KomCERT - Aus der Praxis eines kommunalen CERTs

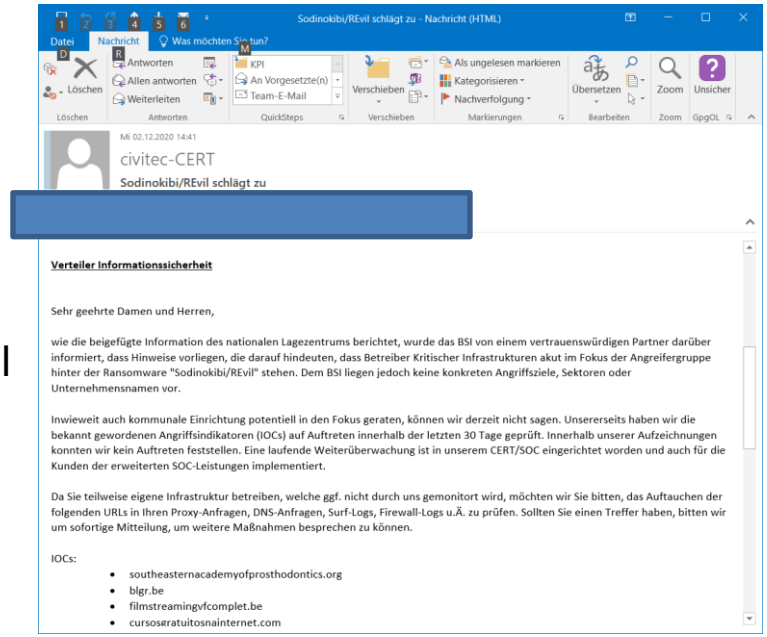
7. KITS, Mai 2021

regio IT

Aufgaben des CERT

Präventiv

- Warnmeldungen zu Sicherheitslücken
- Sensibilisierungsmails zu aktuellen Themen
- Rückfragen zu konkreten Sachverhalten



Reaktiv

- Unterstützung im konkreten Sicherheitsvorfall
- Analyse von Systemen (Forensik)
- Koordination vor Ort

Nachhaltig

- Beratungsangebot
- Durchführung von Sensibilisierungen
- Aufbau von Security Monitoring

Grundsätzlich gilt:

- **Es darf nichts nach außen dringen**
- **Wir müssen versuchen das intern zu regeln**
- **Geld haben wir auch keins**
- **Und bitte nicht die Polizei einschalten**

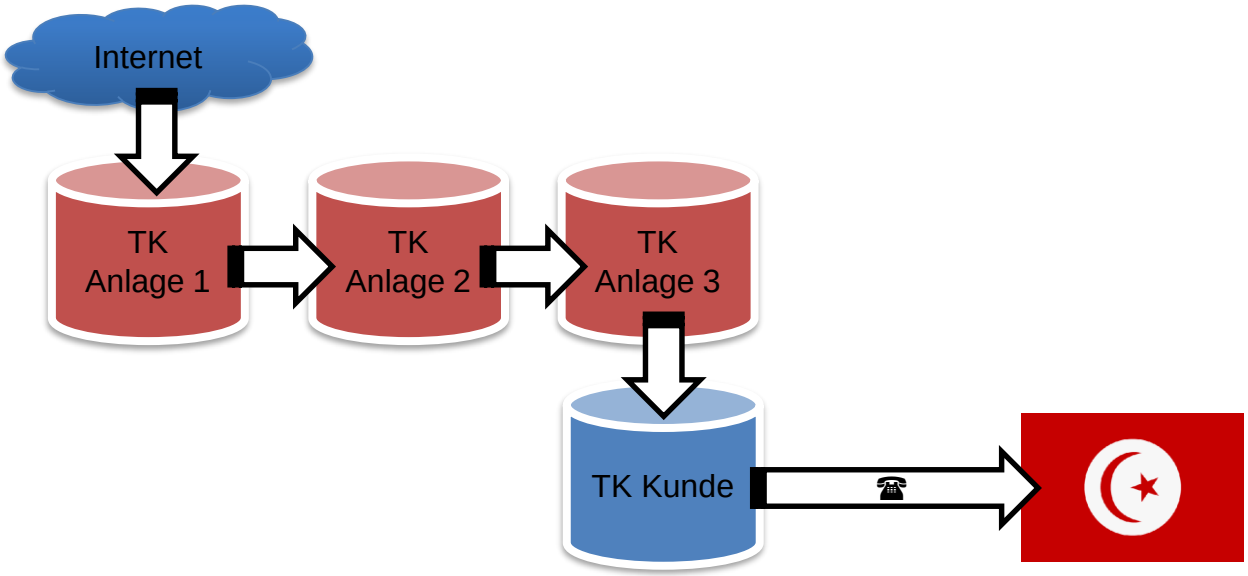
„Nie passiert“ – Wenn die Webseite plötzlich komisch wird

Backdoors auf Websites:

vielen Dank für das Telefonat. Wie eben besprochen sende ich Ihnen die uns bekannten URLs:
https://[redacted]/wordpress/wp-content/uploads/2019/06/door.php
https://[redacted]/wordpress/wp-content/uploads/2019/06/class-wc-settings-tax.php
https://[redacted]/wordpress/wp-content/uploads/2019/06/network-admin-alert.php
https://[redacted]/wordpress/wp-content/uploads/2019/06/po.php
https://[redacted]/wordpress/wp-content/uploads/2019/06/pagination.php

„Nie passiert“ – Angriffe auf Telefonanlagen

Beispiel: Angriff auf eine Telefon-Anlage mittels Voice-over-IP (VoIP)



Alternativ: Angriffe gegen „Anrufbeantworter“
Schaden: mehrere 1.000 €

„Nie passiert“ – Ransomware – Oktober 2020

Das komplette Verwaltungsnetz einer Schule wurde verschlüsselt. Der Angreifer verlangt 25.000 € in der Krypto-Währung Monero.

- Verlust der Schülerdaten
- Verlust der Noten-Daten
- Datensicherung komplett verschlüsselt

Aufgabenstellung des CERT:

- Koordination mit der Schulleitung
- Koordination mit der Stadt
- Pressemitteilung
- Forensik und Versuche Daten zu retten
- Vorgehenskoordination „zurück zum Betrieb“
- Abstimmung mit Staatsanwaltschaft und Ermittlungsbehörden

Herausforderungen für Betroffene

Für die Betroffenen „bricht ein Kartenhaus“ zusammen.

- Notlage
  - Ungewohntes Terrain
  - Plötzlich im Mittelpunkt
- Koordination
  - Was ist jetzt wichtig?
  - Welche Reihenfolge?
- Einbindung externer Stellen
  - Datenschutz?
  - Ermittlungsbehörden?
- Kommunikation
  - Wie?
  - Was?
  - Überhaupt?

Seien Sie vorbereitet

Irgendwann wird es auch SIE treffen – Bereiten Sie Ihre IT und Ihr Haus vor!

Security geht nur gemeinsam!
Wir leben von Kooperation!

Polizei NRW.

CERT Bund

ZAC NRW
Zentral- und Ansprechstelle Cybercrime

Bundesamt für Verfassungsschutz

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Allianz für Cyber-Sicherheit

BUNDESNACHRICHTENDIENST

Bundeskriminalamt

Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen

eco

Vielen Dank für Ihre Aufmerksamkeit!

www.regioit.de
Thomas Stasch, komcert@regioit.de

regio IT