cybercrime
Komplettschutz

Fachvortrag Cybercrime & Solutions CEO

cybercrime
Komplettschutz

Fachvortrag

CYBERCRIME & SOLUTIONS

„Die primäre Frage ist nicht ob, sondern wann und wie man Opfer einer Cyberattacke wird!“

Ransomware Attacken sind aktuell die größte Cyber-Gefahr für die Wirtschaft. Zu den potentiellen Angriffszielen zählen Unternehmen, unabhängig von Branche und Größe, genauso wie Gebietskörperschaften,Behörden, Regierungen, Gesundheits- und Bildungswesen - und das länderübergreifend – 24/7/52.

Industrie, Konzerne, bis zu Klein- und Mittelbetrieben zählen aufgrund der hochsensiblen Datenmengen zu beliebten Angriffszielen Cyberkrimineller.

Wird **Ihr Unternehmen** Opfer einer Ransomware Attacke wird Ihr gesamtes IT-System verschlüsselt – ***„rien ne va plus – nichts geht’s mehr“*** – Sie haben keinen Zugriff mehr auf Ihr System. Alles steht still. Dem nicht genug kommt es parallel dazu zum Diebstahl Ihrer gesamten Daten. Sensible Mitarbeiter- und Kundendaten, Ihr gesamter interner und externer Schriftverkehr, Ihre Buchhaltung und Steuerunterlagen, Verträge, Versicherungsdokumente, Kunden- und Mitarbeiter Zugangsdaten und Passwörter – ALLES unwiderruflich WEG – in den Händen von Verbrecherbanden. Anschließend stellen die Cyberkriminellen Lösegeldforderungen – geben Sie der Erpressung nicht nach, werden Ihre gesamte Daten im **Darknet** veröffentlich und weltweit einer Vielzahl von Schwerstkriminellen zum Verkauf angeboten. Die Folgen sind meist existenzbedrohend – Neben IT-Problemen, DSGVO Verpflichtungen, Schadensersatzklagen, leiden und kämpfen die betroffenen Kunden, Mitarbeiter und Sie selbst über viele Jahre unter verschiedensten Betrugs- und Erpressungsversuchen, Mails, Anrufe, Banken- und Behördenproblemen.

- **Folgen Sie uns ins DARKNET – ihre Daten sind schon lange dort**
- **Wir erklären Ihnen Ablauf und die existenzbedrohenden Folgen von Ransomware und DDos Attacken**
- **Wir beleuchten die Wechsel- und Geschäftsbeziehung zwischen Ransomware-Gangs und den verschiedensten Verbrecherbanden**
- **Wir zeigen Ihnen auf mit welchen technischen und psychologischen Tricks Social Engineering Delikte verübt werden und stellen Ihnen die aktuellsten Cyberbetrugs- und Erpressungsdelikte vor**
- **Wir stellen Ihnen die 3 Säulen der IT-Sicherheit vor, erklären das 3 Phasenmodell und vermitteln Lösungsansätze abseits gutgemeinter, aber meist nutzloser IT-Security Tipps**

cybercrime
Komplettschutz

Programm Cybercrime & Solutions

Zahlen, Daten, Entwicklung

Statistiken – Schadenshöhen und Prognosen – Organisierte Kriminalität wechselt ins Home-Office: Vorteile der Täter im Netz – Dunkelfeld - Underground Economy

Cybercrime vs herkömmliche Kriminalität

Vergleich der herkömmlichen Kriminalität zu Cybercrime anhand des Fallbeispiels Einbruchsdiebstahl – zeitliche, örtliche Komponente / Schadenssummen / Modi Operandi

Kategorien

breitgefächerter / zielgerichteter Angriff - Cybercrime im engeren Sinn / im weiteren Sinn Ransomware / Cyberschurken

Ransomware Gangs

Ablauf von Ransomware und DDos Attacken – Folgen und Schäden – Vorstellung der aktivsten und größten Ransomware Gangs (Lockbit – Play – Black Cat – VICE) – Cybercrime as a service: „Wen soll es wann womit treffen“

Darknet

„Folgen Sie uns ins Darknet – Ihr Daten sind bereits dort“
Live Einstieg zu Ransomware Gangs Webseiten und Darknet-Märkten

Cyberschurken

Tätergruppen - Werkzeuge und Tools der Cyberkriminellen – VPN / Voive over IP / Call ID Spoofing / Fakeshops / Fakemailer / Passwort-Hacking - Psychologische Tricks der Täter

Social Engineering

Der Weg vom Daten-Leak zum Social Engineering Delikt – Social Engineering verstehen: Das Delikts Puzzle

Aktuelle Cyberdeliktsformen

Phantasie der Täter kennt keine Grenzen – Abwandlungen der Deliktsformen Unternehmen / Privatpersonen – CEO Fraud / PHISHING / PHARMING / Stranded Traveller / Polizei Trojaner / FluBot SMS / Warenbestellbetrug / BEC Fraud / Love Scam / Sextortion / Gewinnversprechen / Scheckbetrug / Cyber Trading Fraud / Fake Calls

Lösungsansätze

Die 3 Säulen der IT-Sicherheit und das Cybercrime-Komplettschutz 3 Phasenmodell

cybercrime

Cybercrime Komplettschutz

Medieninhaber und Hersteller:
Agentur Cyberschutz HIETZ e.U. – 2500 Baden – FN: 560 753m – LG Wr. Neustadt