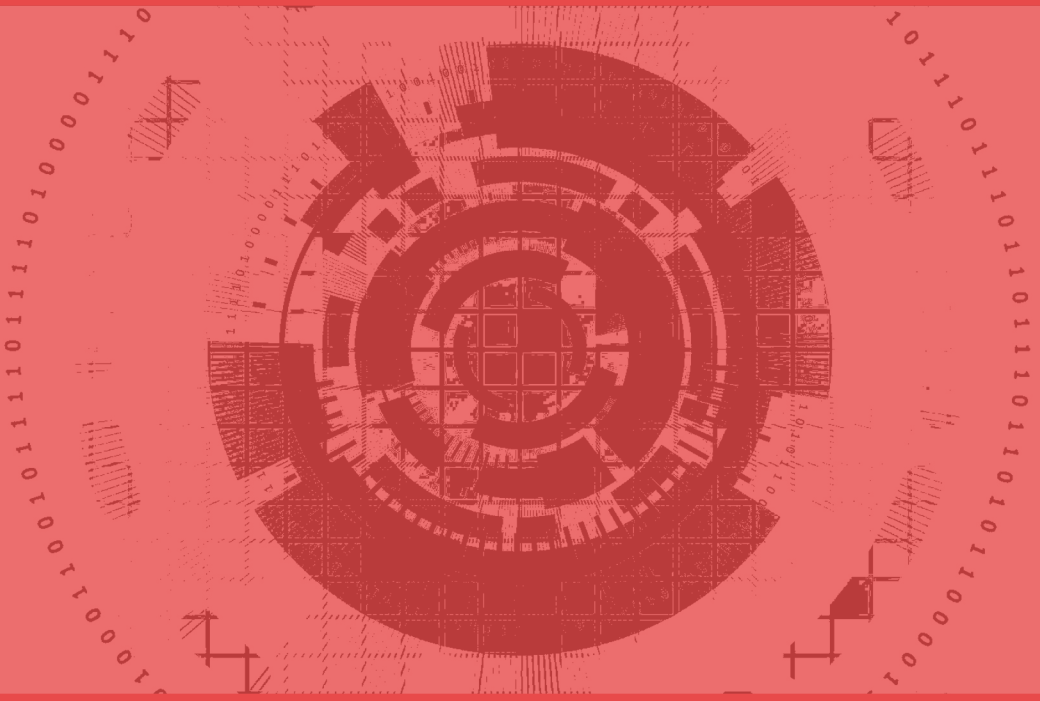
Cyber-Sicherheitsrat Deutschland e.V.

6 Basics Cybersicherheit



Kleine und mittlere Unternehmen (KMU)

Wie schütze ich mein Unternehmen?

Der Mittelstand, kleine und mittlere Unternehmen sind das Rückgrat der deutschen Wirtschaft. Sie erwirtschaften einen großen Teil des Bruttosozialproduktes und bieten Arbeitsplätze für Millionen. Kleine und mittlere Unternehmen sind attraktiv, allerdings leider auch für Cyber-Kriminelle.

Mehr als die Hälfte der Cyber-Angriffe trifft kleine und mittelgroße Unternehmen mit weniger als 500 Mitarbeitern. Bei vielen kleineren Mittelständlern kommt noch hinzu, dass sie nicht die gleiche Cybersicherheitsinfrastruktur wie große Konzerne aufweisen, die eigene IT-Abteilungen und flächendeckenden IT-Sicherheitsschutz finanzieren und aufrechterhalten können.

Die gute Nachricht ist, dass sich auch kleine Unternehmen durch konkrete Schritte schützen können, die leicht einzuführen und beizubehalten sind. Die große Mehrheit der Cyber-Angriffe kann durch diese Schritte verhindert oder abgefangen werden.

In diesem Leitfaden, der kontinuierlich gemäß der aktuellen technologischen Entwicklungen und neuster Erkenntnisse angepasst wird, stellt der Cyber-Sicherheitsrat Deutschland e.V. ihnen die wichtigsten Schritte vor.

Mit freundlichen Grüßen

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

1. Schadsoftware verhindern!

Jeder mit dem Internet verbundene Computer ist ein Einfallstor für **Schadsoftware**. Für die Sicherheit und den Betrieb ist daher ein Schutz vor diesen Programmen unabdingbar. Mit einigen wenigen Schritten ist ihr Unternehmen gegenüber vielen Bedrohungen aus dem Netz geschützt. Wichtig ist eine funktionierende **Antivirensoftware** und **Firewall** sowie regelmäßige **Software-Updates**. Wichtig ist außerdem, **keine externen Speicher** zuzulassen, durch die Schadsoftware auf den PC gelangten kann.

- ✓ **Antivirensoftware auf allen Geräten**
- ✓ **Regelmäßige Updates aller Software**
- ✓ **Keine externen USB-Sticks/Festplatten**
- ✓ **Firewall installieren**

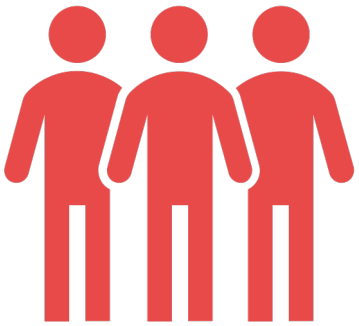
2. Passwörter managen!

Einer der wichtigsten Grundsätze für IT-Sicherheit ist ein vernünftiges **Passwortmanagement.** Das heißt **gute, sichere und für jeden Account verschiedene Passwörter** zu verwenden, die für Angreifer nicht einfach zu erraten, aber für Mitarbeiter leicht zu merken sind. Mit einem **Passwort-Manager** ist es einfacher: Das Programm speichert alle ihre Passwörter, sie müssen sich nur ein Masterpasswort merken. **Standardpasswörter** sollten niemals verwendet werden. Für wichtige Konten sollte die **2-Faktoren-Authentifizierung** verwendet werden, etwa ein nach Passworteingabe am PC einzugebender Code vom Smartphone. Mitarbeitenden sollte die Möglichkeit gegeben werden, **Passwortkopien sicher aufzubewahren**, um den „Zettel unter der Tastatur" zu vermeiden.

- ✓ **2-Faktoren Authentifizierung**
- ✓ **Standardpasswörter vermeiden**
- ✓ **Sichere Passwörter verwenden**
- ✓ **Sichere Aufbewahrung von Passwortkopien**

3. Den Faktor Mensch kontrollieren!

Bei den meisten Cyber-Angriffen ist das schwächste Glied mittlerweile nicht mehr das Netzwerk oder der PC, sondern der **Mensch**, der davor sitzt. Techniken wie **Social Engineering** und **Phishing** zielen darauf ab, Informationen wie Passwörter oder Zugänge durch Vorspielen falscher Tatsachen zu erschleichen. **Externe E-Mails** sollten automatisch als solche **gekennzeichnet** werden. Mitarbeitende sollten möglichst wenig Zugriffe an ihrem Arbeitsplatz haben, **Administratorrechte** nur wenn sie absolut notwendig sind. Das Melden von Cyber-Angriffen sollte gefördert werden , um Mitarbeitenden bei zukünftigen Angriffen nicht von Meldungen abzuschrecken.
Mitarbeiterschulungen in Cybersicherheit helfen, Phishing-Techniken zu erkennen und deren Erfolg zu mindern.



- ✓ **Keine Administratorenrechte für Mitarbeiter**
- ✓ **Meldung von Cyber-Angriffen fördern**
- ✓ **Kennzeichnung externer E-Mails**
- ✓ **Schulung zum Erkennen von Phishing**

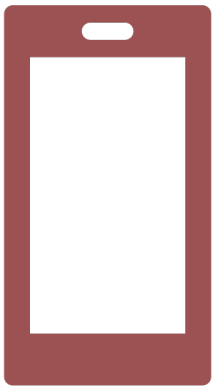
4. Daten sichern!

Eine Folge von Cyber-Angriffen, aber auch von Hardwareschäden können Datenverluste sein. Kundendaten, Aufträge und Zahlungsdaten könnten durch Angriffe verloren gehen. Deswegen ist **Datensicherung** für den fortlaufenden Betrieb unabdingbar. Wichtig ist, Daten regelmäßig zu sichern und **vom PC unabhängig und für Mitarbeitende unzugänglich** zu speichern. Zusätzlich wären eine **Datensicherung in der Cloud** (auf Servern im Internet) oder eine Verschlüsselung der Daten ideal. Durch Datensicherung in der Cloud läuft die Synchronisierung in der Regel automatisch. Durch **Datenverschlüsselung** sind Daten zusätzlich gesichert.

- ✓ **Identifikation von wichtigen Daten**
- ✓ **Diversifizierung der Datensicherung**
- ✓ **Datensicherung in der Cloud**
- ✓ **Datenverschlüsselung als Zusatzschutz**

5. Geräte sichern!

Die Arbeitswelt verändert sich und viel Kommunikation passiert mittlerweile mit **mobilen Endgeräten**. Um Cybersicherheit herzustellen müssen auch diese Geräte sicher sein. Standardmäßig müssen **alle Geräte passwortgeschützt** oder durch PIN zugangsbeschränkt sein. Veraltete Apps oder von inoffiziellen Seiten heruntergeladene Apps auf Geräten sind ein Sicherheitsrisiko: **Regelmäßige Updates** schließen Sicherheitslücken. In der Öffentlichkeit sollten Sie sich **nie mit ungesicherten Hotspots oder WLAN-Netzen verbinden.** Für viele Geräte, Betriebssysteme und Software gibt es **ab einem gewissen Alter keine Updates mehr.** Diese sollten dann **schnell ersetzt** und nicht mehr verwendet werden.



- ✓ **Sicherung aller Geräte mit PIN/Passwort**
- ✓ **Regelmäßige Updates**
- ✓ **Nicht mit ungesicherten Netzen verbinden**
- ✓ **Veraltete Software/Geräte ersetzen**

6. Krisenmanagement!

Der schlimmste Fall ist eingetreten: Die IT in ihrem Betrieb wurde durch einen Cyber-Angriff oder Hardwareausfall lahmgelegt. Jetzt ist vor allem Krisenkommunikation wichtig, mit internen und externen Stellen. Cyber-Angriffe können bei Behörden meldepflichtig sein, Kunden und Öffentlichkeit müssen gegebenenfalls informiert werden. In jedem Fall ist es wichtig, dass **Notfallpläne** bereitliegen, die genau vorschreiben was im Falle des Falles zu tun ist. Schlüsselstellen müssen zusammenarbeiten und **kommunizieren.** Spezielle **Krisenkommunikationstrainings** für Mitarbeitende sind hier unabdingbar. Gegebenenfalls muss externe Hilfe hinzugezogen werden, um ein schnellstmögliches **Wiederherstellen der Systeme** und damit den weiteren Betriebsablauf zu ermöglichen. Dafür müssen Verantwortlichkeiten klar benannt und verteilt werden, die Verantwortlichen müssen die **notwendigen Entscheidungen dann schnell und konsequent treffen.**

- ✓ **Notfallpläne erarbeiten**
- ✓ **Verantwortliche benennen**
- ✓ **Krisenkommunikationstrainings**
- ✓ **Schnelle Entscheidungen**

Cybersicherheit
auf einen Blick

1 Schadsoftware verhindern!

- ✓ Antivirensoftware
- ✓ Regelmäßige Updates
- ✓ Keine externen USB-Sticks
- ✓ Firewall installieren

2 Passwörter managen!

- ✓ 2-Faktoren Authentifizierung
- ✓ Standardpasswörter vermeiden
- ✓ Sichere Passwörter verwenden
- ✓ Sichere Aufbewahrung von Passwortkopien

3 Faktor Mensch kontrollieren!

- ✓ Keine Administratorenrechte
- ✓ Meldung von Cyber-Angriffen
- ✓ Kennzeichnung externer E-Mails
- ✓ Schulung zum Erkennen von Phishing

4 Daten sichern!

- ✓ Identifikation wichtiger Daten
- ✓ Datensicherung
- ✓ Sicherung in der Cloud
- ✓ Datenverschlüsselung

5 Geräte sichern!

- ✓ Alle Geräte mit PIN/Passwort
- ✓ Regelmäßige Updates
- ✓ Keine ungesicherten Netze
- ✓ Software/Geräte ersetzen

6 Krisenmanagement!

- ✓ Notfallpläne erarbeiten
- ✓ Verantwortliche benennen
- ✓ Krisenkommunikationstrainings
- ✓ Schnelle Entscheidungen

Ganzheitlich denken:
Zugang beschränken, Daten sichern, Systeme schützen!

Cyber-Sicherheitsrat Deutschland e.V.