

Checkliste von Sicherheitsmaßnahmen zur Vorbeugung gegen Ransomware-Attacken

1. Systemlandschaft

Ein vollständiger und aktueller Überblick über alle eingesetzten IT-Systeme und IT-Komponenten (wie Clients, Server, Firewall, Switches, VPN-Endpunkte) des eigenen Betriebs ist vorhanden (IT-Inventar, Netzplan). Es findet hierfür ein ordnungsgemäßes Netz- und Systemmanagement statt (u. a. IT-Netzwerke-Trennung, Absicherung von Fernzugriffen, sichere Basiskonfiguration der Systeme und Anwendungen), das die Dokumentation des IT- Netzes als wesentlichen Bestandteil umfasst. Auch Aspekte zum sicheren mobilen Arbeiten (z. B. im Home Office) werden in der Behandlung der Systemlandschaft ausreichend beleuchtet (wie Anbindung der Telearbeitsplätze und anderer mobiler Clients, Mobile Device Management, Regelungen zu Bring Your Own Device, Freigaberichtlinien).

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	Vollständige und aktuelle Liste aller vorhandenen PCs und Notebooks samt Betriebssystem und Betriebssystemversion vorhanden.	Voraussetzung für wirksames Patch Management.
<input type="checkbox"/>	Vollständige und aktuelle Liste aller dienstlichen Smartphones, Tablets und sonstigen mobilen Endgeräte samt Betriebssystem und Betriebssystemversion vorhanden.	Voraussetzung für wirksames Patch Management.
<input type="checkbox"/>	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. vorhandener Netzsegmentierung vorhanden.	Voraussetzung für wirksames Patch Management.
<input type="checkbox"/>	Interne Netzbereiche unterschiedlicher Sicherheitsstufen werden mittels Firewalls getrennt.	Soll das Ausbreiten von Schadcode bzw. von Angreifern innerhalb des Netzwerks erschweren/verhindern (sog. Lateral Movement).
<input type="checkbox"/>	Über das Internet erreichbare Server wie Mailserver, Webserver oder VPN-Endpunkte befinden sich in einem eigenen internen Netzsegment und sind dabei mittels einer Firewall vor dem internen Netzwerk abgesichert (sog. Demilitarisierte Zone – DMZ).	Soll verhindern, dass Angreifer die ggf. kurzzeitig einen derartigen Dienst übernehmen, nicht mühelos auf weitere interne Systeme zugreifen oder zumindest einen Angriffsversuch durchführen können.
<input type="checkbox"/>	Anbindung mobiler Arbeitsplätze (z. B. dienstliche Notebooks, dienstliche Smartphones) über das Internet erfolgt über verschlüsselte und auch kryptographisch authentifizierte Verbindungen (z. B. verschlüsselte VPN mit Authentifizierung mittels starken Passwörtern und kryptographischen Client-Zertifikaten).	Angreifer sollen nicht alleine anhand entwendeter Benutzernamen/Passwörtern ins Unternehmensnetz gelangen können.

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	Aus dem Internet geladene Programme können nicht ohne Nutzerinteraktion ausgeführt werden.	Verhinderung der automatisierten Ausführung von aus dem Internet nachgeladenen Schadcodeprogrammen, nachdem unbeabsichtigt ein Office-Makro aktiviert wurde.
<input type="checkbox"/>	Programme ohne valide Signierung der Authentizität durch das Betriebssystem können nicht ausgeführt werden.	Vom Benutzer fälschlicherweise selbst aus dem Internet heruntergeladene Schadsoftware wird nicht zur Ausführung gebracht.
<input type="checkbox"/>	Es werden keine Privatgeräte im Homeoffice vollständig an das Unternehmensnetz angebunden – Empfehlung: ausschließlich dienstlich administrierte Endgeräte verwenden.	Das Schutzniveau privater Endgeräte kann vom Verantwortlichen nicht gewährleistet werden.
<input type="checkbox"/>	Dienstliche Smartphones und Tablets werden über eine Mobile-Device-Management-Lösung verwaltet.	Voraussetzung für wirksames Patch-Management sowie Datenlöschung im Verlustfall.
<input type="checkbox"/>	Die Installation von Software auf einem PC ist nur mittels Admin-Rechten (durch den Administrator) möglich.	Verhinderung, dass Nutzer aus Versehen als normale Software getarnten Schadcode installiert.
<input type="checkbox"/>	Browser-Plugins (z. B: Flash, Java) werden nur dann installiert, wenn eine (ältere) Anwendung dies unbedingt erforderlich macht.	Viele Browser-Plugins besitzen Sicherheitslücken, die schon beim Besuch einer Webseite ausgenutzt werden können (sog. Drive-By-Angriff).
<input type="checkbox"/>	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.	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.
<input type="checkbox"/>	Microsoft-Office-Pakete sollten so konfiguriert werden, dass diese nur signierte Makros ausführen.	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.

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	Prüfung, ob die Ausführung von Programmen nur aus festgelegten Verzeichnissen (sog. Execution Directory Whitelisting) möglich ist.	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.
<input type="checkbox"/>	Auf dem E-Mail-Server wird ein Spam- und Antivirenfilter eingesetzt.	Damit können schon bekannte Schadprogramme erkannt und verdächtige E-Mails gesondert behandelt werden.
<input type="checkbox"/>	E-Mails mit gefährlichen Dateianhängen wie ausführbaren Dateien, mit Passwort verschlüsselten ZIP-Archiven oder Office-Dokumente mit Makros werden vom Mailserver in einen Quarantäne-Ordner zur Analyse verschoben.	Derartige E-Mails enthalten häufig Schadcode bzw. kleine Programme, die Schadcode herunterladen sollen. Da diese mittlerweile nicht häufig sind, kann eine manuelle Analyse durch die IT-Administration gut durchgeführt werden.
<input type="checkbox"/>	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).	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 internen Absenderadresse haben und nicht gefälscht sind.
<input type="checkbox"/>	Administratoren besitzen zwei Benutzer-Accounts: Einen für reine Administrationsaufgaben und einen für andere Tätigkeiten wie E-Mails lesen oder im Internet surfen.	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.
<input type="checkbox"/>	Auf jedem PC/Server wird für das lokale Administrator-/Root-Konto ein unterschiedliches und starkes (mind. 16 Stellen) Passwort verwendet.	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.

2. Patch Management

Es besteht ein geregelter Updateprozess für alle eingesetzten IT-Systeme und Anwendungen inklusive dazugehöriger Dokumentation zur Versionsübersicht bzw. zu Updates. Es findet eine regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Komponenten statt, damit wichtige Sicherheitsupdates unverzüglich eingespielt werden können. Die eigene Serverlandschaft wird hinsichtlich Patch-Level und Schwachstellen geprüft. Gerade die an das Internet angeschlossenen Server werden dabei regelmäßig kontrolliert (u. a. auch laufendes Monitoring). Vorbereitungen für nicht-patchbare Sicherheitslücken (Zero Day Exploits) wurden getroffen, um im Ernstfall zeitnah angemessen reagieren zu können.

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	Alle PCs und Notebooks sind so konfiguriert, dass Softwareupdates des Betriebssystems automatisch eingespielt werden.	Sicherheitslücken werden unverzüglich geschlossen und können nicht mehr von Angreifern verwendet werden.
<input type="checkbox"/>	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.	Sicherheitslücken werden unverzüglich geschlossen und können nicht mehr von Angreifern verwendet werden.
<input type="checkbox"/>	Es werden ausschließlich Betriebssysteme eingesetzt zu denen der Hersteller Sicherheitsupdates zur Verfügung stellt.	Sicherheitslücken können sonst gar nicht geschlossen werden.
<input type="checkbox"/>	Es besteht eine vollständige Liste der auf allen PCs und Notebooks eingesetzten Anwendungssoftware samt Softwarestand.	Voraussetzung um das Einspielen von Softwareupdates organisieren zu können.
<input type="checkbox"/>	Anwendungssoftware auf PCs und Notebooks wird so konfiguriert, dass Softwareupdates (zumindest Sicherheitsupdates) automatisch eingespielt werden sofern dies möglich ist.	Ein Angriff mittels bekannter Sicherheitslücken (z. B. Browser, PDF-Reader) kann verhindert werden.
<input type="checkbox"/>	Sofern Anwendungsprogramme nicht automatisch aktualisiert werden können, wird sichergestellt, dass diese spätestens monatlich auf den aktuellsten Stand gebracht werden.	Ein Angriff mittels bekannter Sicherheitslücken (z. B. Browser, PDF-Reader) kann verhindert werden.
<input type="checkbox"/>	Es werden ausschließlich Server-Betriebssysteme eingesetzt, für die vom Hersteller noch Sicherheits-Updates bereitgestellt werden.	Sicherheitslücken können sonst gar nicht geschlossen werden.
<input type="checkbox"/>	Es wird für alle Server geprüft, inwiefern diese so konfiguriert werden können, dass Sicherheitsupdates automatisch eingespielt werden können.	Verhinderung, dass mittels Ausnutzung bekannter Sicherheitslücken Angreifer interne Server erfolgreich angreifen und damit zur weiteren Ausbreitung im

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	<p>Für alle Server, bei denen keine automatisierte Einspielung von Sicherheitsupdates aufgrund von Risiken möglicherweise instabiler Serverzustände möglich ist, werden Sicherheitsupdates nach Tests unverzüglich manuell eingespielt. Kritische Sicherheitslücken werden innerhalb weniger Tage zur Anwendung gebracht, sofern keine gleichwertigen anderen Schutzmaßnahmen ergriffen werden.</p>	<p>lokalen Netzwerk missbrauchen können.</p> <p>Verhinderung, dass mittels Ausnutzung bekannter Sicherheitslücken Angreifer interne Server erfolgreich angreifen und damit zur weiteren Ausbreitung im lokalen Netzwerk missbrauchen können.</p>
<input type="checkbox"/>	<p>Sicherheitsupdates aller Netzwerkkomponenten, insbesondere Firewalls und VPN-Appliances werden unverzüglich mit hoher Priorität eingespielt.</p>	<p>Insbesondere bei über das Internet erreichbaren, zentralen Systemen bedeutet ein erfolgreicher Angriff einen sofortigen Ausfall kritischer Schutzkomponenten.</p>
<input type="checkbox"/>	<p>Es besteht eine aktuelle und vollständige Dokumentation darüber, welche PCs, Notebooks, Server, Netzwerkkomponenten automatisch oder manuell upgedatet werden. Bei nicht-automatischen Updates werden dabei die jeweiligen IT-Systeme samt Softwareständen erfasst.</p>	<p>Nur durch eine minimale und schlanke Dokumentation kann auch die Wirksamkeit eines Update-Konzepts sichergestellt und kontrolliert werden.</p>
<input type="checkbox"/>	<p>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.</p>	<p>Verhinderung, dass Angreifer mittels Ausnutzung bekannter Sicherheitslücken mobile Endgerät erfolgreich angreifen und damit Zugang zum Unternehmensnetz erhalten können.</p>

3. Backup-Konzept

Es besteht ein wirksames Backup-Konzept, das entweder die Idee der „3-2-1 Regel“ (3 Datenkopien, 2 verschiedene Speichermedien, 1 davon an externen Standort) bedarfsgerecht umsetzt oder das einen anderen, speziell auf Ransomware-Bedrohungen ausgerichteten wirksamen Ansatz berücksichtigt. Backups werden regelmäßig automatisiert durchgeführt. Es werden Tests durchgeführt, ob alle relevanten Daten im Backup-Prozess enthalten sind und eine Wiederherstellung funktioniert. Das Backup-Konzept wird somit regelmäßig hinsichtlich seiner Wirksamkeit geprüft. Es werden zudem Maßnahmen ergriffen, damit Datensicherungen nicht verschlüsselt werden können.

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	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.	Im Falle einer Ransomware-Attacke können die (personenbezogenen) Daten und die betroffenen IT- System wieder hergestellt werden.
<input type="checkbox"/>	Mindestens ein Backup-System ist durch Schadcode nicht unmittelbar verschlüsselbar (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).	Viele Ransomware-Angriffe versuchen vor einer Verschlüsselung, die Backupssysteme ebenfalls zu verschlüsseln oder die Backups zu löschen. Durch auf Ransomware-Angriffe ausgerichtete Lösungen sollen Risiken bezüglich aktiver Lösversuche der Backups minimiert werden.
<input type="checkbox"/>	Es besteht eine dokumentierte Regelung, welche Daten von welchen Servern oder PCs/Notebooks in ein Backup-Konzept aufgenommen wurden.	Sicherstellung, dass alle relevanten (personenbezogene) Daten auch von einer Backup-Lösung umfasst sind.
<input type="checkbox"/>	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.	Vorbereitung auf den Worst-Case, um prüfen zu können, ob auch alle erforderlichen Daten im Backup enthalten sind.
<input type="checkbox"/>	Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird.	Ein Backup muss täglich durchgeführt werden – es ist auch sicherzustellen, dass dieses funktioniert.
<input type="checkbox"/>	Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert.	Verhinderung der Situation, dass im Worst-Case festgestellt wird, dass bspw. ein Backup-Medium defekt ist oder für eine Systemwiederherstellung erforderliche Information nicht im Backup enthalten sind.

4. Überprüfung des Datenverkehrs

Aufrufe am Internetübergangspunkt werden von uns derart überprüft, dass Netzwerkaktivitäten aus dem internen Netz an bekannte kompromittierte externe Server erkannt werden können (z. B. an der Firewall die Indicators of Compromise, kurz: IoC). Es findet eine Blockierung, Protokollierung und Alarmierung hierzu samt täglicher Aktualisierung der IoC-Listen durch geeignete Quellen statt. Es besteht zudem ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz, Logging, Überwachung und Absicherung der Logfiles). Firewall-Systeme werden regelmäßig hinsichtlich der ordnungsgemäßen Konfiguration überprüft.

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	Der zentrale Internetübergangspunkt vom internen Netzwerk zum Internet ist mittels einer Firewall abgesichert.	Mindeststandard zur Absicherung vertraulicher Netze gegenüber dem Internet.
<input type="checkbox"/>	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 freigeschaltet.	Voraussetzung für Analyse von möglichem Schadcode-Netzwerkverkehr.
<input type="checkbox"/>	Die Web-Proxy-Komponente filtert aufgerufene Internetseiten bezüglich bekannten und täglich aktualisierten Endpunkte, die als (meist gehackte) Server zur Auslieferung von Schadcode verwendet werden (sog. Indicator of Compromise, kurz: IoC) und blockiert sowie protokolliert derartige Aufrufe.	Schadcode wird meistens in mehreren Schritten „ausgeliefert“, was mitunter auf diese Art und Weise unterbunden werden kann.
<input type="checkbox"/>	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 einen missbräuchliche Verwendung zu verhindern und die datenschutzrechtliche Zweckbindung sicherzustellen.	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

Mitarbeiterinnen und Mitarbeiter werden regelmäßig und passend zur öffentlich bekannten Bedrohungslage geeignet über Angriffswege geschult. Im Fokus stehen aktuelle Social-Engineering-Techniken und gefälschte E-Mails, die auch einen Bezug zu bekannter, zum Teil eigener E-Mail-Korrespondenz haben können. Die Geschulten werden dabei instruiert, welches Verhalten angemessen ist (u. a. kein Klick auf fremde Links, kein Öffnen von bestimmten Dateien, kein Aktivieren von Makros). Mitarbeiterinnen und Mitarbeiter steht für die Arbeit an den Endgeräten eine Auswahl von sicheren Authentifizierungsverfahren zur Verfügung (u. a. starke Passwörter mit mind. 10 Stellen für Standard-Passwörter und mind. 16 Stellen für administrative Passwörter, Zwei-Faktor-Lösungen insbesondere für Administration, keine Wiederverwendung von lokalen administrativen Kennungen auf Windows-Rechnern). Die Rollen- und Berechtigungen werden dabei nach dem Least-Privilege-Prinzip eingerichtet.

	Maßnahme	Warum sollte diese Maßnahme umgesetzt werden?
<input type="checkbox"/>	Regelmäßige Schulung der Beschäftigten bezüglich aktueller und häufiger Cyberangriffe (z. B. einmal pro Jahr).	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.
<input type="checkbox"/>	Konsequente Einweisung neuer Beschäftigter zum fachgerechten Umgang mit den IT-Komponenten und Verhalten bei Social-Engineering-Angriffen.	Social-Engineering-Angriffe verursachen nach wie vor hohe Schäden.
<input type="checkbox"/>	Sensibilisierung neuer Beschäftigter bezüglich IT-Risiken vor der Aufnahme der Datenverarbeitung (z. B. auch bei Aushilfskräften).	Sicherheitstechnisches Fehlverhalten von Beschäftigten beruht oft auf fehlender Sensibilisierung und Unterrichtung im Vorfeld.
<input type="checkbox"/>	Darstellung des Ablaufs von Social-Engineering-Angriffen zur Sensibilisierung der Beschäftigten (z. B. Möglichkeit der Manipulation von Telefonnummern).	Social-Engineering-Angriffe verursachen nach wie vor hohe Schäden – die Darstellung konkreter Abläufe verbessert das Wissensbild.
<input type="checkbox"/>	Informationen an die Mitarbeiter über Meldewege (z. B. durch den ISB oder DSB) und Zuständigkeiten.	Eine angemessene Reaktion auf sicherheitstechnisches Fehlverhalten ist ein entscheidender Faktor für eine wirksame und zeitnahe Reaktion auf einen Cyberangriff.