# Im Visier der Erpresser – Ransomware-Angriffe, ihre Folgen und Schutzstrategien

**Forum 19**

**Public-IT-Security 2024**

**Performance Management**

**Impulsvortrag, 13.06.2024**

Prof. Dr. René Treibert

Institutsleiter Clavis – Institut für Informationssicherheit der Hochschule Niederrhein

CYBER CAMPUS NRW

Hochschule Niederrhein
University of Applied Sciences

Cyber Management Campus MG

# Teilnehmer Forum 19 der PITS 2024

- Moderation: Prof. Dr. René Treibert
- Markus Wiegand
  Stellvertretender Leiter, Hessen Cyber Competence Center
- Thomas Biere
  Referatsleiter Informationssicherheitsberatung für den Bund und Grundsatz, Bundesamt für Sicherheit in der Informationstechnik
- Dr. Katja Papenkort
  Referatsleiterin Cyberfähigkeiten der Sicherheitsbehörden – Lagebezogene Aufgaben, Bundesministerium des Innern und für Heimat
- Michael Tullius
  Sales Director Germany, Exeon Analytics

# Studienangebote

**Bachelor Cyber Security Management**

- Vollzeit: 6 Semester / Teilzeit: 8 Semester
- Start im Wintersemester 2020/21

**Master Cyber Security Management**

- Vollzeit: 4 Semester / Teilzeit: 6 Semester
- Start im Sommersemester 2021

**Der Cyber Security-Experte . . .**

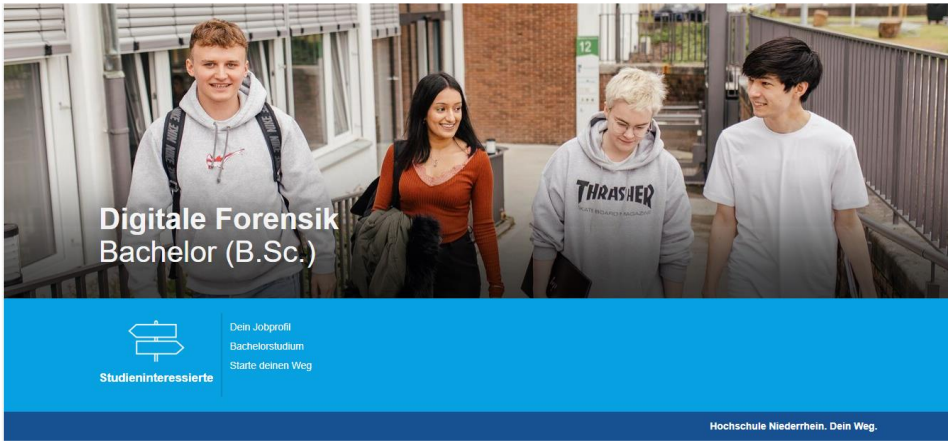
- sorgt für die IT-Sicherheit in allen Unternehmensprozessen und im eGovernment
- verteidigt sein Unternehmen und seine Organisation gegen IT-Risiken und Sicherheitsvorfälle
- trägt zur Sicherheit von öffentlichen Einrichtungen und kritischen Infrastrukturen bei
- administriert Sicherheitstechnologien in den IT-Systemen wie Clouds und Firewalls
- implementiert sichere Anwendungssysteme in Unternehmen und öffentlicher Verwaltung
- ist ein Berater, Trainer und Aufklärer für die Teams in seiner Organisation
- wirkt als Auditor, Berater/Consultant nach ISO/IEC 27001

# Neues Studienangebot seit WiSe 23/24

**Bachelor Digitale Forensik**

- Vollzeit: 6 Semester / Teilzeit: 8 Semester
- Start im Wintersemester 2023/24 mit ca. 100 Studienanfängern
- offener Studiengang (nicht nur für Polizeibeamte)
- in Kooperation mit der HS Bonn-Rhein-Sieg

*ca. 50 Polizeibeamte pro Jahr*




# Ransomware – Eine Defintion

**‚ransom', ist der englische Begriff für Lösegeld,**
**‚ware', ist die Abkürzung für Malware (dt.: Schadsoftware).**

"Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (Ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung."

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6

# Ransomware – Phasen

1. **Aufklärung**: Beobachten und Ausspionieren des Ziel-Systems

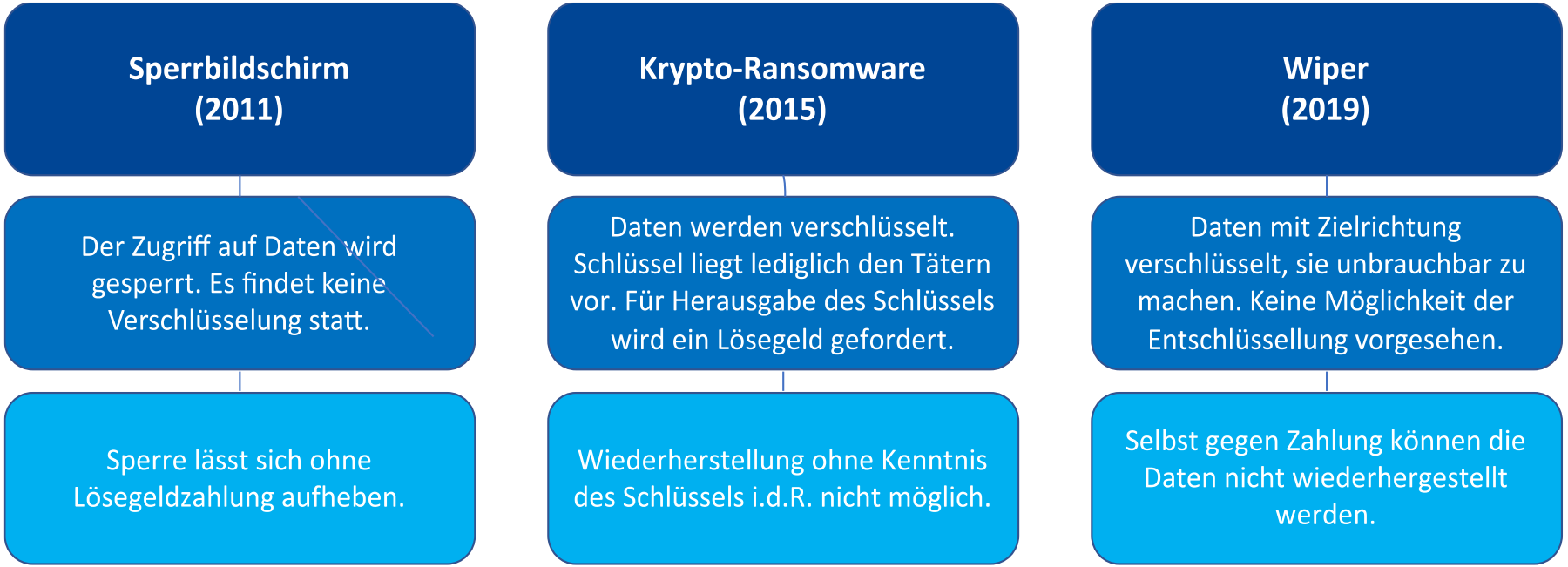
2. **Eindringen**: Zugriff der Angreifer in die Systeme ihrer Opfer. Dies kann über verschiedene Wege wie zum Beispiel Phishing, E-Mails, Drive-by- Downloads, infizierte Speichermedien etc. erfolgen.

3. **Laterale Bewegung**: Ist der Angreifer im Netz seines Opfers, wird das System erkundet. Es werden sämtliche Daten und Informationen gesammelt, die es dem Angreifer ermöglichen und erleichtern sich im System auszubreiten.

4. **Verschlüsselung**

5. **Erpressung**

# Varianten von Ransomware




Darstellung, basierend auf Quelle:
https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=5

# Wirtschaftliche und betriebliche Auswirkungen nach Ransomware-Angriffen

Aussagen aus der Studie **Sophos - The State of Ransomware 2022**

## Grundlage der Befragungen

- 5600 IT-Profis in 31 Ländern wurden befragt
- 400 davon in Deutschland
- 100 bis 5000 Mitarbeiter je Organisation
- Zeitpunkt der Erhebung: Januar bis Februar 2022

Quelle: https://www.sophos.com/de-de/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

# Wirtschaftliche und betriebliche Auswirkungen nach Ransomware-Angriffen

**Kernaussagen der Sophos Studie The State of Ransomware 2022**

- 67% der befragten Unternehmen in Deutschland sind betroffen
- Bei 61% der betroffenen Unternehmen kam es auch zu einer Verschlüsselung
- Ransom Payment beträgt hier durchschnittlich: 273.453 USD
- Kosten für Behebungen:
  - 2020: 1.170.000 USD
  - 2021: 1.730.000 USD
- Ist eine Cyber-Versicherung der in Deutschland betroffenen Unternehmen vorhanden
  - 41%: Ja
  - 40%: Ja, aber mit Einschränkungen bei der Haftung

# Wirtschaftliche und betriebliche Auswirkungen nach Ransomware-Angriffen

**Kernaussagen der Sophos Studie The State of Ransomware 2022**

- Angriffe, Komplexität und Auswirkungen nehmen zu
- Unternehmen werden besser bei der Wiederherstellung
- Unternehmen sind häufig nicht in der Lage, Budgets und Ressourcen effektiv zu nutzen, um Ransomware zu stoppen
- Ransomware hat erhebliche wirtschaftliche und betriebliche Auswirkungen
- Ransomware treibt Cyber-Versicherungsschutz voran

# Wirtschaftliche und betriebliche Auswirkungen nach Ransomware-Angriffen

**Kernaussagen der Sophos Studie The State of Ransomware 2022**

- 90% der Ransomware-Angriffe beeinträchtigten die Betriebsfähigkeit
- 86% der Ransomware-Angriff verursachten Geschäfts-oder Einnahmeverluste
- 72% vertrauen auf Ansätze, die einen Angriff nicht verhindern können
- 1 Monat benötigen die Unternehmen durchschnittlich bis zur Wiederherstellung nach einem Angriff
- Wie schon oben (Seite 7 gesagt)
- 1.73 Millionen USD betrugen die durchschnittlichen Kosten für die Behebung der Folgen eines Angriffs in Deutschland (Vorjahr: 1.17 Millionen USD)
- Ransom Payment eines Angriffs in Deutschland beträgt durchschnittlich: 273.453 USD

# Wirtschaftliche und betriebliche Auswirkungen nach Ransomware-Angriffen

**Weitere Zahlen zu Ransomware aus der Sophos Studie The State of Ransomware 2022**

- 99% der Betroffenen konnten einige Ihrer Daten wiederherstellen
  - Ransom Payment
  - Backups
  - Sonstige Maßnahmen
- 46% haben eine Ransom Payment geleistet
- 61% der Betroffenen konnten die verschlüsselten Daten nach der Zahlung wiederherstellen
- Die Anzahl der Ransom Payments über 1 Millionen USD hat sich verdreifacht
- 21% der Betroffenen zahlten ein Ransom Payment unter 10k USD

# Wer sind die Angreifer mittels Ransomware

- **Kriminelle Organisationen**
  - Professionell organisiert.
  - Haben Geschäftsmodelle wie andere Unternehmen mit folgenden Unterschieden:
    - Agieren anonym.
    - Lassen sich in Kryptowährung bezahlen.
- **Ausländische Geheimdienste**

# Diskussion mit Experten und Publikum

- Grundsätzlich zu Ransomware
- Präventive Maßnahmen
- Reaktive Maßnahmen

Wir freuen uns auf die Diskussion mit Ihnen!

Hochschule Niederrhein. Dein Weg.