CruSec Solutions

Anti-Hacker-Guide

www.crusecsolutions.com

Disclaimer:

Die in diesem Guide enthaltenen Informationen dienen ausschließlich allgemeinen Informationszwecken und stellen keine Rechts-, Steuer- oder verbindliche IT-Sicherheitsberatung dar. Alle Inhalte, Empfehlungen, Benchmarks und technischen Hinweise beruhen auf anerkannten Best Practices der IT-Sicherheitsbranche sowie öffentlich zugänglichen Quellen (u. a. BSI, ENISA, NIST) und wurden nach bestem Wissen zusammengestellt. Eine Garantie für Vollständigkeit, Richtigkeit oder Aktualität wird nicht übernommen.

Die Umsetzung konkreter Sicherheitsmaßnahmen sowie die Prüfung regulatorischer Anforderungen insbesondere im Rahmen der NIS-2-Richtlinie oder anderer gesetzlicher Vorgaben, hängt von der individuellen Situation Ihres Unternehmens ab und muss durch qualifizierte IT-Sicherheitsexperten, Rechtsanwälte oder Steuerberater geprüft und begleitet werden. Aussagen zu Schutzwirkungen oder Risikoreduzierungen sind praxisbezogene Einschätzungen und keine Garantien.

CruSec Solutions UG (haftungsbeschränkt) übernimmt keine Haftung für Schäden, die durch die Umsetzung oder Nicht-Umsetzung der in diesem Guide enthaltenen Empfehlungen entstehen.
Dies gilt insbesondere für Schäden durch Cyberangriffe, Datenverluste, Betriebsunterbrechungen oder Bußgelder infolge von Compliance-Verstößen.
Dieser Guide ersetzt keine individuelle Beratung. Für eine auf Ihr Unternehmen zugeschnittene Sicherheitsstrategie empfehlen wir ein persönliches Erstgespräch.

Warum IT-Sicherheit jetzt kritisch ist

90% aller Cyberangriffe starten mit **Phishing-E-Mails.**

Jedes 2. Unternehmen in Deutschland war bereits Opfer eines Cyberangriffs.

Durchschnittlicher **Schaden** eines Ransomware-Angriffs: **> 200.000 €.**

Mitarbeiter verursachen 60–70% der **Sicherheitsvorfälle** – oft unabsichtlich.

Cyberkriminelle brauchen im **Schnitt nur 9 Minuten,** um ein System zu kompromittieren.

Sicherheitsbewusste **Mitarbeiter reduzieren** das Risiko von Angriffen um bis zu **80%.**

Die 3-2-1-0 Backup Regel

3

Kopien

Mindestens 3 Kopien deiner Daten. Das Original zählt als eine davon.

2

Medien

Auf 2 verschiedenen Speichermedien: z.B. NAS + externe Festplatte.

1

Extern

Mindestens 1 Backup außerhalb des Standorts – Cloud oder Offsite.

0

Fehler

0 Fehler beim Restore! Regelmäßige Wiederherstellungstests sind Pflicht.

Ransomware verschlüsselt verbundene Laufwerke sofort – die 0-Fehler-Regel ist entscheidend!

Passwortmanager:
Schluss mit Chaos

OHNE Passwortmanager	MIT Passwortmanager
✗ Gleiche Passwörter auf mehreren Seiten	✓ Einzigartiges Passwort für jedes System
✗ Passwörter in Excel oder Post-its	✓ Verschlüsselter Tresor für alle Zugänge
✗ Zu kurze, erratbare Passwörter	✓ 32-Zeichen-Passwörter auf Knopfdruck
✗ Kein Überblick bei Mitarbeiterabgang	✓ Zugänge bei Abgang sofort entziehen
✗ Kein 2FA – ein Klick reicht Angreifern	✓ 2FA integriert – doppelte Absicherung

Empfehlenswert: Bitwarden (Business) · 1Password Teams · Keeper Enterprise

NIS-2: Was Unternehmen jetzt Wissen müssen

Was ist NIS-2?

Die NIS-2-Richtlinie (Network and Information Security) ist eine EU-weite Cybersicherheitspflicht, die seit Oktober 2024 in Deutschland gilt. Sie ersetzt NIS-1 und erfasst deutlich mehr Unternehmen.

Betroffen ab:

- ☐ 50+ Mitarbeiter ODER
- ☐ 10 Mio. € Jahresumsatz
- ☐ Kritische Sektoren: Energie, Gesundheit, Verkehr, IT, Finanzen u.v.m.

NIS-2 Pflichten auf einen Blick

Risikomanagement
Dokumentierte Risikoanalyse & Maßnahmen

Incident Response
Meldepflicht: 24h Erstmeldung, 72h Detail

Lieferkette sichern
Sicherheitsanforderungen an Lieferanten

Backup & Verschlüsselung
Gesicherte & verschlüsselte Datenspeicherung

MFA & Zugriffskontrolle
Multi-Faktor für alle kritischen Systeme

Bußgelder bis zu 10 Mio. € oder 2% des weltweiten Jahresumsatzes – Geschäftsführer haften persönlich!

Port Scanning:
Sehen, was Hacker sehen

Was ist Port Scanning?

Angreifer scannen systematisch alle offenen Ports deines Netzwerks – wie ein Einbrecher, der jede Tür und jedes Fenster prüft. Mit denselben Tools kannst auch du prüfen, was von außen sichtbar ist.

Typische Risiko-Ports

Port: 22 (SSH)	Brute Force
Port: 3389 (RDP)	Remote-Angriffe
Port: 445 (SMB)	Ransomware-Einfallstor
Port: 80/443 (HTTP/S)	Web-Exploits

So schützt du dich in 3 Schritten

01 Eigenen Scan durchführen

Tools wie Nmap oder Shodan.io zeigen, was von außen sichtbar ist. Führe regelmäßige Scans durch.

02 Unnötige Ports schließen

Firewall-Regeln: Nur Ports öffnen, die wirklich gebraucht werden. Least Privilege Principle.

03 Monitoring einrichten

IDS/IPS-Systeme erkennen verdächtige Scan-Aktivitäten und alarmieren dein Team in Echtzeit.

Was ist für mein Unternehmen wichtig?

Maßnahme	Aufwand	Wirkung	Für wen?	Priorität
3-2-1-0 Backup	Mittel	Sehr hoch	Jedes Unternehmen	SOFORT
Passwortmanager	Niedrig	Hoch	Ab 1 Mitarbeiter	SOFORT
NIS-2 Compliance	Hoch	Hoch + Pflicht	50+ MA / krit. Sektor	GESETZLICH
Port Scanning	Niedrig	Sehr hoch	Jedes Unternehmen	QUARTALSWEISE

Fazit & Nächste Schritte

Die Security-Checkliste

- 3-2-1-0 Backup eingerichtet und getestet
- Passwortmanager für alle Mitarbeiter
- NIS-2 Betroffenheit geprüft
- Firewall-Regeln auf dem neuesten Stand
- Port Scan des Netzwerks durchgeführt
- Multi-Faktor-Authentifizierung aktiviert
- Mitarbeiter-Schulung zu Phishing
- Incident Response Plan vorhanden

Unsere Kunden

CruSec Solutions

Buche dir jetzt deinen Termin unter

kontakt@crusecsolutions.com

+49 4161 505 3678

www.crusecsolutions.com

Tom Bohn
Geschäftsführer

CruSec Solutions UG (haftungsbeschränkt)
Rudolf-Diesel-Straße 2b
21614 Buxtehude
Handelsregister Tostedt: HRB 211890

Vertreten durch
Tom Bohn

Kontakt
Telefon: +49 4161 505 3678
E-Mail: info@crusecsolutions.com