

VERSTEHEN.
ERKENNEN.
HANDELN.

Cybercrime Awareness Workshop für Mitarbeitende

Daniel Rossgatterer Cybercrime Keynote Speaker

DER WORKSHOP

Angreifer brauchen keine Sicherheitslücke. Oft reicht ein Klick.

Cyberkriminelle nutzen gezielt Neugier, Vertrauen, Zeitdruck und Unsicherheit. Viele Angriffe beginnen mit einem Anruf, einer gefälschten Rechnung oder einer scheinbar harmlosen Anfrage.

Regeln allein schützen deshalb nicht. Mitarbeitende müssen verstehen, wie Täter denken, wie sie Vertrauen aufbauen und wie sie Druck erzeugen.

Genau hier setzt der Workshop an. Statt Theorie gibt es echte Einblicke aus realen Angriffen, Darknet-Recherchen, Ransomware-Fällen und Verhandlungen mit Cyberkriminellen.

FÜR WEN

Mitarbeitende aus allen Unternehmensbereichen, die mit E-Mails, Dokumenten, Kundendaten, Zahlungen, IT-Systemen oder externer Kommunikation arbeiten. Vor Ort oder online, die Teilnehmerzahl ist flexibel anpassbar.

AUF EINEN BLICK

½ Tag
oder kompakt in 2 bis 4 Stunden

Flexibel
Teilnehmerzahl individuell anpassbar

300+
Verhandlungen mit Cyberkriminellen

1
Handout mit Inhalten und Empfehlungen

MENSCH

ZENTRALE FRAGEN

Darauf gibt der Workshop Antworten.

01 Was wollen Cyberkriminelle wirklich erreichen?

02 Wie wählen sie Unternehmen und Mitarbeitende als Ziel aus?

03 Warum funktionieren E-Mail, Telefon und gefälschte Rechnungen so gut?

04 Wie erkennt man Phishing, Social Engineering und Betrug?

05 Welche Rolle spielen Zeitdruck, Vertrauen, Autorität und Unsicherheit?

06 Wie läuft ein Ransomware-Angriff in der Praxis ab?

07 Was passiert mit gestohlenen Daten nach einem Angriff?

08 Wie sehen Darknet-Seiten von Hackergruppen aus?

09 Wie treten Cyberkriminelle gegenüber Unternehmen auf?

10 Wie laufen Lösegeldforderungen und Verhandlungen ab?

11 Welche Fehler passieren besonders häufig?

12 Was kann jeder Einzelne konkret tun?

INHALTE

Sechs Teile. Vom Täter bis zur richtigen Reaktion.

TEIL 01

Cyberkriminelle verstehen

Wie professionell Cybercrime heute organisiert ist: Denkweise, Motivation und Arbeitsweise moderner Tätergruppen.

TEIL 02

Darknet und Hackergruppen

Wie Hackergruppen im Darknet auftreten, gestohlene Daten veröffentlichen und Unternehmen öffentlich unter Druck setzen. Anhand realer Beispiele.

TEIL 03

Angriffe im Arbeitsalltag

Phishing, Social Engineering, Schadsoftware und Identitätsmissbrauch. Wie Angriffe mit einem Link, einem Anhang, einer falschen Rechnung oder einem Anruf beginnen.

TEIL 04

Ransomware aus der Praxis

Ein realer Fall vom ersten Zugriff über die Ausbreitung im Netzwerk bis zu Verschlüsselung, Datendiebstahl und Erpressung. Und warum frühe Warnsignale entscheiden.

TEIL 05

Lösegeld und Verhandlung

Wie Erpresserschreiben aussehen, wie Forderungen aufgebaut sind und warum Unternehmen überhaupt über eine Zahlung nachdenken.

TEIL 06

Richtig handeln

Ungewöhnliche Zahlungsanfragen, wann man nachfragt, welche Warnsignale zählen. Und warum einmal zu viel melden besser ist als einmal zu wenig.



WAS BLEIBT

Angriffe früher erkennen. Im Alltag sicherer handeln.

Die Teilnehmenden verstehen, wie Cyberkriminelle denken und warum gerade Menschen angegriffen werden. Sie erkennen typische Muster früher und schätzen Risiken besser ein.

Das schafft Bewusstsein und nimmt Unsicherheit. Nicht durch abstrakte Regeln, sondern durch echte Fälle und einen klaren Blick hinter die Kulissen.

ERGEBNIS

Ihr Handout: Inhalte und Empfehlungen für den Arbeitsalltag

E-Mails und Anhänge	Links und Logins	Passwörter	Zahlungsfreigaben
Dokumente	Telefonate	Externe Anfragen	Ungewöhnliche Situationen

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

DIESER FOLDER

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

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