CHECKLISTE

Erste Hilfe bei laufenden Ransomware-Angriffen

Allein 2019 gab es über 187 Millionen Ransomware-Vorfälle. Das sind täglich über 500 000 Angriffe auf Unternehmen. Sollten Sie noch nicht zu den Ransomware-Opfern gehören, ist es wahrscheinlich nur eine Frage der Zeit, bis es auch Sie trifft. Und falls Sie bereits angegriffen wurden, sind Sie nicht immun. Deshalb ist es wichtig, dass Sie wissen, wie Sie die Folgen eines Ransomware-Angriffs minimieren können.

Im Folgenden finden Sie eine kurze Übersicht über die notwendigen Schritte, damit Ihr Unternehmen mit einem aktiven Ransomware-Angriff fertig wird:

Vorgehensweise bei Ransomware-Angriffen

Erstens: Keine Panik!

- Sie müssen schnell, aber methodisch vorgehen. Bleiben Sie ruhig und leiten Sie Ihre geplante Reaktion auf Sicherheitsvorfälle ein. Haben Sie keine solchen Incident-Response-Pläne, können die folgenden Schritte helfen. Oder bitten Sie Ihren Security-Anbieter um Hilfe. Sollten Sie den Vorfall Ihrer Versicherung melden, erhalten Sie womöglich dort Versicherer eine Liste mit kompetenten Anbietern, die Sie bei der Ransomware-Bekämpfung unterstützen.
- Spielen Sie die möglichen Folgen des Sicherheitsvorfalls durch. Berücksichtigen Sie nicht nur offensichtlich gefährdete Bereiche wie verschlüsselte Daten und ausgefallene Anwendungen, sondern auch weitere potenzielle Kompromittierungen.
- Informieren Sie Ihr PR-Team und die Rechtsabteilung bzw. Ihre Rechtsberater, damit sie mit den Vorbereitungen beginnen können. Teilen Sie ihnen mit, dass Sie eine offiziellere Kommunikations- und Berichtsstruktur einrichten werden, sobald Sie weitere Informationen haben.
- Legen Sie in einem Kommunikations- und Update-Protokoll fest, wie Sie einen bestimmten Ansprechpartner in jedem Geschäftsbereich informieren und auf dem neuesten Stand halten wollen. Verpflichten Sie sich z. B., alle 3 Stunden die relevanten Teamleiter über die Lage zu informieren. So lassen sich ständige Nachfragen vermeiden, damit sich Ihr Team ganz auf die Eindämmung konzentrieren kann.

Systeme isolieren und Ausbreitung stoppen

- Sie haben mehrere Möglichkeiten, die Bedrohung zu isolieren und ihre Ausbreitung zu stoppen. Ist die Ransomware bereits weitverbreitet, können Sie Blockierungen auf Netzwerk-Ebene implementieren, z. B. den Datenverkehr am Switch oder am Firewall-Edge isolieren oder die Internetverbindung vorübergehend unterbrechen. Sollte bereits feststehen, dass sich der Schaden in Grenzen hält und nur wenige Systeme infiziert sind, können Sie die betroffenen Geräte isolieren, indem Sie sie vom LAN oder WLAN trennen. Wenn Sie bereits mit Technologien wie einer Endpunkt-Erkennung und Reaktion (EDR) arbeiten, können Sie gezielter vorgehen und den Angriff auf Prozessebene blockieren – das wäre die beste Soforthilfe mit den geringsten Betriebsunterbrechungen. Sie sollten möglichst alle Systeme eingeschaltet lassen, damit keine forensischen Beweise verloren gehen. Wichtig: Sobald Sie die Aktivität eines Angreifers stören, weiß er, dass Sie ihn entdeckt haben. Manche Angreifer werden dann inaktiv, wodurch sich der gesamte Umfang des Angriffs schwerer einschätzen lässt.
- Falls notwendig, erstellen Sie forensische Images der Laufwerke und des Arbeitsspeichers der infizierten Systeme – aber nur, wenn Sie damit Erfahrung haben. Sollten Sie und Ihr Team so etwas noch nie gemacht haben, ist davon abzuraten.

Wenn Sie Online- oder cloudbasierte Tools verwenden, denken Sie daran, dass alle von Ihnen hochgeladenen Dokumente von öffentlichen Stellen geprüft werden können.

Ransomware-Variante identifizieren

- Viele Taktiken, Techniken und Prozeduren (TTP) eines Angriffs sind für einzelne Ransomware-Varianten öffentlich dokumentiert. Wenn Sie geklärt haben, mit was für einem Angriff Sie es zu tun haben, wissen Sie eher, wo Sie nach Kompromittierungen suchen müssen, wie die Ransomware sich verbreitet und wie hartnäckig die Infektion ist.
- Vielleicht gibt es ja für Ihre Variante bereits Decryption-Tools, um befallene Dateien zu entschlüsseln. Ein Blick auf die Website No More Ransom lohnt auf jeden Fall. Oft lässt sich auch an der Lösegeldforderung erkennen, welche Ransomware-Gruppe und/oder -Variante verwendet wurde. Das Hochladen der Ransomware auf ID Ransomware kann ebenfalls beim Identifizieren der Variante helfen.
- Wenn Sie Online- oder cloudbasierte Tools verwenden, denken Sie daran, dass alle von Ihnen hochgeladenen Dokumente von öffentlichen Stellen geprüft werden können.

Wo trat die Ransomware zuerst auf?

- Die Bestimmung des ursprünglichen Zugangspunkts – des „Patienten Null“ – hilft beim Schließen von Sicherheitslücken. Ransomware wird häufig über Phishing, Exploits Ihrer Edge-Diensten (z. B. von Remote-Desktop-Diensten) oder mit gestohlenen Anmeldedaten eingeschleust. Andere Vektoren für den Erstkontakt können Drive-by-Kompromittierungen, Exploits von öffentlich zugänglichen Websites und Anwendungen, Wechselmedien, Hardware-Erweiterungen oder über die Lieferkette eingeschleuste Infektionen sein.
- Dieser Schritt ist manchmal schwierig. Womöglich benötigen Sie das Fachwissen von digitalen Forensik- oder Incident-Response-Experten, um den ursprünglichen Zugangspunkt herauszufinden.

Alle infizierten Systeme und Konten bestimmen (Ausmaß)

- Selbst nach dem Ende eines Angriffs ist es sehr wahrscheinlich, dass die Angreifer weiterhin in Ihrem Netzwerk ausharren. Es ist wichtig, dass Sie aktive Malware oder dauerhafte Überreste finden, die noch mit dem Command-Control-Server (CC) kommunizieren. Zu den gängigen Persistenz-Techniken gehören:
  - Erstellen neuer Prozesse, die bösartige Payloads ausführen
  - Verwenden von Run-Registry-Schlüsseln
  - Erstellen neuer geplanter Aufgaben

- Höchstwahrscheinlich haben die Angreifer auch mehrere Konten mit normalen Benutzerrechten und Administratorrechten wie Active Directory (AD)-Konten infiziert. Diese Konten müssen Sie ebenfalls deaktivieren. Sorgen Sie auch dafür, dass keine neuen Rogue-Konten erstellt werden. Andere AD-Komponenten wie Gruppenrichtlinienobjekte (GPO) sollten auf Änderungen oder neue Elemente überprüft werden. Dies ist eine gängige Taktik, mit der Angreifer Ransomware auf alle Systeme übertragen.
- Dokumentieren Sie die Ergebnisse, bevor Sie den Angriff aktiv bekämpfen. Gegenmaßnahmen können Angreifer alarmieren und dazu führen, dass sie einen weitaus schwerwiegenderen Angriff starten. Auch riskieren Sie, nicht mehr alle Daten wiederherstellen oder die gesamten Konsequenzen der Datenpanne feststellen zu können.

Häufig versuchen Angreifer, Online-Backups zu beschädigen. Daher müssen Sie nicht nur nachsehen, ob es ein Backup gibt, sondern auch, ob dessen Daten frei von Infektionen und wiederherstellbar sind.

Wurden Daten abgegriffen?

- Oft verschlüsseln Ransomware-Angriffe nicht nur Ihre Dateien, sondern greifen auch Daten ab. Cyber-Kriminelle erhöhen so ihre Chancen auf Lösegeldzahlungen, indem sie damit drohen, Geschäftsgeheimnisse oder rufschädigende Informationen zu veröffentlichen. Suchen Sie auf Ihren Firewall-Edge-Geräten nach Anzeichen für eine Datenexfiltration, z. B. große Datenübertragungen. Suchen Sie auch nach ungewöhnlichen Anfragen von Servern zu Cloud-Speicheranwendungen wie Dropbox oder AWS. Sollten Sie eine CASB-Lösung (Cloud Access Security Broker) haben, ist dies gemeinsam mit den Firewall-Protokollen Ihre Hauptquelle, wo Sie solche Informationen finden.
- Dieser Schritt kann schwierig sein. Oft ist es sinnvoll, ein Team für digitale Forensik oder Incident-Response-Experten zur gründlicheren Untersuchung hinzuzuziehen.

Backups suchen und Brauchbarkeit klären

- Bei einem Ransomware-Angriff wird auch versucht, Ihre Online-Backups und Schattenkopien von Laufwerken zu löschen. Angreifer wollen so die Wahrscheinlichkeit verringern, dass Sie Ihre Daten wiederherstellen und letztlich kein Lösegeld zahlen. Klären Sie, ob Ihre Backup-Technologie von dem Vorfall verschont geblieben und noch betriebsbereit ist. Überprüfen Sie dann, ob es Online- oder Offline-Backups für die Wiederherstellung gibt.
- Häufig versuchen Angreifer, auch die Online-Backups zu beschädigen. Daher müssen Sie nicht nur nachsehen, ob es ein Backup gibt, sondern auch, ob dessen Daten frei von Infektionen und wiederherstellbar sind.

Integrität der Backups prüfen und letzten bekannten einwandfreien Zustand wiederherstellen

- Bei vielen Ransomware-Angriffen waren Angreifer normalerweise tagelang, wenn nicht sogar wochenlang in Ihrem Netzwerk unterwegs, bevor sie Ihre Dateien verschlüsselt haben. Dies bedeutet, dass womöglich auch Ihre Backups infiziert sind. Nach der Untersuchung des Vorfalls sollten Sie Datum und Uhrzeit der Erstinfektion grob eingrenzen können. Versuchen Sie zunächst, Backups vom Vortag wiederherzustellen – aber erst, nachdem Sie alle Backups auf Kompromittierungen überprüft haben.

Systeme desinfizieren oder neu anlegen

- Wenn Sie zuversichtlich sind, dass Sie alle aktiven Malware-Vorfälle und langfristigen Infektionen – Stichwort „Persistenz“ – in Ihren Systemen aufspüren werden, sparen Sie womöglich Zeit, wenn Sie auf eine Neuerstellung verzichten. Es kann jedoch einfacher und sicherer sein, neue, saubere Systeme anzulegen. Vielleicht ist sogar die Erstellung einer völlig getrennten, sauberen Umgebung sinnvoll, auf die Sie dann migrieren können. Dies dürfte bei virtuellen Umgebungen nicht zu lange dauern. Achten Sie aber darauf, beim Wiederaufbau bzw. der Desinfektion des Netzwerks oder Netzwerk-Segments Sicherheitskontrollen zu installieren und Best Practices zu befolgen, damit Geräte nicht erneut kompromittiert werden.

Vorfall melden

- Jetzt ist es an der Zeit, sich wieder mit der Rechtsabteilung kurzzuschließen. Es ist wichtig, dass Sie alle zuständigen Stellen wie Ihre Rechtsberater oder Ihren Versicherer informieren. Sie sollten auch klären, ob Sie den Fall den Strafverfolgungsbehörden melden müssen.

- Ihre Rechtsabteilung kann Ihnen dabei helfen, alle rechtlichen Verpflichtungen im Zusammenhang mit regulierten Daten wie PCI, HIPAA usw. zu erfüllen. Auch wenn Sie keine spezielle Cyberversicherung haben, übernimmt Ihre Versicherungsgesellschaft womöglich einen Teil der Wiederherstellungskosten. Sollten Sie außerdem Experten für die Bedrohungserkennung und -reaktion (IR, Incident Response) benötigen, hat Ihr Versicherer höchstwahrscheinlich eine Liste mit geeigneten IR-Anbietern, die Sie bei der Untersuchung des Vorfalls unterstützen können.
- Klären Sie, ob Sie die Öffentlichkeit über den Angriff auf Ihr Unternehmen informieren müssen. In einigen Fällen sind Sie u. U. gesetzlich verpflichtet, einige oder alle Details zum Netzwerk offenzulegen. Finden Sie heraus, in welchem Zeitrahmen Sie den Angriff ggf. melden müssen. Sobald Sie die Art der vermutlich kompromittierten Daten kennen, werden Ihre Rechtsberater Ihnen bei dieser Frage weiterhelfen können. Denken Sie daran, dass das Informieren der Strafverfolgungsbehörden von öffentlichem Interesse sein kann und in öffentlichen Registern eingetragen werden muss, was praktisch einer öffentlichen Bekanntgabe gleichkommt.

Es ist wichtig, dass Sie Ihre Reaktion auf Sicherheitsvorfälle nachträglich analysieren. Sie wissen dann, was richtig gemacht wurde und wo Verbesserungsbedarf besteht.

- Ist der Angriff schwerwiegend und Ihr Unternehmen operiert in verschiedenen Regionen, müssen Sie sich ggf. an bundes- bzw. landesweite Strafverfolgungsbehörden wenden.
- Unter Umständen kann es von Vorteil sein, sich an die Strafverfolgungsbehörden zu wenden, insbesondere hinsichtlich der zusätzlichen Ressourcen, die diese zur Bewältigung des Sicherheitsvorfalls bereitstellen können. In einigen Fällen können die Behörden auch beim Auffinden Ihrer Daten helfen, wenn diese abgegriffen wurden. Darüber hinaus verlangen viele Cyberversicherungen, dass ein Polizeibericht vorgelegt wird (fragen Sie hierzu Ihre Rechtsabteilung oder Rechtsberater).

Erst verhandeln, bevor Sie Lösegeld zahlen

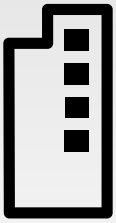
- Strafverfolgungsbehörden sehen es nicht gern, wenn Erpressern nachgegeben wird. Wenn Sie jedoch erwägen, das Lösegeld zu zahlen, sollten Sie einen spezialisierten Security-Anbieter beauftragen, der Ihnen beim Aushandeln des Lösegelds hilft. Cyber-Kriminelle sind meistens verhandlungsbereit. Ihre Rechtsabteilung oder Ihr Anwalt hat wahrscheinlich eine Liste mit empfohlenen Verhandlungsführern. Beachten Sie, dass die Zahlung von Lösegeld an bestimmte Bedrohungsakteure (wie Länder, die mit Wirtschaftssanktionen belegt sind) u. a. in den USA gegen die OFAC-Vorschriften (Office of Foreign Assets Control) verstoßen.
- Denken Sie daran, dass Verhandlungen über Ransomware langwierig sein können. Sie sollten nur verhandeln, um Ihre Daten zurückzubekommen. Seien Sie sich bewusst, dass es keine Garantie dafür gibt, dass Verhandlungen den Angreifer daran hindern, Daten zu löschen oder Ihre Daten zu veröffentlichen.
- Behaupten die Angreifer während der Verhandlungen, Ihre Daten gestohlen zu haben, lassen Sie sich einen überprüfbaren Beweis vorlegen, z. B. eine Verzeichnisstruktur. Diesen Nachweis erbringen Angreifer in der Regel.
- Nicht vergessen: Durch die Zahlung des Lösegelds werden die von den Angreifern ausgenutzten Schwachstellen nicht automatisch geschlossen. Sie müssen auf jeden Fall die Erstinfektion bestimmen und alle Sicherheitslücken schließen.

Rekapitulation nach dem Vorfall

- Beim Militär gibt es ein berühmtes Sprichwort: „Jeder hat einen Plan, bis er auf den Feind trifft.“ Kein Plan ist perfekt – schon gar nicht, wenn er nie zuvor in einer realen Umgebung getestet wurde. Daher ist es wichtig, dass Sie Ihre Reaktion auf Sicherheitsvorfälle nachträglich analysieren. Sie wissen dann, was richtig gemacht wurde und wo Verbesserungsbedarf besteht. Die Fragestellung „Was haben wir gelernt?“ trägt zur kontinuierlichen Verbesserung Ihrer Reaktions- und Wiederherstellungsfähigkeiten bei. Diese Überprüfung sollte so schnell wie möglich nach der Wiederherstellungsphase erfolgen, wenn noch alles frisch im Gedächtnis ist.
- Erwägen Sie, die technischen und nichttechnischen Details des Angriffs bei Red-Team- und Planübungen zu simulieren, um Ihre Optionen durchzugehen.
- Ziehen Sie in Betracht, einen Vertrag mit einem Drittanbieter abzuschließen, um Ihre gesamte Angriffsfläche zu bewerten und fehlende Sicherheitskontrollen zu identifizieren. Diese externen Berater sollten gängige Standards wie vom NIST (National Institute of Standards and Technology) zugrunde legen, damit Sie Fortschritte messen können.

Jeder wird angegriffen. Jeder braucht einen Plan. Beginnen Sie noch heute.

- Wenn Sie diese Checkliste lesen, weil Sie Opfer eines Ransomware-Angriffs wurden, befolgen Sie alle Schritte genau – vor allem den ersten. Panikmache führt zu Fehlern und kann das Problem verschlimmern. Denken Sie daran: Es gibt Fachleute, die Ihnen helfen können.
- Wurden Sie noch nicht angegriffen, ist es an der Zeit, einen Incident-Response-Plan (IR-Plan) für die Reaktion auf Sicherheitsvorfälle und einen Plan für den kontinuierlichen Geschäftsbetrieb zu erstellen. Diese Schritte sind aber lediglich Ihre Ausgangsbasis. Sie müssen noch weitere Planungen und Dokumentierungen vornehmen, z. B. wer zum Notfall-Team bei Sicherheitsvorfällen gehört, wer welche Aufgaben übernimmt und wer gegenüber wem weisungsbefugt ist. Außerdem müssen Sie einen Sprecher ernennen, kritische Ressourcen für die Wiederherstellung anlegen und isolieren, wirksame Backups außerhalb des Netzwerks erstellen, Bedrohungssimulationen mit dem Red- und Blue-Team durchführen, um nur einiges zu nennen.
- Es gibt viele Unternehmen, die helfen können. Sprechen Sie zunächst mit den Security-Anbietern Ihres Vertrauens. Viele haben eigene Expertenteams, die Ihr Netzwerk testen, einen IR-Plan erstellen sowie Forensik- und Wiederherstellungsaufgaben für Sie übernehmen. Aber was auch immer Sie tun: Zögern Sie nicht. Denn genau damit rechnen die Cyber-Kriminellen, die Ihr Unternehmen ins Visier genommen haben.



Es gibt viele Unternehmen, die helfen können. Sprechen Sie zunächst mit den Security-Anbietern Ihres Vertrauens.

Haftungsausschluss: Die in diesem Dokument zitierten externen Websites und die darin enthaltenen Informationen wurden von den FortiGuard Labs als zuverlässig erachtet. Diese Quellen wurden jedoch weder von uns unabhängig validiert noch implizieren diese Zitate irgendeine Art von Empfehlung, da alle Netzwerke und Bereitstellungen einzigartig sind.

FORTINET

www.fortinet.com/de

1. Juli 2021

863720-A-1-DE