@eHealthSummitAT

eHEALTH SUMMIT AUSTRIA

HIMSS Europe

In Kooperation mit

eHEALTH 2017 www.eHealth2017.at

23. – 24. MAI 2017

Schloß Schönbrunn, Wien
Apothekertrakt und Orangerie

Praxisbericht IT Sicherheitsvorfälle – Konsequenzen und Möglichkeiten der Prävention

Ing. Thomas Mandl, Sr. Security Consultant, Inhaber Cyber Defense Consulting Experts
thomas.mandl@cdce.at

Präsentiert von

HIMSS CHIME INTERNATIONAL

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Österreichische Gesellschaft für Biomedizinische Technik
Austrian Society for Biomedical Engineering

OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

UMIT

AGENDA

- Einleitung – Rückblick auf aktuelle Sicherheitsvorfälle
- Praxisbericht Sicherheitsvorfälle – was kann alles passieren?
- Grenzen der Schutztechnologie und Lösungsansätze

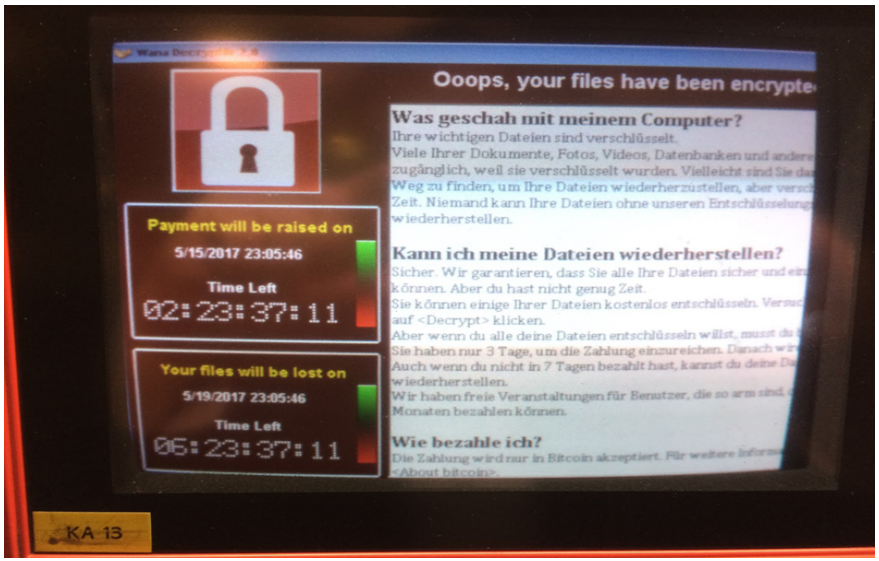
ING. THOMAS MANDL - WER BIN ICH?

- Seit 1988
  - 8 Jahre Alcatel Research Center (Eisenbahnsicherungstechnik), Inhaber EU Patent
- 22 Jahre IT und IT-Security Erfahrung
  - Sr. IT Admin, später IT Leiter bei Analog Devices & Leitung World Wide UNIX Security Team
- 5 Jahre Anti-Virus Industrie (CTO von Ikarus Security Software)
- Lektor
  - Seit 2003. Lektor an der Donau-Uni Krems, Seit 2006 Lektor an der FH Technikum Wien
- Mitgliedschaften
  - Stv. Vorsitzender CERT.at Beirat, Mitglied in AIT Projektteams zum Schutz krit. Infrastruktur
- Seit 2009
  - selbständig, Sr. Security Consultant – Cyber Defense Consulting Experts

VORWORT ZU WANNACRY RANSOMWARE (12. MAI 2017)

Deutsche Bahn

Parkautomaten, Flughafen Berlin/Tegel



Quelle: https://heise.de/-3713426

MASSENWEISE INFEKTIONEN VON COMPUTERSYSTEMEN

In ganz England hat ein Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgelegt. Und das ist offenbar nur die Spitze des Eisbergs einer globalen Welle von Infektionen mit Wana Decrypt0r 2.0 oder einfach WannaCry.

In ganz England sind Krankenhäuser offenbar Opfer eines Cyberangriffs, bei dem die Angreifer Computer mit Krypto-Trojanern sperren und nur gegen ein Lösegeld wieder freigeben wollen. Wie der *Guardian* berichtet, sind Krankenhausverbände im Süden und Norden Englands betroffen. Die IT ist dort entweder wegen des Trojaners nicht mehr benutzbar, oder weil Rechner aus Vorsicht heruntergefahren wurden. Teilweise werden Patienten gebeten, nicht in die Notaufnahmen zu kommen, sondern nur Notrufnummern zu wählen. Der Nationale Gesundheitsdienst hat inzwischen erklärt, dass der Angriff wohl nicht gezielt war, die IT-Abteilung eines Krankenhausverbunds in Liverpool spricht von einem "mutmaßlich nationalen Cyberangriff".

Quelle: https://heise.de/-3713235

HABEN WIR WIRKLICH NICHTS DAZUGELERNT?

ZDNet / Sicherheit

Warnung: Wurm „Conficker.C“ infiziert tausende Computer

Neue Malware-Variante nutzt Microsoft-Schwachstelle MS08-067 und USB-Anschluss zur Verbreitung

von Britta Widmann am 13. Januar 2009 , 17:53 Uhr

Laut Panda Security ist derzeit die Gefahr einer Infektion durch den Wurm Conficker.C groß. Er stellt die dritte Variante einer neuen Malware-Familie dar. Die Varianten A, B und C sind bereits für tausende Infektionen verantwortlich.

Conficker.C nutzt die Microsoft-Schwachstelle MS08-067. Dabei versucht er, in Netzwerke mit einem schwachen Administrator-Kennwortschutz zu dringen, indem er eine Reihe häufiger Passwörter durchprobiert. Gelingt ihm der Zutritt, verbindet er sich mit der RPC-Schnittstelle (Remote Procedure Call). Darüber hinaus dient auch der USB-Anschluss als Ausgangspunkt einer Infektion.

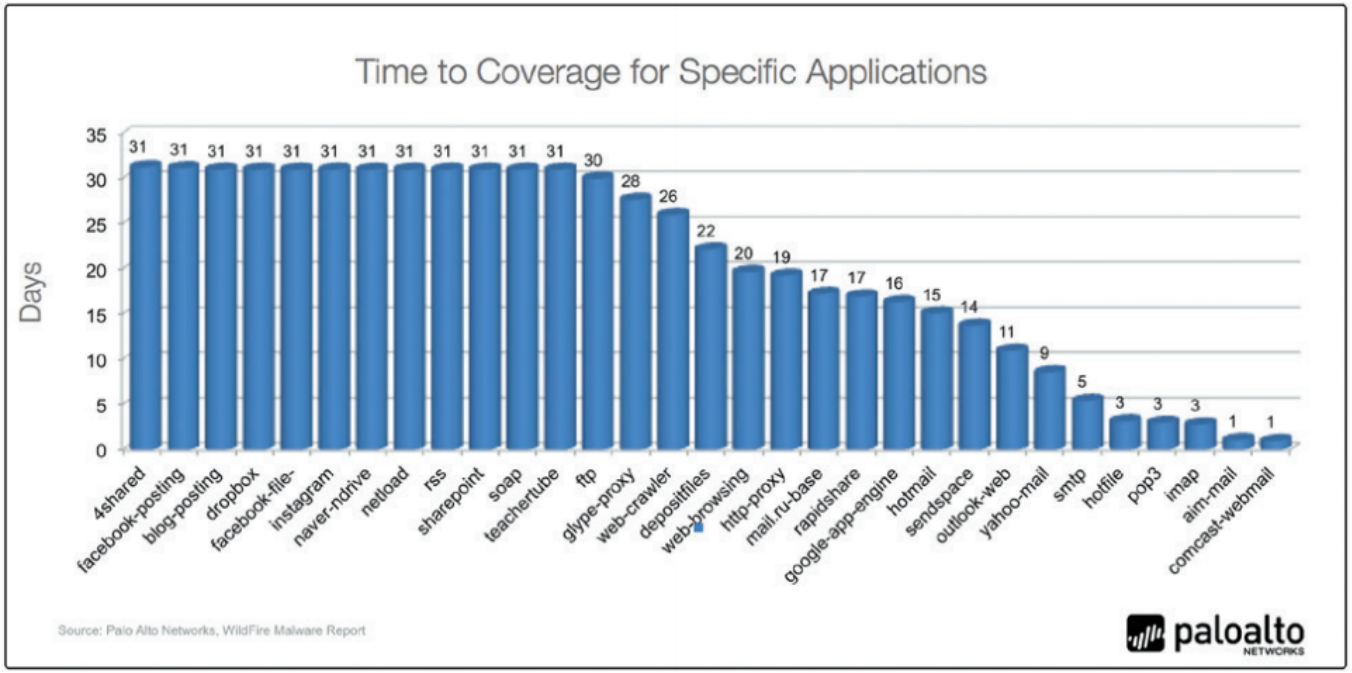
Quelle: http://www.zdnet.de/39201150/warnung-wurm-conficker-c-infiziert-tausende-computer/

DIE
(FRÜH)ERKENNUNG
VON RANSOMWARE IST
(VERGLICHEN MIT ANDEREN CYBER-BEDROHUNGEN)
SEHR EINFACH!

ABER DIE ABWEHR VON CYBER-ANGRIFFEN IST SEHR KOMPLEX UND BEDARF ZUSÄTZLICHER (TECHNISCHER U. ORGANISTORISCHER) MASSNAHMEN!

LIVE DEMO “ENDPOINT ATTACKE”

REAKTIONSZEITEN KLASSISCHER ANTI-VIRUS LÖSUNGEN



Quelle: „The modern Malware Review, March 2013“ (Paloalto Networks, 2013) S.7
http://media.paloaltonetworks.com/documents/The-Modern-Malware-Review-March-2013.pdf

CONCLUSIO

- Kaum Bewusstsein vorhanden selbst nachdem etwas passiert ist,
  - da unmittelbar keine Konsequenzen erkennbar (Ausnahme bei Ransomware)
- Unternehmen sind selten auf Sicherheitsvorfälle vorbereitet
  - Kaum Nachvollziehbarkeit von “Aktivitäten eines Angreifers” im Netzwerk vorhanden (EUDSGVO)
  - Kaum Log Management, keine Big Data Analyse Tools (SIEM) im Einsatz
  - Wenig Security Know-How bei ”First Responder” (interne IT) – unabsichtliche Beweisvernichtung
  - Forensische Untersuchungen werden kaum durchgeführt, sind aber essentiel um festzustellen, was genau passiert ist und was der Grund für den Sicherheitsvorfall war
  - Notfallprozesse manchmal vorhanden, aber nicht immer aktuell oder nur auf klassische IT Themen beschränkt (Ausfall eines IT Systems, aber nicht flächendeckend Malwarebefall)
  - Meist nur ”reaktives” Handeln, Schadsoftware hinterlässt i.d.R. immer Indicators of Compromise (IOC), aber solange keine präventive Sicherheit gelebt wird (inhouse CSIRT Team) wird man immer “hinten nachsein” und erfolgreiche Angriffe nicht rechtzeitig erkennen können.

LÖSUNGSANSÄTZE

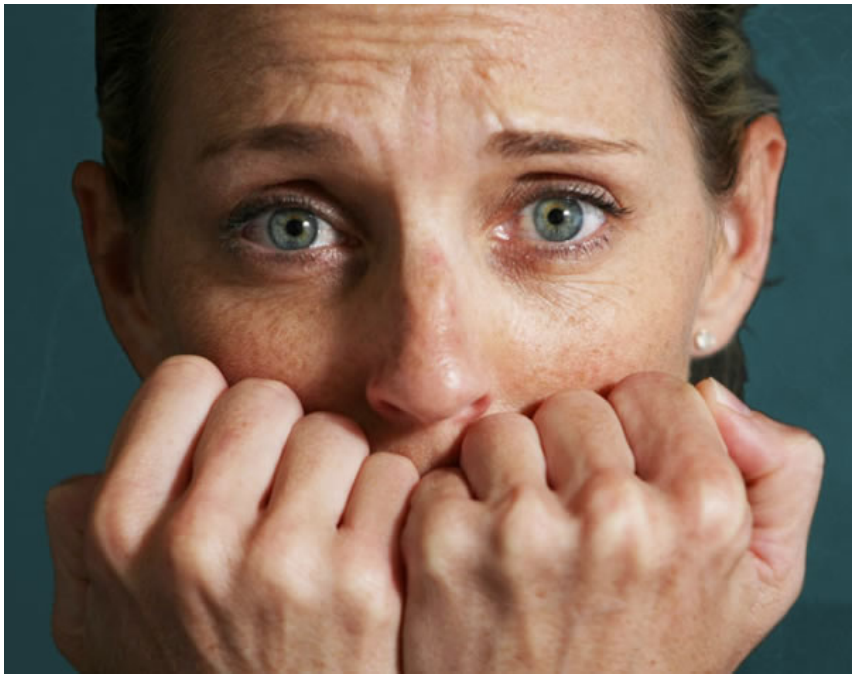
- Aufbau von Awareness, IT Grundlagen vermitteln, Anwender fallen auf die simplesten Tricks rein – kaum Aufwand für Angreifer
- Ausbau von IT Grundschutz– richtige Auswahl von Schutztechnologie (Fleckerteppich vs. Key Account Manager)
- Aufbau von CSIRT Teams und Prozessen, um proaktiv nach Anzeichen (IOC) von Angriffen suchen und Gegenmaßnahmen einleiten
- Nachvollziehbarkeit schaffen - Big Data Analysetools kombiniert mit menschlichem Know-How planen und einsetzen

- "Obduktion" (vgl. dig. Forensik) durchführen, nur dann wissen wir warum ein Angriff erfolgreich war, und evtl. welche Daten/Systeme noch betroffen sind
- Realistische Audits (DPI) durchführen, und nicht nur "just another PenTest"

WAS LERNEN WIR VON DER MEDIZIN?

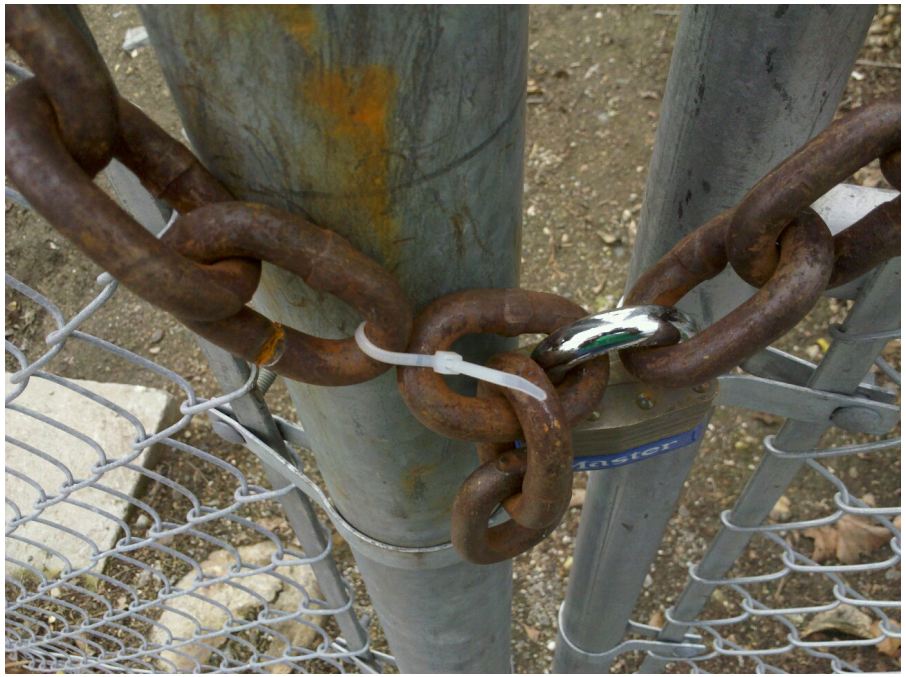
- Je früher wir eine schlimme Krankheit entdecken, umso eher besteht Heilungschance
- Vorsorgeuntersuchungen (Prävention) sind daher besondern wichtig geworden
- Ohne genaue Analyse der Begleitumstände und Rahmenparameter (Blutbild, MRT/CT, …) einer Krankheit, keine genaue Diagnose
- Security Incidents "trainieren" und Verhaltensregeln aufstellen (vgl. Notfallmedizin)
- Orga. Prozesse schaffen um Technik & Mensch zu unterstützen

BITTE VERSTEHEN SIE DIE GEZEIGTEN FAKTEN NICHT FALSCH

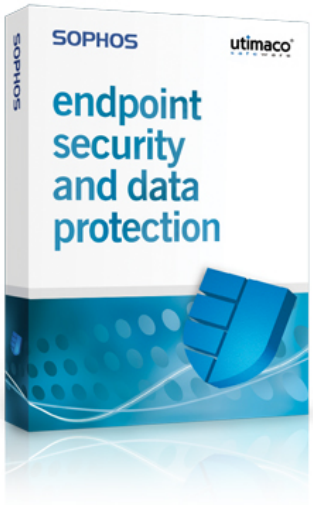


ABER DAS FUNKTIONIERT SCHON LANGE NICHT MEHR

UNSERE SITUATION HEUTE



WIR HABEN SCHON (FAST) JEDE TECHNOLOGIE



Warum sind dann Cyber-Angriffe noch immer so erfolgreich?

WIR MÜSSEN UNSER DENKEN U. HANDELN ANPASSEN

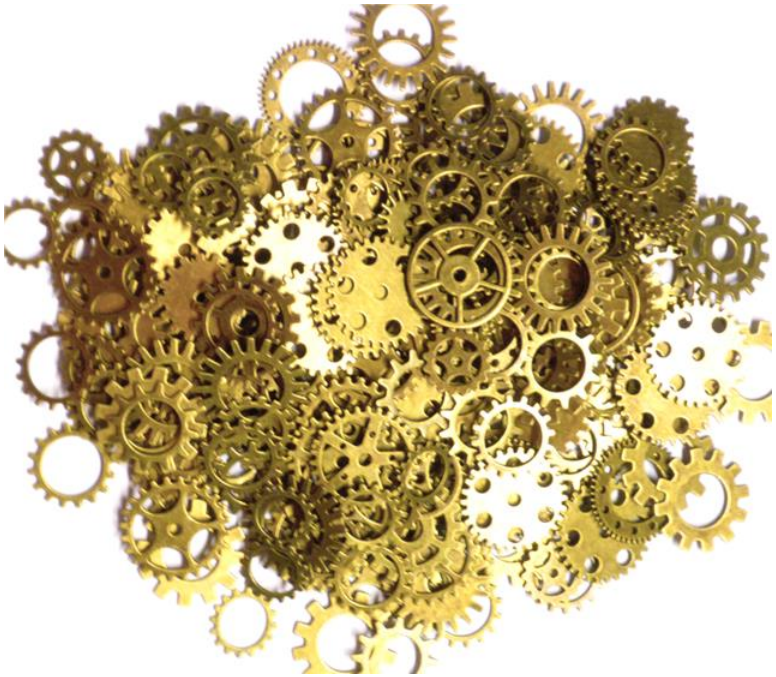
IN ANDEREN BEREICHEN AKZEPTIEREN WIR SICHERHEITSVORGABEN JA AUCH!

versus

TECHN. LÖSUNGEN ALLEINE HELFEN NICHT (MEHR)! ÜBERTRIEBENE VORSICHT BREMST PRODUKTIVITÄT

SICHERHEITSKONZEPTE MÜSSEN PRAKTIKABEL WERDEN, AWARENESS AUFBAUEN

NUR WEN SICHERHEITSMASSNAHMEN AUFEINANDER ABGESTIMMT SIND SIND DIESE AUCH EFFEKTIV!



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Kontaktdaten

Ing. Thomas Mandl
Sr. Security Consultant und Inhaber
Cyber Defense Consulting Experts e.U.
eMail: thomas.mandl@cdce.at
Mobile: +43 664 392 16 68
Web: www.cdce.at