IT-Notfallmanagement
für den Mittelstand (KMU)

→ 1. SCHUTZMASSNAHMEN

Die nachfolgenden Trennpunkte sollten umgesetzt werden, um auf einen IT-Notfall vorbereitet zu sein:

- Bestimmung eines IT-Sicherheitsbeauftragten zur Steuerung des Notfallmanagements
- Erstellung eines Notfallkonzeptes mit Verantwortlichen, Alarmierungs- und Meldewegen
- Identifizierung von kritischen Geschäftsprozessen und Vermögenswerten und Bestimmung von Erstmaßnahmen
- Erstellung einer Liste mit Ansprechpartnern und deren Kontaktdaten
- Abstimmung der Möglichkeiten des IT-Dienstleisters bei auftretenden IT-Vorfällen zu unterstützen.
- Festlegung von Kommunikationswegen zur Information von betroffenen Behörden und der Medien
- Identifizierung und Beauftragung von IT-Dienstleistern oder Sachverständigen, die auf die Bewältigung von IT-Vorfällen spezialisiert sind.
- Implementierung von datenschutzgerechten Überwachungsmaßnahmen für wichtige IT-Ressourcen
- Auditieren und Testen der erarbeiteten IT-Notfallkonzepte
- Überprüfung der IT-Infrastruktur und Organisation bezüglich Angreifbarkeit
- Schulung und Sensibilisierung aller Mitarbeiter zu Datenschutz und Datensicherheit
- Regelmäßige und zeitnahe Installation von Sicherheits-Updates
- Installation von aktueller Antiviren- und Schutzsoftware
- Einsatz von Firewalls und Einschränkung des Netzwerkverkehrs
- Änderung von Hersteller-Passwörtern und Nutzung komplexer Passwörter
- Regelmäßige Erstellung von Sicherheitskopien und Test der Wiederherstellbarkeit der Daten
- Erstellung von Berechtigungskonzepten und Genehmigungsprozessen zur Rechtevergabe
- Erstellung von verbindlichen IT-Sicherheitsrichtlinien und Arbeitsanweisungen für alle Mitarbeiter
- Segmentierung von Netzwerken nach Zweck und nach Bedarf
- Einsatz von VPN- und Verschlüsselungsverfahren bezüglich Remotearbeit
- Definition von Verantwortlichkeiten und Meldewegen hinsichtlich gesetzlicher Meldepflichten (Datenschutz, KRITIS etc.).

→ 2. ACHTSAMKEIT

Folgende Punkte sollten Beachtung finden, um einen IT-Notfall entgegnen zu können:

- Überwachung vergeblicher Anmeldeversuche auf IT-Systeme
- Überprüfung der Gültigkeit von Sicherheitszertifikaten und dem Sicherheitsstatus von IT-Systemen
- Überwachung von auffälligen Zugriffen und Kopiervorgängen im Netzwerk
- Sicherstellung, dass Mitarbeiter die IT-Sicherheitsrichtlinien und Meldewege für IT-Notfälle kennen.
- Sicherstellung der Verfügbarkeit und Erreichbarkeit aller erforderlichen Personen für den Notfall

→ 3. NOTFALLBEARBEITUNG

Zur Bewältigung eines IT-Notfalls sind die nachfolgenden Punkte zu beachten:

- Kontaktaufnahme zu allen vordefinierten und hilfreichen Ansprechpartnern
- Befragen der betroffenen Nutzer und genaue Dokumentation der Vorkommnisse
- Kontaktaufnahme zu IT-Dienstleistern und Sachverständigen, die zur Bewältigung des IT-Notfalls beitragen können.
- Auswertung, Sammlung und Sicherung von Systemprotokollen, Logdateien usw.
- Dokumentation aller Sachverhalte, die mit dem IT-Notfall in Zusammenhang stehen.
- Kontaktaufnahme bzw. Meldung an Staatsanwaltschaft, Polizei und Aufsichtsbehörden
- Ermittlung und Analyse der betroffenen Datensätze
- Information an die betroffenen Personen zu Zwecken der Schadensbegrenzung
- Meldung an Behörden wie Verfassungsschutz oder MAD, sofern es sich um Daten handelt, die dem Geheimschutz unterliegen.
- Strikte Beachtung der Meldepflichten und -fristen.

→ 4. NACHBEREITUNG

Jeder IT-Notfall muss analysiert und nachbearbeitet werden, hierzu sind folgende Punkte zu beachten:

- Untersuchung und Schließung der Schwachstellen und Sicherheitslücken, durch die es zum IT-Notfall gekommen ist.
- Besonders gründliche Überwachung von Netzwerk und IT-Systemen bezüglich weiterer ungewöhnlicher Aktivitäten
- Gründliche Überprüfung aller Sicherheits-Maßnahmen auf Aktualität und Wirksamkeit
- Sofern erforderlich, Anpassung der IT-Sicherheitsrichtlinie, bestehender Prozesse und Arbeitsanweisungen
- Anpassung der Dokumentationen zum Notfallmanagement, sofern erforderlich.
- Ermittlung und Beauftragung weiterer Dienstleister, sofern die aktuell eingesetzten den IT-Notfall nicht vollumfänglich aufklären konnten.

Rufen Sie uns an –
wir beraten Sie gerne.



IHR STARKER IT-PARTNER

tec4net GmbH | Lohenstraße 13 | 82166 Gräfelfing | T +49 89 54 04 36 30 | info@tec4net.com | **www.tec4net.com**