Ransomware

Anatomie, Netzwerkerkennung und Zero-Loss Recovery

Ihr Name

Ihre Institution

2. Januar 2026

Agenda

Entwicklung & Geschichte

Aktuelle Bedrohungslage

Ziele & Motivation

Arten von Ransomware

Die Phasen eines Angriffs

Gegenmaßnahmen

Forschung & Ausblick

Fazit

Entwicklung & Geschichte

Historischer Abriss

Meilensteine:

- 1989: AIDS Trojan - erster dokumentierter Ransomware-Angriff
- 2005: Wiederaufleben durch Internet und Kryptowährungen
- 2017: WannaCry-Ausbruch mit globaler Aufmerksamkeit

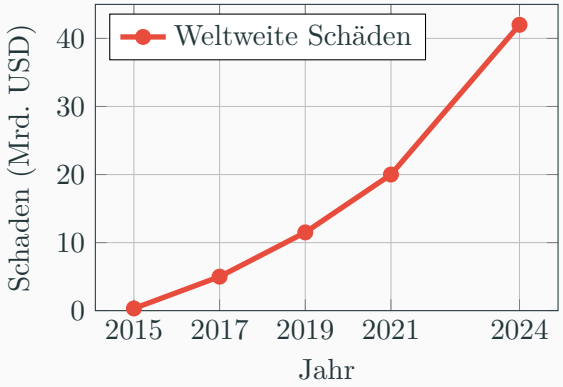
Abbildung 1: Entwicklung von Ransomware über die Jahre

Aktuelle Bedrohungslage

Finanzielle Auswirkungen

Geschätzte Weltweite Schäden

- 2017: 5 Mrd. USD
- 2024: 42 Mrd. USD

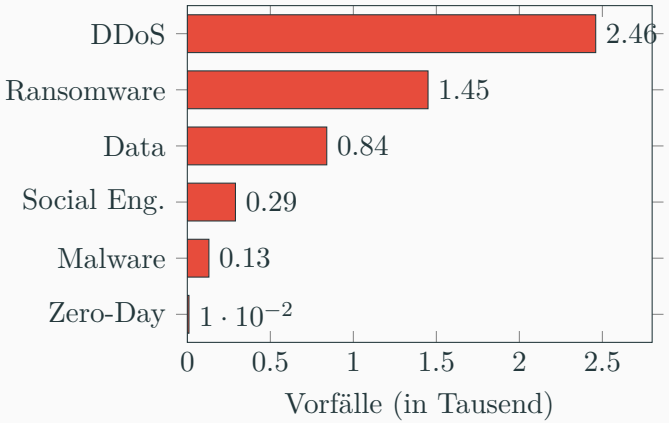


ENISA Threat Landscape 2024

Top-Bedrohungen EU (Prime Threats):

1. DDoS/RDoS (46,31%)
2. Ransomware (27,33%)
3. Data Breaches (15,87%)
4. Social Engineering (5,37%)
5. Malware (2,45%)
6. Zero-Day (0,11%)

Ransomware: Zweitgrößte Bedrohung



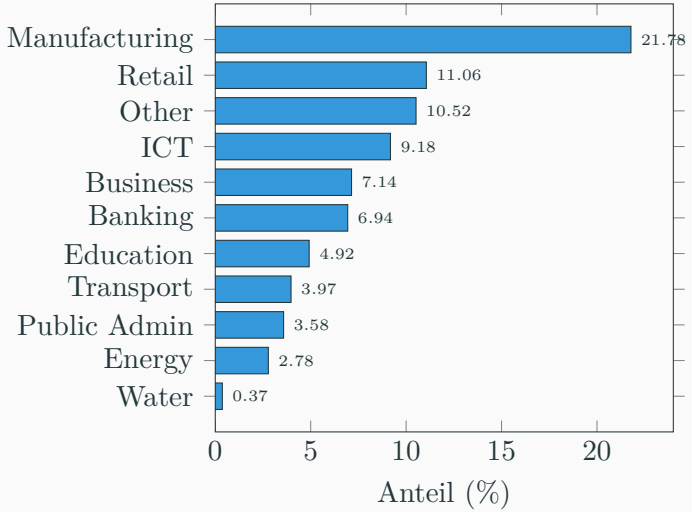
Ziele & Motivation

Am häufigsten betroffene Sektoren

Top 5 Sektoren:

1. Manufacturing (21,78%)
2. Retail (11,06%)
3. ICT Services (9,18%)
4. Business Services (7,14%)
5. Banking/Finance (6,94%)

Industrie und Fertigung am stärksten betroffen



Motivation der Angreifer

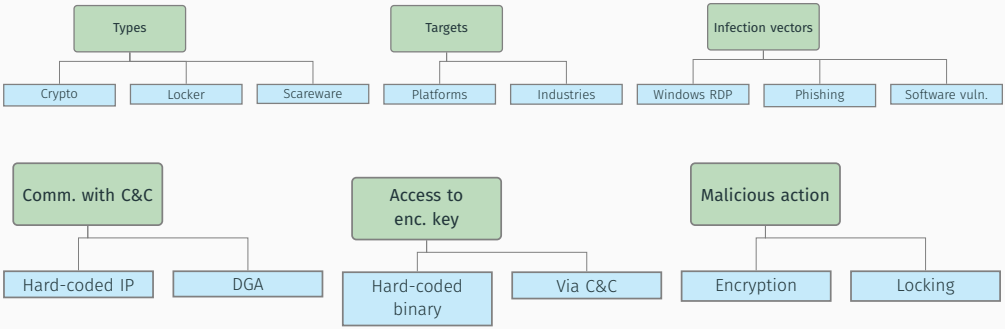
Warum diese Ziele?

- Finanzielle Motive: Zahlungsbereitschaft bei kritischen Systemen
- Kritische Infrastrukturen: Hoher Druck durch Ausfallkosten
- Sensible Daten: Erpressungspotenzial durch Datenleaks
- Geopolitische Faktoren: Destabilisierung und Spionage

Zunehmende Professionalisierung und Organisation

Arten von Ransomware

Ransomware Taxonomy



Grundlegende Typen

1. Crypto-Ransomware
   - Verschlüsselt Benutzerdateien
   - Verwendet AES, RSA
   - System bleibt funktional
   - Wiederherstellung oft unmöglich

2. Locker-Ransomware
   - Sperrt Systemzugriff
   - Bildschirmsperre
   - Keine Datenverschlüsselung
   - Einfacher zu beheben

Moderne Erpressungsformen

Evolution der Angriffsmethoden:

- Leakware/Doxware: Drohung mit Veröffentlichung sensibler Daten
- Double Extortion:
  - Verschlüsselung und Datenexfiltration
  - Doppelter Zahlungsdruck
- Triple Extortion:
  - Zusätzliche Drohung gegen Kunden/Partner
  - DDoS-Angriffe als dritte Ebene
- Ransomware-as-a-Service (RaaS):
  - Mietmodell für Cyberkriminelle
  - Keine technischen Kenntnisse erforderlich
  - Demokratisierung der Cyberkriminalität

Wichtige RaaS-Varianten

LockBit : Globale Dominanz, schnelle Verschlüsselung, hochprofessionell

Maze : Pionier der Double-Extortion-Methode

Ryuk : Gezielter gegen Großunternehmen

Die Phasen eines Angriffs

Ransomware Kill Chain: Überblick

Abbildung 2: Die vier Phasen eines Ransomware-Angriffs

Phase 1-2: Distribution & Infection

Distribution - Angriffsvektoren:

- Phishing-E-Mails (häufigster Vektor)
  - Bösartige Anhänge
  - Manipulierte Links
- Remote Desktop Protocol (RDP)
  - Brute-Force-Angriffe
  - Gestohlene Credentials
- Software-Schwachstellen
  - Ungepatchte Systeme
  - Zero-Day-Exploits

Infection:

- Installation der Malware
- Ausführung des Schadcodes
- Umgehung von Sicherheitsmechanismen
- Moderne Techniken:
  - Rootkit-Technologien
  - Verzögerte Ausführung

Phase 3-4: Staging & Scanning

Staging - Etablierung im System:

- Persistenzmechanismen (Registry, Autostart)
- Aufbau der Command & Control (C2) Kommunikation
- Lateral Movement im Netzwerk
- Rechteerweiterung (Privilege Escalation)

Scanning - Zielerkennung:

- Durchsuchen lokaler Laufwerke
- Identifikation von Netzwerkfreigaben
- Cloud-Speicher-Erkennung
- Priorisierung wertvoller Daten

Phase 5-6: Encryption & Payment

Encryption:

- Starke Verschlüsselung (AES, RSA)
- Hybride Verschlüsselungsverfahren
- Schnelle Verarbeitung
- Löschung von Backups/Schattenkopien

Payment:

- Anzeige der Lösegeldforderung
- Zahlungsanweisungen (Kryptowährung)
- Zeitlimit mit Preiserhöhung
- Drohung mit Datenlöschung/-veröffentlichung

Moderne Entwicklungen in Angriffstechniken

KI-gestützte Angriffe:

- KI-generierte Phishing-Kampagnen
- Umgehung von ML-basierten Detektionssystemen
- Automatisierte Zielerkennung und -priorisierung

Weitere Trends:

- Rootkit-Fashion: Tiefere Systemintegration
- Wiper-Ransomware: Zerstörung statt Verschlüsselung
- Supply-Chain-Angriffe über vertrauenswürdige Software

Abbildung 3: Evolution der Angriffstechniken

Gegenmaßnahmen

Prävention

Technische Maßnahmen:

- Backups: 3-2-1-Regel (3 Kopien, 2 Medien, 1 Offsite)
- Patch-Management: Regelmäßige Updates und Schwachstellenbeseitigung
- Netzwerksegmentierung: Begrenzung der lateralen Bewegung
- Access Control: Least Privilege Prinzip, MFA

Organisatorische Maßnahmen:

- Security Awareness Training
- Incident Response Pläne
- Regelmäßige Sicherheitsaudits

Detektion und Reaktion

Detektionsansätze:

- Statische Analyse: Untersuchung ohne Ausführung
- Dynamische Analyse: Verhaltensbeobachtung in Sandbox
- Machine Learning: Erkennung unbekannter Varianten
- Netzwerkbasierte Detektion: Anomalie-Erkennung im Traffic

Wichtige Merkmale:

- API-Aufrufe und Systemverhalten
- Datei-/Verzeichnisaktivitäten
- Netzwerkverkehrsmuster
- Verschlüsselungsoperationen

Incident Response

Sofortmaßnahmen bei Verdacht:

1. Isolation betroffener Systeme
2. Identifikation des Ransomware-Stamms
3. Bewertung der Schadenausbreitung
4. Benachrichtigung relevanter Stellen

Wiederherstellung:

- Wiederherstellung aus Backups (wenn möglich)
- Key-Escrow-Mechanismen
- Forensische Analyse
- Systemhärtung vor Wiederinbetriebnahme

Zahlungsempfehlung: Keine Lösegeldzahlung (keine Garantie, finanziert weitere Angriffe)

Forschung & Ausblick

Aktuelle Forschungslandschaft

Fokusgebiete:

- 72,8% der Studien: Ransomware-Detektion
- Machine Learning dominiert als Detektionsmethode
- Hohe Genauigkeit bei unbekannten Varianten

Innovative Ansätze:

- REDFISH: Netzwerkbasierte Früherkennung
  - Monitoring von SMB-Protokoll
  - Erkennung von Verhaltensmustern (schnelles Lesen/Schreiben/Löschen)
  - 99% Erkennung vor Verlust von 10 Dateien
- Near-Zero-Loss-Szenario durch Traffic-Wiederherstellung
- Moving Target Defense (MTD)

Zero-Loss Recovery: REDFISH

Funktionsweise:

- Analyse des Netzwerk-Traffics zu Freigaben
- Erkennung anomaler Zugriffsmuster
- Aufzeichnung der Dateiinhalte
- Automatische Alarmierung

Abbildung 4: REDFISH Architektur

Vorteile:

- Früherkennung (99% bei <10 Dateien)
- Wiederherstellung ohne Backups
- Minimaler Datenverlust

Abbildung 5: Erkennungsrate vs. Datenverlust

Zukünftige Herausforderungen

Technologische Entwicklungen:

- KI in Ransomware: Adaptives, intelligentes Verhalten
- Quantencomputing: Bedrohung für aktuelle Verschlüsselung
- IoT-Ransomware: Neue Angriffsflächen
- Cloud-native Ransomware: Angriffe auf Cloud-Infrastrukturen

Forschungsbedarf:

- Echtzeit-Schutz und Zero-Day-Erkennung
- Post-Quantum-Kryptographie
- Automatisierte Incident Response
- Internationale Zusammenarbeit bei Strafverfolgung

Fazit

Zusammenfassung

Kernaussagen:

- Ransomware bleibt eine der größten Cyberbedrohungen
- Kontinuierliche Evolution der Angriffsmethoden (RaaS, Multi-Extortion)
- Kritische Infrastrukturen besonders gefährdet
- Prävention ist der beste Schutz

Handlungsempfehlungen:

- Mehrschichtige Sicherheitsarchitektur
- Regelmäßige Backups und Tests
- Kontinuierliche Schulung der Mitarbeiter
- Investition in moderne Detektionssysteme
- Vorbereitung von Incident Response Plänen

Quellen

- The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions (Razulla et al.)
- ENISA (2024): Threat Landscape Report 2024 (European Union Agency for Cybersecurity)
- Ransomware early detection by the analysis of file sharing traffic (REDFISH) (Morato et al.)
- A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions (Oz et al.)