SECURITY-NOTFALL?

NETCLOUD ICT PROFESSIONALS BERN WINTERTHUR BASEL

Zu den Security-Notfällen gehören die folgenden Szenarien:

- Ausbruch Malware
- Dateien auf einem PC/Server sind verschlüsselt (Ransomware)
- Möglicher Missbrauch von Credentials, Accounts oder Passwörtern
- Unerklärliche Benutzerkonten
- Erfolgreiche Zugriffe in der Firewall auf einem C&C Server im internen Netzwerk
- Drohung erhalten, dass Dokumente veröffentlicht werden

Eskalation zum CISO und zur Geschäftsleitung, um zu entscheiden:

- Kann das Internet abgeschaltet werden? Wenn ja, wie und von wem?
- Kann das Backup isoliert werden?
- Muss die Notfallorganisation aufgeboten werden?
- Wo ist der Business Continuity Management (BCM) Plan?
- Wer gibt das Budget für die Untersuchung/Spurensuche frei?

7/24 Notfallhotline des Netcloud Cyber Defence Centers: **0800 843 922**

Bevor ich das Netcloud Cyber Defence Center anrufe, trage ich noch folgende Informationen zusammen:

- Wann ist der Notfall eingetreten?
- Wie ist der Notfall festgestellt worden?
- Wurden Files, Server und/oder Backups bereits verschlüsselt?
- Was wurde bereits unternommen, um das Ausmass des Problems zu identifizieren?
- Was wurde bereits unternommen, um das Problem einzugrenzen, um die Ausbreitung zu stoppen?
- Welche Standorte sind betroffen?

Winterthur: Gewerbehaus Nägelsee, Schlachthofstrasse 19, 8406 Winterthur
Bern: Carba Center, Waldeggstrasse 37, 3097 Liebefeld
Basel: Schützengraben 21, 4051 Basel