HELMSAUER

GRUPPE

Top Cybercrime Trends 2023

und wie Sie sich aktiv dagegen schützen

Aktuelle Zahlen und Fakten zur Cyberkriminalität verheißen nichts Gutes. Man spricht sogar von einem neuen Höhepunkt der Bedrohungslage. Innovative Methoden und Professionalisierung im Bereich Cyberkriminalität sorgen für ernst zu nehmende neue Risiken im Alltag, vor denen es sich zu schützen gilt.

Gezieltes, anlassbezogenes Phishing

Zum Einsatz kommen nach wie vor bekannte Werkzeuge und kombinieren diese mit aktuellen Trends. Über Phishing-Mails manipulieren Cyberkriminelle die Gefühle ihrer Opfer, um an vertrauliche Daten zu gelangen und diese abzugreifen und anschließend für ihre Machenschaften zu nutzen. Dazu werden immer häufiger und schneller aktuelle Themen und gesellschaftliche Entwicklungen in die trügerischen Nachrichten aufgenommen. Diese konkret anlassbezogenen Phishing-Mails wecken oftmals Emotionen und Unsicherheit in den Opfern, wodurch sie eher auf die schädlichen Inhalte klicken und die Cyberkriminellen zielsicher Daten abgreifen.

Multiple Extortion – Mehrfacherpressung

Seit 2021 hat sich Anzahl der Angriffe mit Erpressungssoftware im Vergleich zu 2020 mehr als verdoppelt. Bei dieser Angriffsart schleusen Cyberkriminelle Schadsoftware in IT-Systeme ein, verschlüsseln sensible Daten, die sie nur nach Zahlung eines Lösegelds (engl. „ransom") freigeben. Doch das alleine ist nicht mehr alles. Mehrfacherpressungen stehen hoch im Kurs. Bei Multiple Extortions setzen die Cyberkriminellen zusätzlich zum eigentlichen Raub, der Verschlüsselung der sensiblen Daten sowie der Drohung, diese bei Nicht-Zahlung zu veröffentlichen, beispielsweise auf DDoS-Attacken, die die Webseiten ihrer Opfer lahm legen, bis diese sich ihren Forderungen fügen.

Cybersicherheits-Strategie: Was muss jetzt beachtet werden

Um sich adäquat und möglichst umfassend zu schützen, ist es wichtig, mehrgleisig zu fahren. Zum einen sollten Unternehmen die Schwachstellen in ihrem IT-System, über die sie Einfallstore bieten, identifizieren und beheben.

Zum anderen ist es notwendig, sich selbst und seine „Mannschaft" im Betrieb mit den Gefahren und Risiken vertraut zu machen. Untersuchungen zeigen, dass die größten Risikofaktoren Unwissenheit der Betroffenen, schlechte Passwörter, mangelnde Notfallkonzepte, etc. sind. So auch wieder im Human Risk Review 2022 bestätigt.

Berücksichtigt man beispielsweise, dass über 50% der erfolgreichen Cyberangriffe auf mit Schadsoftware belastete Emails zurückzuführen sind, so zeigt sich ein erhebliches Schutzpotenzial in Trainings und Schulungen zum Erkennen solcher Emails.

In letzter Instanz, um die Folgen von Cyberattacken möglichst einzudämmen und die finanziellen Risiken zu minimieren, macht eine gute Cyberversicherung für Unternehmen absolut Sinn. Fakt ist, dass es für alle Unternehmen unerlässlich ist, sich mit der aktuellen Bedrohungslage auseinanderzusetzen, Maßnahmen zu ergreifen und umzusetzen.

Im Interview:
Joachim Berg, Präsident des Digitalverbands Bitkom (Sosafe, Human Risk Review 2022)

Was sind die 3 wichtigsten Aspekte für eine ausgewogene Informationssicherheitsstrategie?

„Sicherheit ist ein Prozess und keine Einmallösung. Dieses Verständnis muss in Unternehmen und Behörden gelebt werden. Konkret ist es also die Balance der drei Säulen:

1. Technik,
2. Organisation und
3. Mensch."

Starten Sie Ihr ganzheitliches Cyber-Sicherheitskonzept für Verbandsmitglieder:

- ✓ **Cyber-Security-Check**
- ✓ **Live-Webinarreihe**

Sicherheit durch Wissen: Der Security-Check

Kostengünstig. Professionell. Unkompliziert.

Prüfen Sie das Sicherheitskonzept Ihres Unternehmens.

Anhand eines Fragebogens sowie technischer und organisatorischer Begutachtung wird der aktuelle Sicherheitsstandard eines Unternehmens bestimmt. Gerade für die Untersuchung des Sicherheitsniveaus und die Risikobewertung durch Versicherungsunternehmen ist ein solcher Status quo enorm hilfreich.

Der Security-Check ist für Sie in nur wenigen Schritten unkompliziert durchzuführen und sollte regelmäßig erfolgen.

Ziel des Checks

- Nutzerkonten-Sicherheit
- Schutz gegen Schadsoftware
- Netzwerk-Sicherheit
- Patch-Management
- Datensicherungskonzept

Genau richtig: Nur wenige Schritte

1 Fragebogen

Eigene Angaben:

Mithilfe eines von uns vorgegebenen Leitfadens geben Sie Ihre Einschätzungen zunächst selbst ab.

2 Risikodialog

Direkter Austausch:

Ihre vorigen Angaben werden dann telefonisch besprochen, um alle Aspekte genauestens abzudecken.

3 Analyse & Dokumentation

Fremdcheck:

Ein Analyst überprüft und dokumentiert im Anschluss die technische Umsetzung von Sicherheitsaspekten in Ihrem System per Fernverbindung.

Technische Checks

User-Management
Nutzer des Betriebssystems, Berechtigungen und geteilte Konten werden ebenso geprüft wie die Sicherheit der Passwörter.

Anti-Virus-Software
Die im Unternehmen genutzte Anti-Virus-Software inkl. Signaturen, Autostart und Lizenz wird getestet.

Konfiguration der Firewall
Der Firewall-Regelsatz auf Zugänge zu internen Systemen und Internetservices wird untersucht.

Patch-Management
Der Patchstand des Betriebssystems wird ebenso kontrolliert wie die Patch-Management-Konfiguration. Außerdem wird der Patchstand installierter Standardprogramme stichprobenartig geprüft.

Organisatorische Checks

Backup-Konzept
Es wird überprüft, ob Sicherheitskonzepte oder -prozesse und dazugehörige empfohlene Vorgehensweisen in Unternehmen eingehalten werden.

Umfang der Analyse

Um die Sicherheitsanforderungen zu prüfen, werden stichprobenartig einzelne Systeme (maximal drei) analysiert und zufällig ausgewählte Dokumente gesichtet. Außerdem werden Mitarbeiter zu bestimmten Sicherheitsaspekten befragt. Bei einer solchen Analyse werden nur die wichtigsten Einstellungen, also die Basiskonfigurationen, betrachtet. Das spart Zeit und Aufwand, deckt aber dennoch die Anforderungen an ein sicheres Unternehmen ab.

Ihre Vorteile auf einen Blick

- Status quo des aktuellen Sicherheitsstandards Ihrer IT-Systeme
- Aufdecken von Sicherheitslücken und Verbesserungspotenzialen
- Prüfung technischer und organisatorischer Maßnahmen zur Cybersicherheit
- Reportbericht zur Dokumentation und ggf. Unterstützung zur Enthaftung
- Optionaler Zusatzbaustein p.a. in Ihrem Cyberversicherungskonzept
- Versicherungsschutz unabhängig vom Check-Ergebnis möglich
- Verzicht auf den Einwand der Obliegenheiten möglich
- Kein Selbstbehalt beim ersten Schadenfall

Machen Sie den Check!

Wie sicher ist Ihr Unternehmen? Fragen Sie jetzt Ihr persönliches Sicherheitsrisiko ab.

Wenn alle Stricke reißen

Sollte es trotz aller Vorsicht und Schutzmaßnahmen dennoch zu einem Cyberangriff kommen, ist es hilfreich, das Unternehmen über eine leistungsstarke Cyberversicherung abgesichert zu haben. Hier bieten wir ein spezielles Konzept für Verbandsmitglieder, das besonders auf die Bedürfnisse von Unternehmen ausgelegt ist. Neben dem Versicherungsschutz erhalten Sie auch bereits einige der genannten Service-Leistungen und Schulungsprogramme kostenfrei. Durch Gründung unserer Assekuradeur GmbH ist es uns gelungen, die Inhalte des Rahmenkonzeptes nochmals zu verbessern.

Rahmenkonzept für Verbandsmitglieder nochmals verbessert:

- ✓ **Kostenfreies Cyber-Security-Training für alle** Ihre Mitarbeiterinnen und Mitarbeiter mit Online-Training und Erklär-Videos und einem Wissenstest sowie Bereitstellung einer datenschutzkonformen Softwareplattform zur Prüfung von potenziell infizierten E-Mails und eines Werkzeugkastens für eine sichere Passwort-Programmierung
- ✓ **Zweifache Maximierung der Versicherungssumme**
- ✓ **Garantierte und unverzügliche Hilfestellung durch Cybercrime-Experten** im Schadenfall – rund um die Uhr!
- ✓ **Mitversicherung von Eigenschäden** in der Forensik und Schadenfeststellung
- ✓ **Vermögensschäden aus gefälschten E-Mails** mit Aufforderung zu Geldtransaktionen
- ✓ **Wiederherstellungskosten** (inkl. Hardware-Ersatz),
- ✓ **Mitversicherung von Drittschäden**, z. B. Abwehr unberechtigter Schadenersatzansprüche
- ✓ Soweit gesetzlich zulässig: **Übernahme von Bußgeldern**
- ✓ **„Bring your own device"-Deckung** z. B. berufliche Nutzung privater Smartphones
- ✓ **Betriebsunterbrechung zur Sicherung Ihres Umsatzes** – Dies gilt auch bei technischen Störungen
- ✓ **Erweiterung** der Betriebsunterbrechungs-Leistung um Mehrkosten
- ✓ **Internet-Diebstahl**
- ✓ **Cyber-Spionage**
- ✓ **Cyber-Erpressung**
- ✓ **Sicherheitsanalyse: Cyber-Security-Check**

Ihre Cyber-Hotline bei der Helmsauer Gruppe: **0911-9292 185**

> Rückantwortfax: 0911-9292 432 **> oder über unser digitales Kontaktformular:**

Ja, ich möchte weitere Informationen zu folgenden Themen erhalten: ☐ Cyberversicherung ☐ Security-Check

Bitte nehmen Sie mit mir Kontakt auf:

☐ Herr ☐ Frau _____

Name, Vorname

_____ _____

E-Mail Telefon

Stempel:

ANTWORTSCHREIBEN an:

Helmsauer Gruppe
Dürrenhofstraße 4
90402 Nürnberg

Per E-Mail **service@helmsauer-gruppe.de**
oder per Fax **0911- 9292 432**

Hinweis zum Datenschutz: Die o. a. Angaben werden ausschließlich zur Berechnung/Beratung von Angeboten verwendet. Sie können der Speicherung Ihrer personenbezogenen Daten jederzeit widersprechen.
Weitere Infos zum Datenschutz finden Sie unter: www.helmsauer-gruppe.de/datenschutz

Stand 14/11/2023