Cyber Security.

Angriffen vorbeugen. Bedrohungen erkennen, eindämmen und bereinigen.

Cyber Angriffe: Die Realität!

Fast täglich wird in den Medien über komplexe Cyber Attacken berichtet. Viele Unternehmen und Behörden sind gefährdet oder bereits kompromittiert – ohne es nur zu ahnen.

Vergleicht man Angriffe auf Netzwerke und IT-Systeme von heute mit denen von vor 10 Jahren, so haben sich nicht nur die Angriffsvektoren, sondern auch die verwendeten Techniken geändert. Signaturabhängige Sicherheitslösungen, wie z. B. herkömmliche Antiviren-Software, sind machtlos gegen die raffinierten Cyber Attacken von heute.

Grundsätzlich unterscheidet man zwischen

„opportunistischer" Cyberkriminalität

- Nicht auf ein bestimmtes Ziel/Unternehmen ausgerichtet
- Ziel: Möglichst viele Opfer infizieren

und organisierter Cyberkriminalität

- Gut organisierte Gruppen mit hoher Spezialisierung und enormen finanziellen Ressourcen
- Ziel: gezielter Angriff auf ein Unternehmen oder eine kritische Infrastruktur

Warum es auch Ihr Unternehmen betrifft

Die Motivationen für Cyber Angriffe sind vielfältig (Protest, Spionage, Sabotage, Kriminalität, politische Hintergründe...) und nicht jeder Angriff erfolgt gezielt. Aber nahezu alle anspruchsvollen Attacken haben gemeinsam, dass sie bestehende Schutzmechanismen einfach umgehen.

Mit der Unterstützung von analytischen Abwehr-Tools und Experten, die diese Technologien beherrschen, lassen sich Angriffe erkennen und ihre Auswirkungen schnellstmöglich eingrenzen.

Prävention allein reicht nicht mehr aus. Infektionen müssen akzeptiert werden.

Es geht heute um **schnellstmögliches Erkennen, Eindämmen und Bereinigen**.

Nachhaltige IT-Sicherheitsstrategie

- Wie steigern Sie Ihre Cyber Security auf allen Ebenen systematisch?
- Wie minimieren Sie Ihr Risiko gegenüber Cyberkriminellen?
- Wie reduzieren Sie unkalkulierbare, finanzielle Schäden und Reputationsverlust so weit wie möglich?
- Welche externen Anforderungen gilt es zu beachten (Kunden, Gesetze, Regularien)?
- Wer trägt für Cyber Security Vorfälle die Verantwortung im Unternehmen?
- Wie reportet man Cyber Security Vorfälle an das Management?

Mit unserem ganzheitlichen Cyber Security Readyness Programm bereiten wir Sie heute auf die Bedrohungen von morgen vor!

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

Lebenszyklus einer Cyber Attacke

Cyber Security managen: Der Weg zu mehr Sicherheit erfolgt oft in mehreren Stufen - den richtigen Mix an Maßnahmen für Ihr Unternehmen entwickeln wir gerne gemeinsam mit Ihnen.

Unsere Services und Lösungen

- Computer Security Incident Response Team (CSIRT) – hochqualifizierte schnelle Eingreiftruppe, die Cyber Attacken erkennt und wirksam begrenzt
- Konzeption/Architektur, Implementierung und Betrieb (wenn gewünscht im Managed Service) von:
  - Advanced Threat Protection Lösungen und Sensoren
  - Next Generation Firewalls
  - DDos Protection
  - SIEM
- Infrastruktur-Architekturdesign
- Unterstützung beim Aufbau von Management-systemen zur Steuerung von Cyber Security (ISMS, BCMS)
- Analyse und Bewertung von Outsourcing Part-nern bis hin zu Cloud Analysen und Zertifizie-rungen
- Sicherstellung der Verfügbarkeit der unterneh-mensrelevanten Prozesse durch BCM Consulting
- Sicherheitstests von Applikationen und Beratung zur Entwicklung von sicherem Code
- IT-Compliance Checkups
- Readiness Assessments nach ISO 27001 und ISO 22301
- Datenschutz-Checkups
- 360 Grad Analyse

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
Fax +49 221 806-2295
service@i-sec.tuv.com