VORFALLART 02 · ERKENNEN & MELDEN

Ransomware & zerstörte Dateien

Wenn Dateien verschlüsselt werden und Lösegeld gefordert wird – die richtige Sofortreaktion.

Was ist das?

Ransomware verschlüsselt Dateien oder ganze Systeme und fordert Lösegeld. Häufig beginnt sie unbemerkt nach einem geöffneten Anhang oder über einen gekaperten Zugang und breitet sich im Netzwerk aus.

Zunehmend wird zusätzlich mit der Veröffentlichung gestohlener Daten gedroht („doppelte Erpressung“).

Was kann im Betrieb passieren?

- Dateien und Server sind nicht mehr nutzbar – der Betrieb steht
- Der Angriff breitet sich auf verbundene Geräte und Backups aus
- Personenbezogene Daten sind betroffen – es entsteht eine Meldepflicht
- Erpressung mit Zahlungsdruck und drohender Veröffentlichung

Woran erkennst du es?

- Lösegeldmeldung auf dem Bildschirm
- Dateien mit fremden Endungen oder nicht mehr zu öffnen
- Ungewöhnlich langsame Systeme, Programme reagieren anders
- Sicherheitssoftware schlägt Alarm oder wurde deaktiviert

Sofort richtig reagieren

Der Handlungsrahmen aus der Fortbildung – Schritt für Schritt:

1	**Trennen**	Betroffenes Gerät sofort vom Netz nehmen (Kabel und Funk), um die Ausbreitung zu stoppen. Nicht neu starten. An zentralen Systemen keine Kabelaktionen auf eigene Faust – IT hinzuziehen.
2	**Festhalten**	Lösegeldmeldung fotografieren. Uhrzeit, betroffenes Gerät und die zuletzt ausgeführte Aktion notieren.
3	**Melden**	IT sofort, dann Geschäftsleitung. Kein Kontakt und keine Zahlung an die Erpresser ohne Entscheidung der Leitung; ggf. Notfallnummer des Versicherers.
4	**Bewahren**	Kein Backup in eine noch kompromittierte Umgebung zurückspielen. Kein Wiederherstellungsversuch auf eigene Faust. Übergabe mit Protokoll.

Merksatz

Nicht zahlen, nicht basteln – trennen, melden, Fachhilfe holen.

Buch zur Fortbildung: „Betrieblicher Cyber-Ersthelfer“ · ISBN 978-3-6967-6362-6

Das ist erst der erste Schritt

In der Fortbildung „Geprüfter Betrieblicher Cyber-Ersthelfer“ (290 €, 2× 100 Min live & digital) übst du genau diesen Ablauf für jede typische Vorfallart – mit Checklisten, Mailvorlagen, Urkunde & Badge. Empfehlung: zwei Ersthelfer je Betrieb. Anmeldung & Termine: info@secumetrix.de

Grenzen dieses Whitepapers: Es vermittelt allgemeines Wissen und ersetzt keine Rechtsberatung, keine technische Einzelfallprüfung und keine Versicherungszusage. Die Bewertung eines konkreten Vorfalls, die verbindliche rechtliche Einordnung und die Entscheidung über Versicherungsschutz erfordern die Prüfung des Einzelfalls. Führe nur Maßnahmen aus, für die du im Betrieb beauftragt und eingewiesen bist.