sure[secure]
your security operations center

secure mag

LÖSEGELD ZAHLEN?

Warum die naheliegendste Antwort fast immer die falsche ist.

Eine ehrliche Einschätzung für Unternehmen, die mitten in der Entscheidung stecken - von Menschen, die schon zu oft am anderen Ende der Lösegeldforderung saßen.

MONTAGMORGEN.
SCHWARZER BILDSCHIRM.
800.000 DOLLAR.

So fängt es bei den meisten an. Nicht mit einer Strategiesitzung, sondern mit einem Schock.

Sonne, guter Kaffee, ein Montag wie jeder andere. Dann der Laptop: schwarzer Bildschirm, eine Lösegeldforderung, ein Countdown... 72 Stunden, sonst werden die Daten veröffentlicht. Genau in diesem Moment beginnt eine der teuersten und unangenehmsten Entscheidungen, die ein Unternehmen treffen kann: zahlen oder nicht zahlen?

Dieser Ratgeber gibt dir keine Schritt-für-Schritt-Checkliste für den Krisenfall im luftleeren Raum, sondern die Einschätzung von jemandem, der diese Entscheidung schon zu oft begleitet hat: Andreas Papadaniil, CEO und Incident Responder, suresecure.

DREI WEGE
AUS DER VERSCHLÜSSELUNG

Bevor es um die Details geht, zunächst die Landkarte: Sind die Systeme verschlüsselt, gibt es im Kern drei Handlungswege. Jeder hat eine andere Erfolgsquote, ein anderes Zeitfenster und ein anderes Risiko, welches damit verbunden ist.

1. **Recovery aus dem Backup**
   Du verzichtest auf jeden Kontakt mit den Angreifern und baust aus eigener Kraft wieder auf. Langsamer, aber sauber.
2. **Verhandeln, ohne sofort zu zahlen**
   Ein professioneller Negotiator nimmt Kontakt zu den Angreifern auf, um Zeit zu gewinnen und die Lage einzuschätzen.
3. **Lösegeld zahlen**
   Die teuerste Entscheidung und laut Datenlage die mit der geringsten Erfolgsquote. Trotzdem manchmal der einzige Weg.

Diese drei Handlungswege sind nicht immer als Entweder-oder zu verstehen. In der Praxis werden zunächst die Möglichkeiten einer Recovery geprüft, während parallel dazu eine Verhandlung Zeit verschaffen kann. Eine Lösegeldzahlung bleibt – wenn überhaupt – der letzte Ausweg, wenn alle anderen Optionen ausgeschöpft sind.

1. RECOVERY
AUS DEM BACKUP

Der Standardweg und in der überwiegenden Mehrheit der Fälle auch der richtige: Systeme aus dem Backup wiederherstellen, ohne überhaupt mit den Angreifern in Verhandlung zu treten. Selbst ein einen Monat altes Backup hat in der Praxis bereits ausgereicht, um ein Unternehmen über Wasser zu halten.

Es gibt jedoch genau ein Szenario, in dem Andreas Papadaniil von diesem Vorgehen abrät und stattdessen zu einer direkten Lösegeldzahlung rät:

„Wenn du tatsächlich null Backups hast, weder Cloud, noch lokal, noch Tape, und ohne Wiederherstellung Insolvenz anmelden musst, dann zahl lieber und versuch's, bevor du komplett tot bist."

- Andreas Papadaniil

In jedem anderen Fall gilt: Zuerst die Recovery prüfen, auch wenn es schmerzt. Die unbequeme Wahrheit ist jedoch: Diese Entscheidung wird nicht erst am Montagmorgen vor einem schwarzen Bildschirm getroffen. Sie muss Monate vorher getroffen werden.

2. VERHANDELN, OHNE SOFORT ZU ZAHLEN

Unabhängig davon, ob am Ende gezahlt wird, erfolgt der Kontakt zu den Angreifern in den meisten professionell begleiteten Fällen über einen erfahrenen Verhandlungsführer. Diese sogenannten Ransomware Negotiators kontaktieren die Angreifergruppe. Die Höhe der Lösegeldforderung ist dabei jedoch selten das einzige Thema.

Die Verhandlung erfüllt gleich mehrere Funktionen:

1. **Zeit gewinnen:**
   Während verhandelt wird, kann das interne Team parallel die Lage analysieren und an der Wiederherstellung arbeiten.
2. **Informationen sammeln:**
   Über die Angreifergruppe, ihre Taktiken und wie ernst die Drohung tatsächlich ist.
3. **Den Preis drücken, falls es doch zur Zahlung kommt:**
   Laut Marktbeobachtungen lässt sich die ursprüngliche Forderung im Schnitt um rund 47–52% reduzieren.
4. **Beweise verlangen:**
   Ob die Angreifer überhaupt entschlüsseln können, sollte vor jeder Zahlung über Testdateien geprüft werden.

Wichtig: Ein Broker verhandelt nicht anstelle der Geschäftsleitung. Die letzte Entscheidung über Zahlung oder Nichtzahlung bleibt immer beim Unternehmen. Der Broker liefert die Faktenbasis und die professionelle Distanz, die in dieser Situation oftmals fehlt, wenn das eigene Team unter Schock selbst verhandelt. Emotionen haben in dieser Art der Verhandlung nichts zu suchen, denn wer in Panik verhandelt, verhandelt häufig schlechter.

Und ja, dieser Markt hat auch seine Schattenseiten: In einem bekannt gewordenen US-Fall soll ein Verhandlungsführer über Monate Insiderinformationen an eine Angreifergruppe weitergegeben haben, um die Lösegeldforderung künstlich in die Höhe zu treiben. Genau deshalb gilt: Ein Broker sollte sorgfältig ausgewählt werden, idealerweise schon im Voraus und nicht erst in der Notsituation.

3. ZAHLEN, TEUER UND OHNE GARANTIE

Der oftmals teuerste und unsicherste der drei Handlungswege und genau deshalb der, der am meisten Aufklärung erfordert. Die meisten Ransomware-Angriffe laufen heute zweigleisig: Daten werden verschlüsselt und gleichzeitig gestohlen. Daraus ergeben sich zwei getrennte Forderungen, die häufig als eine verkauft werden:

- **Zahlung 1:**
  Entschlüsselung. Angeblich bekommst du deine Systeme zurück.
- **Zahlung 2:**
  Schweigegeld. Angeblich veröffentlichen die Angreifer die gestohlenen Daten nicht.

Beides hält nur selten, was es verspricht. Genau deshalb lohnt sich der Blick auf beide Versprechen getrennt.

PODCAST

CYBER SECURITY Basement

In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.

Jetzt reinhören

Spotify

Apple Podcast

YouTube Music

amazon music

und noch mehr...

VERSPRECHEN 1

„WIR GEBEN DIR DEN SCHLÜSSEL“

Selbst wenn der Schlüssel kommt und funktioniert, ist das nicht der Moment, in dem alles wieder läuft. Die Entschlüsselung ist ein langer und fehleranfälliger Prozess: Datenbanken, die mitten im Schreibvorgang verschlüsselt wurden, sind danach oft inkonsistent. Anwendungsserver müssen neu verbunden werden.

Genau das hat Andreas Papadaniil selbst erlebt:

Es handelte sich um einen klassischen Ransomware-Vorfall. Da bei dem Unternehmen wichtige Auslieferungen unmittelbar bevorstanden, war der Druck besonders hoch und die Situation entsprechend kritisch. Das Unternehmen entschied sich deshalb für die Zahlung und erhielt sogar umgehend einen funktionierenden Schlüssel. Trotzdem dauerte der Wiederaufbau so lange, dass am Ende dennoch aus den Backups wiederhergestellt werden musste. Bezahlt, der Schlüssel funktionierte und trotzdem wochenlang offline.

Der Recovery-Aufwand bleibt also bestehen, unabhängig davon, ob gezahlt wird oder nicht. Genau das wird häufig unterschätzt.

VERSPRECHEN 2

„WIR VERÖFFENTLICHEN DIE DATEN NICHT“

Hier wird es zynisch: Man verhandelt mit Kriminellen, die bereits gegen jedes Gesetz verstoßen haben, über deren Ehrenwort. Selbst wenn die Daten von einer Leak-Seite verschwinden, sind sie oftmals längst kopiert, vervielfältigt und im Umlauf. Realistisch ist: Die Daten werden häufig weiter monetarisiert, nur leiser – etwa über Darknet-Auktionen oder gezielte Angebote an Wettbewerber oder andere Ransomware-Gruppen. Zurückverfolgen lassen sich diese Transaktionen in der Regel nicht.

Erschwerend kommt hinzu, dass zu Beginn eines Incidents niemand zuverlässig weiß, welche Daten tatsächlich abgeflossen sind. Forensisch lässt sich ein Datenabfluss oft nicht eindeutig nachweisen, weil Spuren unvollständig sind, Logs fehlen und Angreifer ihre Bewegungen im Netzwerk gezielt verschleiern. Genau diese Unsicherheit treibt Unternehmen zu Kurzschlussreaktionen: Lieber zahlen, „damit die Daten wenigstens aus dem Darknet verschwinden.“ Oftmals eine Hoffnung, die sich in der Realität nicht erfüllt.

4 %

der zahlenden Organisationen erhalten ihre Daten laut Sophos State of Ransomware 2025 vollständig und unbeschädigt zurück.

8 %

vollständige Datenrückgabe weist der Underground Report 2025 aus. Beide Studien zeigen: “Zahlung = Lösung” ist eine Illusion.

DIE RECHTLICHE SEITE:

ZAHLEN IST NICHT VERBOTEN, ABER AUCH NICHT RISIKOFREI

Ein Gesetz, das eine Lösegeldzahlung pauschal verbietet, gibt es in Deutschland nicht. Wer erpresst wird, macht sich nicht automatisch strafbar, weil er der Forderung nachgibt. Dennoch sollte immer auch eine juristische Einschätzung Bestandteil des Prozesses sein.

Denn das relevante Risiko heißt § 129 StGB: Unterstützung einer kriminellen Vereinigung. Die meisten Ransomware-Gruppen erfüllen die rechtliche Definition einer solchen Vereinigung. Wer zahlt, stellt dieser Vereinigung finanzielle Mittel zur Verfügung und genau das kann als strafbare Unterstützungshandlung gewertet werden. Entscheidend ist dabei nicht die Absicht, Kriminelle zu fördern, sondern, ob die Geschäftsleitung es zumindest für möglich hält und in Kauf nimmt, dass genau das passiert. Bei der aktuellen Bedrohungslage lässt sich dieses Wissen kaum noch wegargumentieren.

Hinzu kommen drei weitere, seltenere Risiken: Verstöße gegen Sanktionsrecht, wenn unwissentlich an eine sanktionierte Gruppe gezahlt wird (relevant z. B. über das AWG oder US-Sanktionslisten der OFAC), Terrorismusfinanzierung nach § 89c StGB sowie Geldwäsche nach § 261 StGB. In der Praxis bleiben diese drei meist theoretisch, weil dem zahlenden Unternehmen das nötige Wissen über die Verwendung des Geldes fehlt.

Bislang ist jedenfalls kein Fall bekannt, in dem ein zahlendes Unternehmen in Deutschland tatsächlich aufgrund der Zahlung angeklagt wurde. Staatsanwaltschaften ermitteln aktuell in der Regel nicht aktiv gegen die Opfer, sondern gegen die Täter. Ein Restrisiko bleibt trotzdem, gerade bei sehr hohen Summen, die die kriminelle Struktur besonders stark fördern.

Was das für dich heißt: Eine Lösegeldentscheidung ist nie nur eine IT- oder Finanzentscheidung, sie ist auch eine juristische.

Vor jeder Zahlung gehört zwingend:

1. Anwalt mit Erfahrung im Cyberstrafrecht ins Boot holen.
2. Anzeige bei der Polizei: vom BSI ausdrücklich empfohlen und Teil einer rechtssicheren Vorgehensweise.
3. Abgleich der Empfängerstruktur mit Sanktionslisten.

Diese Schritte schützen dich nicht vor jedem Risiko, aber sie sind der Unterschied zwischen einer dokumentierten Abwägung unter Zeitdruck und einer Eigenmächtigkeit, die später schwer zu rechtfertigen ist.

DIE CYBERVERSICHERUNG:

FLUCH ODER SEGEN?

Viele Policen decken Lösegeldzahlungen mit ab. Das klingt nach Sicherheit, hat aber zwei Haken.

Erstens: Eine Deckungszusage verschiebt die Entscheidung in Richtung „zahlen“, weil sich Verhandeln finanziell einfacher anfühlt, obwohl die Erfolgsquote dieselbe bleibt.

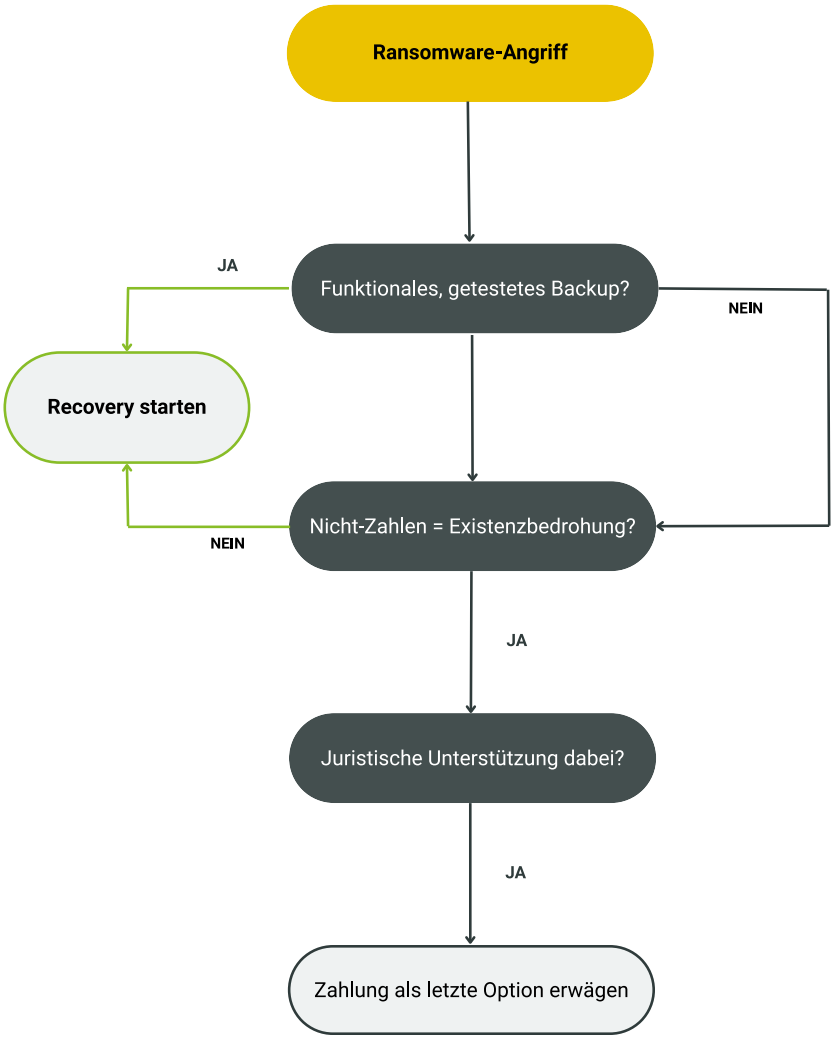
Zweitens: Wenn Angreifergruppen wissen, dass ein Unternehmen versichert ist, macht das dieses Unternehmen tendenziell zu einem attraktiveren Ziel, da die Wahrscheinlichkeit einer Zahlung aus Sicht der Angreifer steigt.

Eine Lösegeld-Deckung ist kein Freifahrtschein. Sie ist ein Werkzeug für den absoluten Notfall, sollte aber nie der bevorzugte Weg sein.

DER ENTSCHEIDUNGSBAUM:

IN DREI FRAGEN ZUR ANTWORT

Wer mitten in der Krise steckt, hat keine Zeit für lange Abwägungen. Deshalb hier die Essenz der drei vorherigen Fragen als Entscheidungsbaum zum Ausdrucken, Aufhängen und hoffentlich nie im Ernstfall benötigen.



In den allermeisten Fällen führt dieser Baum zu: nicht zahlen, Recovery starten.

FAZIT:

ZAHLEN IST EINE WETTE.

Die ehrliche Bilanz aus der Praxis: In fast allen Fällen lautet die Empfehlung, nicht zu zahlen, sondern die Recovery anzustoßen, auch wenn das schmerzhaft und teuer ist. Eine Zahlung ist nur dann eine nachvollziehbare Entscheidung, wenn ohne Wiederherstellung die Existenz des Unternehmens auf dem Spiel steht. In allen anderen Fällen finanziert sie lediglich ein Geschäftsmodell, das sich am nächsten Tag das nächste Opfer sucht.

Diese Erkenntnis setzt sich offenbar durch: Laut BSI liegt die Zahlungsquote in Deutschland inzwischen bei rund 7 %, was auf einen klaren Lernprozess hindeutet. Natürlich gibt es auch hier eine nicht unerhebliche Dunkelziffer. Dennoch bleibt das Geschäftsmodell lukrativ genug, dass Angreifergruppen ihre Strukturen weiter ausbauen, befeuert auch durch neue Werkzeuge wie KI. Das Geschäft ist nicht am Ende. Es erfindet sich immer wieder neu.

Die eigentliche Entscheidung fällt also nicht erst am Montagmorgen vor einem schwarzen Bildschirm. Sie fällt heute – mit der Frage, wie belastbar das Backup-Konzept, der Incident-Response-Plan und die Kommunikationsstrategie tatsächlich sind.

Steh nicht erst am Montagmorgen vor dieser Entscheidung. Wir begleiten Unternehmen, bevor der Bildschirm schwarz wird: mit Incident-Response-Vorbereitung, belastbaren Backup- und Recovery-Konzepten und einer Kommunikationsstrategie, die im Ernstfall trägt. Lass uns reden, solange noch Zeit dafür ist.

CISO
TAKEAWAYS

- Eine Lösegeldzahlung bleibt der letzte Ausweg.
- Getestete Backups sind wichtiger als funktionierende Entschlüsselung.
- Verhandlungen dienen der Entscheidungsfindung, nicht der Problemlösung.
- Die wichtigste Entscheidung fällt vor dem Angriff.
- Cyber-Resilienz reduziert die Abhängigkeit von den Angreifern.

SCHLUSSWORT:

Ransomware ist längst kein Ausnahmefall mehr. Die Frage ist nicht, ob Unternehmen mit dieser Bedrohung konfrontiert werden können, sondern wie gut sie darauf vorbereitet sind.

Wer erst im Ernstfall darüber nachdenkt, ob gezahlt werden soll, hat die wichtigste Entscheidung bereits zu spät getroffen. Belastbare Backups, klare Verantwortlichkeiten, geübte Abläufe und eine realistische Vorbereitung schaffen den Handlungsspielraum, den es in einer Krise braucht.

Denn am Ende entscheidet nicht die Höhe der Lösegeldforderung über den Ausgang eines Angriffs, sondern die Qualität der Vorbereitung.

Weitere Informationen zum Thema:

Podcast-Folge:

Ransomware ist ein professionelles Geschäftsmodell. Ransomware as a Service senkt die Einstiegshürden für Cyberkriminelle und sorgt dafür, dass Angriffe effizienter, skalierbarer und erfolgreicher werden.

Quellen

1. Sophos, State of Ransomware 2025
2. Underground Report 2025
3. BSI - Bundesamt für Sicherheit in der Informationstechnik, Lagebericht zur IT-Sicherheit
4. Coveware, Quarterly Ransomware Report Q4 2025
5. CIO.de / GTK Rechtsanwälte / Kanzlei Tsambikakis - Einordnung der Strafbarkeitsrisiken bei Lösegeldzahlungen (§ 129 StGB, § 34 StGB)
6. SRF, Ransomware-Negotiator: der mit den Cyberkriminellen feilscht
7. Computerwoche, Ransomware-Strategien: Wie Sie mit Cybererpressern verhandeln

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de