SICHERHEIT ALS RÜCKGRAT DER DIGITALISIERUNG

STREAM TECHNIK 1

Luzern, 22.6.2017

Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
Informatik

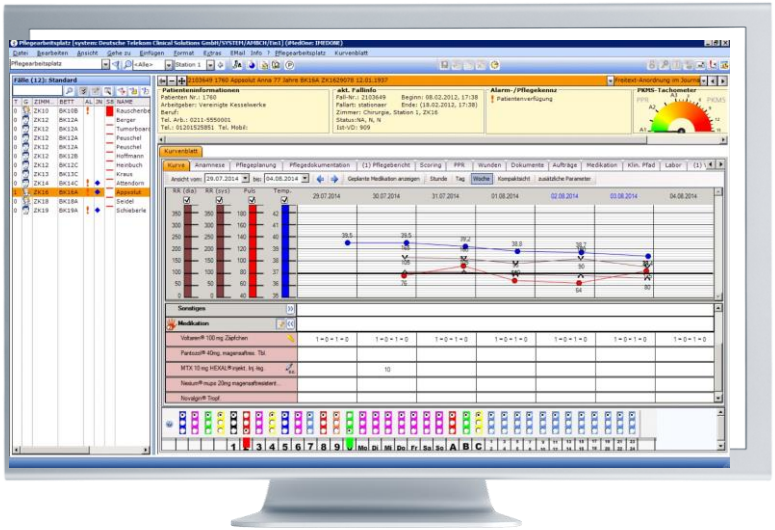
Timo Baumann

HEALTHCARE SOLUTIONS

WIE SCHÜTZEN WIR UNSERE SPITÄLER VOR CYBER-ANGRIFFEN?

»IT-SICHERHEIT IST EIN PROZESS, KEIN PRODUKT. UND NIE WAR ES EINFACHER, AUF AUGENHÖHE MIT ANGREIFERN ZU KOMMEN.«

IST CYBER SICHERHEIT EIN NEUES TREND THEMA?



CYBER-VERSICHERUNGEN. AUCH EIN WEG.

KOSTEN DURCH CYBER-ANGRIFFE

- 50-60 Millionen $ p.a. in D
- Bsp. Krankenhaus 1 Mio €

VISION: AUCH PRIVAT UND KMU

- 1/3 Privathaushalte, 150-200€ p.a.
- 1/2 Unternehmen bis 5 Mio.€ Umsatz p,a,

DURCHDRINGUNGSGRAD

- 4.000-5.000 Unternehmen von ca. 3,6 Mio.
- „Cyber hat das Potenzial, der Kfz-Versicherung im Laufe der nächsten 20 Jahre den Rang als volumen-stärkste Schaden/Unfall-Versicherungssparte abzulaufen.“

Quelle: Zwischen Panik und Euphorie, Handelsblatt, 16.5.2017; Riesiges Potenzial, Börsenzeitung 9.2.2017

SO SICHERN WIR DIE SPITÄLER BISHER. REICHT DAS AUS?

- Virenscanner Server und Clients
- Mobile Device Management
- Windows-Ökosystem per WUS
- File-Rechte
- Aktualisierung der 3rd party tools wie z.B. Adobe-Software
- DMZ, Firewall
- VPN-Zugänge
- ...

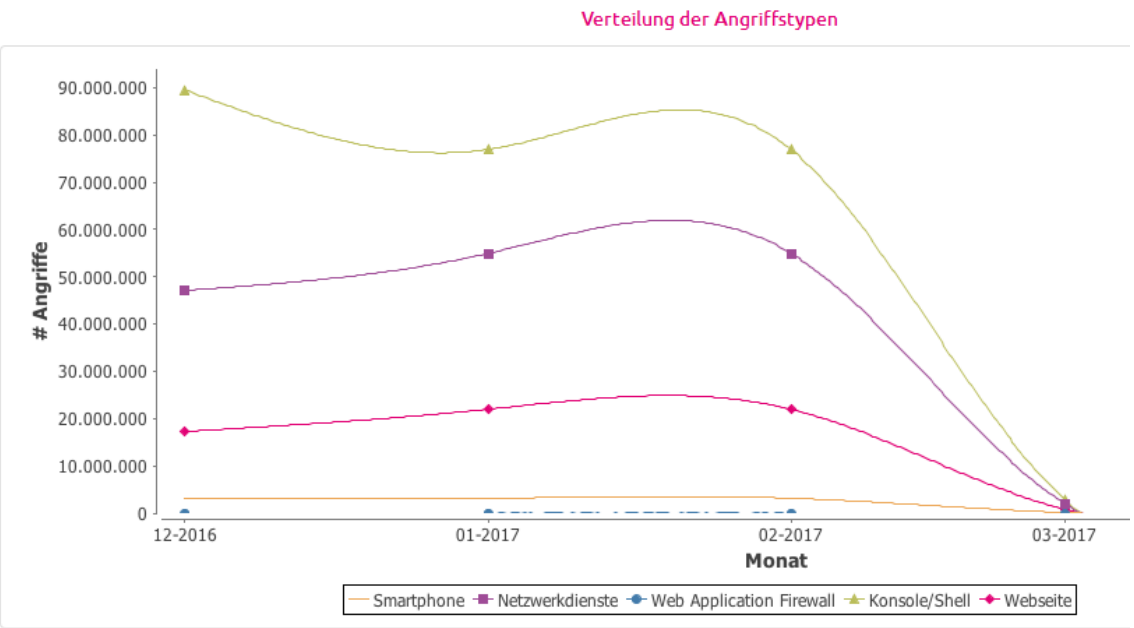
IM CYBERSPACE IST DIE HÖLLE LOS.

- Telekom Honeypots: 4 bis 6 Millionen Angriffe täglich
- Vergleichszeitraum des Vorjahres noch 500.000
- >220.000 Mails und Briefe von Telekom jeden Monat an Kunden, deren Rechner von Kriminellen missbraucht werden
- 2015 verschickte das Abuse-Team 2.704.462 Mails und Briefe und erhielt 25.617.165 Hinweise. 2014 waren es 938.471 Mails und Briefe und 21.875.441Hinweise, 2013 verschickten wir 424.925 Mahnungen und 11.484.413 Hinweise.
- Mehr Infos unter www.telekom.com/abuse

68 % der Unternehmen hatten in den **letzten 6 Monaten** eine **Infektion mit Ransomware**	**3,6 Mio. €** **durchschnittliche Kosten** durch Datenschutz-verletzungen	**69 %** von **Wirtschaftsspionage, Sabotage und Daten-diebstahl** betroffene Unternehmen

DIESE TECHNOLOGIEN WERDEN ANGEGRIFFEN.

SICHERHEITSTACHO.EU



neueste Meldungen

2017-06-19 2017-0846	Linux Kernel: Schwachstelle ermöglicht Offenlegung von Informationen
Neu	
2017-06-19 2017-0845	QT: Schwachstelle ermöglicht Offenlegung von Informationen
Neu	
2017-06-19 2017-0844	PHP: Mehrere Schwachstellen

DCERT.DE

KENNEN SIE DIESE GRUPPIERUNGEN?

- Anonymous
- Lizard Squad
- Lulz Security
- Syrian Electronic Army

KENNEN SIE DIESEN MARKT?

Wert von digitalen Daten

1 Cent

für **persönliche Daten**
wie Haushaltseinkommen,
Ehestand, Wert des Hauses

4,34 $

pro **Facebook-Profil**

0,85 $ – 30$

für **Kreditkarteninformationen**
auf dem Schwarzmarkt

60$

für eine **Patientenakte**
auf dem Schwarzmarkt

Ein typischer Datensammler verfügt über 50 Mio. Privatadressen aus Deutschland und 10 Mrd. Zusatzinformationen.

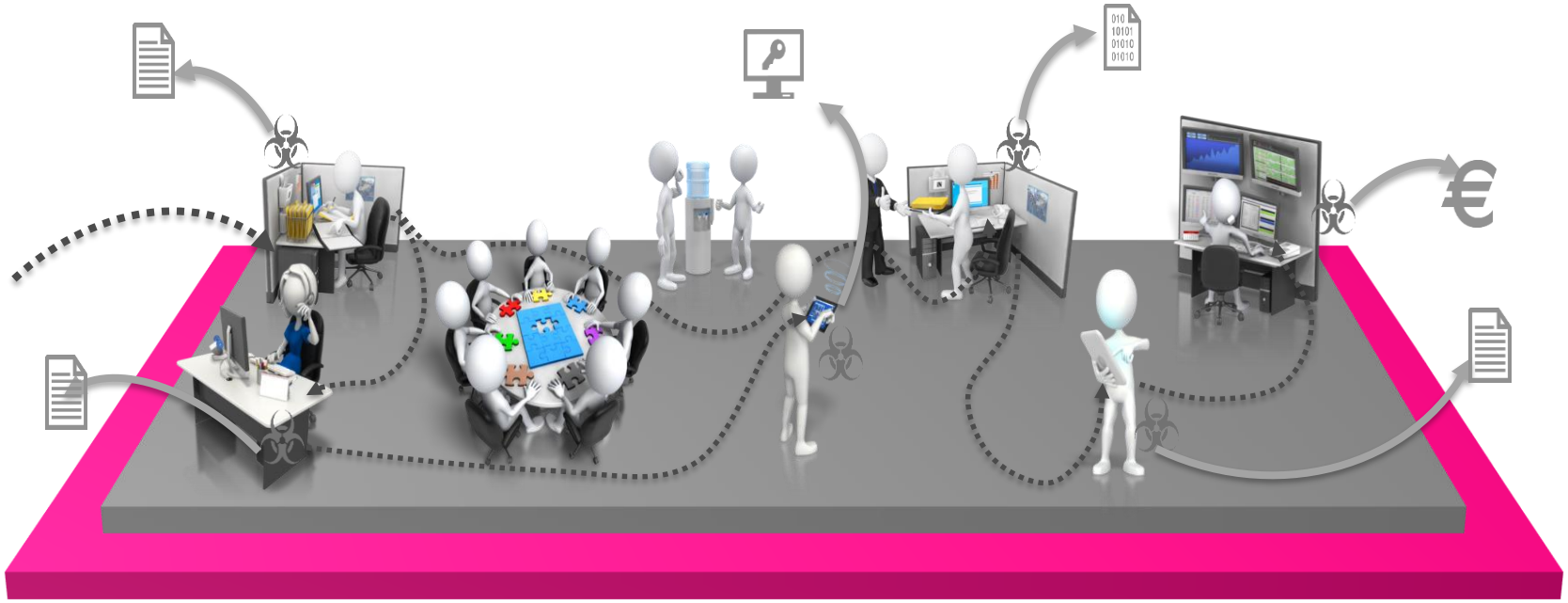
Quelle: www.bpb.de/gesellschaft/medien/wissen-und-eigentum/73338/datenhandel?p=all
und Trendguide 2016
EHEALTHCOMPENDIUM

CYBER SECURITY BEDEUTET EINEN PARADIGMEN-WECHSEL. VON FIREWALLS UND ANTIVIRUS ...

Firewalls und Perimeter Sicherheit

Anti-Viren-Installationen auf Clients und Servern

… ZU ADVANCED PERSISTENT THREATS.



Initial exploitation ➡ Command and control ➡ Privilege escalation ➡ Data exfiltration ➡ Intelligence gathering

INFI-
ZIERUNG

UNENTDECKTE ANGRIFFE

SCHADENS-
BESEITIGUNG

209 TAGE Zeitraum, in denen Angreifer im Netz präsent sind, bevor sie entdeckt werden.

> There are two types of companies that use computers:
> Victims of cyber crime that know they are victims and victims of cyber crime that don't have a clue **yet.**

James Routh, 2007
CISO Depository Trust and Clearing Cooperation

EINFACH NUR WIEDERHERSTELLEN SCHLIESST NICHT DAS EINFALLSTOR.

Payments In Ransomware Attack On Hospital

May 25, 2016 - By Chris Brunau

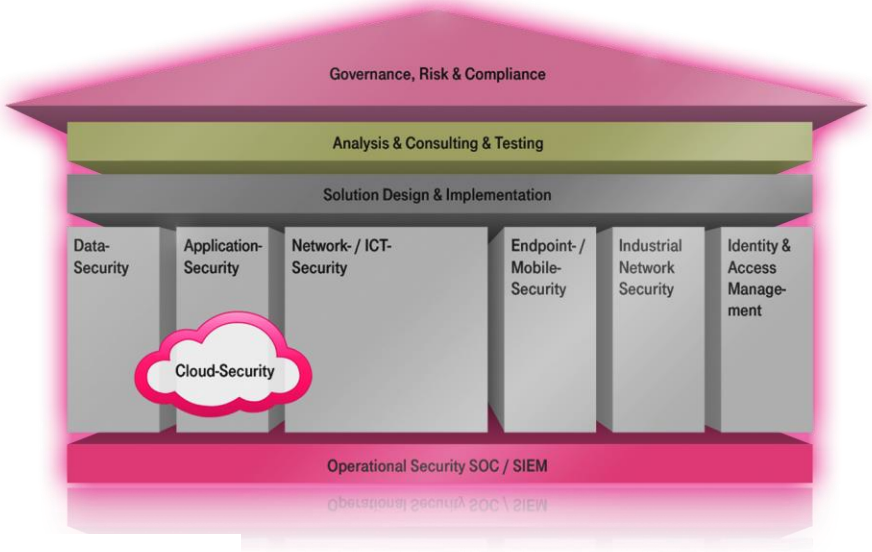
The trend of ransomware attacks on hospitals just keeps on go
World, Kansas Heart Hospital in Wichita was hit with an attac

... nach der ersten Lösegeldzahlung verlangten die Hacker mehr Geld.

While little information is readily available about the attack, the hospital did pay an undisclosed ransom (referred to as a 'small amount' by Hospital President Dr. Greg Duick) to regain access to their files. And, after the first ransom payment, the hackers demanded more money, according to FierceHealthIT.com. This is further proof that paying a ransom doesn't guarantee the integrity or safe return of your data. Even though you can't fully protect yourself from an attack, you can take precautions to limit data loss and downtime. With a modern BCDR solution, you can restore critical business data to a point in time before corruption occurred and avoid paying a hefty ransom.

BEWÄHRTES VORGEHEN: IT-SECURITY IST EIN PROZESS, KEIN PRODUKT.

ZITAT; UM DIE JAHRTAUSENDWENDE.



Phase	*Arbeitsschritte*
Vorbereitende Aktivitäten	Schritt 1: IT-Risikoanalyse als Projekt initialisieren Schritt 2: Schutzziele festlegen Schritt 3: Untersuchungsbereich abgrenzen Schritt 4: Prozesse erheben
Kritikalität analysieren	Schritt 5: Kritische Prozesse ermitteln Schritt 6: IT-Unterstützung ermitteln Schritt 7: Kritikalität der IT-Unterstützung bestimmen Schritt 8: Kritische IT-Komponenten ermitteln
Risiken identifizieren und bewerten	Schritt 9: Risikoszenarien ermitteln Schritt 10: Eintrittswahrscheinlichkeiten abschätzen Schritt 11: Auswirkungen bewerten Schritt 12: Risikowert ermitteln Schritt 13: Bestehende Maßnahmen berücksichtigen
Risiken behandeln	Schritt 14: Behandlung der Risiken entscheiden Schritt 15: Präventive Maßnahmen bestimmen und Ersatzverfahren vorsehen

Quelle: BSI, Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT, Leitfaden

UND WIR BRAUCHEN AUCH NEUES HANDWERKSZEUG.

1. Vorbeugen

- Analyse des IST-Zustands, priorisierte Handlungsempfehlungen.
- z.B. Standort-Bestimmung, Mitarbeiter-Sensibilisierung oder Penetrations-Tests.
- Schwachstellen-Scan aaS zur lfd. Prüfung von innen/außen.

2. Erkennen

- z.B. Drohnen Sicherheit zur Detektion, Alarmierung und Dokumentation, insbesondere im Bereich von Hubschrauber-Landeplätzen.
- z.B. Internet Protect Pro, die Datenwaschmaschine aus dem entfernten RZ.

4. Vorhersagen

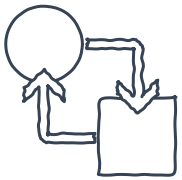
- Advanced Cyber Defense: Managed Service aus der Telekom-Cloud (alternativ auch Betrieb im Krankenhaus).
- Netzwerk-Sicherheits-Monitoring + vorhandene Logs (z.B. Firewall, MS Active Directory) werden korreliert (Security Incident and Event Management), Reporting + monatliche Reviews.

3. Reagieren

- Incident Response Service: Bei Angriffen stehen über eine 24*7-Notfallrufnummer versierte Ansprechpartner der Telekom zur Verstärkung der KH-IT bereit.
- z.B. 30 min telefonische Reaktionszeit und inklusive 5 Consulting-Tage für Reaktion auf einen Intrusion Incident, forensische und Malware-Analysen.

SO FUNKTIONIERT CYBER DEFENSE BISHER.

CLIENTS	NETWORK	SERVICES	PROCESSES
ANTI-VIRUS	FIREWALLS ANTI-SPAM	ANTI-VIRUS	RISK MGMT



SO FUNKTIONIERT DAS VORHERSAGEN MIT SIEM ...

CYBER DEFENSE

SECURITY VISIBILITY

THREAT INTELLIGENCE

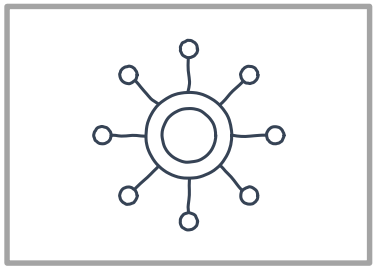
COMBINED REPORTING

MONITORED BY SECURITY OPERATIONS CENTER (24X7)

FIREWALLS

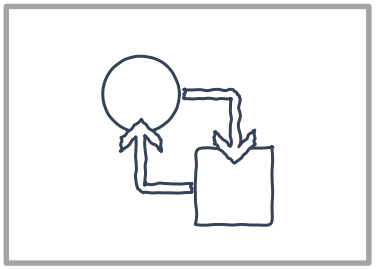
ANTI-VIRUS | ANTI-SPAM | ANTI-VIRUS | RISK MGMT

CLIENTS



NETWORK

SERVICES



PROCESSES

… ABWEICHUNGEN VOM NORMALZUSTAND ERKENNEN.

SENSOR

- Sammelt Informationen ein, normalisiert und gibt sie an Server weiter
- Events sammeln
  z.B. 1x Perimeter Firewall, 1x Forwarding Proxy, 1x VPN Gateway, 1x Antivirus, 2x Active Directory; ca. 200-400 Events/s, 3GB logs/d
- Netzwerkverkehr analysieren
- Schwachstellenscans ausführen
- Assets inventarisieren

SERVER

- Das Kommandozentrum
- Threat Intelligence
- Korrelation
- Zentrales Management
- Bedienoberfläche

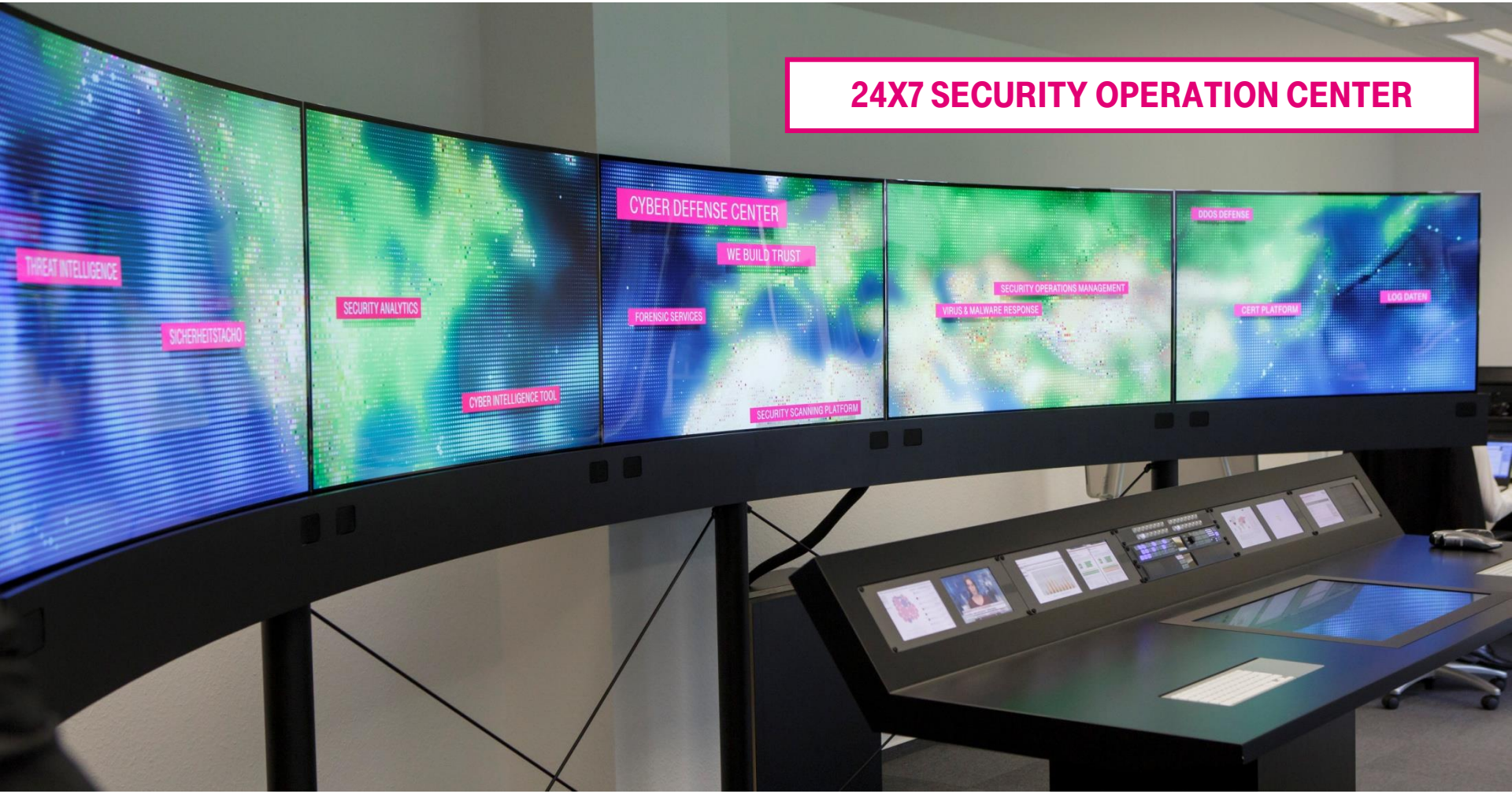
LOGGER

- Sichere Langzeitarchivierung
- Speichert Events für Compliance und Forensik-Zwecke
  z.B. 90 Tage Datenzurück-haltung
- Digital signierte Archivierung

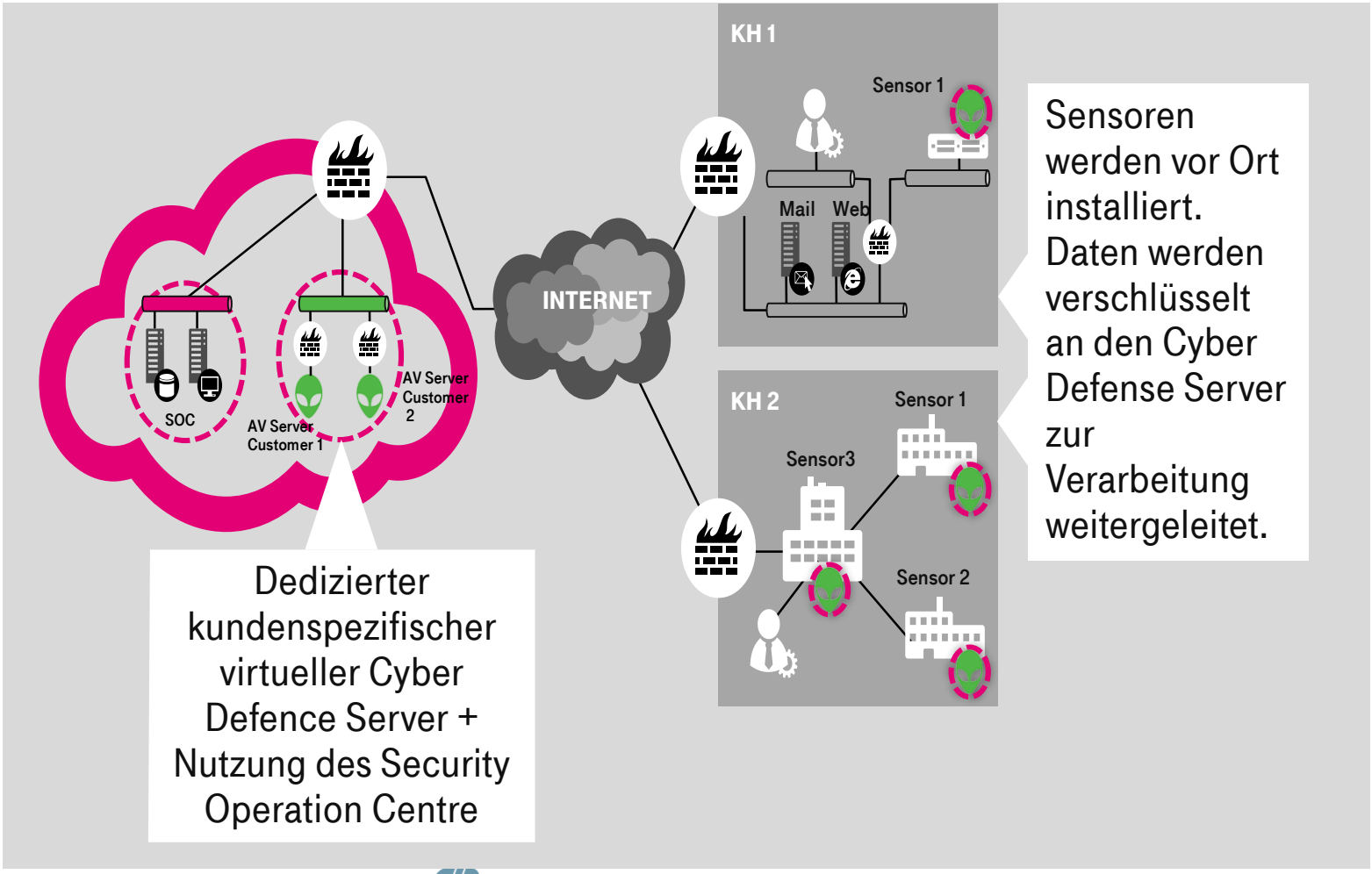
+

24X7 SECURITY OPERATION CENTER

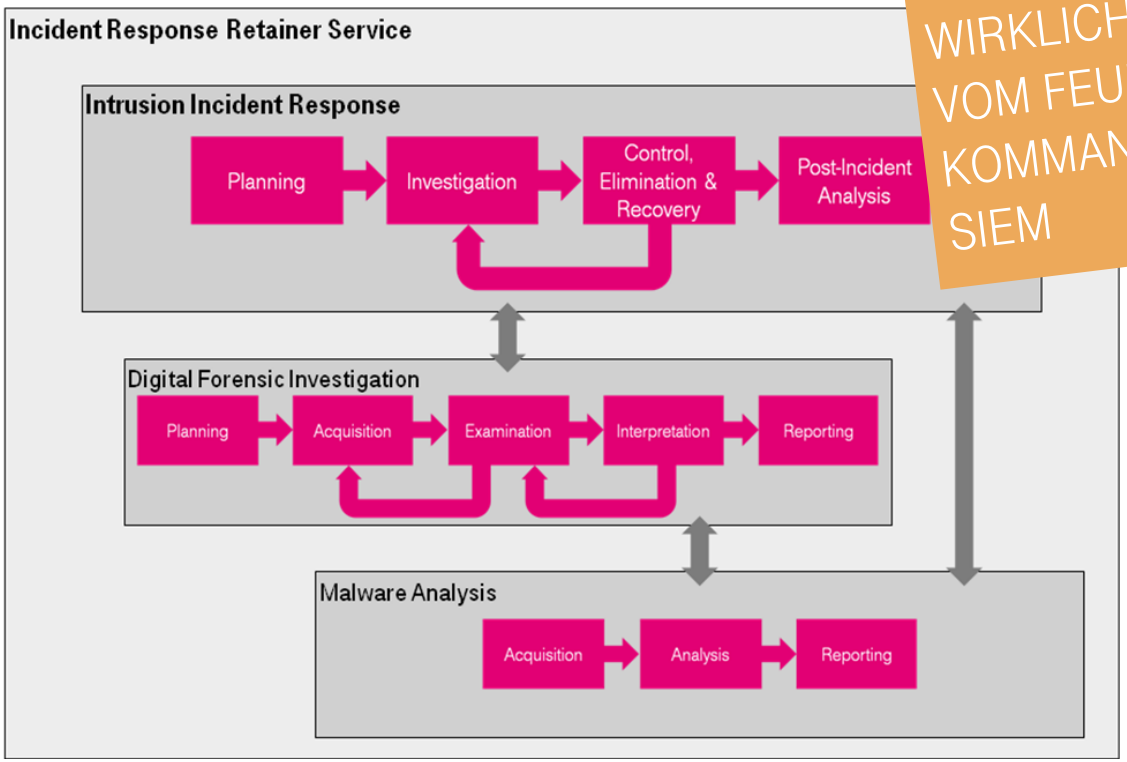
WER REAGIERT AUF EINE CYBER ATTACKE?



GETEILTE UMGEBUNGEN BAUEN DIE EINSTIEGS-HÜRDEN FÜR CYBER DEFENSE AB.



INCIDENT RESPONSE: WAS ZU TUN IST BEI EINEM ANGRIFF.



WIRKLICH PASSIERT: VOM FEUERWEHR-KOMMANDANTEN ZUM SIEM

- JUST REINSTALLING A SERVER OR A DESKTOP SYSTEM WILL NOT FIX THE PROBLEM, THE ATTACKER WILL COME BACK BY THE SAME WAY AS BEFORE.
- IF YOU DO NOT KNOW, HOW THE ATTACKER IS WORKING, YOU CANNOT FIGHT HIM!
- IF YOU DO NOT KNOW, WHAT THE ATTACKER DID, YOU CAN NOT ESTIMATE THE DAMAGE!

»IT-SICHERHEIT IST EIN PROZESS, KEIN PRODUKT. GLEICHWOHL MÜSSEN WIR ETWAS AUFRÜSTEN, UM UNSERE SPITÄLER ZU SCHÜTZEN.«

„Innerhalb von wenigen Stunden war das gesamte System installiert, startklar und zeigte erste Ergebnisse. Wir hatten so eine betriebsbereite SIEM-Lösung. Sehr zufrieden sind wir auch mit der webbasierten Oberfläche, die Wesentliches von Unwesentlichem trennt und schnelle Entscheidungen ermöglicht. Außerdem können wir viele weitere Security-Komponenten anbinden."

Sascha Müller, stellvertretender IT-Leiter des Robert-Bosch-Krankenhauses

VIELEN DANK

www.telekom-healthcare.com

DIPL.-INFORM. MED. TIMO TOBIAS BAUMANN, MBA
timo.baumann@t-systems.com