IT-Notfallordner

Firma: _____

Inhaltsverzeichnis

Versionen / Aktualisierungen

Version	Datum	Änderungen	Wer

Der Antrieb für diesen Ordner

Unser Ziel ist, dass keiner unserer Kunden mehr durch einen IT-Sicherheitsvorfall oder Datenschutzvorfall nennenswert zu Schaden kommt.

Aus diesem Antrieb und der Erfahrung aus über 60 von uns begleiteten IT-Notfällen seit 2011 entstammt dieser Notfallordner.

Unternehmen, die diesen Ordner aktiv nutzen erhalten einen erheblichen Mehrwert und einen hervorragenden Schutzmechanismus gegen betriebliche Schäden.

Aktualisierungsservice

Die von uns erstellen Inhalte werden regelmäßig überarbeitet und zum Austausch zur Verfügung gestellt.

Melden Sie sich bei unserem Aktualisierungsservice unter **https://www.vicotec.de/aktualisierung** an. Sie erhalten regelmäßig Tipps und Hinweise sowie jährlich überarbeitete, aktuelle Inhalte.

Impressum & Haftung

Herausgeber:
ViCoTec IT-Sicherheit & Datenschutz GmbH & Co. KG
August-Wilhelm-Kühnholz Str. 5, 26135 Oldenburg
0441 20572220, info@vicotec.de, www.vicotec.de

Ausfüllhinweise

Dieser Ordner funktioniert am besten, wenn Sie ihn vollständig ausfüllen und ihn mindestens jährlich komplett überarbeiten – dann kann er seine ganze Kraft entfalten.

Viele Inhalte sind von uns vorgegeben (siehe Aktualisierungsservice). Einige Kapitel sind jedoch von Ihnen auszufüllen:

Folgende Kapitel müssen Sie füllen:

- 2.1 Notfallnummern intern
- 2.3 Mitarbeiter – Kontaktliste
- 2.4 (Key-)Kunden – Kontaktliste
- 6. Zentrale Zugänge
- 7. IT-Struktur
- 8. Wiederanlaufplan

Die Vorlagen zu diesen Kapiteln finden Sie unter
https://www.vicotec.de/downloads

- **Halten Sie den Ordner aktuell!**
- **Sichern Sie den Zugang zum Ordner (wegschließen)!**
- **Weisen Sie wichtige Personen in den Ordner ein!**
- **Benutzen Sie den Ordner im Notfall!**

Rufen Sie uns an, wenn Sie Fragen haben oder Unterstützung möchten:
0441 20572220 oder info@vicotec.de

Dieser Ordner reicht für KRITIS-Unternehmen nicht aus!

1. Sofortmaßnahmen

1.1 Technische Sofortmaßnahmen

1.2 Organisatorische Sofortmaßnahmen

1.3 Kommunikation

1.4 Hackerangriff

1.5 Viren-/Trojanerbefall

1.6 Technisches Versagen

1.7 Menschliche Fehlhandlung

1.8 Brand / Wasserschaden

1.9 Einbruch Diebstahl

1.1 Technische Sofortmaßnahmen

A. Keine Anmeldung mit Administratorkonten auf infizierten Systemen.

B. Sofortige Trennung des Backupsystems vom Netzwerk.

C. Sofortige Trennung infizierter Systeme vom Netzwerk (Kabel ziehen).

D. Schalten Sie das WLAN aus.

E. Infizierte Systeme sind grundsätzlich als vollständig kompromittiert anzusehen.

F. Active-Directory und domain-joined Systeme neu aufsetzen.

G. Alle Passwörter ändern, die mit infizierten Geräten in Verbindung gebracht werden können. Auch:
    a. Im Webbrowser gespeicherte Zugangsdaten
    b. E-Mail-Clients
    c. RDP/VNC Verbindungen
    d. Andere Anwendungen wie FTP-Programme, PuTTY, WinSCP, …

H. Blockieren Sie Remoteverbindungen.

I. Prüfen Sie, ob Backups kompromittiert sind.

J. Gehen Sie bei einer Verschlüsselung nicht auf den Erpressungsversuch ein, sondern setzen das Netzwerk neu auf und spielen ein sauberes Backup ein.

K. Benachrichtigen Sie die Cyberversicherung und lassen Sie sich von Spezialisten beraten.