Cyber-Erpressung zum Mitmachen – Wie RaaS den Mittelstand ins Visier nimmt

Inhalt

Aktuelle Bedrohungslage für mittelständische Unternehmen in Deutschland

Die **Cyber-Bedrohungslage für den Mittelstand ist so kritisch wie nie zuvor.** Ransomware-Angriffe zählen weiterhin zu den größten Gefahren – und mittelständische Firmen rücken immer stärker in den Fokus der Täter[1]. Während früher vor allem große Konzerne im Visier standen, *richten Cyberkriminelle ihre Angriffe zunehmend auf kleine und mittlere Unternehmen* (KMU), da sie dort oft die schwächste Gegenwehr erwarten. Im **BSI-Lagebericht 2024** wird betont, dass Angreifer „bevorzugt dort angreifen, wo sie am wenigsten Gegenwehr erwarten“ – also bei Firmen mit unzureichenden Schutzmaßnahmen, wozu viele Mittelständler zählen. Entsprechend **fielen 2023 vermehrt KMUs Ransomware-Attacken zum Opfer**[2].

Diese Entwicklung hängt eng mit dem Konzept *Ransomware-as-a-Service* (RaaS) zusammen. RaaS hat Ransomware-Angriffe quasi zu einem **Massengeschäft** gemacht. Professionelle Hackergruppen bieten ihre Schadsoftware und Infrastruktur auf Untergrund-Marktplätzen an – **gegen Bezahlung kann praktisch jeder Angriffe einkaufen**. Dadurch ist eine arbeitsteilig organisierte Untergrund-Industrie entstanden, in der **über 100 kriminelle Gruppen aktiv deutsche Unternehmen angreifen**. Laut BSI sind allein die fünf aktivsten Gruppen für rund die

[1] mittelstand-heute.committelstand-heute.com
[2] bsi.bund.de

Hälfte aller erfassten Angriffe verantwortlich[3]. Die Folge: **Die Bedrohungslage bleibt angespannt.** Unternehmen stehen heute nicht mehr einzelnen Hackern gegenüber, sondern einer effizienten kriminellen Dienstleistungsindustrie.

Zugleich beobachten Ermittlungsbehörden die **Ausweitung von „Doppelerpressung“** (Double Extortion): Immer häufiger stehlen Ransomware-Gangs vertrauliche Daten und drohen mit Veröffentlichung, falls kein Lösegeld gezahlt wird. Der **BSI-Lagebericht** verzeichnete einen Anstieg solcher Datenleak-Fälle um 30 % (2021–2023) in Deutschland. Dieser Trend erhöht den **Druck auf mittelständische Opfer** beträchtlich, da ein reines Backup-Konzept zwar die Datenwiederherstellung ermöglicht (tatsächlich sank der Anteil der zahlenden Opfer seit 2021 von 56 % auf 36 %[4]), die Drohung mit Datenveröffentlichung jedoch weiterhin großen Schaden zufügen kann. Mittelständler müssen sich also nicht nur vor Verschlüsselung schützen, sondern auch vor Datendiebstahl und Erpressung an der „Pranger-Leak-Seite“ der Angreifer.

Fazit dieser Lage: Die Kombination aus finanziell motivierten Kriminellen, die gezielt auf schwächer geschützte mittelständische Firmen abzielen, und dem professionellen RaaS-Geschäftsmodell führt zu einer realen und akuten Bedrohung für den deutschen Mittelstand.

Professionelle RaaS-Gruppen: Wer steckt dahinter?

Der **RaaS-Markt wird von einigen hochprofessionellen Gruppen dominiert**, die teils weltweit, teils mit Fokus auf Deutschland operieren. Diese Gruppen agieren wie Unternehmen: Sie entwickeln die Ransomware, betreiben Erpresser-Webseiten und koordinieren ein Netzwerk von Affiliates (Partnerkriminellen). Eine neutrale Betrachtung der Strukturen und Reichweite der bekanntesten RaaS-Anbieter zeigt die Dimension der Gefahr:

- **LockBit:** Eine der gefährlichsten und erfolgreichsten RaaS-Gruppen der letzten Jahre. Bis zu ihrer teilweisen Zerschlagung im Februar 2024 galt **LockBit** als weltweit führend. Im Beobachtungszeitraum veröffentlichte LockBit die Daten von **40 deutschen Opfern** auf ihrer Leak-Seite; weltweit wurden der Gruppe sogar **944 Opfer** zugeschrieben. Nach dem Schlag der Strafverfolger ist LockBit zwar noch aktiv, aber nicht mehr so dominant wie zuvor.
- **Black Basta:** Ebenfalls eine etablierte Gruppe im RaaS-Geschäft. **Black Basta** reklamierte 21 erfolgreiche Angriffe auf deutsche Firmen für sich. Auffällig ist, dass Black Basta oft **ältere, bekannte Sicherheitslücken** ausnutzt – viele Opfer hätten durch verfügbare Updates geschützt werden können.
- **8Base:** Diese Gruppe erlangte 2023 Aufmerksamkeit, obwohl sie international weniger bekannt ist. Nach eigenen Angaben hat **8Base mindestens 15 deutsche Unternehmen** erpresst. Interessant ist die Arbeitsweise: 8Base **kauft Zugänge von sogenannten Access Brokern** ein, anstatt selbst in Netzwerke einzubrechen. Das verdeutlicht die enge Verzahnung von RaaS mit anderen kriminellen Dienstleistungen (dazu später mehr).
- **Play:** Hinter **Play** steckt eine RaaS-Gruppe, die 13 Opfer in Deutschland für sich beansprucht. Play fiel durch Angriffe über Schwachstellen in exponierten IT-Systemen

[3] bsi.bund.de
[4] mittelstand-heute.com

(z. B. ungepatchte VPN-Server oder E-Mail-Systeme) auf. Auch Play arbeitet mit **Zugangsdatenhändlern** zusammen, um initial in die Netzwerke der Opfer zu gelangen.

- **Cloak:** Eine relativ neue Gruppe, die offenbar einen besonderen **Deutschland-Fokus** hat. Cloak brüstet sich mit 12 erfolgreichen Attacken auf hiesige Firmen. International taucht Cloak kaum in den Top-Listen auf, doch in Deutschland zählte sie zuletzt zu den aktivsten fünf Gruppen. Wie viele andere greift Cloak bevorzugt auf **gekaufte Zugangsdaten** zurück.

Diese Beispiele zeigen, dass **RaaS-Betreiber global agierende kriminelle Organisationen** sind. Ihre „Marken" (wie LockBit, Black Basta, etc.) stehen für jeweils eigene Ransomware-Varianten, Leak-Webseiten und Affiliate-Netzwerke. **Die Reichweite ist enorm:** LockBit etwa war 2023 laut Europol die **produktivste RaaS-Gruppe weltweit**[5]. Andere wie **Cl0p** verfügen über hochentwickelte Tools – Cl0p nutzte z. B. Zero-Day-Schwachstellen für großflächige Angriffe (etwa die MOVEit-Transfer-Lücke 2023. **Neue Akteure** drängen ebenfalls nach: Gruppen wie **Alphv/BlackCat** oder **Akira** haben sich in jüngster Zeit einen Namen gemacht. All diese Gruppen eint, dass sie **auf professionelle Infrastrukturen und ausgefeilte Geschäftsmodelle setzen**, um möglichst viele Opfer zu erpressen.

Trotz ihres „Erfolgs" bleiben RaaS-Gangs nicht unverwundbar: Durch internationale Ermittlungen wurden 2023 mehrere Netzwerke empfindlich getroffen. Takedown-Operationen richteten sich u. a. gegen **QakBot** (ein verbreitetes Botnetz als Ransomware-Helfer), **RagnarLocker**, **Alphv/BlackCat** und sogar **LockBit**. Solche Aktionen führen jedoch meist nur zu kurzen Unterbrechungen – oft füllt schnell eine Nachfolgegruppe die Lücke. Die RaaS-Landschaft ist dadurch sehr dynamisch: Gruppen spalten sich, tauchen unter neuem Namen wieder auf oder es entstehen *Rebrandings*, um nach Verhaftungen weiterzumachen. Für Opfer und potenzielle Ziele ändert das wenig: Die **Gefahr durch Ransomware-Erpressung bleibt bestehen**, unabhängig vom konkreten Namen der Gruppe.

Funktionsweise des RaaS-Ökosystems: Akteure und Arbeitsweise

Ransomware-as-a-Service funktioniert nach dem Prinzip einer arbeitsteiligen „Cyber-Industrie". Ähnlich einer Wertschöpfungskette übernimmt jeder Akteur einen Teil des Angriffs. Die wichtigsten Rollen in diesem kriminellen Ökosystem sind:

- **Entwickler / RaaS-Betreiber:** Dies sind die **Profis im Hintergrund**, die die Ransomware-Software programmieren und die technische Infrastruktur betreiben. Sie stellen z. B. Verschlüsselungs-Malware, Kontrollserver, Leak-Webseiten und Zahlungsportale bereit. Die Betreiber **vermieten diese Werkzeuge an Affiliates** oder nehmen sie in eine Partnerprogramm-Struktur auf. Im Gegenzug verlangen sie entweder **Einrichtungsgebühren oder einen Anteil am erbeuteten Lösegeld**[6]. Typischerweise erhält der RaaS-Anbieter etwa **20–30 % der Lösegeldsumme**, während der Großteil an den ausführenden Affiliate geht. Die RaaS-Admins verwalten zudem die Krypto-Geldströme: Zahlungen der Opfer fließen oft zunächst in **die Wallet der Betreiber**,

[5] industrialcyber.co
[6] cloudflare.com

werden dort ggf. durch Krypto-Mixer geschleust und anschließend **automatisiert zwischen Betreiber und Affiliate aufgeteilt**[7]. Insgesamt tritt der RaaS-Betreiber also als **Dienstleister im Hintergrund** auf, der „Crimeware"-Tools bereitstellt und für die reibungslose Abwicklung des Erpressungsbetriebs sorgt.

- **Affiliate (Angreifer vor Ort):** Die Affiliates sind die **ausführenden Täter**, also diejenigen, die den eigentlichen Einbruch und die Verteilung der Ransomware beim Opfer vornehmen. **Affiliates mieten oder kaufen den Zugang zur RaaS-Plattform** und erhalten dort die fertige Schadsoftware sowie oft weitere Hilfsmittel. Anschließend suchen sie sich Ziele aus und **führen die Angriffe durch** – sei es via Phishing-Mail, mittels Ausnutzen offener Sicherheitslücken oder durch zugekaufte Zugangsdaten. Gelingt eine Erpressung, teilen sie die Beute mit dem RaaS-Betreiber (Beispiel: bei einem Erlös von 100.000 € erhält der Affiliate ca. 70–80 %, der Rest geht an die Betreiber). Die Affiliates **spezialisieren sich darauf, Ransomware-Angriffe tatsächlich durchzuführen**, ohne selbst programmieren zu müssen. In gewissem Sinne sind sie die „Franchisenehmer" im RaaS-System. Manche Affiliate-Gruppen arbeiten sehr professionell und international; andere sind Einzelgänger oder kleine Zellen, die mit den bereitgestellten Tools erste Gehversuche im Cybercrime unternehmen.

- **Initial Access Broker (Zugangsdatenhändler):** Eine eigenständige, aber eng verbundene Rolle im RaaS-Ökosystem sind die **Zugangshändler**. Diese Kriminellen **sammeln kompromittierte Zugangsdaten** (z. B. gestohlene Passwörter, VPN-Logins oder Zugänge über Malware-Infektionen) und verkaufen sie an Interessenten. Viele RaaS-Affiliates greifen auf diese Dienste zurück, um **einfach und schnell in die Netzwerke** von Unternehmen zu gelangen, anstatt mühsam selbst Schwachstellen aufzuspüren. Das Geschäft mit Zugängen blüht: Ein funktionierendes Admin-Konto oder ein offener RDP-Zugang zu einem Unternehmensnetzwerk kann auf dem Schwarzmarkt je nach Größe des Ziels mehrere tausend Euro einbringen. **RaaS-Gruppen arbeiten häufig mit Access Brokern zusammen**, wie Beispiele (8Base, Play, Cloak) gezeigt haben. Diese Arbeitsteilung senkt die Einstiegshürde für Angreifer weiter – wer kein Talent für Hacking hat, **kauft sich den Zugang einfach ein**.

- **Weitere Dienstleister:** Das Cybercrime-as-a-Service-Ökosystem bietet noch mehr Bausteine, die RaaS-Akteure nutzen. So gibt es **spezielle Malware-Dienste** („Malware-as-a-Service"), z. B. **EDR-Killer** zum Ausschalten von Sicherheitssoftware. Ebenso können **Exploit-Kits** (für bekannte Schwachstellen) oder **Phishing-Kits** gemietet werden. Manche Gruppen rekrutieren auch **„Inkasso-Spezialisten" oder Verhandlungsführer**, um den Druck auf Opfer zu erhöhen – etwa durch professionelle Kommunikation in Erpresserschreiben oder das Veröffentlichen von Musterdaten auf Leak-Seiten. **Geldwäscher** und „Exchanger" sorgen dafür, dass Krypto-Lösegelder in Fiat-Geld umgewandelt und verteilt werden. Insgesamt entsteht so eine **vollständige Wertschöpfungskette**, in der **für jeden Schritt einer komplexen Cyber-Attacke ein passender Service verfügbar ist**[8]. Für die Angreifer hat das zwei Vorteile: Zum einen können sich die „Service-Provider" auf einzelne Tools spezialisieren und diese schnell verbessern. Zum anderen stehen dadurch selbst hochentwickelte Angriffsmittel sofort

[7] eucrim.eu
[8] bsi.bund.de

einer großen Zahl weniger versierter Krimineller zur Verfügung. Diese Industrialisierung potenziert die Bedrohungslage erheblich.

Zusammengenommen bildet RaaS ein Ökosystem, das Cyberkriminellen jeden Könnensniveau ermöglicht, gemeinsam effiziente Angriffe durchzuführen. Es gibt Spezialisten für jede Aufgabe – vom Erstzugang über Verschlüsselungssoftware bis zur Lösegeldabwicklung – und all diese Akteure treiben sich gegenseitig zu weiterer Professionalisierung an.

Leistungen der RaaS-Plattformen: „Cybercrime as a Service“ im Detail

RaaS-Plattformen werben in Untergrundforen oft offensiv mit einem **Rundum-Service für angehende Erpresser**. Im Folgenden ein Überblick, welche **konkreten Dienstleistungen** typische RaaS-Angebote umfassen:

- **Schadsoftware „aus der Box“:** Der Kern jeder RaaS-Plattform ist die **bereitgestellte Ransomware**. Affiliates erhalten Zugriff auf ein Portal, in dem sie mit wenigen Klicks ihre **individuelle Ransomware** konfigurieren können – etwa die Verschlüsselungsstärke, die Lösegeldforderung, die Sprache der Erpressernachricht etc. Häufig wird eine **benutzerfreundliche Web-Oberfläche** geboten[9]. Beispielsweise hatte die RaaS-Variante *Karmen* ein Dashboard, das **in Echtzeit Infektionszahlen und Profite anzeigte** und es selbst technisch unerfahrenen Nutzern ermöglichte, mit wenigen Schritten ihren Ransomware-Build zu erstellen. Diese *One-Click-Oberflächen* machen es extrem leicht, Schadprogramme zu generieren, ohne Programmierkenntnisse.

- **Technische Infrastruktur:** Neben der Malware selbst stellen RaaS-Anbieter die nötige **Server-Infrastruktur** bereit. Dazu gehören **Command-and-Control-Server** zur Steuerung der Malware, **Leak-Seiten** im Darknet (meist als .onion-Seiten im Tor-Netzwerk) für die Veröffentlichung gestohlener Daten, sowie **Kommunikationsportale** für die Opfer. Über letztere können Opfer z. B. auf einer gesicherten Webseite Kontakt aufnehmen, den Zahlungsprozess starten oder den Decryptor herunterladen. Die gesamte **Zahlungsabwicklung** läuft typischerweise über das RaaS-Portal: Opfer werden angewiesen, den geforderten Betrag in Kryptowährung (meist Bitcoin oder Monero) an eine **vom RaaS-System generierte Wallet-Adresse** zu überweisen. Die Plattform überwacht den Zahlungseingang und **organisiert die Verteilung** des Geldes (automatisch oder manuell) an die Beteiligten. Für den Affiliate hat das den Vorteil, dass er sich nicht selbst um die technischen Aspekte von Zahlung und Datenveröffentlichung kümmern muss – all das wird vom „Service“ erledigt.

- **Schulung und Anleitungen: RaaS wird oft mit einem Handbuch geliefert.** Viele Betreiber stellen **Schritt-für-Schritt-Guides** zur Verfügung, in denen erklärt wird, wie man die Ransomware verteilt, typische Sicherheitsmaßnahmen umgeht und die Kommunikation mit dem Opfer führt[10]. Diese Anleitungen können schriftlich vorliegen oder als Videos/Tutorials in Untergrund-Foren. Darüber hinaus existieren oft

[9] thehackernews.com
[10] cloudflare.com

Community-Foren oder Chat-Gruppen für Kunden (Affiliates), in denen sie sich austauschen und Tipps holen können. Kurzum: Wer einen RaaS-Zugang erwirbt, bekommt meist eine **komplette Einarbeitung** in die „Kunst" der Ransomware-Erpressung mitgeliefert.

- **Technischer 24/7-Support:** Erstaunlich aber wahr – viele RaaS-Anbieter werben mit **Rund-um-die-Uhr Kundensupport** für ihre kriminellen Kunden. So, wie seriöse Softwarefirmen ihren Nutzern helfen, bieten RaaS-Foren Hilfestellung, falls ein Affiliate **technische Probleme** hat oder die Malware nicht wie erwartet funktioniert. Dieser Support läuft zumeist über die gleichen Kanäle im Darknet (Foren, verschlüsselte Messenger) und kann z. B. Hilfestellung bei der Konfiguration von Malware, der Nutzung von Exploits oder bei Entschlüsselungsfragen leisten. **Einige RaaS-Programme haben sogar Ticket-Systeme und „Kundenbewertungen"**, sodass neue Interessenten sehen können, ob der Service zuverlässig ist[11]. Die professionelle Aufmachung dieses Supports senkt die Hemmschwelle für Einsteiger enorm – man fühlt sich als „Kunde" einer Dienstleistung, nicht wie ein Einzelgänger-Verbrecher.

- **Zielvorgaben und Regeln:** Interessanterweise geben manche RaaS-Betreiber **Richtlinien vor**, welche Opfer angegriffen werden dürfen. Häufige Regel: **Keine Angriffe auf GUS-Staaten (insbesondere Russland)** – ein Hinweis darauf, wo viele Betreiber sitzen und lokale Behördenärger vermeiden wollen. Einige RaaS-Gruppen untersagen ihren Affiliates auch bestimmte Branchen, etwa **kritische Infrastrukturen oder Krankenhäuser**, da solche Fälle zu großen Ermittlungsdruck führen und moralisch „schlechte PR" für das „Geschäftsmodell" bedeuten. Andere Plattformen wiederum sind **weniger wählerisch** und nehmen jeden zahlenden Kunden auf, der irgendein Ziel angreifen will. In Untergrund-Foren werben RaaS-Anbieter auch gezielt um **„erfolgreiche" Affiliates**, die sich durch große Coupes auszeichnen – denn jeder große Vorfall steigert den Ruf der RaaS-Gruppe und zieht neue Kunden an. Unterm Strich zeigt das: **RaaS ist ein Business**, in dem selbst Marketing, Reputation und Kundenbindung (bzw. Täterbindung) eine Rolle spielen.

- **„Inkasso" und Zusatzleistungen:** Hat ein Affiliate erfolgreich ein Netzwerk verschlüsselt, unterstützen viele RaaS-Dienste auch in der **weiteren Erpressungsphase**. So wird über die erwähnten Leak-Webseiten der Druck aufrecht erhalten – die Betreiber kümmern sich um das Hosten und ggf. auch um das Veröffentlichen von Beweisdaten (z. B. ein paar sensible Dokumente als Beweis für den Datendiebstahl). Manche RaaS-Portale verfügen über integrierte **Chat-Funktionen**, damit Opfer direkt mit den Tätern (Affiliate oder dem RaaS-Support) verhandeln können. Es gibt Hinweise, dass einige RaaS-Teams sogar **Verhandlungsexperten** bereitstellen, die helfen, maximale Zahlungen herauszuschlagen oder auf vertrauenswürdig zu machen (z. B. Versprechungen eines Decryptors liefern). **Treuhand-Funktion:** In gewisser Weise fungiert der RaaS-Betreiber auch als eine Art Treuhänder zwischen Opfer und Affiliate – er verwaltet den Decryption Key und gibt ihn meist erst frei, wenn die Zahlung bestätigt ist, was dem Affiliate die lästige Aufgabe erspart und zugleich sicherstellt, dass der Betreiber seinen Anteil erhält. All diese **Dienstleistungen ermöglichen es selbst technisch unbedarften Kriminellen, einen kompletten**

[11] crowdstrike.com

Erpressungsangriff „als Service“ durchzuführen, vom Erstzugang bis zum Geldeinsammeln[12].

Zusammengefasst bieten RaaS-Plattformen **eine kriminelle Rundumlösung** an: **Malware, Infrastruktur, Anleitung, Support und Zusatzdienste** aus einer Hand. Für „Kunden“ der Plattform reduziert das die erforderlichen eigenen Fähigkeiten auf ein Minimum – der Erfolg eines Angriffs hängt weniger von IT-Know-how ab, sondern eher von der Skrupellosigkeit des Affiliates bei der Auswahl und Einschüchterung seiner Opfer.

Unterstützung für technisch Unbedarfte: Wie RaaS Cybercrime demokratisiert

Eines der beunruhigendsten Merkmale von Ransomware-as-a-Service ist, **wie stark es die Einstiegshürden für Kriminalität senkt**. Selbst Personen mit minimalem IT-Wissen können dank RaaS gefährliche Angriffe starten. Diese „Demokratisierung“ des Cybercrime wird durch mehrere Faktoren begünstigt:

- **Einfache Bedienbarkeit:** Moderne RaaS-Portale sind oft so gestaltet, dass sie **intuitiv bedienbar** sind – vergleichbar mit legaler Software. Über **grafische Oberflächen** lässt sich per Mausklick ein Ransomware-Build erstellen[13]. Viele Prozesse (Schadcode-Erstellung, Schlüsselgenerierung, Opfernachverfolgung) sind automatisiert. Das heißt, ein Angreifer muss technisch kaum mehr können, als z. B. eine Phishing-Mail zu versenden oder einen bereits erhaltenen Zugang zu nutzen. **Coding-Kenntnisse sind nicht nötig**: Wie Cloudflare anmerkt, **benutzen viele Täter fertige Exploits, weil sie selbst nicht programmieren können**. Die eigentliche „schmutzige Arbeit“ – das Schreiben von Verschlüsselungssoftware – erledigen die RaaS-Entwickler. Damit wird Ransomware-Erpressung quasi zu einem **Plug-and-Play-Geschäft**.
- **Allzeit verfügbare Hilfe:** Die Hemmung, eine Straftat zu begehen, sinkt, wenn man sich dabei **nicht allein gelassen** fühlt. Genau das passiert im RaaS-Umfeld: Unerfahrene Täter bekommen über Foren und Chats **Rückhalt von der Community** und den Betreibern. Treten Probleme auf – z. B. die Malware läuft nicht auf dem Zielsystem oder der Decryptor funktioniert nicht – kann der Affiliate **jederzeit Support anfordern**. Das Gefühl, im Notfall Hilfe zu haben, nimmt vielen die Unsicherheit. Einige RaaS-Gruppen stellen sogar **persönliche Ansprechpartner** bereit oder beantworten Fragen „der Kundschaft“ binnen Minuten. Diese professionelle Betreuung vermittelt selbst absoluten Laien das Gefühl, **eine Erfolgschance zu haben**, und senkt die Lernkurve dramatisch.
- **Vorhandene kriminelle Toolkits:** Dank des gesamten Crimeware-Ökosystems muss ein Amateur nicht mal wissen, wie man sich Zugang zu einem Unternehmensnetzwerk verschafft. **Für nahezu jede Phase gibt es ein fertiges Tool oder einen Dienstleister**, den man nutzen kannbsi.bund.de. Beispiel: Jemand ohne Hacking-Erfahrung kauft sich einfach über einen Access Broker die Zugangsdaten, lädt im RaaS-Portal seinen Verschlüsselungstrojaner herunter und folgt dem mitgelieferten Leitfaden, um das Firmennetzwerk lahmzulegen. **Komplexe Aufgaben wie das Spurenverwischen** (Anti-

[12] bsi.bund.de
[13] thehackernews.com

Forensik, Löschen von Backups) übernimmt teils die Ransomware automatisch oder es gibt Skripte dafür. Dadurch können selbst **„Script Kiddies" – ein abfälliger Begriff für technisch unbedarfte Hacker – hochwirksame Angriffe durchführen**, die früher nur gut ausgebildeten Cyberkriminellen vorbehalten waren.

- **Geringes Entdeckungsrisiko (scheinbar):** In Untergrund-Foren wird RaaS als **schneller Weg zu großem Geld** angepriesen – oft mit dem Hinweis, das Risiko erwischt zu werden, sei gering. Tatsächlich operieren viele Banden aus Ländern mit begrenzter Strafverfolgung (z. B. Russland), was ein Gefühl von Straflosigkeit vermittelt. **„Mit Versprechen von Millionen und kaum Strafverfolgungsrisiko"** lockt das RaaS-Modell neue Täter an[14]. Aus Tätersicht klingt das attraktiv: Man muss nur ein paar Tausend Euro für Zugänge und Tools investieren und hat die Chance, ein Vielfaches als Lösegeld zu erpressen. Die Realität ist komplexer (siehe Risiken unten), aber die **Marketing-Botschaften der RaaS-Szene verleiten** auch technisch weniger Versierte, ihr Glück zu versuchen.

All diese Faktoren führen dazu, dass **Ransomware-Erpressung längst kein exklusives Metier von Elite-Hackern mehr ist**. Vielmehr kann praktisch jeder mit krimineller Energie – vom frustrierten Insiders bis zum jugendlichen „Gamer", der sich beweisen will – innerhalb kurzer Zeit die Fähigkeiten erwerben, um ein mittelständisches Unternehmen digital in die Knie zu zwingen. Europol berichtet, dass die **Zahl der Cyberkriminellen stetig anwächst und immer mehr auch junge Täter ohne volles Unrechtsbewusstsein einsteigen**[15]. Diese Entwicklung stellt Unternehmen vor die Herausforderung, dass die Angreifer aus **unberechenbar vielen Ecken** kommen können. Es ist nicht mehr nur der Profi-Cybergangster aus dem Ausland – theoretisch kann auch der lokale Kleinkriminelle zum Affiliate einer großen RaaS-Bande werden.

Für die Geschäftsführer und Inhaber mittelständischer Firmen bedeutet dies: **Die Gefahr, Opfer einer Ransomware-Erpressung zu werden, ist breiter gestreut als je zuvor.** Man hat es nicht nur mit einzelnen Meistern ihres Fachs zu tun, sondern potentiell mit einer Vielzahl von weniger qualifizierten, aber durch RaaS **befähigten Kriminellen**. Dieses „Breitbandrisiko" erfordert eine erhöhte Wachsamkeit und umfassende Schutzkonzepte, wie im Fazit skizziert.

Mögliche Einnahmen für Täter und eingegangene Risiken

Warum floriert RaaS aus Täterperspektive? – Kurz gesagt: **hohe potenzielle Gewinne bei oft als beherrschbar eingeschätztem Risiko.** Doch neben den Verlockungen stehen auch beträchtliche Gefahren für die Angreifer selbst, die nicht unterschätzt werden sollten. Dieser Abschnitt beleuchtet die **möglichen Einnahmen eines RaaS-Affiliates** und die **Risiken (rechtlich, finanziell, operativ)**, die er dabei eingeht.

Verlockende Gewinne: Lösegeldsummen in schwindelerregender Höhe

Die finanziellen Möglichkeiten im RaaS-Geschäft sind erheblich. **Lösegeldforderungen von mehreren Hunderttausend Euro sind inzwischen üblich**, bei größeren Unternehmen fordern die Täter oft Millionenbeträge. Laut Sicherheitsanalysen betrug die durchschnittlich **bezahlte**

[14] intel471.com
[15] **eucrim.eu**

Lösegeldsumme Anfang 2024 rund **382.000 US-Dollar** (ca. 350.000 €) pro Vorfall[16]. In Einzelfällen werden auch viel höhere Summen erzielt: So forderte eine RaaS-Gruppe 2023 vom Halbleiterhersteller TSMC rund 70 Mio. $ – und auch deutsche Mittelständler sahen sich schon zweistelligen Millionenforderungen gegenüber[17].

Insgesamt strich die Ransomware-Industrie 2023 gewaltige Beträge ein. Allein im ersten Halbjahr 2023 wurden weltweit **449 Millionen US-Dollar an Lösegeldern gezahlt**[18] – damit steuert 2023 auf einen der profitabelsten Rekorde für Erpresser zu. Diese Zahlen verdeutlichen: **Für einen erfolgreichen Affiliate können bereits wenige Angriffe finanziell lohnend sein.** Beispielrechnung: Erpresst ein Affiliate ein mittelständisches Unternehmen und erzielt eine Zahlung von 200.000 €, so behält er – nach Abzug des RaaS-Anteils – vielleicht **140.000 €**. Mehrere solche Coups im Jahr könnten also Einkünfte in Millionenhöhe bedeuten – weit mehr, als viele legale Berufe in so kurzer Zeit einbringen.

Die **finanzielle Motivation dominiert** denn auch in der Szene. RaaS-Anbieter werben gezielt mit Erfolgsgeschichten: Etwa, dass Top-Affiliates monatlich sechsstellig verdienen. Einige Affiliates haben Berichten zufolge in Luxusgütern und Kryptowerten ein Vermögen angehäuft. Zudem kommt hinzu, dass Lösegelder meist in **anonymen Kryptowährungen** fließen, was Tätern die unmittelbare **Verfügbarkeit des Geldes** ermöglicht (vorausgesetzt, sie können es waschen). Diese rosigen Aussichten erklären, warum trotz aller Risiken stetig neue Akteure ins RaaS-Geschäft einsteigen.

Rechtliche Risiken: Hohes Strafmaß und Fahndungsdruck

Den potenziellen Gewinnen stehen **erhebliche rechtliche Risiken** gegenüber. **Ransomware-Erpressung ist eine schwere Straftat** – in Deutschland fallen solche Delikte u.a. unter Computer-Sabotage, Erpressung und Datenveränderung, was in Summe mit mehrjährigen Freiheitsstrafen geahndet werden kann. Wer glaubt, im Internet anonym agieren zu können, **wiegt sich in trügerischer Sicherheit**. Zwar operieren viele RaaS-Banden aus rechtlich „schwierigen“ Staaten, doch die internationale Zusammenarbeit der Strafverfolger hat zuletzt spürbar zugenommen. Europol und Interpol koordinieren grenzüberschreitende Ermittlungsgruppen, und 2023 gab es **zahlreiche Festnahmen von RaaS-Affiliates und Betreibern**[19]. So wurden etwa Mitglieder der Gruppen REvil, NetWalker, Hive und anderen in verschiedenen Ländern verhaftet und vor Gericht gestellt. Auch in Deutschland gab es Verurteilungen im Zusammenhang mit Ransomware-Kriminalität. Die **Wahrscheinlichkeit, für einen unvorsichtigen Affiliate identifiziert zu werden, steigt** – insbesondere, wenn dieser keine ausgefeilte OpSec (Operation Security) beherrscht. RaaS-Anbieter selbst wissen um dieses Risiko: Einige akzeptieren **nicht jeden x-beliebigen Kunden**, sondern verlangen gewisse Referenzen oder Fähigkeiten, um zu vermeiden, dass **unbedarfte Neulinge schnell erwischt werden und die Spur zur Plattform zurückverfolgt wird**. Für den Täter bedeutet das: **Wer technische Fehler macht oder Spuren hinterlässt, läuft Gefahr, enttarnt zu werden.** Und die Konsequenzen – Hausdurchsuchung, Strafverfahren, Schadensersatzforderungen der Opfer – können das Leben nachhaltig ruinieren. Gerade weil viele Täter jung und unerfahren sind, unterschätzen sie diese juristischen Folgen oft.

---

[16] swisscybersecurity.net
[17] it-daily.net
[18] emsisoft.com
[19] industrialcyber.coindustrialcyber.co

Ein weiterer Aspekt: **Cyberkriminelle agieren in einem unsicheren Umfeld – es gibt keinen „Ehrencodex“.** Sollte ein Affiliate beispielsweise von der RaaS-Gruppe betrogen werden oder in einem Konkurrenzkampf geraten, kann er sich schlecht an Behörden wenden. Es gab Fälle, in denen RaaS-Admins unzufriedene Affiliates selbst enttarnt oder deren Gelder einbehalten haben. All dies unterstreicht: **Das rechtliche Risiko und die allgemeine Unsicherheit des kriminellen Milieus sind immens**, selbst wenn die Täter es oft anders einschätzen.

Finanzielle und operative Risiken: Kosten, Betrug und Fehlschläge

Neben der Strafverfolgung tragen RaaS-Angreifer auch **finanzielle Risiken**. Zwar wird oft nur im Erfolgsfall ein Prozentsatz fällig (Revenue Share Modell), doch manche RaaS-Anbieter verlangen **Vorauszahlungen oder Abogebühren** für ihre Dienste. Ein Affiliate könnte also Geld investieren (für Zugänge, Malware, evtl. „Premium“-Funktionen), ohne garantiertes Einkommen. **Scheitert der Angriff oder zahlt das Opfer nicht**, bleibt der Täter auf diesen Kosten sitzen. Angesichts dessen, dass mittlerweile **über 60 % der Opfer kein Lösegeld zahlen**, ist das Ausfallrisiko real. Ein Angreifer muss evtl. mehrere Unternehmen attackieren, um einen „Treffer“ zu landen – jeder Versuch birgt Kosten (gekaufte Exploits, Arbeitszeit, evtl. neue Zugänge), sodass unterm Strich **der Profit geringer ausfallen kann als erhofft**.

Die **operative Umsetzung** eines Angriffs bringt ebenfalls Risiken mit sich. Ein RaaS-Kunde ist zwar mit Tools ausgestattet, doch die Praxis kann schiefgehen: Möglicherweise **endet der Befall in einer Sandbox** (und wird wirkungslos), oder ein Sicherheitssystem schlägt Alarm, bevor genug Schaden angerichtet wurde. In solchen Fällen hat der Angreifer nicht nur keinen Erlös, sondern ggf. sogar **seine Exploits „verbrannt“**, d.h. preisgegeben, welche Lücke er nutzte – was zukünftige Angriffe erschwert. Außerdem müssen Affiliates bedacht vorgehen, um **eigene Identitätsspuren zu verwischen** (VPN nutzen, Krypto-Mixer verwenden, keine persönlichen Accounts). Unerfahrene Täter machen hier Fehler: Beispielsweise wurde ein Affiliate gefasst, weil er Lösegeld über eine Kryptobörse mit schwacher Anonymität auszahlen wollte. **Jede Unachtsamkeit kann die gesamte Operation auffliegen lassen.**

Auch **Abhängigkeiten im Ökosystem** stellen ein Risiko dar. Wenn etwa der RaaS-Betreiber selbst von Ermittlern hochgenommen wird oder beschließt, spontan unterzutauchen, **steht der Affiliate plötzlich ohne Support da** – womöglich mitten in einer Erpressung. So ging es etwa Affiliates von REvil, als die Gruppe 2021 überraschend offline ging; einige saßen auf verschlüsselten Netzwerken fest, ohne Zugang zu Decryptor-Servern. Ähnlich gefährlich: **Lecks in der Untergrundszene.** 2022 wurde bspw. der Quellcode der Conti-Ransomware geleakt[20], inklusive interner Chat-Protokolle – die Auswertung solcher Daten durch Sicherheitsforscher oder Behörden kann ebenfalls Täteridentitäten enthüllen. Generell bewegen sich Affiliates in einem Feld, wo jederzeit **unvorhergesehene operative Probleme** auftreten können (sei es durch technische Bugs, interne Querelen in der Gang oder externe Eingriffe). Diese Unwägbarkeiten machen das „Geschäft“ riskant.

Zusammengefasst: Aus Sicht eines RaaS-Kunden winken zwar potenziell hohe Erlöse, doch erkauft mit erheblichen Risiken. Rechtlich drohen harte Strafen, finanziell kann ein Angriff auch Verlust bedeuten, und operativ erfordert das Unterfangen viel Disziplin, um nicht aufzufliegen oder vom eigenen Partner betrogen zu werden. **Viele Täter blenden diese Gefahren aus**, was sie letztlich anfälliger für Fehler macht – ein Umstand, den Strafverfolger zunehmend ausnutzen.

[20] industrialcyber.co

Die Realität ist: RaaS ist **kein „sicheres Geschäftsmodell“** – weder für die Opfer (deren Existenz auf dem Spiel steht) noch für die Täter selbst.

Fazit: Realistische Bedrohung – was Mittelständler jetzt tun sollten

Die Analyse von Ransomware-as-a-Service zeigt, dass **die Bedrohung für den deutschen Mittelstand real und akut ist.** RaaS hat das Feld der Cyber-Erpressung professionalisiert und skaliert: **Angriffe können jeden treffen**, auch Unternehmen ohne hohe Medienpräsenz oder Milliardenumsätze. Gleichzeitig haben die Täter-Communities gelernt, mit minimalem Aufwand maximalen Schaden anzurichten – eine gefährliche Kombination.

Für Geschäftsführer und Inhaber mittelständischer Firmen bedeutet dies vor allem: **Prävention und Vorbereitung** sind entscheidend. Aus der aktuellen Bedrohungslage lassen sich einige **Abwehrmaßnahmen** ableiten:

- **Security-Basics stärken:** Viele Angriffe gelingen, weil grundlegende Schutzmaßnahmen fehlen. **Patch-Management, starke Passwörter + Multi-Faktor-Authentifizierung und aktuelle Backups** sind essenziell. Gerade regelmäßige **Backups** haben sich als Lebensversicherung erwiesen – sie ermöglichen es, ein verschlüsseltes System ohne Lösegeld wiederherzustellen (was mit ein Grund für sinkende Zahlungsquoten ist). Allerdings müssen Backups **offline oder vor Löschung geschützt** aufbewahrt werden, sonst löschen Ransomware oder Angreifer sie mit.
- **Sensibilisierung und Training:** Der „Faktor Mensch“ bleibt kritisch. Mitarbeiter sollten über Phishing und Social Engineering Bescheid wissen, da dies häufig Einfallstore sind. Ein geschultes Team kann verdächtige E-Mails oder Zugriffsversuche erkennen und melden, bevor ein Schaden entsteht.
- **Netzwerkhärtung:** Da Access Broker oft über bekannte Schwachstellen eindringen, sollten Unternehmen **ihre exponierten Systeme absichern**. Das heißt: VPN, RDP-Server, E-Mail-Gateways etc. immer updaten, unnötige Dienste schließen, **Intrusion Detection/Prevention Systeme** einsetzen. Angreifer nutzen „Low-Hanging Fruits“ – je höher der Aufwand, desto eher ziehen sie weiter.
- **Zero-Trust-Prinzip verfolgen:** Interne Netzwerke segmentieren und **Mindestrechte** vergeben. So kann ein kompromittiertes Konto nicht gleich das ganze Netz verschlüsseln. Zudem verdächtige Aktivitäten (z. B. Massenverschlüsselung von Dateien) aufspüren und automatisch stoppen (Stichwort: **Endpoint Detection & Response**, das allerdings wiederum von Angreifern mit EDR-Killern bekämpft wird– ein Katz-und-Maus-Spiel, aber jede Hürde zählt).
- **Notfallplan und Übungen: Weniger als ein Drittel der Unternehmen in Deutschland haben einen schriftlichen Notfallplan für Cybervorfälle**– dieser Wert muss höher werden. Ein **Incident-Response-Plan** mit klaren Zuständigkeiten, Kommunikationswegen (inkl. Behörden) und Entscheidungsrichtlinien (z. B. ob zahlen oder nicht) ist unabdingbar. Dieser Plan sollte regelmäßig in **Simulationen** getestet werden, damit im Ernstfall jeder weiß, was zu tun ist. Auch der **Kontakt zu externen Experten** (BSI, CERT, Incident Response Dienstleister) sollte vorbereitet sein.

- **Transparenz und Melden:** Immer mehr Firmen gehen offen mit Cybervorfällen um. Das ist positiv, denn es erleichtert Hilfe von außen und warnt andere. Bei einem Ransomware-Angriff sollte **sofort das Landeskriminalamt/Zentralstelle Cybercrime** eingebunden werden. Auch wenn die Versuchung besteht, den Vorfall zu vertuschen – **Kooperation mit Behörden** kann helfen, Täter zu fassen und ggf. Entschlüsselungstools zu erhalten. Übrigens rät das **BSI grundsätzlich davon ab, Lösegeld zu zahlen**, da es keine Garantie für eine Entschlüsselung oder Nichtveröffentlichung der Daten gibt und jede Zahlung das Geschäftsmodell der Kriminellen weiter befeuert.

Abschließend lässt sich sagen: **Ransomware-as-a-Service hat die Bedrohungslage verändert.** Mittelständische Unternehmen müssen dieses Risiko ernst nehmen und sich genauso professionell aufstellen, wie die Angreifer es längst tun. Die gute Nachricht ist, dass **präventive Maßnahmen wirken** – sinkende Lösegeldzahlungen zeigen, dass Backups und Co. Angriffe ins Leere laufen lassen können[mittelstand-heute.com](mittelstand-heute.com). Doch die Angreifer passen sich an, wie die Zunahme von Datendiebstahl-Erpressungen zeigt.

Es gilt also, einen **ganzheitlichen Ansatz** zu verfolgen: technische Abwehr stärken, organisatorisch vorbereitet sein und im Ernstfall besonnen reagieren. So kann der deutschen Mittelstand der wachsenden RaaS-Bedrohung etwas entgegensetzen. Denn letztlich hat Cyber-Erpressung nur so lange Erfolg, wie wir als Gesellschaft – und jedes einzelne Unternehmen – **verwundbar und unvorbereitet** sind. Ein robust aufgestellter Mittelstand ist der beste Schutz gegen die „Dienstleistung“ RaaS, die dann hoffentlich bald an Rentabilität für Kriminelle verliert.