Anlage A

Verantwortlicher:
Empfänger

Bayerisches Landesamt für Datenschutzaufsicht
- Antwort Prüfbogen -
Bitte elektronisch einreichen unter www.lda.bayern.de/kontrolle

Name der Prüfung: **Absicherung von E-Mail-Accounts**
Online-Kennung zur Prüfung:
Aktenzeichen:

Prüfbogen „Absicherung von E-Mail-Accounts“

1. Phishing-Awareness und allgemeines Sicherheitsbewusstsein

Die Mitarbeiterinnen und Mitarbeiter werden regelmäßig und passend zur öffentlich bekannten Bedrohungslage geeignet über E-Mail-Angriffsarten geschult. Insbesondere aktuelle Phishing-Kampagnen stehen hierbei im Vordergrund. So werden Social-Engineering-Techniken und gefälschte E-Mails, die auch einen Bezug zu bekannter, zum Teil eigener E-Mail-Korrespondenz haben können, dargestellt und Erkennungstechniken zum Aufspüren von Fälschungen erläutert. Die Geschulten werden dabei instruiert, welches Verhalten präventiv angemessen ist (u. a. kein unbedachter Klick auf Links bzw. Öffnen von Dateien, kein Aktivieren von Makros), aber auch, welche Reaktion zu erfolgen hat, falls der Verdacht einer fehlerhaften Handlung oder eines Sicherheitsproblems besteht.

☐ **Ja**, diese Aussage trifft für unsere Organisation zu.

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Eine ausführliche Begründung hierzu wird beigelegt.

2. Passwörter, Mehr-Faktor-Authentifizierung und Benutzerverwaltung

Den Mitarbeiterinnen und Mitarbeitern steht eine Auswahl von sicheren Authentifizierungsverfahren zur Verfügung, um sich an den relevanten Systemen und dem E-Mail-Client anzumelden (bspw. Passwörter mit ausreichender Länge und Komplexität, mehrstufige Authentifizierung). Dort, wo eine erhöhte Form der Absicherung erforderlich erscheint, werden Zugänge zwingend mit einem zusätzlichen Authentifizierungsfaktor als Ergänzung zum Passwort geschützt. Die Rollen- und Berechtigungen zu den E-Mail-Konten werden nach dem Least-Privilege-Prinzip eingerichtet (= nur erforderliche Rechte für die Nutzer). Richtlinien zur Benutzerverwaltung sind vorhanden und werden regelmäßig geprüft und ggf. angepasst. Zudem werden Nutzerkonten regelmäßig hinsichtlich ihrer Notwendigkeit überprüft (u. a. nicht mehr benötigte E-Mail-Accounts werden stillgelegt, bspw. die von ehemaligen Mitarbeiterinnen und Mitarbeiter).

☐ **Ja**, diese Aussage trifft für unsere Organisation zu.

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Eine ausführliche Begründung hierzu wird beigelegt.

3. Administrative Pflege der Accounts und Konfiguration

Die Verwaltung der E-Mail-Postfächer erfolgt strukturiert durch eine Fachabteilung. Durch administrative Einstellungen werden die Clients gezielt konfiguriert und abgesichert (z. B. Verhinderung von vollständigen Downloads ganzer Postfächer). So werden die Default-Einstellungen der verwendeten E-Mail-Software geprüft und durch geeignete Profile organisationsweit kontrolliert. Einstellungen zu Weiterleitungsregelungen und Abwesenheitsassistenten werden unter Sicherheitsaspekten betrachtet und ggf. eingeschränkt. Zugänge über Websites wie bspw. Outlook Web Access und andere Online-Zugänge zum E-Mail-Client (z. B. Smartphone) werden sicher ausgestaltet. Homeoffice-Faktoren zur sicheren Einwahl werden zudem berücksichtigt (u. a. VPN, eingeschränkte Zugriffsmöglichkeiten per IP-Adressraum).

☐ **Ja**, diese Aussage trifft für unsere Organisation zu.

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Eine ausführliche Begründung hierzu wird beigelegt.

4. Überprüfung des Datenverkehrs

Aktivitäten am Internetübergangspunkt werden kontrolliert, sodass Aufrufe aus dem internen Netz an bekannte kompromittierte externe Server erkannt werden können (z. B. an der Firewall durch Indicators of Compromise, kurz: IoC). Es findet hierfür eine Blockierung, Protokollierung und Alarmierung samt regelmäßiger Aktualisierung der IoC-Listen durch geeignete Quellen statt, damit das versehentliche Öffnen schadhafter Websites aus Phishing-Mails verhindert bzw. erkannt wird. Zudem besteht ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz, Logging, Überwachung und Absicherung der Logfiles). Firewall-Systeme werden darüber hinaus regelmäßig hinsichtlich der ordnungsgemäßen Konfiguration überprüft.

☐ **Ja**, diese Aussage trifft für unsere Organisation zu.

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Eine ausführliche Begründung hierzu wird beigelegt.

5. Device und Patch Management sowie Backup-Konzept

Ein vollständiger und aktueller Überblick aller eingesetzten IT-Komponenten des eigenen Betriebs ist vorhanden (IT-Inventar bspw. mit Notebooks aus dem Homeoffice). Es findet hierfür eine sichere Basiskonfiguration der Systeme und Anwendungen statt. Auch Aspekte zum sicheren mobilen Arbeiten (z. B. im Homeoffice) werden in der Behandlung der Systemlandschaft ausreichend beleuchtet (Anbindung der Telearbeitsplätze und anderer mobiler Clients). Zur Absicherung der E-Mail-Komponenten besteht ein geregelter Updateprozess inklusive dazugehöriger Dokumentation zur Versionsübersicht. Wichtige Sicherheitsupdates werden unverzüglich eingespielt. Die eigene IT-Landschaft wird regelmäßig hinsichtlich des Patch-Levels geprüft, insbesondere wegen bekannter Schwachstellen. Darüber hinaus besteht ein wirksames Backup-Konzept zur Sicherung personenbezogener Daten, auch für die Daten aus der E-Mail-Kommunikation.

☐ **Ja**, diese Aussage trifft für unsere Organisation zu.

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Eine ausführliche Begründung hierzu wird beigelegt.