Handreichung zum Prüfbogen

Details zur Absicherung von E-Mail-Accounts – Schwerpunkt Phishing

Hinweis:
Diese checklistenartige Auflistung stellt wesentliche Elemente zu den untersuchten Prüfungsschwerpunkten dar. Diese Handreichung ist somit nicht als Prüfbogen zu verstehen und muss daher auch nicht dem BayLDA ausgefüllt vorgelegt werden. Vielmehr soll diese Handreichung die Aussagen, die auf dem Prüfbogen (Anlage A) dargestellt werden, näher erläutern und als Hilfestellung dienen. Es handelt sich um Basisanforderungen – nicht jede gelistete Maßnahme ist zwingend erforderlich, sofern andere Maßnahmen ein gleichwertiges Schutzniveau schaffen.

1. Phishing-Awareness und allgemeines Sicherheitsbewusstsein

☐ Regelmäßige Schulung der Beschäftigten bezüglich aktueller und häufiger Cyberangriffe (ggf. auch durch ein externes Unternehmen für Cybersicherheitsschulungen bei Bedarf)

☐ Wesentlicher Bestandteil dieser Sensibilisierungsmaßnahmen für das eigene Personal: Aktuelle E-Mail-Angriffsarten und bekannte Phishing-Kampagnen

☐ Erläuterung der Gefahren von Emotet und anderer Malware, die durch die Verwendung echter E-Mail-Kommunikationselemente versuchen, Nutzerinnen und Nutzer mit gefälschten Nachrichten zu täuschen

☐ Hilfestellung für die Mitarbeiterinnen und Mitarbeiter zur Erkennung von Fälschungen sowie zum angemessenen Verhalten auf E-Mails (u. a. kein unbedachter Klick auf Links bzw. kein Öffnen von verdächtigen Dateien, kein Aktivieren von Makros, Erkennen der Gefahren von Short-Links)

☐ Durchspielen eines solchen Schadcode-Angriffsszenarios per E-Mail im Rahmen der Schulung mit realistischen Bedrohungen wie z. B. Qakbot oder Emotet

☐ Darstellung des Ablaufs von E-Mail-Angriffen zum finanziellen Betrug zur Sensibilisierung der Beschäftigten, z. B. E-Mails an die Buchhaltung mit Zahlungsaufforderungen und abweichenden Bankdaten: Mechanismen erstellen, um derartige Betrugsversuche frühzeitig zu erkennen (bspw. nur nach direkter Rücksprache mit dem Partnerunternehmen/Kunden Transaktionen in bestimmter Höhe freigeben oder feste Partnerliste mit Bankdaten verwenden)

☐ Erklärung der unterschiedlichen E-Mail-Formate wie Plain-Text, Rich-Text und HTML sowie Hinweis auf die Gefahren der HTML-E-Mails (bspw. eingebundene Bilder und Skripte, grafische Overlays, versteckte Links und Formulare)

☐ Konsequente Einweisung neuer Mitarbeiterinnen und Mitarbeiter zum fachgerechten Umgang mit den E-Mail-Komponenten und zum Verhalten bei Social-Engineering-Angriffen

☐ Sensibilisierung neuer Mitarbeiterinnen und Mitarbeiter bezüglich allgemeinen IT-Risiken vor der Aufnahme ihrer Tätigkeit zur Datenverarbeitung (z. B. auch bei Aushilfskräften, Praktikanten, Werkstudenten)

☐ Informationen an die Mitarbeiterinnen und Mitarbeiter über Meldewege (insbesondere Rollen des Datenschutzbeauftragten und Informationssicherheitsbeauftragten) und Zuständigkeiten – intern wie extern

☐ Mitarbeiterinnen und Mitarbeiter werden geeignet auf einen Sicherheitsvorfall vorbereitet, entsprechende Handlungsschritte dafür werden durchgespielt

☐ Nicht mehr benötigte E-Mails und Kontaktinformationen werden regelmäßig archiviert oder gelöscht, sofern keine Aufbewahrungspflicht dagegenspricht (Datenminimierung)

☐ Keine private Nutzung der dienstlichen E-Mail-Accounts

2. Passwörter, Zwei-Faktor-Authentifizierung und Benutzerverwaltung

☐ Mitarbeiterinnen und Mitarbeitern steht eine Auswahl von sicheren Authentifizierungsverfahren zur Verfügung, um sich an den relevanten Systemen und dem E-Mail-Client anzumelden

☐ Passwortrichtlinie zur Verpflichtung der Nutzung starker Passwörter (u. a. Länge, Komplexität, Ein-Passwort-pro-Dienst-Regel): Starke Passwörter mit mind. zehn Stellen für Standard-Passwörter und mind. 16 Stellen für administrative Passwörter

☐ Multi-Faktor-Authentifizierung bei E-Mail-Accounts; insbesondere falls es der Schutzbedarf des jeweiligen Postfachs erfordert, ist mindestens eine Zwei-Faktor-Authentifizierung als wirkungsvolle Maßnahme gegen Phishing-Angriffe etabliert

☐ Multi-Faktor-Lösungen sind durchgängig bei sämtlichen Administrationsarbeiten im Einsatz

☐ Rollen- und Berechtigungen zu den E-Mail-Konten werden nach dem Least-Privilege-Prinzip eingerichtet (d. h. nur erforderliche Rechte für die Nutzerinnen und Nutzer)

☐ Richtlinien zur Benutzerverwaltung sind vorhanden und werden geprüft (und ggf. angepasst)

☐ Nutzerkonten werden regelmäßig hinsichtlich ihrer Notwendigkeit überprüft (u. a. nicht mehr benötigte E-Mail-Accounts werden stillgelegt, bspw. die von ehemaligen Mitarbeiterinnen und Mitarbeiter)

☐ Keine Wiederverwendung von lokalen administrativen Kennungen auf Windows-Rechnern

☐ Verwenden dedizierter Administratorkonten

☐ Administratoren besitzen mind. zwei Benutzer-Accounts: Einen für reine Administrationsaufgaben und einen für nicht-administrative Tätigkeiten, d. h. abseits des Aufgabengebiets zur IT-Administration

☐ Auf jedem PC/Server wird für das lokale Administrator-/Root-Konto ein unterschiedliches und starkes (mind. 16 Stellen langes) Passwort verwendet

☐ Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administratorkonto) auf einem potenziell infizierten System erfolgen, während es sich noch im Netzwerk befindet

3. Administrative Pflege der Accounts und Konfiguration

☐ Anti-Spoofing: Konfiguration des Mailservers derart, dass E-Mails mit Absenderadressen der eigenen Organisation, die aber von außerhalb zugestellt werden sollen, blockiert werden

☐ Blacklisting von (potentiell) schadhaften Mailservern

☐ Auf dem E-Mail-Server wird ein Spam- und Antivirenfilter mit aktuellen Signaturen eingesetzt

☐ Unterbinden eines automatischen Nachladens von Dateien wie Bilder oder Skripten bei eingehenden E-Mails

☐ Schutz vor bösartigen Anlagen (Dateien): Blockieren von Anlagen mit bestimmten Dateitypen: Potentiell gefährliche E-Mail-Anhänge werden entweder blockiert, in Quarantäne verschoben oder geeignet markiert (z. B. bei .exe, .cmd, .jar)

☐ Schutz vor bösartigen URLs: Links können derart angepasst werden, dass Nutzerinnen und Nutzer diese nicht versehentlich anklicken können

☐ Verhinderung von vollständigen Downloads ganzer E-Mail-Postfächer

☐ Eingrenzung bzw. Monitoring von E-Mails mit großer Anzahl von Empfängern

☐ Einheitliche und gezielt konfigurierte E-Mail-Profile auf den Clients, bspw. auch unter Ansteuerung zentraler Möglichkeiten wie Gruppenrichtlinien

☐ Beenden der automatischen Weiterleitung für E-Mails: Bestehende Regelungen zu automatischen Weiterleitungen, zur Nutzung von Abwesenheitsassistenten und zum Einsatz automatischer Lesebestätigungen werden unter Sicherheitsaspekten geprüft und die Verwendung ggf. stark eingeschränkt

☐ Zugänge über Websites, wie bspw. Outlook Web Access und andere Online-Zugänge zum E-Mail-Client (u. a. Smartphone), werden sicher ausgestaltet (bspw. eingeschränkte Zugriffsmöglichkeiten per IP-Adressraum, Multi-Faktor-Authentifizierung wo möglich und sinnvoll)

☐ 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 ist vorhanden

☐ Interne Netzbereiche unterschiedlicher Sicherheitsstufen werden mittels Firewalls getrennt

☐ 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)

☐ Die Anbindung mobiler Arbeitsplätze (z. B. im Homeoffice: Dienstliche Notebooks, dienstliche Smartphones) über das Internet erfolgt über verschlüsselte und authentifizierte Verbindungen (z. B. verschlüsselte VPN mit Authentifizierung mittels starker Passwörter und kryptographischen Client-Zertifikaten)

☐ Aus dem Internet geladene Programme können nicht ohne Nutzerinteraktion ausgeführt werden

☐ Programme ohne valide Signierung der Authentizität durch das Betriebssystem können nicht ausgeführt werden

☐ Die Installation von Software auf einem PC ist nur mittels Admin-Rechten (durch den Administrator) möglich

☐ Browser-Plugins (z. B. Java) werden nur dann installiert, wenn eine (ältere) Anwendung dies unbedingt erforderlich macht

☐ Skripte wie JavaScript oder Visual Basic werden nur dann vom Betriebssystem ausführbar gelassen, wenn (ältere) Software dies unbedingt erfordert (Anmerkung: Nicht vom Browser, hier ist zumindest JavaScript in der Regel erforderlich)

☐ Microsoft-Office-Pakete sollten so konfiguriert werden, dass diese nur signierte Makros ausführen können, falls Makros erforderlich sind

☐ Prüfung, ob die Ausführung von Programmen nur aus festgelegten Verzeichnissen (sog. Execution Directory Whitelisting) möglich ist

☐ Erweiterte Prüfung von Logs auf sicherheitsrelevante Ereignisse (ggf. Log-Level erhöhen)

☐ Anti-Phishing-Möglichkeiten des eingesetzten Software-Produkts nutzen (z. B. bei Microsoft: Anti-Phishing-Richtlinien in Microsoft Defender für Office 365)

☐ Einrichtung von Verschlüsselungsmöglichkeiten für Mitarbeiterinnen und Mitarbeiter zum sicheren Versenden vertraulicher Nachrichten

4. Überprüfung des Datenverkehrs

☐ Der Internetübergangspunkt vom internen Netzwerk zum Internet ist mittels einer Firewall abgesichert

☐ Der http(s)-Verkehr wird über einen Web-Proxy geleitet: Der Netzwerkverkehr anderer Protokolle ins Internet wird als Standard von der zentralen Firewall weitestgehend geblockt und nur im Einzelfall dokumentiert freigeschalten

☐ 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 (Hinweis: Diese Protokolle sollten verschlüsselt werden, um eine missbräuchliche Verwendung zu verhindern und die datenschutzrechtliche Zweckbindung sicherzustellen)

☐ Einsatz von Intrusion Prevention- und Detection-Systemen zur frühzeitigen Erkennung und Verhinderung von Angriffen

☐ Blockierung, Protokollierung und ggf. Alarmierung von gefährlichen Aufrufen – als Grundlage hierfür dient die Liste zu Indicator of Compromise (IoC)

☐ Die IoC-Liste wird regelmäßig aktualisiert, damit insbesondere das versehentliche Öffnen schadhafter Websites aus Phishing-Mails verhindert werden kann

5. Device und Patch Management sowie Backup-Konzept

☐ Vollständige und aktuelle Liste aller vorhandenen PCs und Notebooks samt Betriebssystem und Betriebssystemversion ist vorhanden

☐ Vollständige und aktuelle Liste aller internen und externen Server samt Betriebssystem und Betriebssystemversion ist vorhanden

☐ Vollständige und aktuelle Liste aller dienstlichen Smartphones, Tablets und sonstigen mobilen Endgeräte samt Betriebssystem und Betriebssystemversion ist vorhanden

☐ Alle PCs und Notebooks sind so konfiguriert, dass Softwareupdates des Betriebssystems automatisch eingespielt werden

☐ Es werden keine Privatgeräte im Homeoffice vollständig an das Unternehmensnetz angebunden (Empfehlung: ausschließlich dienstlich administrierte Endgeräte verwenden)

☐ Dienstliche Smartphones und Tablets werden über eine Mobile-Device-Management-Lösung verwaltet

☐ Es werden keine mobilen Endgeräte eingesetzt, für die es keine Sicherheitsupdates (mehr) gibt

☐ Regelmäßiges Patchen ist als fester Bestandteil der IT-Organisation etabliert: Es besteht eine aktuelle und vollständige Dokumentation darüber, welche PCs, Notebooks, Server, Netzwerkkomponenten etc. automatisch oder manuell upgedatet werden

☐ Es werden ausschließlich Betriebssysteme (sowohl Client als auch Server) eingesetzt, zu denen der Hersteller Sicherheitsupdates zur Verfügung stellt

☐ Es besteht eine vollständige Liste der auf allen PCs und Notebooks eingesetzten Anwendungssoftware samt Softwarestand

☐ Anwendungssoftware auf PCs und Notebooks wird so konfiguriert, dass Softwareupdates (zumindest Sicherheitsupdates) automatisch eingespielt werden, sofern dies möglich ist

☐ Sofern Anwendungsprogramme nicht automatisch aktualisiert werden können, wird sichergestellt, dass diese spätestens monatlich auf den aktuellsten Stand gebracht werden

☐ Es wird für alle Server geprüft, inwiefern diese so konfiguriert werden können, dass Sicherheitsupdates automatisch eingespielt werden können

☐ Für alle Server, bei denen keine automatisierte Einspielung von Sicherheitsupdates aufgrund von Risiken instabiler Serverzustände möglich ist, werden Sicherheitsupdates nach Tests manuell eingespielt: Kritische Sicherheitslücken werden innerhalb weniger Tage zur Anwendung gebracht, sofern keine gleichwertigen anderen Schutzmaßnahmen ergriffen werden

☐ Sicherheitsupdates aller Netzwerkkomponenten, insbesondere Firewalls und VPN-Appliances, werden unverzüglich mit hoher Priorität eingespielt

☐ Ein Notfallplan für technische Störungen oder Cyberangriffe besteht

☐ Ein strukturiertes Backup-Konzept ist vorhanden

☐ 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
(Hinweis: Alternative Konzepte mit mind. gleichem Schutzeffekt ebenso möglich)

☐ Es besteht eine dokumentierte Regelung, welche Daten von welchen Servern oder PCs/Notebooks in das Backup-Konzept aufgenommen wurden

☐ Es wird/wurde ein Planspiel durchgeführt, wie das komplette IT-System in dem Fall wieder aufgesetzt werden kann, falls Server aufgrund einer Vollverschlüsselung nicht mehr funktionsfähig wären

☐ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird

☐ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert