



Ganzheitlicher Umgang mit

Erpressungssoftware Ransomware

Entscheidungshilfen für den Ernstfall

[**HIER REGISTRIEREN**](#)

13. März 2024

10 - 12:00 und 13 – 16:00 Uhr MEZ

Online-Training

Meetingplattform Zoom



Unser Experte

[Michael Krausz](#) studierte Physik, Informatik und Rechtswissenschaften in Wien und den USA und ist ausgebildeter Berufsdetektiv sowie Buchautor zum Thema Behandlung von Sicherheitsvorfällen. Er hat seit 1998 Kunden in 32 Ländern auf 4 Kontinenten bei der Vorbeugung und Behandlung schwerer und schwerster extern oder intern ausgelöster Sicherheitsvorfälle unterstützt und widmet sich seit 2002 besonders der Vorbeugung durch Informationssicherheitsmanagementsysteme sowie der Verhandlungsführung und Unterstützung des Executive Managements und der IT im Ernstfall.

Follow us on





Zielgruppe

- Firmenjurist:innen
- Compliance Manager:innen
- Rechtsanwält:innen
- Geschäftsführer:innen
- Sicherheitsmanager:innen
- Anlagenbauunternehmer:innen

Hintergrund

Mittels Ransomware – bei uns auch als Erpressungs- oder Verschlüsselungstrojaner bekannt – verschlüsseln Cyberkriminelle Daten auf Ihren Computern oder verhindern, dass Sie weiter darauf zugreifen können.

Ziel dieses Angriffs ist zumeist die Erpressung von Lösegeld. Während in Deutschland sehr offen mit dem Problem umgegangen wird, wird in Österreich eher geschwiegen. Dennoch ist es auch hier eine immer häufiger auftretende Angriffsmethode. Einer der bekannteren Fälle war der Angriff auf die Firma Palfinger, wo 2021 Standorte weltweit für 2 Wochen lahmgelegt und Lösegeld gezahlt wurden.

Wird Ihr Unternehmen angegriffen, können schwerwiegende und kostspielige Probleme auftreten:

- Produktionsverzögerung oder -stillstand
- Datenverlust
- Rechtliche Folgen



Das Wesentliche

- Zahlen oder nicht?
- Verhandlungsstrategien
- Verhandlungsführung
- Zahlungsabwicklung
- IT-Aspekte
- Steuerliche Aspekte (Absetzbarkeit)
- Rechtliche Aspekte (Strafrecht, Verwaltungsrecht, Zivilrecht, Arbeitsrecht)
- Vorbeugende Maßnahmen
- [Praxisbeispiele möglicher Vorgangsweisen zur Bewältigung](#)

Dieses Training zeigt Gefahren durch Ransomware auf, hilft Ihnen diesen vorzubeugen und versorgt Sie mit praxisbezogenen Entscheidungshilfen um im Anlassfall schadensminimierend handeln zu können.

Online-Training Erpressungssoftware/Ransomware

13. März 2024

10:00 – 12:00 und 13:00 – 15:00 Uhr MEZ

HIER REGISTRIEREN

Teilnahmegebühr pro Person

€ 355,00 + 20% USt.

inkl. elektronischen Trainingsunterlagen, Teilnahmezertifikat

Ermäßigter Preis für ICC Austria Mitglieder:

€ 284,00 + 20% USt.

Erhalten Sie 10% Rabatt p. P. bei zeitgleicher Buchung ab 3 Teilnehmenden eines Unternehmens pro Online-Training Termin !

Technische Voraussetzung

Internetfähiger Rechner/Laptop/Tablet oder Smartphone.

Das Online-Training wird über Zoom abgehalten. Sollte Ihr Unternehmen Zoom nicht standardmäßig nutzen, ist dennoch eine Teilnahme möglich.

Bei Fragen wenden Sie sich bitte an Ihre hausinterne IT oder auch gerne direkt an uns.

Sie erhalten 3 Werktage vor Beginn den Link und die Zugangsdaten zur Teilnahme an der Onlineschulung.