Ransomware:
Bestmögliche Vorbereitung
Handout für Mitarbeiter

Ransomware ist eine spezielle Form von Schad-Software (Malware) und eine der **größten Bedrohungen für Unternehmen** weltweit. Ransomware zielt darauf ab, die Daten eines Opfers zu verschlüsseln oder den Zugriff auf Systeme zu blockieren, um anschließend ein Lösegeld (engl. »ransom«) zu fordern.

Betroffen sind Unternehmen jeder Größe – vom Kleinbetrieb bis hin zu Konzernen. Ransomware ist eine ernstzunehmende Bedrohung, die nicht nur die IT, sondern ganze Geschäftsprozesse lahmlegen kann.

Um sich zu schützen, ist **Prävention die effektivste Maßnahme** – eine einmal infizierte Umgebung kann meist nur schwer wiederhergestellt werden.

Dieses **Handout soll Ihnen helfen**, sich bestmöglich gegen Ransomware zu schützen und **im Ernstfall richtig zu reagieren**.

1

Warum Ransomware jeden treffen kann

- Ransomware-Angriffe richten sich nicht nur gegen große Unternehmen, sondern zunehmend auch gegen kleine und mittelständische Betriebe.
- Häufige Verbreitungswege: Phishing-E-Mails, infizierte Anhänge, kompromittierte Webseiten und unsichere Netzwerkverbindungen.
- Typische Folgen: Datenverlust, Betriebsunterbrechungen, Image-Schäden.

2

PRÄVENTIVE MASSNAHMEN FÜR MITARBEITER

Sicherer Umgang mit E-Mails

- Verdächtige E-Mails nicht öffnen und Anhänge nicht herunterladen.
- Links in E-Mails vor dem Klicken überprüfen – Mauszeiger darüber halten und Zieladresse prüfen.
- Bei Unsicherheit sofort die IT-Abteilung kontaktieren.

Passwortsicherheit

- Starke Passwörter verwenden: mindestens 12 Zeichen, Sonderzeichen, Zahlen und Groß-/Kleinbuchstaben.
- Passwortmanager nutzen, um komplexe Passwörter sicher zu speichern.
- Passwörter regelmäßig ändern und nicht mehrfach verwenden.

Melden von Unregelmäßigkeiten: Keine unnötige Besorgnis

Ransomware: Bestmögliche Vorbereitung

PRÄVENTIVE MASSNAHMEN FÜR MITARBEITER

Geräte aktuell halten

- Sicherheits-Updates und Patches sofort installieren.
- Automatische Updates aktivieren, wo möglich.
- Keine Software aus unsicheren Quellen herunterladen.

Datensicherung

- Regelmäßig Backups auf externen Medien oder Cloud-Lösungen erstellen.
- Sicherstellen, dass Backups vom Netzwerk getrennt aufbewahrt werden.

3

RICHTIGES VERHALTEN IM ERNSTFALL

Ransomware-Infektion erkennen

- Unerwartete Dateiverschlüsselungen oder veränderte Dateiendungen.
- Fehlermeldungen oder Hinweise auf verschlüsselte Daten.
- Aufforderung zur Zahlung von Lösegeld.

Sofortmaßnahmen

- Gerät sofort vom Netzwerk trennen.
- IT-Abteilung umgehend informieren.
- Keine Zahlungen an die Angreifer leisten.
- Gerät nicht eigenständig bereinigen.

4

WICHTIGE KONTAKTE

- **IT-Support:** [Telefonnummer/ E-Mail-Adresse]
- **Datenschutzbeauftragter:** [Kontaktinformationen]
- **Melden von Cybervorfällen:** [Link zum Datenschutzteam bzw. zu internen Richtlinien]

MELDEN VON UNREGELMÄSSIGKEITEN: KEINE UNNÖTIGE BESORGNIS

Wenn Sie **verdächtige Aktivitäten bemerken** – etwa unerklärliche Systemverlangsamungen, ungewöhnliche Fehlermeldungen oder plötzlich verschlüsselte Dateien –, **zögern Sie nicht**, dies sofort der IT-Abteilung zu melden.

Es gibt in solchen Fällen keine »falsche Hektik« – im Gegenteil: Je schneller ein möglicher Ransomware-Angriff erkannt wird, desto besser stehen die Chancen, den Schaden zu minimieren. Auch wenn sich der Verdacht später als unbegründet herausstellt, ist eine frühzeitige Meldung immer die sicherste Option.

Melden von Unregelmäßigkeiten: Keine unnötige Besorgnis