recretix systems

HEALTH TECH CLUSTER SWITZERLAND

ISSS Information Security Society Switzerland

One fine day at YOUR hospital

7.8.2018 ISH'18

Stefan Peter — Security Engineer & Inhaber
Fabian Riechsteiner — Security Engineer

recretix systems

Agenda: One fine day at YOUR hospital

- Einleitung / Vorstellung
- Herleitung Gefahrenpotential & Vektoren
- Show Case 1: Device übernehmen
- Show Case 2: Lateral Movement & Active Directory Takeover
- Exkurs Health Layer 7 (HL7 Protokoll)
- Show Case 3: Health Layer 7 Datenstream Analyse & Missbrauch
- Abschluss

Wir sind die recretix systems AG und schützen kritische Infrastrukturen

- Unternehmen:

- recretix systems AG
- Kompetent in IT-Sicherheit und IT-Infrasturktur
- Kunden aus allen Verticals, von Industrie über Militär bis Healthcare

- Portfolio IT-Sicherheit:

- Beratung & Konzepte
- Penetration Test
- Passive Abwehr von Bedrohungen
- Aktive Abwehr von Bedrohungen
- Incident Response

recretix systems

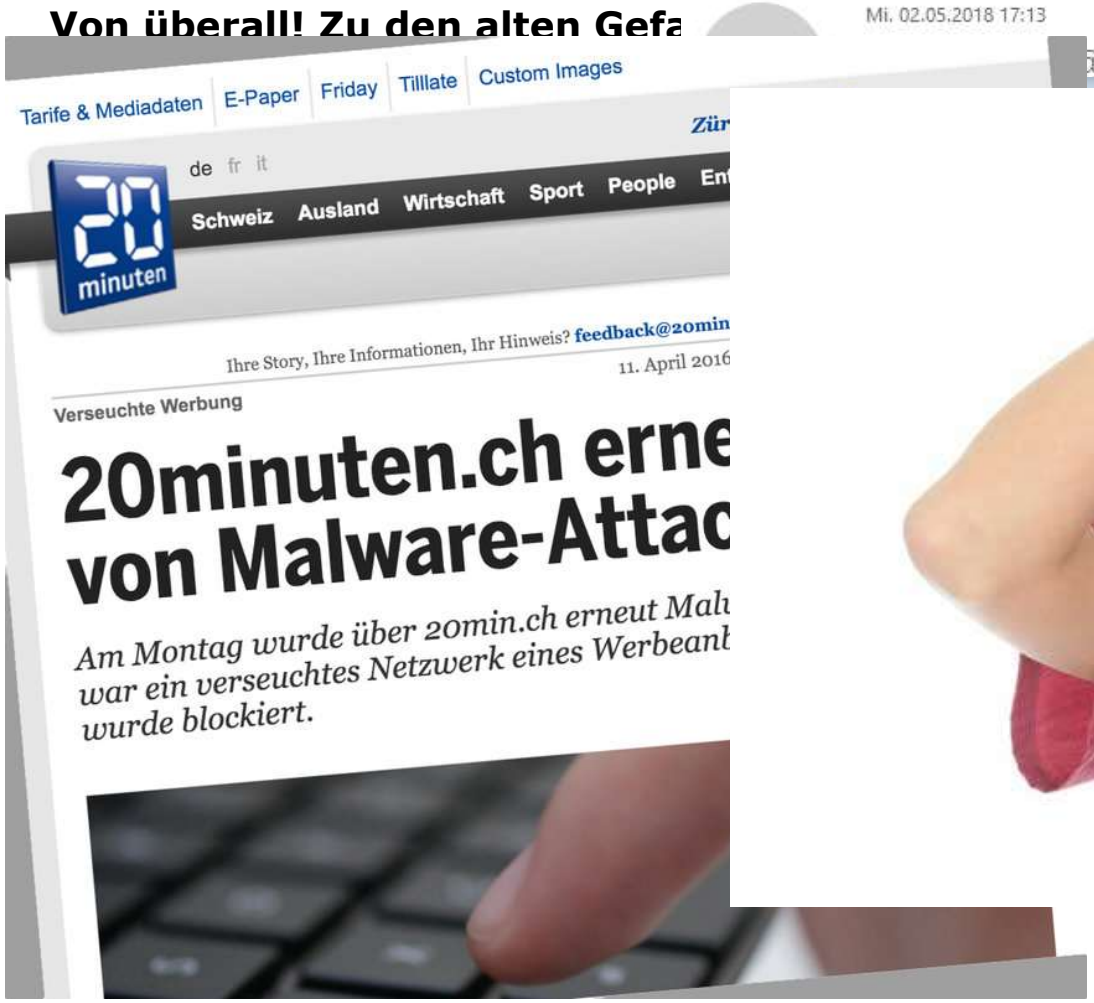
Wir demonstrieren die Anatomie eines Angriffs

- Heute wollen wir dem Publikum aufzeigen,
  - wie ein Angriff auf ein Spital ausgeführt werden könnte
  - dass Hacker keine Übermenschen sind und auch nur mit Wasser kochen
  - dass jedes Mal viel Glück bzw. Pech im Spiel ist
  - dass Angriffe viel Kreativität und Out-of-the-box Denken erfordert

- Aber in erster Linie wollen wir aufzeigen, wie erschreckend einfach der Hack ist, wenn die Security vernachlässig wird!

Woher kommt die Gefahr?

Von überall! Zu den alten Gefa



recretix systems

Kein System ist 100% sicher..

- Jedes System muss geprüft werden
- Ein Breach kann nicht verhindert werden
- Die Auswirkungen eines Breaches müssen minimiert werden
- Alle müssen mithelfen und mitdenken
- Best Practices kennen
- **Best Practices auch anwenden!**

Wir alle kennen die fünf Angriffsphasen einer Cyberattacke

recretix systems

Heute geht es los mit Stufe 3!

1. • **Reconnaissance**
2. • **Scanning**
3. • **Gaining Access – Demo 1**
   • Pwn a single Device
4. • **Maintaining Access – Demo 2**
   • Laterales Movement zu “höherwertigen” Zielen
5. • **Monetizing the attack – Demo 3**
   • Erpressung durch Datenmanipulation

recretix systems

Real World Show Cases: Device übernehmen

- Aufbau Show Case:

- **Ziel Show Case: Tablet Computer für bildgebende Anwendungen, validiert, nicht gepatcht.**

- Alternative Ziele:
  - Alles im Spitalnetz!
  - Ungepatche Devices, BYOD, validierte Systeme ohne Patches, alte und neue Devices, IoT Systeme

- Eingesetzte Technik:
  - USB Stick (Rubber Ducky)
  - Kali Linux / Meterpreter

- Alternative Vektoren:
  - Phising
  - Malvertising

Wir alle kennen die fünf Angriffsphasen einer Cyberattacke

recretix systems

Heute geht es los mit Stufe 3!

1. • **Reconnaissance**
2. • **Scanning**
3. • **Gaining Access – Demo 1**
   • Pwn a single Device
4. • **Maintaining Access – Demo 2**
   • Laterales Movement zu “höherwertigen” Zielen
5. • **Monetizing the attack – Demo 3**
   • Erpressung durch Datenmanipulation

recretix systems

Real World Show Cases: Lateral Movement & AD Takeover

- Aufbau Show Case:

- **Ziel Show Case: Computer für bildgebende Anwendungen, validiert, nicht gepatcht, AD Integration**

- Real World Alternativen:
  - Alles im Spitalnetz mit AD Integration
  - Validierte Systeme ohne Patches, Systeme mit bekannten oder unbekannten Sicherheitslücken

- Eingesetzte Technik:
  - Ethernal Blue (sponsored by NSA)
  - Kali Linux / Meterpreter
  - Powershell

- Alternative Vektoren:
  - Vor Ort im Spital, Netzwerke geschützt?

Wir alle kennen die fünf Angriffsphasen einer Cyberattacke

recretix systems

Heute geht es los mit Stufe 3!

1. • **Reconnaissance**
2. • **Scanning**
3. • **Gaining Access – Demo 1**
   • Pwn a single Device
4. • **Maintaining Access – Demo 2**
   • Laterales Movement zu “höherwertigen” Zielen
5. • **Monetizing the attack – Demo 3**
   • Erpressung durch Datenmanipulation

Exkurs Health Level 7 (HL7 Protokoll)

Was ist Health Level 7?

- Health Level 7 ist überall im Spital, jeder Event triggert einen eine HL7 Nachricht, die von einem System an ein anderes System geschickt werden.

- Use Cases:

- Ein Patient wird in einen anderen Raum verlegt
- > Ein HL7 ADT (Admission, Discharge and Transfer) Statement wird abgesetzt

- Jemand fordert einen Test oder ein Medikament an
- > Ein HL7 ORM (Order) Statement wird verschickt

- Es werden Testresultate oder Telemetriedaten verschickt
- > Eine HL7 ORU (Observation Result) wird über das Netzwerk geliefert

- Normalerweise werden alle HL7 Nachrichten von einer zentralen Stelle angenommen und weitergeleitet (KIS)

Exkurs Health Level 7

Warum ist Heath Level 7 ein potentielles Problem?

- HL7 ermöglich Device to Device Kommunikation

- HL7 ist offen für alle Teilnehmer

- Keine eingebaute Security, keine Verschlüsselung

- Jeder im gleichen Netzwerk kann HL7 mithören, wenn er über die entsprechenden Skills und Rechte verfügt!
- > Skills: ARP-Poisoning / Man in the Middle
- > Rechte: Zugang zum Layer 2 Netzwerk

- Angreifer kann persönliche, medizinische Werte mitschneiden!

- Angreifer kann persönliche, medizinische Werte schicken!

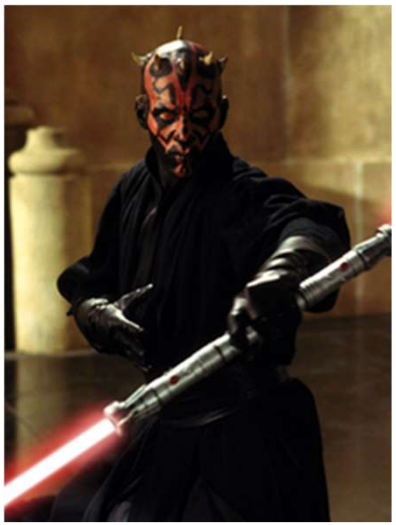
Exkurs Health Level 7

recretix systems

Wie muss ich mir das genau vorstellen?

- Daten, die aus einer ADT Message gelesen werden können

```
MSH|^~\&|SENDING_APPLICATION|SENDING_FACILITY|RECEIVING_APPLICATION|RECEIVING_FACILITY|20170613083617||ADT^A01|91157616011061308361 7|P|2.3||||
EVN|A01|20170613083617|||
PID|1||1337||MAUL^DARTH^||19850929|M|||Sith Lord Compound^^Death-Star-Valley^Dathomir^8056||+41 939 1234
^^d.maul@galacticempire.com|||||1719|756.254.551.666||| |Galactic Empire Privat-Versicherung||||||||||||||||
NK1|1|MAUL^QIRA|WIFE||||||NK
PV1|1|O|||||^^^^^^^^^|^^^^^^^^^
AL1|1||^Bacta||Anaphylactic Shock
AL1|2||^Sun||Skin rash
```



PID = Patienten-ID mit allen Daten
NK1 = “Next of Kin” mit Angehörigen-Daten
AL1 = Allergie Informationen

Wie kann ein Angreifer das verwerten?
Sende eine Order Message für ein Medikament “Bacta” und der Patient erleidet einen lebensgefährlichen, anaphylaktischen Schock

Exkurs Health Level 7

Was kann ich sonst noch mit HL7 anstellen?

- Login-Daten abfangen
- > Meldet sich ein Arzt am System an, benutz er sein Login und Passwort. Je nach System wird dieses Passwort in Klartext mitgeschickt oder als Hash, beides kann für neue Abfragen benutzt werden.

- Mit diesen Login-Daten kann der gesamte Patientenstamm ausgelesen werden!
- > Wie?
- > Eine Abfrage ohne Suchparameter liefert sämtliche Patienten, auf die mit dem Login zugegriffen werden können

- > Eine Akte pro Abfrage kann dann ausgelesen werden

- Es können selber beispielsweise ADT Message abgesetzt warden
- > Patienten warden im KIS in andere Zimmer verlegt, bleiben aber physikalisch im gleichen Zimmer

recretix systems

Real World Show Cases: HL7 Stream abfangen & auslesen

- Aufbau des Show Case:

- **Ziel Show Case: HL7 Stream abfangen, auslesen und manipulieren**

- Real World Alternativen:
  - Alle Devices die mit HL7 kommunizieren, HL7 bietet keine Verschlüsselung!

- Eingesetzte Technik:
  - Wireshark
  - Kali
  - HL7 Tools

- Alternative Vektoren:
  - Vor Ort im Spital, Layer 2 Netzwerke geschützt?

Was sagt der HL7 Standard dazu?

Die Abstract Transport Specification sagt:

- Architektur hat folgende Funktionen zu erfüllen:
  - Addressing
  - Reliable Messaging
  - Security*
  - Attachments
  - Compression

In YOUR hospital:

- Was eingesetzt wird:
- IP
- TCP
- ???
- Applikationsspezifisch
- Gar nicht

* Integrity, Confidentiality, Non Repudiation, Authorization, Authentication, Auditing

recretix systems

Conclusion

- IT Security Best Practices
  - Haben alle anderen Speaker heute schon erwähnt?

- Testen Sie Ihr Netzwerk bevor es jemand anderes tut!

- Denken Sie wie Angreifer, nicht wie die interne IT-Abteilung

- Die Mittel und Wege, die für diese Demo benutzt wurden, lassen sich mit Talent innerhalb kurzer Zeit erlernen und anwenden

- Wenn die Security vernachlässigt wird, braucht es keine “government-sponsored” Gruppierungen, die ein Spital bedrohen, eine kleine Bande von Cyberkriminellen kann bereits grossen Schaden anrichten

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:
info@recretix.ch
+41 62 508 13 49