CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Häufig ausgenutzte konzeptionelle Schwächen bei IT-Sicherheitsarchitekturen

- Prüfdokument -

Inhaltsverzeichnis

1. Zweck des Dokuments

Dieses Prüfdokument für häufig ausgenutzte konzeptionelle Schwächen bei IT-Sicherheitsarchitekturen soll bei folgenden Aufgaben helfen:

- Die bestehende IT-Sicherheitsarchitektur prüfen und möglichst sicher gestalten.
- Nach einem Cyberangriff ein möglichst sicheres Netz wiederaufbauen.

Das vorliegende Dokument hat die Cybersicherheitsagentur Baden-Württemberg (CSBW) zusammengestellt. Es erhebt keinen Anspruch auf Vollständigkeit, vielmehr soll es einen allgemeinen Überblick über den Aufbau, die Konfiguration und den Betrieb von IT-Systemen bieten. Die CSBW spricht keine Empfehlungen zur technischen Infrastruktur aus.

Für ein detaillierteres und weitreichenderes IT-Sicherheitskonzept verweist die CSBW auf das IT-Grundschutz-Kompendium[1] des Bundesamt für Sicherheit in der Informationstechnik (BSI). Um der fortschreitenden Entwicklung der Technik gerecht zu werden, aktualisiert die CSBW das Dokument fortlaufend.

2. IT-Dokumentation

Eine aktuell gehaltene IT-Dokumentation hilft bei der Analyse und Erkennung von Schwachstellen und gibt helfenden Dritten die Möglichkeit, sich im Netz zurechtzufinden. Eine solche Dokumentation ist grundsätzlich empfehlenswert.

2.1. Netzwerkplan

Ein ausführlicher Netzwerkplan mit definierten Netzwerkübergängen und skizzierten Servern und Clientnetzen hilft, das Netzwerk strukturiert und übersichtlich zu halten. Ein detaillierter Netzwerkplan ist unabdingbar.

2.2. Asset-Management

Die Dokumentation von Servern, Clients und mobilen Endgeräten dient dazu, den Installations- und Konfigurationsstand dieser Geräte zu überwachen. Ein Überblick über alle verwendeten Geräte im Netz ist wünschenswert.

3. Netzwerk

Die nachfolgenden Abschnitte gehen auf die Netzsegmentierung ein sowie auf die Verwendung von Firewalls, VPN[2], Ports, EDR[3] und SIEM[4].

---

[1] BSI IT-Grundschutz-Kompendium: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[2] Virtual Private Network

[3] Endpoint Detection and Response

[4] Security Information and Event Management

3.1. Netzsegmentierung

Netze sollten segmentiert werden. Achten Sie dabei auf eine möglichst feingranulare Unterteilung des Netzwerkes. Dies erschwert die Ausbreitung eines Angreifers im Netzwerk stark. Es kann sinnvoll sein, bspw. das Netzwerk nach Sachgebieten zu unterteilen (bspw. Verwaltungsnetz, Technikernetz, Forschungsnetz). Diese Sachgebiete können Sie wiederum in Aufgabengebiete unterteilen, bspw. Administrator, Technische Redaktion, Technik.

Warum sollte eine feingranulare Segmentierung stattfinden?

- Nicht alle Personen benötigen Zugriff auf alle Server oder sonstige Systeme.
- Erschwert das Lateral Movement[5] für den Angreifer.
- Nur wenn zwingend erforderlich, können auch Betriebssysteme eingesetzt werden, die vom Hersteller nicht mehr unterstützt und aktuell gehalten werden. Diese sollten allerdings zwingend von anderen Clients separiert werden (kein Internetzugriff usw.).

Eine geeignete Netzsegmentierung sollte anhand des Netzwerkplans umgesetzt werden. Übergänge in ein Netzwerk einer dritten Institution sollten in einem separaten Netzsegment implementiert werden.

3.2. Zugangskontrollen

Neben der oben genannten VLAN[6]-Trennung helfen auch Netzwerkzugangskontrollen dabei, den Zugang zum Netzwerk zu kontrollieren. Diese Kontrollen können greifen, sobald ein Client nicht den Sicherheitsmaßnahmen entspricht (z. B. keine Antivirus-Software, kein offiziell ausgegebener Client). Eine solche Zugangskontrolle ist empfehlenswert.

3.3. Firewall

Jeder Netzübergang sollte mit einer Firewall abgesichert werden. Bei Netzübergängen ins Internet ist zusätzlich der Einsatz eines IDS/IPS[7]-Systems sinnvoll. Die Absicherung zwischen den Netzen mit einer Firewall ist essenziell wichtig. Zusätzlich können bestimmte Kategorien über die Firewall gesperrt werden (bspw. Pornografie, Waffen).

3.3.1. VPN (2FA[8])

Richten Sie keine automatische VPN-Einwahl beim Hochfahren des Clients ein. Die Einwahl ins VPN sollte immer explizit erfolgen, bestenfalls mit einem weiteren Authentifizierungsschritt. Setzen Sie wenn möglich immer eine 2FA um.

---

[5] Lateral Movement: Hierunter wird die schrittweise, durch unbekannte Täter vorgenommene Ausbreitung im Netzwerk der geschädigten Institution verstanden.
[6] Virtual Local Area Network
[7] Intrusion Detection System / Intrusion Prevention System
[8] Two Factor Authentication

3.3.2. Ports öffnen

Eine gute Herangehensweise ist, zunächst gar keinen Port freizugeben. Jede Portfreigabe sollte im Einzelfall beurteilt werden.

3.4. EDR

Eine weitere empfehlenswerte Ausbaustufe ist der Einsatz eines geeigneten EDR-Systems.

3.5. SIEM - Security Information and Event Management

Ein SIEM liefert eine wichtige Komponente im IT-Sicherheitskonzept. Ohne ein SIEM wäre ein kurzfristiger bis mittelfristiger Ansatz, zumindest folgende Punkte umzusetzen:

- Generell werden in Windows-Betriebssystemen nur wenige Ereignisse aufgezeichnet. Prüfen Sie daher, über welchen Zeitraum Log-Einträge auf den Systemen vorhanden sind.
- Da das Speichervolumen auf den Systemen immer begrenzt ist, müssen früher oder später Log-Files gelöscht werden. Es empfiehlt sich Log-Dateien auf einem dedizierten Collector-System zu sammeln. Dies können Sie bspw. über das Windows-Event-Forwarding realisieren.
- Die Implementierung eines zentralen Logging-Systems hat den Vorteil, dass insbesondere die Sicherheit innerhalb eines Netzwerkes erhöht wird. So können Ereignisse in Echtzeit überwacht werden und auf verdächtige Aktivitäten kann kurzfristig reagiert werden. Eine Löschung lokal gespeicherter Logdateien ist somit nicht möglich.
- Prüfen Sie, ob der Einsatz von Sysmon oder bspw. Graylog relevant sein könnte. Betrachten Sie außerdem die erweiterten „Windows Event Log Auditing“-Funktionalitäten (Command-line Auditing, Security Auditing, …)

Logs sollten so groß sein, dass sie einen Zeitraum von mindestens einer Woche umfassen:

Windows-Events	**Client**	**Server**	**Domaincontroller**
Anwendung/Application	20 MB	100 MB	100 MB
System	20 MB	500 MB	500 MB
Sicherheit/Security	500 MB	2 GB	> 2 GB
Windows Powershell	500 MB	1 GB	1 GB
PowerShell Operational	500 MB	1 GB	1 GB

4. Server- und Clientsysteme

Für Server- und Clientsysteme sind die nachfolgenden Punkte zur Erhöhung der Sicherheit empfehlenswert.

4.1. Patchmanagement

Hier empfiehlt es sich, einen Patchmanagement-Prozess einzuführen. Damit ist man in der Lage, Schwachstellen zeitnah zu schließen. Systeme, die keine Systempatches mehr erhalten, sollten ggf. isoliert werden, sodass die Wahrscheinlichkeit eines Angriffes deutlich minimiert wird.

In der Windows-Umgebung bietet sich ein WSUS[9]-Server an. Hierbei können zentral gesteuerte Update-Rollouts für Microsoft-Betriebssysteme, Microsoft Office und weitere Microsoft-Applikationen geplant und initiiert werden. Um Updates für andere wichtige Applikationen automatisiert bereitzustellen, bietet sich insbesondere der Einsatz eines Patchmanagementsystems an.

4.2. Backup-Konzept

Eine unvollständige oder nicht vorhandene Datensicherung birgt große Risiken. Daher ist ein vollständiges Datensicherungskonzept unerlässlich. Neben allgemeingültigen Sicherungskonzepten wie der 3-2-1 Regel empfiehlt sich die Umsetzung folgender Maßnahmen:

- Der Backupserver sollte nicht in der Domäne angesiedelt sein.
- Der Wiederherstellungsprozess sollte detailliert dokumentiert sein.
- Weiter bietet es sich an, die Wiederherstellung der Daten zu testen. So können evtl. auftretende Probleme im Ernstfall vermieden werden.
- Der Zugang zu den Backups sollte möglichst mit einer Multi-Faktor-Authentifizierung (MFA) abgesichert werden.
- Die Backups sollten nicht veränderbar sein (bspw. Immutable Flag).

Zu bedenkende Punkte

Um bei einem Ransomware-Angriff nicht die Kompromittierung des Backups zu riskieren und um bei einem möglichen Gebäudebrand einen Datenverlust zu umgehen, müssen folgenden Punkte bedacht werden:

- In welchem Zyklus werden die Sicherungen auf ein vom Netz getrenntes Medium geschrieben?
- Ist ein Backup an einem anderen Standort geplant?

4.2.1. Backup-Recovery-Konzept:

Die Erstellung eines Backup-Recovery-Konzepts ist notwendig. Dabei sind regelmäßige Wiederherstellungstests ratsam.

[9] Windows Server Update Services

4.3. Monitoring

Generell ist ein Monitoring von Server, Netzwerk, Applikationen und Speichern sinnvoll. Hierbei stehen auffällige Systemzustände im Fokus; diese sollen schneller entdeckt werden.

Zu bedenkende Punkte

- Welche Systemzustände sollen überwacht werden?
- Was ist der Grenzwert zu einer Anomalie und wie werden Anomalien entdeckt?
- Welches System soll für das Monitoring eingesetzt werden?
- Ist der zyklische Einsatz eines AD[10]-Auditing-Tools wie bspw. Bloodhound angedacht?

Empfehlung

Die Etablierung neuer Prozesse zur Reaktion auf eine Alarmierung durch das Überschreiten von Schwellenwerten wird empfohlen. Bspw. sollten zuständige Mitarbeitende informiert werden, wenn es Anzeichen auf eine Brute-Force-Attacke gibt. Je nach Schwere und Intensität des Ereignisses müssen die Mitarbeiter in die Analyse des Vorfalls übergehen.

4.4. Makro Policy

Nur solche Makros, welche mit einer bekannten Signatur signiert sind, sollten ausführbar sein (z.B. über eine Gruppenrichtlinie geregelt). Hierzu ist der Einsatz eines Zertifizierungsservers zur Validierung der bekannten Signaturen sinnvoll.

4.5. Remotedesktopverbindungen

Soweit möglich empfiehlt es sich keine RDP[11]-Nutzung zuzulassen. Sollte eine Nutzung von RDP unumgänglich sein, ist die Erarbeitung eines Konzepts für die RDP-Nutzung empfehlenswert:

- Entfernung der administrativen Gruppe für die RDP-Nutzung.
- Nur explizite, personalisierte Accounts zulassen. Dies verhindert, dass ein neu angelegtes Administratorkonto direkt Zugriff auf den RDP-Dienst erhält.
- Schützen von Remotedesktop-Anmeldeinformationen mit Remote Credential Guard.

4.6. AV[12]-Lösung

Der Schutz vor Viren und Malware gehört zur Basisausstattung. Dabei müssen vor allem die Endpoints (Clients sowie Server) innerhalb des Netzwerks geschützt werden.

Neben der Endpoint-Protection sollte idealerweise auch auf dem Web- bzw. Mail-Gateway ein Virenscanner eines zweiten Herstellers platziert werden. Hinsichtlich des Rollouts und Konfiguration der Antivirensoftware bzw. der zentralen

[10] Active Directory
[11] Remote Desktop Protocol
[12] Anti-Virus

Überwachung ist eine zentralisierte Konsole (lokale Installation oder Cloud-Lösung) empfehlenswert.

So können bspw. der Update-Zustand, Virenbefunde oder Störungen innerhalb der Managementkonsole ausgewertet bzw. bei Bedarf Gegenmaßnahmen eingeleitet werden. Daneben bieten Hersteller Produkte zur Abwehr von Ransomware-Angriffen sowie Exploit-Prevention an, die mit Verhaltensanalysen bzw. Machine-Learning-Algorithmen Bedrohungen auf den Clients bzw. innerhalb des Netzwerks feststellen können.

4.6.1. E-Mail-Vorprüfung

Eingehende E-Mails werden auf schadhafte Anhänge geprüft. Externe E-Mails werden im Betreff gekennzeichnet.

4.6.2. Micro-Virtualisierung

Für den Aufruf unbekannter Quellen sollte der Browser besonders gesichert sein (bspw. Sandbox Browser). Werden Dokumente aus externen Quellen geöffnet, so sind diese ebenfalls in einer Micro-Virtualisierung zu öffnen.

4.7. BitLocker

Eine vollständige Verschlüsselung der Festplatte ist auf physischen Systemen empfehlenswert. Durch das Tool kann nicht nur eine vollständige Verschlüsselung der Festplatte vorgenommen werden, sondern auch die Verschlüsselung belegter Bereiche. Wird die Festplatte gestohlen, so ist der Zugriff auf die verschlüsselten Daten nicht möglich.

4.8. Passwortkomplexität

In den vom BSI[13] vorgeschlagenen Empfehlungen sollte eine Passwortrichtlinie auf folgenden Regeln basieren:

- Das Passwort sollte nicht einfach zu erraten sein.
- Namen, Straßennamen und Geburtsdatum sollten nicht verwendet werden.
- Das Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen.
- Passwörter mit 12 Zeichen oder mehr bieten einen besseren Schutz als komplexe Passwörter mit häufigem Änderungsintervall.
- Für die Speicherung von Passwörtern bieten sich sogenannte Passwort-Safes an (bspw. KeePass).

4.9. Device- und Applikationskontrolle

Schnittstellen (bspw. USB-Ports oder Bluetooth) und Laufwerke stellen in IT-Systemen in Kombination mit den Berechtigungen von Usern ein Risiko dar. So können bspw. je nach Berechtigung ausführbare Dateien von einem USB-Stick gestartet werden. Im Worst-Case-Szenario gelangt so Schadcode ins Netzwerk.

[13] Bundesamt für Sicherheit in der Informationstechnik

Durch den Einsatz von speziellen Software-Lösungen können via Richtlinie nur bestimmte Speichermedien zugelassen werden. Anhand von Richtlinien können Administratoren festlegen, welcher Benutzer an welchem Gerät ein bestimmtes Device anschließen und verwenden darf. Die Umsetzung eines Verfahrens zur Device-Kontrolle ist mittelfristig empfehlenswert.

Applikationskontrollen können die Ausführung von Malware, Adware und sonstige PUA[14]s vermeiden. Hierfür bietet Microsoft seit Windows 10 standardmäßig die Windows Defender-Anwendungssteuerung und AppLocker-Features an.

Hinsichtlich der Umsetzung empfiehlt es sich, dass nur Applikationen, die auf einer Whitelist gelistet sind vom Benutzer ausgeführt werden können.

Die Identifikation der Applikationen erfolgt im Idealfall anhand des Datei-Hashes. Digitale Signaturen sind nur bei Ausstellern mit hohem Vertrauensniveau geeignet, da PUAs nicht selten auch über legitime Signaturen verfügen und Malware potentiell mit kompromittierten Zertifikaten signiert werden kann. Für die Erstellung der einzelnen WDAC[15]-Richtlinien existiert mit dem WDAC Policy Wizard ein geeignetes Softwaretool.

4.10. Schwachstellenmanagement

Mit der stetig ansteigenden Anzahl von Geräten in einem Netzwerk ist ihre Überprüfung auf Schwachstellen immer schwieriger und umfangreicher. Daher empfiehlt es sich, gelegentlich Schachstellenscans durchzuführen. Ein geeignetes Tool hierfür ist beispielsweise OpenVAS[16].

4.11. Cloudservices

Für die Nutzung von Cloud-Diensten sollte eine Dienstanweisung zur Verfügung gestellt werden, die den sicheren Umgang mit solchen Cloud-Diensten beschreibt. Zudem ist der Cloud Service Provider über vertragliche Anforderungen dazu gehalten, seine Systeme aktuell zu halten. Sofern Schnittstellen zwischen den Cloud-Diensten und der eigenen Netzwerkinfrastruktur bestehen, sollten diese abgesichert sein.

5. Active Directory

Der DC[17] einer Domäne ist meistens das Hauptangriffsziel einer Tätergruppierung und muss daher besonders geschützt werden. Hierbei helfen Methoden wie die nachfolgend beschriebenen.

[14] Potentially unwanted Application
[15] Windows Defender Application Control
[16] https://www.openvas.org/index-de.html (open Vulnerability Assessment Scanner)
[17] Domain Controller

5.1. Passwort Policy

Passwortrichtlinien sind per GPO zu erzwingen. Hierzu muss man die Passwortrichtlinien bspw. durch eine Gruppenrichtlinie (GPO[18]) initiieren (Domain Policy). Die Gruppenrichtlinie sollte dabei die vom BSI empfohlenen Kennwort- bzw. Kontosperrungsrichtlinien besitzen (Kennwortalter, Kennwortlänge, Kennwortchronik, Kontosperrungsschwelle, Kontosperrdauer, Kerberos-Richtlinien usw.)

5.2. Tier-Modell

Ein Tier-Modell wird verwendet, um administrative Berechtigungen eindeutig voneinander abzugrenzen. Hierbei darf ein Account immer nur für ein Tier Level berechtigt werden. Diese Accounts dürfen nur zur Administration im jeweiligen Tier Level verwendet werden und nicht für andere Tätigkeiten. Grundsätzlich muss ein mindestens dreischichtiges Konzept umgesetzt werden.

Tier 0

- Domänencontroller, Zertifizierungsstellen, Identitätsverwaltung.
- Bei „Tier 0“-Systemen handelt es sich typischerweise um die vorhandenen Domänencontroller, Exchange Server bzw. auch Antiviruslösungen. Accounts, die zur Administration der Domäne berechtigt sind, dürfen nur Systeme auf Tier-Level 0 administrieren.

Tier 1

- Dateiserver, Datenbankserver, Anwendungsserver.
- Bei „Tier 1“-Systemen handelt es sich unter anderem um Anwendungsserver, die Dienste für Benutzer bereitstellen.

Tier 2

- Clients, Drucker, Multifunktionsgeräte, Smartphones usw.

Empfehlung

Zusätzlich zu dedizierten Admin-Accounts kann man LAPS[19] (Microsoft Tool) auf den Computersystemen ausrollen. Weiterhin ist die Verwendung von personalisierten Accounts sehr empfehlenswert. Die personalisierten Accounts sollten dabei unterschiedliche Passwörter besitzen. Dies hat folgende Vorteile:

- Erleichtert die Nachverfolgung der Aktivitäten.
- Gegenmaßnahmen können schneller initiiert werden.
- Personalisierte Accounts können schneller und einfacher gesperrt werden, ohne dass dies einen Einfluss auf weitere Admin-Accounts hat.

5.3. Active Directory Sicherheitsgruppen

- **Empfehlung**: Standard-Sicherheitsgruppen wie die Administratorengruppe entfernen und neue Gruppen für diese Zwecke definieren.

[18] Group Policy Object
[19] Local Administrator Password Solution

- **Domain Protected User Security Group**: Für High-Privilege-Accounts (Admin-Accounts) wäre der Einsatz dieser AD-Gruppe sinnvoll, um das NTLM[20]-Auth-Verfahren zu boykottieren usw.
- **Group Managed Service Accounts**: Services sind bestenfalls mit einem Account abgesichert, der Mitglied in der Gruppe „Managed Service Accounts“ ist.

5.4. User- bzw. Rollen-Konzept

Bei der Planung des User-Konzepts ist vor allem das Least-Privilege-Prinzip ratsam. Dabei erhalten Anwender und Administratoren nur die Rechte, die sie zur Erledigung ihrer Aufgaben unbedingt benötigen. Dabei ist es vorteilhaft, umfangreiche Analysen durchzuführen, um die notwendigen Zugriffsrechte zu ermitteln. Dies ist zwar mit einem großen Aufwand verbunden, jedoch sind diese Analysen notwendig, um die Umgebung absichern zu können.

Die Ermittlung von Zugriffsrechten kann durch diverse Werkzeuge (bspw. ProcMon) erleichtert werden. Weiterhin empfiehlt sich eine zyklische Prüfung aller Benutzerkonten hinsichtlich ihrer Daseinsberechtigung und der hinterlegten Rollen. Insbesondere ist die Daseinsberechtigung zu prüfen, wenn jemand die Institution verlässt.

6. Aktuell gehaltener Stand der Technik

Der ISB sollte sich stets aktuelle Informationen zur Cyber-Sicherheit verschaffen, diese auswerten und anwenden.

7. DNS-Absicherung

Um bspw. DNS-Poisoning zu verhindern, wird empfohlen, eine DNS-Absicherung einzurichten. Hierfür kann DNSSEC[21] verwendet werden. DNSSEC verwendet digitale Signaturen, um die Authentizität von DNS-Daten zu überprüfen. Jeder DNS-Eintrag besteht aus der IP-Adresse des Servers sowie dem zugehörigen Domainnamen.

Fordert ein System die IP-Adresse für einen Domänennamen an, gibt der DNS-Server den entsprechenden DNS-Eintrag zurück. DNSSEC fügt diesen DNS-Datensätzen digitale Signaturen hinzu, sodass die Systeme überprüfen können, ob die vom Server zurückgegebenen Informationen während der Übertragung manipuliert oder geändert wurden.

[20] NT LAN Manager
[21] Domain Name System Security Extensions

8. Notfallmanagement

Es ist ratsam, einen Notfallplan zu erstellen. Dieser definiert Schritt für Schritt Vorgehensweisen, die zur schnellen Beseitigung eines Vorfalls führen. Es ist zu empfehlen, einen Vorfall unter Zuhilfenahme des erstellten Notfallplans regelmäßig zu simulieren.

9. Multifaktor-Authentifizierungsverfahren

Eine sinnvolle Ergänzung zu den herkömmlichen Authentifizierungsmechanismen ist ihre Erweiterung um einen weiteren Authentifizierungsschritt (bspw. One-Time-Password).

10. Sensibilisierung des Personals

Eine zielgruppenversierte Sensibilisierung, die die Gefahren eines Cyber-Angriffs, den sicheren Umgang mit Cloud-Anwendungen sowie den sicheren und seriösen Umgang mit diversen Social Media Plattformen verdeutlicht, sollte den Mitarbeitenden anhand von Trainings nahegebracht werden.

11. Penetrationstests

Eine regelmäßige Durchführung von Penetrationstests ist ratsam. Wenn die Systeme nach einem Sicherheitsvorfall wiederhergestellt wurden, sollte ebenfalls ein Penetrationstest durchgeführt werden.