DER ORTENAU KREIS

Ransomware

Ernsthafte Bedrohung für Kommunen

Agenda

DER ORTENAU KREIS

- Heutige Ransomware-Angriffe
- Kommunale Informationssicherheit
- Verbesserungspotentiale

Ransomware-Angriffe: Ablauf

Erstinfektion

z.B. über E-Mail-Anhang/Link oder Server am Internet

Ausleitung

(sensibler) Daten

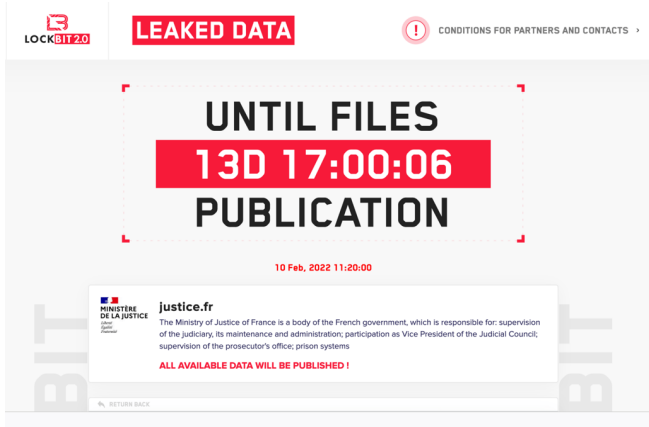
Erkundung und Ausbreitung

Ausbreitung im Netzwerk und Identifikation von lukrativen Zielen

Verschlüsselung

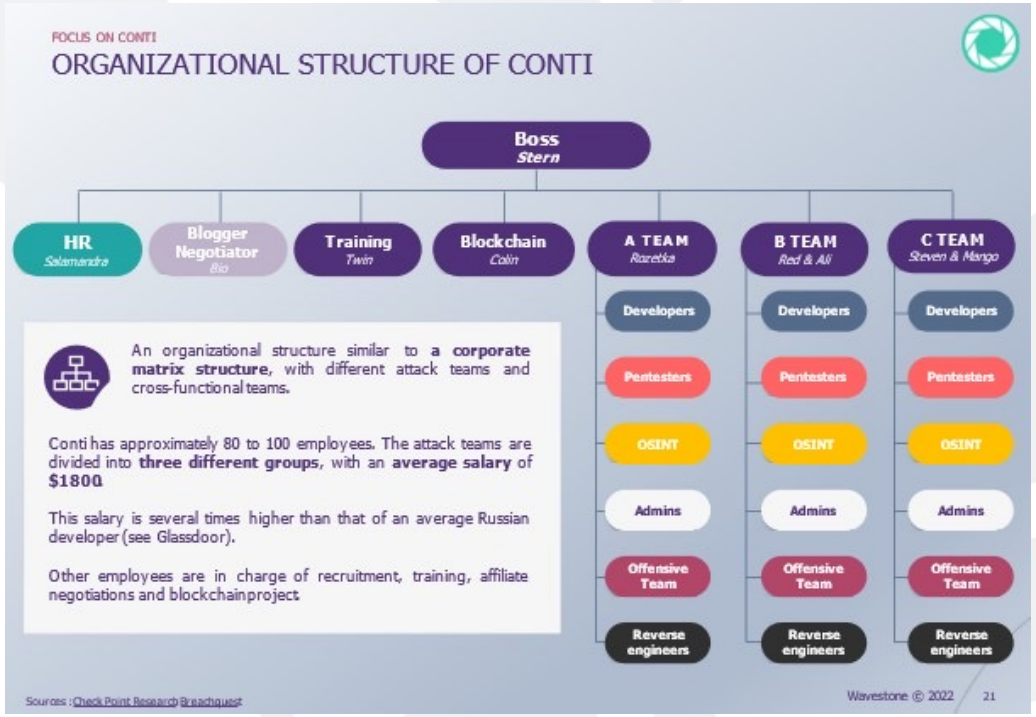
kritischer Services

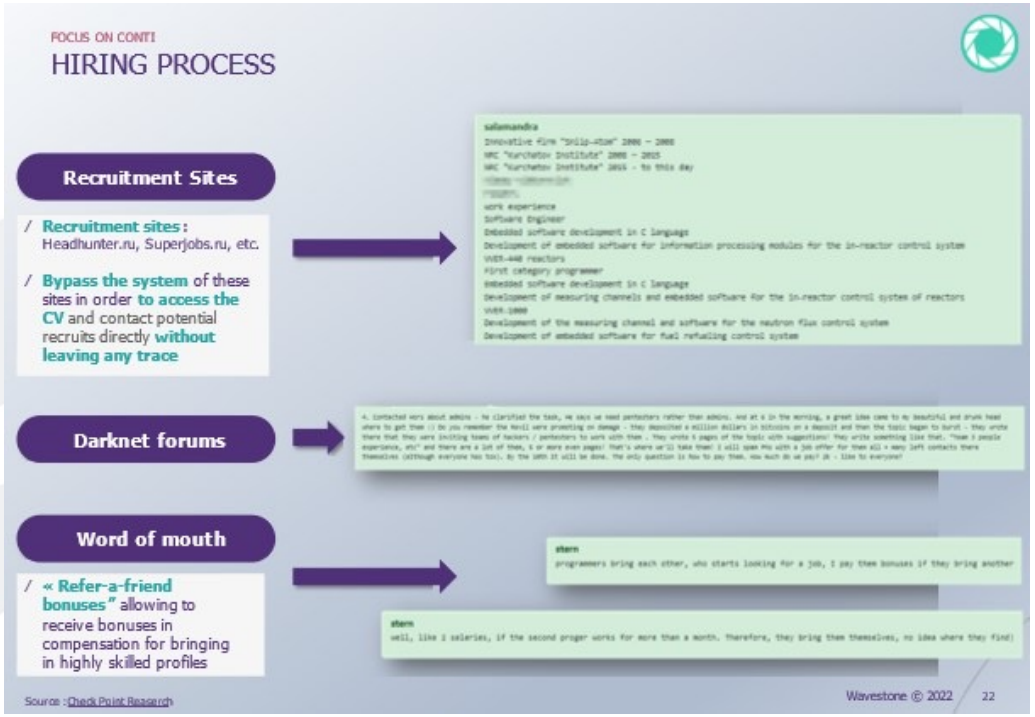
Erpressung



Ransomware-Angriffe: Angreifer-Gruppen

- Ransomware-Gruppen sind organisiert wie Unternehmen mit Arbeitsteilung und Personalbeschaffung

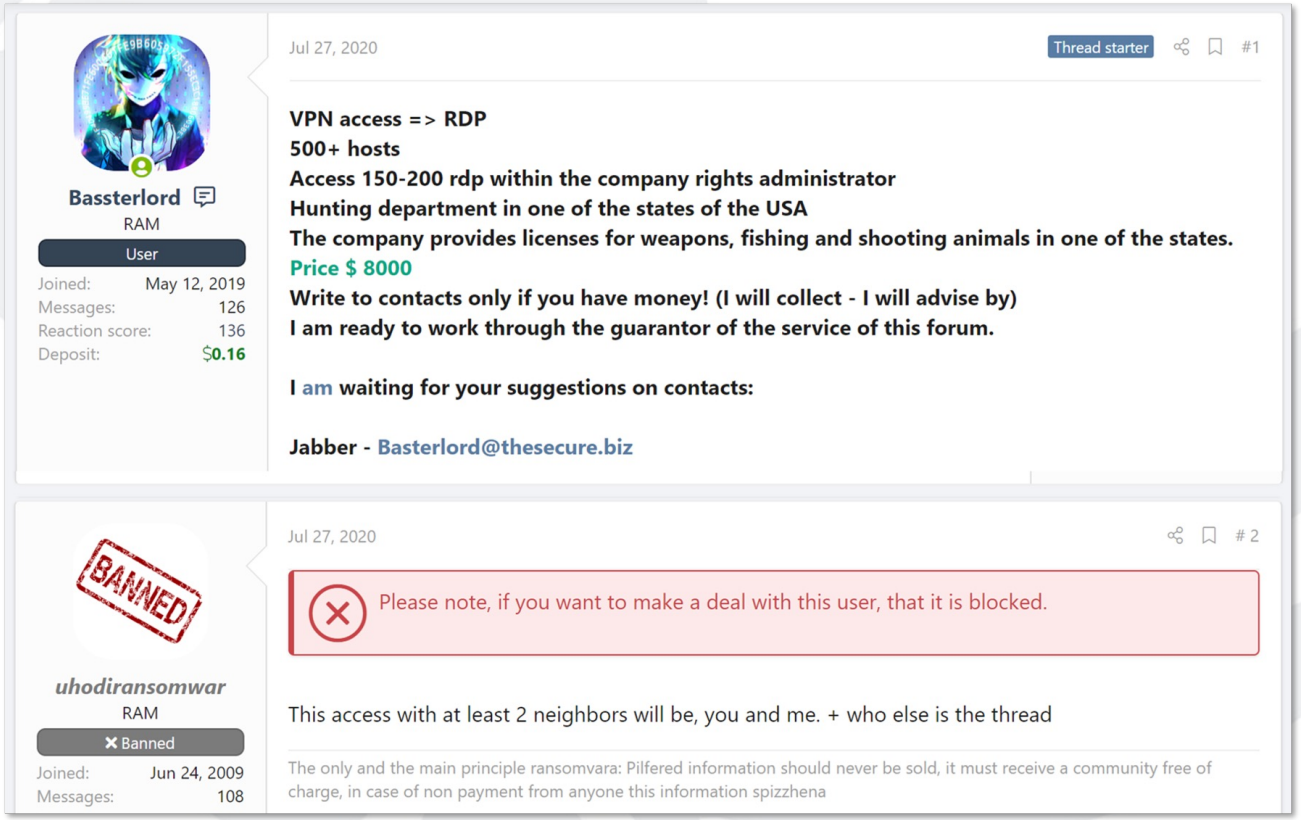


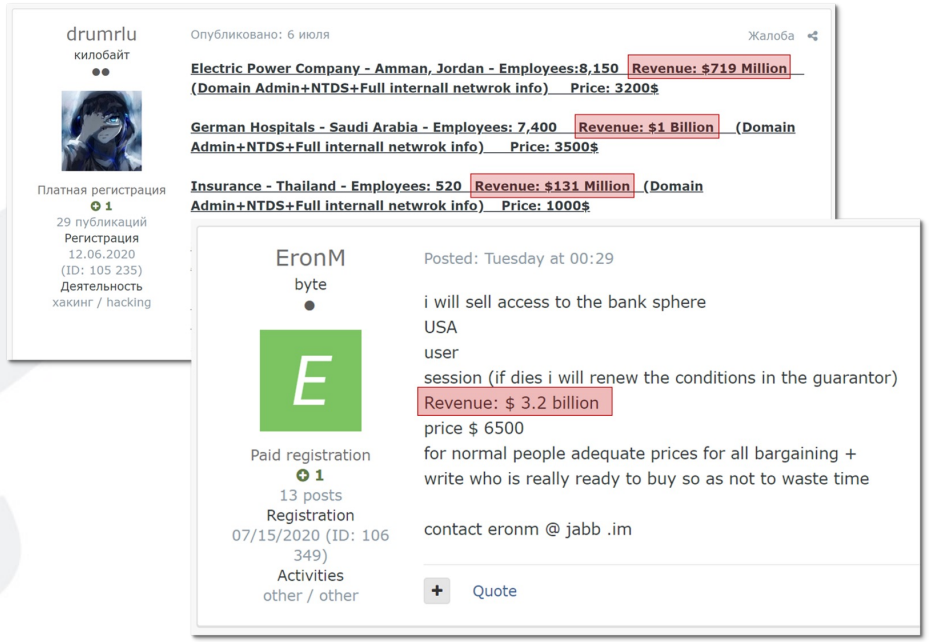


Ransomware-Angriffe: Angreifer-Gruppen

DER ORTENAU KREIS

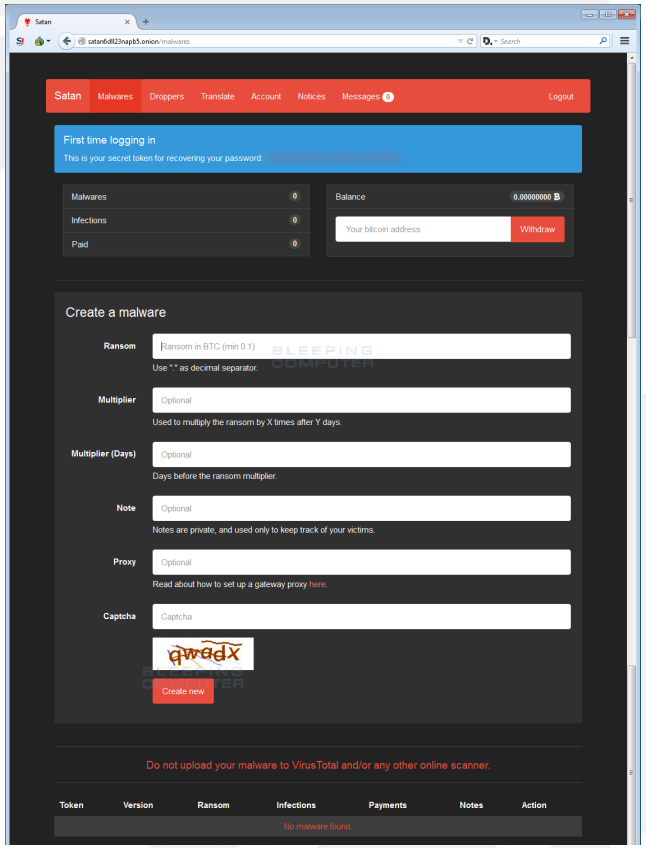
- Ausnutzung von Synergien und Partnerschaften

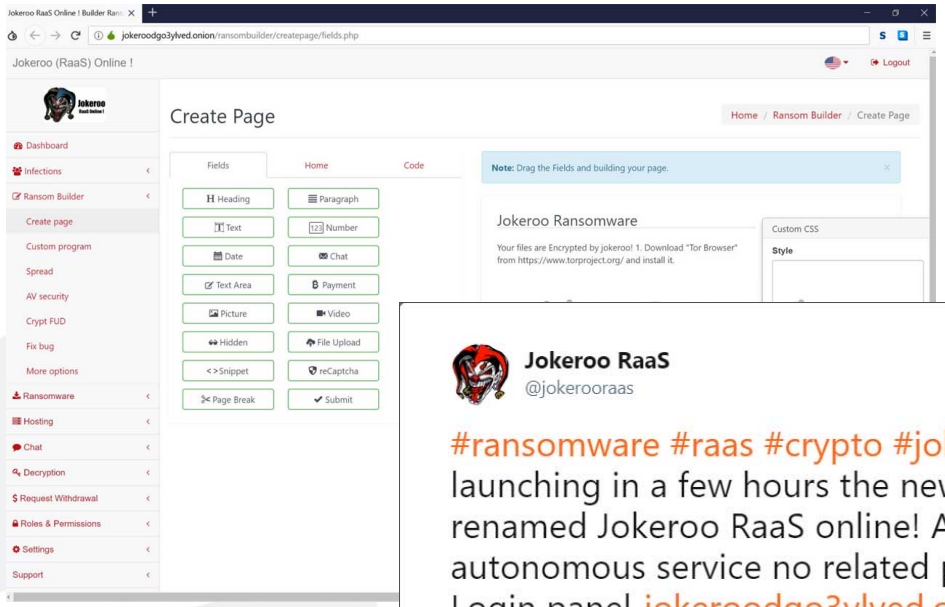




Ransomware-Angriffe: Angreifer-Gruppen

- Geschäftsmodelle wie Ransomware-as-a-Service (RaaS)





Ransomware-Angriffe: Schadenspotential

- Erhebliche Schäden auch bei Kommunen

TEURER ALS GEDACHT

Neue Zahlen: Cyberangriff kostet Anhalt-Bitterfeld 2,5 Millionen Euro

10. März 2024, 10:30 Uhr

Geisweid. Vor 2025 wird nicht alles wieder „normal“ sein bei der Stadt Siegen. Sie rechnet mit einem Millionenbetrag, der sie die Cyberattacke kosten wird.

Rhein-Pfalz-Kreis: 1,7 Millionen Euro Schaden

Seit dem Hackerangriff im Oktober 2022 habe das Landratsamt bisher etwa 9.000 Briefe verschickt, um Bürger darüber zu informieren, dass ihre Daten im Darknet abrufbar sind, so der

Ransomware-Angriffe: Zwischenfazit

DER ORTENAU KREIS

- Störung des kompletten Geschäftsbetriebs und massive Schäden auch bei “erfolglosen“ Angriffen
- Professionelle Organisation und Arbeitsteilung bei den Tätern
- Angriffe werden bleiben

=> Kommunen müssen sich vorbereiten, auch hinsichtlich Notfallmanagement!

„Ransomware-Banden machen viele 100 Millionen $ Umsatz pro Jahr und dieser Umsatz ist gleich Gewinn, weil steuerfrei. […]. Es ist einfach ein sehr lukrativer Markt und die Erfolgsquoten die Hintermänner hochzunehmen ist sehr gering.“ (Manuel Atug, AG KRITIS)

DER ORTENAU KREIS

Können sich kommunale Behörden wirksam gegen Ransomware-Angriffe zur Wehr setzen?

Kommunale Informationssicherheit

DER ORTENAU KREIS

- Qualitative Forschung durch Experteninterviews:
  - Kommunale Expertise: Landratsämter, IT-Dienstleister für kleine Kommunen
  - Fachexpertise: Bundesamt für Sicherheit in der Informationstechnik (BSI), Atruvia AG (KRITIS-Sektor), HiSolutions AG (Qualifizierter BSI-Dienstleister)

- Verständnis der Experten
  - Offene Fragen zur Überprüfung des Wissens
  - Heutige Ransomware-Angriffe korrekt erkannt
  - Auch durch kommunale Experten

Kommunale Informationssicherheit

DER ORTENAU KREIS

- Maßnahmen gegen Ransomware-Angriffe:
  - Prävention: Sensibilisierung MA, Patchmanagement u.a.
  - Kein vollständiger Schutz möglich auch bei sehr guten Präventionsmaßnahmen
  - Bedrohungslage wird bleiben…

  => Notfallmanagement ist notwendig!

- Notfallmanagement bei Kommunen:
  - Grundsätzlich ist eine Notfallplanung möglich
  - Ausgestaltung abhängig von verschiedenen Parametern (z.B. Organisationsgröße)
  - Externe Dienstleister für den Notfall unabdingbar (im Vorfeld klären)

Kommunale Informationssicherheit

DER ORTENAU KREIS

- Lage kommunale Informationssicherheit:
  - Keine passende Informationssicherheit für heutige Ransomware-Angriffe
  - Professionelle, spezialisierte Experten vs. allgemeine IT
  - Fehlende Ressourcen und Bewusstsein

„Das ist keine Schuldfrage. […] Als IT-Experte ist man auf dem Markt sehr, sehr gefragt und soll dann ein kleine Kommunalgehalt bekommen und dafür den ISB machen und diese Monsteraufgabe in der Kommune lösen […]. Da ist es klar, dass man nicht so schnell wen findet, der dann auch kompetent ist.“

(Maike Vossen, BSI)

Kommunale Informationssicherheit

DER ORTENAU KREIS

- Problemfelder:
  - Fehlende Technik (z.B. SIEM-System)
  - Fehlende Fachkräfte
  - Keine Standards bzw. Vorgaben
  - Zu wenige Synergien
  - Fehlendes Bewusstsein

Verbesserungspotentiale

DER ORTENAU KREIS

- Technische Lösungen nutzen
- Mehr Ressourcen schaffen
- Bessere Nutzung von Ressourcen
- Synergien nutzen
- Mehr Bewusstsein schaffen

Handeln!

- BSI-Materialien / -Angebote:
  - Verschiedene Standards: 200-1, 200-2, 200-3, 200-4
  - IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung
  - Vereinfachter Einstieg: “Weg in die Basis-Absicherung“ (WiBA)
  - “BSI-IT-Grundschutz-Praktiker“

- Cybersicherheitsagentur Baden-Württemberg (CSBW)
  - Lernplattform
  - Beratung für Kommunen

- „Fangen Sie an!“

DER ORTENAU KREIS

Vielen Dank für die Aufmerksamkeit

Haben Sie noch Fragen?

Kontaktmöglichkeit im Nachhinein:

christian.dinger@ortenaukreis.de

Quellen

DER ORTENAU KREIS

Folie 03:
- Bild – Erpressungstext Akira: https://www.truesec.com/wp-content/uploads/2023/11/Akira.png
- Bild– Lockbit: https://cyberscoop.com/wp-content/uploads/sites/3/2022/01/Screen-Shot-2022-01-27-at-1.19.54-PM.png?resize=2048,1353

Folie 04:
- Bild - Organigramm: https://www.riskinsight-wavestone.com/wp-content/uploads/2022/06/EN4.jpg
- Bild – Hiring Process: https://www.riskinsight-wavestone.com/wp-content/uploads/2022/06/EN3.jpg

Folie 05:
- Bild – IAB „Bassterlord“: https://www.kelacyber.com/wp-content/uploads/2020/08/9.png
- Bild – IAB „drumlru“, „EronM“: https://www.kelacyber.com/wp-content/uploads/2020/08/14.png

Folie 06:
- Bild – RaaS – Satan: https://www.bleepstatic.com/images/news/ransomware/s/satan-raas/raas-malware-page.png
- Bild – RaaS – Jockeroo - Twitter: https://www.bleepstatic.com/images/news/ransomware/j/jokeroo/twitter-promotion.jpg
- Bild - RaaS – Jockeroo – Create Page: https://www.bleepstatic.com/images/news/ransomware/j/jokeroo/ransom-note-creator.jpg

Folie 07:
- Ausschnitt – Anhalt-Bitterfeld (MDR): https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/anhalt/cyberangriff-kreis-kosten-teurer-als-gedacht-102.html
- Ausschnitt – Stadt Siegen (Westfalenpost): https://www.wp.de/staedte/siegerland/article241667924/Siegen-Cyber-Krise-nur-auf-den-ersten-Blick-vorbei.html
- Ausschnitte – Rhein-Pfalz-Kreis (SWR): https://www.swr.de/swraktuell/rheinland-pfalz/ludwigshafen/neuer-stand-hackerangriff-100.html

Folie 08:
- Zitat Manuel Atug aus einem Interview der Bachelorarbeit „Ausarbeitung eines Notfallkonzepts für das Landratsamt Ortenaukreis zur Reaktion auf Ransomware-Angriffe“ von Christian Dinger (Digitales Verwaltungsmanagement an der HS Kehl, abgegeben im Sommersemester 2023)

Folie 12:
- Zitat Maike Vossen aus einem Interview der Bachelorarbeit „Ausarbeitung eines Notfallkonzepts für das Landratsamt Ortenaukreis zur Reaktion auf Ransomware-Angriffe“ von Christian Dinger (Digitales Verwaltungsmanagement an der HS Kehl, abgegeben im Sommersemester 2023)