INFORMATIONSSICHERHEIT IN ÖFFENTLICHEN GEBÄUDEN

25.04.2023 9. Kommunaler IT-Sicherheitskongress

Thomas Stasch, CISO der regio iT, Leiter KomCERT

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

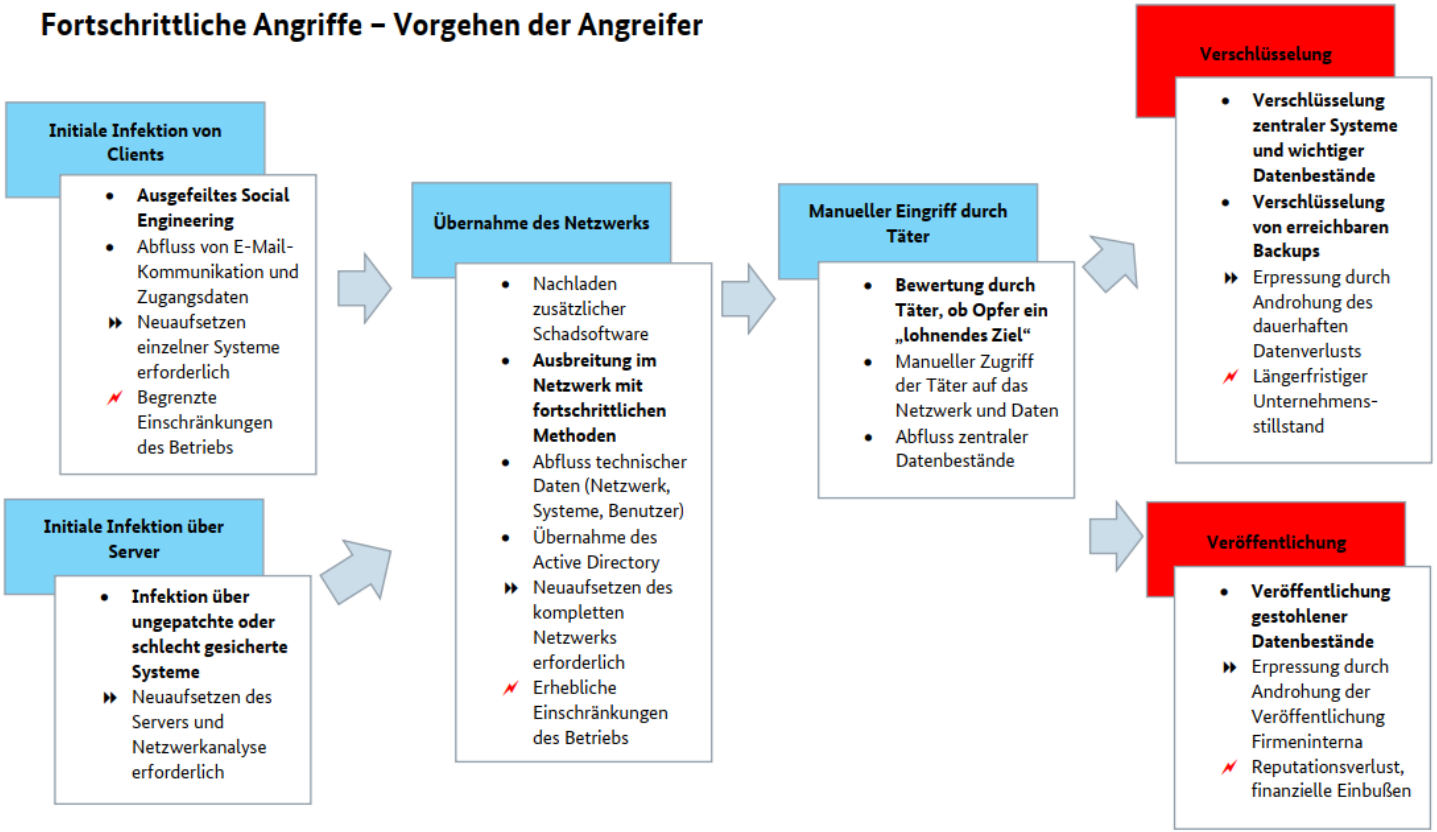
- Nebenberuflich: Dozent für IT-Security, Wilhelm Büchner Hochschule

BEDROHUNGSLAGE

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

ANGRIFFSMETHODIK REALER ANGRIFFE

regio IT



Zeitleiste

Gemeindeverwaltur

Stadtverwaltung

Kreisverwaltung Bö

Gemeindever
Butj

Stadt Rodgau will ihre Systeme gegen neue Angriffe „härten“

Die ersten drei Wochen nach dem Angriff galten der Schadensbegrenzung und der systematischen Untersuchung. Auch Polizei und Staatsanwaltschaft ermitteln. Seit vier Wochen sind die IT-Fachleute dabei, das komplette Netzwerk von Grund auf neu aufzubauen. Jeder der 150 Server muss neu eingerichtet werden. Das dauert acht bis 15 Stunden pro Gerät. Auch alle 650 Arbeitsplatzrechner werden neu aufgesetzt.

Die Stadt nutzt die Gelegenheit, ihre Systeme verstärkt gegen Angriffe zu „härten“, wie Bürgermeister Breitenbach sagt. Ohnehin hatte der Magistrat bereits im vergangenen Jahr beschlossen, für rund 400000 Euro eine komplett neue Server-Architektur zu beschaffen. Der Angriff erfolgte, als die ersten Geräte gerade geliefert waren. (Ekkehard Wolf)

Eine Firewall als Vorhängeschloss alleine ist keine ausreichende Sicherheit

„RECHTLICHE“ SITUATION

Der Blick ins Grundschutzprofil Kommunalverwaltung verrät, worauf man achten sollte…

Die Verantwortung trägt die Behördenleitung

INF.1.A9

Bei der Planung der Gebäudenutzung ist aufgrund des regen Publikumsverkehrs in Verwaltungsgebäuden darauf zu achten, schützenswerte Räume oder Gebäudeteile nicht in exponierten oder besonders gefährdeten Bereichen unterzubringen.

INF.10.A6

Da im Bürgerbüro reger Publikumsverkehr herrscht, muss sichergestellt werden, dass Verbindungen ins interne Netz der Kommunalverwaltung nur von dafür vorgesehenen Arbeitsplätzen und nur im notwendigen Maße möglich sind.

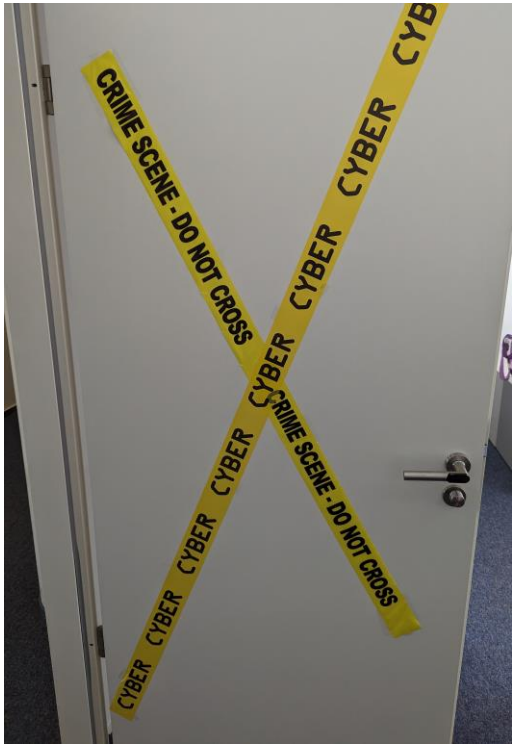
INF.7.A6

Da im Bürgerbüro reger Publikumsverkehr herrscht, müssen Mitarbeiter besonders darauf achten, dass sie vertrauliche Informationen Unbefugten nicht (unfreiwillig) zugänglich machen.

INF.7.A7

Da stets (unbekannte) Besucher im Bürgerbüro zu Gast sind, müssen vertrauliche Informationen und Datenträger sicher aufbewahrt werden.

- Bürgerfreundlichkeit
- Offene Eingänge
- Etagendrucker
- Freie Netzwerkdosen
- Ggf. WLAN



- Der „verlorene“ USB-Stick
- Hardware-Keylogger
- Rouge Access Points
- Der RasPi im Netz
- LAN-Taps
- ...

Hacker sind aus verschiedenen Gründen erfolgreich, wenn sie einmal im Netz sind:

- 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

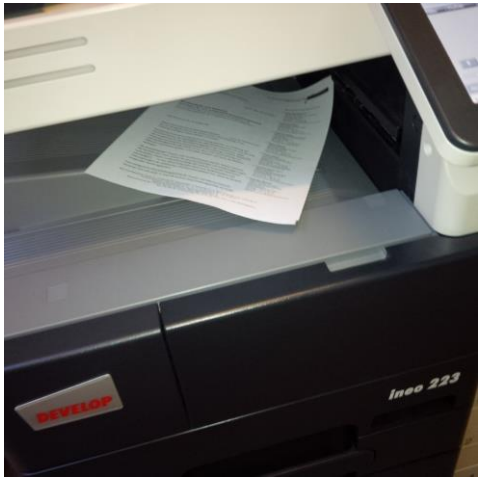
… ABER AUCH GESCHLOSSENE TÜREN LASSEN SICH ÖFFNEN

Quelle: Robin Meis – „WhiteHat“

NICHT NUR IT KANN EIN PROBLEM SEIN

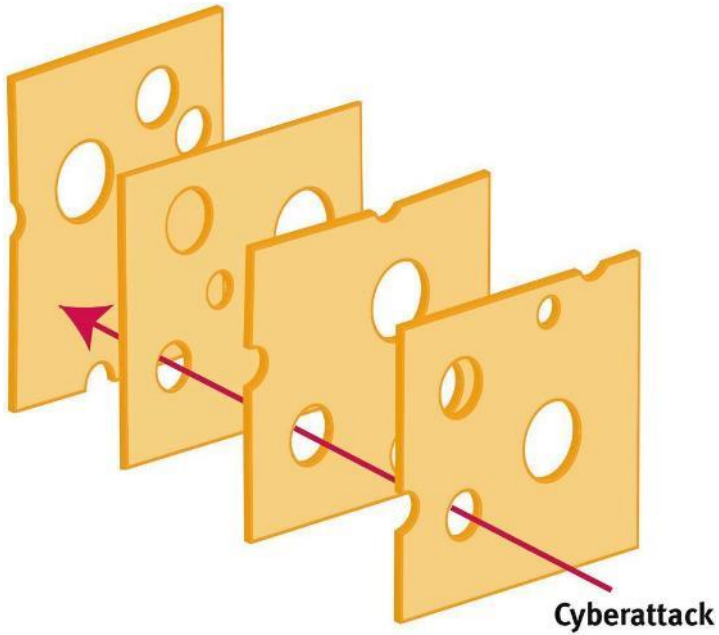
Auch Dokumente, Akten, Notizen, (…) können ein Problem darstellen, wenn sie einfach ungeschützt zugreifbar sind.

- Datenschutzverletzungen
- „neugierige“ Medien
- Diebstahl



Es gibt aber Lösungen zu den Problemen:

- Netzwerk-Separierung
- NAC-Lösungen
- Clean Desk
- Sensibilisierte Anwender



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