Checkliste

Auf diese 10 Maßnahmen der Informationssicherheit kommt es an

So schützen Sie Ihr Unternehmen vor Cyberattacken

Nie war Informationssicherheit wichtiger: Im Jahr 2022 waren über 84 Prozent der Unternehmen von Datendiebstahl betroffen – Tendenz steigend (Bitkom Research, 2022). Dabei sollte klar sein, dass kein Weg an umfassenden Sicherheitsmaßnahmen im IT-Bereich vorbeiführen kann.

Eine Schlüsselrolle kommt den Mitarbeitenden zu. Sie sollten unbedingt grundlegende Regeln und Prinzipien kennen, um sich effektiv vor Cyberattacken schützen zu können. In unserer Checkliste haben wir die 10 wichtigsten Tipps zur Informationssicherheit für Ihren Betrieb zusammengefasst.

Hinweis: Diese Liste ist als Empfehlung zu betrachten. Die domeba distribution GmbH übernimmt keine Gewähr für die Aktualität, Vollständigkeit oder Richtigkeit der Checkliste.

1. Umgang mit Spam und Phishing Mails

Alle Beschäftigten müssen unbedingt wissen, woran sie verdächtige E-Mails erkennen und wie sie mit diesen umgehen sollten. Die wichtigsten Grundregeln: Beantworten Sie entsprechende E-Mails niemals, öffnen Sie keine Anhänge und klicken Sie nicht auf Links. Tippen Sie Hyperlinks im Zweifelsfall lieber selber ein. Geben Sie zudem niemals Ihre Daten an, wenn Sie von unbekannten Mailabsendern dazu aufgefordert werden. Leiten Sie E-Mails, denen Sie misstrauen, am besten direkt an Ihre IT-Abteilung weiter.

2. Sichere Passwörter

Nicht weniger wichtig ist die Verwendung sicherer Passwörter. Legen Sie hierfür einheitliche Richtlinien zu Mindestlänge, Komplexität und Änderungsintervall fest. Empfehlenswert sind mindestens acht, besser aber zwölf gemischte Zeichen. Entscheidend ist, dass Sie Kennwörter niemals mehrfach verwenden und auch nirgendwo notieren.

Die Arbeit mit einem Passwort-Manager kann hierbei sinnvoll sein. Daneben bietet es sich an, die Zwei-Faktor-Authentifizierung (2FA) einzusetzen, wenn diese zur Verfügung steht.

3. Daten klassifizieren und verschlüsseln

Verschaffen Sie sich einen Überblick über alle im Unternehmen verarbeiteten Daten und Informationen. Klassifizieren Sie dann, welche Daten besonders vertraulich sind und daher einem besonderen Schutz bedürfen. Verschlüsseln Sie sensible Informationen wie Verträge, Kundendaten oder Gehaltsinformationen in jedem Fall.

4. Zugriffskontrollen

Eine Grundvoraussetzung sind auch klare Regeln für den Zugriff auf vertrauliche Informationen. Dabei gilt: Vergeben Sie Zugänge nur so viel wie nötig und so wenig wie möglich, um unautorisierte Zugriffe zu vermeiden. Möglich ist es, bspw. auf Gruppenrichtlinien zurückzugreifen, um die Freigabe von Daten und den Zugang zu Anwendungen zu steuern. Überprüfen Sie regelmäßig, ob die Zugriffsrechte von Beschäftigten und externen Benutzern noch aktuell sind.

Der Einfachheit und besseren Lesbarkeit halber wird im Text das generische Maskulinum verwendet – gemeint sind damit immer alle Geschlechter.

Checkliste

Auf diese 10 Maßnahmen der Informationssicherheit kommt es an

5. Netzwerksicherheit

Um den Datenverkehr zu kontrollieren, sollten Sie in jedem Fall eine Firewall einrichten. Bei der Konfiguration Ihrer Firewall legen Sie fest, wann der Datenfluss blockiert oder weitergeleitet wird. Empfehlenswert ist es außerdem, Netzwerke nach ihrer Vertrauenswürdigkeit voneinander zu trennen. Prüfen Sie dabei, wann der Datenverkehr zwischen WLAN, LAN usw. wirklich erforderlich ist.

6. Sicherer Umgang mit Cloud-Diensten

Wenn Sie im Unternehmen mit Cloud-Diensten arbeiten, sollten Sie im Vorfeld einen Blick auf die Datenhoheit des Cloud-Anbieters werfen. Wie sehen die Nutzungsrechte und der Datenschutz des Dienstes aus? Wichtig ist auch hier, eine Verschlüsselung Ihrer Daten vorzunehmen und den Zugang für Dritte zu kontrollieren. Bei der Freigabe von Dokumenten sollten Sie klare Ablauffristen festlegen, um zu verhindern, dass Unberechtigte auf die Informationen zugreifen können.

7. Aktuelle Updates und Antivirus-Software

Spielen Sie verfügbare Updates so zeitnah wie möglich auf allen Geräten ein. Das gilt nicht nur für das Betriebssystem, sondern auch für jegliche installierte Software. So halten Sie das Sicherheitsniveau immer auf dem aktuellen Stand. Für einen zentralen Schutz sorgt natürlich ebenso eine Antivirus-Software, die auf allen IT-Systemen vorhanden sein sollte. Regelmäßige Komplettscans und Aktualisierungen sind hierbei Pflicht.

8. Regelmäßige Backups und Notfallpläne

Vor dem Verlust wertvoller Daten schützen natürlich auch Backups, die es regelmäßig zu erstellen gilt. Kontrollieren Sie unbedingt, ob das Backup funktionsfähig ist und im Ernstfall problemlos wiederhergestellt werden kann. Hilfreich ist dafür ein Notfallwiederherstellungsplan bzw. Disaster-Recovery-Plan, den Sie regelmäßig überprüfen sollten. Überlegen Sie dazu im Vorfeld, welche Schritte bei Störungen oder Angriffen notwendig sind, um schnellstmöglich wieder einsatzfähig zu sein.

9. Mobile Geräte berücksichtigen

Schnell in Vergessenheit geraten bei Maßnahmen rund um die Informationssicherheit oftmals mobile Geräte. Dabei treffen die wesentlichen Sicherheitsprinzipien ebenso auf diese zu. Wir empfehlen Ihnen, eine VPN-Verschlüsselung zu verwenden und App-Berechtigungen kritisch zu hinterfragen. Auch hier sind aktuelle Software-Updates durchzuführen. Löschen Sie zudem nicht mehr benötigte WLAN-Netzwerke aus der Liste des Smartphones.

Der Einfachheit und besseren Lesbarkeit halber wird im Text das generische Maskulinum verwendet – gemeint sind damit immer alle Geschlechter.

Checkliste

Auf diese 10 Maßnahmen der Informationssicherheit kommt es an

10. Mitarbeitende schulen

Zuletzt noch eine goldene Regel: Sensibilisieren Sie Ihre Belegschaft für Informationssicherheit. Alle Schutzvorkehrungen der IT-Abteilung nützen wenig, wenn sich die Beschäftigten, die täglich mit den Daten und Systemen arbeiten, nicht den Gefahren bewusst sind. Angestellte müssen wissen, wie Cybercrime-Angreifer vorgehen und mit welchen Prinzipien diese arbeiten.

Wiederholte Schulungen zu den Themen Security Awareness, IT-Sicherheit oder Datenschutz sind daher unerlässlich. Darin vermitteln Sie auch die wichtigsten betriebsspezifischen Regeln und Vorgaben im Umgang mit den Informationen.

Weitere Informationen finden Sie auch hier:

Allianz für Cyber-Sicherheit (o. J.): 10 Tipps zur Cyber-Sicherheit für Unternehmen.
Online verfügbar unter
https://www.allianz-fuer-cybersicherheit.de/dok/10349920
(Abgerufen am 08.03.2023).

Bundesamt für Sicherheit in der Informationstechnik (2023): Cyber-Sicherheit für KMU. Die TOP 14 Fragen.
Online verfügbar unter
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_KMU.pdf?__blob=publicationFile&v=8
(Abgerufen am 08.03.2023).

Der Einfachheit und besseren Lesbarkeit halber wird im Text das generische Maskulinum verwendet – gemeint sind damit immer alle Geschlechter.