

# Cyber Sicherheits Check für KMU

## Basismaßnahmen für Ihre Cybersicherheit

- 1 Sicherheitslücken schließen
- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen
- 5 Netzübergänge absichern
- 6 Schadprogramme abwehren
- 7 Notfallplan erstellen
- 8 Inventarisieren und dokumentieren



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



 Hochschule Aalen

CSBW

CYBER  
SICHERHEITS  
AGENTUR  
BADEN-WÜRTTEMBERG

# Inhalt

## Einleitung

CYBERSICHERHEIT IST FÜHRUNGSAUFGABE  
VERANTWORTUNG  
GEFAHRENBEWUSSTSEIN  
ZUSTÄNDIGKEITEN  
IT-SICHERHEITSRICHTLINIE

## Basismaßnahmen

1 SICHERHEITSLÜCKEN SCHLIESSEN  
2 BENUTZERZUGÄNGE ABSICHERN  
3 DATENSICHERUNG DURCHFÜHREN  
4 GEFAHRENBEWUSSTSEIN SCHAFFEN  
5 NETZÜBERGÄNGE ABSICHERN  
6 SCHADPROGRAMME ABWEHREN  
7 NOTFALLPLAN ERSTELLEN  
8 INVENTARISIEREN UND DOKUMENTIEREN

## Weitere Themen

HOMEOFFICE UND MOBILES ARBEITEN  
PHYSISCHE IT-SICHERHEIT  
CLOUDBASIERTE LÖSUNGEN  
CYBERVERSICHERUNGEN

## Checkliste



# CYBERSICHERHEIT IST FÜHRUNGSaufgabe

## VERANTWORTUNG

Stellen Sie sich als Unternehmensleitung Ihrer Verantwortung, Cybersicherheit umzusetzen und ihr entsprechende Relevanz einzuräumen.

Entscheiden Sie, welches Sicherheitsniveau Sie anstreben und welche Restrisiken gegebenenfalls akzeptabel sind.

Stellen Sie ausreichend finanzielle und personelle Ressourcen für die IT-Sicherheit zur Verfügung.

Seien Sie als Unternehmensleitung ein Vorbild bei der Einhaltung von Sicherheitsregeln.

## GEFAHRENBEWUSSTSEIN

Seien Sie sich der Gefahr bewusst, dass die Unternehmensleitung ein bevorzugtes Angriffsziel von Cyberkriminellen darstellt.

Sensibilisieren Sie Ihre Führungskräfte für das Thema Cybersicherheit. Setzen Sie es z. B. regelmäßig auf die Tagesordnung von Besprechungen.

Stellen Sie sicher, dass Ihre Beschäftigten regelmäßig sensibilisiert werden z. B. durch Schulungen und Newsletter.

## ZUSTÄNDIGKEITEN

Legen Sie eindeutig fest, welche Person oder Stelle im Unternehmen für den Bereich der IT-Sicherheit zuständig ist.

Falls Sie mit einem IT-Dienstleister zusammenarbeiten, legen Sie die von ihm übernommenen Aufgaben explizit in einem Dienstleistungsvertrag fest.

## IT-SICHERHEITSRICHTLINIE

Entwickeln Sie für Ihr Unternehmen eine IT-Sicherheitsrichtlinie, in der klare Verhaltensregeln, Anforderungen und Zuständigkeiten festgelegt sind.

Halten Sie Ihre IT-Sicherheitsrichtlinie stets aktuell.

Kommunizieren Sie die Vorgaben bezüglich Cybersicherheit regelmäßig an Ihre Mitarbeitenden und prüfen Sie deren Einhaltung.

Regeln Sie den Zugriff auf IT-Systeme und Dokumente, indem Sie für Ihr Unternehmen ein rollenbasiertes Berechtigungskonzept erstellen.

Weisen Sie jeder Rolle nur die Zugriffsberechtigungen zu, die sie zur Erfüllung ihrer Aufgaben benötigt (Prinzip der minimalen Rechte).



Ein Beispiel einer IT-Sicherheitsrichtlinie finden Sie hier: DIHK. Nutzungsrichtlinie IT-Sicherheit  
<https://sl.csc-kmu.de/ek-01.html>



# 1

## Sicherheitslücken schließen

### SOFTWAREAKTUALISIERUNGEN (UPDATES UND PATCHES)

Legen Sie einen Update-Prozess fest und benennen Sie einen Verantwortlichen.

Aktualisieren Sie alle Anwendungen regelmäßig.

Aktivieren Sie möglichst die automatischen Aktualisierungsfunktionen.

Ermitteln Sie Hard- und Software, die manuell zu aktualisieren sind.

Aktualisieren Sie Betriebssysteme und Anwendungssoftware sobald Sicherheitsupdates vom Hersteller zur Verfügung stehen.

Ersetzen Sie Systeme, die nicht mehr vom Hersteller unterstützt werden (d. h. keine Sicherheitsupdates mehr erhältlich) durch neue Produkte.

Können Sie das System nicht ersetzen, dann isolieren Sie es (z. B. mittels Firewall).



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



 Hochschule Aalen

CSBW

CYBER  
SICHERHEITS  
AGENTUR  
BADEN-WÜRTTEMBERG

#### 1 Sicherheitslücken schließen

- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen
- 5 Netzübergänge absichern
- 6 Schadprogramme abwehren
- 7 Notfallplan erstellen
- 8 Inventarisieren und dokumentieren

# 1

## Sicherheitslücken schließen

### ARGUMENTE:

Software-Updates und -Patches sind ein Grundpfeiler der Cybersicherheit und ein Erfolgsrezept gegen Cyberangriffe. Zu spät oder nicht installierte Updates sind ein häufiger Grund für gelungene Cyberangriffe auf kleine und mittlere Unternehmen.

### WEITERFÜHRENDE INFORMATIONEN:

Verschaffen Sie sich einen vollständigen Überblick der gesamten im Unternehmen eingesetzten Software (Inventarisierung siehe Basismaßnahme 8). Prüfen Sie, ob neue Softwareversionen mehr Schutz bieten. Updates und Patches dürfen sich nicht nur auf das Betriebssystem beschränken. Sie sollten alle Anwendungssoftware umfassen, also auch Office-Anwendungen, ERP, Controlling, Webbrowser, Rechnungsprogramme u. a. Hierfür ist vorab eine grundlegende Erhebung erforderlich.

### FALLBEISPIEL

Ein Unternehmen erfährt von einer kritischen Sicherheitslücke in Microsoft Exchange, spielt aber das Sicherheitsupdate nicht zeitnah ein. Die Täter nutzen die Sicherheitslücke bereits nach zwei Tagen aus und verschlüsseln alle Dateien auf Servern und Arbeitsplatzrechnern. Die Lösegeldforderung beträgt mehrere 10 Tsd. Euro in Bitcoin.

### FOLGEN

Verlust aller digital gespeicherten Unterlagen inklusive der Sicherungen.  
Massive Beeinträchtigung des Geschäftsbetriebs ggf. inklusive finanziellem Schaden, Rückgriff auf Papierunterlagen erforderlich! Erheblicher personeller Aufwand: manueller Notbetrieb, Neuaufsetzen der internen IT-Infrastruktur.



Falls Sie einen Dienstleister beauftragt haben, stellen Sie vertraglich sicher, dass er auch tatsächlich alle in Ihrem Unternehmen verwendeten IT-Systeme aktualisiert. Haben Sie keinen Dienstleister beauftragt, dann weisen Sie jemandem die Aufgabe eindeutig zu.

*BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, Seite 13, Frage 4*

<https://sl.csc-kmu.de/b1-01.html>



Kann eine Schwachstelle nicht durch Softwareupdates geschlossen werden, sind weitergehende Maßnahmen notwendig.

*BSI – Management von Schwachstellen und Sicherheitsupdates, siehe Punkt 4*

<https://sl.csc-kmu.de/b1-02.html>



Management von Schwachstellen und Sicherheitsupdates. Empfehlungen für kleine Unternehmen und Selbstständige.

*BSI – Veröffentlichungen zur Cybersicherheit*

<https://sl.csc-kmu.de/b1-03.html>



Prüfen Sie, ob auf Ihren Geräten automatische Updates aktiviert sind.

*BSI – Sind automatische Updates auf meinem Gerät aktiviert?*

<https://sl.csc-kmu.de/b1-04.html>



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 2

## Benutzerzugänge absichern

### TRENNUNG VON AUTHENTISIERUNGSDATEN

- Identifizieren Sie Bereiche unterschiedlichen Schutzbedarfs.
- Trennen Sie die Konten von Administratoren und anderen Nutzern.
- Vergeben Sie für jedes Konto und jeden Zugang ein eigenes Passwort. Ändern Sie vor-eingestellte Passwörter ab.

### PASSWORTSICHERHEIT

Bei der Passwortsicherheit sind Länge und Komplexität entscheidend.

Legen Sie eine Passwortrichtlinie fest, die von allen Mitarbeitenden einzuhalten ist.

Stellen Sie sicher, dass alle Passwörter geheimgehalten werden.

### ZWEI-FAKTOR-AUTHENTISIERUNG

Schützen Sie zumindest kritische Konten und Konten mit weitreichenden Rechten durch die Einrichtung einer Zwei-Faktor-Authentisierung (2FA).

Richten Sie bei Fernzugriffen und VPN möglichst immer eine 2FA ein.

Grundsätzlich gilt: Wenn von einem Dienst-anbieter (E-Mail, soziale Medien usw.) eine 2FA angeboten wird, sollte diese auch genutzt werden.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



BADEN-WÜRTTEMBERG  
LANDESKRIMINALAMT  
BADEN-WÜRTTEMBERG

 Hochschule Aalen



CSBW  
CYBER  
SICHERHEITS  
AGENTUR  
BADEN-WÜRTTEMBERG

1 Sicherheitslücken schließen

**2 Benutzerzugänge absichern**

3 Datensicherung durchführen

4 Gefahrenbewusstsein schaffen

5 Netzübergänge absichern

6 Schadprogramme abwehren

7 Notfallplan erstellen

8 Inventarisieren und dokumentieren

## ARGUMENTE:

Viele Angriffe aus dem Internet werden dadurch ermöglicht, dass zu einfache Passwörter oder dieselben Passwörter für verschiedene Dienste verwendet werden. Schlecht gewählte Passwörter stehen auf der »Hitliste« besonders häufiger IT-Sicherheitsdefizite ganz weit oben.

## WEITERFÜHRENDE INFORMATIONEN:



Passwörter sind besonders wichtig für die IT-Sicherheit. Achten Sie darauf, komplexe, den Richtlinien entsprechende Passwörter zu verwenden.  
*BSI – Cyber-Sicherheit für KMU – Die TOP 14 Fragen, S. 16-17, Frage 7*  
<https://sl.csc-kmu.de/b2-01.html>



*BSI – Sichere Passwörter erstellen*  
<https://sl.csc-kmu.de/b2-02.html>



*BSI – Passwörter Schritt für Schritt merken*  
<https://sl.csc-kmu.de/b2-03.html>



*CSBW-Factsheet: Sichere Passwörter*  
<https://sl.csc-kmu.de/b2-04.html>



Sie können herausfinden, ob Ihre Identitätsdaten (E-Mail-Adresse, Passwort) ausspioniert wurden.  
*Hasso-Plattner-Institut – Wurden Ihre Identitätsdaten ausspioniert?*  
<https://sl.csc-kmu.de/b2-05.html>



Ein Passwort-Manager ist ein hilfreiches Werkzeug, um verschiedene, komplexe Passwörter zu verwalten. Es gibt gute Passwort-Manager, auch kostenfreie Open-Source-Produkte.  
*BSI – Passwörter verwalten mit dem Passwort-Manager*  
<https://sl.csc-kmu.de/b2-06.html>



Zwei-Faktor-Authentisierung (2FA) ist die letzte Brandmauer gegen Angriffe auf Ihre Benutzerkonten. Deshalb sollten alle, insbesondere aber wichtige Konten und Zugänge mit 2FA abgesichert werden. Wenn Sie dies nicht selbst tun können, sollten Sie auf fachliche Unterstützung zurückgreifen.  
*BSI – Zwei-Faktor-Authentisierung*  
<https://sl.csc-kmu.de/b2-07.html>



*CSBW-Factsheet: Zwei-Faktor-Authentifizierung*  
<https://sl.csc-kmu.de/b2-08.html>



Zugriffsschutz: Ihre Geräte (PC, Mobilgeräte etc.) müssen auch vor physischen Zugriffen – also vor Personen, die sich dem Rechner nähern – geschützt werden. Stellen Sie sicher, dass ein Sperrbildschirm eingerichtet ist, der nur mit einem Passwort entsperrt werden kann.  
Clean-Desk: Ein aufgeräumter Desktop und ein aufgeräumter Schreibtisch sind ebenfalls wichtiger Bestandteil guter Informationssicherheit.  
*CSBW-Factsheet: Clean Desk und Clean Desktop*  
<https://sl.csc-kmu.de/b2-09.html>

## FALLBEISPIEL

Bei einem mittelgroßen Unternehmen in Süddeutschland erlangten Täter Zugriff auf mehrere Server, die wegen Fernwartung und mobilem Arbeiten über das Internet erreichbar waren. Sie verschlüsselten alle erreichbaren Dateien und löschten Originaldateien. Lösegeld wurde gefordert. Das Unternehmen nutzte die Standard-Konfiguration der Microsoft-Systeme und hatte keinen Schutz gegen Password-Guessing-Angriffe.

## FOLGEN

Alle IT-Systeme waren kompromittiert und mussten auf Basis einer vorhandenen Datensicherung aufwendig neu aufgesetzt werden.



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 3

## Datensicherung durchführen

### REGELMÄSSIG BACKUPS ERSTELLEN

Führen Sie eine regelmäßige und automatische Datensicherung durch.

Orientieren Sie sich beim Turnus des Backups an der Frequenz der anfallenden geschäftskritischen Daten.

Beachten Sie die 3-2-1-Regel:  
Drei Kopien auf zwei unterschiedlichen Medienträgern und ein Medium physisch von der Arbeitsumgebung getrennt an einem anderen, sicheren Ort aufbewahren.

Verschlüsseln Sie die Datensicherung, vor allem wenn Daten an einen anderen Ort gebracht werden. Der Schlüssel sollte in diesem Fall separat auf einem externen Datenträger und in physischer Form aufbewahrt werden.

Testen und dokumentieren Sie regelmäßig die Wiederherstellung der Daten.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



 Hochschule Aalen



1 Sicherheitslücken schließen

2 Benutzerzugänge absichern

**3 Datensicherung durchführen**

4 Gefahrenbewusstsein schaffen

5 Netzübergänge absichern

6 Schadprogramme abwehren

7 Notfallplan erstellen

8 Inventarisieren und dokumentieren

# 3 Datensicherung durchführen

## ARGUMENTE:

Wenn Daten verloren gehen und nicht vorher gesichert wurden, kann das existenzbedrohende Folgen haben. Wenn regelmäßige Datensicherungen/Backups durchgeführt werden, können die betrieblichen Aktivitäten nach einem Vorfall, gerade auch nach einem Ransomware-Angriff, schneller wieder aufgenommen werden.

## HINWEISE:

### 1- Identifizieren Sie die Daten, die gesichert werden sollen.

Um die relevanten Daten zu identifizieren, müssen Sie zunächst Ihre Datenverarbeitungssysteme inventarisieren und dann bestimmen, welche Daten von wesentlicher Bedeutung für Ihre Geschäftstätigkeit sind.

### 2- Legen Sie fest, wie häufig Datensicherungen durchgeführt werden sollen.

Das Intervall der Datensicherungen sollte in Abhängigkeit von der Menge der in einem bestimmten Zeitraum anfallenden digitalen Daten festgelegt werden.

### 3- Wählen Sie geeignete Speichermedien, mit denen die Daten gesichert werden sollen.

Dabei kann es sich um physische Medien wie eine externe Festplatte handeln, oder um Speicherplatz in einer Cloud, die aber nach der Datensicherung vom Informationssystem getrennt werden müssen.

### 4- Prüfen Sie, welche Daten verschlüsselt werden sollen.

Die Verschlüsselung von Daten vor dem Speichern ist eine empfohlene Praxis. Sie ist besonders wichtig bei Daten, die in der Cloud oder auf mobilen Geräten gespeichert werden: Bei einem unberechtigten Zugriff bleiben die Daten geschützt.

## FALLBEISPIEL

Ein Einzelhändler hatte von zu Hause einen VPN-Zugang eingerichtet über den Angreifer sich auf seinen Computer in der Firma Zugriff verschafften und die gespeicherten Daten verschlüsselten.

Der Betriebsinhaber hatte regelmäßig Backups auf eine externe Festplatte überspielt, allerdings versäumt die Wiederherstellung der Daten zu testen.

## FOLGEN

Das Backup war nicht funktionsfähig und die Wiederherstellung der Daten nicht möglich. Der Verlust der kompletten Firmendaten führte zum Konkurs des Unternehmens.

## WEITERFÜHRENDE INFORMATIONEN:



*BSI – Cybersicherheit für KMU – Die TOP 14 Fragen,  
Seite 11-12, Frage 3.*

<https://sl.csc-kmu.de/b3-01.html>



*BSI – Datensicherung – wie geht das?*

<https://sl.csc-kmu.de/b3-02.html>



*BSI – Backup: Doppelt gesichert hält besser*

<https://sl.csc-kmu.de/b3-03.html>



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 4

## Gefahrenbewusstsein schaffen

### AKTUELLEN INFORMATIONENSTAND SICHERSTELLEN

Definieren Sie die Quellen, aus denen man sich regelmäßig über neue Sicherheitslücken informiert.

Abonnieren Sie Newsletter, von denen Sie bzw. die Verantwortlichen regelmäßig automatisch über neue Sicherheitslücken und aktuelle Entwicklungen benachrichtigt werden.

Sorgen Sie für die Weitergabe und Umsetzung der Erkenntnisse an Ihre Mitarbeitenden und legen Sie dazu Verantwortlichkeiten fest.

### SENSIBILISIERUNG UND SCHULUNG

Stellen Sie Ihr Personal in den Mittelpunkt. Motivieren Sie die Mitarbeitenden durch wirksame Kommunikation und betriebliche Initiativen.

Versorgen Sie die Mitarbeitenden regelmäßig mit Kurzinformationen.

Schulen Sie alle Beschäftigten regelmäßig, realitätsnah und abgestimmt auf die speziellen Bedürfnisse. Dies gilt von der Arbeits- bis zur Leitungsebene und auch für den Ausbau der Kompetenzen der Administration.

Sensibilisieren Sie Ihre Beschäftigten insbesondere für das Verhalten in sozialen Medien in Form verbindlicher Vorgaben und Aufklärungsmaßnahmen.

Schärfen Sie das Verantwortungsbewusstsein bei Ihren Beschäftigten, dass Sicherheitsvorfälle und verdächtige Wahrnehmungen gemeldet werden. Definieren Sie entsprechende Meldewege.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



**POLIZEI**  
BADEN-WÜRTTEMBERG  
LANDESKRIMINALAMT  
BADEN-WÜRTTEMBERG

 Hochschule Aalen



**CSBW** CYBER  
SICHERHEITS  
AGENTUR  
BADEN-WÜRTTEMBERG

- 1 Sicherheitslücken schließen
- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen**
- 5 Netzübergänge absichern
- 6 Schadprogramme abwehren
- 7 Notfallplan erstellen
- 8 Inventarisieren und dokumentieren

# 4 Gefahrenbewusstsein schaffen

## ARGUMENTE:

Phishing, CEO-Fraud und andere Versuche von Cyberkriminellen im großen Stil an Daten von Firmen zu gelangen, erfolgen meist über den Faktor Mensch.

Technische Schutzmaßnahmen können noch so gut sein – wenn sorglos und nachlässig mit Daten, Programmen und Rechnern umgegangen wird, nützen sie recht wenig.

## WEITERFÜHRENDE INFORMATIONEN:

Informieren Sie sich immer aktuell über seriöse, externe Quellen und stellen Sie sicher, dass auch Ihre Mitarbeitenden über Gefahren und Sicherheitsmaßnahmen unterrichtet werden.

## NEWSLETTER UND INFOSEITEN



Cybersicherheitsagentur Baden-Württemberg

Tel.: 0711 137-99999

Cyber-Ersthilfe der Cybersicherheitsagentur Baden-Württemberg

<https://sl.csc-kmu.de/b4-01.html>



CSBW-Sicherheitshinweise

<https://sl.csc-kmu.de/b4-02.html>



Zentrale Ansprechstelle Cybercrime (ZAC)  
beim LKA Baden-Württemberg

Tel.: 0711 5401-2444

Aufnahme in Verteiler möglich über E-Mail: [cybercrime@polizei.bwl.de](mailto:cybercrime@polizei.bwl.de)

<https://sl.csc-kmu.de/b4-03.html>



Newsletter bestellen

BSI – Newsletter

<https://sl.csc-kmu.de/b4-04.html>



BSI- Cyber-Sicherheitswarnungen

BSI – Cyber-Sicherheitswarnungen

<https://sl.csc-kmu.de/b4-05.html>



## LERNSPIELE

Kostenfreie Schulungsmöglichkeiten und  
Bedrohungsanalyse durch Lernspiele

BAKGame – IT-Sicherheit in der Wirtschaft

<https://sl.csc-kmu.de/b4-06.html>

## FALLBEISPIEL

Eine Mitarbeiterin der Buchhaltung eines Unternehmens erhielt eine gefälschte E-Mail. Laut dieser forderte ihr Chef sie dringlich auf, einen fünfstelligen Betrag für den Kauf einer Maschine auf die beigefügte Bankverbindung zu überweisen. Da sich der Chef zu diesem Zeitpunkt auf Geschäftsreise im Ausland befand, erschien dies der Mitarbeiterin logisch.

## FOLGEN

Die Mitarbeiterin kam der sehr bestimmten Aufforderung des vermeintlichen Chefs nach. Als der Betrug erkannt wurde, war das Geld bereits in der Hand der Täter.



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 5

## Netzübergänge absichern

### FIREWALL EINRICHTEN

Nutzen Sie Firewalls zum Schutz aller kritischen Systeme, insbesondere als Schutzmauer zwischen Firmennetzwerk und Internet.

Sichern Sie möglichst auch alle internen Netzübergänge mit einer Firewall ab.

Schützen Sie Zugänge zu Netzen und IT-Systemen für Administratoren, vor allem für Fernwartung und Fernadministration.

Achten Sie auf eine strenge Filtereinstellung, die alle nicht zwingend notwendigen Verbindungen blockiert.

### NETZÜBERGÄNGE IDENTIFIZIEREN UND SEGMENTIEREN

Sorgen Sie für eine Netzwerksegmentierung (z. B. mittels physikalischer Trennung oder VLAN) sowie weitgehende Minimierung externer Netzübergänge.

Identifizieren und dokumentieren Sie alle Netzübergänge.

Überlegen Sie, was am Netz hängen muss und was physikalisch getrennt werden kann. Grundsatz: Trennen Sie alles vom Internet, was nicht erforderlich ist.

Lassen Sie Zugriffe von außen auf Ihr Firmennetz nur über ein VPN zu.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



BADEN-WÜRTTEMBERG  
LANDESKRIMINALAMT  
BADEN-WÜRTTEMBERG

 Hochschule Aalen



CSBW  
CYBER  
SICHERHEITS  
AGENTUR  
BADEN-WÜRTTEMBERG

- 1 Sicherheitslücken schließen
- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen
- 5 Netzübergänge absichern**
- 6 Schadprogramme abwehren
- 7 Notfallplan erstellen
- 8 Inventarisieren und dokumentieren

# 5 Netzübergänge absichern

## ARGUMENTE:

Eine Firewall ist unverzichtbar. Ohne einen solchen Schutz sind Unternehmen völlig ungeschützt vor unerwünschten Zugriffen von außen.

Auch ohne besondere IT-Kenntnisse kann eine auf dem Arbeitsplatzrechner vorinstallierte Firewall aktiviert werden. Grundsätzlich sollte eine Firewall zentral konfiguriert werden. Dies ist bereits eine erste Schutzstufe gegen Angriffe. Die Verbindung von IT-Anwendungen mit dem Internet birgt eine Reihe von Risiken, dazu gehören Angriffe mit Ransomware, Datenexfiltration und Identitätsdiebstahl.

## WEITERFÜHRENDE INFORMATIONEN:



### FIREWALL

Eine lokale Firewall (entweder im Betriebssystem integriert oder als Softwarelösung eines Drittanbieters) sollte auf allen Arbeitsplatzrechnern installiert werden.

Darüber hinaus sollten auch kleine und mittlere Unternehmen vorrangig zentrale Firewalls (also spezielle Hardware) einsetzen, um die Verbindung zwischen Informationssystem und Internet zu schützen.

*BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 18, Frage 8*  
<https://sl.csc-kmu.de/b5-01.html>



### NETZÜBERGÄNGE IDENTIFIZIEREN UND SEGMENTIEREN

Verwenden Sie keine Gruppenaccounts, sondern für alle Beschäftigten ein eigenes Nutzerkonto. Normale Nutzende dürfen nicht über Administratorrechte verfügen.

Für das Navigieren im Internet dürfen nur eigene Benutzerkonten ohne Administratorrechte genutzt werden.

Dienstliche Computer sollten ausschließlich für die berufliche Arbeit genutzt werden.

*BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 20-21, Frage 10*  
<https://sl.csc-kmu.de/b5-02.html>



*CSBW-Factsheet: Netzkopplung und Fernzugriffe*  
<https://sl.csc-kmu.de/b5-03.html>

## FALLBEISPIEL

Ein Planungsbüro mit fünf Mitarbeitenden hatte in einem Router eine Portweiterleitung auf den Fileserver eingerichtet, damit die Mitarbeitenden von extern zugreifen können. Eine Firewall war nicht vorhanden. Der Angriff erfolgte mit einem Verschlüsselungstrojaner. Da im Router ein Port offen war, konnten Angreifende auf den ungeschützten Fileserver zugreifen und alle Dateien verschlüsseln.

## FOLGEN

Der Fileserver konnte mehrere Tage nicht genutzt werden. Die Daten konnten größtenteils über ein Backup wiederhergestellt werden.



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 6

## Schadprogramme abwehren

### MAKROS DEAKTIVIEREN

Verwenden Sie für Dokumente aus externen Quellen eine sichere Darstellungsoption, insbesondere bei E-Mails oder Downloads aus dem Internet. Deaktivieren Sie daher Makros und andere aktive Elemente, die in Ihrer Office-Anwendung nicht benötigt werden.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



Hochschule Aalen



### VIRENSCHUTZPROGRAMME VERWENDEN

Installieren Sie auf allen Geräten zentral verwaltete Virenschutzprogramme und halten Sie diese stets aktuell. Ein mehrstufiger Virenschutz ist sinnvoll.

Dies gilt vor allem bei Homeoffice-Lösungen und Systemen, die mit dem Internet verbunden sind.

Prüfen Sie, ob weitere Sicherheitssysteme erforderlich sind, um Ihre IT-Systeme nach außen zu schützen, z. B. Antiviren-Software auf E-Mail-Servern.

### KOMMUNIKATIONSWEGE ABSICHERN

Nutzen Sie Filter gegen Spam- und Phishing-E-Mails sowie gegen E-Mails mit Links zu schädlichen Webseiten oder mit schädlichen Dateianhängen.

Konfigurieren Sie Ihre E-Mail-Anwendung so, dass:

- E-Mails von extern als solche speziell gekennzeichnet werden, z. B. durch die Voranstellung von „Extern“.
- die E-Mail-Adresse angezeigt wird und nicht der E-Mail-Alias (z. B. max.mustermann@email.de, anstatt „Max Mustermann“).

Für die Abwehr von Angriffen über E-Mails und insbesondere E-Mail-Anhänge ist eine zentrale Untersuchung des eingehenden E-Mail-Verkehrs auf Schadprogramme erforderlich.

Sichern Sie auch andere Kommunikationsplattformen ab, z. B. Videochat.

- 1 Sicherheitslücken schließen
- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen
- 5 Netzübergänge absichern
- 6 Schadprogramme abwehren**
- 7 Notfallplan erstellen
- 8 Inventarisieren und dokumentieren

# 6 Schadprogramme abwehren

## ARGUMENTE:

Eines der Haupteinfallstore für Ransomware sind Makros, die sich in Dateianhängen von E-Mails verbergen. Hierbei sind Virenschutzprogramme sehr hilfreich. In vielen Fällen können sie eine Schadsoftware abwehren und einen Angriff mit Ransomware verhindern. Jeden Tag erscheinen hunderttausende neue Schadcodevarianten. Daher müssen die Software selbst und ihre Erkennungsdatenbank immer auf dem neuesten Stand gehalten werden. Phishing per E-Mail ist ebenfalls ein zentraler Angriffsvektor. Insbesondere von gut gemachten Phishing-E-Mails lässt man sich leicht in die Irre führen.

## WEITERFÜHRENDE INFORMATIONEN:



### MAKROS DEAKTIVIEREN

Überlassen Sie die Entscheidung, ob ein Makro ausgeführt werden darf oder nicht keinesfalls den Beschäftigten – denn diese haben oft nicht die erforderlichen Kenntnisse, um so eine Entscheidung treffen zu können.

*BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 14, Frage 5*  
<https://sl.csc-kmu.de/b6-01.html>



Konfiguration von Microsoft Access, Excel, PowerPoint, Word und Outlook.

*BSI – Sichere Konfiguration von Microsoft Office 2013/2016/2019 v1.2*  
<https://sl.csc-kmu.de/b6-02.html>



### VIRENSCHUTZPROGRAMME

Die im Handel erhältlichen (teilweise im Betriebssystem bereits enthaltenen) Virenschutzprogramme bieten automatische Updates und Speicherplatzüberprüfung. Diese Einstellungen müssen unbedingt aktiviert werden.

*BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 15, Frage 6*  
<https://sl.csc-kmu.de/b6-03.html>



### ABSICHERN VON VIDEOKONFERENZEN

Sind nur die autorisierten Personen Teil der Videokonferenz? Hinter einer ausgeschalteten Kamera kann auch ein Angreifer stecken, der mithören will. Die beliebten Screenshots von Videokonferenzen können wertvolle Informationen für Angriffe enthalten. Im Falle einer Veröffentlichung sollten sensible Daten wie URLs, Meeting-IDs sowie Namen und Gesichter unkenntlich gemacht werden.

*CSBW-Factsheet zu Videokonferenzen*  
<https://sl.csc-kmu.de/b6-04.html>

## FALLBEISPIEL

Die Mitarbeiterin eines Handelsunternehmens erhält eine gefälschte E-Mail eines vermeintlichen Kunden. Sie öffnet einen als Bestellung deklarierten Anhang, der Malware (Schadsoftware) enthält. Da Makros nicht deaktiviert sind, wird dadurch automatisch ein Verschlüsselungstrojaner installiert, der die Daten verschlüsselt.

## FOLGEN

Der Geschäftsbetrieb ist nicht mehr möglich. Ein Backup ist auf einer externen Festplatte vorhanden, so dass der Datenverlust nur gering ist. Das System muss dennoch neu aufgesetzt werden.



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 7

## Notfallplan erstellen

### VERANTWORTLICHKEITEN FESTLEGEN

Ihre Planung muss folgende Aspekte umfassen: Definition der technischen und organisatorischen Rollen, Klärung von Verantwortlichkeiten jedes Einzelnen, Festlegung von Zuständigkeiten und die Einbeziehung externer Dienstleister.

Bestimmen Sie Beauftragte für die in einem Notfall erforderlichen Aufgabenbereiche (Notfallteam). Eine Konzentration vieler Zuständigkeiten in einer Rolle ist zu vermeiden.

### NOTFALLPLAN ERSTELLEN

Fertigen Sie eine Liste mit allen Ansprechpersonen an und treffen Sie Vorabsprachen mit diesen. Ein Kommunikationsplan sollte auch Handynummern eines Notfallteams und beispielsweise eine eigene Notfall-E-Mail-Erreichbarkeit enthalten, da betriebliche Festnetztelefone und E-Mail-Konten bei Cyberangriffen oft auch betroffen und nicht funktionsfähig sind. Denken Sie außerdem an Kundenadressen.

Erstellen Sie einen Notfallplan (Vorfallreaktionsplan), der auflistet, was in der jeweiligen Situation zu tun ist, um so schnell wie möglich wieder handlungsfähig zu sein. Der Notfallplan sollte Kontaktdaten von zu informierenden externen Stellen und bestehende Meldepflichten enthalten (z. B. § 33 DSGVO – möglichst binnen 72 Std.).

Dokumentieren Sie Leitlinien, Rollen und Zuständigkeiten für eine zeitnahe, professionelle und angemessene Reaktion auf alle Sicherheitsvorfälle.

### ÜBEN UND BEREITHALTEN

Halten Sie den Notfallplan und die Kommunikationslisten physisch (ausgedruckt) bereit, damit diese den Beschäftigten auch bei einem IT-Ausfall zur Verfügung stehen.

Führen Sie regelmäßig Übungen durch, damit Sie im Ernstfall schnell und richtig reagieren können.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



Hochschule Aalen



- 1 Sicherheitslücken schließen
- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen
- 5 Netzübergänge absichern
- 6 Schadprogramme abwehren
- 7 Notfallplan erstellen**
- 8 Inventarisieren und dokumentieren

### ARGUMENTE:

Ein professioneller Notfallplan ist Führungsaufgabe und darf in keinem Betrieb fehlen. Er ist auch ein Argument gegenüber Versicherungen und Behörden. Durch ein gutes Notfall- und Krisenmanagement können die Auswirkungen eines Sicherheitsvorfalls erheblich reduziert werden.

### HINWEIS:

Erstatten Sie bei einem IT-Sicherheitsvorfall Strafanzeige bei der Polizei oder wenden Sie sich direkt an die inzwischen bundesweit eingerichteten Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC). Gute Gründe für eine Kontaktaufnahme und Adressen finden Sie hier.



Allianz für Cybersicherheit – Zusammenarbeit mit der Polizei  
<https://sl.csc-kmu.de/b7-06.html>

#### NOTFALLNUMMER

ZENTRALE ANSPRECHSTELLE CYBERCRIME  
(ZAC) BEIM LKA BADEN-WÜRTTEMBERG

TEL.: 0711 5401-2444

### WEITERFÜHRENDE INFORMATIONEN:



Einstieg ins IT-Notfallmanagement für kleinere und mittlere Unternehmen (KMU).

BSI – Maßnahmenkatalog zum Notfallmanagement –  
Fokus IT-Notfälle

<https://sl.csc-kmu.de/b7-01.html>



Verhalten bei IT-Notfällen

BSI- IT-Notfallkarte „Verhalten bei IT-Notfällen“

<https://sl.csc-kmu.de/b7-02.html>



TOP 12 Maßnahmen bei Cyberangriffen

BSI – Top 12 Maßnahmen bei Cyberangriffen

<https://sl.csc-kmu.de/b7-03.html>



Erste Hilfe bei einem Cybernotfall

CSBW – Factsheet Erste Hilfe bei einem Cybernotfall

<https://sl.csc-kmu.de/b7-04.html>



Informationssicherheitsvorfall erkennen

CSBW-Factsheet: Informationssicherheits-  
vorfall erkennen

<https://sl.csc-kmu.de/b7-05.html>

### FALLBEISPIEL

Ein Unternehmen hatte erkannt, dass für den Fall eines Angriffs auf seine IT-Systeme ein Notfallplan erforderlich ist. Es wurde ein Plan erstellt, der Kommunikationslisten, Meldepflichten und Checklisten enthielt. Dort waren auch Hinweise hinterlegt, was in der jeweiligen Situation zu tun ist, um möglichst schnell wieder handlungsfähig zu werden. Der Notfallplan war für alle Mitarbeitenden zugänglich im Firmennetz abgelegt. Als das Unternehmen tatsächlich von einem Cyberangriff betroffen und das Firmennetz lahmgelegt war, stellte man fest, dass man den Notfallplan physisch (Notfallordner) nicht vorgehalten hatte.

### FOLGEN

Da man auf den Notfallplan nicht zurückgreifen konnte, entstanden erhebliche Zeitverluste und Aufwände bei der Veranlassung und Durchführung der erforderlichen Maßnahmen.



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# 8

## Inventarisieren und Dokumentieren

### VOLLSTÄNDIGE INVENTARISIERUNG DER EINGESETZTEN IT-SYSTEME

Dokumentieren Sie alle verwendeten Hardwarekomponenten.

Dokumentieren Sie alle eingesetzte Software.

Dokumentieren Sie alle für den Geschäftsbetrieb wichtigen Daten, einschließlich deren Speicherort.

Dokumentieren Sie alle Zugriffsrechte.

Dokumentieren Sie alle IT-Verbindungen mit der Außenwelt.

Klären Sie anhand der Inventarisierung die Frage, ob die erhobene Vielfalt an Systemen sicherheitstechnisch und administrativ beherrschbar ist.

Erstellen Sie einen Netzwerkplan.

Halten Sie die oben genannten Dokumentationen und den Netzwerkplan stets auf dem aktuellen Stand und als physische Kopie (Ausdruck) vor.



Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



- 1 Sicherheitslücken schließen
- 2 Benutzerzugänge absichern
- 3 Datensicherung durchführen
- 4 Gefahrenbewusstsein schaffen
- 5 Netzübergänge absichern
- 6 Schadprogramme abwehren
- 7 Notfallplan erstellen

**8 Inventarisieren und dokumentieren**

# 8 Inventarisieren und Dokumentieren

## ARGUMENTE:

Um sich adäquat zu schützen, muss jedes Unternehmen seine Hard- und Software sowie die Daten und die Verarbeitungsprozesse inventarisieren, welche die Grundlage seiner Informationswerte bilden und zum Fortbestand des Unternehmens beitragen.

Außerdem sind eine Inventarisierung und ein Netzplan für Fachleute (z. B. aus der Forensik) sehr nützlich, die im Falle einer Cyberattacke Maßnahmen zum Erhalt der eigenen IT-Systeme einleiten sollen.

## EINSTIEGSEMPFEHLUNGEN

Als Einstieg in die Inventarisierung bietet sich das folgende Vorgehen an:

1. IT-Geräteliste (Assetliste)
2. Schematischer Netzwerkplan
3. Anwendungsliste  
(»Bauanleitung« um die Infrastruktur wiederherzustellen)

Minimum: Inventarisieren der IT-Geräte und Erstellen einer Anwendungsliste anhand folgender Leitfragen:

- Welche IT-Geräte sind vorhanden?
- Wie kritisch sind die Geräte für einen reibungslosen Geschäftsbetrieb?
- Wie lange kann der Geschäftsbetrieb ohne die jeweiligen Daten und Geräte aufrecht erhalten werden?

## WEITERFÜHRENDE INFORMATIONEN:



Netzplan erheben

*BSI – Online-Kurs IT Grundschutz – Lerneinheit 3.5*

<https://sl.csc-kmu.de/b8-01.html>



*CSBW – Prüfdokument für IT-Sicherheitsarchitekturen*

<https://sl.csc-kmu.de/b8-02.html>

## FALLBEISPIEL

Ein von einem Cyberangriff betroffenes Unternehmen hatte nur eine rudimentäre Inventarisierung und Dokumentation seiner IT-Landschaft. Software und Zugriffsrechte waren nicht dokumentiert.

## FOLGEN

Die eingeschalteten Forensiker hatten große Schwierigkeiten, möglichst schnell die richtigen Gegenmaßnahmen einzuleiten. Die Gegenmaßnahmen und die Wiederherstellung der Systeme wurden sehr zeitaufwändig und teuer.



**NOTFALLKONTAKT  
CYBER-ERSTHILFE BW:**

**0711-137-99999**

# WEITERE THEMEN

## HOMEOFFICE UND MOBILES ARBEITEN

### ORGANISATORISCHES

Legen Sie die Verhaltensregeln für Homeoffice und mobiles Arbeiten verbindlich fest, z. B. in der IT-Sicherheitsrichtlinie (siehe Karte: Cybersicherheit ist Führungsaufgabe).

Regeln Sie den Umgang mit betrieblichen Dateien und Dokumenten außerhalb des Firmengeländes.

Verschlüsseln Sie alle Geräte und Datenträger, die für den mobilen Einsatz vorgesehen sind (Laptops, Smartphones, Tablets, Wechselfestplatten, USB-Sticks etc.).

Planen Sie Vorkehrungen und Prozesse für den Verlust oder den Ausfall mobiler Geräte ein. Geräte sollten aus der Ferne gesperrt und gelöscht werden können. Halten Sie Ersatzgeräte bereit.

Stellen Sie sicher, dass der Zugriff auf das Unternehmensnetzwerk von außen nur über gesicherte Verbindungen möglich ist, z. B. VPN (siehe Basismaßnahme 5).

### WEITERFÜHRENDE INFORMATIONEN:

 *CSBW-Factsheet zu Homeoffice*  
<https://sl.csc-kmu.de/zk-01.html>

 *CSBW-Factsheet zu Clean Desk  
und Clean Desktop*  
<https://sl.csc-kmu.de/zk-02.html>

 *CSBW-Factsheet zur optimalen  
Konfiguration des Home-Routers*  
<https://sl.csc-kmu.de/zk-03.html>

### VERHALTENSREGELN

Sperren Sie Geräte wie PCs oder Bedien-  
displays beim Verlassen des Arbeitsplatzes.  
Aktivieren Sie die automatische Sperrung  
auf allen Geräten.

Lassen Sie sensible Dokumente nicht unbe-  
aufsichtigt liegen. Lassen Sie Laptops und  
Smartphones nie unbeaufsichtigt.

Bewahren Sie vertrauliche Dokumente und  
Datenträger in einem verschließbaren Be-  
hältnis (z. B. Rollcontainer, Aktenschrank)  
auf.

Stellen Sie sicher, dass dienstliche Geräte  
ausschließlich von den berechtigten Perso-  
nen genutzt werden.

Übertragen Sie im mobilen Einsatz entstan-  
dene Daten (Fotos etc.) zeitnah an Daten-  
speicher des Unternehmens, um Datenver-  
luste zu vermeiden.

Verwenden Sie eine Sichtschutzfolie für  
Displays, wenn Sie in öffentlichen Räumen  
arbeiten.

Verwenden Sie niemals USB-Sticks, die Sie  
geschenkt bekommen.

Untersagen Sie den Anschluss von Geräten  
Dritter an Ihre eigenen Geräte (USB-Sticks,  
Presenter, USB-Ladekabel etc.).

Achten Sie bei der Nutzung eines fremden  
Computers darauf, dass dort keine Zugangs-  
daten von Ihnen gespeichert werden.



## **PHYSISCHE IT-SICHERHEIT**

---

Richten Sie Zugangskontrollen für Server-Räume, Schaltschränke etc. ein.



Löschen Sie Datenträger vor der Ausmusterung auf sichere Art und Weise. Beachten Sie hierzu die Hinweise des BSI: <https://sl.csc-kmu.de/zk-04.html>

Vernichten Sie Unterlagen und Datenträger mit vertraulichen oder personenbezogenen Inhalten nach deren Nutzung und auf die vorgeschriebene Art und Weise.

Lassen Sie Service-Personal nie unbeaufsichtigt in die Firmenräume.

Bewahren Sie Ausdrucke von wichtigen Dokumenten an einem sicheren Ort auf (z. B. Zugangsdaten, Service-Verträge, Kontaktdaten von Dienstleistern).

## **CLOUDBASIERTE LÖSUNGEN**

---

Für die sichere Nutzung von Cloud-Diensten gelten dieselben Empfehlungen wie für die Absicherung der lokalen IT-Infrastruktur.

Planen Sie den Weg in die Cloud sorgfältig. Bedenken Sie von Anfang an auch den Weg aus der Cloud heraus, um nicht zu stark von einem Cloud-Anbieter abhängig zu werden.

Machen Sie sich mit den Risiken vertraut, die die Nutzung von Cloud-Computing mit sich bringt.

Erstellen Sie eine Cloud-Strategie. Diese muss die Ziele enthalten, die mittels Cloud-Computing erreicht werden sollen.



Beachten Sie die Hinweise des BSI zum Thema „Sichere Nutzung von Cloud-Diensten“.

<https://sl.csc-kmu.de/zk-05.html>

## **CYBERVERSICHERUNGEN**

---

Entwickeln Sie ein Risikobewusstsein für Cyberangriffe und bewerten Sie dieses für Ihr Unternehmen. Prüfen Sie ob und in welchem Umfang eine Versicherung hilfreich und notwendig ist.

Prüfen Sie, ob sich die jeweiligen Versicherungsklauseln in herkömmliche Versicherungsverträge aufnehmen lassen oder ob eine spezielle Cyber-Versicherungspolice infrage kommt.

Beachten Sie, dass Sie nach Abschluss einer solchen Versicherung stets für die Einhaltung der vertraglich vereinbarten Voraussetzungen Sorge tragen müssen, um den vollständigen Versicherungsschutz nicht zu verlieren.

# CHECKLISTE

## 1

### Sicherheitslücken schließen

JA NEIN k. A.

- |  |                          |                          |                          |
|--|--------------------------|--------------------------|--------------------------|
| 1.1 Haben Sie einen vollständigen Überblick über alle im Unternehmen eingesetzte Software?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 Existiert für das Einspielen von Softwareaktualisierungen (Updates und Patches) ein definierter Prozess?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3 Wird dieser Prozess überwacht (z. B. manuell oder über automatische Benachrichtigungen, die Auskunft über Erfolg/Misserfolg der Maßnahme geben)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4 Ist sichergestellt, dass Softwareaktualisierungen schnellstmöglich nach der Veröffentlichung eingespielt werden?                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5 Sind Quellen definiert, von denen Sie regelmäßig über neue Sicherheitslücken für die eingesetzten IT-Systeme und Anwendungen informiert werden?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

## 2

### Benutzerzugänge absichern

- |   |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|
| 2.1 Existiert für Ihre Mitarbeitenden eine definierte, einzuhaltende Passwortrichtlinie, die Vorgaben zu Länge und Komplexität enthält?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2 Werden besonders kritische Konten/Zugänge (z. B. solche mit weitreichenden Berechtigungen, Fernzugänge u. a.) zusätzlich mit einer Zwei-Faktor-Authentisierung (2FA) abgesichert? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 Sind die Mitarbeitenden sensibilisiert, Passwörter geheim zu halten?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4 Existiert eine Zugangssicherung (Passwort, 2FA) für mobile Endgeräte, die auf das Firmennetzwerk zugreifen können?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |



# 3

## Datensicherung durchführen

---

JA NEIN k. A.

- |  |                          |                          |                          |
|--|--------------------------|--------------------------|--------------------------|
| 3.1 Verfügen Sie über eine Datensicherung (Backup) der geschäftskritischen Daten?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2 Werden Ihre geschäftskritischen Daten auf mehreren unterschiedlichen Speichermedien gesichert?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3 Ist mindestens ein Backup physisch vom Netzwerk getrennt, z. B. über Tapes oder Festplatten, die isoliert gelagert werden oder durch Sicherung in einem externen Rechenzentrum oder einer Cloud? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4 Werden die Funktionsfähigkeit des Backups bzw. der Wiederherstellungsprozess regelmäßig überprüft und geübt?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5 Ist der Turnus des Backups an die Verarbeitung von geschäftskritischen Daten angepasst (zeitlicher Abstand bzw. Häufigkeit und Umfang der Sicherung)?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

# 4

## Gefahrenbewusstsein schaffen

---

- |   |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|
| 4.1 Ist sichergestellt, dass Sie zeitnah über die aktuellen Gefahren und gängigen Arten von Cyberangriffen informiert werden? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2 Sind Ihnen und Ihren Mitarbeitenden die aktuellen und gängigen Vorgehensweisen von Cyberkriminellen bekannt?              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3 Finden regelmäßig Sensibilisierungen zum Thema Cybersicherheit statt, z. B. durch Schulung der Mitarbeitenden?            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

# 5

## Netzübergänge absichern

JA NEIN k. A.

- |  |                          |                          |                          |
|--|--------------------------|--------------------------|--------------------------|
| 5.1 Verfügen Sie an den Übergängen ins Internet über eine dedizierte Firewall und ist diese so konfiguriert, dass nur bestimmte und erwünschte Verbindungen aufgebaut werden können? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2 Sind besonders kritische IT-Systeme vom restlichen Netz getrennt (wichtig vor allem für Backup oder Produktionsnetze mit veralteten Systemen)?                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3 Erfolgen Zugriffe von außen auf Ihr System ausschließlich über gesicherte Zugänge, z. B. VPN?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4 Gibt es eine Übersicht aller Zugänge von extern auf Ihr Unternehmensnetzwerk inklusive deren Berechtigungen?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

# 6

## Schadprogramme abwehren

- |  |                          |                          |                          |
|--|--------------------------|--------------------------|--------------------------|
| 6.1 Haben Sie die Ausführung von Makros in Ihren Office-Anwendungen technisch deaktiviert?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2 Sind Ihr E-Mail-Programm und der Server so konfiguriert, dass E-Mails von externen E-Mail-Konten explizit gekennzeichnet werden?                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3 Ist Ihr E-Mail-Programm so konfiguriert, dass die tatsächliche E-Mail-Adresse als Absender angezeigt wird (Wichtig: vollständige Anzeige aller Absenderinfos)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4 Nutzen Sie auf Ihren Endgeräten eine Antivirenlösung, die regelmäßig aktualisiert wird?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

# 7

## Notfallplan erstellen

JA NEIN k. A.

- |  |                          |                          |                          |
|--|--------------------------|--------------------------|--------------------------|
| 7.1 Haben Sie einen Notfallplan für IT-sicherheitsrelevante Ereignisse?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2 Wird eine Notfallübung regelmäßig durchgeführt?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3 Enthält der Notfallplan einen Kommunikationsplan mit internen und externen Erreichbarkeiten? (z. B. IT-Dienstleister, Polizei, Lieferanten, Kunden, LfDI, CSBW, auch Mobilnummern) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.4 Gibt es eine klar definierte Aufgabenzuweisung der wichtigsten Rollen in diesem Notfallplan?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

# 8

## Inventarisieren und dokumentieren

- |   |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|
| 8.1 Verfügen Sie über eine vollständige Übersicht Ihrer IT-Landschaft, z. B. IT-Systeme, Verbindungen zwischen Systemen, Außenverbindungen? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.2 Ist dokumentiert, welche Zugänge zu den Systemen bestehen (intern & extern)?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3 Beinhaltet die Übersicht auch alle relevanten IT-Anwendungen inklusive deren Abhängigkeiten?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.4 Werden diese Daten regelmäßig aktualisiert?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

### Zur Zitation

Diese Beratungsunterlagen zum CyberSicherheitsCheck für KMU enthalten Passagen und Inhalte aus Publikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Agentur der Europäischen Union für Cybersicherheit (ENISA). Dem Format der Beratungskarten geschuldet stehen die Quellenverweise dafür nicht direkt im Text oder in den Fußnoten. Ebenfalls wird im Rahmen der weiterführenden Links auf zahlreiche Publikationen, viele davon vom BSI verwiesen. Die Verwendung und Nennung der Quellen in dieser Form wurde vom BSI und von ENISA genehmigt. Für die Bereitstellung und die Nutzungsfreigabe der Inhalte bedanken wir uns ausdrücklich.

### Quellen

BSI. (2018). *Basismaßnahmen der Cyber-Sicherheit*. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). [https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS\\_006.pdf?\\_\\_blob=publicationFile&v=1](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_006.pdf?__blob=publicationFile&v=1)

BSI. (2023). *Cyber-Sicherheit für KMU - Die TOP 14 Fragen*. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). <https://sl.csc-kmu.de/b1-01.html>

BSI. (2024). *IT-Notfallkarte „Verhalten bei IT-Notfällen“*. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI). <https://sl.csc-kmu.de/b7-02.html>

ENISA. (2021). *KMU-Leitfaden zur Cybersicherheit - 12 Schritte zur Absicherung Ihres Unternehmens*. Athen, Heraklion: Agentur der Europäischen Union für Cybersicherheit (ENISA). <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>

ENISA. (2021). *Cybersecurity for SMEs - Challenges and Recommendations*. European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>

### Website

[www.csc-kmu.de](http://www.csc-kmu.de)

## Kooperationspartner