DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Verhalten nach einem Ransomware-Angriff

Ransomware-Ratgeber für Unternehmen: 8 wichtige Maßnahmen nach einem Angriff

17.09.2020

Wie sagte schon Benjamin Franklin: „Wer bei der Vorbereitung versagt, bereitet sich auf sein Versagen vor."

Im Falle eines Ransomware-Angriffs kann ein wirkungsvoller Notfallplan entscheidend sein, damit keine Panik aufkommt. Von ihm kann es abhängen, ob sich die Infektion im gesamten Unternehmen ausbreitet oder ein sich in Grenzen haltender Einzelfall bleibt und damit, ob er sich leicht beheben lässt oder das Ende des Unternehmens bedeutet.

In diesem Ratgeber erläutern wir ausführlich, wie Unternehmen auf einen Ransomware-Angriff reagieren sollten. Außerdem stellen wir Vorsichtsmaßnahmen vor, mit denen sich das Infektionsrisiko minimieren lässt.

Empfohlene Reaktion auf einen Ransomware-Angriff

Falls Vorsichtsmaßnahmen versagen, sollten Unternehmen direkt nach dem Erkennen der Ransomware-Infektion die folgenden Schritte durchführen.

1. Betroffene Systeme isolieren

Die Isolation hat höchste Priorität. Die meisten Ransomware-Versionen scannen das Netzwerk, um auch über das Netzwerk freigegebene Dateien zu verschlüsseln und sich auf andere Systeme zu übertragen. Um die Infektion einzudämmen und eine Verbreitung des Schädlings zu verhindern, müssen infizierte Systeme so schnell wie möglich vom Netzwerk getrennt werden.

2. Sicherungen schützen

Sicherungen spielen für die Wiederherstellung eine wichtige Rolle. Dabei darf jedoch nicht vergessen werden, dass auch sie nicht vor Ransomware immun sind. Um eine Wiederherstellung zu verhindern, haben es viele Ransomware-Varianten besonders darauf abgesehen, auch die Sicherungen eines Unternehmens zu verschlüsseln, zu überschreiben oder zu löschen.

Im Falle eines Ransomware-Angriffs muss das Unternehmen die Sicherungen schützen, indem es sie vom Netzwerk trennt und den Zugriff darauf sperrt, bis die Infektion behoben wurde.

In dieser Anleitung erhalten Sie weitere Tipps, wie Sie vor Ransomware geschützte Sicherungen anlegen und verwalten können.

3. Wartungsaufgaben deaktivieren

Außerdem sollten Unternehmen sofort auf den betroffenen Systemen automatisierte Wartungsaufgaben zum Löschen temporärer Dateien oder für Protokollwechsel deaktivieren. Diese könnten anderenfalls Dateien beeinträchtigen, die möglicherweise von Untersuchungs- und Forensikteams benötigt werden.

Dateiprotokolle können beispielsweise wichtige Hinweise auf den Ausgangspunkt einer Infektion liefern. Es gibt auch einige schlecht programmierte Ransomware-Varianten, die wichtige Informationen wie die Verschlüsselungsschlüssel in temporären Dateien speichern.

4. Sicherungen der infizierten Systeme anlegen

Nachdem die infizierten Systeme von Netzwerk getrennt wurden, sollte eine Sicherung oder ein Abbild von Ihnen erstellt werden. Dafür gibt es zwei wesentliche Gründe:

Datenverlust verhindern

Einige Ransomware-Decrypter enthalten Fehler, die Daten beschädigen könnten. Der Decrypter der namhaften Ransomware-Familie Ryuk hat beispielsweise beim Verschlüsseln die Dateien gekürzt, indem diese um jeweils ein Byte beschnitten wurden. Bei einigen Formaten hatte dies keine großen Auswirkungen. Andere Dateitypen (z. B. virtuelle Festplattenformate wie VHD/VHDX sowie viele Oracle- und MySQL-Datenbankdateien) speichern jedoch wichtige Informationen in diesem letzten Byte und wären daher nach dem Entschlüsseln beschädigt.

Eine Sicherung des infizierten Systems gewährt Datenintegrität. Sollte beim Entschlüsseln etwas schief laufen, können Opfer Ihr System zurücksetzen und das Entschlüsseln wiederholen oder sich an einen Spezialisten zur Ransomware-Wiederherstellung wenden, um eine zuverlässige individuell entwickelte Entschlüsselungslösung zu erhalten.

Kostenlose Entschlüsselung könnte möglich werden

Falls die verschlüsselten Daten nicht unternehmenskritisch sind und daher nicht dringend wieder benötigt werden, sollten sie gesichert und gut geschützt aufbewahrt werden, da es durchaus möglich sein kann, dass diese in der Zukunft entschlüsselt werden können.

Es ist bereits vorgekommen, dass Strafverfolgungsbehörden Ransomware-Programmierer und Steuerserver ausfindig gemacht haben, woraufhin Entschlüsselungsschlüssel veröffentlicht werden und die Opfer Ihre Daten kostenlos entschlüsseln konnten. Es gibt auch eine Reihe von Ransomware-Gruppen, wie beispielsweise Shade, TeslaCrypt oder CrySis, die ihre Schlüssel freiwillig veröffentlicht haben, nachdem sie ihre Aktivitäten eingestellt hatten.

5. Malware in Quarantäne verschieben

Opfer sollten niemals infizierte Systeme bereinigen, löschen, neu formatieren oder ein Abbild aufspielen, sofern sie nicht ausdrücklich von einem Ransomware-Wiederherstellungsspezialisten dazu aufgefordert wurden. Stattdessen sollte die Malware die Quarantäne verschoben werden, sodass Infektion analysiert und die genaue Ransomware-Variante bestimmt werden kann, die Dateien verschlüsselt hat. Wird die Infektion entfernt, wird es für Wiederherstellungsteams extrem schwierig, die bei dem Angriff verwendete Ransomware-Version zu identifizieren.

Wird die Malware noch ausgeführt, sollte vor dem Verschieben in Quarantäne ein Speicherabbild erstellt werden, um nachvollziehen zu können, welche schädlichen Prozesse laufen. In dem Speicherabbild könnten wichtige Informationen verzeichnet werden, dass zum Verschlüsseln der Dateien verwendet wurde. Dieses lässt sich möglicherweise extrahieren und dafür einzusetzen, die Dateien des Opfers ohne Zahlung des Lösegeldes wieder zu entschlüsseln.

6. Ausgangspunkt ausfindig machen und untersuchen

Den Ausgangspunkt ausfindig zu machen (also das Gerät, bei dem die Infektion zuerst auftat), ist unerlässlich, um zu verstehen, wie sich die Angreifer Zugriff auf das System verschaffen konnten, welche weiteren Aktionen sie möglicherweise im Netzwerk durchgeführt haben und wie umfangreich die Infektion ist. Das Aufspüren des Ausgangspunktes der Infektion ist also nicht nur nützlich, um den aktuellen Vorfall aufzuklären, sondern kann Unternehmen auch dabei helfen, Schwachstellen ausfindig zu machen und das Risiko zukünftiger Beeinträchtigungen zu senken.

Da die Angreifer möglicherweise bereits Wochen oder sogar Monate im System unterwegs sind, bevor sie die Ransomware bereitstellen, kann es überaus schwierig werden, den Ausgangspunkt der Kompromittierung zu finden. Unternehmen, denen das Personal oder Fachwissen für eine gründliche digitale Untersuchung fehlt, sollten einen professionellen IT-Forensik-Anbieter in Anspruch nehmen.

7. Die Ransomware-Variante identifizieren

Unternehmen können kostenlose Dienste wie das Online-Tool zur Ransomware-Identifikation von Emsisoft oder ID Ransomware nutzen, um herauszufinden, welcher Ransomware-Version sie zum Opfer gefallen sind.

Bei diesen Tools können die Benutzer die Lösegeldforderung, eine verschlüsselte Beispieldatei und die Kontaktdaten des Angreifers hochladen und analysieren lassen, ihre Ransomware-Variante zu identifizieren. Sollte es bereits ein kostenloses Entschlüsselungstool dafür geben, werden sie dorthin weiterverwiesen.

8. Zahlung des Lösegeldes abwägen

Sollten Sicherungen beschädigt sein und es noch kein kostenloses Entschlüsselungstool geben, könnten Unternehmen die Zahlung des Lösegeldes in Betracht ziehen, um ihre Dateien wiederherzustellen.

Auf diese Weise können zwar möglicherweise die allgemeine Betriebsunterbrechung und deren Kosten geringer ausfallen, allerdings sollte diese Entscheidung nicht leichtfertig getroffen werden. Unternehmen sollten die Zahlung des Lösegeldes nur in Betracht ziehen, wenn alle anderen Möglichkeiten erschöpft sind und ein Datenverlust eine Geschäftsaufgabe zur Folge hätte.

Dabei sind folgende Faktoren zu beachten:

- Die Chancen stehen 1 zu 20, dass die Ransomware-Programmierer das Geld nehmen, aber keinen Decrypter bereitstellen. Generell ist es bei großen, „professionelleren“ Ransomware-Gruppen wahrscheinlicher, einen funktionierenden Decrypter zu erhalten, als für Ransomware-Familien wie Dharma und Phobos, die oftmals von Einzelpersonen gekauft und eingesetzt werden. Wer auch immer hinter dem Angriff stecken mag, die Opfer müssen sich immer darauf verlassen, dass die Kriminellen

einen Decrypter bereitstellen. Dabei haben sie allerdings keinerlei Garantie, dass diese ihren Teil der Abmachung auch wirklich einhalten.
- Der von den Angreifern bereitgestellte Decrypter könnte nicht richtig funktionieren.
- Die Lösegeldzahlungen könnten zur Finanzierung schwerer Verbrechen eingesetzt werden, wie Menschenhandel oder Terrorismus.
- Durch Zahlung des Lösegeldes wird das Ransomware-Geschäftsmodell weiter gefördert und zu zukünftigen Angriffen animiert.

Zu vermeidende Reaktion auf einen Ransomware-Angriff

Ein falscher Umgang mit einem Ransomware-Vorfall kann die Wiederherstellung beeinträchtigen, die Daten gefährden und zu einer unnötigen Zahlung des Lösegelds führen. Unternehmen sollten daher nach einem Ransomware-Angriff folgende Fehler vermeiden:

1. Betroffene Geräte neu starten

Unternehmen sollten unbedingt vermeiden, dass von einer Ransomware beeinträchtigte Geräte neu gestartet werden. Viele Ransomware-Versionen erkennen den Neustartversuch und bestrafen die Opfer durch Beschädigung der Windows-Installation, sodass sich das Gerät gar nicht mehr starten lässt. Andere wiederum löschen nach und nach in zufälliger Abfolge die verschlüsselten Dateien. Die im Jahr 2016 vorherrschende berühmt-berüchtigte Jigsaw-Ransomware löschte bei jedem Geräteneustart zufällig 1000 verschlüsselte Dateien.

Ein Neustart kann auch forensische Bemühungen behindern, da dabei der Speicher des Geräts gelöscht wird, in dem jedoch wie bereits erwähnt für die Techniker nützliche Hinweise enthalten sein könnten. Die Systeme sollten stattdessen in den Ruhemodus versetzt werden, wodurch alle Speicherdaten in eine Referenzdatei auf der Festplatte des Gerätes geschrieben werden. Diese kann dann zur weiteren Analyse eingesetzt werden.

2. Externe Speichergeräte an das infizierte System anschließen

Viele Ransomware-Familien zielen auch auf externe Speichergeräte und Sicherungssysteme ab. Folglich dürfen diese nicht mit den infizierten Systemen (physisch oder über das Netzwerk) verbunden werden, bis die Infektion vollständig entfernt wurde

Es ist nicht immer offen ersichtlich, dass eine Ransomware ausgeführt wird. Leider gibt es viele Fälle, bei denen Unternehmen mit einer Wiederherstellung begonnen haben, ohne zu bemerken, dass die Ransomware immer noch auf dem System vorhanden ist. Dies ermöglichte es dem Schädling, auch die Sicherungssysteme und Speichergeräte zu verschlüsseln.

3. Sofortige Zahlung des Lösegelds

Auch wenn Ausfallzeiten und eine mögliche Schädigung des guten Namens beunruhigen sind, sollten Unternehmen niemals sofort ein Lösegeld zahlen. Es sollten immer zunächst alle anderen verfügbaren Möglichkeiten umfassend geprüft werden, bevor diese Entscheidung als letzter Ausweg getroffen wird.

4. Über das betroffene Netzwerk kommunizieren

Während der Wiederherstellung sollten Opfer davon ausgehen, dass die Angreifer weiterhin Zugriff auf das betroffene Netzwerk haben und daher jegliche darüber gesendete oder empfangene Kommunikation abfangen können. Unternehmen sollten sichere Out-of-Band-Kommunikationskanäle (also außerhalb des Netzwerks) einrichten und Anwendern die Kommunikation über das kompromittiert Netzwerk untersagen, bis das Problem behoben und Angreifer aus dem Netzwerk entfernt wurden.

5. Dateien löschen

Es sollten keine Dateien von dem verschlüsselten System gelöscht werden, sofern nicht ein Ransomware-Wiederherstellungsspezialist dazu aufgefordert hat. Verschlüsseln der Dateien sind nicht nur für die Untersuchungen nützlich, sondern können bei einigen Ransomware Familien auch Verschlüsselungsschlüssel enthalten. Werden diese gelöscht, funktioniert Decrypter nicht mehr.

Auch Lösegeldforderungen sollten niemals gelöscht werden. Einige Ransomware-Versionen wie DoppelPaymer und BitPaymer erstellen für jede verschlüsselte Datei eine Forderung, die den für das Entschlüsseln erforderlichen verschlüsselten Schlüssel enthält. Wird die Lösegeldforderung gelöscht, kann die zugehörige Datei nicht mehr entschlüsselt werden.

6. Ransomware-Programmierern vertrauen

Zwar versuchen Ransomware-Programmierer zunehmend, sich eine professionelle Fassade zuzulegen, allerdings sind und bleiben sie Kriminelle, die sich keinerlei Vereinbarungen oder Verhaltenskodexen verpflichtet fühlen. Unternehmen sollten niemals den von Ransomware-Gruppen bereitgestellten Informationen Glauben schenken (nicht einmal der in der Lösegeldforderung angegebenen Ransomware-Version) und auch nicht darauf vertrauen, dass eine Zahlung des Lösegeldes tatsächlich zum Entschlüsseln der Daten führt.

Zum Identifizieren der verwendeten Familie sollten immer vertrauenswürdige Dienste wie das Online-Tool zur Ransomware-Identifikation von Emsisoft oder ID Ransomware verwendet werden. Die Opfer sollten sich auch bewusst sein, dass die Angreifer nach der Zahlung möglicherweise keine Decrypter bereitstellen oder dass diese fehlerhaft sein und/oder die verschlüsselten Daten sogar beschädigen könnten.

So minimieren Sie das Risiko einer Ransomware-Infektion

Indem sie aktiv Sicherheitsvorkehrungen treffen, können Sie das Risiko eines Ransomware-Vorfalls senken. Unternehmen sollten unabhängig von ihrer Größe folgende Vorsichtsmaßnahmen umsetzen und deren Einhaltung und Wirksamkeit regelmäßig überprüfen:

- **Gepflegte Zugangsdaten:** Mit sorgfältig gepflegten Zugangsdaten lassen sich Brute-Force-Angriffe vermeiden, die Auswirkungen beim Diebstahl von Zugangsdaten minimieren und das Risiko eines nicht autorisierten Netzwerkszugriffs senken.
- **Prinzip der geringsten Berechtigungen:** Bei diesem für alle Unternehmen empfohlenen Sicherheitskonzept haben Benutzer, Programme und Prozesse immer nur lediglich die Berechtigungen, die sie zum Durchführen ihrer jeweiligen Aufgabe benötigen.
- **Mitarbeiterschulungen:** Da Ransomware-Angriffe häufig durch Aktionen der Benutzer ausgelöst werden, sollten Unternehmen regelmäßig Cybersicherheitsschulungen zu

den Themen Phishing, bösartige E-Mail-Anhänge und andere Taktiken des Social Engineerings (also die Manipulation der Anwender) durchführen.

- **Mehrstufige Authentisierung (MFA):** Die MFA sollte wann immer möglich obligatorisch sein, um das Risiko eines nicht autorisierten Zugriffs zu minimieren.
- **Überprüfung von Active Directory:** Unternehmen sollten regelmäßig die Active Directory überprüfen, um mögliche Hintertüren wie kompromittierte Dienstkonten aufzuspüren und zu schließen. Diese verfügen oftmals über Administratorberechtigungen und sind ein beliebtes Ziel für Angreifer, um sich Zugangsdaten zu verschaffen.
- **Netzwerksegmentierung:** Eine wirkungsvolle Netzwerksegmentierung ist unerlässlich, um Vorfälle einzudämmen und Störungen des weiteren Geschäfts zu minimieren.
- **Sicherer Fernzugriff:** Da das RDP (Remotedesktopprotokoll) ein extrem beliebter Angriffspunkt ist, sollten Unternehmen den Fernzugriff unbedingt entsprechend absichern oder ganz deaktivieren, sofern dieser nicht benötigt wird. Er sollte nur über bestimmte Netzwerke oder ein VPN mit MSA erfolgen und auf Benutzer beschränkt sein, die diesen unbedingt für ihre Arbeit benötigen.
- **Privatgeräte vermeiden:** Das Implementieren und strenge Durchsetzen von BYOD-Sicherheitsprotokollen auf Privatgeräten von Mitarbeitern ist enorm anspruchsvoll. Im Idealfall stellen Unternehmen eigene Geräte und Hardware zur Verfügung, um Mitarbeiter davon abzubringen, Privatgeräte für berufliche Zwecke zu nutzen.
- **PowerShell:** PowerShell ist eines der am häufigsten von Ransomware-Gruppen eingesetzten Tools, um sich im Zielnetzwerk zu bewegen, und sollte daher möglichst die installiert werden. Wird es weiterhin benötigt, muss es sehr genau mit einem Endpunktschutz überwacht und durch entsprechende Abwehrmaßnahmen geschützt werden. Administratoren sollten jedes einzelne PowerShell-Skript kennen, dass auf ihren Endpunkten ausgeführt wird.
- **Cyberversicherung:** Unternehmen sollten eine Cyberversicherungen in Betracht ziehen, um die Auswirkungen eines Ransomware-Vorfalls zu minimieren. Derartige Versicherungen können insbesondere für MSPs nützlich sein, die oft für den Schutz der Daten anderer Unternehmen verantwortlich sind. Einige Cyberversicherungsanbieter setzen auf ein Bezahlen des Lösegeldes, während andere zunächst alternative Lösungsansätze verfolgen. Unternehmen sollten also die jeweiligen Policen mit den Versicherern durchgehen, bevor sie sich für einen Anbieter entscheiden.

Darüber hinaus sollten Notfallpläne ausgearbeitet und regelmäßig getestet werden, um sicherzustellen, dass die Mitarbeiter mit den Sicherheitsvorkehrungen vertraut sind und genau wissen, was im Falle einer Infektion zu tun ist. Durch die Tests können Unternehmen zudem Sicherheitslücken bei den Notfallmaßnahmen erkennen und schließen. Am ungünstigsten für ein Unternehmen wird es, wenn es erst bei einem tatsächlichen Angriff herausfinden muss, was bei einem Ransomware-Angriffs zu tun ist. In dieser Warnung des FBI erhalten Sie weitere Informationen zum Erkennen und Beseitigen bösartiger Aktivitäten.

Fazit

Verfolgen Unternehmen eine aktive Herangehensweise zum Vorbeugen von Ransomware, können Sie Ihr Infektionsrisiko erheblich senken. Im Falle eines Angriffs müssen Unternehmen außerdem über wirkungsvolle Notfallmaßnahmen verfügen, um den Vorfall einzudämmen, einen Datenverlust zu vermeiden und einen sicheren Wiederherstellungsprozess einzuleiten.

Mit den in diesem Artikel beschriebenen Maßnahmen können Unternehmen jeder Größe die Auswirkungen eines Ransomware-Angriffs mildern. Es handelt sich dabei jedoch um allgemeine Empfehlungen, die keinen Anspruch auf Vollständigkeit erheben. Sicherheitsanforderungen können extrem unterschiedlich sein und Sicherheitssysteme sollten daher immer an die jeweiligen Branchen, gesetzlichen Vorgaben und individuellen Sicherheitsanforderungen des Unternehmens angepasst werden.

Quelle: https://blog.emsisoft.com/de/36930/ransomware-ratgeber-fuer-unternehmen-8-wichtige-massnahmen-nach-einem-angriff/?ref=ticker200918