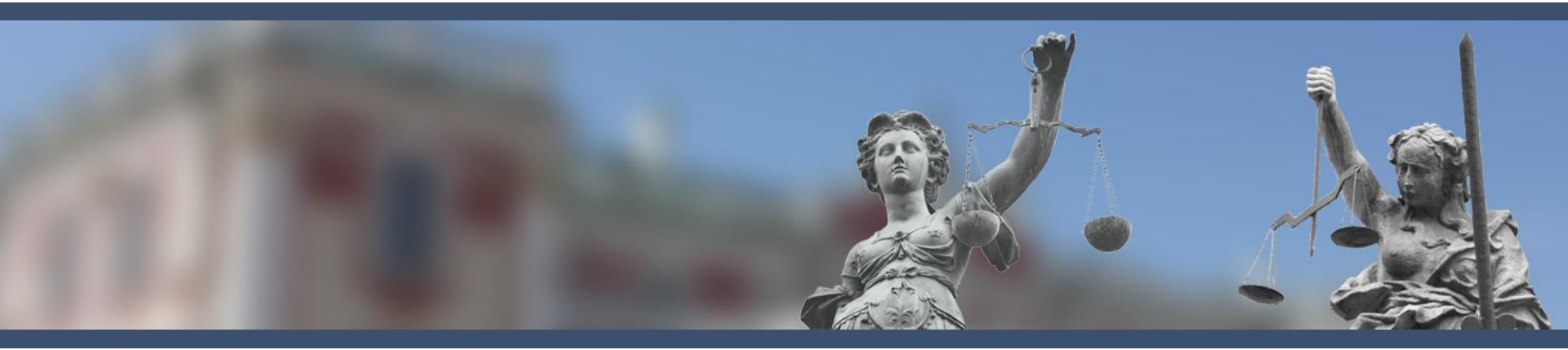


Cyber-Angriffe auf Krankenhäuser und Arztpraxen – Schutz- und Reaktionsmöglichkeiten (aus Strafverfolgungssicht)

13. Düsseldorfer Medizinstrafrechtstag,12.11.2022

Staatsanwalt Christoph Apostel – ZAC NRW

Kurze Vorstellung: ZAC NRW

Schäden durch Cyberangriffe für die deutsche Wirtschaft

- Über 220 Milliarden Euro pro Jahr (im Vergleich zum Zeitraum 2018/2019 mehr als doppelt zu hoch)
- 9 von 10 Unternehmen von Cyberangriffen betroffen
- Für 25 % der deutschen Unternehmen, v.a. Kleinunternehmen, nahezu existenzbedrohende Schäden
- Erpressungsvorfälle im Vergleich zu 2018/2019 mehr als vervierfacht (+ 358 %)

Quelle: Bitkom Research 2021 (bsi.de, bitkom.org)

Kritische Infrastrukturen

Auch Krankenhäuser und sonstige Gesundheitseinrichtungen können Ziele von Angriffen sein, insbesondere von…

- Ransomware (Erpressung)
- „Cybercrime-as-a-Service“
- DDoS (Distributed-Denial-of-Service) - Angriffe
- APT-Angriffe („Advanced-Persistent-Threat“) zum Zwecke der Spionage oder Sabotage

Tätertypologie

- Einzeltäter: Fast vollständig ausgestorben
- Szenetäter: Cybercrime-Szene umfasst einen „harten Kern“ und eine große Gruppe von „Mitläufern“ und Gelegenheitstätern (auch ohne IT-Kenntnisse)
- OK-Gruppierungen
- (Dritt-)Staatlich induzierte Kriminalität

Hauptphänomen: Ransomware

- Ransomware (von englisch *ransom* für „Lösegeld“ und *ware* für Computerprogramme): Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

- Mittlerweile standardmäßig: Neben Verschlüsselung auch Ausspähen/Abgreifen von Daten und Drohung mit der Veröffentlichung der Daten auf einer Leaking-Webseite im Darknet („Double Extortion“), ggf. zusätzlich gezielte Weitergabe der Daten an Konkurrenz („Triple Extortion“) usw.

- Grds. erfüllte Straftatbestände: Erpressung (§ 253 StGB), Ausspähen von Daten (§ 202a StGB), Datenveränderung (§ 303a StGB), Computersabotage (§ 303b StGB)

Verfahren z.N. Universitätsklinikum Düsseldorf

Quelle: https://rp-online.de/nrw/staedte/duesseldorf/uniklinik-duesseldorf-hackerangriff-begann-schon-vor-monaten-spur-fuehrt-wohl-nach-russland_aid-53495689

Verfahren z.N. Universitätsklinikum Düsseldorf

- In der Nacht zum 10.09.2020: Feststellung, dass mehrere Server des Klinikums verschlüsselt wurden.
- Folgen u.a.: Keine Aufnahme von Notfallpatienten mehr → Eine herzkranke Patientin musste an ein weiter entferntes Krankenhaus in Wuppertal verbracht werden und starb kurze Zeit später. Ermittlungen daher auch wegen fahrlässiger Tötung (Kausalität konnte jedoch nicht festgestellt werden).
- Im Bereich der veränderten IT-Systeme: Textdatei mit Erpresserschreiben, gerichtet an die Heinrich-Heine-Universität Düsseldorf (HHU).
- Dort Aufforderung der unbekannten Täter zur Kontaktaufnahme und Drohung, dass für den Fall der Weigerung eine Veröffentlichung von zuvor exfiltrierten Daten im Darknet erfolge. Eine konkreter Geldbetrag wurde (noch) nicht genannt.
- Täter übermittelten später zwar den Wiederherstellungsschlüssel, nachdem sie darauf hingewiesen wurden, dass ein Krankenhaus (UKD) – statt des wohl eigentlichen Ziels (HHU) – betroffen ist, die vollständige Wiederherstellung der Daten sowie des regulären Krankenhausbetriebs dauerte dennoch mehrere Wochen.

Verfahren z.N. Universitätsklinikum Düsseldorf

- Infiltration des Serversystems mittels Sicherheitslücke in „Citrix NetScaler Gateway“ → marktübliche und weltweit verbreitete kommerzielle Software zur Fernsteuerung.
- Mittels „Loader“ (Malware zum Nachladen der eigentlichen Schadsoftware) konnte Verschlüsselungstrojaner „DoppelPaymer“ eingebracht werden.
- „DoppelPaymer“ wurde bereits in zahlreichen weiteren Fällen weltweit zum Nachteil von Unternehmen und Institutionen eingesetzt (überwiegend USA). Aufgrund mehrerer Fälle auch z.N. deutscher Unternehmen wurde bei der ZAC NRW ein Strukturverfahren (bundesweit zentrale Ermittlungen) eingeleitet.
- Anschließend „Rebranding“ der Täter in „PayOrGrief“, aber wohl selbe Tätergruppierung.
- Tätergruppierung nach Einschätzung privater IT-Sicherheitsunternehmen und nach dem Ergebnis der bisherigen Ermittlungen aus dem russischsprachigen Raum.

Verfahren z.N. Universitätsklinikum Düsseldorf

Ermittlungsschritte (im allgemeinen und hier im speziellen):

- Auswertung/Analyse der Schadsoftware
- Ermittlungen zur Kontakt-E-Mailadresse
- Ermittlungen zur Leaking-Webseite
- Überwachung der Leaking-Webseite
- Sich daran anschließende Ermittlungen zu jeder IP etc., die erlangt wurde
- Alles im Ausland → bislang über 60 Rechtshilfeersuchen, Ende offen
- Gut ist: Katalogtat (Erpressung), durch öffentlichen und politischen Druck personelle Ressourcen, internationale Zusammenarbeit mit einem stark in die IT-Infrastruktur eingebundenen EU-Land („Europäische Ermittlungsanordnung“) funktioniert reibungslos.
- Schlecht ist: Identifizierung der Täter schwierig, führt in nahezu allen Fällen in ein Land, mit dem Rechtshilfe kaum oder gar nicht möglich ist. Zudem: „Ransomware-as-a-service“ („RaaS“) auf dem Weg zum Massenphänomen.

Verfahren z.N. Universitätsklinikum Düsseldorf

Besonderheit: Tod einer Patientin im (zeitlichen) Zusammenhang mit dem Ransomware-Angriff

Folgeprobleme:

- Ermittlungen auf fahrlässige Tötung ausgeweitet
- Vorausgesetzt, die Täter hätten gewusst, dass sie ein Krankenhaus angreifen → Ermittlungen wegen Mordes (Mordmerkmal: Habgier)
- Hätten die Täter den Wiederherstellungsschlüssel nicht geliefert und wäre daraufhin ein/e Patient/in gestorben → Ermittlungen wegen (versuchten) Mordes durch Unterlassen

Verdeutlicht die Dimension von Cyberangriffen z.N. von Krankenhäusern/Gesundheitseinrichtungen!

Exkurs: Strafbarkeit der Geschädigten bei Zahlung?

- Keine Strafbarkeit nach § 253 StGB, da Opfer als „notwendiger Teilnehmer“ kein Mittäter oder Gehilfe bei einer Erpressung zum eigenen Nachteil sein kann (vgl. Fischer StGB, 69. Aufl. 2022, § 253 Rn. 48).

- Evtl. Strafbarkeit gem. § 129 Abs. 1 S. 2 StGB (Unterstützen einer kriminellen Vereinigung)?
  - Rechtsgut: Schutz der öffentlichen Sicherheit und der staatlichen Ordnung → d.h. kein individuelles, disponibles Rechtsgut
  - Objektiver Tatbestand: Unterstützen einer kriminellen Vereinigung durch Zahlung des Lösegeldes rechtsdogmatisch grds. erfüllt → Probleme liegen im tatsächlichen Nachweis einer „kriminellen Vereinigung“
  - Subjektiver Tatbestand: Bedingter Vorsatz im Hinblick auf die Verwirklichung der obj. Tatbestandsmerkmale genügt

Exkurs: Strafbarkeit der Geschädigten bei Zahlung?

- Rechtswidrigkeit und Schuld
  - Rechtfertigung gem. § 34 StGB oder Entschuldigung gem. § 35 StGB? → Umstritten

➢ Problem: Zur Anwendbarkeit des § 129 StGB bei Ransomware-Zahlungen keine Rechtsprechung vorhanden. Von der ZAC NRW bisher keine Ermittlungsverfahren gegen zahlende Geschädigte eingeleitet (auch bundesweit keine Ermittlungen bekannt).

➢ In der Literatur lediglich ein Aufsatz zur vorgenannten Problematik bekannt → *Cybercrime und Lösegeld - Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner* von Dr. Tim R. Salomon (vgl. MMR 2016, 575 – beck-online).

Ransomware und sonstige professionelle Cyberangriffe

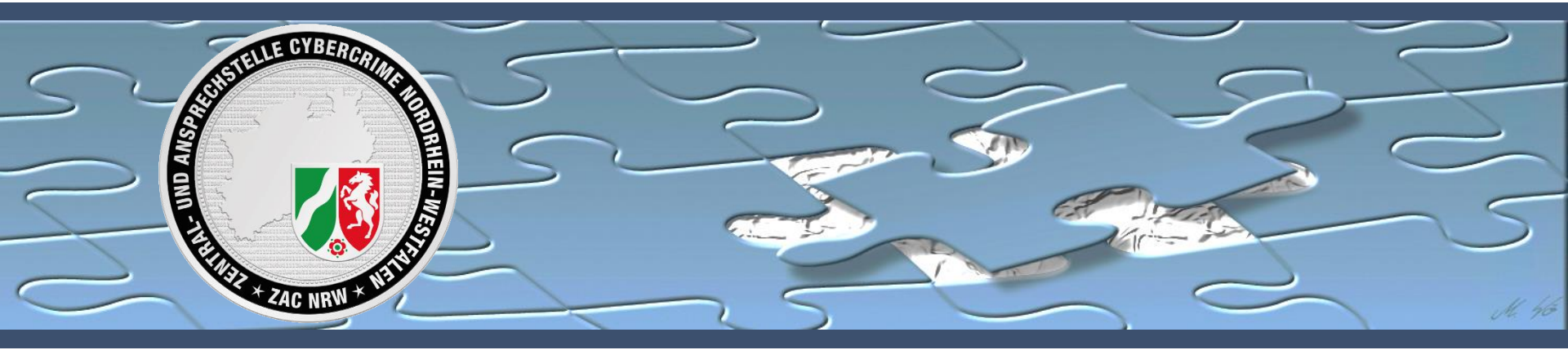
Herausforderungen:

- Schnelle Reaktion erforderlich, gerade auch bzgl. Anstoßen erster Ermittlungsschritte
- Technisch komplex, Sachverstand muss vorhanden sein, ggfs. vertrauensvolle Zusammenarbeit mit technischen Gutachtern
- Auch vertrauensvolle Zusammenarbeit mit den Geschädigten → ohne diese geht bei einer IT-Struktur wie der des UKD gar nichts
- Bereitschaft, auch dem kleinsten Fingerzeig nachzugehen und sich nicht entmutigen zu lassen
- Internationalität der Ermittlungen

Schutz von (potentiell) Betroffenen

IT-Sicherheit ernst nehmen:

- Regelmäßige Updates von Software
- Sicherheitslücken umgehend schließen
- Warnhinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) beachten und umsetzen
- Aktuelle Virenscanner und Firewalls
- Backups vorhalten
- Bei Betroffenheit: Ggf. private IT-Sicherheitsunternehmen (Incident Response Team) mit ins Boot holen und Strafanzeige erstatten → Spezialisten bei der Polizei (insb. LKA) führen nicht nur Ermittlungen durch, sondern geben auch Hilfestellung bei der Wiederherstellung der Daten und Risikominimierung (Remediation)



Christoph Apostel
Staatsanwalt
christoph.apostel@sta-koeln.nrw.de

Zentral- und Ansprechstelle Cybercrime
- ZAC NRW -
http://www.zac.nrw

ZAC NRW
24/7 – Erreichbarkeit über
Zentralrufnummer

+49 221 477 4922

Funktionspostfach
zac@sta-koeln.nrw.de