Bayerisches Landesamt für
Datenschutzaufsicht

Bayer. Landesamt für Datenschutzaufsicht | Postfach 1349 | 91504 Ansbach

Empfänger
Straße
Plz Ort

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18 | 91522 Ansbach
Telefon: 0981 180093 0
Fax: 0981 180093 800
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ihre Kontaktperson
Frau
E-Mail: xxx@lda.bayern.de

Aktenzeichen zu Ihrer Prüfung

Ansbach,

Aufsicht nach Art. 58 Datenschutz-Grundverordnung (DS-GVO);
Prüfung zum Thema Ransomware-Nachprüfung

Datenschutzrechtliche Prüfung Ihrer Organisation hinsichtlich technischer und organisatorischer Maßnahmen zum vorbeugenden Schutz gegen Ransomware-Attacken nach Art. 32 DS-GVO

Anlagen:
A Prüfunterlagen Ransomware-Prävention
B Informationsblatt zur Prüfung Ransomware-Prävention

Sehr geehrte Damen und Herren,

wir, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), überwachen die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, d. h. primär in den privaten bayerischen Wirtschaftsunternehmen, bei den freiberuflich Tätigen, in Vereinen sowie in Verbänden.

Im Rahmen unserer gesetzlichen Aufgaben untersuchen wir regelmäßig Verantwortliche gezielt hinsichtlich grundlegender Sicherheitsanforderungen nach Art. 32 DS-GVO, die bei Ransomware-Cyberattacken mitunter darüber entscheiden, ob ein Angriff erfolgreich abgewehrt bzw. das Schadensausmaß aktiv begrenzt werden kann.

Unseren Aufzeichnungen zufolge nach war **Ihre Organisation innerhalb der letzten Jahre von einer Ransomware-Attacke betroffen** (siehe Meldung nach Art. 33 DS-GVO am , die unter dem Aktenzeichen in unserer Behörde geführt wird).

Wir gehen davon aus, dass Sie im Rahmen der Aufarbeitung des Vorfalls ihrerseits ggf. die Sicherheitsmaßnahmen ausgeweitet oder zumindest angemessen angepasst haben. Im Rahmen der vorliegenden Ransomware-Nachprüfung möchten wir nun Ihren aktuellen Sicherheitsstand diesbezüglich abfragen. Die dazugehörigen **Prüfunterlagen** liegen diesem Schreiben bei (Anlage A). Mit dieser Prüfung bestätigen Sie uns damit bei Ihnen durchgeführte Maßnahmen zur Sicherheit nach Art. 32 DS-GVO.

Falls bestimmte Maßnahmen bei Ihnen nicht ergriffen werden konnten, sind ergänzende Ausführungen zur Begründung möglich. Anlage B dieses Schreiben informiert abschließend über wesentliche Punkte der Ransomware-Prävention.

Neben den ausgefüllten Prüfunterlagen (Anlage A) bitten wir zudem um Zusendung des eigenen **Abschlussberichts** zum Sicherheitsvorfall der bei uns am eingereichten und unter dem Aktenzeichen geführten Meldung. Bitte fügen Sie Ihrem Abschlussbericht den **vollständigen forensischen Bericht** – sofern vorhanden – bei.

Wir fordern Sie auf, die ausgefüllte Prüfliste (sowie ggf. ergänzende Ausführungen) als auch den Abschlussbericht (samt forensischen Bericht) **per Brief** unter Angabe des o. g. Aktenzeichens an die o. g. Adresse zu schicken (alternativ als PDF-Datei per **E-Mail** an xxx@lda.bayern.de).

Für den Eingang haben wir uns **spätestens den 08.03.2024** vorgemerkt.

Bei **Rückfragen** wenden Sie sich bitte ausschließlich schriftlich an xxx@lda.bayern.de.

Bitte beachten Sie, dass unabhängig von der Größe der Organisation grundsätzlich jeder Verantwortliche i. S. d. DS-GVO dazu verpflichtet ist, geeignete technische und organisatorische Maßnahmen (TOM) anzuwenden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Auch wenn ein Verantwortlicher einen Dienstleister in Anspruch nimmt, obliegt es dem Verantwortlichen selbst, zu überprüfen, ob das dem Risiko angemessene Schutzniveau des Art. 32 DS-GVO erreicht wird. Falls bestimmte Maßnahmen bei Ihnen nicht ergriffen werden, sind ergänzende Ausführungen zur Begründung möglich. **Hinweis**: Nicht alle abgefragten Prüfpunkte müssen zwangsläufig erfüllt sein, um ein für Ihre Organisation in Bezug auf Ransomware-Angriffe ausreichendes Sicherheitsniveau nach Art. 32 DS-GVO zu erreichen. Vielmehr hat jeder Verantwortliche für sich festzustellen, welche der Maßnahmen für die eigene Einrichtung erforderlich sind.

Sollten Sie dieser Aufforderung nicht fristgerecht nachkommen, stellen wir Ihnen den Erlass einer förmlichen Anweisung gem. Art. 58 Abs. 1 Buchstabe a DS-GVO samt Zwangsgeldandrohung in Aussicht. Im weiteren Prüfverlauf behalten wir es uns zudem vor, Verantwortliche anlassbezogen mit einem breiteren Prüffokus ggf. auch vor Ort zu kontrollieren, um uns von der erfolgreichen Umsetzung der und kommunizierten datenschutzrechtlichen Vorgaben zu überzeugen. Ebenso können Dokumentationen und andere Unterlagen zu den abgefragten Themenschwerpunkten im weiteren Prüfverlauf angefordert werden.

Gesetzliche Informationen:

Die Datenschutz-Grundverordnung legt in Art. 58 Abs. 1 Buchstabe a fest, dass jede Aufsichtsbehörde über die Befugnis verfügt, den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Daneben verfügt jede Aufsichtsbehörde über die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten (vgl. Art. 58 Abs. 1 Buchstabe e DS-GVO). Ein Verstoß gegen diese Verpflichtung stellt eine Ordnungswidrigkeit dar und kann mit einer Geldbuße geahndet werden.

Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nrn. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde (§ 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz). Die Inanspruchnahme des Auskunftsverweigerungsrechts ist mitzuteilen und nachvollziehbar zu begründen.

Mit freundlichen Grüßen

gez.
Dieses Schreiben wurde elektronisch erstellt und ist ohne Unterschrift gültig.

Hinweis zur Verarbeitung Ihrer personenbezogenen Daten

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten im Rahmen des vorliegenden Kontakts ist das Bayerische Landesamt für Datenschutzaufsicht. Weitere Informationen zur Verarbeitung Ihrer Daten, insbesondere zu den Ihnen zustehenden Rechten, können Sie unserer Homepage unter www.lda.bayern.de/informationen entnehmen.

Anlage A

Prüfunterlagen Ransomware-Nachprüfung

Verantwortlicher: Empfänger

Aktenzeichen:

1. Systemlandschaft

☐ Vollständige und aktuelle Liste aller vorhandenen PCs und Notebooks samt Betriebssystem und Betriebssystemversion ist vorhanden.
Grund: Voraussetzung für wirksames Patch Management.

☐ Vollständige und aktuelle Liste aller internen und externen Server samt Betriebssystem und Betriebssystemversion ist vorhanden.
Grund: Voraussetzung für wirksames Patch Management.

☐ Vollständige und aktuelle Liste aller dienstlichen Smartphones, Tablets und sonstigen mobilen Endgeräte samt Betriebssystem und Betriebssystemversion ist vorhanden.
Grund: Voraussetzung für wirksames Patch Management.

☐ Vollständiger und aktueller Netzwerkplan mit allen intern sowie extern betriebenen IT-Systemen samt aktiver und passiver Netzkomponenten (z. B. Switches, Firewalls, VPN-Appliances) samt ggf. bestehender Netzsegmentierung ist vorhanden.
Grund: Voraussetzung für wirksames Patch Management.

☐ Es liegt ein aktuelles und lückenloses Berechtigungskonzept vor, das Nutzer, IT-Systeme und Anwendungen nach ihren Aufgaben und Rollen sortiert und so eine strikte Zugangs- und Zugriffskontrolle gewährt.
Grund: Ein präzises Konzept, das eine limitierte Berechtigungsvergabe vorsieht, hilft bei der Erfüllung der rechtlichen Anforderungen (DS-GVO).

☐ Interne Netzbereiche unterschiedlicher Sicherheitsstufen werden mittels Firewalls getrennt.
Grund: Soll das Ausbreiten von Schadcode bzw. von Angreifern innerhalb des Netzwerks erschweren/verhindern (sog. Lateral Movement).

☐ Über das Internet erreichbare Server wie Mailserver, Webserver oder VPN-Endpunkte befinden sich in einem eigenen internen Netzsegment (sog. Demilitarisierte Zone - DMZ).
Grund: Soll verhindern, dass Angreifer die ggf. kurzzeitig einen derartigen Dienst übernehmen, nicht mühelos auf weitere interne Systeme zugreifen oder zumindest einen Angriffsversuch durchführen können.

☐ Anbindung mobiler Arbeitsplätze (z. B. dienstliche Notebooks, dienstliche Smartphones) über das Internet erfolgt über verschlüsselte und auch kryptographisch authentifizierte Verbindungen (z. B. verschlüsseltes VPN mit Authentifizierung mittels starker Passwörter und kryptographischen Client-Zertifikaten).
Grund: Angreifer sollen nicht alleine anhand entwendeter Benutzernamen/Passwörtern ins Unternehmensnetz gelangen können.

☐ Aus dem Internet geladene Programme können nicht ohne eine (in den Sicherheitsrichtlinien festgelegte) Nutzerinteraktion ausgeführt werden.
Grund: Verhinderung der automatisierten Ausführung von aus dem Internet nachgeladenen Schadcodeprogrammen.

☐ Vertrauenswürdige Orte für Makros sind im Active Directory vorkonfiguriert.
Grund: Die Ausführung von potenziell schadhaften Skripten aus vertrauensunwürdigen Quellen wird so weitestmöglich unterdrückt.

☐ Programme ohne valide Signierung durch vertrauenswürdige Herausgeber (z. B. das Betriebssystem) können nicht ausgeführt werden.
Grund: Vom Benutzer fälschlicherweise selbst aus dem Internet heruntergeladene Schadsoftware wird nicht zur Ausführung gebracht.

☐ Bei Microsoft Windows Betriebssystemen: Der kontrollierte Ordnerzugriff ist in den Windows Security Einstellungen aktiv geschaltet.
Grund: Zusätzlicher Schutz vor Apps, die Änderungen an Dateien in geschützten Ordnern vornehmen können sowie vor nicht autorisierten oder unsicheren Apps, die einen Zugriff bzw. Änderung von Dateien in diesen Ordnern vornehmen wollen.

☐ Sollten Privatgeräte im Homeoffice zulässig sein, dann haben diese keinen vollständigen Zugriff auf alle IT-Systeme und Daten im Unternehmensnetz.
Grund: Das Schutzniveau privater Endgeräte kann vom Verantwortlichen nicht gewährleistet werden.

☐ Dienstliche Smartphones und Tablets werden über eine Mobile-Device-Management-Lösung verwaltet.
Grund: Voraussetzung für wirksames Patch-Management sowie Datenlöschung im Verlustfall.

☐ Die Installation von Software auf einem PC ist nur mittels Admin-Rechten (durch den Administrator) möglich.
Grund: Verhinderung, dass Nutzer aus Versehen als normale Software getarnten Schadcode installiert.

☐ Browser-Plugins (z. B: Java, aber auch Unterstützung für Flash-Komponenten) werden nur dann installiert, wenn eine (ältere) Anwendung dies unbedingt erforderlich macht.
Grund: Viele Browser-Plugins besitzen Sicherheitslücken, die schon beim Besuch einer Webseite ausgenutzt werden können (sog. Drive-By-Angriff).

☐ Es wird eine sogenannte Deep Packet Inspection verwendet, welche die in einem Netzwerk übertragenen Datenpakete inspiziert und filtert.
Grund: Benutzer werden daran gehindert auf Webinhalte zuzugreifen, die von potenziellen Angreifern kontrolliert werden bzw. mit Schadcode infiziert sind.

☐ Skripte wie JavaScript oder Visual Basic werden nur dann vom Betriebssystem (nicht vom Browser, hier ist zumindest JavaScript in der Regel erforderlich) ausführbar gelassen, wenn (ältere) Software dies unbedingt erfordert.
Grund: Manche Schadsoftware kommt als Skript-Datei im E-Mail-Anhang und kann durch Deaktivierung auf Betriebssystemseite bei einem versehentlichen Klick durch den Nutzer trotzdem an der Ausführung gehindert werden.

☐ Die Ausführung von Skripten (z. B. Powershell) auf Servern (z. B. neue Benutzer anlegen, Netzwerkverbindungen aufbauen etc.) wird an einer zentralen Stelle protokolliert.
Grund: Angriffe auf Server werden mitunter anhand von Skriptdateien durchgeführt. Durch eine Protokollierung kann das Vorgehen der Angreifer (im Nachhinein) nachvollzogen werden.

☐ Microsoft-Office-Pakete sind so konfiguriert, dass diese nur signierte Makros ausführen, sofern die Makro-Ausführung überhaupt in den Sicherheitsrichtlinien vorgesehen ist.
Grund: Schadsoftware kommt häufig in Form präparierter Office-Dokumente wie Word oder Excel. Diese besitzen keine signierten Makros und können so an einer Ausführung gehindert werden.

☐ Die Ausführung von Programmen ist nur aus festgelegten Verzeichnissen (sog. Execution Directory Whitelisting) möglich.
Grund: 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.

☐ Auf dem E-Mail-Server wird ein Spam- und Antivirenfilter eingesetzt.
Grund: Damit können schon bekannte Schadprogramme erkannt und verdächtige E-Mails gesondert behandelt werden.

☐ E-Mails mit gefährlichen Dateianhängen wie ausführbare Dateien, mit Passwort verschlüsselte ZIP-Archive oder Office-Dokumente mit Makros werden vom Mailserver in einen Quarantäne-Ordner zur Analyse verschoben.
Grund: Derartige E-Mails enthalten häufig Schadcode bzw. kleine Programme, die Schadcode herunterladen sollen.

☐ Der E-Mail-Server wird so konfiguriert, dass E-Mails von internen Absendern, die aber von außerhalb des Unternehmens zugestellt werden sollen, blockiert werden (sog. Anti-Spoofing).
Grund: Dieser Angriff ist nicht unüblich, um Beschäftigte bspw. zum Klick auf einen in der E-Mail enthaltenen Link (der zu Schadcode führt) zu verleiten. Da derartige E-Mails immer von „außerhalb" kommen, kann es faktisch nicht sein (außer ggf. bei E-Mail-Verteilern – dies sollte dann getestet werden), dass diese eine interne Absenderadresse haben und nicht gefälscht sind.

☐ Administratoren besitzen zwei Benutzer-Accounts: Einen für reine Administrationsaufgaben und einen für andere Tätigkeiten wie E-Mails lesen oder im Internet surfen.
Grund: Schadcode führt sich immer mit den Benutzerrechten der Person aus, die (versehentlich) zu dessen Aktivierung beigetragen hat. Auf diese Weise kann zumindest verhindert werden, dass der Schadcode gleich mit (lokalen) privilegierten Administrator-Rechten zur Ausführung kommt.

☐ Auf jedem PC/Server wird für das lokale Administrator-/Root-Konto ein unterschiedliches und starkes (mind. 16 Stellen) Passwort verwendet.
Grund: Wenn ein Angreifer/Schadcode das lokale Administratorkonto eines Rechners erlangen kann, ist so nicht gleich die Weiterbewegung (sog. Lateral Movement) über das gesamte Netzwerk möglich.

☐ Der Zugang zu sicherheitskritischen Servern (z. B. Domain-Controller) ist für Administratoren nur mittels Zwei-Faktor-Authentifizierung möglich.
Grund: Selbst, wenn ein Angreifer das Administrator-Passwort (z. B.: mittels Extraktion aus dem Arbeitsspeicher) erlangt, kann dieser damit nicht auf sicherheitskritische Server zugreifen.

☐ Der Zugriff von Dienstleistern mittels Fernwartung auf die eigenen Systeme ist in einer Sicherheitsrichtlinie wirksam geregelt.
Grund: Angreifer versuchen mitunter über eine Kompromittierung eines Dienstleisters (sog. Supply-Chain-Angriff) Angriffswege ins eigene Netzwerk zu finden.

☐ Der Zugriff von Dienstleistern mittels Fernwartung auf die eigenen Systeme wird lückenlos protokolliert.
Grund: Angreifer versuchen mitunter über eine Kompromittierung eines Dienstleisters (sog. Supply-Chain-Angriff) Angriffswege ins eigene Netzwerk zu finden. Eine Protokollierung kann Angriffsversuche rechtzeigt aufdecken oder erfolgte Angriffe aufklärbar machen.

2. Patch Management

☐ Alle PCs und Notebooks sind so konfiguriert, dass Softwareupdates des Betriebssystems automatisch eingespielt werden.
Grund: Sicherheitslücken werden unverzüglich geschlossen und können nicht mehr von Angreifern verwendet werden.

☐ Sofern Softwareupdates des Betriebssystems über eine eigene Softwareverteilung erfolgt (z. B. WSUS), dann ist diese so zu konfigurieren, dass Sicherheitsupdates automatisch vom Hersteller des Betriebssystems geladen und unverzüglich für Updates an alle PCs und Notebooks bereitgestellt werden.
Grund: Sicherheitslücken werden unverzüglich geschlossen und können nicht mehr von Angreifern verwendet werden.

☐ Es werden ausschließlich Betriebssysteme eingesetzt zu denen der Hersteller Sicherheitsupdates zur Verfügung stellt.
Grund: Sicherheitslücken können sonst gar nicht geschlossen werden.

☐ Es besteht eine vollständige Liste der auf allen PCs und Notebooks eingesetzten Anwendungssoftware samt Softwarestand.
Grund: Voraussetzung um das Einspielen von Softwareupdates organisieren zu können.

☐ Anwendungssoftware auf PCs und Notebooks wird so konfiguriert, dass Softwareupdates (zumindest Sicherheitsupdates) automatisch eingespielt werden, sofern dies möglich ist.
Grund: Ein Angriff mittels bekannter Sicherheitslücken (z. B. Browser, PDF-Reader) kann verhindert werden.

☐ Sofern Anwendungsprogramme nicht automatisch aktualisiert werden können, wird sichergestellt, dass diese spätestens monatlich auf den aktuellsten Stand gebracht werden.
Grund: Ein Angriff mittels bekannter Sicherheitslücken (z. B. Browser, PDF-Reader) kann verhindert werden.

☐ Es werden ausschließlich Server-Betriebssysteme eingesetzt, für die vom Hersteller noch Sicherheits-Updates bereitgestellt werden.
Grund: Sicherheitslücken können sonst gar nicht geschlossen werden.

☐ Es wird für alle Server geprüft, inwiefern diese so konfiguriert werden können, dass Sicherheitsupdates automatisch eingespielt werden können.
Grund: Verhindert, dass mittels Ausnutzung bekannter Sicherheitslücken Angreifer interne Server erfolgreich angreifen und damit zur weiteren Ausbreitung im lokalen Netzwerk missbrauchen können.

☐ Für alle Server, bei denen keine automatisierte Einspielung von Sicherheitsupdates aufgrund von Risiken eventuell instabiler Serverzustände möglich ist, werden Sicherheitsupdates nach Tests unverzüglich manuell eingespielt. Kritische Sicherheitslücken werden innerhalb weniger Tage, sofern keine gleichwertigen anderen Schutzmaßnahmen ergriffen werden.
Grund: Verhindert, dass mittels Ausnutzung bekannter Sicherheitslücken Angreifer interne Server erfolgreich angreifen und damit zur weiteren Ausbreitung im lokalen Netzwerk missbrauchen können.

☐ Sicherheitsupdates aller Netzwerkkomponenten, insbesondere Firewalls und VPN-Appliances werden unverzüglich mit hoher Priorität eingespielt.
Grund: Insbesondere bei über das Internet erreichbaren, zentralen Systemen bedeutet ein erfolgreicher Angriff einen sofortigen Ausfall kritischer Schutzkomponenten.

☐ Es besteht eine aktuelle und vollständige Dokumentation darüber, welche PCs, Notebooks, Server, Netzwerkkomponenten etc. automatisch oder manuell upgedatet werden. Bei nicht-automatischen Updates werden dabei die jeweiligen IT-Systeme samt Softwareständen erfasst.
Grund: Nur durch aktuelle Dokumentation kann auch die Wirksamkeit eines Update-Konzepts sichergestellt und kontrolliert werden.

☐ Sicherheitsupdates für dienstliche Smartphones und dienstliche Laptops werden über ein Mobil-Device-Management-System unverzüglich ausgerollt. Es werden keine mobilen Endgeräte eingesetzt, für die es keine Sicherheitsupdates (mehr) gibt.
Grund: Verhinderung, dass Angreifer mittels Ausnutzung bekannter Sicherheitslücken mobile Endgerät erfolgreich angreifen und damit Zugang zum Unternehmensnetz erhalten können.

3. Backup-Konzept

☐ Durchführung von Backups nach der 3-2-1 Regel: 3 Datenspeicherungen (inkl. Originaldaten), 2 verschiedene Backupmedien (auch „Offline" wie Bandsicherungen) und 1 davon an einem externen Standort oder vergleichbar wirksame Backup-Mechanismen bezüglich Ransomware-Angriffen.
Grund: Im Falle einer Ransomware-Attacke können die (personenbezogenen) Daten und die betroffenen IT-Systeme wiederhergestellt werden.

☐ Mindestens ein Backup-System ist durch Schadcode nicht unmittelbar zu verschlüsseln (z. B. spezielles Datensicherungsverfahren wie Pull-Verfahren des Backup-Systems, Air-Gap-getrennt (offline) nach Abschluss des Backup-Prozesses oder Schreibberechtigung auf Backups nur von festgelegten Programmen aus).
Grund: Viele Ransomware-Angriffe versuchen vor einer Verschlüsselung die Backupsysteme ebenfalls zu verschlüsseln oder die Backups zu löschen. Durch auf Ransomware-Angriffe ausgerichtete Lösungen sollen Risiken bzgl. aktiver Löschversuche der Backups minimiert werden.

☐ Es besteht eine dokumentierte Regelung, welche Daten von welchen Servern oder PCs/Notebooks in ein Backup-Konzept aufgenommen wurden.
Grund: Sicherstellung, dass alle relevanten (personenbezogenen) Daten auch von einer Backup-Lösung umfasst sind.

☐ Es wurde ein Planspiel durchgeführt, wie das komplette IT-System in dem Fall wieder aufgesetzt werden kann, falls alle internen wie externen Server aufgrund einer Vollverschlüsselung nicht mehr funktionsfähig wären.
Grund: Vorbereitung auf den Worst-Case, um prüfen zu können, ob auch alle erforderlichen Daten im Backup enthalten sind.

☐ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird.
Grund: Ein Backup muss täglich durchgeführt werden – es ist auch sicherzustellen, dass dieses funktioniert.

☐ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert.
Grund: Verhinderung der Situation, dass im Worst-Case festgestellt wird, dass bspw. ein Backup-Medium defekt ist oder die für eine Systemwiederherstellung erforderliche Information nicht im Backup enthalten ist.

4. Überprüfung des Datenverkehrs

☐ Der zentrale Internetübergangspunkt vom internen Netzwerk zum Internet ist mittels einer Firewall abgesichert.
Grund: Mindeststandard zur Absicherung vertraulicher Netze gegenüber dem Internet

☐ Neben/als Bestandteil der Firewall wird HTTP-Verkehr über einen Web-Proxy geleitet. Netzwerkverkehr anderer Protokolle ins Internet wird als Standard von der zentralen Firewall geblockt und nur im Einzelfall dokumentiert freigeschalten.
Grund: Voraussetzung für Analyse von möglichem Schadcode-Netzwerkverkehr

☐ Die Web-Proxy-Komponente filtert aufgerufene Internetseiten bezüglich bekannten und täglich aktualisierten Endpunkten, die als (meist gehackte) Server zur Auslieferung von Schadcode verwendet werden (sog. Indicator of Compromise, kurz: IoC) und blockiert sowie protokolliert derartige Aufrufe.
Grund: Schadcode wird meistens in mehreren Schritten „ausgeliefert", was mitunter auf diese Art und Weise unterbunden werden kann.

☐ Es findet eine Protokollierung des Datenverkehrs ins Internet auf Basis von externen IP-Adressen und Datenvolumen für bis zu 90 Tage mit dem Ziel einer Auswertung möglicher Unregelmäßigkeiten nach einem Vorfall statt. Diese Protokolle sollten verschlüsselt werden, um eine missbräuchliche Verwendung zu verhindern und die datenschutzrechtliche Zweckbindung sicherzustellen.
Grund: Bei dem Verdacht einer Datenausleitung nach einem Ransomware-Angriff kann auf diese Weise ein Indiz geschaffen werden, ob eine Datenausleitung stattgefunden hat oder nicht. Die IP-Adressen können dann der Polizei für deren Ermittlungen ausgehändigt werden.

5. Awareness und Berechtigungen

☐ Regelmäßige Schulung der Beschäftigten bezüglich aktueller und häufiger Cyberangriffe (z. B. einmal pro Jahr).
Grund: Kriminelle erschleichen sich durch Social-Engineering-Angriffe wichtige Informationen für nachgelagerte Cyberattacken. Entsprechend ist es wichtig, allen Beschäftigten den „Sicherheitsfaktor Mensch" in geeigneten Schulungen zu erläutern.

☐ Konsequente Einweisung neuer Beschäftigter zum fachgerechten Umgang mit den IT-Komponenten und Verhalten bei Social-Engineering-Angriffen.
Grund: Social-Engineering-Angriffe verursachen nach wie vor hohe Schäden.

☐ Sensibilisierung neuer Beschäftigter bezüglich IT-Risiken vor der Aufnahme der Datenverarbeitung (z. B. auch bei Aushilfskräften).
Grund: Sicherheitstechnisches Fehlverhalten von Beschäftigten beruht oft auf fehlender Sensibilisierung und Unterrichtung im Vorfeld.

☐ Darstellung des Ablaufs von Social-Engineering-Angriffen zur Sensibilisierung der Beschäftigten (z. B. Möglichkeit der Manipulation von Telefonnummern).
Grund: Social-Engineering-Angriffe verursachen nach wie vor hohe Schäden – die Darstellung konkreter Abläufe verbessert das Wissensbild.

☐ Es sind Meldewege (z. B. durch den ISB oder DSB) und Zuständigkeiten bei der Erkennung von Sicherheitsverletzungen festgelegt und im System zum Datenschutzmanagement hinterlegt.
Grund: Eine angemessene Reaktion auf sicherheitstechnisches Fehlverhalten ist ein entscheidender Faktor für eine wirksame und zeitnahe Reaktion.

☐ Informationen an die Mitarbeiter über Meldewege (z. B. durch den ISB oder DSB) und Zuständigkeiten bei der Erkennung von Sicherheitsverletzungen werden wirksam kommuniziert.
Grund: Eine angemessene Reaktion auf sicherheitstechnisches Fehlverhalten ist ein entscheidender Faktor für eine wirksame und zeitnahe Reaktion.

☐ Falls die Nutzung von Privatgeräten gestattet ist (Bring your own device), wird eine strikte Sicherheitsrichtlinie verfolgt, die es vorsieht, alle Geräte zu prüfen und ggf. zu blockieren, die bestimmten Sicherheitsstandards nicht entsprechen.
Grund: Die Abwesenheit einer strengen ByoD Sicherheitsrichtlinie kann dazu führen, dass potenzielle Angreifer so Zugang zum Firmennetzwerk erlangen oder sich auf dem Gerät befindende geschäftliche Daten abgezogen werden.

6. Datenschutzorganisation

☐ Der betriebliche Datenschutzbeauftragte (sofern vorhanden) wird auch bei Fragestellungen der Cybersicherheit (von personenbezogenen Daten) von der Informationssicherheit des Unternehmen regelmäßig mit eingebunden.
Grund: Spezifische Datenschutzrisiken und die Rolle der Betroffenen können durch die Expertise des betrieblichen Datenschutzbeauftragten ins Gesamtbild der Unternehmenssicherheit mit einfließen.

☐ Der betriebliche Datenschutzbeauftragte (sofern vorhanden) ist im Bereich der Cyber – und Informationssicherheit geschult und hat ausreichend Ressourcen, um dieses Themenfeld fachlich als auch zeitlich in seine Aufgaben einfließen zu lassen.
Grund: Kenntnisse zur Cybersicherheit gehören zur fachlichen Expertise des betrieblichen Datenschutzbeauftragten.

☐ Sofern ein betrieblicher Datenschutzbeauftragter bestellt ist: Welche Weiterbildungsmaßnahmen im Bereich des technischen Datenschutzes/Cybersicherheit wurden in den letzten 5 Jahren besucht (Kurzbeschreibung)?

_____

_____

_____

_____

☐ Es besteht ein Prozess zur Erkennung von Sicherheitsverletzungen, der auch die Datenschutzrisiken (Risiken der Rechte und Freiheiten einzelner Personen) berücksichtigt und auch Sicherheitsvorfälle, die nicht einer Meldepflicht an die Aufsichtsbehörde unterliegen (z.B. da kein/geringes Risiko), erfasst.
Grund: Die Risikobewertung bei Sicherheitsvorfällen mit Blick auf Unternehmenswerte kann mitunter anders ausfallen als wenn die Risiken für die Betroffenen in den Blick genommen werden. Diese Einschätzungen werden im Rahmen der Kontrollen durch die betrieblichen Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden auch geprüft.

☐ Die Kommunikationswege, über die Sicherheitsvorfälle von Dienstleistern (nach Art. 33 Abs. 3 DS-GVO) gemeldet werden, sind den Stellen im Unternehmen, die Sicherheitsvorfälle erkennen und bewerten müssen bekannt.
Grund: Sicherheitsvorfälle kommen zunehmend auch bei Dienstleistern vor, bei denen entsprechende Informationspflichten an die Auftraggeber vorliegen. Die Gesamtverantwortung trägt aber weiterhin der datenschutzrechtlich Verantwortliche.

7. Angaben zum Unternehmen

a) Anzahl Mitarbeiter (geschätzt/gerundet): _____

b) Anzahl Mitarbeiter, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (geschätzt/gerundet): _____

c) Anzahl der Sicherheitsvorfälle (nach Art. 4 Nr. 12 DS-GVO) in 2023, bei denen ein Risiko der Rechte und Freiheiten angenommen wurde und entsprechend eine Meldung nach Art. 33 DS-GVO erfolgte: _____

d) Anzahl der Sicherheitsvorfälle (nach Art. 4 Nr. 12 DS-GVO) in 2023, bei denen ein hohes Risiko der Rechte und Freiheiten angenommen wurde und entsprechend eine Meldung nach Art. 34 DS-GVO erfolgte: _____

e) Anzahl der Sicherheitsvorfälle (nach Art. 4 Nr. 12 DS-GVO) in 2023, bei denen kein bzw. ein geringes Risiko der Rechte und Freiheiten angenommen wurde und entsprechend keine Meldung nach Art. 33 DS-GVO erfolgte: _____

f) Anzahl der Sicherheitsvorfälle (nach Art. 4 Nr. 12 DS-GVO) in 2023, deren Ursache bei Auftragsverarbeitern nach Art. 28 DS-GVO lag und die Informationen nach Art. 33 Abs. 2 DS-GVO durchführten:

_____

g) Wird ein Informationssicherheitsmanagementsystem (ISMS) im Unternehmen eingesetzt?

☐ Ja. ☐ Nein.

Falls Ja, welche Art von ISMS wird eingesetzt (Kurzbeschreibung):

_____
_____
_____
_____

h) Wird ein Datenschutzmanagementsystem (DSMS) im Unternehmen eingesetzt?

☐ Ja. ☐ Nein.

Falls Ja, welche Art von DSMS wird eingesetzt (Kurzbeschreibung):

_____
_____
_____
_____

Anlage B

Informationsblatt

Ransomware-Präventionsprüfung

Stand: 01.02.2024

Rechtliche Grundlage zur Prüfung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht als Datenschutzaufsichtsbehörde nach Art. 58 der Datenschutz-Grundverordnung (DS-GVO) die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich im Bundesland Bayern, d. h. in privaten Wirtschaftsunternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden. Aufgrund der enorm gestiegenen Gefährdungslage im Internet stärkt das BayLDA seinen Fokus auf präventive Maßnahmen zur Cybersicherheit für bayerische Verantwortliche, damit personenbezogene Daten angemessen und wirksam vor den täglichen Gefahren im digitalen Zeitalter geschützt werden. Das BayLDA führt zu diesem Zweck Prüfungen durch, um grundlegende Sicherheitslücken oder Mängel in der IT-Organisation aufzuzeigen und Verantwortliche somit noch vor einem Vorfall hinsichtlich des Bedarfs an durchzuführenden Maßnahmen hinzuweisen. Auch wenn der vorbeugende Charakter der Datenschutzkontrollen des BayLDA hervorgehoben wird, besteht seit der Anwendbarkeit der DS-GVO neben der bereits existierenden gesetzlichen Verpflichtung, für ein ausreichendes Sicherheitsniveau im Umgang mit personenbezogenen Daten zu sorgen, auch grundsätzlich die Möglichkeit, bei (gravierenden) Verstößen gegen die Sicherheit der Verarbeitung nach Art. 32 DS-GVO Geldbußen zu verhängen.

Ransomware – Mehr als „nur" Verschlüsselung von Daten

Die Verschlüsselung von personenbezogenen Daten mittels Schadcode ist ein seit langer Zeit bekannter und gefürchteter Angriff aus der Cybercrime-Welt. Nicht-verfügbare Daten bedeuten für die meisten Unternehmen Produktionsstillstand oder massive Einschränkungen im Arbeitsalltag – egal ob Arztpraxis, Großkonzern oder Handelsbetrieb. Durch die Möglichkeit der faktisch anonymen Bezahlung per Bitcoin können die daraus abgeleiteten Erpressungen zur Wiederentschlüsselung der Daten unmittelbar und meist ohne großes Risiko einer Entdeckung von Cyberkriminellen durchgeführt werden – die strafrechtlichen Ermittlungen gestalten sich aufgrund der Anonymisierungsmöglichkeiten im Internet als schwierig. Datenschutzrechtlich haben solche Sicherheitsvorkommnisse ebenso Konsequenzen: Als Datenschutzverletzung müssen diese der zuständigen Datenschutzaufsichtsbehörde innerhalb von 72 Stunden nach Kenntniserlangung gemeldet werden. In den vergangenen Jahren wurden dem BayLDA bereits sehr viele Vorkommnisse dieser Art gemeldet, Tendenz steigend.

Verantwortliche begegnen dieser Art der Bedrohung mit zunehmend wirksamen Backup-Konzepten, die einem Angriff mit dem Ziel einer nachhaltigen Datenverschlüsselung unter Umständen standhalten, wenngleich die Wiederherstellung des Datenbestands für viele Betriebe eine Kraftanstrengung im Tagesgeschäft bedeutet. Der größte Aufwand liegt dann darin, Schadcode von den Rechnern zu entfernen, das Einfallstor ausfindig zu machen und zu schließen und letztendlich ein geeignetes Backup einzuspielen. Angreifer-Gruppierungen reagieren jedoch längst auf diese verringerte Wirksamkeit ihrer Schadcode-Kampagnen, indem nach dem erfolgreichen Eindringen in das Netzwerk eines Unternehmens oder nach der Übernahme eines Rechners weiter nach möglichst interessanten Daten, wie Office-Dokumente und Datenbankdateien, gesucht wird. Diese werden nun vor der Verschlüsselung der Daten für die betroffene Organisation unbemerkt auf Server der Angreifer kopiert.

Es werden somit gezielt Daten ausgeleitet. Die Erpresser drohen im Falle, dass Lösegeldforderungen nicht beglichen werden, damit, dass die derart entwendeten Dateien dann entweder im Internet veröffentlicht oder im Darknet an andere Cyberkriminelle verkauft werden. Auch können damit die eigenen Endkunden konfrontiert und erpresst werden.

Eingehende Meldungen zu Verletzungen der Sicherheit nach Art. 33 DS-GVO („Datenschutzverletzungen") beim BayLDA bestätigen, dass dieses Vorgehen weit verbreitet ist. Anhand dieses Trends verändert sich die datenschutzrechtliche Einschätzung von Verschlüsselungstrojanern hinsichtlich der möglichen Schäden grundlegend. Während früher noch häufig von einer ausschließlichen Verschlüsselung ausgegangen wurde und sich das datenschutzrechtliche Risiko nach dem Schaden einer Nicht-Verfügbarkeit von personenbezogenen Daten, IT-Systemen oder Fachprozessen richtete, ist längst auch das Risiko des Vertraulichkeitsverlustes zwingend einzubeziehen. Bei einer Vielzahl typischer Ransomware-Angriffe muss längst davon ausgegangen werden, dass personenbezogene Daten von Angreifern im Kontext von Ransomware entwendet und missbräuchlich weiterverwendet werden. Das Risiko, für die vom Vorfall betroffenen Personen (bzw. für deren Rechte und Freiheiten), dürfte damit als „hoch" einzustufen sein. In der Konsequenz bedeutet dies, dass in solchen Fällen meist auch die betroffenen Personen – z. B. Beschäftigte, Lieferanten, Kunden, Mandaten oder Patienten – gemäß Art. 34 DS-GVO über den Vorfall benachrichtigt werden müssen.

Diese Weiterentwicklung des Ransomware-Vorgehensmodells der Cyberkriminellen bedeutet folglich für Organisationen, die nach einer Ransomware-Infektion nicht von einer Datenausleitung ausgehen, erhöhte Nachweispflichten gegenüber der zuständigen Datenschutzaufsichtsbehörde gerade hinsichtlich der Begründung des Risikos. Insbesondere die Frage einer hinreichenden Wahrscheinlichkeit, dass keine Datenflüsse an die Angreifer stattgefunden haben, muss ausreichend beantwortet werden (z. B. Web-Proxy blockte verdächtigen Serveraufruf, Datenvolumen im Auswertezeitraum erscheint nicht hoch genug). Nachweise dieser Art sind im Rahmen einer Meldung nach Art. 33 DS-GVO beizulegen.

Weiterführende Links zum Thema:

- ✓ BayLDA: Schadcode Informationsseite
  https://www.lda.bayern.de/de/thema_schadcode.html
- ✓ BayLDA: Cyberprävention – Acht Schutzmaßnahmen on top
  https://www.lda.bayern.de/de/cyberpraevention.html
- ✓ BayLDA: Cyberreaktion – Strukturiertes Vorgehen zur Schadensminimierung
  https://www.lda.bayern.de/de/cyberreaktion.html
- ✓ BSI: Ransomware: Bedrohungslage, Prävention und Detektion 2021
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf
- ✓ BSI: Maßnahmenkatalog Ransomware – Arbeitspapier
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf
- ✓ BayLDA: Cybersicherheit in medizinischen Einrichtungen
  https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf
- ✓ BayLDA: Patch Management Checkliste nach Art. 32 DS-GVO
  https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf
- ✓ BayLDA und BayLfD: Microsoft Exchange Security Check & Incident Response
  https://www.lda.bayern.de/media/themen/exchange_security_check_incident_response.pdf