



BE SAFE!

CYBER CRIME. BE SAFE!

DER OPTIMALE KOMPLETTSCHUTZ!

CYBER CRIME. VERSICHERUNG.
KRISENMANAGEMENTPLAN.

CYBER CRIME. KRISENMANAGEMENTPLAN.

Das vorliegende Dokument unterstützt Sie bei der Behandlung von Cyber-Krisen und kann als Anleitung zum Cyber-Krisenmanagement genutzt werden. Eine Cyber-Krise liegt vor, wenn mindestens eine der folgenden Fragen mit "ja" beantwortet werden muss:

Ein IT-Ausfall ist existenzbedrohend oder stört den Geschäftsbetrieb erheblich. ja nein

Ein schwerwiegender Hackerangriff ist erfolgt. ja nein

Ein schwerwiegender IT-basierter Betrugs-/Erpressungsfall ist aufgetreten. ja nein

Vertrauliche Daten sind abgeflossen. ja nein

Reputationsschäden durch Negativnachrichten sind zu erwarten. ja nein

Es wurde ein meldepflichtiger Gesetzesverstoß begangen. ja nein

Bei Vorliegen einer Cyber-Krise - auch nur im Verdachtsfall - informieren Sie bitte für technische Maßnahmen und zur Unterstützung bei der Krisenkommunikation umgehend die Hotline des Sicherheitsberaters ACCENTURE unter:

DE +49 800 7235192

Bitte unterstützen Sie unsere Experten dabei die Lage zu analysieren, indem Sie Personen mit IT-Fachkunde (IT-Dienstleister oder interne IT-Verantwortliche) als Ansprechpartner für Accenture benennen. Des Weiteren benötigen wir für die Kommunikation mit XL Insurance Company SE Ihre Versicherungsscheinnummer.

Versicherungsscheinnummer: _____

„HINWEISE ZUM DOKUMENT“:

Eine digitale Version dieses Planes zur weiteren Bearbeitung erhalten Sie per Anfrage über die folgende Adresse: cyber@apml.de

Das fertig bearbeitete Dokument sollte an einer sicheren Stelle redundant in elektronischer und gedruckter Form aufbewahrt werden.

DIGITAL 1. Ablageort _____ 2. Ablageort _____

GEDRUCKT 1. Ablageort _____ 2. Ablageort _____

CYBER CRIME. KRISENMANAGEMENTPLAN.

„EREIGNISBEWÄLTIGUNG“:

Die folgende Checkliste unterstützt Sie bei der Ergreifung von Sofortmaßnahmen, nachdem Sie einen Schaden erkannt haben.

Checkliste Sofortmaßnahmen Mitarbeiterinnen und Mitarbeiter

- | | | |
|---------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------|
| Beenden der unerwünschten Verbindungen oder Prozesse auf dem betroffenen System | <input type="radio"/> ja | <input type="radio"/> nein |
| Trennen der Verbindung der betroffenen Systeme zum Internet oder sonstigen Netzwerken | <input type="radio"/> ja | <input type="radio"/> nein |
| Gegebenenfalls ausschalten der betroffenen Systeme | <input type="radio"/> ja | <input type="radio"/> nein |
| Betroffenes System NICHT erneut starten, bevor nicht eindeutig klar ist, dass dadurch nicht weiterer Schaden erzeugt wird | <input type="radio"/> ja | <input type="radio"/> nein |
| Zusammenfassen der bekannten Fakten für die Kontaktaufnahme mit Accenture | <input type="radio"/> ja | <input type="radio"/> nein |
| Kontaktaufnahme mit Accenture: DE +49 800 7235192 | <input type="radio"/> ja | <input type="radio"/> nein |
| Nehmen Sie ggf. Kontakt mit der Polizei auf. | <input type="radio"/> ja | <input type="radio"/> nein |

„KRISENKOMMUNIKATION“:

Die goldenen Regeln der Krisenkommunikation

- One voice policy: Mit einer Stimme sprechen. Nur die Geschäftsführung bzw. Krisenstabsleitung sollte nach außen kommunizieren. In jeden Fall gibt die Geschäftsführung bzw. Krisenstabsleitung die Kommunikationsstrategie für alle Beschäftigten vor.
- Formulieren Sie aktiv, eindeutig und positiv.
- Kommunizieren Sie abgesicherte Fakten und auf keinen Fall Unwahrheiten.
- Erzählen Sie offen und ehrlich - aber nicht alles.
- Zeigen Sie Verständnis für Ärger oder Ängste betroffener Personen.
- Lassen Sie sich nicht unter Druck setzen.
- Unterlassen Sie Schuldzuweisungen.

CYBER CRIME. KRISENMANAGEMENTPLAN.

„ANHANG A CHECKLISTE IT-VERANTWORTLICHER / IT-DIENSTLEISTER“:

Um eine möglichst schnelle und zielgerechte Hilfe durch Accenture sicherzustellen, sollte die folgende Checkliste vor der Kontaktaufnahme durch eine/n IT-Verantwortliche/n oder den IT-Dienstleister ausgefüllt werden.

Allgemeine Angaben

- Wann und durch wen wurde der Vorfall gemeldet?
- Beschreibung des Ausfalls / der Störung
- Vermutete Auswirkungen

UMFANG DES IT-AUSFALLS / DER IT-STÖRUNG

1. Betroffene Systeme / Festplatten:

Desktop-Systeme / Welche: _____ ja nein

Laptop- / Notebook Systeme / Welche: _____ ja nein

Wechselmedien (USB, Flash, SD, ...) / Welche: _____ ja nein

Serversysteme / Welche: _____ ja nein

Ermittlung der Rahmenbedingungen für betroffene Festplatten
(Größe, Anschlussart, RAID-Einbindung, Verschlüsselung) ja nein

2. Betroffene Software:

Betriebssystem / Welche: _____ ja nein

Browser / Welche: _____ ja nein

Sonstige / Welche: _____ ja nein

Datenbank / Welche: _____ ja nein

CYBER CRIME. KRISENMANAGEMENTPLAN.

3. Um welche Verdachtsmomente handelt es sich?

(Vermuteter) Hacker Angriff ja nein

Ausfall von IT Ressourcen ja nein

Missbrauch eines Systems durch legitimen Benutzer ja nein

Viren-/Ransomware-/Wurmbefall ja nein

Sonstige _____ ja nein

4. Welche Maßnahmen zur Eindämmung des Vorfalles sind getroffen worden?

„ANHANG B WICHTIGE KONTAKTE“:

Kontakt	Name	Kontaktdaten
IT-Sicherheitsbeauftragter		
Ansprechpartner für Cybervorfälle		
Ansprechpartner für Crimevorfälle		