INFORMATIONSSICHERHEIT
BEDROHUNGSLAGE UND GEGENMASSNAHMEN

17.04.2023 Digitalausschuss Kreisstadt Siegburg

Thomas Stasch, CISO

VORSTELLUNG

Persönliches

- 51 Jahre alt
- verheiratet
- zwei Kinder
- Diplom Informatiker (FH)
- Master of Science Wirtschaftsinformatik

Lebenslauf

- Mitarbeiter Stadtkasse bei der Kreisstadt Siegburg, 1991
- Systemadministrator bei der Kreisstadt Siegburg, bis 1999
- Service Manager bei der Deutschen Post DHL, IT-Services GmbH, bis 2010
- Leiter Stabsstelle IT-Sicherheit und Service Management bei civitec
- Leiter civitec-CERT beim Zweckverband civitec
- Leiter KomCERT und Informationssicherheitsbeauftragter bei der regio iT GmbH

- Nebenberuflich: Dozent für IT-Security, Wilhelm Büchner Hochschule

BEDROHUNGSLAGE

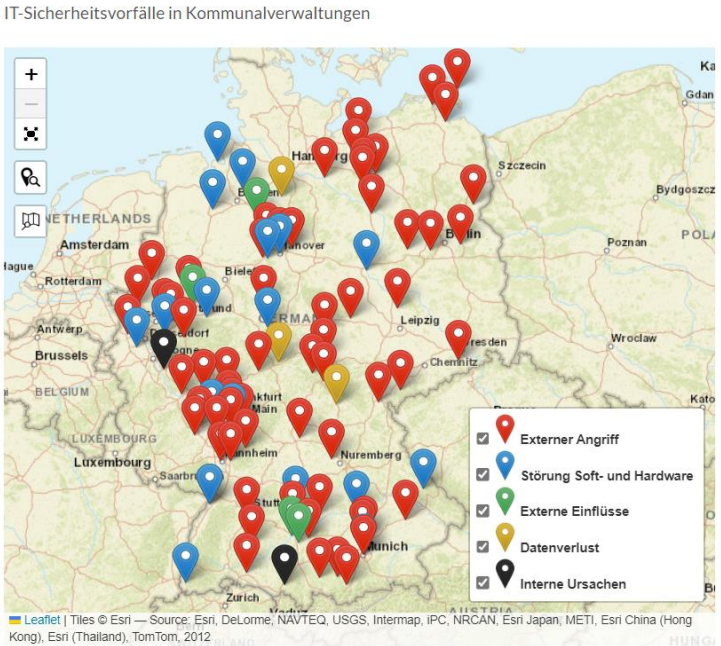
- **Das BSI stuft die Bedrohungslage als „erhöht“ ein**
- **KRITIS-Unternehmen und Behörden im Fokus**
- **Verfassungsschutz sieht Engergie-Versorger und Ogranisationen die sich um Geflüchtete kümmern im Fadenkreuz**
- **ZAC (Zentrale Ansprechstelle Cybercrime) NRW berichtet über immer versiertere Angriffsvektoren**
- **Boom der erfolgreichen Angriffe mit Verschlüsselungen**

VORFÄLLE

Zeitleiste

Gemeindeverwaltung Elbtal	16.03.2023	
	07.03.2023	Stadtverwaltung Bad Kreuznach
Stadtverwaltung Rastatt	07.03.2023	
	24.02.2023	Stadtverwaltung Rodgau
Kreisverwaltung Böblingen	20.02.2023	
	17.02.2023	Stadtverwaltung Wuppertal
Gemeindeverwaltung Butjadingen	17.02.2023	

Übersichtskarte



Quelle: https://kommunaler-notbetrieb.de/

… UND WIE VIELE NOCH?

regio IT

KREISSTADT SIEGBURG

ERFAHRUNG IM UMGANG MIT KRITISCHEN DATEN

Die Kommunalverwaltung und die Kreisverwaltung begleitet den Bürger durch sein ganzes Leben:

- Beurkundung der Geburt
- Beantragung des Personalausweises / Reisepasses
  (und Ausgabe der Dokumente)
- Beantragung des Führerscheins
- Eintragung eines Gewerbebetriebes
- Einzug von Gewerbesteuern
- An-/Ab-/Ummeldung von Kraftfahrzeugen (Kreise/kreisfreie Städte)
- Durchführung von Eheschließungen
- …
- bis hin zur Festlegung der Grabstelle mit Dauer der Ruhefrist.

KOMMUNALES GRUNDSCHUTZPROFIL

Dieses IT-Grundschutz-Profil richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen. Es ist adressiert an die Verantwortlichen in der Verwaltung, welche für die Umsetzung und Aufrechterhaltung der Informationssicherheit zuständig sind. Dies sind typischerweise die Hauptverwaltungsbeamtinnen und -beamten, welche die Ressourcen bereitstellen und das angestrebte Sicherheitsniveau einschließlich der Risiken verantworten, sowie die für die Steuerung und Koordination des Informationssicherheitsprozesses zuständigen Informationssicherheitsbeauftragten.

Dieses Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, um sich nach hiesiger Einschätzung nicht der groben Fahrlässigkeit schuldig zu machen.

9.1.4 ORP.3 - Sensibilisierung und Schulung zur Informationssicherheit

Anforderungen	**ORP.3.A1 – A3; A6**
Besonderheiten	ORP.3.A6 Um sicherzustellen, dass Sicherheitsmaßnahmen nicht versehentlich falsch umgesetzt oder unwissentlich ignoriert werden, müssen Mitarbeiter strukturiert und fortlaufend sensibilisiert werden.

KLISCHEE

Hacker tragen keine Hoodies und sitzen nicht in Kellerlöchern!

- Sie sind hochprofessionell
- Sie arbeiten arbeitsteilig
- Sie garantieren Erfolge
- Sie verbessern sich stetig
- Sie führen Unternehmen und stellen „Administratoren“ ein

Sie sind Geschäftsleute!

regio iT
KREISSTADT SIEGBURG

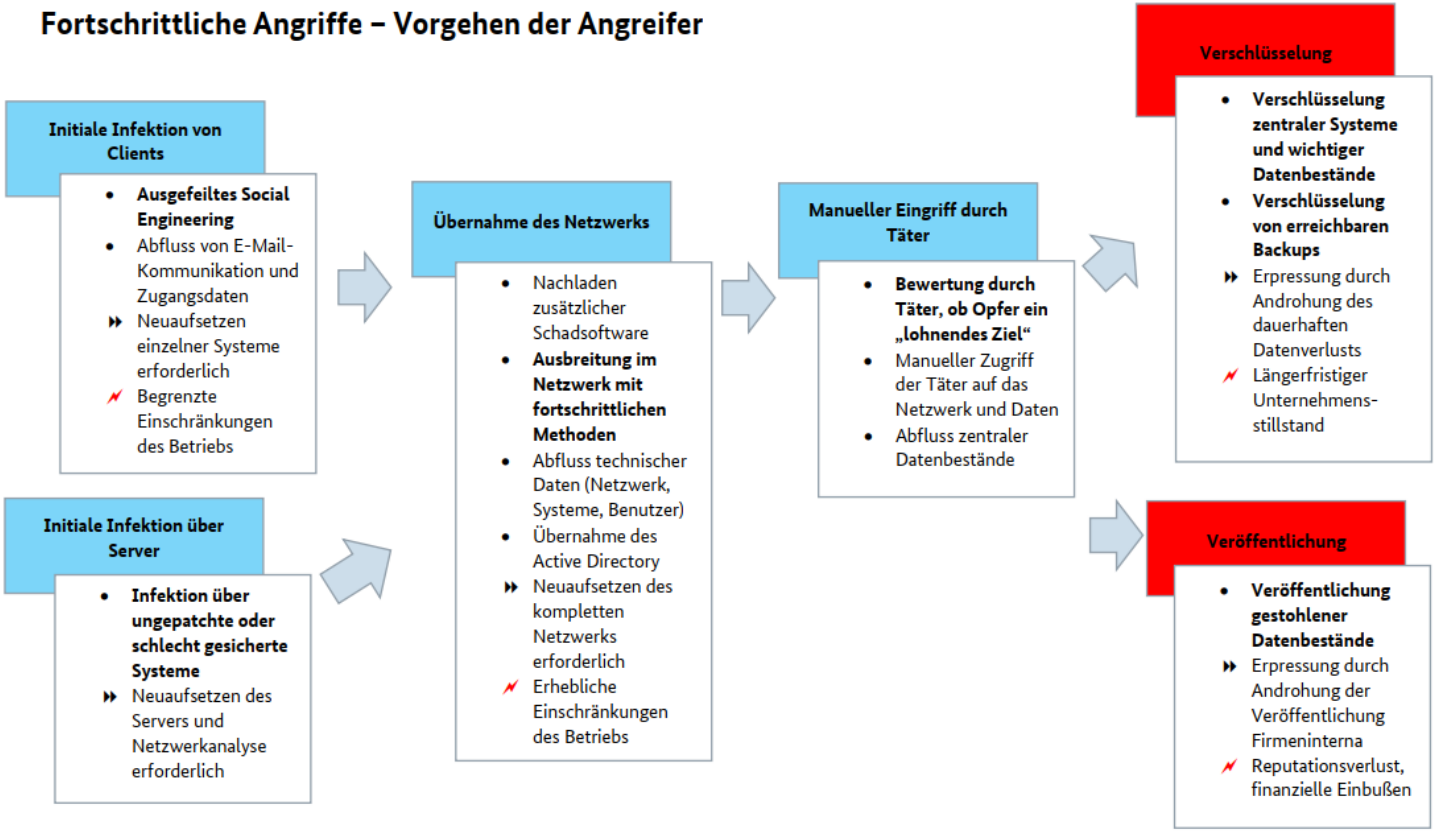
Hacker sind aus verschiedenen Gründen erfolgreich:

- Schlecht gepatchte Systeme und veraltete Anwendungssoftware
- Mangelhafte Absicherung technischer Komponenten
- Unzureichende Handlungsanweisungen für die Mitarbeitenden
- Gutgläubige und mäßig sensibilisierte Anwender
- Argloser Umgang mit Informationen
- Schwache Passworte

ANGRIFFSMETHODIK REALER ANGRIFFE

regio IT
KREISSTADT SIEGBURG

Fortschrittliche Angriffe – Vorgehen der Angreifer



VORFÄLLE DIE NIE PASSIERT SIND (OKTOBER 2020)

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

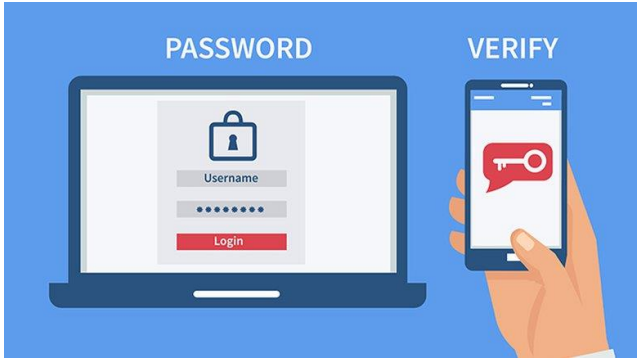
- Verlust der Schülerdaten
- Verlust der Noten-Daten
- Datensicherung komplett verschlüsselt

Aufgabenstellung:

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

Erfolgreicher Angriff von außen

- Einem Angreifer gelang es mittels einer Benutzerkennung und einem Passwort (Qualität: ~ „Kommunenname-2022“) von außen auf ein System zuzugreifen
- Das AD wurde ausgelesen
- Alle Kennungen wurde auf einfache Passworte geprüft
- Der Angreifer bewegte sich quer durch die Organisation
- Eine zweistellige Zahl an Rechnern wurde komproittiert
- Passworte wurden mitgelesen
- ….

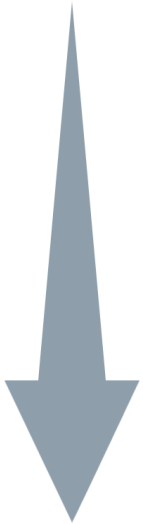


Bild/Quelle: datatrans.ch

➔ Glück: Der Angreifer wurde durch Zufall entdeckt. Ohne die Entdeckung wüsste heute wahrscheinlich jeder den Namen der Kommune, da sie jetzt spätestens verschlüsselt wäre!

Eine Firewall als Vorhängeschloss alleine ist keine ausreichende Sicherheit

Defense in the depth



- Redundanter DDoS Schutz
- Mail-Sicherheit (Blacklisting, Greylisting, Spam-Behandlung)
- Mehrstufiger Virenschutz
- Loganalyse – SOC, SIEM
- automatisierte Schwachstellenscans
- Netzwerksegmentierung
- Advanced Persistent Threat Scans

ZUSAMMENSPIEL KOMMUNE – REGIO IT

Verantwortung für die Informationssicherheit der Kreisstadt Siegburg

- Sicherstellung der Einhaltung innerhalb der Verwaltung
- Aufbau eines ISMS
- Fortwährende Weiterentwicklung und Review
- Definition von Vorgaben für Dienstleister
- Maßnahmen zur Sicherheit in der Verwaltung

Definition und Prüfung von Sicherheits-anforderungen

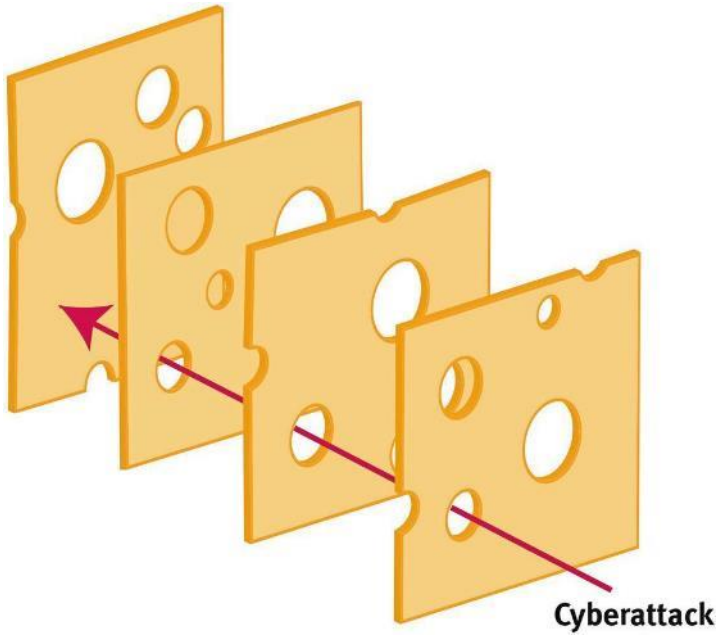
Verantwortung für die Informationssicherheit der regio iT

- Sicherstellung der Einhaltung innerhalb der regio iT
- Aufbau eines ISMS
- Fortwährende Weiterentwicklung und Review
- Definition von Vorgaben für Dienstleister
- Maßnahmen zur Sicherheit in der regio iT

DEFENCE IN THE DEPTH

Nur im optimalen Zusammenspiel von Systemen und Menschen kann es gelingen, die Eintrittswahrscheinlichkeit zu reduzieren.

Uns muss aber bewusst sein: 100%ige Sicherheit werden wir nie erlangen



UND: Der wirksamste Schutz sitzt immer noch 60 cm vor dem Bildschirm

SICHERHEIT IST EINE GEMEINSCHAFTSAUFGABE

Know-how
Ausbildung von Security Fachkräften

Kooperation
Zusammenarbeit auf nationaler Ebene zwischen den Sicherheitsteams

Awareness
Sensibiilisierung der Mitarbeitenden und Kunden

Reaktionsfähigkeit
Konsolidierung und Stärkung des Business Continuity Managements für den Krisenfall

Ausbau der Detektionsmöglichkeiten
Angriffe und Versuche frühzeitig erkennen und agieren.

Technologie
Nutzung neuer technischer Ansätze in der Cyber-Defense: Von Backup über Virenschutz bis zu künstlichen Intelligenz

SICHERHEIT IST EINE GEMEINSCHAFTSAUFGABE

regio iT

KREISSTADT SIEGBURG

POLIZEI Nordrhein-Westfalen Landeskriminalamt

ZAC NRW Zentrale Ansprechstelle Cybercrime

CERT Bund

Bundeskriminalamt

Bundesamt für Sicherheit in der Informationstechnik

Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen

Bundesnachrichtendienst

Polizei NRW.

IHR KONTAKT

THOMAS STASCH

Chief Information Security Officer

+49 2241 999-1107

thomas.stasch@regioit.de

DER IT-PARTNER FÜR BEGEISTERTE KUNDEN!

VISION

VIELEN DANK!

FINDEN SIE UNS AUF