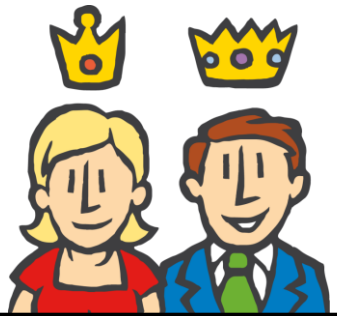
das Krankenhaus im Fokus der Organisierten Kriminalität (OK)

kombinierte Angriffsvektoren aus CyberCrime, physischer Security und Betrug

Zoom-Webinar, 06.09.2021



WISAG

FACHVEREINIGUNG KRANKENHAUSTECHNIK E.V.

Das Krankenhaus im Fokus der Organisierten Kriminalität (OK)

kombinierte Angriffsvektoren aus

- **CyberCrime**
- **physischer Security**
- **Betrug**

WISAG

Agenda

Agenda

- Angriffsziel Krankenhaus
- Kurzvorstellung der Angriffsvektoren
  - CyberCrime
  - physische Security
  - Betrug
- Hintergründe ("Wo", "Wer", "Warum" und „Wie“)
- Beispielrisiken
- Gegenmaßnahmen
- Diskussion

WISAG

Kurzvorstellung Referent

Thomas Schuy
Senior Consultant
Sec-IT

Aufgaben

- Risikoanalysen
- Sicherheitskonzepte
- SecurityProzesse / ITIL4-Prozesse
- Betrugsermittlung
- BSI-Grundschutz

Erfahrung

- 30 Jahre in IT-Security und IT-Operations
- Industrial IT, SCADA, OT, IIoT
- Drohnendetektion und -abwehr
- F&E mobiler Schutz für high-value-Transporte
- F&E mobiler Notruf (über- und unterirdisch)
- Projektplanung von Großprojekten uvm.

WISAG

Angriffsziel Krankenhaus

Frage: Warum ist ein Krankenhaus ein attraktives Angriffsziel für die Organisierte Kriminalität (OK)?

- hohes „Marktpotential“
  - Roland Berger: „64% der KH in D wurden 2017 Opfer eines Hackerangriffs“
  - Bitkom: „88% der Unternehmen in D waren in 2020/21 von Datenklau, Spionage oder Sabotage betroffen“
  - Bitkom: „Schadenssumme 220 Mrd € p.a. in 2020/21 mehr als doppelt so hoch als 2018/19“
- Allianz Risk Barometer: „Cyber steigt zum weltweiten Top-Risiko für Unternehmen auf – noch vor Betriebsunterbrechungen“
- starke Druckmittel („gefährdete Menschenleben“)
- sehr leichte Beute
  - Raub und Diebstahl
  - „Selbstbedienungsladen“

Kurzvorstellung der Angriffsvektoren

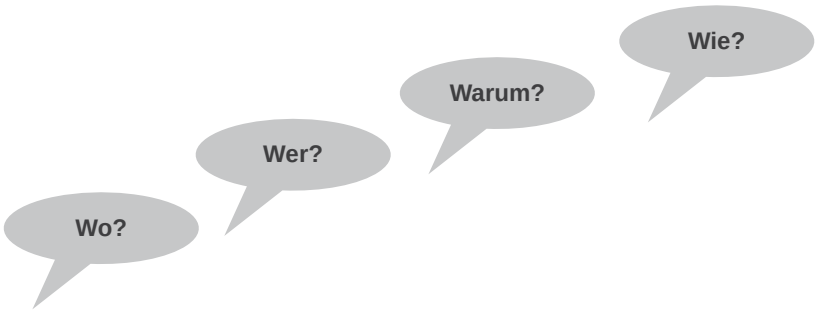
CyberCrime
- Ransomware (Gesundheitssystem Irland / Uniklinik Düsseldorf)
- Datenabfluß (NextMotion (F) >100K Datensätze / 2.300 DICOM/PACS-Server 24 Mio. Personen aus 52 Ländern und 373 Mio. Bilddaten)

physische Security
- Diebstahl/Raub (medizinische Geräte / BTM)

Betrug
- feindliche Übernahme – Kaufpreis reduzieren
- Immobilien = gering kontrollierte Bereiche für Geldwäsche (ML)
- Abrechnung Rezepte (AvP Rezeptabwickler / Apotheke zu Krankenkassen)

Hintergründe

Hintergründe



Hintergründe "Wo" bestehen diese Risiken?

Arbeitsprozesse (BCM)

- Regelprozesse (OP, Diagnostik, Apotheke, Pflege usw.)
- Störfallprozesse (Notfallversorgung, Katastrophenfall)

OfficeIT (IT)

- Dokumentation
- Patientendaten (DSGVO, Patientendaten-Schutzgesetz (PDSG), IT-SiG 2.0)
- Dienstleister- & Lieferantendaten (GeschGehG, IT-SiG 2.0, VerSanG)
- zukünftig: Telematikinfrastruktur (ePA, eAU, eMP, eRezept, NFDM)

Hintergründe "Wo" bestehen diese Risiken?

Wo?

Operational Technology (OT)

- Gebäudeleittechnik (GLT) (KRITIS-VO, IT-SiG 2.0, VerSanG)
  - Strom
  - Kommunikation
  - Wasser
  - Wärme
- Krankenhaustechnik / medizinische Geräte
  - Intensivbetreuung (Monitoring, Beatmung usw.)
  - Radiologie-Arbeitsplätze (Röntgen, CT, MRT, Ultraschall)
  - HL7-Gateways (Austausch klinischer Dokumente im Gesundheitswesen)
  - PACS-Archive (Picture Archiving and Communication System)
  - Strahlentherapiesysteme
  - Sterilisation
  - zukünftig: Telemedizin

Hintergründe "Wer"?

Wer?

Tätergruppe: Organisierte Kriminalität (OK)

OK-Definition lt. BKA:

- „Gruppierungen, die kriminelle Ziele systematisch verfolgen“
- „Bandenkriminalität“
- Gewinnerzielungsabsicht der Täter (Markt: 220 Mrd € p.a. in D)
- umfasst nicht Straftaten des Terrorismus

Strafgesetzbuch

- organisierter Kriminalität (§ 129, Bildung krimineller Vereinigungen)
- Terrorismus (§ 129a, Bildung terroristischer Vereinigungen)

Transnationale Ausrichtung

- die OK in Deutschland ist stark von international agierenden Gruppen geprägt
- 80 Prozent der Ermittlungsverfahren haben internationalen Bezug

Hintergründe "Warum"?

„Gib den Menschen ein ´Warum´ und sie verstehen das ´Wie´."

"Warum" hat denn die OK überhaupt Interesse an der Zielgruppe „Krankenhaus"?

- „Gewinnerzielungsabsicht der Täter" (Zitat BKA)
- „Das Ausmaß und die Komplexität der Geldwäsche-Aktivitäten in der EU sind unterschätzt worden" (Zitat Europol)
- Krankenhäuser sind sehr leichte Beute („Selbstbedienungsladen")
- in Krankenhäusern gibt es starke Druckmittel („Menschenleben")

Hintergründe "Wie"?

zwischen dem "Wo", "Wer" und "Warum" verbleibt nur noch der Weg - das "Wie"

- hybride Angriffe werden immer häufiger
- Kombination von physischen und IT-Angriffen
- industrielle Aufgabenaufteilung „crime as a service"
  - automatisierte Breitband-Analyse auf Sicherheitslücken
  - Bewertung der dahinterliegenden Opfer auf potentiellen Marktwert (A, B, C)
  - Verkauf der Daten an spezialisierte Zielgruppen (Uniklinik Düsseldorf war ein Versehen)
  - Daten-Exfiltration (meist über mehrere Monate)
  - Ransomware: gemietete Softwarelösung (z.B. "REvil" lizenzbasiertes Geschäftsmodell / prozentuale Beteiligung)
  - „Zweitvermarktung" mittels der vorher heruntergeladenen Daten (Erpressung / Verkauf)
  - „Drittvermarktung" an andere Tätergruppen („wer einmal bezahlt hat, zahlt auch zweimal")

Beispielwerkzeug für einen hybriden Angriff

Werkzeug für einen hybriden Angriff
(Einbringen eines IT-Tools über physisches Team)

WISAG

HERAUSFORDERUNGEN

Themenfelder

Gefährdung
- physikalische Angriffe
- Cyber-Angriffe
- kombinierte Angriffe

Tätergruppen
- organisierte Kriminalität (OK)
- Beschaffungskriminalität
- staatliche Akteure
- Besucher / Patienten

Allgemeine Risiken
- Personalbedrohung
- Patientenbedrohung
- Ransomware
- Diebstähle / Raubüberfälle
- in- / externe Straftaten

Juristische Risiken
- DSGVO, GeschGehG, KRITIS-VO, IT-SiG 2.0, VerSanG
- Verpflichtung: aktueller „Stand der Technik"
- persönliche Haftungsrisiken

Finanzielle Risiken
- Bußgelder seitens Gesetzgebung (additiv)
- mittelgroßes KH bis zu siebenstellige Beträge

interdisziplinäre Beratung

personelle Ressourcen

finanzielle Ressourcen

Verantwortlichkeiten

Potentielle Schäden (Diebstahl/Raub)
- Beatmungsgeräte
- Op-Saal
- Dialysegerät
- Endoskop
- Defibrilator
- ....

\+

- Folgekosten
- Wiederbeschaffung
- Wiederherstellung

X Mio €

Bei Verstoß gegen
- DSGVO = 4 %
- GeschGehG = 4 %
- KRITIS-VO / IT-SiG 2.0 = 4 %
- VerSanG = 10 %

22%
vom weltweiten Jahresumsatz

WISAG

Beispielrisiken

Risiko Kernprozesse (Betrieb)

- Materialverluste
- Prozesskosten

„Selbstbedienungsladen“ Krankenhaus
Beispiele aus einer Risikoanalyse

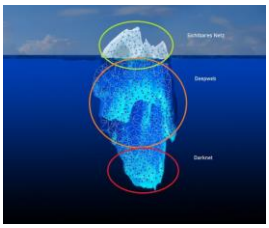
Materialverluste				Prozesskosten			
Schutzziel	Wert je Gerät	mögliche Anzahl	Summe Material-verlust	Wieder-beschaffungs-zeit	Umsatz je Tag & Gerät	Summe Umsatz-verlust	Gesamt-summe
Endoskope groß	25 T€	50	1.250 T€	30 T	1 T€	1.500 T€	2.750 T€
Endoskope einfach	2,5 T€	50	125 T€				
Beatmungsgeräte	25 T€	10	250 T€	21 T	3 T€	630 T€	880 T€
Ultraschallgerät mit 3 Sonden	50 T€	5	250 T€				
Wagen mit Mikroskopie (Augen)	50 T€	2	100 T€	30 T	2 T€	120 T€	220 T€
…			…			…	…
Summe:			**2,4 Mio €**			**3 Mio €**	**5,4 Mio €**

Beispielrisiken

Risiko Erpressung

- zielgerichtete Ransomware-Attacken gegen
  - Krankenhäuser
  - medizinische Forschungsinstitute
  - Pharmaunternehmen
- Druckmittel:
  - bedrohte Menschenleben auf Intensivstationen
  - Straftatbestände (DSGVO, IT-SiG 2.0, GeschGehG, VerSanG)
- Lösegeld
  - Datenverschlüsselung (Ransomware)
  - Datenveröffentlichung (Data Exfiltration)

Beispielrisiken



Risiko Wissensabfluß und Verkauf von wichtigen Daten

- Wert eines Patientendatensatzes
  - 2.000 € (lt. c´t / R. Eikenberg)
  - 5.000 US$ (lt. ICIT (Institute for Critical Infrastructure Technology)
  - 40 US$ € (lt. Greenbone / 1 Mrd US$ für 24 Mio Datensätze / D. Schrader)
- Interesse an gestohlenen Patientendaten im Darknet steigt (2019 – Kaspersky)
- Forschung & Entwicklung (z.B. Studien / Impfstoffentwicklung)

Beispielrisiken

Risiko Geldwäsche

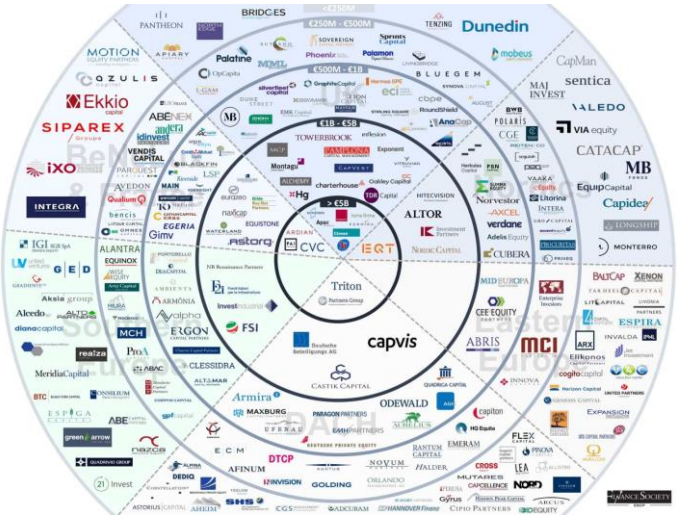
- möglicher Weg: Übernahme Krankenhäuser durch Private Equity
- hinter Private Equity stehen meist weitere Geldgeber, die öffentlich nicht in Erscheinung treten wollen
- diese Geldgeber haben häufig einen Sitz im gering kontrollierten Ausland
- aus anderen Branchen gibt es Beispiele, wie gezielt herbeigeführte Security-Incidents den Kaufpreis beeinflusst haben (inkl. provozierter Insolvenz)

Beispielrisiken

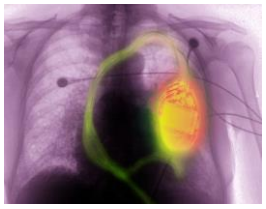
Beispiele Übernahme Krankenhäuser durch Private Equity

- Klinikgruppe Ameos (2011 / CH) durch Carlyle (USA), Quadriga und Paeger
- Oberberg-Gruppe (2017 / D) durch Trilantic Capital Partners (USA)
- DRK-KH-Gruppe Thüringen-Brandenburg (2019 / D) durch KMG (D)
- Einbeck Bürgerspital (2019 / D) durch Summit Partners (USA)
- Sana Kliniken (2019 / D) durch AMEOS (CH)
- KH Warstein (2019 / D) durch Altor Equity Partners (S)
- KH Rhön-Klinikum (2020 / D) durch Asklepios / Braun
- DRK-Kliniken Nordhessen (2021) durch Helios (D)

Private Equity Landschaft



Beispielrisiken



Risiko zielgerichtete Angriffe auf Einzelpersonen

- politisch exponierte Personen (PEP) als Patienten
- Manipulation von Patientendaten
- Cyberangriffe gegen medizinische Implantate
  - Insulinpumpen
  - Herzschrittmacher

Beispielrisiken

Risiko Betrug

- mit erbeuteten medizinischen Informationen ist es einfacher, Betroffene und Angehörigen zu betrügen
- Abrechnung von Rezepten zwischen Krankenhausapotheke und Krankenkassen (Beispiel AvP)

Gegenmaßnahmen

ZIELE

Sicherstellung der Funktionsfähigkeit des Krankenhauses 24/7

Schutz von Patienten und Personal

Risikomanagement „KRITIS“

Security-Konzept
- Abdeckung vielschichtiger Bedarfsfelder-

SECURITY ALS **TEAMWORK**

DIGITALE SOUVERÄNITÄT

keine Reputationsschäden oder finanzielle Verluste

Qualitätssteigerung
- Versorgung, Sicherheit, Digitalisierung -

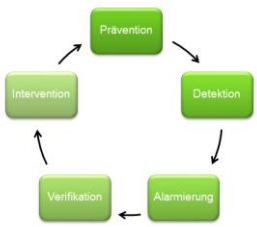
Gegenmaßnahmen

Gegenmaßnahmen (Übersicht)

- Annahme der Risiken (Geschäftsführung & Gesellschafter)
- „security-chain“ vollständig umsetzen („wirksam“)
- Schutzziele und schützenswerte Güter definieren
- Analyse der Lage (Gefährdungsanalyse)
- Sicherheitskonzept, physisch
- Sicherheitskonzept, SecIT
- SecurityProzesse (in Anlehnung an ITIL4)
- Readiness
- BSI-Grundschutz (200-x / B3S / basierend auf ISO 27001)
- Budget: Krankenhauszukunftsgesetz (KHZG)

mündliche Details gerne auch umfassender in einem Folgetermin dargestellt

Empfehlungen aus der Praxis



Technisch

- Offline Datensicherung
- Netzwerksegmentierung („Teile und Herrsche“)
- regelmäßige Updates
- „harte“ Isolierung von nicht updatefähigen IT-Geräten (z.B. Medizintechnik mit Zulassung, aber WinXP oder Win7)
- Zugriff von außen ausschließlich über VPN (auch für OT-Dienstleister)
- AntiSPAM-Gateway mit zentraler Malware-Erkennung
- NextGeneration-Firewall (Applikationsebene / Schicht 7)
- Mehrfaktor-Authentifizierung (MFA)

Empfehlungen aus der Praxis

Technisch

- sichere PWD – hashwerte gegenprüfen (haveibeenpwned.com)
- Paßwort-Tresor für alle User (auch privat kostenfrei ermöglichen / Seitenangriff verhindern)
- Mobile Device Management (MDM) für Smartphones, Tablets, Notebooks
- Notebook-Verschlüsselung mit 2FA

UND

- regelmäßiges Üben, Üben, Üben

Empfehlungen aus der Praxis

Menschlich / Organisation

- Sensibilisierung der Mitarbeiter schaffen
  - Awareness
  - Aufmerksamkeit schaffen
  - physical Security & IT-Security
- Security-Chain vollständig implementieren
  - Sicherheitskonzept
  - BSI-Schutzzonen
  - Securityprozesse
- Incident-Hotline
- Whistleblower-Hotline (Hinweisgebersystem wg. EU-Richtlinie 2019/1937)

Empfehlungen aus der Praxis

bei einem akuten Security-Incident

- Ruhe bewahren
- Digitale Erste Hilfe
- unverzüglich professionelle Hilfe einbinden (Notarzt = Beweismittelsicherung und Incident Response Team)
- Notfallmanagement aktivieren (Krisenstab / BSI 200-4)
- kein Lösegeld zahlen
  - Straftatbestand Finanzierung von OK
  - Positionswechsel vom Opfer zum Täter
  - Liquidität ermöglicht den Kauf weiterer zero-day-exploits (=Brandbeschleuniger)

WISAG

Empfehlungen aus der Praxis

Betrugsermittlung vs. Desaster Recovery

- zuerst Beweismittel gerichtsfest sichern („chain of custody“)
- dann erst Desaster Recovery (DR) beginnen
- denn DR zerstört Beweismitteln
- die Erkenntnisse über „wo, wer, warum, wie“ hilft dem „Incident Response Team“ beim Desaster Recovery
- fehlende / zerstörte Beweise können die Opfer zum Täter machen
- die möglichen Vorgehensweisen der Täter lassen sich mit Erfahrung, Spürsinn, Phantasie und vor allem wirtschaftlichem Verstand ermitteln
- bewährter Ansatz: "follow the Money" - also "folge dem Geld"
- er scheint simpel - aber er führt sehr häufig zum Erfolg

WISAG

Fazit

Risiko:

- Gefahr x Eintrittswahrscheinlichkeit = Risiko
- Risiken sind teilweise sogar finanziell bewertbar (BIA)
- Sicherheitsvorfälle kosten 10er Potenzen mehr als die Prävention

Hürde:

- „there is no glory for prevention“
- „Es gibt keine Orden für eine gute Vorbereitung“

Chance:

- die Prävention kostet 10er-Potenzen weniger als eine Vorfallbewältigung

WISAG

Diskussion

Diskussion

FACHVEREINIGUNG KRANKENHAUSTECHNIK E.V.

Weil Gesundheit die beste Technik braucht

WISAG

Kontaktdaten

Thomas Schuy
Senior Consultant
Sec-IT

Thomas Schuy
Senior Consultant Security-IT (BSc, BBA, CFE)

WISAG Sicherheit & Service Holding GmbH & Co. KG
Herriotstraße 3
60528 Frankfurt am Main
Mobil +49 162 41 22 628
thomas.schuy@wisag.de
www.wisag.de

Disclaimer

Vielen Dank für Ihre Aufmerksamkeit!

WISAG Sicherheit & Service Holding GmbH & Co. KG

Herriotstraße 3
60528 Frankfurt am Main
Mobil +49 162 41 22 628
thomas.schuy@wisag.de

www.wisag.de