Bayerisches Landesamt für
Datenschutzaufsicht

10 Maßnahmen gegen Cybercrime und für mehr Datensicherheit

Cyberfestung Bayern

Sicher. Stark. Widerstandsfähig.

Andreas Sachs
Vize-Präsident und
Bereichseiter Cybersicherheit

Dorit Buschmann
Stellvertretende Bereichsleiterin
Cybersicherheit

Wer steht heute vor Ihnen?

Andreas Sachs

Vize-Präsident und **Bereichsleiter Cybersicherheit und Technischer Datenschutz** beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Dorit Buschmann

Stellvertretende Bereichsleiterin **Cybersicherheit und Technischer Datenschutz**

Cybersicherheit Bayern heute

Wir schauen heute nicht bange in die Zukunft …

… sondern hoffnungsvoll in die Vergangenheit

Die Festung Rosenberg in Kronach wurde nie im Rahmen eines Angriffs eingenommen.

Grund: Diese hatten **wirksame Schutzmaßnahmen** gegen Angreifer.

Datenschutz im Jahr 2025

- Cybersicherheit ist gesetzliche Anforderung
- Risikoorientierter Ansatz
- Bedrohungslage weiter hin sehr hoch (wird sich wohl kaum ändern)
- Anzahl der Meldungen nach Art. 33 DS-GVO weiterhin sehr hoch (Dunkelfeld?)
- DS-GVO möchte, dass Datenschutzaufsichtsbehörden sensibilisieren

- Dann schauen wir uns nun mal **Standardschutzmaßnahmen** gegen Cyberangriffe im Jahr 2025 an

Abwehrmaßnahme 1: Burgmauer

Schutzmaßnahmen, die den äußersten Rand des Netzwerks oder Systems absichern.

Schutzmaßnahme: Den eigenen Perimeter prüfen

Schutzmaßnahme 1: Den eigenen Perimeter prüfen

Existiert eine vollständige Liste von:

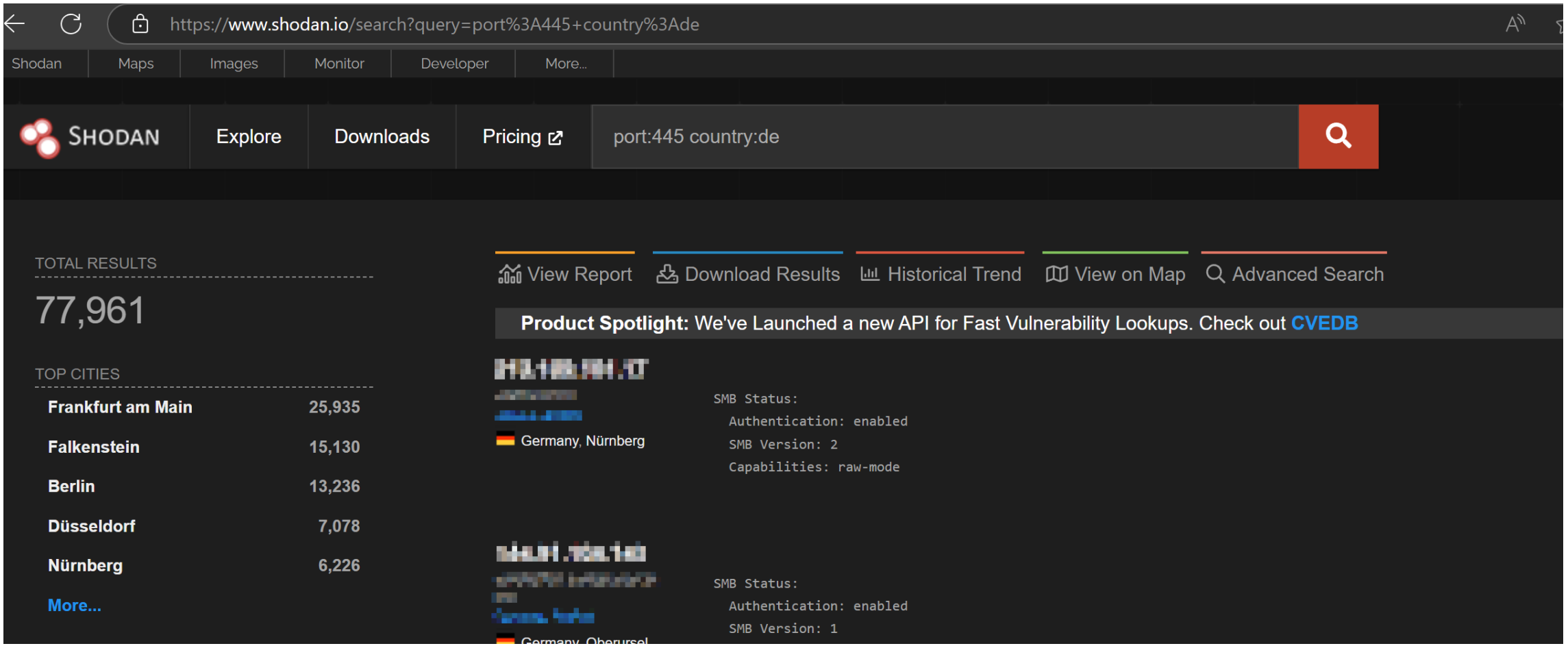
- Allen über das Internet erreichbaren IP-Adressen des eigenen Netzwerks?
- Alle API-Endpunkte von genutzten Webservices?
- Alle Server die bei externen Hostern gemietet sind?
- Allen Services, die bei Cloud-Diensten betrieben werden?
- Allen Cloud-Diensten, die als Software as a Service genutzt werden?

Mentimeter

Schätzen Sie ab, wie viele Dateiserver in Deutschland ohne Firewall erreichbar sind?

a) 34
b) 77.961
c) 1.200.401

Shodan-Beispiel



Abwehrmaßnahme 2: Burgtor

Einen geschützten Bereich darf nicht jeder betreten

Technische Maßnahme: Gutes Identitätsmanagement und Authentifizierung

Schutzmaßnahme 2: Mehrfaktorauthentifizierung

- **Multi-Faktor-Authentifizierung** (MFA) ist ein Sicherheitsverfahren, bei dem neben einem **Passwort** ein **weiterer Faktor** (z. B. Token, Biometrie, kryptografischer Schlüssel) verwendet wird
- Ein Cyberangreifer, der ein Passwort entwendet, kommt damit nicht mehr direkt weiter
- **Umsetzung** mittels App, SMS-Code, Smartcard, Windows-Hello, USB-Token,…

Bei Microsoft 365: Setzen Sie eine MFA-Lösung bei sich im Unternehmen ein?

a) Nein, gar nicht
b) Ja, für Admin-Tätigkeiten
c) Ja, für Admin-Tätigkeiten und bestimmte Benutzer (z. B. Führungskräfte)
d) Ja, für ausnahmslos alle Benutzer

Abwehrmaßnahme 3: Kein Generalschlüssel

Es gibt **keinen Generalschlüssel** für verschiedene Bereiche innerhalb eines schützenswerten Perimeters (z. B. Waffenkammer, Vorratskammer, Server und Dienste)

Technische Maßnahme: Keine einheitlichen, **lokalen Admin**-Passwörter

Schutzmaßnahme 3: Keine lokalen Admin-Passwörter

- Gelangt ein **Angreifer** auf einen (evtl. unwichtigen/veralteten Server), dann kann dieser ggf. das dort gespeicherte **lokale Admin-Passwort** erlangen
- Mit diesem kann dann auf wichtige/kritische Server (beim **Lateral Movement**) zugegriffen werden, wenn diese das gleiche Passwort haben
- In typischen AD-Umgebungen wird meist das **gleiche lokale Admin-Passwort** verwendet

Schutzmaßnahme 3: Keine lokalen Admin-Passwörter

Umgesetzungsmöglichkeiten:

- Verwendung von **Microsoft Local Administrator Password Solution** (LAPS) Beschreibung:
  - LAPS ist ein kostenloses Microsoft-Tool, das für jede verwaltete Windows-Maschine ein eindeutiges, sicheres lokales Administratorpasswort generiert und dieses zentral in Active Directory (AD) speichert.
- **Cloud-Lösungen** wie Azure AD und Windows Hello for Business verwenden
- **Drittanbieter-Tools** verwenden (meist in größeren Umgebungen)

Welchen Umgang mit lokalen Admin-Passwörtern haben Sie in Ihrem Unternehmen?

a) Voreinstellung: Auf jedem System gleich
b) Wir verwenden die Microsoft-LAPS Umgebung
c) Wir verwenden eine Microsoft Azure Cloud Lösung
d) Wir haben ein Drittanbieter-Tool
e) Weiß nicht

Abwehrmaßnahme 4: Dem Angreifer keine Waffen schenken

Die Waffen in einer Burg sind gut verschlossen in der Waffenkammer versteckt. Diese sollten nicht offen über den Burghof zugänglich sein.

Technische Maßnahme: Powershell-Skripte begrenzen

Was ist Powershell?

- Powershell ist ein skriptbasiertes Verwaltungstools für Windows Umgebungen
- Dieses ist standardmäßig installiert
- Angreifer können diese z. B. nutzen für:
  - Nachladen und Ausführen von Angriffstools aus dem Internet
  - Rechteerweiterung
  - Portscanning im lokalen Netzwerk
  - Remoteausführung von Kommandos

Abwehrmaßnahme 4: Powershell begrenzen

- Powershell ist **Bestandteil zentraler administrativer Funktionen** (z. B. Windows Management Instrumentation (WMI))
- Eine vollständige Deinstallation ist nur in engen Einsatzszenarien möglich (z. B. dedizierte Kiosk-Geräte)
- **Deaktivierung** mittels Gruppenrichtlinie für **bestimmte Benutzer/Gruppen**
- Einsatz von **Application-Control** Techniken (z. B. Windows AppLocker damit nur bestimmte Nutzer Powershell nutzen könne)
- **Reduzierung** des Funktionsumfangs (z. B. kein Nachladen aus Internet)
- **Logging** und Alarmierung von deaktivierten Funktionen

Abwehrmaßnahme 5: Mehrere Verteidigungszonen

Selbst wenn ein Angreifer die erste Hürde überwindet, ist dieser noch nicht am Ziel seines Angriffs. Verteidiger ziehen sich in die nächste Ebene zurück und kämpfen weiter.

Technische Maßnahme: Netzwerksegmentierung

Abwehrmaßnahme 5: Netzwerksegmentierung

- **Unterteilung eines Netzwerks** in kleinere Bereiche
- Dies verhindert/erschwert das Lateral Movement eines Angreifers
- **Typische Zonen**:
  - Benutzerzone (Mitarbeiter PCs)
  - Serverzone
  - Gastnetzwerk
  - Produktionsnetz (z. B. Produktionsanlagen)
  - DMZ (z. B. Webserver, Mailserver, VPN-Endpunkte)
- Umsetzung:
  - **Interne Firewalls** (mit Deep Paket Inspection und IDS/IPS) zwischen den Zonen, die nur definierten Traffic durchlassen (z. B. HTTP, RDP, …)
  - Einrichtung von **VLAN** auf Netzwerkebene mit Access Control Lists
  - Anwendung von **Zero-Trust-Prinzipien** (Benutzer und Geräte müssen sich authentifizieren, bevor sie Zugriff auf andere Netzwerksegmente erhalten)

Wie sieht es bei Ihnen mit der Netzwerksegmentierung aus?

a) Wir haben im Prinzip noch ein komplett verbundenes internes Netzwerk
b) Wir setzen VLAN zur konsequenten Netzsegmentierung ein
c) Wir setzen bereits den Zero-Trust-Gedanken um; Geräte und Benutzer müssen sich gegenseitig authentifizieren
d) Weiß nicht

Abwehrmaßnahme 6: Die Infiltration verhindern

Bei **verdeckten Angriffen** schleicht sich eine unauffällige Person in den geschützten Bereich.
Diese lässt, möglichst unerkannt, weitere Angriffsressourcen in den inneren Perimeter ein, die einen **Angriff von Innen** starten

Technische Maßnahme: Internetverkehr kontrollieren

Abwehrmaßnahme 6: Internetverkehr kontrollieren

- **Cyberattacken** finden i. d. R. ausschließlich über das **Internet** statt
- Es gibt zwei **typische Angriffsvektoren**:
  - Mitarbeiter führen eine Aktion aus, von der sie an sich wissen, das sie das nicht machen sollten (z. B. Klicken auf Link einer Mail)
  - Schwachstelle in über das Internet erreichbaren Netzwerkkomponente wird ausgenutzt
- Dabei werden **Angriffstools** über das Internet **(nach-) geladen**
- Ansatz: Den Internetverkehr **kontrollieren**

Abwehrmaßnahme 6: Internetübergang kontrollieren

- **Next-Generation Firewalls** (NGFWs) können den Datenverkehr auf Anomalien und bösartige Aktivitäten analysieren und verdächtige Verbindungen blockieren.
- **DNS-Filterung** verhindert Zugriffe auf bösartige Domänen und blockiert Command-and-Control-Kommunikation.
- **Intrusion Detection/Prevention Systeme** (IDS/IPS) erkennen und verhindern bekannte Exploits oder ungewöhnliche Traffic-Muster.
- **Indicators of Compromise** (IOCs) können dabei genutzt werden, um bekannte bösartige IPs, Domains oder Hashes automatisch zu blockieren.
- **Zentralisierte Überwachung** des Netzwerks und Sicherheitsereignisse (mittels SIEM-Systemen) hilft, Angriffe frühzeitig zu erkennen.

Abwehrmaßnahme 7: Die Schätze sichern

Manche Angriffe lassen sich ggf. doch nicht verhindern. Allerdings sollten die Angreifer nicht gleich alle Schätze auf einmal mitnehmen können,

Technische Maßnahme: Ransomwaresichere Backups

Abwehrmaßnahme 7: Ransomwaresichere Backups

- **Ransomware** stellt nach wie vor eine der größten Cyberbedrohungen dar
- (Personenbezogene) Daten werden dabei als „**Geisel**“ genommen:
  - **Verschlüsselung** (Entschlüsselung nach Lösegeldzahlung)
  - Entwendung (Keine Veröffentlichung nach Lösegeldzahlung)
  - Erpressung Dritter (bspw. mit Gesundheitsdaten)
- Zur Variante „Verschlüsselung (Entschlüsselung nach Lösegeldzahlung)“ gibt es gute Schutzmaßnahmen

Abwehrmaßnahme 7: Ransomwaresichere Backups

- **Stand der Technik**: Backups nach der **3-2-1 Regel** umsetzen
  - 3 Versionen eines Datenbestandes
  - 2 Arten von Backupmedium
  - 1 davon an anderem Standort
- Das reicht aber gegen einen Angreifer nicht immer aus
- **Lösungen**:
  1. **Offline-Backups** (Speicherung physisch getrennt vom Netzwerk)
  2. **Versteckte Backupsysteme** (Nur Daten-Pull Funktion auf Netzwerkebene)
  3. **Immutable Backups** (Keine physikalische Löschung/Änderung möglich, z. B. WORM Medien)
  4. **Cloud-Backups** mit Schutzmechanismen (z. B. Versionierung statt Überschreibung)

Wie sieht es mit Ihrer Backupstrategie aus?

a) Wir haben gar keine wirkliche Backupstrategie und hoffen, das das Backupband noch funktioniert
b) Wir setzen zwar die 3-2-1 Regel um, ob diese aber ransomwaresicher ist weiß ich nicht
c) Wir haben explizit eine ransomwaresichere Maßnahme umgesetzt
d) Weiß nicht

Abwehrmaßnahme 8: Die Bürgerwehr

Die Verteidigung einer Burg wurde nicht nur durch die Berufssoldaten sichergestellt. Im Zweifel haben auch die Bewohner mitgemacht.

Organisatorische Maßnahme: Awareness

Abwehrmaßnahme 8: Awarenessmaßnahmen

1. Schulung zur Erkennung von Social Engineering

Warum wichtig?

- **Social Engineering**, wie Phishing, bleibt eine der **effektivsten Methoden für Cyberangriffe**. Angreifer nutzen psychologische Manipulation, um sensible Informationen zu stehlen.

Maßnahmen:

- Regelmäßige **Schulungen**, um Mitarbeiter und Privatpersonen für typische Phishing-Anzeichen zu sensibilisieren (z. B. verdächtige Links, gefälschte E-Mails).
- Praktische **Übungen**, z. B. simulierte Phishing-Angriffe, um das Erkennen solcher Taktiken zu trainieren.

Abwehrmaßnahme 8: Awarenessmaßnahmen

2. Förderung der Meldekultur und Notfallbewusstsein

Warum wichtig?

- **Schnelle Reaktionen** auf potenzielle Sicherheitsvorfälle können den **Schade**n erheblich **reduzieren**.

Maßnahmen:

- Etablierung einer klaren **Meldekultur**, bei der Nutzer verdächtige Vorfälle sofort melden, ohne Angst vor negativen Konsequenzen.
- Aufklärung über die **Schritte**, die im Falle eines Cyberangriffs zu **unternehmen** sind, z. B. Kontosperrung, Kontakt mit der IT-Abteilung oder Benachrichtigung von Behörden.
- Simulation von **Notfallplänen** durch regelmäßige Cybersecurity-Drills.

Abwehrmaßnahme 9: Instandhaltung

Die Mauern (innen und außen), die Türen und Gitter und auch die Waffen und Schilde müssen instand gehalten werden. Kurzfristige Sparbemühungen können schnell das Ende bedeuten.

Technische Maßnahme: Softwareupdates

Abwehrmaßnahme 9: Softwareupdates

- Voraussetzung: Vollständige aktuelle **Liste aller Hardware und Software**
- Voraussetzung: Vollständige aktuelle **Liste** aller **über das Internet erreichbarer Systeme** (auch bei z. B. Hostern)

- **Maßnahmen:**
  - Ausschließlich Software verwenden, für die es noch **Sicherheitsupdates** gibt
  - **Automatische Updates** aktivieren (sofern möglich)
  - Kritische **Serverupdates** priorisieren (Update-First Konzept)
  - Automatisierte Updates mittels **Softwaretools**
  - Bei **sicherheitskritischen Komponenten** (Firewalls, VPN-Zugänge, …) -> Updates haben immer **Prio 1**, ggf. Notfall-Alternativsysteme vorhalten

Wie sieht es mit Ihren Updates aus?

a) Wir führen Updates ad hoc manuell aus
b) Wir setzen ein automatisiertes Updatetool für Clients ein, Serverupdates verzögern sich aber häufig, da wir ein Running-System nicht anfassen wollen
c) Wir setzen ein automatisiertes Updatetool für Clients ein, Serverupdates werden priorisiert, bei Bedarf innerhalb eines Tages eingespielt
d) Weiß nicht

Abwehrmaßnahme 10: Schütze den König (die Königin)

Ein Angriff auf eine Burg ist dann meist erfolgreich gewesen, wenn der Herrscher in die Gewalt der Angreifer gekommen ist. Aus diesem Grund wurde dieser speziell beschützt (Leibgarde) und hatte sich im innersten gesicherten Bereich (Burgfried) aufgehalten

Technische Maßnahme: Schutz des Domain-Controller

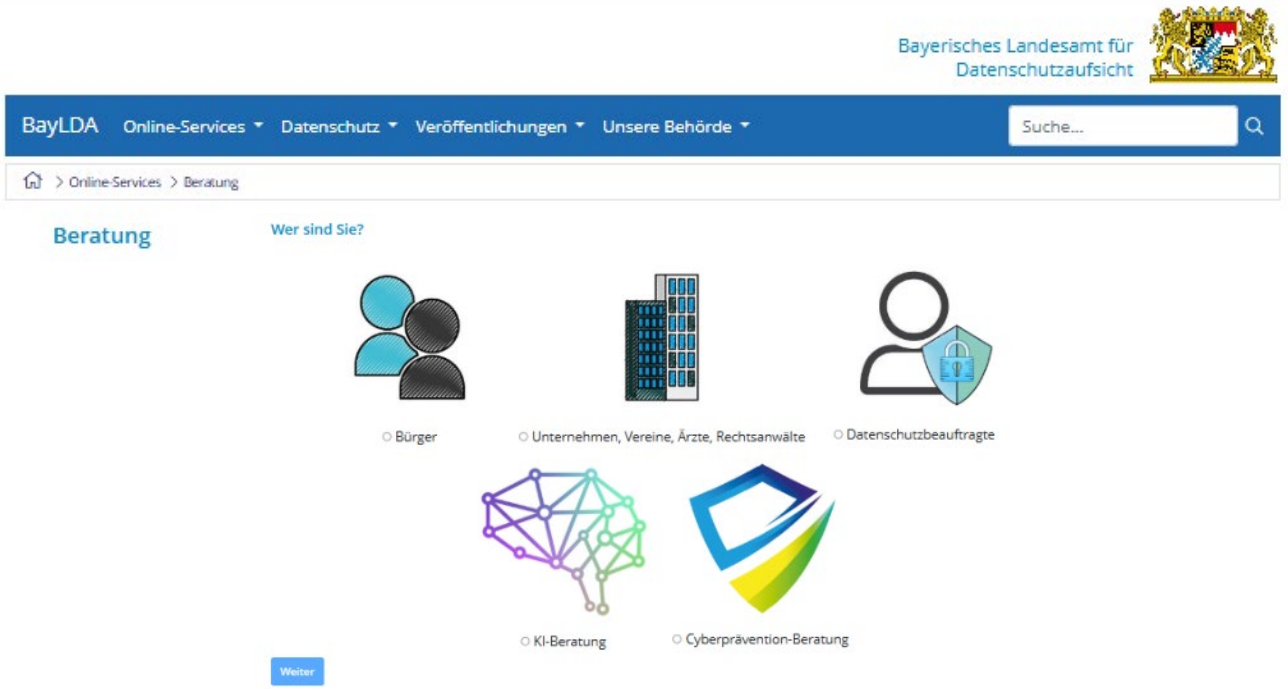
Abwehrmaßnahme 10: Schutz Domaincontroller

Maßnahmen:

- **Rechtebeschränkung** des Zugangs zum Domaincontroller auf ein Minimum. Nur Administratoren mit spezifischem Bedarf sollten Zugriff haben. Nutzung von Prinzipien wie "Least Privilege" und Segmentierung administrative Aufgaben.
- **Serverhärtung** mittels Deaktivierung unnötiger Serverdienste
- Isolierung des Domaincontroller in einem geschützten **Netzwerksegment** mit Nutzung von Intrusion-Detection-System (IDS)
- **Multi-Faktor-Authentifizierung** (MFA) für Administratorzugriffe
- **Monitoring** mit Tools wie SIEM (Security Information and Event Management), um Anomalien frühzeitig zu erkennen.
- Erstellung regelmäßiger, überprüfter **Backups** des DC und Offline-Aufbewahrung dieser Backups

Wie geht es weiter?

- Das BayLDA baut momentan seine Beratungsleistungen wieder aus
- Neben der KI-Beratung ist auch die Cyberprävention ein Schwerpunkt



www.lda.bayern.de/beratung

Wie geht es weiter?

- Auch die **Sensibilisierung** im Bereich **Cybersicherheit** stellt wieder einen Schwerpunkt in 2025 dar
- Dazu wird der dieses Jahr der Ansatz „**Defense in Depth als neuer Stand der Technik**“ verfolgt
- In **Ihrer Ritterburg** gibt es dazu auch ein digitales „**Schild**“: Sie erhalten exklusiven Zugang zu Entwurfsversionen von neuen und überarbeiteten Checklisten zur „Cyberfestung Bayern“

Wie geht es weiter?

Exklusiver Zugang zur Preview-Version für die IHK-Workshop-Teilnehmenden


Entwurfsstand 0.8

Bayerisches Landesamt für
Datenschutzaufsicht

Checkliste Cyberfestung
10 Punkte für mehr Datensicherheit
Aktuelle Prüfkriterien nach Art. 32 DS-GVO

Stand der Checkliste: 29.01.2025

Ziel und Inhalt dieses Papiers

Die in diesem Dokument enthaltene Checkliste stellt wesentliche Punkte zur Absicherung der eigenen Systeme und Dienste im Umgang mit personenbezogenen Daten bereit. Die aufgeführten Prüfpunkte sind nicht als abschließend zu betrachten, sondern stellen einen Good-Practice-Ansatz dar, der im Sinne einer Soll-Ist-Überprüfung verwendet werden kann.

Vielen Dank für Ihre Aufmerksamkeit und Ihre aktive Teilnahme am Workshop