CYBERANGRIFF - SOFORTPLAN

Checkliste für die ersten Minuten nach der Entdeckung

WK IT
WE KNOW IT

WICHTIG: Nicht ausschalten, nicht löschen, nicht neu installieren. Betroffene Systeme kontrolliert isolieren - bei akuter Gefahr nur nach Freigabe durch IT/Security herunterfahren.

1. SOFORT HANDELN

1. Lage aufnehmen, Krisenteam aktivieren

- ☐ IT/Security, IT-Leitung und Geschäftsführung informieren.
- ☐ Incident Lead benennen; Krisenteam aktivieren: IT, Management, Datenschutz, Recht, Kommunikation.
- ☐ Uhrzeit, Melder, betroffene Systeme, Symptome und erste Entscheidungen dokumentieren.

2. Eindämmen - ohne Spuren zu zerstören

- ☐ Betroffene Geräte kontrolliert isolieren: LAN trennen, WLAN deaktivieren, aber nicht neu starten.
- ☐ Kompromittierte Konten, VPN-, Admin-, Cloud- und Dienstleisterzugänge sperren; Sessions, Tokens und API-Keys widerrufen.
- ☐ Backups vor Veränderung schützen: Schreibzugriffe stoppen, immutable/offline Kopien prüfen.

3. Beweise und Logs sichern

- ☐ Screenshots, Erpressernotizen, verdächtige E-Mails und Warnmeldungen sichern.
- ☐ Kurzlebige Logs sofort exportieren: EDR/SIEM, Firewall, VPN, E-Mail, Cloud, Identity Provider, DNS/Proxy, Server.
- ☐ Originaldaten nicht verändern; Sicherung, Verantwortliche und Zeitpunkte dokumentieren.

4. Umfang und Risiko bewerten

- ☐ Was ist betroffen: Systeme, Daten, Standorte, Benutzer, Partner, Dienstleister?
- ☐ Gibt es Datenabfluss, Ransomware, Zahlungsbetrug oder Betriebsausfall?
- ☐ Sind personenbezogene Daten, regulierte Bereiche oder vertragliche Meldepflichten betroffen?

2. MELDEPFLICHT PRÜFEN

SOFORT

Bei Straftat, Erpressung, Betrug, Datenabfluss: Polizei/ZAC einbinden. Cyberversicherung gemäss Police informieren

24h

BSI/NIS2, **falls** Unternehmen **meldepflichtig** ist. Bei schwerem Sicherheitsvorfall: Erstmeldung über BSI-Portal/MIP.

72h

DSGVO prüfen: personenbezogene Daten betroffen und Risiko für Betroffene? Datenschutzaufsicht informieren.

FORTLAUFEND

Folgemeldungen, Updates, Betroffeneninformation, Abschlussbericht mit Recht/Datenschutz abstimmen.

3. ZENTRALE KONTAKTE

BSI / IT-SICHERHEIT

Tel.	0800 274 1000
E-Mail	service-center@bsi.bund.de
Adresse	Godesberger Allee 87, 53175 Bonn
WEB	mip.bsi.bund.de / BSI-Portal

POLIZEI / ZAC*

Jedes Bundesland hat eine eigene zentrale Ansprechstelle für Unternehmen und Behörden. Die Liste findet sich unter:

WEB	polizei.de/zac
Hinweis bei	Straftat/Erpressung/Betrug

*Zentrale Ansprechstelle Cybercrime

CYBERANGRIFF - RECOVERYPLAN

Was nach der Sofortphase passieren muss

WK IT
WE KNOW IT

4. NICHT VERGESSEN

- ☐ Keine Backups ungeprüft zurückspielen.
- ☐ Keine Systeme produktiv nehmen, solange Eintrittsweg, Persistenzen und Kontenrisiko nicht bewertet sind.
- ☐ Keine Täterkommunikation, Zahlung, Zusage oder Verhandlung ohne Krisenteam, Geschäftsführung, Recht, Versicherung und ggf. Behörden.
- ☐ Keine öffentlichen Aussagen ohne Freigabe.

5. WIEDERHERSTELLEN

1. Lagebild und Freigabe

Incident Lead koordiniert. Prioritäten,Business Impact, RTO/RPO, Systemabhängigkeiten und Go-/No-Go-Kriterien klären.

2. Eintrittsweg eingrenzen

Phishing, VPN, Patchlücke, RDP, Dienstleisterzugang sowie Cloud, API-Keys, Tokens und Mail-Regeln prüfen.

3. Konten bereinigen

Identity Provider, Admin-Konten, Servicekonten, MFA, Tokens, Sessions, Cloud-Rollen und externe Zugänge sichern.

4. Systeme härten

Patches, EDR, Firewall-Regeln, Segmentierung, Logging. Persistenzen entfernen: Backdoors, Tasks, Webshells, Remote-Tools, neue Konten.

5. Backups prüfen

Integrität, Malwarefreiheit und Wiederherstellbarkeit testen. Keine ungeprüften Backups produktiv zurückspielen.

6. Betrieb starten

Kritische Prozesse zuerst. Produktivsetzung nur mit Freigabe; engmaschiges Monitoring, Rückfallplan und Abschluss-dokumentation aktivieren.

6. KOMMUNIKATION

- ☐ Zentrale Sprecherrolle festlegen; Incident Lead und Geschäftsführung stimmen Botschaften ab.
- ☐ Mitarbeitende erhalten klare System- und Verhaltensanweisungen.
- ☐ Alternative Kanäle vorbereiten, falls E-Mail, Teams, Telefonanlage, Intranet nicht vertrauenswürdig sind.
- ☐ Kunden, Partner und Dienstleister nur mit Fakten informieren; vertragliche Meldepflichten prüfen.
- ☐ Presse, Öffentlichkeit, Social Media nur nach Freigabe durch Geschäftsführung und Recht informieren
- ☐ Bei personenbezogenen Daten prüfen, ob betroffene Personen informiert werden müssen.

7. NOTFALLKONTAKTE

Rolle	Name	Telefon	E-Mail / Notfallkanal
IT-Security			
Geschäftsführung			
Datenschutz/Recht			
Cyberversicherung			