TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Essen, 29./30.06.2017

Ransomware trifft uns alle!

Sascha Dubbel

Senior Systems Engineer, T.I.S.P., GCED

Cylance Deutschland GmbH

Ist Ransomware die erfolgreichste Malware dieser Tage?

- Warum kommt es immer wieder zu erfolgreichen Vorfällen?
- Ist Ransomware technisch raffinierter als andere Malware-Familien?
  - GoldenEye Ransomware
  - WannaCry

Welche Gegenmaßnahmen sind sinnvoll/wirksam? Ist die Prävention überhaupt möglich?

- Technische Maßnahmen:
  - Netzwerk-Gateways
  - Sandboxen
  - signaturbasierte Verfahren
  - Patch Management
  - Next-Gen-Lösungen
  - ...Stand der Technik?
- Organisatorische Maßnahmen:
  - Awareness-Training
    - Phishing-Tests
  - Ansprechpartner/Hotline im Verdachtsfall
  - ...

Ist ein spezieller Ransomware-Schutz sinnvoll?

- Ransomware ist nur die Spitze des Eisbergs!
  - Angreifer bedienen sich den gleichen Taktiken um Infostealer/Backdoors/Remote Access Tools zu platzieren und sind damit genau so erfolgreich
  - Anders als Ransomware bleiben die Infektionen aber weitgehend sehr lange unentdeckt, das es keine Lösegeldforderung gibt

Was tun, wenn es zu einem Vorfall kommt?

- Sollte ein Unternehmen zahlen?
  - Vor und Nachteile
- Was lerne ich aus einem Vorfall?
  - Was ändern wir für die Zukunft
- Wie verhindere ich die Ausbreitung?
- Wer kann mir helfen?
  - Incident Response und Compromise Assessment