PRAXISNAH
VERSTÄNDLICH
UMSETZBAR

IT-SICHERHEIT
VERSTÄNDLICH ERKLÄRT

PRAXISLEITFADEN

Umfassender Leitfaden
für Privatnutzer,
Selbstständige und
kleine Unternehmen

Schützen
Ihre Daten, Geräte
und Identität

Verstehen
Risiken, Angriffe und
Schwachstellen

Sichern
Backups, Passwörter
und wichtige Inhalte

Handeln
Praktische Schritt-für-Schritt-
Anleitungen und Checklisten

PRAKTISCH.
AKTUELL.
ALLTAGSTAUGLICH.

- 10 wichtigste Maßnahmen
- Phishing & Ransomware schützen
- Backups richtig umsetzen
- Netzwerk und Geräte absichern
- Checklisten und Quick Wins

IT-Sicherheitsvorfall
Notfallcheckliste

Inhalt

1) Notfallcheckliste IT Sicherheitsvorfall

1.1 Sofortmaßnahmen bei Sicherheitsvorfällen

Allgemeine Erstreaktion

Prüfpunkte	erledigt
Ruhe bewahren und Vorfall dokumentieren	☐
Zeitpunkt des Vorfalls festhalten	☐
Betroffene Systeme identifizieren	☐
Verantwortliche informieren	☐
Incident-Response-Team aktivieren	☐

Eindämmung

Prüfpunkte	erledigt
Betroffene Systeme isolieren	☐
Netzwerkverbindungen trennen	☐
Verdächtige Benutzerkonten sperren	☐
Externe Zugriffe deaktivieren	☐
Schadsoftware-Ausbreitung verhindern	☐

Beweissicherung

Prüfpunkte	erledigt
Logdateien sichern	☐
Screenshots erstellen	☐
Speicherabbilder sichern (wenn erforderlich)	☐
Keine unnötigen Neustarts durchführen	☐
Änderungen dokumentieren	☐

1.2 Ransomware-Notfallcheckliste

Erkennung

Prüfpunkte	erledigt
Ungewöhnliche Verschlüsselungen erkannt	☐
Lösegeldforderung dokumentiert	☐
Betroffene Systeme identifiziert	☐

Sofortmaßnahmen

Prüfpunkte	erledigt
Systeme sofort vom Netzwerk trennen	☐
WLAN deaktivieren	☐
Gemeinsame Laufwerke trennen	☐
Backup-Systeme isolieren	☐
Administratorzugänge prüfen	☐

Kommunikation

Prüfpunkte	erledigt
Geschäftsführung informieren	☐
Datenschutzbeauftragten informieren	☐
CERT/IT-Dienstleister kontaktieren	☐
Mitarbeiter warnen	☐

Wiederherstellung

Prüfpunkte	erledigt
Ursache analysieren	☐
Systeme neu aufsetzen	☐
Backups prüfen	☐
Datenwiederherstellung testen	☐
Schwachstelle schließen	☐

1.3 Phishing-/Business-E-Mail-Compromise (BEC)

Prüfung

Prüfpunkte	erledigt
Verdächtige E-Mail sichern	☐
Header analysieren	☐
Links und Anhänge isoliert prüfen	☐
Betroffene Benutzer identifizieren	☐

Maßnahmen

Prüfpunkte	erledigt
Passwortänderung erzwingen	☐
MFA aktivieren oder zurücksetzen	☐
Session-Tokens invalidieren	☐
Mail-Regeln prüfen	☐
Kontoaktivitäten analysieren	☐

Kommunikation

Prüfpunkte	erledigt
Interne Warnung versenden	☐
Kunden/Lieferanten informieren (falls nötig)	☐

1.4 Datenverlust / Datenschutzvorfall

Sofortmaßnahmen

Prüfpunkte	erledigt
Betroffene Daten identifizieren	☐
Umfang des Datenabflusses bewerten	☐
Zugriff stoppen	☐
Systeme absichern	☐

DSGVO-relevante Schritte

Prüfpunkte	erledigt
Datenschutzbeauftragten informieren	☐
Risiko für Betroffene bewerten	☐
Meldepflicht prüfen	☐
72h-Frist dokumentieren	☐
Behördenmeldung vorbereiten	☐
Betroffene informieren (falls erforderlich)	☐

1.5 Server- oder Systemausfall

Analyse

Prüfpunkte	erledigt
Ursache identifizieren	☐
Hardwarefehler prüfen	☐
Netzwerk prüfen	☐
Stromversorgung prüfen	☐
Logs analysieren	☐

Wiederherstellung

Prüfpunkte	erledigt
Failover aktivieren	☐
Systeme priorisieren	☐
Backup-Restore durchführen	☐
Funktionstests durchführen	☐
Monitoring aktivieren	☐

1.6 Netzwerkvorfall

Sofortmaßnahmen

Prüfpunkte	erledigt
Betroffene Segmente isolieren	☐
Firewall-Regeln prüfen	☐
Verdächtigen Traffic blockieren	☐
VPN-Verbindungen kontrollieren	☐

Analyse

Prüfpunkte	erledigt
IDS/IPS-Meldungen prüfen	☐
Netzwerklogs sichern	☐
Angriffsvektor identifizieren	☐

1.7 Insider-Vorfall

Sofortmaßnahmen

Prüfpunkte	erledigt
Benutzerkonto sperren	☐
Zugriffsrechte entziehen	☐
Geräte sichern	☐
Aktivitäten protokollieren	☐

Untersuchung

Prüfpunkte	erledigt
Zugriffshistorie analysieren	☐
Datenbewegungen prüfen	☐
Kommunikationsdaten sichern	☐

1.8 Kommunikationscheckliste

Intern

Prüfpunkte	erledigt
Geschäftsführung informiert	☐
IT-Abteilung informiert	☐
Datenschutzbeauftragter informiert	☐
Fachbereiche informiert	☐
Helpdesk vorbereitet	☐

Extern

Prüfpunkte	erledigt
Kundeninformation vorbereitet	☐
Lieferanten informiert	☐
Behörden informiert	☐
Pressekommunikation abgestimmt	☐
Cyberversicherung kontaktiert	☐

1.9 Wiederanlaufcheckliste

Vor Wiederinbetriebnahme

Prüfpunkte	erledigt
Ursache beseitigt	☐
Systeme gepatcht	☐
Malware-Scan durchgeführt	☐
Passwörter geändert	☐
Sicherheitslücken geschlossen	☐

Nach Wiederinbetriebnahme

Prüfpunkte	erledigt
Monitoring intensiviert	☐
Funktionstests abgeschlossen	☐
Benutzer informiert	☐
Vorfall dokumentiert	☐
Lessons Learned durchgeführt	☐

1.10 Notfallkontakte

Funktion	Name	Telefon	E-Mail
IT-Leitung			
ISB / CISO			
Datenschutzbeauftragter			
Geschäftsführung			
CERT / Dienstleister			
Cyberversicherung			
Strafverfolgung			

1.11 Kritische Systeme & Prioritäten

System	Kritikalität	Verantwortlich	Wiederanlaufziel
ERP	Hoch		
E-Mail	Hoch		
File-server	Hoch		
Backup	Kritisch		
VPN	Mittel		

1.12 Abschlussbewertung nach Vorfall

Prüfpunkte	erledigt
Ursache identifiziert	☐
Sicherheitsmaßnahmen verbessert	☐
Prozesse angepasst	☐
Mitarbeiterschulung durchgeführt	☐
Bericht erstellt	☐
Managementreview durchgeführt	☐
Versicherungsfall abgeschlossen	☐
Dokumentation archiviert	☐

1.13 Freigabe und Revision

Rolle	Name	Datum	Unterschrift
Erstellt durch			
Geprüft durch			
Freigegeben durch			

Hinweise

Diese Checkliste dient als organisatorische und technische Mindestanforderung für den IT Sicherheitsvorfall im Rahmen eines Informationssicherheitsmanagementsystems (ISMS). Die konkreten Anforderungen sind an Schutzbedarf, Unternehmensgröße sowie regulatorische Vorgaben anzupassen.

2) Impressum

Herausgeber:
MINCOM GmbH
Unterhachinger Straße 55
85521 Ottobrunn
www.mincom.de

Geschäftsleitung:
Dr. Rainer Wittmann