QUANSATECH IT

ERSTE SCHRITTE FÜR UNTERNEHMEN

IT-Notfall: die ersten 30 Minuten richtig handeln

Für Geschäftsführung und interne Ansprechpartner bei Ransomware, Hackerangriff, verdächtigen Anmeldungen oder einem kritischen IT-Ausfall. Die Checkliste hilft, Schaden zu begrenzen und spätere Entscheidungen nicht durch übereilte Eingriffe zu erschweren.

Grundregel: Betroffene Systeme vom Netzwerk trennen, aber nichts löschen, neu installieren oder vorschnell aus einer Sicherung zurückspielen. Für weitere Kommunikation möglichst ein sauberes, unabhängiges Gerät nutzen.

Sofort - in den ersten 10 Minuten

Ziel: Ausbreitung bremsen, Kontrolle herstellen und einen nachvollziehbaren Ausgangspunkt sichern.

- [ ] Auffällige Computer, Server oder Geräte vom Netzwerk trennen: LAN-Kabel abziehen sowie WLAN und VPN deaktivieren. Nicht wieder verbinden.
- [ ] Bei mehreren betroffenen Systemen den betroffenen Netzwerkbereich oder Fernzugang gemeinsam mit der IT eingrenzen.
- [ ] Eine Person koordiniert. Uhrzeit, erste Auffälligkeit, betroffene Geräte, Benutzer und bereits gesetzte Schritte werden laufend notiert.
- [ ] Für Telefonate und Nachrichten ein sauberes Gerät verwenden. Firmen-E-Mail kann bei einem Angriff mitgelesen werden.
- [ ] Auf verdächtigen Systemen keine Administrator-Zugänge eingeben, keine Anhänge öffnen und keine unbekannten Warnfenster bestätigen.

Danach - bis Minute 30

Ziel: Belege erhalten, die wichtigsten Geschäftsabläufe schützen und fachliche Hilfe arbeitsfähig machen.

- [ ] Fehlermeldungen, Erpressungstext, ungewöhnliche Anmeldungen und sichtbare Änderungen fotografieren oder als Screenshot sichern.
- [ ] Protokolle, Sicherheitsmeldungen, verdächtige E-Mails samt Kopfzeilen und bekannte Uhrzeiten aufbewahren. Keine Bereinigung starten.
- [ ] Mitarbeitende kurz anweisen: betroffene Geräte nicht neu starten, nicht weiterarbeiten und keine unkoordinierten Nachrichten versenden.
- [ ] Kritische Abläufe benennen: Was muss heute weitergehen, was darf warten und welche saubere Zwischenlösung ist vorhanden?
- [ ] IT-Betreuer oder Incident-Response-Hilfe verständigen. Falls vorhanden, auch Cyberversicherung und interne Datenschutzverantwortliche früh einbinden.

Nicht blind ausschalten: Ein ungeplanter Neustart oder das Trennen vom Strom kann flüchtige Spuren verlieren lassen. Betroffene Systeme zuerst vom Netzwerk isolieren und das weitere Vorgehen abstimmen. Bei Brand-, Strom- oder Personengefahr hat die Sicherheit selbstverständlich Vorrang.

Kurzes Vorfallprotokoll

Beginn / entdeckt um		**Koordination**	
Betroffene Systeme		**Erstes sichtbares Zeichen**	
Getrennt / gesperrt um		**Letzter bekannter Normalzustand**	
Interne / externe Kontakte		**Nächste Entscheidung um**	

QUANSATECH IT

ERSTE STUNDEN UND WIEDERANLAUF

Geordnet prüfen, melden und wiederherstellen

Sobald die unmittelbare Ausbreitung gebremst ist, werden Umfang, Geschäftsauswirkung und Wiederherstellungsweg geklärt. Jede Maßnahme bleibt mit Uhrzeit und verantwortlicher Person dokumentiert.

In den ersten Stunden

Ziel: saubere Entscheidungsgrundlagen schaffen, ohne Beweise oder Sicherungen zu gefährden.

- [ ] Umfang bestimmen: betroffene Konten, Geräte, Standorte, Cloud-Dienste, Partnerzugänge und möglicherweise abgeflossene Daten.
- [ ] Wichtige Kennwörter und aktive Sitzungen von einem sauberen Gerät aus zurücksetzen. Zuerst Administratoren, E-Mail, VPN und Cloud-Zugänge.
- [ ] Sicherungen schützen und den letzten glaubhaft sauberen Stand feststellen. Sicherungsmedien nicht unkontrolliert mit der betroffenen Umgebung verbinden.
- [ ] Kunden, Lieferanten oder Mitarbeitende nur mit bestätigten Fakten informieren. Eine Person koordiniert die externe Kommunikation.
- [ ] Alle Entscheidungen, Beteiligten, Belege und Wiederherstellungsschritte in einem zentralen Vorfallprotokoll festhalten.

Meldewege und rechtliche Prüfung

Datenschutz prüfen	Strafanzeige	CERT.at
Sind personenbezogene Daten betroffen, Risiko und Meldepflicht sofort fachlich prüfen. Eine meldepflichtige Verletzung ist der Datenschutzbehörde unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden zu melden.	Eine formelle Anzeige wird bei einer Polizeidienststelle erstattet. Die Cybercrime-Meldestelle des Bundeskriminalamts dient für Hinweise und Fragen, ersetzt aber keine Anzeige.	CERT.at nimmt freiwillige Meldungen zu IT-Sicherheitsvorfällen entgegen und koordiniert bei Bedarf. Die Stelle ist kein allgemeiner Endkunden-Helpdesk.

Vor dem Wiederanlauf

Wiederherstellen erst, wenn Ursache und Zugänge ausreichend unter Kontrolle sind.

- [ ] Angriffsweg oder technische Ursache ist soweit möglich geklärt und geschlossen.
- [ ] Missbrauchte oder gefährdete Konten, Schlüssel und Fernzugänge sind gesperrt oder erneuert.
- [ ] Verwendete Sicherung ist geprüft, vom betroffenen System getrennt und zeitlich plausibel sauber.
- [ ] Updates, Schutzmaßnahmen und Protokollierung sind aktiv, bevor Systeme wieder produktiv verbunden werden.
- [ ] Verantwortliche Person gibt den Wiederanlauf frei; erhöhte Überwachung und Nachkontrolle sind vereinbart.

Offizielle Grundlagen: CERT.at - Vorfall melden | Österreichische Datenschutzbehörde - Data Breach | Bundeskriminalamt - Cybercrime | BSI - Ransomware-Erste-Hilfe

Allgemeine Orientierung, keine Rechtsberatung. Meldepflichten, Beweissicherung und Wiederanlauf immer anhand des konkreten Vorfalls prüfen.