# IT-Sicherheit, Datensicherheit

## Gefahren erkennen, Sicherheitsstrategien entwickeln, Schutzmaßnahmen umsetzen

Die Sicherheit der IT-Systeme, aber auch die Kompetenz im Umgang damit, schützt vor Datenverlust, Datenverfälschung, Computer- und Internetkriminalität. Unternehmen sollten daher eine geeignete Sicherheitsstrategie entwickeln, die vor potentiellen Gefahren schützt. Die Sensibilisierung der Mitarbeiter ist dabei ein wichtiger Sicherheitsfaktor. Diese Seite bietet einen Überlick über IT-Sicherheit im Unternehmen.

15.11.2021

## Strategien und Ratgeber zur IT-Sicherheit

Jedes Unternehmen sollte seine Sicherheitsmaßnahmen zentral organisieren und ein regelmäßiges Sicherheits-Update durchführen. Eine Sicherheitsstrategie für die Unternehmens-IT zu entwickeln, ist daher von Vorteil. So kann man Gefahren für die Informationstechnologie und die Datensicherheit besser einschätzen und angemessen darauf reagieren.

Das Webinar-Video Datensicherheit im eigenen Unternehmen und beim Auftragsverarbeiter zeigt wichtige Aspekte von IT-Sicherheit im Unternehmen und was im Zusammenhang mit dem neuen Datenschutzrecht zu beachten ist.

Das IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter hilft bei der Sensibilisierung der Belegschaft vor Gefahren und unterstützt als Schulungsunterlage.

## IT-Sicherheit für KMU und EPU

Klein- und Mittelbetriebe (KMU) können mithilfe des Online-Ratgebers it-safe die unternehmenseigene IT-Infrastruktur auf ihre Sicherheit hin beurteilen. Das IT-Sicherheitshandbuch für KMU bietet praktische Informationen über mögliche Gefahren und die richtigen technischen Maßnahmen dagegen.

Mit der EPU-Checkliste für Ein-Personen-Unternehmen kann man in wenigen Minuten feststellen, ob und wo es Sicherheits-Probleme im IT-Bereich geben könnte.

Im Notfall (z. B. bei einer Cyberattacke oder Verschlüsselung Ihrer Daten durch einen Erpressertrojaner) erhalten Sie bei der Cyber-Security-Hotline unter 0800 888 133 rund um die Uhr kostenlos Hilfe.

## Gesetzliche Richtlinien zur IT- und Datensicherheit

Die Verantwortung für die IT-Sicherheit liegt laut Unternehmensgesetzbuch (UGB) und GmbH-Gesetz (GmbHG) grundsätzlich immer bei der Geschäftsführung.

Auch wenn sicherheits-relevante IT-Aufgaben an Mitarbeiter übergeben werden, trägt die Unternehmensführung für die Einhaltung der gesetzlichen Bestimmungen letztendlich die Verantwortung.

Die EU-Datenschutzgrundverordnung (DSGVO) und das österreichische Datenschutzgesetz regeln den Umgang mit personenbezogenen Daten (z. B. Name, Geburtsdatum, E-Mail-Adresse, IP-Adresse).
Mit der NIS-Richtlinie (EU) 2016/1148, die in Österreich Ende 2018 durch das Netz- und Informationssystemsicherheitsgesetz (NISG) umgesetzt wurde, gibt es erstmals umfassende Regelungen im Bereich Cybersicherheit für strategisch wichtige Unternehmen, digitale Diensteanbieter und Behörden auf europäischer und nationaler Ebene.

Unternehmen müssen geeignete technische und organisatorische Maßnahmen (z. B. Datensicherung, Verschlüsselung, Zutrittskontrollen) treffen, um Daten vor zufälliger Zerstörung, Datenverlust oder unrechtmäßiger Verwendung Dritter zu schützen. Andernfalls drohen hohe Geldstrafen.

Die WKO bietet Unterstützung zur Umsetzung der DSGVO mit branchenspezifischen Informationen, Leitfäden, Musterdokumenten und Checklisten. Der Leitfaden technische und organisatorische Maßnahmen im Rahmen der DSGVO bietet eine praxisgerechte Übersicht, welche technischen Sicherheitsvorkehrungen notwendig und sinnvoll sind und wie diese im Unternehmen umgesetzt werden können.

## Umgang mit Daten, Datensicherung

Das richtige Datensicherungskonzept hilft gegen Datenverlust. Ein regelmäßiges Daten-Backup gehört dabei zu den Pflichtaufgaben. Nur so können Daten vor Verlust und Beschädigung geschützt werden.

Folgende Punkte sind bei der Datensicherungsstrategie zu beachten:

- Umfang und Klassifizierung der zu sichernden Daten (Geschäfts- und Produktionsdaten, Systemdateien, Datenbanken, Laufwerke...)
- Sicherungstechnologie und -medien (Sicherungsbänder, Wechselfestplatten, Cloud-Speicher, USB-Sticks, CD/DVD...)
- Zeitintervall und Zeitpunkt der Sicherungen (z. B. täglich, wöchentlich, an Werktagen)
- Anzahl der aufzubewahrenden Sicherungen aus der Vergangenheit
- Zuständigkeit für Durchführung, Überwachung und Dokumentation der Sicherungen
- Aufbewahrung der Backup-Datenträger
- Überprüfung der Datensicherungen, Wiederherstellungstests und -übungen

Das Video Datensicherung in 4 Schritten erklärt, was Sie bei der Sicherung Ihrer Daten beachten müssen. Mit dem Online-Ratgeber Datensicherung können Sie eine Bestandsaufnahme über die Datensicherung in Ihrem Unternehmen machen und Tipps erhalten, wie Sie die Sicherung Ihrer Daten optimieren können.

## Gefahrenquellen

Unternehmer sollten sich einen Überblick möglicher Bedrohungen aus dem Internet verschaffen. Menschliches Versagen (z. B. unabsichtliches Löschen von Daten, Verlust von Smartphone), Schadprogramme ("Malware"), Datendiebstahl und Cyberkriminalität stellen die größten Sicherheitsrisiken dar.

Um Schadsoftware wie Viren, Würmer und Trojaner abzuwehren, ist es wichtig, die verschiedenen Malware-Infektionswege und die grundlegenden Schutzmaßnahmen zu kennen. Malware-Angriffe lassen sich rechtzeitig bekämpfen, wenn man die Warnsignale dafür erkennt.

Gefahren stellen auch Denial of Service-Attacken auf einen Server, Rechner oder sonstige Komponenten in einem Datennetzwerk sowie gezielt eingesetzte Erpressersoftware ("Ransomware") dar. Schutzmaßnahmen gegen die Manipulation von Telefonanlagen durch Telefon-Hacking ("Phreaking") sollten sowohl der Provider als auch das Unternehmen ergreifen. Einige Sicherheits-Tipps gegen Telefon-Hacker können die Gefahr reduzieren.

## Sicherheit in Netzwerken

Zum Schutz vor Gefahren durch eine Netzwerkverbindung zum Internet gelten Virenschutzprogramme und Firewalls als Mindestanforderung, um Computer- und Netzwerke zu schützen.

Ob Local Area Network (LAN) oder Wireless LAN (WLAN): Durch Internetverbindung entstehen Gefahren, wenn nicht zusätzlich Schutzmaßnahmen eingerichtet werden. Zum sicheren Internetsurfen bieten sich teilweise verschlüsselte Verbindungen und vollständig verschlüsselte Verbindungen an.

Vorsicht ist bei der Nutzung von Drahtlosen Netzwerken (sogenannte WLAN-Technologie) angebracht. WLAN-Netzwerke stellen ein Sicherheitsrisiko dar, wenn der Datenverkehr unverschlüsselt stattfindet.

## IT- und Datensicherheit auf mobilen Endgeräten

Bei der Nutzung von Laptops, Tablets, Smartphones liegen die größten Probleme im Sicherheitsbereich. Gefahrenpotenziale entstehen besonders durch das Verwenden privater Endgeräte im Unternehmen ("Bring your own device"). Die Risiken bei Mobiltelefonen bestehen vor allem bei der Freigabe mobiler Applikationen, der GPS-Funktion, dem Datenklau oder Geräteverlust.

Beim Einsatz von betriebsfremden Geräten sollte zur Gefahrenvermeidung eine Festlegung von IT Sicherheitsstandards erfolgen und eine IT-Betriebsvereinbarung mit den Mitarbeitern getroffen werden.

Zur Datensicherheit bei der Nutzung mobiler Endgeräte im Unternehmen sollten folgende zwei Punkte eingehalten werden:

1. Sicherstellung des passwortgeschützten Zugriffs
2. Das regelmäßige Sichern der Daten

# Informationssicherheit im Unternehmensalltag

Unerwünscht zugesendete Spam- oder Phishing-Mails sowie mit Schadsoftware verseuchte Nachrichten können im täglichen E-Mail-Verkehr in den Posteingangs-Ordner gelangen. Auch Social Engineering ("Human Hacking") und soziale Netzwerke stellen Gefahrenquellen im Arbeitsalltag dar.

In Fällen von Phishing-Angriffen, Spam-Mails oder Social Engineering geht es darum, an Passwörter (z. B. PIN oder TAN), persönliche Daten oder an vertrauliche Informationen zu gelangen. Auch Betrugsabsichten, die Infizierung mit Computerviren oder das Eindringen in Computernetzwerke sind möglich.

Die Einhaltung von Umgangs- und Verhaltensregeln durch die Mitarbeiter und der Einsatz von Sicherheitsprogrammen können Risiken minimieren. Passwörter sind daher ein wichtiges Mittel gegen unberechtigte Zugriffe auf IT-Systeme und Daten.

Praktische Tipps, um Mitarbeiterinnen und Mitarbeiter gezielt auf das Thema IT Security aufmerksam zu machen und zu schulen, finden Sie im IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter.