# CHECKLISTE ZUR CYBER SECURITY

**Handlungsfelder und Links**

Der Schutz von IT-Infrastrukturen ist eine komplexe Aufgabe. Insbesondere kleinen und mittleren Einrichtungen fällt es aber oft schwer, ihre IT ausreichend vor Cyberkriminalität zu schützen, weil die Ressourcen dafür knapp sind. Mit der nachfolgenden Übersicht möchten wir Sie beim Aufbau eines wirksamen IT-Grundschutzes bestmöglich unterstützen.

Die Checkliste basiert auf den Handlungsempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und greift die wichtigsten Handlungsfelder für IT-Sicherheit auf. Diese Tipps und Hinweise können auch schon mit geringem Aufwand umgesetzt werden. Die Übersicht wurde im interaktiven PDF-Format erstellt, sodass Sie mit Klick auf den gewünschten Link direkt auf die Webseite des BSI weitergeleitet werden.

Die Checkliste zur Cyber Security ersetzt zwar kein methodisches IT-Sicherheitskonzept, unterstützt Sie aber dabei, einen Grundschutz für Ihre IT-Infrastruktur aufzubauen und diesen zu erhalten.

**Inhaltsverzeichnis**


| | |
|---|---|
| Patch-Management | 2 |
| Änderungsmanagement | 2 |
| Nutzer- und Rechtemanagement | 3 |
| Datensicherung | 3 |
| Sicherheitsbeauftragte/-r | 3 |
| Sensibilisierung und Schulung | 3 |
| Social Network | 4 |
| Fernzugriff | 4 |
| Protokollierung | 4 |
| Notfallmanagement | 4 |
| Cloud-Nutzung | 4 |


### Patch-Management

… beschäftigt sich mit der Beschaffung, dem Test und der Installation benötigter Updates für Applikationen, Treiber und Betriebssystem von Computern.

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_4_Schutz_vor_Schadprogrammen.html

»» **Virenscanner einsetzen und aktuell halten**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04226.html

»» **Schadsoftware zentral und dezentral filtern**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04083.html

»» **Betriebssystem aktuell halten**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04324.html

»» **Anwendungssoftware und Plug-ins aktuell halten**

### Änderungsmanagement

… beschäftigt sich mit dem systematischen Schutz der Informationen bei der Erneuerung/Anpassung von Hard- und Software

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_4_Auswahl_und_Einsatz_von_Standardsoftware.html

»» **Hardware und Software auswählen**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03301.html

»» **Firewall aufbauen**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05072.html

»» **nicht benötigte Dienste deaktivieren**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_4_Auswahl_und_Einsatz_von_Standardsoftware.html?nn=10137140#doc10095844bodyText14

»» **Software und Daten aus sicheren Quellen verwenden**

### Nutzer- und Rechtemanagement

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

»» **nicht mehr Berechtigungen als erforderlich vergeben**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_2_Ordnungsgem%C3%A4%C3%9Fe_IT-Administration.html

»» **nicht mit Administratorenrechten arbeiten**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

»» **sichere Passwörter verwenden**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03098.html

»» **Passwörter nicht aufschreiben und liegenlassen**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

»» **Computer vor unberechtigtem Zugriff schützen**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKatalo-ge/Inhalt/_content/m/m04/m04002.html

» **Computer bei Abwesenheit immer sperren**

### Datensicherung

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html

» **Daten und System sichern**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/CON/CON_3_Datensicherungskonzept.html?nn=10137140#doc10095836bodyText16

» **Datensicherung vor unbefugtem Zugriff schützen**

### Sicherheitsbeauftragte/-r

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/ISMS/ISMS_1_Sicherheitsmanagement.html?nn=10137156#doc10095894bodyText6

» **eine Person innerhalb oder außerhalb der Einrichtung für die IT-Sicherheit benennen**

### Sensibilisierung und Schulung

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html

» **Mitarbeitende regelmäßig schulen und Wachsamkeit erhöhen**

- regelmäßige Sicherheitsschulungen durchführen
- zweifelhafte E-Mails nicht öffnen, erst recht nicht bearbeiten oder beantworten
- sensible Informationen nicht leichtfertig preisgeben
- personenbezogene Informationen nicht laut preisgeben (beispielsweise am Empfang)
- sensible Daten nicht über oder an private E-Mail-Accounts senden

### Social Network

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_2_Personal.html

» **in Social Media-Kanälen Informationen zurückhaltend platzieren**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKatalo-ge/Inhalt/_content/g/g05/g05158.html

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKatalo-ge/Inhalt/_content/g/g05/g05042.html

» **vor Social Engineering schützen**

### Fernzugriff

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKatalo-ge/Inhalt/_content/m/m05/m05164.html

» **Fernzugriff per RDP absichern**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_2_2_Windows_Server_2012.html

### Protokollierung

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html

» **Protokolldaten von IT-Anwendungen und -Systemen zentral speichern**

### Notfallmanagement

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_4_Notfallmanagement.html

» **Informationssicherheit auch im Notfall gewährleisten**

### Cloud-Nutzung

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Zielgruppen/Grundschutz/IT-Grundschutz.html?cms_pos=1

» **Cloud-Anwendungen sicher nutzen**

Stand 16. Mai 2019



2151.01/06.19

GRB Gesellschaft
für Risiko-Beratung mbH
Ecclesiastraße 1–4
32758 Detmold
Telefon + 49 (0) 05231 603-0
Telefax + 49 (0) 05231 603-197

info@grb.de
**www.grb.de**

Ein Unternehmen
der Ecclesia Gruppe
**www.ecclesia-gruppe.de**

HiSolutions AG

Bouchéstraße 12
12435 Berlin
Telefon +49 (0) 30 533 289-0
Telefax +49 (0) 30 533 589-900

ecclesia@hisolutions.com
**www.hisolutions.com**