

VERSTEHEN.
VORBEREITEN.
BEGRENZEN.

Executive Resilience Workshop für das Management

Daniel Rossgatterer Cybercrime Keynote Speaker

DER WORKSHOP

Im Ernstfall entscheidet nicht die IT. Sondern die Geschäftsführung.

Cyberkriminelle arbeiten strukturiert, wirtschaftlich motiviert und mit gezieltem psychologischem Druck. Wer sein Unternehmen vorbereiten will, muss verstehen, wie Täter Opfer auswählen, Druck aufbauen und verhandeln.

Dieser Workshop vermittelt kein Lehrbuchwissen. Er zeigt Denkweise, Methoden und Abläufe professioneller Cybercrime-Gruppen, auf Basis realer Vorfälle, Ransomware-Fälle und Verhandlungen mit Erpressern.

Das Ziel: Geschäftsführung und Management so vorzubereiten, dass sie im Ernstfall schneller, strukturierter und sicherer entscheiden können.

FÜR WEN

Geschäftsführung, Vorstand, Eigentümer und Management-Teams sowie ausgewählte Mitglieder des Krisenstabs: Verantwortliche aus IT, Security, Recht, Datenschutz, Kommunikation, Risiko und Compliance. Die Gruppengröße ist individuell anpassbar.

AUF EINEN BLICK

½ Tag
oder kompakt in 2 bis 4 Stunden

Flexibel
Gruppengröße individuell anpassbar

24 h
Die ersten Stunden nach dem Angriff im Fokus

1
Management-Playbook als Ergebnis

ERNSTFALL

ZENTRALE FRAGEN

Was die Geschäftsführung vorher klären muss.

01 Was muss die Geschäftsführung vor einem Angriff geklärt haben?

02 Welche Entscheidungen fallen in den ersten Minuten und Stunden?

03 Wer gehört in den Krisenstab und wer ausdrücklich nicht?

04 Welche Rolle spielen IT, Anwälte, Versicherung, Datenschutz und Behörden?

05 Welche Fehler sollten in der Kommunikation vermieden werden?

06 Wie laufen Lösegeldverhandlungen in der Praxis ab?

07 Wann zahlen Unternehmen Lösegeld und warum?

08 Welche Risiken entstehen durch Zahlung oder Nichtzahlung?

09 Wie erkennt man, ob Daten tatsächlich gestohlen wurden?

10 Was passiert, wenn Daten im Darknet veröffentlicht werden?

11 Welche Fehler passieren im Ernstfall besonders häufig?

12 Welche Vorbereitung senkt Schaden, Kosten und Entscheidungsdruck?

INHALTE

Sechs Teile. Von der Lage bis zum Playbook.

TEIL 01

Aktuelle Bedrohungslage

Ransomware, Datendiebstahl und Erpressung: wie professionell Täter heute arbeiten und warum das Management eingebunden sein muss. Anhand realer Fälle.

TEIL 02

Der Angriff als Management-Krise

Ein Cyberangriff trifft das ganze Unternehmen. Welche Entscheidungen auf Managementebene entstehen und warum fehlende Vorbereitung zu massiven Verzögerungen führt.

TEIL 03

Die ersten 24 Stunden

Wer muss informiert werden? Welche Systeme dürfen abgeschaltet werden? Welche Kommunikation ist intern und extern nötig? Und welche Fehler gilt es zu vermeiden?

TEIL 04

Lösegeld und Verhandlung

Wie Täter auftreten, wie Erpresserschreiben aussehen und Forderungen entstehen. Welche Rolle Zahlungsfähigkeit, Datenabfluss, Zeitdruck und öffentlicher Druck spielen.

TEIL 05

Playbook für den Ernstfall

Gemeinsam erarbeitet: Entscheidungswege, Krisenstab, Kommunikationsplan, Notfallkontakte, Versicherung, rechtliche Fragen, Backup und externe Unterstützung.

TEIL 06

Lessons Learned

Was hat in echten Fällen funktioniert, was hat geschadet? Welche Maßnahmen den größten Unterschied machen und wie sich die Resilienz realistisch verbessern lässt.



WAS BLEIBT

Im Ernstfall nicht hektisch reagieren, sondern handlungsfähig bleiben.

Die Teilnehmenden wissen, welche Rolle Geschäftsführung und Management im Ernstfall übernehmen, welche Entscheidungen vorbereitet sein müssen und welche Fehler besonders teuer werden.

Der Workshop schafft Klarheit, bevor es darauf ankommt. Damit ein Unternehmen im Angriff strukturiert, vorbereitet und handlungsfähig bleibt.

ERGEBNIS

Ihr Management-Playbook für den Ernstfall

Krisenstab und Rollen	Kommunikation	Versicherung	Rechtsanwälte
Behörden	Notfallkontakte	Lösegeldstrategie	Technische Mindeststandards

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

DIESER FOLDER

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

FORMAT 04

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

Sicherheitsgipfel
Handelsverband

Cyber Crime Forum Linz
Opening Keynote

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