Anforderungskatalog Cybersicherheit

Dieser Anforderungskatalog ermöglicht einen Überblick zu Maßnahmen für eine wirksame Abwehr von Angriffen über das Internet. Aufgrund individueller Gegebenheiten in der jeweiligen Organisation sind die einzuhaltenden Maßnahmen unter den Gesichtspunkten des Art. 32 DS-GVO zu treffen.

Netzstruktur und IT-Systeme

Alle Netzübergänge der Organisation sind im Rahmen einer Netzstrukturaufnahme sowohl im Hinblick auf ihre Anzahl als auch auf die spezifische Art zu identifizieren und zu dokumentieren. Kritisch sind hierbei insbesondere Lösungen, die Schutzmaßnahmen der allgemeinen Netzinfrastruktur umgehen können (bspw. individuelle DSL-Zugänge, UMTS-Datenverbindungen mobiler Endgeräte, verschlüsselte Kommunikationswege wie selbsteingerichtete VPN-Verbindungen).

Absicherung von Netzübergängen: *Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet.*

- ☐ Identifikation aller Netzübergänge
- ☐ Vorhandensein eines strukturierten und aktuellen Netzplans
- ☐ Am Schutzbedarf der Organisation ausgerichtete Netzsegmentierung
  - ☐ Betrieb einer demilitarisierten Zone (DMZ)
  - ☐ Restriktiver Trennung unterschiedlicher Netze
- ☐ Minimierung externer Netzübergänge
- ☐ Absicherung mit geeigneten Sicherheitsgateways
  - ☐ Application Level Gateway bzw. Proxy Firewall
  - ☐ Intrusion Detection
  - ☐ Intrusion Prevention
- ☐ Technische Schnittstellenkontrolle
- ☐ Beschränkung von Berechtigungen mobiler IT-Systeme (Smartphones, Laptops) im Netz auf ein Minimum
- ☐ Absicherung mobiler Zugänge im Verlustfall
  - ☐ Sperrung von Netzzugängen
  - ☐ Einleitung von Lokalisierungsmaßnahmen
  - ☐ Löschmöglichkeit mobiler IT-Systeme aus der Ferne

Firewall:

- ☐ Abschottung des internen Netzes gegenüber dem Internet
- ☐ Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall
- ☐ Monitoring, um Zugriffsversuche zu erkennen
- ☐ Protokollierung auf Firewall-Ebene, um unberechtigte Zugriffe zwischen den Netzen zu erkennen

Administratoren: *Gezielte Sicherung der privilegierten Nutzerkonten.*

- ☐ Nicht-privilegierte Standardkonten für Administratoren für Arbeit außerhalb der administrativen Tätigkeit
- ☐ Begrenzung von Administratoren auf ein Minimum
- ☐ Verwendung sehr starker Passwörter für lokale Admin-Konten
- ☐ Soweit möglich konsequenter Einsatz von Zwei-Faktor-Authentifizierung
- ☐ Keine Abhängigkeit der Organisation von einzelnen Beschäftigten mit Administratorenkennung

☐ Gewährleistung der Arbeitsfähigkeit bei Ausfall des IT-Administrators

Fernwartung: *Der Einsatz von Fernzugängen bietet zahlreiche weitere Angriffsflächen.*

☐ Begrenzung von Fernwartungszugängen auf die konkret zu wartenden Systemen (ggf. „Jump-Server“)
☐ Freischaltung von Fernwartungszugängen nur für konkrete Zwecke und Dauer
☐ Deaktivierung der Übertragung von Dateien – sofern nicht für die Fernwartung erforderlich
☐ Vollständige Protokollierung der Fernwartungszugriffe
☐ Regelmäßige Kontrolle der Zugriffsprotokolle
☐ Kryptographische Absicherung der Fernwartungszugänge (z.B. VPN, TLS)
☐ Sperren bzw. Unterbinden von Fernzugriffen nach Beendigung eines Dienstleistungsvertrages

Home-Office: *Durch Auslagerung der IT-Systeme werden die Gefährdungskreise regelmäßig erweitert.*

☐ Aufstellung der im Home-Office tätigen Beschäftigten
☐ Aufstellung der im Home-Office genutzten Geräte
☐ Gewährleistung der Erreichbarkeit im Home-Office über verschiedene Kommunikationskanäle
☐ Festplattenverschlüsselung mobiler Endgeräte per starker Kryptographie (z.B. AES 256 Bit)
☐ Absicherung der Zugänge mittels VPN-Verbindungen und/oder Zwei-Faktor-Authentifizierung
☐ Regelung zur Nutzung von privaten Endgeräten (z.B. ausschließlich Verbindung zum Terminalserver)
☐ Bei Bedarf Containerlösung zur Trennung von dienstlichen und privaten Inhalten
☐ Informationen zu Umgang mit Videokonferenzen
☐ Regelung zur Mitnahme und Entsorgung sensibler Papierdokumente

Gewährleistung der Verfügbarkeit notwendiger Ressourcen

Backups: *Ausfälle von Datenträgern können nachhaltigen Schaden für die betroffene Organisation auslösen. Regelmäßige Sicherungen sind daher Voraussetzung, um bei einem Ausfall von IT-Komponenten sich möglichst schadlos halten zu können.*

☐ Schriftlich fixiertes Backup-Konzept
☐ Durchführung der Backups nach 3-2-1-Regel (3 Sicherungen, 2 Speichermedien, 1 ausgelagerter Speicherort)
☐ Geeignete physische Aufbewahrung von Backupmedien (z.B. unterschiedliche Brandabschnitte, Tresor)
☐ Regelmäßige Prüfung der Funktionsfähigkeit der Backups
☐ Regelmäßige Prüfung der Wiederherstellungsfunktion im Backup-Prozess

Einbindung externer Dienstleister: *Wesentliche Bereiche, in denen auf externen Sachverstand zurückgegriffen werden sollte, sind:*

☐ Durchführung einer herstellerneutralen Cyber-Sicherheitsberatung
☐ Penetrationstests gegen die eigene IT
☐ Informationssicherheits-Revisionen
☐ Durchführung forensischer Maßnahmen

Notfallkonzept: *Ein Notfall-Konzept stellt die Basis für den Ernstfall dar.*

☐ Vorhandensein eines Notfallkonzeptes (inkl. regelmäßiger Prüfung und Aktualisierung)
☐ Vorhandensein einer Notfall-Reserve-Hardware
☐ Rasche Aufbaumöglichkeit einer Ausweichinfrastruktur

☐ Information an die Beschäftigten über Ansprechpartner in Sicherheitsvorfällen
☐ Sichere Aufbewahrung zentraler Administrationszugangsdaten im Notfall

Abwehr von Schadprogrammen

Die gestaffelte Verteidigung von Angriffen mittels Einsatzes von Schadprogrammen (Viren, Würmer, Trojanische Pferde usw.) muss über eine große Zahl von Systemen verteilt werden. Der Einsatz von Schutzprogrammen ist unerlässlich. Der Einsatz von Schutzprogrammen sollte auf jeden Fall durchgängig auf den Sicherheitsgateways, dem E-Mail-Server, dem Dateiserver sowie mobilen und stationären Arbeitsplatzsystemen vorhanden sein. Bei der Auswahl der Schutzprogramme sollte außerdem darauf geachtet werden, dass mehrere Lösungen unterschiedlicher Anbieter eingesetzt werden. Für die Erreichung einer ausreichenden Schutzwirkung ist, dass unterschiedliche Lösungen auf verschiedene Virensignatur-Datenbanken zurückgreifen (bei Nutzung der gleichen Datenbank, wird keine erhöhte Schutzwirkung entfaltet). Außerdem erweist sich als wertvoll, die Installation und ggf. Ausführung von nichtautorisierter Software mit technischen Mitteln zu unterbinden.

Maleware-Schutz: *Durch Antiviren-Software werden viele Standard-Angriffe erkannt und abgefangen.*

☐ Endpoint Protection auf jedem Arbeitsplatzrechner
☐ Zentrale Erfassung von Alarmmeldungen durch die IT-Administratoren
☐ Automatische Aktualisierung der Antivirensignaturen
☐ Anweisungen an die Beschäftigten zum Umgang mit Maleware-Angriffen
☐ Ablaufplan der IT-Administratoren bei Maleware-Befall
☐ Antiviren-Software mit als „hoch“ konfigurierter lokaler heuristischer Erkennung

Ransomeware-Schutz: *Schadprogramme, die Daten gezielt verschlüsseln, können den Betriebsablauf zum Erliegen bringen. Proaktive Maßnahmen sind unabdingbar, um drohende negative Auswirkungen frühzeitig erkennen und behandeln zu können.*

☐ Makros in Office-Dokumenten
  ☐ Weitestgehender Verzicht auf Makros in Microsoft-Office-Dokumenten
  ☐ Zulassen ausschließlich signierter Microsoft-Office-Makros
☐ Verhinderung einer automatischen Ausführung von heruntergeladenen Programmen
☐ Deaktivierung von Windows Script Hosts auf Clients (sofern nicht zwingend benötigt)
☐ Nutzen eines Web-Proxys mit (tages-)gleichen Sperrlisten von Schadcode-Download-Seiten
☐ Prüfung, ob Einschränkung von PowerShell Scripten mit dem „Constrained Language Mode“ durchführbar ist
☐ Notfallplan für den Umgang mit Verschlüsselungstrojanern

Vermeidung von offenen Sicherheitslücken

Patchmanagement: *Der überwiegende Teil von Angriffen gegen IT-Systeme erfolgt über Schwachstellen in eingesetzten Softwareprodukten. Potenzielle Schwachstellen ergeben sich durch veraltete Softwarebestände. Die im Einsatz befindliche Software muss daher durch regelmäßige Sicherheitsupdates aktuell gehalten werden. Mit vergleichsweise geringem Aufwand kann daher eine große Schutzwirkung durch ein effizientes Patchmanagement erzielt werden.*

☐ Konzept zum Patchmanagement vorhanden (z.B. Update-Plan mit Übersicht zur eingesetzten Software)
☐ Ausschließlicher Einsatz von Desktop-Betriebssystemen
☐ Automatische Updates der Desktop-Betriebssysteme
☐ Prozess für Updates zum zeitnahen Einspielen von Sicherheitsupdates der Server

☐ Geregelter Prozess für Updates der Browser
☐ Geregelter Prozess für Updates von Basiskomponenten
☐ Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software
  ☐ Betriebssystem
  ☐ Office-Software
  ☐ Anwendungssoftware

Sichere Authentisierung

Passwortschutz: *Der Zugang zu personenbezogenen Daten ist Unbefugten durch geeignete Maßnahmen zu erschweren. Starke Passwörter tragen u.a. zur Absicherung von Logins der Beschäftigten bei.*

☐ Authentifikation mit Benutzername und Passwort oder gleichwertigem Verfahren
☐ Zentrale Passwortvergabe
☐ Passwortrichtlinie oder Identity-Management-System inkl. Vorgabe von Passwortlänge und -zusammensetzung
☐ Forderung verschiedener Passwörter für verschiedene Dienste
☐ Verwendung eines Passwortsafes
☐ Regelung zur Sperrung und Neuvergabe von Passwörtern nach einem Vorfall
☐ Sensibilisierung der Beschäftigung hinsichtlich des Umgangs mit Passwörtern

Zwei-Faktor-Authentifizierung: *Eine Authentisierung allein mit Nutzername und Passwort kann im Einzelfall nicht ausreichend sein. Schadprogramme wie Trojanische Pferde oder Keylogger greifen unmittelbar Passwörter ab, sodass auch komplexe Passwörter oder ein häufiger Passwortwechsel keinen hinreichenden Schutz bieten kann. Die Verwendung weitere Zugangsfaktoren kann erforderlich sein, um besonders schützenswerte Zugänge gesondert abzusichern.*

☐ Zwei-Faktor-Authentisierung für Administratorenzugänge (z.B. Cloud-Mail-Dienste)
☐ Grundsätzliche Absicherung von VPN-Verbindungen mit kryptischen Zertifikaten oder Einmalpasswörtern
☐ Bei Chipkartenausgabe als Mitarbeiterausweise Verwendung selbiger zur Standardauthentifizierung

Sichere Interaktion mit dem Internet

Alle Vorgänge zur Abfrage von Diensten und Informationen aus dem Internet sind durch geeignete Maßnahmen abzusichern. Der Schutzmechanismus ist auf den Schutzbedarf des jeweiligen IT-Systems anzupassen.

Sichere Browser: *Eine besonders kritische Komponente bildet der Internet-Browser. Aus diesem Grund ist auf die Absicherung besonderes Augenmerk zu legen.*

☐ Einsatz von Virtualisierungssoftware
☐ Minimierung von Ausführungsrechten
☐ Abschottung besonders gefährdeter Codestellen durch eine Sandbox

Sichere E-Mail-Anwendung: *Durch die unabdingbare E-Mail-Kommunikation werden häufig große Sicherheitsrisiken verursacht.*

☐ Zentrale Untersuchung eingehender E-Mails (insb. der Anhänge) auf Schadprogramme
☐ Zentrale Filterung von Spam-Nachrichten
☐ Nutzung geeigneter Verschlüsselungstechnologie

☐ Anzeige von E-Mails im „Nur-Text-Format“, um manipulierte Links sichtbar zu machen
☐ Einsatz von Security-Komponenten, um Links vor Abruf zu prüfen
☐ Blockieren von gefährlichen Anhängen (z.B. .exe, .doc, .cmd)
☐ Sensibilisierung der Beschäftigung hinsichtlich des Umgangs mit E-Mails (Erkennung gefälschter E-Mails)

Sichere Darstellung von Dokumenten: *Für die Darstellung von Dokumenten aus externen Quellen empfehlen sich folgende Maßnahmen:*

☐ Sichere Darstellungsoption („Geschützte Ansicht“ oder „Geschützter Modus“)
☐ Absicherung der Darstellungskomponenten durch Applikationsvisualisierung

Bewältigung von Sicherheitsvorfällen

Vorbereitung auf Sicherheitsvorfälle: *Die Bewältigung von Sicherheitsvorfällen sollte geübt werden, um die Geschäftsabläufe auch unter erschwerten Bedingungen aufrechterhalten oder zumindest schnell wiederherstellen zu können.*

☐ Umfassende Sensibilisierung und Schulung von Beschäftigten bzgl. Cyberangriffe
☐ Definition von technischen und organisatorischen Rollen
☐ Konsequente Einweisung neuer Beschäftigter zum fachgerechten Umgang
☐ Festlegung von Zuständigkeiten
☐ Sichere Nutzung Sozialer Netze (durch Richtlinien, Sensibilisierung etc.)
☐ Gewährleistung der Erreichbarkeit von Notfallkontakten
☐ Kenntnis der zuständigen Behörden

Meldung von Sicherheitsvorfällen:

☐ Meldung an zuständige Behörden
☐ Konsequente Einbindung des betrieblichen DSB bei Sicherheitsfragen
☐ Konsequente Einbindung des Informationssicherheitsbeauftragten bei Sicherheitsfragen

Sonstiges

☐ Regelmäßige Logdatenerfassung und -auswertung
☐ Sicherstellung eines aktuellen Informationsstands
☐ Automatische Aktualisierung der Antivirensignaturen
☐ Anweisungen an die Beschäftigten zum Umgang mit Maleware-Angriffen
☐ Ablaufplan der IT-Administratoren bei Maleware-Befall
☐ Antiviren-Software mit als „hoch“ konfigurierter lokaler heuristischer Erkennung