Absender:

Empfänger
Straße
Plz Ort

Bayerisches Landesamt für Datenschutzaufsicht
- Antwortbogen Prüfung -
Postfach 1349
91504 Ansbach

Aktenzeichen:

Prüfbogen zur Ransomware-Präventionsprüfung

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).

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

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Die ausführliche Begründung hierzu befindet sich auf einem Begleitblatt, das diesem Prüfbogen in unserer Antwort beigelegt wird.

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.

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

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Die ausführliche Begründung hierzu befindet sich auf einem Begleitblatt, das diesem Prüfbogen in unserer Antwort beigelegt wird.

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 regemäßig hinsichtlich seiner Wirksamkeit geprüft. Es werden zudem Maßnahmen ergriffen, damit Datensicherungen nicht verschlüsselt werden können.

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

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Die ausführliche Begründung hierzu befindet sich auf einem Begleitblatt, das diesem Prüfbogen in unserer Antwort beigelegt wird.

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.

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

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Die ausführliche Begründung hierzu befindet sich auf einem Begleitblatt, das diesem Prüfbogen in unserer Antwort beigelegt wird.

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.

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

☐ **Nein**, diese Aussage trifft für uns nicht oder nicht vollständig zu. Die ausführliche Begründung hierzu befindet sich auf einem Begleitblatt, das diesem Prüfbogen in unserer Antwort beigelegt wird.

_____	_____	_____
Unterschrift des Verantwortlichen	Name des Verantwortlichen (leserlich in Druckbuchstaben)	Datum