Ransomware ist auch eine Angelegenheit für die Chefetage
Ein Leitfaden für das IT- und Unternehmensmanagement

Ein Ransomware-Angriff kann ein ganzes Unternehmen ruinieren und sollte daher insbesondere auch auf Managementebene ernst genommen werden. Es gilt, die nötigen Grundlagen und Vorbereitungen zu treffen, um die Auswirkungen einer Cyberattacke nicht nur in der IT, sondern für das gesamte Unternehmen auf ein Maß zu senken, das dem Business im besten Fall nicht schadet. Was IT-Verantwortliche und Manager konkret beachten sollten, hat Sophos in diesem Artikel zusammengefasst.

Ransomware ist eine reale Bedrohung für Organisationen aller Größen und hat das Potenzial, diesen beträchtlichen Schaden zuzufügen. Mehr noch, durch Ransomware-as-a-Service (RaaS)-Angebote sind Cyberkriminelle sämtlicher Kenntnis- und Fähigkeitsstufen jetzt in der Lage, ihre Angriffe aus einem Baukastensystem zusammenzustellen, wirkungsvoll in Unternehmen einzuschleusen und ihre Ransomware-Forderungen zu erhöhen. Im neuen Sophos 2022 Threat Report wird die Entwicklung der Gefahrenlage und die Aussichten für 2022 und darüber hinaus von den Spezialisten der Sophos Labs, der Rapid Response Teams und von SophosAI, deutlich beschrieben. Das Resümee: Die Gefahrenlage spitzt sich weiter zu. Allerdings kann man mit modernster Security und mit menschlichen Spezialisten jetzt den Cyberkriminellen einen entscheidenden Schritt voraus sein.

Der erste und wichtigste Schritt zur Gegenwehr ist es, die Bedrohungslage für das Unternehmen individuell zu verstehen und zu analysieren: Was bedeutet Ransomware für das Business? Wieviel kostet sie dem Unternehmen und wie kann es sich schützen? Welche anderen Cybergefahren lauern im Internet, im internen Netzwerk oder auf den digitalen Geräten den Mitarbeiter?
Vorbereitung ist das A&O, um nicht unvorbereitet von der Wucht einer Ransomware oder anderer Bedrohungen getroffen und handlungsunfähig zu werden.

Schritt 1: Ransomware verstehen
Streng genommen ist Ransomware eine schadhafte Software, entwickelt, um den Zugang zu einem Computersystem zu blockieren, und zwar so lange, bis eine bestimmte Geldsumme bezahlt wird. Sie sperrt den Zugriff, so dass sämtliche Daten auf einen Computer (zuhause oder im Büro) sowie Daten auf dem verbundenen Netzwerk unerreichbar sind – es sei denn, ein Geldbetrag fließt an die Cyberkriminellen (zumeist in Form von Kryptowährung). Der Angriff erfolgt entweder von Einzeltätern oder – wahrscheinlicher – durch eine Gruppe von Cyberkriminellen, die das Eigentum bei Bezahlung (vielleicht) wieder freigeben. Zumindest in der Theorie.

In den letzten Monaten sahen die Forscher von Sophos allerdings eine Reihe neuer Variationen dieses Modells. Bei typischen Ransomware-Angriffen verschlüsseln die Kriminellen die Daten und machen sie damit unbrauchbar. Einzig durch Zahlung eines Lösegeldes sind sie bereit, die Daten per Entschlüsselung wieder freizugeben. Nun aber zeigen sich immer öfter Angriffe, bei denen Angreifer Systeme infiltrieren und die Daten kopieren, statt diese zu verschlüsseln. Das Opfer hat weiterhin Zugang auf die Systeme und Daten. Die Bedrohung der Täter ist eine andere, nämlich die Veröffentlichung der gestohlenen Daten im Internet bei Nichtzahlung. Im Idealfall (für den Angreifenden) bringt die Bekanntmachung privater Daten das Opfer in große Schwierigkeiten. Wenn es schlecht läuft, sind darunter sehr sensible Informationen, wie zum Beispiel personenbezogene Daten, Betriebsgeheimnisse oder Krankenakten im Falle von Krankenhäusern.

Auch wenn die erpresserische Variante bislang noch einen geringen Anteil an Ransomware-Attacken ausmacht, so lässt sich doch ein Wachstumstrend verzeichnen. Sophos hat in seinem State of Ransomware Report 2021 einen Anstieg von 3 Prozent in 2020 auf 7 Prozent in diesem Jahr festgestellt.

Neben der Tatsache, dass Ransomware mittlerweile auch als Baukasten in Form von Ransomware-as-a-Service (RaaS) für Cyberkriminelle immer leichter verfügbar ist, trägt zu diesem Wachstum auch bei, dass die Angriffe immer ausgefeilter und schwieriger abzuwehren sind. Von den 62 Prozent der Organisationen weltweit, die im letzten Jahr von Ransomware verschont blieben, erwarten 47 Prozent einen zukünftigen Angriff allein aus dem Grund, weil die Attacken viel zu ausgefeilt sind, um sie stoppen zu können.

Zudem sind den Sophos-Forscher:innen bereits private Ransomware-Gruppierungen bekannt, die zunehmend die Taktiken von Nationalstaaten übernehmen und Angriffsmethoden wie Zero-Day-Schwachstellen, speicherinterne Angriffe und Anschläge auf kritische Punkte in Verteilungssystemen und in Lieferketten einsetzen. Bei den Angreifern handelt es sich nicht um Amateur-Hacker, sondern um professionelle kriminelle Organisationen.

Schritt 2: Die Kosten von Ransomware
Laut dem Sophos State Of Ransomware-Report 2021 steigen die Ransomware-Forderungen kontinuierlich. Die durchschnittlichen Kosten zur Erholung nach einer Ransomware-Attacke hat sich in den letzten zwölf Monaten weltweit mehr als verdoppelt – von 656.492 Euro (US-Dollar 761.106) auf 1.595.810 Euro (US-Dollar 1,85 Millionen). Im Mittel beträgt allein die Lösegeldzahlung über 146.642 Euro (US-Dollar 170.000), wobei die Summen von 8.626 Euro (US-Dollar 10.000) bis hin zu 2.587.800 Euro (US-Dollar 3 Millionen) variieren.

Schritt 3: Das Unternehmen schützen
In Anbetracht dieser hohen Kosten und den nicht monetären Folgeschäden sollten Unternehmen und Organisationen nicht nur reaktiv auf Ransomware reagieren, sondern präventive Maßnahmen aktiv einleiten. Folgende Schritte helfen, sowohl die Wahrscheinlichkeit einer Attacke zu reduzieren und auch den Schaden im Falle eines Angriffs zu verringern:

Drei wichtige aktive Maßnahmen:
- Einen Notfallplan erstellen, um im Falle eines Angriffs schnell und koordiniert handeln zu können. Das SANS Incident Handler's Handbook und der Incident Response Guide von Sophos können bei der Planerstellung sehr hilfreich sein. Beide enthalten ausführliche Abschnitte zur Vorbereitung.
- Erstellen von regelmäßigen und möglichst häufigen Backups der Daten. Mindestens eine Kopie dieser Datensicherungen sollte off-line beziehungsweise extern gelagert sein.
- Für einen mehrstufigen Schutz auf so vielen Endgeräten wie möglich sorgen.
- Die Anti-Ransomware-Technologie mit einem aktiven Threat-Hunting-Team koppeln, um die Vorteile beider Schutzmaßnahmen für ein bestmögliches Frühwarnsystem zu vereinen.

Fünf reaktive Maßnahmen im Falle einer Attacke:
- Aktivieren von Plänen für den Notfall und die Betriebsweiterführung.
- Infizierte Geräte vom Netzwerk isolieren, anstatt das gesamte Netzwerk abzuschalten. Denn das könnte forensische Beweise des Angriffs löschen, die zur Nachuntersuchung hilfreich sind.
- Relevante Unternehmensabteilungen einbeziehen. Ransomware ist nicht nur eine Angelegenheit für das IT-Team: auch die Kommunikations- und Rechtsabteilung sowie die Versicherung müssen ins Bild gesetzt werden, so dass sie sich gemeinsam absprechen können. Das gilt auch für spezialisierte Anbieter und Security Operations Center (SOCs), mit denen das Unternehmen zusammenarbeitet.
- Backups und die Kommunikation offline halten. Insbesondere das Absprechen über das

weitere Vorgehen sollte vis-a-vis oder per Telefon erfolgen, denn wenn die Kriminellen E-Mail und Nachrichten-Apps überwachen, bleiben ihnen keine Details des Notfallplans verborgen.

- Ein letzter Tipp: kein Lösegeld bezahlen. In einer verzweifelten Situation wie bei einer Ransomware-Attacke erscheint die Lösegeldzahlung als der einfachste und schnellste Weg, um das Problem zu lösen. Aber: der Freikauf erhöht nur den Anreiz für mehr Ransomware-Angriffe. Im Übrigen zahlt es sich für die Opfer nicht aus – im Durchschnitt bekommen Organisationen nach einer Lösegeldzahlung nur rund 65 Prozent ihrer Daten wieder. Wer in Backups investiert hat, sollte sich die Erpressungssumme sparen und sich auf Backups zur Wiederherstellung der Dateien verlassen. Das garantiert volle Restauration der Dateien beim Opfer und den Entzug weiterer Mittel für den nächsten Ransomware-Angriff bei den Tätern.

Für Organisationen und Unternehmen ist es sinnvoll, sich mit dem Gedanken vertraut zu machen, dass sie mit hoher Wahrscheinlichkeit einmal Ransomware-Opfer werden. Erst dann ist es keine vage, abstrakte Situation mehr, die nur jemand anderen betrifft. Sollte ein Angriff geschehen, dann dürfen Organisationen nicht unvorbereitet sein. Das Bewusstsein, jederzeit in diese kritische Lage zu kommen, regt proaktive und defensive Maßnahmen an.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de