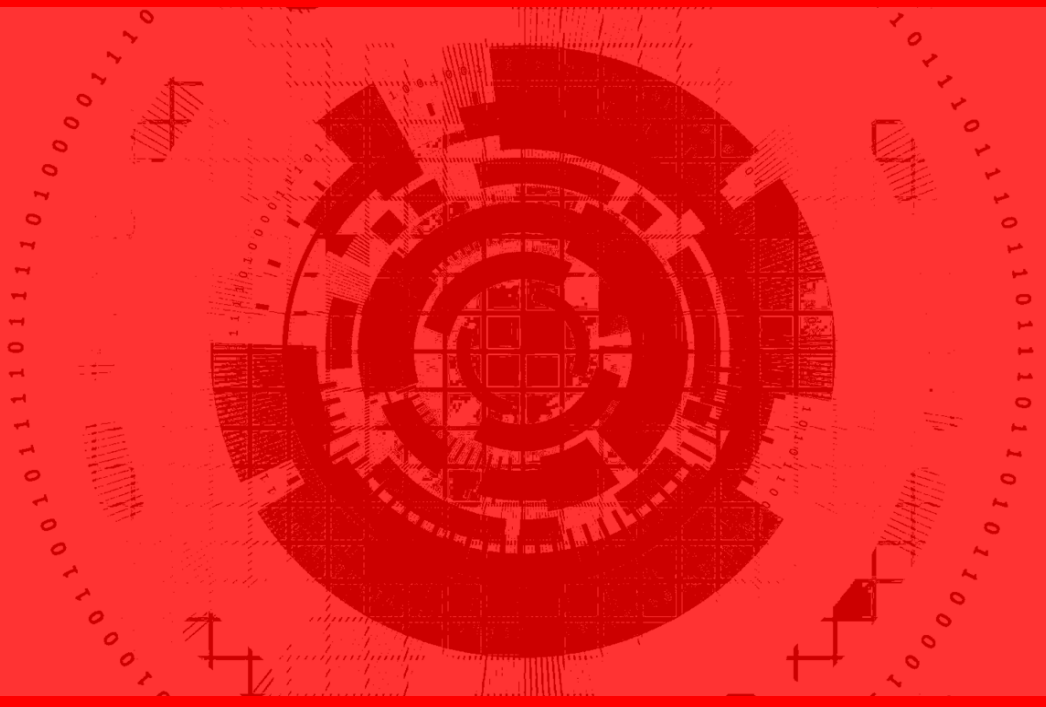
www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

6 Basics Cybersicherheit



Privathaushalte

Wie schütze ich mich im Cyberspace?

Die allermeisten Menschen verbringen viel Zeit im Internet. Sie bestellen in Online-Shops, sie buchen Reisen, sie erledigen Überweisungen oder streamen Serien. Das Internet ist selbstverständlicher Teil des Alltags geworden.

Wenn man von Cyber-Angriffen auf große Unternehmen oder Behörden hört, kann man schnell auf den Gedanken kommen, dass das Risiko für Verbraucher viel kleiner ist. Leider sind gerade Einzelpersonen einem sehr hohen Risiko ausgesetzt. Das fängt bei Schadsoftware und Spam E-Mails an und reicht bis zu Phishing-Angriffen, um Bankdaten und Passwörter abzugreifen.

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

In diesem Leitfaden stellt der Cyber-Sicherheitsrat Deutschland e.V. ihnen die wichtigsten Schritte vor.

Mit freundlichen Grüßen,

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

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

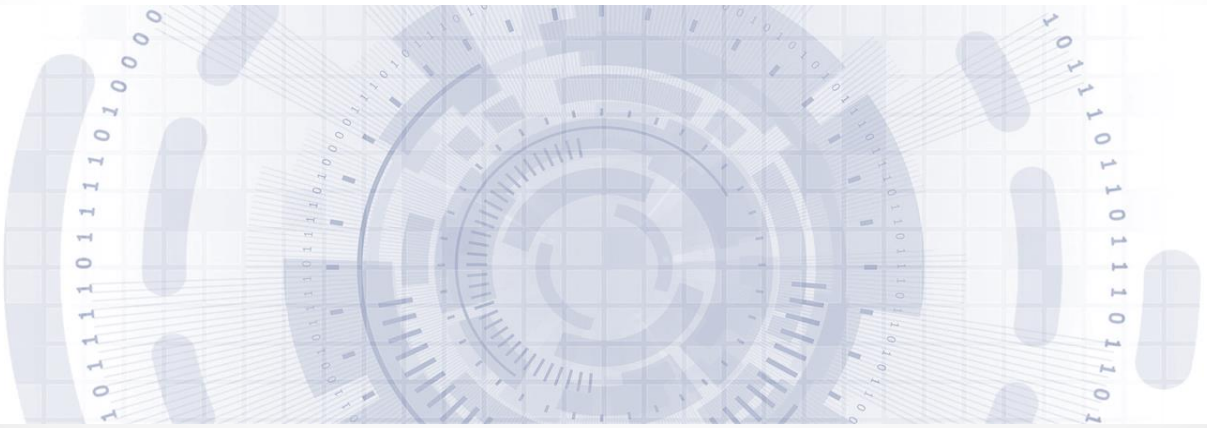
Was ist Cybersicherheit?

Unter Cybersicherheit verstehen sich alle technischen und nicht-technischen Schritte und Werkzeuge, die Hardware und Software von PCs, Servern und Netzwerken gegenüber Cyber-Kriminellen und Cyber-Angriffen schützen und das Risiko von Ausfällen und Datenverlust reduzieren.

Hauptaufgabe von Cybersicherheit ist der Schutz unserer Geräte: PCs, Laptops, Tablets und Smartphones, aber auch Smart Speaker und andere Geräte im Smart Home, wenn sie mit dem Internet verbunden sind.

Nutzer sind jederzeit unterschiedlichen Bedrohungen aus dem Cyberspace ausgesetzt: Beim Browsen im Internet oder beim Öffnen von Mail-Anhängen können sie ihren PC mit Malware infizieren, die ihre Aktivitäten ausspioniert, aber auch die Funktion des PCs unterbricht um Geld zu erpressen. Gefährlich sind auch Spam-E-Mails, die mit Angeboten locken oder mit Rechnungen drohen. Auch hier soll durch gefälschte Links oder infizierte Anhänge Schadsoftware verbreitet werden.

Der Schutz gegen diese Attacken hat mehrere Facetten. Wichtig ist ein allgemeines Bewusstsein für Sicherheit: Welche E-Mails und Webseiten wirken vertrauensvoll, welche nicht? Natürlich sind aber auch technische Instrumente nützlich und notwendig. Ein Antivirenprogramm sollte standardmäßig auf jedem PC installiert sein, jeder PC sollte passwortgeschützt sein und Betriebssysteme und Software sollten regelmäßig durch Updates sicher gehalten werden.



www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

1. Gegen Schadsoftware schützen!

Jeder mit dem Internet verbundene Computer ist ein Einfallstor für Schadsoftware. Für die Sicherheit ihrer Daten und ihrer Software ist daher ein Schutz vor diesen Programmen unabdingbar. Mit einigen wenigen Schritten sind sie gegenüber vielen Bedrohungen aus dem Netz geschützt. Wichtig ist eine funktionierende Antivirensoftware und Firewall sowie regelmäßige Software-Updates. USB-Sticks können Malware enthalten. Nutzen sie für Datentransfers also eher Filehosting-Dienste und nehmen sie keine externen Speicher an.

- ✓ **Antivirensoftware auf allen Geräten**
- ✓ **Regelmäßige Updates aller Software**
- ✓ **Filehosting-Dienste statt USB-Sticks**
- ✓ **Firewall installieren**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

2. Sichere Passwörter verwenden!

Einer der wichtigsten Grundsätze für IT-Sicherheit sind gute Passwörter. Das heißt gute und sichere Passwörter zu verwenden, die für jeden Account verschieden sind! Auf keinen Fall leicht zu erratende Passwörter wie *„passwort“* oder *„12345“* verwenden. Mit einem Passwort-Manager ist es einfacher: Das Programm speichert alle ihre Passwörter, sie müssen sich nur ein Masterpasswort merken. Für wichtige Konten sollte eine 2-Faktoren-Authentifizierung verwendet werden, etwa ein nach Passworteingabe am PC einzugebender Code vom Smartphone.

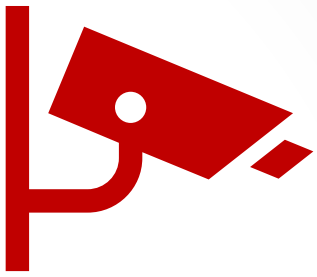
- ✓ **Sichere Passwörter**
- ✓ **Passwort-Manager**
- ✓ **Für jeden Account ein eigenes Passwort**
- ✓ **2-Faktoren-Authentifizierung**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

3. Auf Privatsphäre achten!

Jedes Mal wenn sie im Internet sind, hinterlassen sie digitale Spuren. Webseiten sammeln Informationen über ihre Besucher und können die Daten auswerten. Es ist daher wichtig im Internet auf Privatsphäre zu achten. Sie sollten ihre Daten und ihre Kommunikation verschlüsseln, informieren sie sich bei ihrem E-Mail-Anbieter über die Möglichkeiten zur End-zu-End-Verschlüsselung. Löschen sie regelmäßig den Browserverlauf und die Cookies. Geben sie über soziale Netzwerke keine sensiblen Informationen oder Daten preis.



- ✓ **Sensibilisierung für Privatsphäre**
- ✓ **End-zu-End-Verschlüsselung**
- ✓ **Browserdaten löschen**
- ✓ **Keine sensiblen Infos in Social Media**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

4. Daten sichern!

Sie speichern große Mengen an persönlichen Daten auf den Festplatten ihrer Geräte: Bilder, Nachrichten und Videos.
Eine Datensicherung ist unabdingbar, damit sie ihre Daten nicht verlieren. Wichtig ist, Daten regelmäßig zu sichern und vom PC unabhängig etwa auf externen Festplatten zu speichern. Zusätzlich sollten sie eine Datensicherung in der Cloud und eine Verschlüsselung der Daten in Erwägung ziehen. Durch Datensicherung in der Cloud läuft die Synchronisierung in der Regel automatisch.

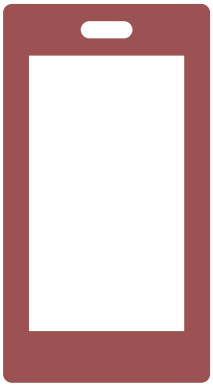
- ✓ **Datensicherung**
- ✓ **Externe Festplatten**
- ✓ **Datensicherung in der Cloud**
- ✓ **Datenverschlüsselung**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

5. Sicherheit bei Smartphones!

Um Cybersicherheit herzustellen müssen alle Geräte , die mit dem Internet verbunden sind, geschützt und gesichert werden. Besonders wichtig ist das bei Smartphones, die von einer Mehrheit der Menschen viele Stunden am Tag verwendet werden. Standardmäßig müssen alle Geräte passwortgeschützt oder durch PIN zugangsbeschränkt sein. Veraltete Apps und Software auf den Geräten ist 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.



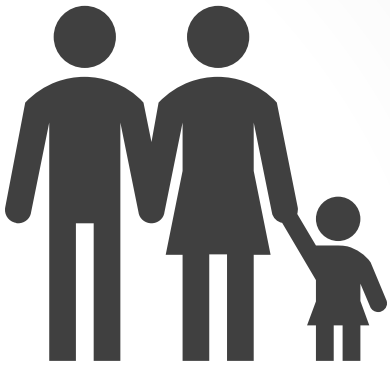
- ✓ **Sicherung aller Geräte mit PIN/Passwort**
- ✓ **Regelmäßige Updates**
- ✓ **Nicht mit ungesicherten Netzen verbinden**
- ✓ **Veraltete Software/Geräte ersetzen**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

6. Kinder im Netz schützen!

Schon ab einem sehr jungen Alter sind Kinder im Internet aktiv und mit Smartphone, Tablet oder Computer online und dabei den Gefahren des Cyberspace ausgesetzt: Von Programmen und Apps geht neben einem finanziellen auch ein Cybersicherheitsrisiko aus. Geräte von Kindern sollten daher möglichst im Kindersicherungsmodus betrieben werden. Möglichkeiten zum Kauf von Apps sollten ausgestellt werden. Eine Gefahr geht auch von Cyber-Grooming aus: Erwachsene kontaktieren Kinder über das Internet, kontrollieren Sie also deren Kommunikation. Posten sie außerdem niemals Bilder ihrer Kinder in den sozialen Medien. Schon ab einem jungen Alter sollten Kinder im Umgang mit Medien trainiert werden um ein Bewusstsein für Risiken zu entwickeln.



- ✓ **Geräte mit Kindersicherung**
- ✓ **Keine Kinderbilder in Social Media**
- ✓ **Kommunikation kontrollieren**
- ✓ **Medientraining**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

Cybersicherheit
auf einen Blick

1 Gegen Schadsoftware schützen!

- ✓ Antivirensoftware
- ✓ Regelmäßige Updates
- ✓ File-Hosting statt USB-Sticks
- ✓ Firewall installieren

2 Sichere Passwörter verwenden!

- ✓ Gute/Sichere Passwörter
- ✓ Passwort-Manager
- ✓ Ein Passwort pro Account
- ✓ 2-Faktor Authentifizierung

3 Auf Privatsphäre achten!

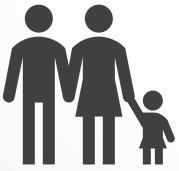
- ✓ Sensibilisierung für Privatsphäre
- ✓ Ende-zu-Ende Verschlüsselung
- ✓ Browserdaten löschen
- ✓ Keine persönlichen Daten in Social Media

4 Daten sichern!

- ✓ Datensicherung
- ✓ Externe Festplatten
- ✓ Datensicherung in der Cloud
- ✓ Datenverschlüsselung

5 Sicherheit bei Smartphones!

- ✓ Alle Geräte mit PIN/Passwort
- ✓ Regelmäßige Updates
- ✓ Keine öffentlichen Netze
- ✓ Veraltete Software/Hardware ersetzen



6 Kinder im Netz schützen!

- ✓ Geräte mit Kindersicherung
- ✓ Keine Kinderbilder in Social Media
- ✓ Kommunikation kontrollieren
- ✓ Medientraining

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

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.