Cyber-Angriffe auf Krankenhäuser und Arztpraxen – Schutz- und Reaktionsmöglichkeiten – aus Betroffenensicht

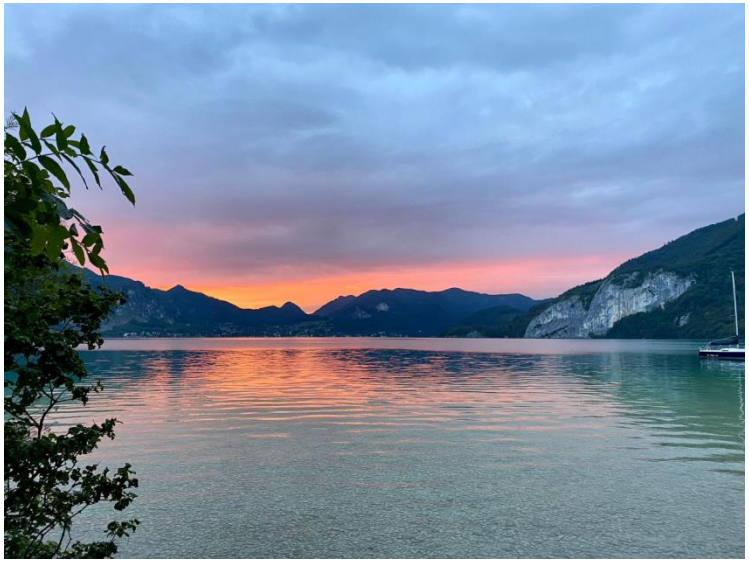
13. Düsseldorfer Medizinstrafrechtstag - 12.11.2022

Charlotte von der Heyde – Leiterin der Stabsstelle Recht und Compliance

I. Der Fall

Erste Anzeichen einer Störung am 10.09.2020

Bis zum 10.09: Alltagsbetrieb



Ab 10.09: Unruhe

SMS-Nachricht
Do. 10. Sept., 04:31

Guten Morgen,

wir haben im UKD seit ca 2:30 Uhr einen Ausfall weiter Teile der IT. Medico, Copra, PACS, Mail und SAP scheinen nicht zu funktionieren. Auch der Citrix-Desktop soll unvollständig sein. Dies wurde eben von der ZNA an den Notfallkoordinator gemeldet [redacted]. Herr Dr. [redacted] hat das Haus von der Notfallversorgung abgemeldet.

BG

[redacted]

SMS-Nachricht

Der Sturm bricht los!

SMS-Nachricht

Do. 10. Sept., 04:31

Guten Morgen,

wir haben im UKD seit ca 2:30 Uhr einen Ausfall weiter Teile der IT. Medico, Copra, PACS, Mail und SAP scheinen nicht zu funktionieren. Auch der Citrix-Desktop soll unvollständig sein. Dies wurde eben von der ZNA an den Notfallkoordinator gemeldet [redacted]. Herr Dr. [redacted] hat das Haus von der Notfallversorgung abgemeldet.

BG

[redacted]

Do. 10. Sept., 08:44

Wir wurden verschlüsselt.
Alles ist down.

SMS-Nachricht

Status bis 12:00 Uhr

Ausfall von:

- Alle Windows-basierten IT-Anwendungen (ca. 650 Server)
- Alle klinischen IT-Systeme (Patientendaten!)
- IT-Systeme der Verwaltung (SAP)
- E-Mail
- Logistik
- Gebäudeleittechnik
- Internetzugang

Akute Gefährdung der Patienten!

Konsequenzen:

- Abmeldung von der Notfallversorgung
- Elektive Patientenaufnahmen eingestellt
- Verlegung von Patienten in umliegende Häuser
- Ambulante Patienten werden abbestellt
- Der OP-Bereich behandelt ausschließlich Notfälle
- Zytostatika-Herstellung nur eingeschränkt möglich
- Sterilgutversorgung zu 50% eingeschränkt
- Anforderungen ausschließlich per FAX oder Telefon
- Kommunikation der Lage an alle Beschäftigten über täglich verteilte Flugblätter und FAX

Schnelle Unterstützung durch externe Organisationen

Information an **Behörden**
(BSI / Polizei / LKA)

Zusammenarbeit mit Polizei und dem LKA:

- Um welche Verschlüsselung handelt es sich?
- Wie viele Systeme sind betroffen?
- Wer ist der Angreifer + wurde ein Kontakt hinterlegt?

Kontaktaufnahme und Rückzug der Angreifer

- Identifikation eines **digitales Erpresserschreibens** – adressiert an die Heinrich-Heine-Universität
- Die Kontaktaufnahme zu den Angreifern erfolgte über das **LKA-Verhandlungsteam**.
- Es wurde ein Versuch gestartet darauf hinzuweisen, dass die Angreifer eine Universitätsklinik verschlüsselt haben und **Menschenleben gefährdet** seien.
- Vermutlich gaben daraufhin die Angreifer den **Entschlüsselungscode** heraus.

Nächste Schritte

ZNA nach 13 Tagen wieder **im Normalbetrieb**

Neues Übergangs-Rechenzentrum per Container-Modul (Storage und Server)

Client Check‘n Clean z.B. Corona-Notfall-PCs und Laptops für das externe Arbeiten prüfen u

Ausgabe von 11.500 neuer Passwörter
(05.10.2020 – 09.10.2020)

II. Rechtliches

Der Angriff als solcher

- Straftatbestände zum Schutze von Daten: Ausspähen und Abfangen von Daten einschließlich der Vorbereitungshandlungen (§§ 202 a–202 d StGB)
- Datenintegrität, Datenveränderung, Computersabotage (§§ 303 a, 303 b StGB)
- Vermögenserhebliche Datenvorgänge, Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, Computerbetrug (§§ 263 a, 269, 270 StGB)
- Schutz des bargeldlosen Zahlungsverkehrs (§§ 152 a, 152 b StGB)
- Schutz von Betriebs- und Geschäftsgeheimnissen (§ 23 GeschGehG)
- Schutz des geistigen Eigentums, Softwarepiraterie (§ 106 UrhG)
- Erpressung (§ 253 StGB)

Risikomanagement und „Response“

- Der Umgang mit Ransomwareangriffen und etwaige Sorgfaltspflichten zur Verhütung derartiger Angriffe werden im juristischen Schrifttum zunehmend diskutiert.

- Im Schrifttum wird unterschieden zwischen:

  - „Response“ (Vorgehen bei einem Cyberangriff)

  - „Prepardness“ (Verhütung eines Cyberangriffs)

Response

Response: Sorgfaltspflichten beim Umgang mit dem Angriff

- Vorgehen bei einem Angriff (*Habbe/Gergen* CCZ 2020, 281, 284 f):
  - Analyse des Angriffs
  - Risikobeseitigung
  - Beweissicherung
  - Wiederherstellung des Betriebsablaufs
- Entscheidungen zur „Response“ unterliegen dem unternehmerischen Ermessen (*Kiefner/Happ* BB 2020, 2051, 2056)

Response: Besondere Handlungspflichten?

- Gibt es eine Pflicht zur Zahlung des „Lösegelds“ bzw. ein Verbot der Zahlung?
- Datenschutzrechtliche Aspekte?
- Kapitalmarktrechtliche Pflichten (adhoc-Publizität)?
- Pflicht zum Einschalten von Strafverfolgungsbehörden?
- Meldepflicht nach BSI-Gesetz?

Datenschutzrechtliche Meldepflicht

- Art. 33 DSGVO: Meldung von Hackingangriffen an die Aufsichtsbehörden, insbesondere wenn ein Risiko für die Betroffenen besteht. Eine Meldung muss dabei innerhalb von 72 Stunden erfolgen.

  „Ein typisches Beispiel für eine möglicherweise meldepflichtige Datenschutzverletzung ist etwa die Verschlüsselung von Datenbanken durch Hacker im Rahmen einer Ransomware-Attacke“ (Wybitul NJW 2020, 2577, 2578).

Meldepflicht nach BSI-Gesetz

- § 8b Abs. 4 BSIG:

  „Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

  1. *Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,*

  2. *erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.“*

„Prepardness“

Pflicht zur „Prepardness“

- Verantwortung für digitale Infrastruktur ist Ausfluss aus § 76 Abs. 1 AktG (Habbe/Gergen CCZ 2020, 281, 282; Schmidt-Versteyl, NJW 2019, 1637, 1640).
- Dabei soll ein Leitungsermessen bestehen.
- Weniger „Compliance-Maßnahme“ (so aber *Habbe/Gergen* CCZ 2020, 281, 282) als eher Bestandteil des Risikomanagements (zutreffend: *Kiefner/Happ* BB 2020, 2051).
- Besondere Pflicht zur „Prepardness“: § 8a Abs. 1 BSI-Gesetz

„… angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.“

Ausprägung der „Sicherungspflicht“

- Grds. Gesamtverantwortung des Vorstands
- Horizontale und vertikale Delegation (Habbe/Gergen CCZ 2020, 281, 282: IT als „Spezialkenntnis“).
- Maßnahmen (u.A.):
  - Risikoanalyse
  - Aufstellen eines Cyber Incident Response Plan
  - Laufende Überwachung
  - Dokumentation
  - Befolgen des BSI-Grundschutz

Implikationen nach einem Cyberangriff: unzureichende Prepardness?

„Nach einer Datenpanne stellt sich naturgemäß die Frage, ob eine unzureichende Datensicherheit diesen Vorfall verursacht oder begünstigt hat.“ (*Wybitul* NJW 2020, 2577)

- Cyber-Versicherung: Mitverschulden (§ 254 BGB)?
- Datenschutzrecht: Bußgelder wegen unzureichender Datensicherheit *(*Wybitul NJW 2020, 2577, 2580)
- Organhaftung wegen unzureichender Prepardeness/unzureichender Response (*Kiefner/Happ* BB 2020, 2051, 2057)?
- Strafrechtliche Verantwortung?

III. Lessons Learned

Lessons Learned

Positiv

- Cyber-Versicherung abgeschlossen (Unterlagen der Versicherung nicht nur digital abspeichern!)
- Versicherungsmakler mit Erfahrungswerten im Cyber-Schadensbereich
- Notfallmanagement der KEL implementiert und erprobt
- Sehr kurze Reaktionszeit auf das Ereignis
- schneller Wiederanlauf durch den Einsatz von Server-Virtualisierung
- Hochmotivierte Mitarbeiter in der IT
- komplexe Systemlandschaft beugte Komplettausfall vor (z.B. Einsatz eines Linux-basiertem Systems im Labor)

Verbesserungsbedürftig

- Kaum analoge Kommunikationswege vorhanden – Fax wird zum Großteil nur digital als Mail zugestellt
- Fachexpertise personell weiter verstärken (CISO)
- Beteiligung an einem Security Operations Centers zur Überwachung von Ereignissen
- Ausreichend Ressourcen für Notfälle vorhalten (z.B. Speicherplatz, PC‘s)
- Vorbereitung auf IT-Ausfälle z.B. Einführung eines „Paper-Day“
- Eine verantwortliche Person benennen, um im Schadensfall die Dokumentation zu führen