LEITFADEN FÜR UNTERNEHMEN BEI RANSOMWARE-VORFÄLLEN

Dieser Leitfaden wurde als Originalversion von der Counter Ransomware Initiative (CRI) auf Englisch publiziert.

Einleitung

1. Die Mitglieder[1] der Counter Ransomware Initiative (CRI, Counter-Ransomware Initiative, auf Deutsch: Initiative zur Bekämpfung von Ransomware) haben sich mit Versicherungsgesellschaften[2] zusammengetan, um gemeinsam einen Leitfaden für Unternehmen, die Opfer eines Ransomware-Angriffs geworden sind, und unterstützende Partnerunternehmen herauszubringen.
2. Das Nachkommen von Lösegeldforderungen treibt das Geschäft mit Erpressungssoftware an: Im Jahr 2023 wurden weltweit so viele Lösegeldzahlungen getätigt wie nie zuvor (Chainalysis).
3. Bei Ransomware handelt es sich um ein komplexes und grenzüberschreitendes Problem, das eine enge internationale Zusammenarbeit erfordert. Auf dem 3. Gipfel der CRI im Jahr 2023 gaben die CRI-Mitglieder eine gemeinsame Erklärung ab, in der sie dringend davon abrieten, Lösegeldforderungen nachzukommen. In dieser Erklärung wurde darauf hingewiesen, dass die Zahlung eines Lösegelds an Ransomware-Akteure:
    - weder das Ende einer Bedrohung noch die Entfernung der Schadsoftware von Ihren Systemen garantiert;
    - Kriminellen einen Anreiz bietet, ihre Aktivitäten fortzusetzen und auszuweiten;
    - Kriminellen Mittel verschafft, die sie für illegale Aktivitäten nutzen können, und
    - keine Garantie dafür ist, dass Sie Ihre Daten zurückerhalten.
4. Diese Empfehlungen sind rechtlich nicht bindend und setzen keine konkreten Gesetze und Vorschriften ausser Kraft, die in den Gerichtsbarkeiten der CRI-Mitglieder zur Anwendung kommen können.
5. Für Unternehmen, die Opfer eines Ransomware-Angriffs werden, kann es schwierig sein, sich für oder gegen die Zahlung eines Lösegelds zu entscheiden. Die CRI hat einen Leitfaden für Unternehmen, die von einem Ransomware-Vorfall betroffen sind, erstellt. Dieser Leitfaden bietet einen umfassenden Überblick über die einzelnen Massnahmen, die Unternehmen vor einer möglichen Zahlung an Ransomware-Kriminelle in Betracht ziehen sollten. Darin werden auch die möglichen negativen Folgen einer Zahlung an Ransomware-Kriminelle beleuchtet.

[1] Albanien, Argentinien, Australien, Bahrain, Bulgarien, Kanada, Tschad, Kolumbien, Costa Rica, Dänemark, Kommission der ECOWAS, Frankreich, Deutschland, Griechenland, INTERPOL, Irland, Israel, Japan, Kenia, Litauen, Mexiko, Moldau, Niederlande, Neuseeland, Nigeria, Philippinen, Republik Korea, Rumänien, Ruanda, Sierra Leone, Singapur, Slowakei, Slowenien, Spanien, Schweiz, Vereinigte Arabische Emirate, Vereinigtes Königreich, Vereinigte Staaten, Uruguay, Vanuatu, Vietnam.

[2] American Property Casualty Insurance Association, Association of British Insurers, British Insurance Brokers' Association, Dutch Association of Insurers, Insurance Council of Australia, Insurance Council of New Zealand, International Underwriting Association, MSIG Asia Pte Ltd, Singapore Reinsurers' Association, Schweizerischer Versicherungsverband SVV

6. Ziel dieses Leitfadens ist es, das Gesamtausmass eines Ransomware-Vorfalls auf ein Unternehmen zu minimieren und dazu beizutragen, Folgendes einzudämmen:
    - Ausfälle und Kosten für Unternehmen;
    - die Anzahl der Lösegeldzahlungen von Ransomware-Opfern;
    - die Höhe der Lösegeldzahlungen, wenn sich Opfer für eine Zahlung entscheiden.
7. Eine Cyberversicherung kann eine wichtige Massnahme zur Risikobewältigung sein. Die CRI-Mitglieder sind sich der wichtigen Rolle bewusst, die eine Cyberversicherung zur Stärkung der Abwehrkraft gegen Cyberangriffe spielen kann, unter anderem durch die Unterstützung der von ihnen versicherten Unternehmen bei der Verbesserung bestehender Schutzmassnahmen. Die CRI-Mitglieder und Verbände der Versicherungsbranche werden zusammenarbeiten, um die wichtige Rolle, die die gewerbliche Cyberversicherungsbranche bei der Stärkung und Unterstützung der Widerstandsfähigkeit von Unternehmen gegen Ransomware spielt, weiter auszubauen.
8. Die CRI-Mitglieder und Verbände der Versicherungsbranche empfehlen betroffenen Unternehmen, den folgenden Leitfaden genau durchzulesen, bevor sie ihre endgültige Entscheidung im Hinblick auf eine Lösegeldzahlung an eine Gruppe von Cyberkriminellen treffen.

Leitfaden für Unternehmen bei Ransomware-Vorfällen

1. Unternehmen wird empfohlen, sich im Rahmen ihres Betriebskontinuitätsplans vorzubereiten und intern Richtlinien, Verfahren, Regelwerke und Kommunikationspläne zum Umgang mit möglichen Ransomware-Angriffen zu entwickeln und einzuführen.

Rechtliche und regulatorische Rahmenbedingungen für Zahlungen

2. Unternehmen sollten vor einer Lösegeldzahlung die rechtlichen und regulatorischen Rahmenbedingungen prüfen. Fachleute können entsprechende Beratung bieten. Cyberversicherer können Opfer auch mit Rechtsberatern in Kontakt bringen.

3. Unter bestimmten Umständen sind Zahlungen möglicherweise nicht rechtmässig, z. B. wenn eine Lösegeldzahlung an eine sanktionierte Organisation erfolgt.

Meldung des Vorfalls an die Behörden

4. Eine möglichst frühzeitige Meldung von Vorfällen an die Behörden kann den Opfern zugutekommen. Auf diese Weise können die Behörden den Opfern die notwendige Beratung und Unterstützung

zukommen lassen, was wiederum deren Widerstandsfähigkeit stärkt und künftige Ransomware-Vorfälle verhindert. Die rechtzeitige Meldung von Angriffen und geleisteten Zahlungen ist auch für Behörden wie die der Strafverfolgung notwendig, damit diese erfolgreiche Ermittlungen durchführen, Beweise für eine künftige Störung der Aktivitäten von Ransomware-Akteuren sammeln und das allgemeine Verständnis der Behörden für kriminelle Aktivitäten im Zusammenhang mit Ransomware verbessern können. Auf diese Weise können zukünftige Opfer besser unterstützt und möglicherweise zukünftige Angriffe gestoppt werden. Dies kann unter anderem durch die Festnahme und strafrechtliche Verfolgung der Verantwortlichen sowie die Beschlagnahme und Zerschlagung ihrer Infrastruktur und Dienste erfolgen.

Abwägung aller Optionen

5. Betroffene sind nach einem Ransomware-Angriff unter Umständen zunächst überfordert. Ransomware-Akteure wissen genau, wie sie Unternehmen zu schnellen Entscheidungen drängen können. Wenn sich die Betroffenen jedoch die Zeit nehmen, alle Optionen abzuwägen, kann dies zu besseren Entscheidungen und letztlich zu einem besseren Ergebnis führen.

6. Sorgfältige Untersuchungen, eine angemessene Informationsbeschaffung wie auch die Analyse potenzieller Schäden sollten Bestandteil des Notfall- und Wiederherstellungsplans eines jeden Unternehmens sein. Sorgfältige Untersuchungen können folgende Vorteile bieten:
    - die Gewissheit, dass keine wichtigen Informationen oder Beweise übersehen werden;
    - klare, datengestützte Begründungen für Entscheidungen;
    - die Möglichkeit, alle relevanten nationalen rechtlichen Anforderungen zu erfüllen, wie z.B. die Meldung von Vorfällen.

Hinzuziehung von Fachleuten, wo dies möglich ist

7. Externe Fachleute wie Versicherungsunternehmen, nationale Aufsichtsbehörden, Strafverfolgungsbehörden oder Unternehmen zur Bekämpfung von Cybervorfällen (CIR-Unternehmen), die sich mit Ransomware-Angriffen gut auskennen, können bei der Entscheidungsfindung unterstützen. Versicherungsunternehmen empfehlen betroffenen Unternehmen häufig bekannte CIR-Unternehmen, die ihnen behilflich sein können. Wenn Unternehmen eine Cyberversicherung abgeschlossen haben, sollten sie die in der Versicherungspolice festgelegten Vorgaben zu Meldungen einhalten.

Prüfung von Alternativen zu Lösegeldzahlungen

8. In Übereinstimmung mit der gemeinsamen Erklärung, die auf dem 3. CRI-Gipfel im Jahr 2023 abgegeben wurde, wird Unternehmen generell dringend davon abgeraten, Zahlungen zu leisten.

9. Auch wenn Unternehmen in der CRI-Erklärung nachdrücklich davon abgeraten wird, Zahlungen zu leisten, kann es in Übereinstimmung mit den örtlichen Gesetzen und Vorschriften Situationen geben, in denen ein Opfer letztlich die Zahlung eines Lösegelds in Betracht zieht.

10. Entscheidungen über Zahlungen sollten nach Möglichkeit auf der Grundlage eines umfassenden Verständnisses der Auswirkungen des Vorfalls und unter Berücksichtigung der Frage, wie wahrscheinlich es ist, dass eine Zahlung zu einem anderen Ergebnis führt, getroffen werden. Cyberkriminelle werden ihren Opfern weismachen wollen, dass eine Zahlung die einzige Möglichkeit zur Wiederherstellung ihrer Daten ist –trotz der Nachteile, die mit der Zahlung von Lösegeld verbunden sind.

Sammlung relevanter Informationen zur Einschätzung der Auswirkungen und Prüfung der rechtlichen Verpflichtungen

Unsere Empfehlungen für betroffene Unternehmen:

11. Bewerten Sie in Ruhe die technischen Gegebenheiten. Dazu gehören die Verfügbarkeit von Back-ups, alternative Quellen für Dekodierungsschlüssel und die geschätzte Zeit für die Wiederherstellung des Betriebs nach Erhalt der Dekodierungsschlüssel. Einige dieser Lösungen können möglicherweise von Cybersicherheitsfirmen, Strafverfolgungsbehörden oder in Form anderer handelsüblicher oder Open-Source-Tools bereitgestellt werden.

12. Erarbeiten Sie Behelfslösungen, um Betriebsunterbrechungen in den Griff zu bekommen, und ermitteln Sie, wie lange Sie auf diese Behelfslösungen zurückgreifen können. Bei der Überprüfung der Auswirkungen eines solchen Vorfalls müssen Unternehmen die Funktionalität ihres Systems, die Auswirkungen auf ihren Geschäftsbetrieb und auf ihre Kunden und Mitarbeitenden (einschliesslich indirekter Auswirkungen auf die Lieferkette, falls zutreffend) sowie die Wahrscheinlichkeit weiterer Datenexfiltrationen bewerten.

Bewertung der Auswirkungen des Vorfalls

13. Durch Massnahmen zur Bewertung der Auswirkungen eines Vorfalls sind Unternehmen im Hinblick auf künftige Vorfälle besser vorbereitet und für Gespräche über Versicherungsschutz gerüstet. Hierbei ist zu beachten, dass einige Kosten – wiezum Beispiel die Benachrichtigung der betroffenen Personen, behördliche Strafen im Zusammenhang mit dem Datenschutz usw. – bereits infolge der Datenexfiltration während des Ransomware-Vorfalls anfallen können, unabhängig davon, ob die Informationen letztendlich durchgesickert sind. Die Auswirkungen dieser Kosten sollten daher getrennt von der Entscheidung für oder gegen eine Zahlung betrachtet werden. Gehen Sie unter anderem wie folgt vor:
    - Prüfen Sie, ob Sie über einen Versicherungsschutz für solche Fälle verfügen.
    - Machen Sie sich ein Bild von dem durch die Betriebsunterbrechung entstandenen Umsatzverlust. Schätzen Sie die Kosten ein, die durch die Verbesserung der Sicherheitsmassnahmen und die Überstunden der Mitarbeitenden anfallen werden, sowie die Kosten für Rechtsberatung und mögliche Strafen.
    - Stellen Sie fest, welches geistige Eigentum oder welche Daten möglicherweise gestohlen wurden, und beziffern Sie den potenziellen Schaden, der dem Unternehmen, den Kunden und gegebenenfalls den Klienten durch die Veröffentlichung gestohlener Daten entstehen könnte.

14. Nicht zuletzt stehlen Cyberkriminelle bei vielen Ransomware-Vorfällen auch Daten. Opfer sollten sich daher nicht auf das Versprechen verlassen, dass die gestohlenen Daten nach Zahlung des Lösegelds gelöscht werden. Es hat sich bewährt, dass Unternehmen eine Bewertung durchführen, um festzustellen, welche Daten betroffen und wie sensibel diese sind. Rechtsberatung hilft bei der Einhaltung von Gesetzen und Vorschriften sowie im Hinblick auf die Meldungen an und die Unterstützung durch die zuständigen Behörden. Unternehmen sollten auch die Risiken bewerten, die für Leib und Leben, personenbezogene Daten oder die nationale Sicherheit bestehen, falls Daten veröffentlicht werden. Es wird empfohlen, zu überprüfen, ob die Angaben zu Art und Umfang der gestohlenen Daten der Wahrheit entsprechen.

Aufzeichnung Ihrer Entscheidungsfindung

15. Dokumentieren Sie genau, wie Sie auf den Vorfall reagiert, welche Entscheidungen und Massnahmen Sie getroffen und welche Daten Sie erfasst (oder nicht erfasst) haben. Dies ist sowohl für die Nachbesprechung des Vorfalls als auch die Analyse der gewonnenen Erkenntnisse oder die Vorlage

von Beweismitteln bei einer Aufsichtsbehörde von Bedeutung. Am besten zeichnen Sie Entscheidungen, die Sie während eines Vorfalls treffen, offline auf oder auf Systemen, die nicht von dem Vorfall betroffen sind.

16. Ziel dieser Vorgehensweise ist es, überprüfbare Entscheidungswege zu gewährleisten, kurz gefasste Erklärungen für Entscheidungen zu entwickeln und die Wahrscheinlichkeit eines weiteren erfolgreichen Angriffs zu verringern.

17. Je nach Rechtsordnung können die Massnahmen unterschiedlich gestaltet sein, da die behördlichen Verfahren, gesetzlichen Regelungen und internen organisatorischen Anforderungen unterschiedlich sind.

Einbindung relevanter Interessengruppen im gesamten Unternehmen in die Entscheidungen, einschliesslich des technischen Personals und der hochrangigen Entscheidungsträger

18. Es gibt nur wenige Szenarien, in denen Unternehmensleitung und Entscheidungsträger so schnell reagieren müssen wie bei der Entscheidung über eine Lösegeldzahlung. Unternehmen sollten jedoch sicherstellen, dass die Möglichkeiten nicht überstürzt präsentiert und alle relevanten Fakten dargelegt werden.

Achtung – eine Zahlung ist keine Garantie dafür, dass Sie tatsächlich Zugriff auf Ihre Geräte oder Daten erhalten.

19. Selbst wenn Sie in den Besitz eines Dekodierungsschlüssels gelangen, ist es unwahrscheinlich, dass Sie sofort wieder zum normalen Geschäftsbetrieb zurückkehren können. Der Einsatz eines Dekodierungsschlüssels in komplexen Netzwerken kann einige Zeit in Anspruch nehmen. Wenn ein betroffenes Unternehmen sowohl auf Back-ups als auch auf einen Decryptor zugreifen kann, kann die Verwendung von Back-ups die schnellere Lösung sein.

20. Unternehmen sollten unbedingt berücksichtigen, dass die Zahlung von Lösegeld und der Erwerb eines Dekodierungsschlüssels nicht unbedingt das Ende des Vorfalls garantieren. Ein betroffenes Unternehmen sollte nicht davon ausgehen, dass ein angegriffenes System, das wiederhergestellt wurde – sei es durch ein Back-up oder durch die Verwendung eines Dekodierungsschlüssels –, sicher ist. Auch ein Back-up könnte betroffen sein, und böswillige Akteure könnten dafür gesorgt haben, dass ein

System, das mit einem Dekodierungsschlüssel wiederhergestellt wurde, anfällig für weitere Angriffe bleibt.

21. Es gilt auch zu bedenken, dass die böswilligen Akteure ihr Versprechen, gestohlene Daten zu löschen, möglicherweise nicht einhalten und dass Sie wahrscheinlich keine Möglichkeit haben werden, zu überprüfen, ob sie dies tatsächlich getan haben.

Bewertung nach dem Vorfall: Ermitteln der Ursache des Vorfalls und Treffen der notwendigen Vorkehrungen, um einen erneuten Angriff zu verhindern

22. Wenn Sie eine Zahlung leisten, ohne der eigentlichen Ursache für das Sicherheitsrisiko auf den Grund zu gehen, und dann entsprechende Massnahmen zur Schadensbegrenzung ergreifen, ist Ihr Unternehmen anfällig für weitere Vorfälle. Unternehmen sollten versuchen, den Hergang des Angriffs eigenständig zu ermitteln und etwaige Schwachstellen beheben.

23. Des Weiteren sollten sie prüfen, ob das ursprüngliche Sicherheitsleck und die damit verbundenen Schwachstellen beseitigt wurden. Wenn Unternehmen den Hergang des Ransomware-Angriffs genau analysieren, können sie sich besser vor weiteren Angriffen dieser Art schützen. Dazu gehört die Umsetzung von Präventions- und Risikominderungsmassnahmen wie die Verwaltung von Anmeldedaten, die Trennung und Segmentierung von Netzwerken und die Erstellung von Offline- oder getrennten Back-ups.

Quelle: Counter Ransomware Initiative (CRI)