Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

HISCOX

Checkliste
10 Tipps für mehr Cyber-Sicherheit

In der heutigen digital vernetzten Welt ist Cyber-Sicherheit nicht mehr nur eine Option, sondern eine Notwendigkeit für Freelancer, Selbstständige und Unternehmen jeder Größe. Die Bedrohungen durch Cyber-Angriffe entwickeln sich ständig und in raschem Tempo weiter. Deshalb ist es wichtig ist, dass Sie sich und Ihr Business schützen. In dieser Checkliste bieten wir Ihnen 10 essenzielle Tipps, um Ihre Cyber-Sicherheit zu stärken und die Risiken für Ihr Business zu minimieren.

1. Patchen (Sicherheitslücken schließen) – und zwar regelmäßig

Eine Sicherheitslücke ist ein Softwarefehler, durch den Kriminelle in Ihr Computersystem eindringen können. Diese kann durch Programmierfehler im Betriebssystem, Internetbrowser oder anderen Softwareanwendungen entstehen. Um diese Lücken zu schließen oder Verbesserungen zu integrieren, bieten Hersteller sog. Patches (von Englisch „to patch“, übersetzt „flicken“) an. Sicherheitslücken in Software können Angreifern den Zugang zu Ihren Systemen ermöglichen. Regelmäßige Updates und Patches sind daher essenziell, um bekannte Schwachstellen zu schließen.

Checken Sie konkret:

- ☐ Sind **Betriebssysteme, Browser und Anwendungen** auf allen Geräten aktuell?
- ☐ Werden **Patches und Sicherheitsupdates** regelmäßig und zeitnah eingespielt?
- ☐ Sind die **Patchdays** der Software-Anbieter bekannt und im Kalender vermerkt?
- ☐ Gibt es einen strukturierten **Patchmanagement-Prozess** im Unternehmen?
- ☐ Werden auch **kritische Updates (Fixes)** außerhalb der regulären Update-Zyklen berücksichtigt?

2. Firewalls und Virenscanner verwenden

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von über 300.000 neuen Varianten von Malware und über 20.000 infizierten Systemen in Deutschland pro Tag. Firewalls und aktuelle Virenscanner sind eine zentrale Grundlage, um Ihr IT-System vor Angriffen zu schützen.

Checken Sie konkret:

- ☐ Ist auf allen Geräten ein **tagesaktueller Virenscanner** installiert und aktiv?
- ☐ Werden **Virensignaturen und Updates** regelmäßig und automatisch eingespielt?
- ☐ Ist eine **Firewall** eingerichtet, die den Datenverkehr zwischen **internem und externem Netzwerk** kontrolliert?
- ☐ Werden **ein- und ausgehende Daten** über die Firewall überprüft?
- ☐ Ist das **Netzwerk** so aufgebaut, dass nicht jeder Bereich frei erreichbar ist?

3. Sichere Passwörter und Multi-Faktor-Authentifizierung einrichten

Unsichere Passwörter gehören zu den häufigsten Einfallstoren für Cyber-Angriffe. Schützen Sie Ihre Zugänge daher mit starken Passwörtern und zusätzlicher Authentifizierung.

Checken Sie konkret:

- ☐ Werden **sichere, individuelle Passwörter** für jedes Konto und System verwendet?

- ☐ Entsprechen Passwörter den **gängigen Anforderungen**
  - lang oder komplex,
  - mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen,
  - keine Wörterbuchbegriffe?
- ☐ Gibt es im Unternehmen eine **verbindliche Passwortrichtlinie**?
- ☐ Ist für wichtige Systeme eine **Multi-Faktor-Authentifizierung (MFA)** aktiviert?
- ☐ Werden Passwörter bei **Sicherheitsvorfällen oder Verdacht** konsequent geändert?

4. Zugriffsrechte einschränken

Je mehr Personen und Systeme Zugriff auf Ihre IT haben, desto größer ist die Angriffsfläche. Ziel ist es, Zugriffe gezielt zu begrenzen und Systeme so voneinander zu trennen, dass sich ein Angriff nicht ungehindert ausbreiten kann.

Checken Sie konkret:

- ☐ Hat jeder Nutzer nur die Zugriffsrechte, die er / sie wirklich benötigt (**Least-Privilege-Prinzip**)?
- ☐ Sind **Fernzugriffe** klar geregelt und technisch abgesichert?
- ☐ Werden **Zugriffsrechte** regelmäßig überprüft und angepasst?
- ☐ Sind **IT-Systeme netzwerksegmentiert** und nicht unnötig miteinander verbunden?
- ☐ Können im Ernstfall einzelne **Systeme isoliert** werden?

5. Sicherheitskopien erstellen

Ransomware-Angriffe zielen darauf ab, Ihre Daten zu verschlüsseln und Lösegeld zu erpressen. Regelmäßige, gut geschützte Backups helfen, handlungsfähig zu bleiben und Erpressungen zu vermeiden.

Checken Sie konkret:

- ☐ Werden **regelmäßig Backups** aller wichtigen Daten erstellt?
- ☐ Sind Backups auf einem **separierten System** mit eigener Nutzerverwaltung gespeichert?
- ☐ Ist sichergestellt, dass **kein direkter Zugriff** vom Produktivsystem auf das Backup-System möglich ist?
- ☐ Sind **Cloud-Backups** zusätzlich durch **MFA, Token oder PIN** abgesichert?
- ☐ Werden **Zugangsdaten** sicher aufbewahrt, sodass Angreifer keinen Zugriff erhalten?
- ☐ Werden Backups über einen **längeren Zeitraum** aufbewahrt, um auch spät entdeckte Angriffe abzufangen?
- ☐ Werden Backups regelmäßig auf **Funktionalität, Konsistenz und Aktualität** getestet?

6. Überwachungs- und Warnsysteme einrichten

Viele Angriffe bleiben zunächst unbemerkt, da Angreifer oft „still“ in IT-Systemen verbleiben, um möglichst viele Daten abgreifen bzw. den größtmöglichen Schaden anrichten zu können. Überwachungs- und Warnsysteme helfen, Auffälligkeiten frühzeitig zu erkennen und schneller zu reagieren.

Checken Sie konkret:

- ☐ Werden **IT-Systeme kontinuierlich überwacht**, um ungewöhnliche Aktivitäten zu erkennen?
- ☐ Gibt es **Warnmechanismen**, die bei Abweichungen oder verdächtigen Ereignissen alarmieren?
- ☐ Werden **Sicherheitsereignisse dokumentiert**, um Vorfälle nachvollziehen zu können?
- ☐ Werden **Cyber-Sicherheitswarnungen** einschlägiger Medien oder Institutionen regelmäßig verfolgt?
- ☐ Ist das **IT-System vollständig dokumentiert**, um im Schadenfall einen schnellen Wiederaufbau zu ermöglichen?

7. Ernstfall durchspielen

Ein vorbereiteter Krisenplan hilft, im Ernstfall schnell und besonnen zu handeln. Wer Abläufe vorab detailliert durchdenkt, spart im Schadenfall wertvolle Zeit.

Checken Sie konkret:

- ☐ Gibt es einen bereits **Krisenplan mit klaren Ablauf- und Sofortmaßnahmen**?
- ☐ Sind mögliche **Szenarien und aktuelle Schwachstellen** identifiziert?
- ☐ Ist festgelegt, **wer im Ernstfall technische Unterstützung** leistet?
- ☐ Ist geklärt, **wer für juristische Beratung** zuständig ist?
- ☐ Ist definiert, **wen Sie wann informieren müssen** (intern und extern)?

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

8. Umgang mit Cyber-Risiken schulen

Cyber-Angriffe zielen häufig auf den Menschen ab. Regelmäßige Schulungen helfen, Manipulationsversuche frühzeitig zu erkennen und richtig zu reagieren.

Checken Sie konkret:

- ☐ Werden Mitarbeitende **regelmäßig zu Cyber-Risiken und Angriffsmethoden** geschult?
- ☐ Ist das Thema **Social Engineering** (z. B. Phishing, gefälschte Anrufe oder E-Mails) Bestandteil der Schulungen?
- ☐ Wissen Mitarbeitende, **wie sie verdächtige Nachrichten erkennen** und melden?
- ☐ Werden Schulungsinhalte **regelmäßig aktualisiert**, um neue Angriffsmethoden abzudecken?
- ☐ Wird berücksichtigt, dass sich Cyber-Angriffe **ständig weiterentwickeln**, z. B. durch den Einsatz von KI?

9. Altsysteme im Blick behalten und gezielt absichern

Ältere oder nicht mehr unterstützte Systeme stellen ein erhöhtes Sicherheitsrisiko dar. Prüfen Sie regelmäßig, wie diese Systeme geschützt oder perspektivisch ersetzt werden können.

Checken Sie konkret:

- ☐ Sind **alle eingesetzten Altsysteme vollständig erfasst**?
- ☐ Ist bekannt, **ob diese Systeme noch Updates oder Hersteller-Support** erhalten?
- ☐ Ist klar, **welche Prozesse** von den Altsystemen abhängen und **welche Risiken** bestehen?
- ☐ Sind bestehende **Schutzmaßnahmen** (z. B. Segmentierung, Zugriffsrechte, starke Authentifizierung, Monitoring) ausreichend?
- ☐ Werden besonders kritische Altsysteme **isoliert betrieben**, falls nötig?
- ☐ Gibt es einen **realistischen Modernisierungs- oder Ablöseplan**?
- ☐ Ist der **Cyber-Versicherungsschutz** auch für Risiken aus Altsystemen geklärt?

10. Restrisiko absichern

Die genannten Tipps helfen Ihnen dabei, Ihre Cyber-Sicherheit zu stärken. Leider lässt aber auch mit umfassenden Schutzmaßnahmen ein Cyber-Angriff nicht vollständig ausschließen. Um im Ernstfall handlungsfähig zu bleiben, sollten Sie Ihr Restrisiko zusätzlich absichern. Aber Cyber-Policen unterscheiden sich inhaltlich stark voneinander, daher ist es wichtig, bei einer bestehenden Versicherung oder bei der Auswahl einer Versicherung auf bestimmte Punkte zu achten.

Checken Sie konkret:

- ☐ Ist der Versicherungsschutz genau auf die **Größe, Branche und IT-Struktur** Ihres Unternehmens abgestimmt?
- ☐ Deckt die Versicherung **typische Cyber-Schäden** ab (z. B. Datenverlust, Betriebsunterbrechung, Wiederherstellungskosten)?
- ☐ Sind **IT-Forensik und technische Soforthilfe** eingeschlossen?
- ☐ Stehen **24/7 erreichbare Experten** zur Verfügung – **auch bereits bei Verdacht**?
- ☐ Erfolgt die Unterstützung **koordiniert aus einer Hand**?
- ☐ Umfasst der Schutz **juristische Unterstützung** (z. B. bei Datenschutz- oder Haftungsfragen)?
- ☐ Sind **Krisen-Kommunikationsleistungen** (für interne & externe Ziegruppen) enthalten?
- ☐ Greift der Schutz bei **Cyber-Schäden infolge einer IT-Kompromittierung**, auch durch **menschliche Fehler** (z. B. Phishing)?
- ☐ Sind **Reaktionszeiten** und **Meldewege** klar geregelt?
- ☐ Sind auch **bestehende IT-Risiken wie Altsysteme oder Abhängigkeiten von externen Dienstleister** berücksichtigt?

Erfahren Sie hier mehr über unserer vielfach preisgekrönte Lösung Cyber Clear by Hiscox: **www.hiscox.de/cyber**

Hiscox
Bernhard-Wicki-Straße 3, 80636 München
T +49 89 54 58 01 700 **E** myhiscox@hiscox.de
W **hiscox.de/cyber**