts kompromittierter E-Mail-Account kann bei erfolgtem Phishing erheblichen Schaden verursachen.

- ☐ Protokollierung bei MFA: Fehlgeschlagene Login-Versuche mittels MFA werden an geeigneter Stelle protokolliert und regelmäßig (automatisiert) ausgewertet.
  - ✓ Grund: Dient der Erkennung von Angriffsversuchen. Voraussetzung ist aber, dass die Protokolle tatsächlich aktiv ausgewertet und nicht erst im Schadensfall herangezogen werden.

- ☐ MFA-Regelungen: Es existieren verbindliche Regelungen zur Verlustmeldung von MFA-Hardware (z. B. sofortige Sperrung) sowie für den Umgang mit dieser beim Austritt von Mitarbeitenden.
  - ✓ Grund: Es darf keine aktive MFA-Hardware abseits des regulären Einsatzzwecks vorhanden sein, da verloren gegangene oder nicht mehr benötigte Hardware unbefugte Zugriffe auf Systeme ermöglichen kann. Solche muss umgehend gesperrt und deaktiviert werden.

- ☐ Schulung zu MFA-Nutzung: Mitarbeitende werden zum sachgerechten Einsatz von MFA geschult.
  - ✓ Grund: MFA-Hardware muss sicher verwahrt und verwendet werden. Regelungen zum Verlust müssen klar kommuniziert werden. Nur bei aktiver Information über den Verlust kann auch zeitnah eine effektive Sperrung erfolgen und so der betroffene Zugang geschützt werden.

- ☐ Fernwartung mit MFA: Fernwartung durch Administratoren (z. B. Remote Desktop Protokoll – kurz: RDP) erfolgt ausschließlich mit einer MFA-Absicherung. Das Transportprotokoll ist so konfiguriert, dass die Datenübertragung nach Stand der Technik verschlüsselt ist (z. B. TLS 1.2, AES-256).
  - ✓ Grund: Angreifer (auch im lokalen Netzwerk) könnten durch Mitlesen des Fernwartungsverkehrs an sensitive Daten oder sogar Administrationspasswörter kommen. Fernwartung ist nach wie vor ein bei Cyberkriminellen beliebter Angriffspfad.

- ☐ MFA bei VPN: Alle VPN-Verbindungen (z. B. Homeoffice) sind zusätzlich zum Benutzername/Passwort mit MFA abgesichert.
  - ✓ Grund: VPN-Zugänge ohne MFA werden häufig im Rahmen sog. Brute-Force-Attacken mit dem Ziel, Zugangsdaten zu erraten, angegriffen.

3. Umgang mit lokalen Administratorkonten regeln

Administratoren stellen aufgrund ihrer weitreichenden Konfigurations- und Rechtemöglichkeiten ein attraktives Ziel für Angreifer dar. Lokale Administratorkonten entziehen sich teilweise den Sicherheitsmechanismen verwalteter Umgebungen oder werden ohne Einsatz zusätzlicher Schutzwerkzeuge betrieben. Der Umgang mit solchen Konten ist daher ein zentraler Aspekt der IT-Sicherheitsstrategie. Lokale Administratorkonten ermöglichen tiefgreifende Eingriffe in das System, inklusive der Installation von Software, Änderungen an Systemeinstellungen und Zugriff auf sensible Daten. Wird ein solches Konto kompromittiert, kann dies schwerwiegende Folgen für die gesamte IT-Infrastruktur haben. Ungepflegte Sicherheitsroutinen bei lokalen Administratorkonten erhöhen das Risiko, dass Angreifer diese Konten ausnutzen, um sich unbefugten Zugriff zu verschaffen, persistente Hintertüren zu installieren oder das System für weiterführende Angriffe zu nutzen. Um dem entgegenzuwirken, sind strenge Richtlinien im Umgang mit lokalen Administratorkonten notwendig. Dazu gehören beispielsweise die Begrenzung der Anzahl solcher Konten, die Verwendung von einzigartigen, komplexen Passwörtern sowie die regelmäßige Überprüfung und Deaktivierung nicht mehr benötigter Konten. Zudem sollte die Nutzung von lokalen Administratorkonten auf das notwendige Minimum beschränkt werden, um das Risiko eines Missbrauchs zu reduzieren. Weiterhin empfiehlt es sich, MFA einzusetzen sowie die Konten regelmäßig auf ungewöhnliche Aktivitäten zu überwachen. Die Implementierung zentraler Verwaltungstools kann dazu beitragen, die Kontrolle über lokale Administratorkonten zu verbessern, Zugriffe zu protokollieren und im Verdachtsfall schnell zu reagieren. Insgesamt ist der bewusste und kontrollierte Umgang mit lokalen Administratorkonten ein essentieller Baustein, um die Sicherheit der IT-Infrastruktur zu erhöhen und potenzielle Angriffspunkte zu minimieren.

Administratorkonten-Bausteine:

- ☐ Kontenregelung: Es existiert eine Regelung, dass Administratoren mit lokalen Administratorkonten ausschließlich administrative Tätigkeiten durchführen dürfen. Für alle anderen Tätigkeiten (z. B. Internet, E-Mails) haben sie ein eigenes Benutzerkonto mit nicht-privilegierten Rechten.
  - ✓ Grund: Viele Angriffe (z. B. Schadcode in E-Mails, Drive-By-Angriffe beim Besuch auf Webseiten) führen Aktionen mit dem aktuell angemeldeten Nutzer aus. Um diesbezügliche Gefahren zu reduzieren, ist es wichtig, dass Administatoren in solchen Momenten nicht mit erweiterten Rechten angemeldet sind – denn auch Administatoren sind vor Angriffen nicht geschützt.

- ☐ Unterschiedliche Passwörter: Die Passwörter der lokalen Administrator-Konten unterscheiden sich für jedes System. In Windows-Umgebungen geht dies bspw. durch Einsatz des Microsoft Tools LAPS („Local Administrator Password Solution“) oder andere vergleichbare Drittanbieter-Tools.
  - ✓ Grund: Angreifer, die Passwörter auf einem IT-System erlangen können (z. B. mittels Angriffstool Mimikatz), können diese dann nicht für das Lateral-Movement in der Organisation oder die Kompromittierung anderer IT-System im Netzwerk verwenden.

- ☐ Einschränkung der Anzahl von Administratorkonten: Die Anzahl der Benutzerkonten mit administrativen Rechten ist auf das absolute Minimum zu reduzieren.
  - ✓ Grund: Je mehr Benutzer mit Administratorrechten arbeiten, desto größer ist das Risiko einer Zweckentfremdung im Angriffsfall. Eine unkontrollierte Vermehrung von Administratorkonten ist zu vermeiden – ansonsten gelingt es nicht mehr, den Überblick zu bewahren und ungewöhnliche Aktivitäten festzustellen.

- ☐ Protokollierung: Login- und Administrationsaktivitäten von lokalen Admins werden an geeigneter Stelle protokolliert (z. B. zentraler Log-Server oder Security Information and Event Management (SIEM)-System) und – sofern möglich – automatisiert ausgewertet. Sollten verdächtige Aktivitäten erkannt werden, erfolgt eine geeignete Alarmierung oder sogar ein automatisiertes Sperren des möglicherweise kompromittierten Systems bzw. betroffenen Benutzerkontos.
  - ✓ Grund: Sollte ein Angreifer in den Besitz von Zugangsdaten eines lokalen Admins kommen, können Angriffsversuche möglicherweise noch rechtzeitig erkannt und ggf. begrenzt werden. Ist dies nicht mehr möglich, kann im Rahmen der Aufarbeitung eines Vorfalls ggf. zumindest der Ablauf des Angriffs rekonstruiert und bestenfalls der Schaden minimiert werden.

- ☐ Jump-Server-Einsatz prüfen: Es werden sog. Jump-Server (dezidierte Rechner, über die der Zugriff auf zu wartende IT-Systeme erfolgt) eingesetzt, die mit MFA abgesichert sind. Lokale Passwörter bleiben zwar auf den Zielsystemen, werden aber nur über den MFA-gesicherten Jump-Server eingegeben. Es erfolgt keine direkte Eingabe von (lokalen) Administrator-Zugangsdaten auf beliebigen IT-Systemen.
  - ✓ Grund: Lokale Administrator-Passwörter sind zwar weiterhin auf den Zielsystemen vorhanden, jedoch werden diese lediglich auf dem Jump-Server eingeben, was das Risiko einer Kompromittierung (z. B. durch Keylogger-Malware) senken kann.

- ☐ Just-In-Time-Zugriffe: In Windows-Umgebungen wird der Einsatz von sog. Just-In-Time-Zugriffen für Administratorkonten, z. B. mittels Microsoft Privileged Identity Management (PIM), die mit MFA abgesichert sind, geprüft.
  - ✓ Grund: Durch Verwendung von optionalen Systemerweiterungen bzw. Drittanbietertools können MFA-Absicherungen auch für lokale Administratorkonten eingesetzt werden.

4. PowerShell-Skripte einschränken

PowerShell-Skripte sind leistungsfähige Werkzeuge, die es Administratoren ermöglichen, administrative Aufgaben effizient zu automatisieren und komplexe Verwaltungsprozesse durchzuführen. Durch die Flexibilität und die umfangreichen Funktionen von PowerShell können wiederkehrende Tätigkeiten vereinfacht und die Systemverwaltung deutlich effizienter gestaltet werden. Allerdings bergen diese Skripte auch erhebliche Sicherheitsrisiken, da sie bei Missbrauch oder unzureichender Kontrolle als Angriffswerkzeuge genutzt werden können. Angreifer verwenden PowerShell-Skripte häufig, um Schadcode auszuführen, sich dauerhaft im System zu etablieren oder lateral innerhalb eines Netzwerks zu bewegen. Sie können beispielsweise automatisierte Skripte einsetzen, um Schwachstellen auszunutzen, Daten zu exfiltrieren oder Backdoors zu installieren. Da PowerShell standardmäßig auf vielen Windows-Systemen aktiviert ist, besteht ein erhebliches Grundrisiko, wenn keine geeigneten Schutzmaßnahmen getroffen werden. Um diese Risiken gezielt zu minimieren, sollte die Ausführung von PowerShell-Skripten und andere Shell-Skripte streng eingeschränkt werden. Hierbei lässt sich die Ausführungsrichtlinie (Execution Policy) so konfigurieren, dass unautorisierte Skripte blockiert werden. Es ist sinnvoll, die Verwendung von PowerShell nur auf autorisierte Nutzerinnen und Nutzer zu beschränken und die Aktivitäten durch Protokollierung und Überwachung zu kontrollieren. Weiterhin empfiehlt sich der Einsatz von speziellen Sicherheitslösungen wie Endpoint Detection and Response (EDR) oder Anti-Malware-Tools, die verdächtige PowerShell-Aktivitäten erkennen und blockieren können. Die Schulung der Mitarbeitenden, insbesondere der Administratoren, im sicheren Umgang mit PowerShell sowie die regelmäßige Überprüfung der Skriptaktivitäten tragen ebenfalls dazu bei, Missbrauch zu verhindern. Insgesamt sind die Einschränkung und Kontrolle von PowerShell-Skripten wichtige Bausteine, um die Angriffsflächen zu reduzieren und die Sicherheit der IT-Infrastruktur zu erhöhen.

PowerShell-Skripte-Bausteine:

- ☐ Restriktiver PowerShell-Einsatz: Es wird geprüft, welche IT-Systeme keine PowerShell-Skripte benötigen (z. B. dezidierte Kiosk-Systeme oder Kassensysteme). Bei diesen wird PowerShell deinstalliert.
  - ✓ Grund: Häufig ist PowerShell für verwaltende Administrationsaufgaben grundsätzlich erforderlich. Falls nicht, kann eine Angriffsfläche durch die Deinstallation deutlich reduziert werden.

- ☐ PowerShell bei älterer Software: Skripte wie JavaScript oder Visual Basic werden durch das Betriebssystem nur dann zur Ausführung zugelassen, wenn (z. B. ältere) Software dies zwingend erfordert. Browser sind von dieser Regelung ausgenommen, da JavaScript dort regelmäßig benötigt wird.
  - ✓ Grund: Schadsoftware kommt auch versteckt als Skript-Datei im E-Mail-Anhang. Bei einem versehentlichen „Klick" durch den Nutzer kann diese trotzdem an der Ausführung gehindert werden, falls auf Betriebssystemseite eine Deaktivierung erfolgt.

- ☐ Nur signierte Skripte: Die Ausführung unsignierter PowerShell-Skripte ist entweder komplett untersagt („AllSigned") oder zumindest nur für lokal vorhandene Skripte („RemoteSigned") erlaubt.
  - ✓ Grund: Angreifer laden häufig im Rahmen eines Angriffs eigene PowerShell-Skripte nach.

- ☐ Ausgewählte Verzeichnisse bestimmen: Prüfung, ob die Ausführung von Programmen nur aus festgelegten Verzeichnissen möglich ist (sog. Execution Directory Whitelisting).
  - ✓ Grund: Von Angreifern präparierte E-Mails enthalten häufig nicht den Schadcode selbst, sondern kleine Programme, die diesen automatisch aus dem Internet laden. Die derart heruntergeladenen Schadprogramme werden in festgelegten Verzeichnissen des Betriebssystems gespeichert und können durch eine Freigabe gültiger – und in diesem Fall anderer – Verzeichnisse an einer Ausführung gehindert werden.

- ☐ PowerShell 2.0 vermeiden: Die veraltete Version PowerShell 2.0 wird nach Möglichkeit deaktiviert und nur in absoluten Ausnahmefällen nach sorgfältiger Prüfung aktiviert.
  - ✓ Grund: PowerShell 2.0 fehlen wichtige Sicherheitsfeatures. Dadurch ist das Risiko erhöht, dass schädliche Skripte oder Angriffe ungehindert ausgeführt werden können. Ohne ausreichende Kontrolle und moderne Sicherheitsfeatures könnten potenziell schädliche Befehle oder Skripte leichter ausgeführt werden.

- ☐ Gruppenrichtlinien nutzen: PowerShell wird nur für diejenigen Benutzergruppen erlaubt, die es für ihre Tätigkeiten zwingend benötigen (z. B. Administration) – für alle anderen Nutzer wird es mittels Gruppenrichtlinie deaktiviert.
  - ✓ Grund: Dadurch wird verhindert, dass PowerShell bei normalen Nutzern für Angriffe genutzt werden kann (z. B. Office-Makros, die PowerShell zur Ausführung schädlichen Codes verwenden).

- ☐ Reduktion von Funktionen: In Umgebungen, in denen PowerShell nur für grundlegende Administrationsaufgaben genutzt wird, ist der sog. „Constrained Language Mode" (Reduktion bestimmter sicherheitskritischer Funktionen) aktiviert (z. B. mittels Gruppenrichtlinie).
  - ✓ Grund: Durch den eingeschränkten Funktionsumfang können bestimmte von Angreifern genutzte Funktionen wie die dynamische Code-Ausführung oder der Zugriff auf .NET Objekte nicht mehr verwendet werden.

- ☐ Protokollierung von Skripten: Die Protokollierung von PowerShell-Skripten auf zentralen Log-Servern oder SIEM-Systemen ist aktiviert (zumindest „Script Block Logging" zur Protokollierung vollständiger PowerShell-Skripte, ggf. auch „Transcription Logging" für die Protokollierung interaktiver Sitzungen).
  - ✓ Grund: Auf diese Weise können Angriffe erkannt und ggf. verhindert oder zumindest im Nachgang nachvollzogen werden.

- ☐ Einschränkung der Ausführbarkeit: Es werden sog. Application Control Techniken (AppLocker oder Windows Defender Application Control) genutzt, um nur autorisierte Skripte, Befehle und PowerShell-Versionen auszuführen und ggf. auch die Verzeichnisse der Skripte festzulegen.
  - ✓ Grund: Damit können Funktionsumfang und Speicherort von zulässigen Skripten zentral festgelegt werden.

5. Netzwerksegmentierung nutzen

Angesichts der zunehmenden Komplexität und der stetig wachsenden Bedrohungslage ist es mittlerweile realistischer denn je, davon auszugehen, dass ein Angreifer den äußeren Perimeter des Netzwerks überwinden kann. Daher reicht der Schutz durch eine einzige Sicherheitsbarriere oft nicht mehr aus, um die gesamte Infrastruktur wirksam zu sichern. Um das Risiko einer Bewegung innerhalb des Netzwerks („Lateral Movement") zu minimieren, ist die Netzwerksegmentierung ein gewinnbringendes Sicherheitsinstrument als weitere Schutzebene. Durch die Aufteilung des Netzwerks in mehrere, voneinander getrennte Segmente können so sensible Systeme, Daten und Anwendungen besser geschützt werden. Bei einer erfolgreichen Kompromittierung eines Segments bleibt der Angriff auf dieses begrenzt und die Angreifer können nicht ohne Weiteres auf andere Bereiche zugreifen. So wird die Ausbreitung eines Angriffs deutlich erschwert und die Schadensauswirkung reduziert. Die Netzwerksegmentierung kann auf verschiedenen Ebenen erfolgen, beispielsweise durch Virtual Local Area Network (VLAN), physische Trennung oder durch den Einsatz von Firewalls zwischen den Segmenten. Dabei ist es wichtig, klare Zugriffsregeln und Kontrollen zu definieren, sodass nur autorisierte Verbindungen zwischen den Segmenten erlaubt sind. Zusätzlich sollte der Datenverkehr zwischen den Segmenten überwacht und protokolliert werden, um verdächtige Aktivitäten frühzeitig erkennen zu können. Ein weiterer Vorteil der Segmentierung ist die erleichterte Umsetzung von Sicherheitsrichtlinien, etwa durch die Anwendung unterschiedlicher Schutzmaßnahmen in den jeweiligen Segmenten, die auf das jeweilige Bedürfnis zugeschnitten sind. Besonders bei sensiblen Daten oder kritischen Systemen ist eine strikte Trennung der verschiedenen Bereiche unerlässlich. Insgesamt trägt die Nutzung von Netzwerksegmentierung dazu bei, die Angriffsflächen zu reduzieren, die Kontrolle über die Infrastruktur zu erhöhen und im Falle eines Angriffs die Auswirkungen rasch einzudämmen.

Netzwerksegmentierung-Bausteine:

- ☐ Netzwerkzonen definieren: Einheiten wie Arbeitsplätze, Server und Produktionssysteme sind physisch und logisch voneinander getrennt.
  - ✓ Grund: Eine klare Aufteilung in verschiedene Netzwerkzonen verringert das Risiko unberechtigter Zugriffe oder dass Schadsoftware sich ungehindert im gesamten Netzwerk ausbreitet.

- ☐ Interne Firewalls implementieren: Zwischen den definierten Netzwerkzonen sind Firewalls oder vergleichbare Lösungen eingerichtet, um den Datenverkehr zu überwachen und zu kontrollieren.
  - ✓ Grund: Die segmentweise Überwachung erhöht die Transparenz und erschwert das Lateral Movement von Angreifern innerhalb des Netzwerks.

- ☐ Zonen regelmäßig testen: Penetrationstests, Netzwerkscans oder andere Prüfungen werden regelmäßig durchgeführt, um sicherzustellen, dass keine unerwünschten Verbindungen bestehen.
  - ✓ Grund: Durch diese Tests lassen sich Fehlkonfigurationen, offene Ports oder Schwachstellen frühzeitig erkennen und beheben. Eine Nachjustierung ist so schnell möglich.

- ☐ Zero-Trust-Prinzipien anwenden: Jeder Zugriff auf Ressourcen wird strikt nach dem Motto „Vertraue niemandem, überprüfe alles" gehandhabt. Das bedeutet, dass Nutzer und Geräte sich vor jedem Zugriff authentifizieren müssen, z. B. mittels kryptografischer Zertifikate. Das Netzwerk vertraut keinem Gerät per se – auch nicht, wenn dieses sich bereits innerhalb des Perimeters befindet. Sicherheitsrichtlinien werden dabei dynamisch durchgesetzt. Richtlinien für Zugriffsrechte und Netzwerkressourcen können so je nach Standort, Benutzerrolle oder Gerätezustand variieren.
  - ✓ Grund: Das Zero-Trust-Modell reduziert Angriffsflächen und erschwert es Angreifern erheblich, sich „frei" im Netzwerk zu bewegen. Selbst im Falle einer Kompromittierung eines Geräts bleiben die Auswirkungen dank restriktiver, überprüfter Zugriffsregeln begrenzt.

- ☐ VLANs: VLANs werden zur granularen Trennung von Netzwerksegmenten eingesetzt.
  - ✓ Grund: Virtuelle LANs erleichtern die Administration und lassen sich flexibel an neue Anforderungen anpassen, ohne dabei physische Änderungen vornehmen zu müssen.

- ☐ Sicherheitsrichtlinien auf Netzwerkebene dokumentieren: Die Konfigurationen und Zugriffsregeln jeder Zone sind schriftlich oder in einem zentralen System dokumentiert und nachprüfbar.
  - ✓ Grund: Eine lückenlose Dokumentation ermöglicht schnellere Fehlerbehebung, erleichtert Sicherheits-Audits und unterstützt die Einhaltung von Compliance-Anforderungen. In erster Linie dient sie aber der Sicherheit, um Zugriffsregeln im Bedarfsfall schnell überprüfen zu können.

- ☐ Network Access Control (NAC) einsetzen: Die Implementierung einer NAC-Lösung ist möglich, um Geräte zu identifizieren und deren Sicherheitsstatus (z. B. Patch-Stand, Anti-Virus-Status) vor der Netzwerkzulassung zu prüfen. Systeme, die den Sicherheitsstatus (zeitweise) nicht mehr haben, wird der Zugriff auf besonders schützenswerte Ressourcen entzogen.
  - ✓ Grund: Mit NAC lässt sich sicherstellen, dass nur vertrauenswürdige und konforme Geräte auf bestimmte Zonen zugreifen können.

- ☐ Intrusion Detection/Prevention-Systeme (IDS/IPS) integrieren: IDS/IPS-Technologien werden eingesetzt, um verdächtige Aktivitäten oder Anomalien innerhalb der Segmentierung frühzeitig zu erkennen und ggf. zu blockieren.
  - ✓ Grund: IDS/IPS-Lösungen erhöhen die Sichtbarkeit von Angriffsmustern und verkürzen die Zeit zum Erkennen und Reagieren auf Sicherheitsvorfälle. Der fachgerechte Einsatz der professionellen Abwehrmaßnahmen ist entscheidend, um die gewünschte Wirkung zu entfalten.

- ☐ Micro-Segmentierung durch Software-Defined Networking (SDN) erwägen: SDN-Lösungen werden eingesetzt, um Zugriffe auf Anwendungsebene oder Workload-Ebene feingranularer zu steuern und zu überwachen.
  - ✓ Grund: Durch Micro-Segmentierung können spezifische Sicherheitsregeln für einzelne Anwendungen oder Dienste definiert und somit Angriffsflächen weiter reduziert werden.

6. Zentralen Internetübergangspunkt überwachen

Angreifer sind in der Regel nicht physisch vor Ort, sondern starten ihre Angriffe meist über das Internet. Die Überwachung des zentralen Internetübergangspunkts (z. B. Gateway, Firewall oder Router) ist daher von entscheidender Bedeutung für die eigene Sicherheit. Dieser Übergangspunkt bildet die erste Verteidigungslinie gegen eingehende und ausgehende Netzwerkkommunikation und ist somit ein besonders kritischer Kontrollpunkt. Durch eine kontinuierliche Überwachung des Datenverkehrs an diesem Übergangspunkt können verdächtige Aktivitäten frühzeitig erkannt werden. Dazu gehören beispielsweise ungewöhnlich hohe Datenmengen, Verbindungen zu bekannten Schadservern, verdächtige IP-Adressen oder abweichende Zugriffsmuster. Angreifer laden oft Angriffswerkzeuge oder Malware von bekannten Servern herunter oder sie kommunizieren mit Command & Control-Servern, um die Kontrolle über kompromittierte Systeme aufrechtzuerhalten. Moderne Überwachungssysteme wie Intrusion Detection Systeme (IDS), Intrusion Prevention Systeme (IPS) und Security Information and Event Management (SIEM)-Lösungen sammeln und analysieren die Netzwerkdaten in Echtzeit. Diese Tools können Anomalien erkennen, Warnungen ausgeben und im besten Fall automatisch Gegenmaßnahmen einleiten, um Angriffe zu stoppen oder einzudämmen. Darüber hinaus ist es wichtig, den Datenverkehr regelmäßig zu protokollieren und auszuwerten, um Muster zu identifizieren, die auf einen laufenden Angriff hindeuten. Die Implementierung von Blacklists, Whitelists und Deep Packet Inspection (DPI) kann die Überwachung noch effektiver machen. Auch die Nutzung von Verschlüsselung (z. B. TLS) sollte überwacht werden, um sicherzustellen, dass keine schädlichen Inhalte unbemerkt übertragen werden. Nicht zuletzt ist eine enge Zusammenarbeit mit dem IT-Sicherheitsteam sowie regelmäßige Schulungen der Mitarbeitenden notwendig, um die Überwachung effizient und reaktionsschnell zu gestalten. Insgesamt trägt eine konsequente Überwachung des Internetübergangspunkts wesentlich dazu bei, Angriffe frühzeitig zu erkennen, abzuwehren und die Sicherheitslage insgesamt zu verbessern.

Internetübergang-Bausteine:

- ☐ Next-Generation Firewall (NGFW) implementieren: Am zentralen Internetübergangspunkt ist eine NGFW installiert und konfiguriert, um Datenverkehr mittels Deep Packet Inspection auf Anomalien und bösartige Aktivitäten zu analysieren und verdächtige Verbindungen zu blockieren.
  - ✓ Grund: NGFWs bieten erweiterte Sicherheitsfunktionen und erhöhen die Transparenz im Netzwerkverkehr. So lassen sich Angriffe frühzeitig erkennen und effektiv unterbinden.

- ☐ DNS-Filterung aktivieren: Am zentralen Internetübergang ist eine DNS-Filterung eingerichtet, die Zugriffe auf bösartige Domänen unterbindet und Command & Control-Kommunikation blockiert.
  - ✓ Grund: Eine granular gesteuerte DNS-Auflösung verhindert, dass infizierte Systeme Kontakt zu Angreifern aufnehmen. Zudem erhöht sie die allgemeine Netzwerkhygiene.

- ☐ E-Mail-Sicherheitsgateway einsetzen: Ein spezielles E-Mail-Sicherheitsgateway prüft eingehende und ausgehende E-Mails auf Malware, Phishing und andere Bedrohungen.
  - ✓ Grund: Da ein Großteil von Angriffen weiterhin per E-Mail erfolgt, ist eine effektive E-Mail-Filterung entscheidend, um das Netzwerk am zentralen Übergang abzusichern.

- ☐ IDS/IPS für den Netzwerktraffic: IDS/IPS wird eingesetzt, um den gesamten eingehenden und ausgehenden Traffic am Internetgateway zu überwachen und ungewöhnliche Muster oder bekannte Exploits zu erkennen. Bei Bedarf werden Angriffe automatisch blockiert (IPS-Funktion).
  - ✓ Grund: IDS/IPS-Systeme sind wirksam, um bekannte, teils auch nur als verdächtige eingestufte, Datenmuster auf Netzwerkebene zu erkennen.

- ☐ Indicators of Compromise (IoCs) nutzen: Über ein zentrales Threat-Intelligence-Feed oder ähnliche Quellen werden regelmäßig aktualisierte IoCs (z. B. bösartige IPs, Domains, Hashes) in die Sicherheitslösungen (NGFW, IDS/IPS) eingespeist.
  - ✓ Grund: Durch den automatisierten Abgleich mit bekannten IoC-Datenbanken können bekannte Bedrohungen und schädliche Kommunikation sofort erkannt und blockiert werden.

- ☐ Zentralisierte Überwachung via zentralem Sicherheitsverwaltungstool (z. B. SIEM-System): Sämtliche Log-Daten aus Firewalls, DNS-Filter, IDS/IPS und weiteren Sicherheitssystemen werden in einem SIEM-System zusammengeführt und automatisiert ausgewertet.
  - ✓ Grund: Eine zentrale Sicht auf alle Sicherheitsereignisse ermöglicht eine schnelle Reaktion auf Angriffe und trägt zu einer ganzheitlichen Bedrohungserkennung bei.

- ☐ Egress-Filtering strikt gestalten: Auch der ausgehende Datenverkehr wird am zentralen Gateway gefiltert. Nur die unbedingt erforderlichen Ports und Protokolle sind freigegeben.
  - ✓ Grund: Mit einem strengen Egress-Filtering lässt sich verhindern, dass Schadprogramme Daten unbemerkt ins Internet exfiltrieren oder sich zu Command & Control-Servern verbinden.

- ☐ TLS/SSL-Inspection einrichten: Verschlüsselter Datenverkehr wird – unter Einhaltung datenschutzrechtlicher Vorgaben – an zentralen Gateways entschlüsselt, überprüft und dann wieder verschlüsselt.
  - ✓ Grund: Angreifer nutzen u. a. verschlüsselte Verbindungen, um Schadcode zu transportieren. Durch TLS/SSL-Inspection wird dieser Datenverkehr kontrolliert und Bedrohungen so erkannt.

- ☐ Zugriffs- und Konfigurationsprotokolle regelmäßig prüfen: Konfigurationsänderungen an zentralen Netzwerkkomponenten sowie administrative Zugriffe werden protokolliert, regelmäßig überprüft und analysiert.
  - ✓ Grund: Die frühzeitige Erkennung von ungewöhnlichen Änderungen oder Zugriffsversuchen erhöht die Betriebssicherheit und verhindert potenzielle Sabotage oder Datenmanipulation.

- ☐ Sicherheits- und Penetrationstests: Das zentrale Internetgateway und seine Sicherheitsfunktionen (NGFW, DNS-Filter, IDS/IPS) werden regelmäßig mithilfe von Penetrationstests und Audits auf Schwachstellen überprüft.
  - ✓ Grund: Durch Tests können Konfigurationsfehler, Sicherheitslücken und neue Angriffsmethoden aufgedeckt werden. Das ermöglicht eine frühzeitige Behebung von Schwachstellen, bevor sie von Angreifern ausgenutzt werden.

7. Ransomware-sichere Backups verwenden

Ransomware-Angriffe stellen eine ernstzunehmende Bedrohung für Unternehmen und Organisationen dar, da sie neben der Verschlüsselung von Daten zunehmend auch deren Exfiltration umfassen und somit den Geschäftsbetrieb erheblich stören können. Eine wirksame Verteidigung gegen die Folgen solcher Angriffe ist die Implementierung von Ransomware-sicheren Backups. Diese Art von Backups sind speziell so gestaltet, dass sie auch bei einem Angriff nicht verschlüsselt oder gelöscht werden können. Dazu gehören beispielsweise die Nutzung von sogenannten „Air-Gapped"-Backups, bei denen die Backup-Daten physisch vom Netzwerk getrennt sind oder die Speicherung in Write-Once-Read-Many (WORM)-Speichern, die eine nachträgliche Änderung oder Löschung verhindern. Auch die Nutzung von Cloud-Diensten mit speziellen Schutzmechanismen, wie Versionierung und Zugriffskontrollen, kann dazu beitragen, Backups vor Ransomware-Angriffen zu schützen. Ein weiterer wichtiger Aspekt ist die regelmäßige Aktualisierung und Überprüfung der Backups, um sicherzustellen, dass sie im Ernstfall schnell und umfänglich wiederhergestellt werden können. Dabei sollte die Backup-Strategie auch Wiederherstellungstests umfassen, um die Integrität und Verfügbarkeit der Daten zu gewährleisten. Es ist ratsam, mehrere Backup-Versionen zu pflegen, um auch bei längeren Angriffen oder Verschlüsselungen durch die Ransomware eine saubere Version wiederherstellen zu können. Neben technischen Maßnahmen ist die Sensibilisierung der Mitarbeitenden im Umgang mit Phishing und Social Engineering entscheidend, um die Infektionsgefahr zu minimieren. Insgesamt helfen Ransomware-sichere Backups, die Auswirkungen eines Ransomware-Angriffs im Schadensfall zu begrenzen, die Wiederherstellung zu beschleunigen und den Geschäftsbetrieb weitestgehend aufrechtzuerhalten.

Backup-Bausteine:

- ☐ 3-2-1-Regel umsetzen: Es werden mindestens drei Kopien der Daten erstellt, diese auf zwei verschiedenen Medien gespeichert und mindestens eine Kopie an einem anderen Standort aufbewahrt.
  - ✓ Grund: Senkt das Risiko eines totalen Datenverlustes bei Befall durch Ransomware oder physischen Schäden (z. B. Brand, Überspannung).

- ☐ Offline-Backups einrichten: Mindestens eine Kopie der Datensicherung wird vollständig vom Netz getrennt aufbewahrt, z. B. auf externen Festplatten oder magnetischen Bändern.
  - ✓ Grund: Werden Backups nicht permanent mit dem Netzwerk verbunden, können Angreifer sie nicht verschlüsseln oder manipulieren.

- ☐ Versteckte Backup-Systeme nutzen: Backup-Lösungen, die ausschließlich per Daten-Pull arbeiten, können implementiert werden, sodass sie von kompromittierten Systemen nicht aktiv angesteuert werden können.
  - ✓ Grund: Ein Angreifer kann die Backup-Dienste nur schwer entdecken oder sabotieren, wenn sie nicht direkt im Netzwerk als Ressource sichtbar sind.

- ☐ Sog. Immutable Backups (WORM) einsetzen: Backups werden auf schreibgeschützten Medien wie WORM-Tapes oder mit Software-Technologien gespeichert, die Änderungen oder Löschungen rückwirkend unmöglich machen.
  - ✓ Grund: Auf immutable Speichersystemen lassen sich Sicherungsdaten weder löschen noch nachträglich verändern, wodurch Ransomware-Schäden verhindert werden.

- ☐ Cloud-Backups mit Versionierung: Ein Cloud-Speicher mit eingebauter Versionierung und einem Schutzmechanismus hilft vor ungewolltem Überschreiben oder Löschen, z. B. „Object Lock".
  - ✓ Grund: Selbst wenn Ransomware lokale Dateien verschlüsselt, bleiben frühere Backup-Versionen dadurch in der Cloud bestehen und können wiederhergestellt werden.

- ☐ Beschränkte Zugriffsrechte für Backup-Systeme: Backup-Server und Speichermedien sind nur autorisierten Konten zugänglich – idealerweise mit MFA.
  - ✓ Grund: Minimale Berechtigungen und gesicherte Authentifizierung erschweren es Angreifern, die Sicherungsdaten zu kompromittieren.

- ☐ Regelmäßige Überprüfung und Testwiederherstellung: In festen Intervallen werden Restore-Tests durchgeführt und die Integrität der Backup-Daten überprüft.
  - ✓ Grund: Nur wenn Wiederherstellungen erfolgreich getestet wurden, ist sichergestellt, dass die Daten im Ernstfall tatsächlich nutzbar sind.

- ☐ Verschlüsselung der Backup-Daten: Backups werden verschlüsselt gesichert, z. B. mit AES-256, insbesondere bei Cloud-Speicher oder während der Übertragung.
  - ✓ Grund: Selbst bei einem unerlaubten Zugriff auf das Backup-Medium bleiben die Daten für Unbefugte unlesbar.

- ☐ Monitoring: Das Backup-System ist in ein Monitoring- und Alarmsystem integriert, um bei fehlerhaften oder ausbleibenden Sicherungen frühzeitig benachrichtigt zu werden.
  - ✓ Grund: Eine kontinuierliche Überwachung des Backup-Prozesses hilft, Probleme sofort zu erkennen und zeitnah gegenzusteuern.

- ☐ Dokumentation und Schulungen: Abläufe, Zuständigkeiten und Konfigurationen der Backup-Infrastruktur werden in einer zielgerichteten Dokumentation erfasst. Zudem finden regelmäßige Schulungen des IT-Personals zu Ransomware-Gefahren und Recovery-Prozessen statt.
  - ✓ Grund: Eine klare Prozessbeschreibung und geschulte Mitarbeitende beschleunigen die Wiederherstellung und stellen sicher, dass im Notfall richtig gehandelt wird.

8. Awareness und Social Engineering thematisieren

Social Engineering ist eine der häufigsten Angriffsmethoden, um Sicherheitslücken auszunutzen, da sie auf menschliches Verhalten abzielt. Viele Angriffe beginnen mit manipulativen E-Mails, Telefonanrufen oder anderen Kommunikationsformen, bei denen Angreifer versuchen, Mitarbeitende dazu zu bewegen, vertrauliche Informationen preiszugeben, schädliche Links zu öffnen oder Sicherheitsvorgaben zu umgehen. Diese Methoden sind oft so geschickt gestaltet, dass die Betroffenen den Betrugsversuch kaum erkennen. Um dieser Bedrohung wirksam entgegenzuwirken, ist ein gezieltes Awareness-Programm unerlässlich. Schulungen und Sensibilisierungsmaßnahmen sollten regelmäßig durchgeführt werden, um Mitarbeitende für die typischen Merkmale von Social Engineering-Angriffen zu sensibilisieren. Dabei ist es wichtig, konkrete Beispiele und praktische Übungen einzusetzen, damit die Teilnehmenden typische Angriffsszenarien erkennen und entsprechend reagieren können. Ein wichtiger Bestandteil der Awareness-Arbeit ist die Erschaffung und Förderung einer Sicherheitskultur, bei der Mitarbeitende ermutigt werden, bei verdächtigen Aktivitäten sofort das Sicherheits- oder IT-Team zu informieren, anstatt unüberlegt zu handeln. Zudem sollten klare Verfahrensanweisungen vorhanden sein, wie in verdächtigen Situationen zu reagieren ist, beispielsweise bei unerwarteten E-Mail-Anfragen nach Passwörtern oder sensiblen Daten. Neben Schulungen sind auch technische Maßnahmen sinnvoll, wie z. B. Spam-Filter, E-Mail-Authentifizierungsverfahren und Multi-Faktor-Authentifizierung, um die Angriffsflächen zu reduzieren. Die regelmäßige Durchführung von Phishing-Tests kann zudem helfen, das Bewusstsein der Beschäftigten zu stärken und Schwachstellen aufzudecken. Insgesamt ist die kontinuierliche Sensibilisierung der Mitarbeitenden die wichtigste Maßnahme, um Social Engineering-Angriffe frühzeitig zu erkennen und abzuwehren. Eine gut informierte Belegschaft bildet somit die erste Verteidigungslinie gegen diese Art von Angriffen.

Awareness-Bausteine:

- ☐ Regelmäßige Sensibilisierungsschulungen: Für alle Mitarbeitenden werden verpflichtende Schulungen oder E-Learnings organisiert, in denen typische Social-Engineering-Methoden wie Phishing, Vishing oder Tailgating verständlich erklärt sind.
  - ✓ Grund: Durch kontinuierliche Aufklärung und Sensibilisierung lernen Beschäftigte, verdächtige Situationen und manipulative Tricks schneller zu erkennen und richtig zu reagieren.

- ☐ Praxisnahe Phishing-Simulationen: Regelmäßige Phishing-Übungen werden durchgeführt, um das Verhalten der Mitarbeitenden in realistischen Szenarien zu überprüfen.
  - ✓ Grund: Nur durch praktische Tests lassen sich Schwachstellen im Sicherheitsbewusstsein aufdecken und gezielt beheben.

- ☐ Phishing mit KI-generierten E-Mails: Mitarbeitende werden dafür sensibilisiert, dass moderne Angriffe mithilfe Künstlicher Intelligenz realistisch wirkende, individuelle E-Mails erzeugen können.
  - ✓ Grund: KI-Modelle erstellen täuschend echte Texte und erschweren die Erkennung von Phishing. Mitarbeitende sollten entsprechend geschult werden, um solche Angriffe zu entlarven.

- ☐ Meldung bei Vorfall: Es existiert ein Prozess, der klar festlegt, wo Mitarbeitende verdächtige E-Mails oder sonstige Angriffsversuche melden können (z. B. über ein Helpdesk-Ticket-System).
  - ✓ Grund: Frühe Meldungen ermöglichen ein schnelles Eingreifen durch das Security-Team und können größere Schäden verhindern.

- ☐ Gesetzliche Meldeverpflichtungen: Interne Prozesse werden benötigt, um im Fall eines Verstoßes zeitnah die zuständigen Behörden zu informieren (z. B. Meldepflicht nach Art. 33 DS-GVO).
  - ✓ Grund: Das Einhalten gesetzlicher Vorgaben beugt Bußgeldern und Reputationsschäden vor und zeigt professionelles Krisenmanagement.

- ☐ Social-Media-Nutzung: Mitarbeitende werden darauf hingewiesen, mit persönlichen Informationen in sozialen Netzwerken äußerst sparsam umzugehen. Interne Richtlinien zum Thema Datensparsamkeit sind vorhanden oder werden erarbeitet.
  - ✓ Grund: Social Engineers sammeln oft Informationen aus öffentlichen Profilen, um gezielte Angriffe (Spear-Phishing) zu planen.

- ☐ Kontinuierliche Erfolgskontrolle: Die Wirksamkeit der Awareness-Maßnahmen wird regelmäßig durch Auswertung von Phishing-Simulationen und Prüfungen des Sicherheitsbewusstseins überprüft. Die Trainingsinhalte sind entsprechend an neue Bedrohungslagen anzupassen.
  - ✓ Grund: Bedrohungsszenarien ändern sich ständig. Nur wer seine Strategie fortlaufend optimiert, bleibt effektiv gegen Social Engineering gewappnet.

- ☐ Spear-Phishing und Whaling: Spezialisierte Schulungen zu personalisierten Angriffsmethoden wie Spear-Phishing werden angeboten. Dabei wird auch das Thema Whaling behandelt, bei welchen insbesondere Führungskräfte mit individuell zugeschnittenen Angriffen ins Visier genommen werden.
  - ✓ Grund: Gezielte Angriffe erschleichen leichter Vertrauen. Spezielle Schulungen für ausgewähltes Personal helfen, auch hochgradig personalisierte Angriffe zu erkennen.

- ☐ Betrug bei gefälschten Rechnungen: Zahlungen über hohe Beträge erfolgen nur nach einem verbindlichen 4-Augen-Prinzip oder einem zusätzlichen Freigabeprozess.
  - ✓ Grund: Kriminelle nutzen Social-Engineering-Methoden, um per E-Mail scheinbar legitime Rechnungen oder Zahlungsaufforderungen zu fälschen. Eine klare Prozesskette schützt vor teuren Fehlüberweisungen.

- ☐ Kreatives Live-Rollenspiel als Security-Event: Ein internes Rollenspiel kann organisiert werden, bei dem „Angreifer" und „Verteidiger" in realitätsnahen Social-Engineering-Situationen gegeneinander antreten. Zum Beispiel könnte ein Team versuchen, per Telefon oder E-Mail an interne Informationen zu gelangen, während das andere Team dies erkennt und abwehrt.
  - ✓ Grund: Ein spielerisches Event schafft hohe Motivation und vermittelt praxisnah wichtige Verhaltensregeln. Gleichzeitig stärkt es das Bewusstsein, dass jeder Mitarbeitende zur „menschlichen Firewall" des Unternehmens gehört.

9. Software-Updates durchführen

Angriffe sind nicht immer ein technisches Meisterwerk. Viele Cyberangriffe nutzen schlicht bekannte Schwachstellen in Softwareprodukten aus, die bereits in der Vergangenheit identifiziert wurden. Solche Sicherheitslücken werden oftmals in öffentlich zugänglichen Datenbanken dokumentiert und sind für Angreifer leicht auffindbar. Wenn diese Schwachstellen nicht zeitnah geschlossen werden, bieten sie Angreifern eine einfache Möglichkeit, in Systeme einzudringen, Schadsoftware zu installieren oder Daten zu manipulieren. Ein effektiver Schutz gegen solche Angriffspunkte ist die konsequente und regelmäßige Durchführung von Software-Updates und Patch-Management. Durch das zeitnahe Einspielen von Sicherheitsupdates können bekannte Schwachstellen geschlossen werden, bevor sie von Angreifern ausgenutzt werden. Dies gilt sowohl für Betriebssysteme, Anwendungssoftware, Netzwerkkomponenten als auch für spezielle Sicherheitslösungen. Ein gut organisiertes Patch-Management umfasst die Identifikation relevanter Updates, die Priorisierung nach Sicherheitsrisiko, die automatisierte oder manuelle Verteilung der Patches sowie die Überprüfung der erfolgreichen Installation. Zudem ist es wichtig, Updates in einer kontrollierten Umgebung zu testen, um Kompatibilitätsprobleme zu vermeiden, bevor sie in der produktiven Umgebung ausgerollt werden. Neben der technischen Umsetzung ist auch die Sensibilisierung der Mitarbeitenden und der IT-Verantwortlichen notwendig, um die Relevanz regelmäßiger Updates zu vermitteln. Automatisierte Update-Mechanismen – wo möglich – erleichtern die Einhaltung der Aktualisierungsintervalle erheblich. Insgesamt ist die konsequente Aktualisierung der Software eine maßgebliche Sicherheitssäule, um Angriffsflächen zu reduzieren, Sicherheitslücken zu schließen und die Integrität sowie Verfügbarkeit der IT-Infrastruktur zu gewährleisten.

Update-Bausteine:

- ☐ Patch-Management-Plan: Ein strukturierter Plan, der alle Prozesse des Patch-Managements abdeckt – einschließlich der Identifikation, Priorisierung, Tests und Implementierung von Updates –, ist vorhanden.
  - ✓ Grund: Ein klarer Plan minimiert Verzögerungen und stellt sicher, dass kritische Updates zeitnah umgesetzt werden.

- ☐ Inventarisierung der IT-Landschaft: Eine vollständige Übersicht aller eingesetzten Hard- und Softwarekomponenten, inklusive ihrer Versionsstände und Patch-Levels, ist vorhanden.
  - ✓ Grund: Eine solche Übersicht gilt als Grundvoraussetzung für einen geregelten und sicheren IT-Betrieb. Ohne eine genaue Kenntnis der Systeme können kritische Sicherheitslücken übersehen werden. Ein effizienter IT-Betrieb samt Support kann nur mit Überblick und Struktur gelingen.

- ☐ Regelmäßige Informationsbeschaffung zu Sicherheitslücken: Sicherheitswarnungen und Veröffentlichungen von Herstellern, CERT-Bund oder Fachmedien werden aktiv überwacht, um zeitnah über neue Schwachstellen informiert zu sein.
  - ✓ Grund: Eine schnelle Reaktion auf neue Schwachstellen ist entscheidend, um Angriffsmöglichkeiten zu reduzieren. Oftmals werden Lücken nach wenigen Tagen, zum Teil Stunden, ausgenutzt.

- ☐ Testumgebungen: Alle Patches werden in einer dedizierten Testumgebung getestet, bevor sie in der Produktivumgebung ausgerollt werden.
  - ✓ Grund: Fehlerhafte Updates können den Betrieb beeinträchtigen oder zu Ausfällen führen. Ein sorgfältiges Testen kann ungewollte Probleme samt verursachter Lücken aktiv verhindern.

- ☐ Priorisierung von Patches: Um die Sicherheit angemessen zu steuern, findet anhand von festgelegten Kriterien eine Priorisierung von Updates statt, basierend auf der Schwere der Schwachstelle (z. B. CVSS-Score) und der Kritikalität des betroffenen Systems.
  - ✓ Grund: Kritische Systeme und Sicherheitslücken müssen bevorzugt behandelt werden, um das Risiko zu minimieren.

- ☐ Automatisierung: Tools wie WSUS oder Endpoint-Management-Systeme werden genutzt, um Patches automatisiert zu verteilen und den Prozess zu vereinfachen.
  - ✓ Grund: Automatisierung spart nicht nur Ressourcen, sondern sorgt auch für konsistente Update-Implementierungen.

- ☐ Dokumentation aller Patch-Aktivitäten: Alle durchgeführten Patch-Aktivitäten, einschließlich getesteter und eingespielter Updates, werden nachvollziehbar dokumentiert.
  - ✓ Grund: Eine detaillierte Dokumentation erleichtert die Fehlerbehebung und die Erfüllung gesetzlicher Nachweispflichten.

- ☐ Reaktionsstrategie für ungepatchte Sicherheitslücken: Notfallpläne, wie Virtual Patching oder Abschottung durch Firewalls, sind vorhanden oder werden entwickelt, um in dem Falle, dass Patches nicht zeitnah verfügbar oder implementierbar sind, schnell reagieren zu können.
  - ✓ Grund: Zero-Day-Exploits und nicht verfügbare Patches dürfen keine unkontrollierte Sicherheitslücke darstellen. Im Alltag wird es sich nicht vermeiden lassen, dass Lücken ohne direkte Patchmöglichkeit bekannt werden – eine Vorbereitung solcher Szenarien ist entscheidend, um dennoch einen sicheren Betrieb zu gewährleisten.

- ☐ Überprüfung der Update-Prozesse: Die Wirksamkeit und Effizienz des Patch-Managements werden regelmäßig evaluiert, um Prozesse an neue Anforderungen oder Bedrohungen anzupassen.
  - ✓ Grund: Sicherheitsanforderungen und Bedrohungslagen ändern sich stetig, und Prozesse müssen aktuell bleiben.

- ☐ Schulung und Sensibilisierung der Mitarbeitenden: Die IT-Mitarbeitenden werden regelmäßig zu neuen Entwicklungen und Best Practices im Patch-Management geschult.
  - ✓ Grund: Ein geschultes Team ist besser vorbereitet, um Sicherheitslücken schnell und effizient zu schließen.

10. Domain Controller absichern

Was wollen kriminelle Cyberakteuer überhaupt? Am Ende zielt ein Angriff auf eine Organisation meist auf die „Kronjuwelen" ab, d. h. auf die besonders wertvollen Daten. Der ultimative Weg dorthin ist die Übernahme von zentralen und wichtigen Servern wie beispielsweise des Windows Domain Controller. Der Domain Controller ist das Herzstück einer Windows-basierten IT-Infrastruktur, da er die zentrale Verwaltung von Benutzerkonten, Zugriffsrechten und Sicherheitsrichtlinien übernimmt. Aufgrund seiner entscheidenden Bedeutung und der sensiblen Daten, die er verwaltet, stellt der Domain Controller also ein besonders attraktives Ziel für Angreifer dar. Eine erfolgreiche Übernahme eines solchen Servers ermöglicht es, die gesamte Netzwerkumgebung zu kontrollieren, Benutzerkonten zu kompromittieren und damit weitreichende Schadenspotenziale zu realisieren. Um den Schutz des Domain Controllers zu gewährleisten, sind mehrere Maßnahmen erforderlich. Zunächst sollte der Server in einem separaten, besonders abgesicherten Netzwerksegment betrieben werden, um den Zugriff auf autorisierte Personen und Systeme zu beschränken. Die physische Sicherheit sowie der Zugriff auf den Server sollten streng kontrolliert werden. Darüber hinaus ist die Implementierung von Mehr-Faktor-Authentifizierung für administrative Zugriffe auf den Domain Controller essentiell. Es sollten nur notwendige Administratoren Zugriff haben – diese Zugriffe müssen genau protokolliert werden. Die Nutzung von sogenannten „Privileged Access Workstations" (PAWs), also speziell abgesicherten Arbeitsstationen für Administratoren, erhöht die Sicherheit zusätzlich. Regelmäßige Sicherheitsupdates und Patches sind ebenso unerlässlich, um bekannte Schwachstellen zu schließen. Zudem ist der Server durch eine robuste Firewall, Intrusion Detection Systeme (IDS) und Monitoring-Lösungen geschützt, um ungewöhnliche Aktivitäten frühzeitig zu erkennen. Ein weiterer wichtiger Punkt ist die regelmäßige Überprüfung der Sicherheitskonfigurationen sowie das Durchführen von Sicherheitsaudits und Penetrationstests. Die Implementierung eines Backup- und Wiederherstellungsplans für den Domain Controller ist ebenfalls unverzichtbar, um im Falle eines Angriffs schnell reagieren und den Betrieb wiederherstellen zu können. Insgesamt ist der Schutz des Domain Controllers eine zentrale Maßnahme, um die Integrität und Sicherheit der gesamten IT-Infrastruktur zu gewährleisten und die „Kronjuwelen" vor Angriffen zu bewahren.

Domain Controller-Bausteine:

- ☐ Zugangsbeschränkung und Least-Privilege-Prinzip: Der Zugriff auf den Domain Controller ist auf ein absolutes Minimum beschränkt – nur Administratoren mit spezifischem Bedarf haben Zugang. Administrative Rechte werden nach dem Least-Privilege-Prinzip vergeben.
  - ✓ Grund: Minimierung der Angriffsfläche durch Einschränkung auf zwingend erforderliche Berechtigungen.
- ☐ Serverhärtung durch Deaktivierung unnötiger Dienste: Auf dem Domain Controller sind alle nicht benötigten Dienste und Funktionen, wie z. B. Druckdienste oder Webserver, deaktiviert.
  - ✓ Grund: Reduzierung potenzieller Angriffsvektoren durch die Minimierung von Schwachstellen.

- ☐ Netzwerksegmentierung und IDS-Integration: Der Domain Controller ist in einem isolierten Netzwerksegment untergebracht, das nur von autorisierten Systemen erreicht werden kann. Intrusion-Detection-Systeme (IDS) überwachen den Datenverkehr in diesem Segment.
  - ✓ Grund: Dies sorgt für einen Schutz vor unautorisierten Zugriffen und Erkennung potenzieller Angriffe.

- ☐ MFA bei Domain Controller: MFA ist für alle administrativen Zugriffe auf den Domain Controller zwingend vorgeschrieben und aktiv.
  - ✓ Grund: MFA dient hier als zusätzliche Sicherheitsschicht zur Abwehr von Angriffen, selbst wenn Passwörter kompromittiert wurden.

- ☐ Sicherheitsupdates und Patches: Betriebssystem, Active Directory und alle installierten Anwendungen auf dem Domain Controller werden regelmäßig gepatcht und aktualisiert.
  - ✓ Grund: Diese Routine hilft, bekannte Schwachstellen zu schließen, bevor sie von Angreifern ausgenutzt werden können.

- ☐ Monitoring und Anomalieerkennung mit SIEM: Ein SIEM-System sammelt und analysiert Log-Daten des Domain Controllers, um verdächtige Aktivitäten und Anomalien frühzeitig zu erkennen.
  - ✓ Grund: Angriffe können durch proaktive Überwachung identifiziert und abgewehrt werden.

- ☐ Backups: Backups des Domain Controllers werden regelmäßig erstellt, überprüft und offline gespeichert. Mindestens eine Kopie befindet sich physisch vom Netzwerk getrennt.
  - ✓ Grund: Sicherstellung der Wiederherstellbarkeit im Falle eines Angriffs oder Datenverlustes.

- ☐ Netzwerkzugriffskontrollen: Ein Netzwerkzugriff auf den Domain Controller ist nur von autorisierten Quellen erlaubt – gesteuert durch strikte Firewall-Regeln und Zugriffskontrolllisten (ACLs).
  - ✓ Grund: Dies verhindert unbefugte Zugriffe und reduziert das Risiko von Lateral Movement im Netzwerk.

- ☐ Schutz von Administrator-Konten: Administrator-Konten werden überwacht und durch Maßnahmen wie separate Passwörter, Aktivitätsprotokollierung und Zeitbeschränkungen gesichert.
  - ✓ Grund: Administrator-Konten gelten als die am meisten gefährdeten Konten und benötigen daher einen besonderen Schutz.

- ☐ Honeypot-Mechanismen im DC-Segment: Kontrollierte Honeypot-Systeme oder -Konten werden in der Nähe des Domain Controllers platziert, um potenzielle Angreifer anzulocken und deren Vorgehensweise zu überwachen.
  - ✓ Grund: Angreifer werden abgelenkt und identifiziert, während das echte System geschützt bleibt. Gleichzeitig liefert dies wertvolle Informationen über Angriffsstrategien und Schwachstellen.

Bayerisches Landesamt für
Datenschutzaufsicht

Checkliste Cyberfestung:
10 Punkte für mehr Datensicherheit

Stand der Checkliste:
10.11.2025, v1.1

Herausgeber und Kontakt:
Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Promenade 18 | 91522 Ansbach
www.lda.bayern.de | Tel.: 0981 180093-100
poststelle@lda.bayern.de