■ VERHANDLUNG.JETZT · LEITFADEN

Lösegeldforderung nach einem Ransomware-Angriff

Leitfaden für die Geschäftsführung

Was vor der Entscheidung geklärt sein muss, welchen rechtlichen Rahmen Sie kennen sollten und was eine Verhandlung leisten kann.

Stand November 2026

Worum es geht

Eine Lösegeldforderung ist keine IT-Frage. Sie stellt die Geschäftsführung vor eine Entscheidung, die in kurzer Zeit, unter Druck und mit unvollständiger Information fallen muss und die das Unternehmen unter Umständen lange begleitet. Ob verhandelt wird, ob gezahlt wird und wie diese Entscheidung dokumentiert wird, liegt in der Verantwortung der Leitungsorgane.

Dieser Leitfaden beantwortet nicht die Frage, ob Sie zahlen sollen. Die Antwort hängt von Umständen ab, die sich von Fall zu Fall unterscheiden. Er zeigt, welche Fragen vor einer Entscheidung geklärt sein müssen, welchen rechtlichen Rahmen Sie kennen sollten, was eine Verhandlung leisten kann und was Sie heute vorbereiten können, damit die Entscheidung im Ernstfall auf einer belastbaren Grundlage steht.

Er richtet sich an Geschäftsführung, Vorstand und Aufsichtsorgane von Unternehmen in Österreich und ersetzt keine Rechtsberatung im Einzelfall.

Die Ausgangslage im Ernstfall

Wenn eine Erpressernachricht auftaucht, hat der Angriff meist längst stattgefunden. Die Angreifer waren über Tage oder Wochen im Netzwerk, haben Zugänge gesammelt, Sicherungen gesucht und in vielen Fällen Daten kopiert, bevor sie die Verschlüsselung gestartet haben. Die Forderung setzt deshalb häufig an zwei Stellen zugleich an, an der Wiederherstellung der verschlüsselten Systeme und an der Drohung, die gestohlenen Daten zu veröffentlichen.

Die Nachricht enthält in der Regel einen Verweis auf ein Portal im Tor-Netzwerk, oft mit einer Frist und der Ankündigung, dass sich die Forderung nach Ablauf erhöht oder die Daten veröffentlicht werden. Dieser Zeitdruck ist Teil der Methode. Er soll verhindern, dass sich das Unternehmen ein Lagebild verschaffen kann, bevor es reagieren muss.

Für die Geschäftsführung heißt das, die ersten Stunden nicht mit der Frage nach der Zahlung zu verbringen. Die erste Frage lautet, was das Unternehmen zu diesem Zeitpunkt weiß und was es noch herausfinden muss.

Grundregeln für die ersten Stunden

Nehmen Sie keinen Kontakt zu den Angreifern auf, bevor die Geschäftsführung entschieden hat, wer das tut und mit welchem Ziel. Die erste Nachricht an einen Threat Actor prägt den gesamten weiteren Verlauf. Wer unter Druck Informationen über die eigene Zahlungsfähigkeit, eine bestehende Cyberversicherung oder den Zustand der Backups preisgibt, verschlechtert seine Position dauerhaft. Das gilt auch für Mitarbeiter, die aus Neugier oder Pflichtgefühl das Portal öffnen.

Sichern Sie die Erpressernachricht als Foto oder Screenshot und halten Sie fest, wo und wann sie gefunden wurde. Öffnen Sie die darin enthaltenen Links nicht von Systemen des Unternehmens aus.

Informieren Sie Ihre Cyberversicherung, falls Sie eine besitzen, bevor Sie externe Dienstleister beauftragen. Viele Polizzen knüpfen die Kostenübernahme an eine Abstimmung mit dem Versicherer und sehen eigene Notfallnummern vor. Manche Versicherer machen Vorgaben zu Verhandlung und Zahlung, die Sie kennen sollten, bevor Sie sich festlegen. Gute Cyberversicherungen bieten Ihnen die freie Wahl des IT-Forensikers, wollen aber über alle wesentlichen Schritte informiert werden.

Erstatten Sie Anzeige bei der Polizei. Das Bundeskriminalamt empfiehlt Betroffenen ausdrücklich, Anzeige zu erstatten. Die Anzeige hat zudem Bedeutung für die Versicherung und für spätere Verfahren.

Aus unserer Erfahrung wirkt die Polizei an der unmittelbaren Bewältigung des Vorfalls nur in besonderen Fällen mit. Die Anzeige ersetzt deshalb weder Incident Response noch Verhandlungsführung.

Beginnen Sie sofort ein Entscheidungsprotokoll. Halten Sie fest, wer wann welche Information erhalten und welche Entscheidung getroffen hat. Dieses Protokoll ist später Ihre wichtigste Grundlage gegenüber Gesellschaftern, Versicherung, Behörden und gegebenenfalls Gerichten.

Die Entscheidung liegt bei der Geschäftsführung

Die Entscheidung über Verhandlung und Zahlung ist eine unternehmerische Entscheidung. Für die GmbH hält § 25 Abs 1a GmbHG fest, dass ein Geschäftsführer jedenfalls im Einklang mit der Sorgfalt eines ordentlichen Geschäftsmannes handelt, wenn er sich bei einer unternehmerischen Entscheidung nicht von sachfremden Interessen leiten lässt und auf der Grundlage angemessener Information annehmen darf, zum Wohle der Gesellschaft zu handeln. Für den Vorstand einer Aktiengesellschaft enthält § 84 Abs 1a AktG eine entsprechende Regelung.

Für die Lösegeldfrage folgt daraus vor allem eine Pflicht zur Information und zur Dokumentation. Die Geschäftsführung sollte belegen können, dass sie die wesentlichen Grundlagen erhoben hat, also den Zustand der Sicherungen, die voraussichtliche Dauer der Betriebsunterbrechung, den möglichen Datenabfluss, den rechtlichen Rahmen und die Haltung der Versicherung, und dass sie Alternativen abgewogen hat. Ob sich die Entscheidung im Nachhinein als richtig erweist, ist dafür nicht allein maßgeblich, es kommt darauf an, ob sie auf einer angemessenen Grundlage getroffen wurde.

Treffen Sie die Entscheidung deshalb als Gremium und halten Sie sie in einem Beschluss fest, der die Entscheidungsgrundlagen, die erwogenen Alternativen und die Begründung enthält. Binden Sie Aufsichtsrat oder Gesellschafter nach den Regeln Ihres Gesellschaftsvertrages und Ihrer Geschäftsordnung ein. Klären Sie mit Ihrer Rechtsberatung, ob eine Zahlung danach zustimmungspflichtig ist.

Fünf Fragen vor jeder Zahlungsentscheidung

Können wir ohne Zahlung wiederherstellen?

Die wichtigste Frage betrifft die Sicherungen. Gibt es Backups, die der Angreifer nicht erreicht hat? Wann wurden sie zuletzt erstellt, und wurde ihre Wiederherstellung jemals unter realistischen Bedingungen getestet? Wie lange dauert ein vollständiger Wiederaufbau, und in welcher Reihenfolge müssen Systeme zurückkommen, damit das Unternehmen wieder arbeitsfähig ist? Für aussagekräftige Antworten braucht die IT in der Regel einige Stunden Prüfung. Diese Zeit sollte sich die Geschäftsführung nehmen.

Auch eine Zahlung garantiert keinen schnellen Wiederanlauf. Entschlüsselungswerkzeuge der Angreifer arbeiten häufig langsam und nicht immer fehlerfrei. Kompromittierte Systeme müssen in jedem Fall bereinigt oder neu aufgebaut werden.

Was kostet der Stillstand?

Stellen Sie die Kosten der Betriebsunterbrechung realistisch dar. Dazu gehören entgangene Umsätze, Vertragsstrafen, Lieferverzug, Mehrkosten für manuelle Ersatzprozesse und die Folgen für Kunden, die auf Ihre Leistung angewiesen sind. Ebenso gehören die Kosten der Wiederherstellung dazu, die unabhängig von einer Zahlung anfallen. Erst diese Gesamtrechnung macht eine Abwägung möglich.

Welche Daten wurden abgezogen, und was bedeutet ihre Veröffentlichung?

Viele Angreifer drohen mit der Veröffentlichung gestohlener Daten auf einer Leakseite. Ob und welche Daten tatsächlich abgeflossen sind, lässt sich häufig erst durch eine forensische Analyse klären. Einen ersten Anhaltspunkt liefert oft ein Filetree, den die Angreifer als Nachweis bereitstellen. Die Angaben der Angreifer sind ein Hinweis, aber kein Beweis. Threat Actors bleiben Kriminelle, und das darf man zu keinem Zeitpunkt außer Acht lassen.
Bewerten Sie, welche Folgen eine Veröffentlichung hätte, für betroffene Personen, für Geschäftspartner, für Geheimhaltungsverpflichtungen und für die Reputation des Unternehmens.

Eine Zahlung beseitigt die gesetzlichen Pflichten nicht. Sind personenbezogene Daten betroffen, sind die Meldung an die Datenschutzbehörde nach Art. 33 DSGVO und gegebenenfalls die Benachrichtigung der Betroffenen nach Art. 34 DSGVO zu prüfen, ob gezahlt wird oder nicht. Die Aussage der Angreifer, Daten zu löschen, lässt sich nicht überprüfen.

Darf an diesen Empfänger gezahlt werden?

Vor jeder Zahlung ist zu prüfen, ob der Empfänger Sanktionen unterliegt. Die Europäische Union hat mit der Verordnung (EU) 2019/796 ein eigenes Sanktionsregime gegen Cyberangriffe geschaffen. Gelisteten Personen und Organisationen dürfen weder direkt noch indirekt Gelder zur Verfügung gestellt

werden. Daneben können weitere Sanktionsregimes greifen. Verstöße gegen unionsrechtliche Sanktionen sind in Österreich nach dem Sanktionengesetz 2010 strafbar.

In der Praxis liegt die Schwierigkeit darin, dass der Empfänger einer Lösegeldzahlung meist nur als Wallet-Adresse und unter einem Gruppennamen auftritt. Wer tatsächlich hinter einer Forderung steht, lässt sich oft nicht feststellen. Die Sanktionsprüfung muss deshalb dokumentieren, welche Informationen vorlagen, welche Prüfungen durchgeführt wurden und wo ihre Grenzen lagen.

Zusätzlich sollten die US-Sanktionslisten abgefragt und berücksichtigt werden.

Was sagt die Versicherung?

Klären Sie, ob und unter welchen Bedingungen Ihre Cyberversicherung Lösegeldzahlungen, Verhandlungskosten und die Kosten der Wiederherstellung übernimmt. Viele Polizzen enthalten dazu eigene Regelungen, manche Versicherer verlangen eine vorherige Zustimmung oder die Einbindung bestimmter Dienstleister. Eine Zahlung ohne Abstimmung kann den Versicherungsschutz gefährden.

Was eine Verhandlung leisten kann

Verhandeln heißt nicht zahlen. Eine professionell geführte Verhandlung kann auch dann sinnvoll sein, wenn das Unternehmen eine Zahlung für unwahrscheinlich hält.

Eine Verhandlung verschafft Zeit. Jeder Tag, an dem die Angreifer auf eine Antwort warten, ist ein Tag für die forensische Analyse, für den Wiederaufbau und für die Vorbereitung der Kommunikation. Sie verschafft Information. Im Verlauf lässt sich klären, welche Daten die Angreifer tatsächlich besitzen und ob sie Dateien überhaupt entschlüsseln können. Und sie schafft eine Entscheidungsgrundlage, weil die Geschäftsführung am Ende nicht über eine Drohung entscheidet, sondern über ein geprüftes Angebot.

Die Verhandlung gehört nicht in die Hände der IT-Leitung, der Geschäftsführung selbst oder von Mitarbeitern, die persönlich betroffen sind. Sie verlangt Erfahrung mit den Abläufen und Gepflogenheiten solcher Gruppen, eine enge Abstimmung mit dem Krisenstab und die lückenlose Dokumentation jeder Nachricht. Die Verhandlungsführung handelt im Auftrag und nach den Vorgaben der Geschäftsführung. Über die Zahlung entscheidet sie nicht.

Der rechtliche Rahmen in Österreich

Eine ausdrückliche gesetzliche Bestimmung, die betroffenen Unternehmen die Zahlung eines Lösegelds allgemein verbietet, ist uns nicht bekannt. Daraus folgt nicht, dass jede Zahlung rechtlich unbedenklich ist. Die Grenzen ergeben sich aus anderen Regelungen.

Im Vordergrund steht das Sanktionsrecht, das im vorigen Abschnitt beschrieben ist. Strafrechtliche Risiken können sich zudem ergeben, wenn Gelder an terroristische Vereinigungen fließen, etwa unter dem Gesichtspunkt der Terrorismusfinanzierung nach § 278d StGB. Ob eine solche Konstellation vorliegt, ist bei Ransomware schwer zu beurteilen. In die Prüfung gehört sie trotzdem.

Für Unternehmen mit Bezug zu den Vereinigten Staaten, etwa über Konzerngesellschaften, Kunden, Versicherer oder Zahlungsdienstleister, ist zusätzlich das US-Sanktionsrecht von Bedeutung. Das Office of Foreign Assets Control (OFAC) des US-Finanzministeriums hat im September 2021 ein aktualisiertes Advisory zu Sanktionsrisiken bei Lösegeldzahlungen veröffentlicht. Es rät nachdrücklich von Zahlungen ab und hält fest, dass Sanktionsverstöße auch ohne Kenntnis der Sanktionierung verfolgt werden können. Als mildernd berücksichtigt OFAC die frühzeitige Meldung an Behörden und die Zusammenarbeit mit ihnen. Versicherer und Zahlungsdienstleister können diese Maßstäbe auch bei Fällen außerhalb der Vereinigten Staaten anlegen.

Eine Zahlung in Kryptowährung läuft in der Praxis über regulierte Dienstleister. Zwischen diesen Dienstleistern gibt es große Unterschiede. Die Computerforensic & more GmbH bietet Lösegeldzahlungen gemeinsam mit ihrem Kooperationspartner transparent an.

Die Meldepflichten bestehen unabhängig von der Frage der Zahlung. Neben der Meldung an die Datenschutzbehörde nach Art. 33 DSGVO, möglichst binnen 72 Stunden nach Bekanntwerden, haben wesentliche und wichtige Einrichtungen bei einem erheblichen Cybersicherheitsvorfall nach § 34 NISG 2026 binnen 24 Stunden eine Frühwarnung an das zuständige sektorspezifische CSIRT abzugeben, binnen 72 Stunden eine Meldung und spätestens einen Monat danach einen Abschlussbericht. Das CSIRT leitet die Meldung an die Behörde weiter.

Wenn die Geschäftsführung eine Zahlung erwägt

Fällt die Entscheidung für eine Zahlung, sollten einige Voraussetzungen erfüllt und dokumentiert sein. Die Sanktionsprüfung ist abgeschlossen und schriftlich festgehalten. Die Versicherung hat zugestimmt oder ist zumindest nachweislich informiert. Die Fähigkeit der Angreifer zur Entschlüsselung wurde vorab an einzelnen Dateien ohne sensible Inhalte geprüft. Die Bedingungen der Zahlung sind in der Verhandlung klar umrissen. Und es liegt ein Beschluss der Geschäftsführung vor, der Betrag, Empfänger, Begründung und Zahlungsweg nennt.

Die Zahlung selbst kann entweder durch das Unternehmen selbst oder durch einen Dienstleister erfolgen. Mit einer Zahlung ist der Cybervorfall nicht abgeschlossen. Erfahrungsgemäß befinden wir uns zwischen 55% und 65% bis zur Herstellung eines Normalbetriebs.

Auch nach einer Zahlung bleiben Bereinigung und sicherer Wiederaufbau der Systeme notwendig. Ein Entschlüsselungswerkzeug der Angreifer gehört vor dem Einsatz geprüft, weil es selbst Schadfunktionen enthalten kann.

Erfahrungsgemäß greift dieselbe Gruppe nicht erneut an, weil nach einer Wiederherstellung im Regelfall wesentliche IT-Security-Maßnahmen umgesetzt werden und das ursprüngliche Einfallstor damit geschlossen ist. Eine Garantie ist das nicht, denn nach einer Zahlung gilt das Unternehmen als zahlungsbereit.

Wenn die Geschäftsführung nicht zahlt

Die Entscheidung gegen eine Zahlung verlangt ebenso viel Vorbereitung. Planen Sie den Wiederaufbau aus den vorhandenen Sicherungen und priorisieren Sie die Systeme, ohne die der Betrieb nicht läuft. Bereiten Sie sich auf eine Veröffentlichung der Daten vor. Dazu gehören die Information der betroffenen Personen, die Abstimmung mit Geschäftspartnern, eine vorbereitete Stellungnahme für Medien und Belegschaft und die Beobachtung der Leakseite.

Halten Sie fest, dass und warum Sie nicht gezahlt haben. Auch diese Entscheidung kann später überprüft werden, etwa wenn eine Veröffentlichung Schäden bei Dritten verursacht.

Eine laufende Verhandlung muss nicht abrupt enden. Ob und wie die Kommunikation mit den Angreifern beendet wird, entscheiden Sie gemeinsam mit der Verhandlungsführung.

Ein Musterfall

Der folgende Fall ist konstruiert. Er beruht auf keinem konkreten Mandat und dient nur dazu, die Entscheidungspunkte zu veranschaulichen.

An einem Freitagabend stellt die IT-Leitung eines Maschinenbauunternehmens fest, dass Server und Arbeitsplätze verschlüsselt sind. Auf jedem System liegt eine Textdatei mit dem Link zu einem Portal und einer Frist von fünf Tagen. Ein Mitarbeiter hat das Portal bereits geöffnet und dort gelesen, dass die Angreifer über Konstruktionsdaten und Personalakten verfügen.

Die Geschäftsführung stimmt sich noch am selben Abend über private Telefone ab. Sie untersagt jede weitere Kommunikation mit dem Portal, informiert die Cyberversicherung und erstattet Anzeige. Die IT-Leitung meldet, dass die Sicherungen auf einem getrennten System liegen und unverschlüsselt scheinen, ihre Vollständigkeit aber erst geprüft werden muss.

Am Samstag zeigt sich, dass die Sicherungen bis auf die Daten der letzten drei Tage vollständig sind. Die IT-Forensik findet Hinweise auf einen größeren Datentransfer, kann seinen Umfang aber noch nicht bestimmen. Die Versicherung stimmt der Einbindung einer Verhandlungsführung zu. Diese nimmt Kontakt auf, verlangt den Nachweis der Entschlüsselung an zwei unkritischen Dateien und eine Liste der angeblich gestohlenen Daten.

Am Dienstag liegt der Geschäftsführung ein Lagebild vor. Die Produktion kann aus den Sicherungen innerhalb von zehn Tagen schrittweise wieder anlaufen. Die Angreifer besitzen nachweislich einen Teil der Konstruktionsdaten und der Personaldaten. Die Sanktionsprüfung ergibt keinen Treffer, ihre Aussagekraft ist aber begrenzt, weil über die Gruppe wenig bekannt ist.

Nun muss die Geschäftsführung abwägen. Die Wiederherstellung ist ohne Zahlung möglich. Der Datenabfluss lässt sich auch durch eine Zahlung nicht rückgängig machen, und die Löschzusage ist nicht überprüfbar. Auf der anderen Seite stehen die Folgen einer Veröffentlichung für Mitarbeiter und Kunden. Wie die Geschäftsführung entscheidet, lässt der Fall bewusst offen. Wesentlich ist, dass sie auf dieser Grundlage entscheidet, begründet und dokumentiert.

Was Sie heute vorbereiten können

Die meisten Fehler in der Lösegeldfrage entstehen nicht in der Entscheidung selbst, sondern durch fehlende Vorbereitung. Diese Punkte lassen sich mit überschaubarem Aufwand klären.

1. *Legen Sie fest, wer im Ernstfall über Verhandlung und Zahlung entscheidet, wer vertritt und wie das Gremium außerhalb der Geschäftszeiten erreichbar ist.*
2. *Klären Sie, ob eine Zahlung nach Gesellschaftsvertrag oder Geschäftsordnung die Zustimmung von Aufsichtsrat oder Gesellschaftern erfordert.*
3. *Lesen Sie die Bedingungen Ihrer Cyberversicherung zu Lösegeld, Verhandlungskosten, Zustimmungspflichten und vorgegebenen Dienstleistern und legen Sie die Notfallnummer griffbereit ab.*
4. *Halten Sie Kontaktdaten für Incident Response, Verhandlungsführung, Rechtsberatung und Krisenkommunikation offline bereit.*
5. *Bereiten Sie Vorlagen für das Entscheidungsprotokoll und den Beschluss vor.*
6. *Lassen Sie die Wiederherstellung Ihrer Sicherungen unter realistischen Bedingungen testen und halten Sie die Dauer fest.*
7. *Spielen Sie die Entscheidung einmal im Führungskreis durch, etwa in einer Tabletop-Übung.*

Entscheidungsmatrix

Die Matrix fasst die Faktoren zusammen, die in die Abwägung einfließen. Sie ersetzt keine Entscheidung, sie macht sie nachvollziehbar.

Faktor	Spricht eher gegen eine Zahlung	Spricht eher für die Prüfung einer Zahlung
Sicherungen	*Vollständig, unverschlüsselt, Wiederherstellung getestet*	*Fehlend, verschlüsselt oder unvollständig*
Betriebsunterbrechung	*Wiederaufbau in tragbarer Zeit möglich*	*Stillstand gefährdet den Fortbestand des Unternehmens*
Datenabfluss	*Kein Abfluss nachgewiesen oder Daten ohne besondere Sensibilität*	*Nachgewiesener Abfluss besonders schutzwürdiger Daten*
Nachweis der Angreifer	*Keine Entschlüsselung nachgewiesen, keine Datenprobe*	*Entschlüsselung an Testdateien nachgewiesen*
Sanktionsprüfung	*Treffer oder begründete Zweifel am Empfänger*	*Kein Treffer, Prüfung und Grenzen dokumentiert*
Versicherung	*Keine Deckung oder keine Zustimmung*	*Deckung bestätigt, Zustimmung liegt vor*
Rechtliche Prüfung	*Offene straf- oder sanktionsrechtliche Fragen*	*Prüfung abgeschlossen und dokumentiert*

Ein einzelner Faktor in der rechten Spalte begründet für sich keine Zahlung. Ein Treffer in der Sanktionsprüfung schließt eine Zahlung aus.

verhandlung.jetzt

Wir unterstützen Geschäftsführungen in Österreich in der Lösegeldfrage, von der ersten Lagebeurteilung über die Verhandlung mit den Angreifern bis zur dokumentierten Entscheidung. Die Verhandlung führen wir in Ihrem Auftrag und nach Ihren Vorgaben. Die Entscheidung bleibt bei Ihnen.

Hinter verhandlung.jetzt steht Michael Meixner, allgemein beeideter und gerichtlich zertifizierter Sachverständiger für IT-Sicherheit und Computerforensik, mit Erfahrung in Incident Response und in Verhandlungen mit Threat Actors.

+43 664 144 83 63 · verhandlung.jetzt

Dieser Leitfaden gibt den Stand November 2026 wieder und ersetzt keine Rechtsberatung im Einzelfall. Maßgeblich sind die jeweils geltenden Fassungen der genannten Rechtsvorschriften im Rechtsinformationssystem des Bundes (RIS) und im Amtsblatt der Europäischen Union. [Computerforensic & more GmbH]