Ransomware-Angriffe

# 3 Gründe, warum Ransomware-Angriffe heute noch gefährlicher sind

**Ransomware ist die größte Gefahr für Unternehmen im Bereich Cybersecurity. Wir zeigen hier die drei Gründe, die Ransomware noch gefährlicher machen, aber auch das, was Unternehmen machen können, um nicht Opfer zu werden.**

Ransomware ist ein einträgliches Geschäft. So wurden allein im Jahr 2023 weltweit 1 Milliarde Euro an Lösegeld bezahlt. Schlimmer als diese Zahlungen ist jedoch die Spur der Verwüstung, die Ransomware-Angriffe in der Unternehmenslandschaft nach sich ziehen. Nach Bitkom-Angaben beliefen sich allein in Deutschland alle Schäden durch Cyberangriffe im Jahr 2024 auf ~178,6 Mrd. €. Davon geht natürlich ein immenser Teil auf das Konto von Ransomware.

Und die Forderungen der Erpresser werden immer höher, wie auch die Zahl an Ransomware-Attacken weiter nach oben geht. Ransomware ist heute im Security-Bereich die größte Bedrohung für die Existenz eines Unternehmens. Und das hat gute Gründe.

## Grund 1: Industrialisierung der Ransomware

Um profitabler zu werden, schreitet die Industrialisierung (auch Ransomware-as-a-Service (RaaS) genannt) stark voran und ist mittlerweile Realität**.** War Ransomware früher oft ein Einzelprogramm, ist es heute ein Geschäftsmodell. Anbieter entwickeln Verschlüsselungs-Malware und vermieten sie an Kriminelle, die dann als Affiliates die Angriffe ausführen. Dies hat Ransomware zu einem quasi Massenmarkt gemacht.

Ein Beispiel hierfür ist Gruppe ShadowSyndicate, die als Affiliate für verschiedene Ransomware-Familien agiert. Im Jahr 2024 begann ShadowSyndicate, die Ransomware von RansomHub zu nutzen, einer neuen RaaS-Plattform, die nach der Zerschlagung von ALPHV/BlackCat und LockBit entstanden ist. ShadowSyndicate führte Angriffe durch, bei denen sie RansomHub-Ransomware einsetzten, um Daten zu verschlüsseln und zu exfiltrieren.

## Grund 2: Doppelte Erpressung

Die Erpresser erhöhen den Druck. Denn im Gegensatz zu früher sperren Angreifer nicht mehr nur das System, sondern sie exfiltrieren die Daten und drohen darüber hinaus jetzt auch, diese zu veröffentlichen, wenn kein Lösegeld gezahlt wird. Oft wird den Opfern mit Countdowns auf Seiten im Darkweb gedroht, wann ihr Daten freigegeben werden. Diese Double-Extortion kombiniert Verschlüsselung mit Datenleaks und bringt vielfach höhere Summen.

## Grund 3: Unknackbare Verschlüsselung

Um den Druck auf ihre Opfer zu maximieren, verschlüsseln die Angreifer die Daten mit einem **AES/RSA-Verschlüsselungsverfahren**: Jede Datei wird zunächst mit einem symmetrischen AES-Schlüssel verschlüsselt, anschließend wird dieser AES-Schlüssel mit einem asymmetrischen RSA-Schlüssel geschützt und in der Datei abgelegt. Nur der Angreifer besitzt den für jedes Opfer individuellen RSA-Privatschlüssel, sodass nur er die Daten wieder freigeben kann.

**Wie kommen die Angreifer rein?**

Ransomware findet fast immer über eine **erste Schwachstelle** Zugang ins Netzwerk. Die häufigsten Einfallstore sind:

- **Phishing und Social Engineering:** Gefälschte E-Mails und manipulierte Webseiten sind der Hauptvektor. Mitarbeiter erhalten scheinbar seriöse Nachrichten mit versteckten Schad-Links oder -Anhängen. Bitkom fand, dass 26 % aller Unternehmen von Phishing berichteten.
- **Fernzugriffe (RDP/VPN):** Offene oder schwach abgesicherte Remote-Desktop-Verbindungen sind ein beliebter Einstieg. Ohne VPN und Zwei-Faktor-Absicherung kann RDP leicht geknackt oder mit Brute-Force überwältigt werden.
- **Software-Schwachstellen und Zero-Day-Exploits:** Ungepatchte Programme (Betriebssysteme, Server-Software, SMB, Exchange, Browser usw.) bieten Attacken Tore. Besonders gefährlich sind **Zero-Day-Lücken**, für die es noch keinen Patch gibt. Kriminelle nutzen solche Lücken aus, um sich unbemerkt im Netzwerk umzuschauen und Ransomware auszulösen.
- **Lieferketten-Angriffe:** Über Partner und Dienstleister können Täter indirekt ins Ziel-Netzwerk gelangen. Bei sogenannten Supply-Chain-Angriffen knacken die Täter zunächst Zulieferer oder IT-Dienstleister und nutzen deren Vertrauensstellungen (VPN-Zugänge, Wartungs-Accounts etc.), um ins eigentliche Ziel einzudringen.
- **Kompromittierte Zugangsdaten:** Zugangsdaten (Passwörter, SSH-Keys) werden auf Darknet-Marktplätzen gehandelt. Das Eindringen mit gekauften Credentials eröffnet Angreifern direkt Administratorrechte. In vielen Fällen gehen RDP- oder Admin-Logins über genau solche gehackten Konten.

**Abwehrstrategien für Ransomware**

Die Strategie, um Ransomware-Angriffe abzuwehren, beginnt mit **Sicherheitsstandards und Frameworks.** Wir empfehlen unseren Kunden den Aufbau und die Prüfung der IT-Sicherheit

nach etablierten Standards (z. B. NIST Cybersecurity Framework, ISO 27001/IT-Grundschutz), damit sie ihre Resilienz erhöhen können.

Wenn diese Rahmen gesetzt sind, empfiehlt sich die weitere Abwehrstrategie auf zwei Säulen zu Stellen.

**Abwehrsäule I: Technische Schutzmaßnahmen**

Technische Schutzmaßnahmen zielen darauf ab, Angriffe frühzeitig zu erkennen oder ihre Ausbreitung zu verhindern:

- **Endpoint Security (AV/EDR/XDR):** Auf Endgeräten sollte moderne Sicherheitssoftware mit Verhaltensanalyse laufen. Cloud-basierte Lösungen und Intrusion-Prevention-Module erhöhen den Schutz.
- • **NextGen-Firewalls (NGFW):** Moderne Firewalls, die neben klassischer Paketfilterung auch Funktionen wie Deep Packet Inspection, Intrusion Prevention und Applikationskontrolle bieten, um Netzwerke effektiv vor komplexen Bedrohungen zu schützen.
- **Netzwerksegmentierung:** Trennung von Netzbereichen (z. B. Büro, Produktion, Server) verhindert Schadcode-Ausbreitung. Laut BSI lässt sich damit in 80–90 % der Fälle größere Ausbreitung verhindern.
- **Multi-Faktor-Authentifizierung (MFA):** Absicherung von Admin- und Fernzugängen durch MFA schützt vor Missbrauch kompromittierter Passwörter.
- **Monitoring & Logging:** Zentralisiertes Monitoring (SIEM/NDR) erkennt auffälliges Verhalten (z. B. Massenzugriffe, Datenabflüsse). Tools wie IDS/IPS, Firewalls und Log-Auswertung (z. B. mit Splunk) alarmieren bei Vorfällen.
- **Sicherheitsstandards:** Umsetzung nach Frameworks wie NIST, ISO 27001 oder IT-Grundschutz stärkt die Resilienz. Das BSI bietet praxisnahe Leitfäden für IT-Härtung und Überwachung.

**Abwehrsäule II – Organisatorische Schutzmaßnahmen**

Neben Technik hilft vor allem Vorbereitung auf den Ernstfall:

- **Awareness-Trainings:** Regelmäßige Schulungen sensibilisieren Mitarbeiter für Phishing, Social Engineering und sicheres Verhalten. Simulationen („Phishing-Tests“) schärfen das Bewusstsein. Ein engagiertes Sicherheitsbewusstsein auf allen Ebenen verringert Infektionsrisiken erheblich.

- **Notfall- und Incident-Response-Plan:** Ein strukturierter IT-Notfallplan ist essentiell. Darin muss beschrieben sein, welche kritischen Systeme im Ernstfall priorisiert wiederhergestellt werden und wer welche Rolle hat. Hier ist es wichtig, dass alle beteiligten Personen wissen, was zu tun ist und dass dieser Plan immer erreichbar abgelegt ist, also nicht (nur) auf dem Server. In Deutschland verfügen erstaunlicherweise nur etwa 40 % der Unternehmen über einen solchen Plan – 60 % wären im Cyber-Notfall unvorbereitet.
- **Backup- und Wiederanlaufkonzept:** Backups sind die wichtigste Vorsorge: Sie ermöglichen Wiederherstellung ohne Lösegeldzahlung. Wichtig sind auch regelmäßige Tests der Wiederherstellung. Eine zentrale Datenspeicherung (z. B. Netzlaufwerke mit restriktiven Zugriffsrechten) kann verhindern, dass Benutzerdateien verschlüsselt werden können.
- **Incident-Response-Prozesse:** Jenseits des Plans benötigt es klare Abläufe zur Entdeckung und Meldung. Die Meldekette wie auch Kommunikationswege müssen feststehen (z.B. auch externe Experten und Behörden wie CERT-Bund informieren). Bei jedem Vorfall sollte ein IT-Sicherheitsbeauftragter und ein Krisenteam sofort aktiviert werden. Regelmäßige Übungen und Nachbesprechungen verbessern die Reaktion kontinuierlich.

**Praxisbewährte Maßnahmen zur Risikominimierung**

- In großen Umgebungen kommen umfassende Security-Suites zum Einsatz. Moderne EDR/XDR-Systeme wie **CrowdStrike Falcon**, **SentinelOne** oder **Microsoft Defender for Endpoint** bieten automatisierte Bedrohungserkennung. Advanced Firewalls und Sandboxing (z. B. von **Palo Alto**, **Check Point**, **Fortinet**) blockieren Ransomware-Angriffe. SIEM-Plattformen (**Splunk**, **QRadar**, **Elastic**) sowie Managed Detection & Response (MDR) ergänzen die Abwehr. Für Backups und Recovery sind spezialisierte Lösungen empfehlenswert (z. B. **Veeam**, **Acronis**, **Rubrik**), die Schutz gegen Manipulation und Backdoor-Verschlüsselung bieten. Auch dedizierte Phishing-Simulationen oder Awareness-Trainings großer Anbieter (z. B. **KnowBe4, proofpoint**) können die Mitarbeitersicherheit professionalisieren.

## Fazit

Ransomware-Angriffe sind die größte Gefahr für Unternehmen. Die Lösegeld-Forderungen steigen und das Vorgehen der Erpresse wird immer rabiater. Hierzu haben sich die Angreifer auf neue Wege spezialisiert, indem sie

1. Ransomware industrialisieren und als Service anbieten,
2. durch Datenklau und Veröffentlichungs-Drohung den Druck auf die Opfer erhöhen,
3. die Verschlüsselung unknackbar machen.

All dies macht Ransomware zu so einer großen Bedrohung. Sind die Täter einmal im System, gibt es kaum mehr Möglichkeiten und der Reparaturschaden ist existenzgefährdend.

Das Einzige, was Unternehmen machen können, ist mit Regeln, Frameworks sowie mit technischen und organisatorischen Schutzmaßnahmen dafür sorgen, dass niemand in das eigene System kommt. Und das so schnell wie möglich, denn je länger mit Schutzmaßnahmen gewartet wird, desto schwieriger ist es diese überhaupt wieder aufzuholen. Dabei können Beratungs- und Integrationshäuser helfen.

**Zum Autor:**
Philip Huisgen ist Managing Director der DATAKOM GmbH.
Er hat 25 Jahre als Unternehmensberater bei den großen Beratungen wie KPMG, Accenture und Capgemini gearbeitet. Sein Themenschwerpunkt war stets die Entwicklung von Organisationen in der IT. Sein Promotionsstudium widmete er den Organisationssoziologien in Unternehmen mit besonderem Fokus auf die Wirkungsaspekte von organisationsbezogenen Krisen. Er ist heute Managing Director der DATAKOM GmbH, die sich seit 1986 als Beratungs- und Integrationspartner auf die Einführung von IT-Security-Prozessen und -Lösungen in Unternehmen spezialisiert hat.