

VERSTEHEN.
REAGIEREN.
WIEDERANLAUFEN.

Incident Response Workshop für IT und Security

Daniel Rossgatterer Cybercrime Keynote Speaker

DER WORKSHOP

Gehackt. Was nun? Im Ernstfall zählen Minuten.

Ransomware gehört zu den kritischsten Vorfällen für Unternehmen. In kürzester Zeit sind Systeme verschlüsselt, Daten gestohlen und Prozesse unterbrochen. Die Entscheidungen der ersten Stunden bestimmen oft den gesamten weiteren Verlauf.

Wer vorbereitet sein will, muss verstehen, wie Täter vorgehen: welche Angriffswege sie nutzen, wie sie sich im Netzwerk bewegen, wie Daten abfließen und wie Erpressung in der Praxis funktioniert.

Der Workshop bereitet IT-Teams praxisnah auf den technischen und organisatorischen Ernstfall vor. Mit realen Ransomware-Fällen, typischen Angriffsmustern, den Abläufen der ersten Stunden und konkreter Wiederanlaufplanung.

FÜR WEN

IT-Leitung, CISOs, Security-Verantwortliche, Administratoren, SOC- und Infrastruktur-Teams, IT-Dienstleister und technische Krisenteams. Auf Wunsch gemeinsam mit dem Krisenstab, um Schnittstellen zu Management, Kommunikation, Datenschutz, Recht und Versicherung zu klären.

AUF EINEN BLICK

½ Tag
oder kompakt in 2 bis 4 Stunden

Flexibel
Gruppengröße individuell anpassbar

24 h
Die ersten Stunden nach der Entdeckung

1
IT-Playbook für Ransomware und Wiederanlauf

RANSOMWARE

ZENTRALE FRAGEN

Was Ihr IT-Team vorher wissen muss.

01 Wie laufen Ransomware-Angriffe in der Praxis ab?

02 Wie gelangen Täter ins Netzwerk und welche Wege dominieren?

03 Welche Rolle spielen VPN, Schwachstellen, Phishing und Zugangsdaten?

04 Wie bewegen sich Angreifer und wie bereiten sie die Verschlüsselung vor?

05 Wie erkennt man Datenabfluss und welche Spuren zählen?

06 Was muss in den ersten Minuten und Stunden passieren?

07 Welche Systeme dürfen abgeschaltet werden und welche besser nicht?

08 Welche Logdaten, Systeme und Beweise müssen gesichert werden?

09 Wann werden Partner, Versicherung, Management und Behörden eingebunden?

10 Wie funktioniert die Kommunikation mit Cyberkriminellen?

11 Welche Rolle spielen Backups, Wiederherstellung und Wiederanlauf?

12 Was gehört in ein praxistaugliches Ransomware-Playbook?

INHALTE

Sechs Teile. Vom Angriff bis zum Wiederanlauf.

TEIL 01

Bedrohungslage und Täterlogik

Ransomware, Datendiebstahl und Erpressung: wie Täter heute arbeiten und welche Gruppen aktiv sind. Anhand realer Fälle.

TEIL 02

Angriffswege und Muster

Kompromittierte Zugangsdaten, VPN- und Firewall-Zugänge, Phishing, Schwachstellen, unsichere Admin-Konten, laterale Bewegung, Privilege Escalation und Datenabfluss.

TEIL 03

Ein Fall aus der Praxis

Vom ersten Einstieg über die Ausbreitung im Netzwerk bis zu Datendiebstahl, Verschlüsselung, Erpresserschreiben und Wiederherstellung. Mit Warnsignalen und Lessons Learned.

TEIL 04

Die ersten 24 Stunden

Sofortmaßnahmen, Eskalation, Systemisolation, Beweissicherung und Logdaten. Dazu Kommunikation mit Management und Partnern, Versicherung, Entscheidungswege und Prioritäten.

TEIL 05

IT-Playbook und Wiederanlauf

Gemeinsam erarbeitet: Rollen, Notfallkontakte, technische Checklisten, Backup und Restore, Priorisierung kritischer Systeme, Wiederanlaufplanung und Entscheidungslogik.

TEIL 06

Praxisempfehlungen

Was den größten Unterschied macht: Segmentierung, gehärtete Backups, Admin-Konten, Monitoring und Logging, externe Sichtbarkeit, Schwachstellenmanagement und Notfallübungen.



WAS BLEIBT

Im Ransomware-Ernstfall strukturiert statt hektisch.

Die Teilnehmenden wissen, wie Ransomware-Angriffe ablaufen, welche Schritte in den ersten Minuten und Stunden nötig sind und welche Fehler sie unbedingt vermeiden müssen.

Der Workshop schafft Klarheit und nimmt Unsicherheit. Damit das IT-Team im Ernstfall handlungsfähig bleibt und die Wiederherstellung schneller gelingt.

ERGEBNIS

Ihr IT-Playbook für Ransomware und Wiederanlauf

Rollen und Eskalation	Sofortmaßnahmen	Systemisolation	Beweise und Logdaten
Backup und Restore	Notfallkontakte	Kommunikation	Wiederanlaufplanung

DAS ANGEBOT

Ein Thema.
Vier Wege ins Unternehmen.

Keynote und Workshops bauen auf denselben realen Fällen auf. Sie lassen sich einzeln buchen oder kombinieren, zum Beispiel als Keynote für alle Mitarbeitenden, Workshop für die Geschäftsführung und Workshop für die IT.

FORMAT 01

Keynote

Darknet, Hacker & Co.

FÜR	Events, Kunden, Partner und Mitarbeitende
ZIEL	Cybercrime aus Sicht der Täter verstehen
ERGEBNIS	Handout mit Inhalten und Schutzempfehlungen

FORMAT 02

Awareness Workshop

Angriffe erkennen. Richtig handeln.

FÜR	Mitarbeitende aus allen Unternehmensbereichen
ZIEL	Angriffe im Alltag früher erkennen und richtig reagieren
ERGEBNIS	Handout mit Inhalten und Verhaltensempfehlungen

FORMAT 03

Executive Resilience Workshop

Entscheidungen vorbereiten. Schäden begrenzen.

FÜR	Geschäftsführung, Management und Krisenstab
ZIEL	Im Ernstfall schneller und sicherer entscheiden
ERGEBNIS	Management-Playbook für den Ernstfall

DIESER FOLDER

Incident Response Workshop

Reaktion vorbereiten. Wiederanlauf sichern.

FÜR	IT-Leitung, Security-, SOC- und Infrastruktur-Teams
ZIEL	Den technischen Ernstfall beherrschen und schneller wiederanlaufen
ERGEBNIS	IT-Playbook für Ransomware und Wiederanlauf



WORKSHOPLEITUNG

Daniel Rossgatterer

Mag. Daniel Rossgatterer, MBA
Co-Founder und Geschäftsführer
Secutec GmbH

Unternehmer, Cybersecurity-Praktiker und einer der wenigen Speaker, die mit Erpressern selbst verhandelt haben.

Über zwei Jahrzehnte führte er als Miteigentümer und Geschäftsführer ein großes IT-Dienstleistungsunternehmen in Österreich und Deutschland. Heute verantwortet er bei Secutec die DACH-Region und begleitet Kundenprojekte, in denen es um Minuten, Millionen und existenzielle Entscheidungen geht.

In Keynotes und Workshops öffnet er eine Welt, die für die meisten verborgen bleibt: live im Darknet, mit echten Ransomware-Fällen und klaren Schutzmaßnahmen. Er spricht offen, direkt und ohne Fachjargon. Für Entscheider, Führungskräfte und IT-Verantwortliche, die wissen wollen, was im Ernstfall zählt.

ÜBER SECUTEC

Europäischer Hersteller für Cyber Threat Intelligence. Unterstützt Unternehmen, Nachrichtendienste und die NATO, von der Prävention bis zur akuten Krise. Mehrere hundert begleitete Cyberangriffe.

BÜHNEN (AUSWAHL)

IKT-Sicherheitskonferenz
Österreichisches Bundesheer

Cyber Crime Forum Linz
Opening Keynote

Sicherheitsgipfel
Handelsverband

CIO Kongress
LSZ

BUCHUNG UND KONTAKT

Sprechen wir über Ihren Workshop.

SPEAKER-SEITE
danielrossgatterer.com

LINKEDIN
Daniel Rossgatterer

Mag. Daniel Rossgatterer, MBA
+43 664 2050686
daniel.rossgatterer@secutec.com

Secutec GmbH
Gewerbestraße West 14
4921 Hohenzell, Österreich