IT-Notfall – Ihr Wegweiser für den Ernstfall

Handout für Unternehmer im Mittelstand

Kunde / Unternehmen: _____

Datum des Vorfalls: _____

Dokument erstellt durch: _____

1. SOFORT-CHECK – WAS IST PASSIERT?

1.1. Ereignis erfassen

Bitte kreuzen Sie an, was zutrifft. Nur das, was Sie sicher wissen.

☐ Ransomware / Verschlüsselung von Daten
☐ Systemausfall (Server, Netzwerk, Cloud-Dienste)
☐ Datenverlust (versehentlich gelöscht oder durch Angriff)
☐ Unklare Sicherheitslage (verdächtige Aktivitäten, unbekannte Zugriffe)
☐ Sonstiges: _____

1.2. Zeitpunkt und Entdeckung

- Erstmals aufgetreten am: _____ um: _____ Uhr
- Erstmals bemerkt durch (Name, Rolle): _____
- Aktuell verantwortliche Person (Name, direkte Durchwahl):

  _____ Telefon: _____

1.3. Brandherd lokalisieren

- Wo trat das Problem zuerst auf? (Standort, Abteilung, System):

  _____

- Ist der Vorfall isoliert oder breitflächig?

  ☐ Einzelplatz
  ☐ Abteilung
  ☐ Standort
  ☐ Unternehmensweit
  ☐ Unbekannt

2. BETEILIGTE / BEREITS ERGRIFFENE MAßNAHMEN

2.1. Wer ist betroffen oder muss informiert werden?

Rolle / Bereich	Name / Kontakt	Bereits informiert?	Bemerkung
Direkt betroffener Mitarbeiter / Abteilung	_____	◯ Ja ◯ Nein	_____
Interne IT (Administrator, IT-Leitung)	_____	◯ Ja ◯ Nein	_____
Externe IT-Dienstleister (Compose IT oder andere)	_____	◯ Ja ◯ Nein	_____
Datenschutzbeauftragter (DSB)	_____	◯ Ja ◯ Nein	_____
Geschäftsleitung / Aufsichtsrat	_____	◯ Ja ◯ Nein	_____
Kunden / Lieferanten (potenziell betroffen)	_____	◯ Ja ◯ Nein	_____
Versicherung (Cyber-Police vorhanden?)	_____	◯ Ja ◯ Nein	_____

2.2. Bereits durchgeführte Maßnahmen

Maßnahme	Zeitpunkt	War sie erfolgreich?
Betroffene Systeme vom Netzwerk getrennt	_____	◯ Ja ◯ Nein ◯ Unklar
Backup geprüft oder eingespielt	_____	◯ Ja ◯ Nein ◯ Unklar
Passwort-Reset für betroffene Accounts	_____	◯ Ja ◯ Nein ◯ Unklar
Externe Hilfe kontaktiert (wer?)	_____	◯ Ja ◯ Nein ◯ Unklar
Sonstiges	_____	◯ Ja ◯ Nein ◯ Unklar

2.3. Hinweis zur Kommunikationssicherheit

Wenn E-Mail-Systeme von dem Vorfall betroffen sein könnten:

☐ E-Mail-Kommunikation gilt aktuell als **NICHT** sicher

→ Bitte nutzen Sie für den weiteren Austausch alternative Kontaktwege (Telefon, verschlüsselte Messenger).

3. WAS SOLL COMPOSE IT FÜR SIE TUN?

3.1. Auftragsinformationen

Definieren Sie hier priorisiert, was Compose IT für Sie erreichen soll.

Beispiele: Systeme isolieren, Daten retten, Betriebsfähigkeit wiederherstellen, forensische Spuren sichern.

_____

_____

_____

3.2. Verfügbarkeit von Sicherheitskopien

Existiert eine vom Auftraggeber erstellte, verlässliche Sicherheitskopie?

◯ Ja

- Ort / Medium (Onsite, Cloud, Band, extern): _____
- Letzte erfolgreiche Sicherung: _____
- Verantwortlicher für Backups: _____ (Name, Kontakt)

◯ Nein

◯ Unklar – muss durch Compose IT geprüft werden

Hinweis: Auch ältere Backups können im Ernstfall wertvoll sein. Bitte löschen Sie nichts, bevor wir nicht gemeinsam darüber gesprochen haben.

3.3. Ansprechpartner für den Einsatz

Bitte vollständig ausfüllen. Diese Personen sind während des Einsatzes für uns erreichbar.

Rolle	Name	Telefon (direkt)	E-Mail	E-Mail aktuell unsicher?
Hauptansprechpartner (Entscheider)	_____	_____	_____	☐ Ja
Technischer Kontakt (vor Ort)	_____	_____	_____	☐ Ja
Datenschutzbeauftragter	_____	_____	_____	☐ Ja
Geschäftsleitung	_____	_____	_____	☐ Ja
Compose IT Support (Standardkontakt)	Compose IT Team	(0661) 97 77 12-0	support@compose-it.de	☐ Ja

Hinweis: Wenn Sie "E-Mail aktuell unsicher" ankreuzen, kommunizieren wir ausschließlich über alternative, abgesicherte Kanäle.

4. EXTERNE MELDESTELLEN UND NÄCHSTE SCHRITTE

4.1. Offizielle Kontaktstellen im Überblick

Stelle	Wann kontaktieren?	Kontakt / Hinweis
Polizei (Zentrale Anlaufstelle Cybercrime)	Bei Straftatverdacht, Erpressung, Datenabfluss	https://www.polizei-beratung.de
BSI (Bundesamt für Sicherheit in der Informationstechnik)	Bei schwerwiegenden IT-Vorfällen, insbesondere für KRITIS-Betreiber	https://www.bsi.bund.de/meldeportal
Landeskriminalamt (LKA)	Wenn länderbezogene Ermittlungen relevant sind oder die Polizei dies empfiehlt	Über die örtliche Polizeidienststelle oder https://www.bka.de
Zuständige Datenschutzaufsichtsbehörde	Bei Verlust oder unbefugter Offenlegung personenbezogener Daten (DSGVO)	https://www.bfdi.bund.de (Übersicht der Landesbehörden)
Versicherung	Bei bestehender Cyber-Police oder bei Haftungsfragen	Prüfen Sie Ihre Police oder kontaktieren Sie Ihren Versicherer

4.2. Kunden oder Lieferanten kontaktieren?

◯ Ja, weil: _____

◯ Nein, weil: _____

◯ Entscheidung steht aus – prüfen bis: _____

4.3. Nach dem akuten Vorfall

Dieses Dokument haben Sie ausgefüllt und an Compose IT übergeben. Im weiteren Vorgehen:

- Wir analysieren die Lage und priorisieren Maßnahmen gemeinsam mit Ihnen.
- Wir handeln transparent, dokumentiert und mit Ihrem Einverständnis.
- Wir begleiten Sie bei der Aufarbeitung und der Prävention künftiger Vorfälle.

Hinweis: Nachhaltige IT-Sicherheit entsteht durch Vorbereitung. Wenn Sie möchten, sprechen wir im Anschluss gerne über Maßnahmen, die solche Vorfälle künftig verhindern oder abmildern.

Rechtlicher Hinweis
Dieses Dokument dient der ersten Orientierung im IT-Notfall. Es begründet kein Dienstleistungsverhältnis. Eine Haftung für die Vollständigkeit der Angaben oder den Erfolg von Maßnahmen wird ausgeschlossen. Im Zweifel gilt: Ruhe bewahren, sorgfältig dokumentieren und Fachhilfe hinzuziehen.

Compose IT
FI Services GmbH

Rabanusstraße 36
36037 Fulda

Telefon: (0661) 97 77 12-0
E-Mail: support@compose-it.de
Web: https://compose-it.de