Die Ransomware-Krise braucht einen globalen Lösungsansatz

Ransomware hat sich mittlerweile zu einem globalen Problem entwickelt. Cyberkriminelle Gruppen operieren von Ländern aus, die ihnen einen sicheren Unterschlupf bieten und es ihnen ermöglichen, sogar raffinierteste Angriffe zu starten. Um eine Eskalation zu verhindern, braucht es eine gemeinsame, weltweite Strategie. Eine Einschätzung von Michael Veit, Sicherheitsexperte bei Sophos.

Wir befinden uns mitten in einer Ransomware-Krise. In den letzten Monaten wurde eine Fülle von Ransomware-Angriffen beobachtet, die immer extremer waren, wie zum Beispiel die vorübergehende Abschaltung einer großen US-amerikanischen Treibstoffpipeline. Die zunehmenden Ransomware-Angriffe sind kein neues Phänomen, aber in diesem Jahr hat sich diese Art der Cyberkriminalität von einer bösartigen Bedrohung zu einer ausgewachsenen globalen Krise entwickelt und es auf die politische Agenda geschafft.

Bundesbehörden sind es gewohnt, ständig Cyberangriffen ausgesetzt zu sein. Neu ist jedoch, dass sie jetzt auch Ziel kommerzieller Ransomware-Angriffe sind. Diese Eskalation ist zum großen Teil darauf zurückzuführen, dass die Angreifer ihre Fähigkeiten verfeinert haben, indem sie einerseits in staatlich geförderten „Hacking-Armeen" arbeiten und andererseits als Freiberufler für private Ransomware-Anbieter tätig sind.

Die jüngste Anklage des US-Justizministeriums gegen die chinesische Regierung, die Cyberkriminelle bei ihren Angriffen auf einen weit verbreiteten E-Mail-Server unterstützt haben soll, verdeutlicht die Überschneidungen zwischen Nationalstaaten und Ransomware-Gruppen: Die von Staatsgeheimdiensten entdeckten Sicherheitslücken werden von privaten Akteuren als Waffe eingesetzt. Staaten, die Ransomware-Angreifer und andere Cyberkriminelle ausbilden, haben sowohl die Bedrohung durch Ransomware verschärft als auch ihr Profil in den Augen von Regierungen auf der ganzen Welt gestärkt. Das veranlasste neben dem Weißen Haus auch die NATO und den G-7-Gipfel kürzlich dazu, Erklärungen zu Ransomware abzugeben.

Eine globale Ransomware-Krise braucht eine globale Reaktion und konkrete Maßnahmen, die Regierungen und ihre Partner ergreifen können, um sie gegen Ransomware auf der ganzen Welt einzusetzen.

1. Schluss mit Lösegeldzahlungen

Um Ransomware effektiv bekämpfen zu können, müssen die Opfer aufhören, Lösegeld zu zahlen. Solange Ransomware profitabel ist, fehlt den Angreifern der Anreiz aufzuhören. Die Haltung der Regierung „Wir verhandeln nicht mit Terroristen“ sollte auch für Ransomware gelten. Jedes Unternehmen, das Teil der Lieferkette einer Bundes-, Landes- oder Kommunalverwaltung ist, sollte sich vertraglich verpflichten, im Falle eines Ransomware-Angriffs kein Lösegeld zu zahlen. Die Aufnahme dieser Standardklausel in die Beschaffungspolitik der Regierung und die Bekanntgabe, dass jede staatliche Lieferkette verpflichtet ist, kein Lösegeld zu zahlen, könnte zur Abschreckung vor Ransomware zumindest gegen Regierungsbehörden beitragen.

Doch kein Lösegeld zu zahlen ist oftmals leichter gesagt als getan. Aber eine Möglichkeit, diese Idee attraktiver zu machen – vor allem wenn man sie als Empfehlung und nicht als strikte Vorschrift ausgibt – ist die Betonung auf die enormen Kosten der Wiederherstellung. Eine kürzlich von Sophos in Auftrag gegebene unabhängige Studie ergab, dass Ransomware-Opfer im Durchschnitt 1,85 Millionen US-Dollar ausgeben. Denn die Kosten einer Attacke sind

weitaus mehr als „nur“ das Lösegeld: Kosten für Ausfallzeiten, Mitarbeiter, Geräte, Netzwerk plus entgangene Chancen und längst überfällige Upgrades der IT-Infrastruktur kommen noch hinzu.

2. Regulierung der Krypto-Währungsbörsen, über die die Lösegelder fließen
Was Ransomware zu einer globalen Krise gemacht hat, ist das Ausmaß, in dem immer wieder Nationalstaaten die Cyberkriminellen ausbilden und/oder ihnen einen sicheren Aufenthaltsstandort bieten. Leider fehlt hier bislang jegliche Handhabe. Es existiert kein Regressanspruch auf Regierungen, die Ransomware-Gruppen Unterschlupf gewähren. Eine Möglichkeit könnte die Verhängung von Handelssanktionen gegen Länder sein, die mit Ransomware in Verbindung stehen. Effizienter und produktiver ist es aber wahrscheinlich, Ransomware-Gruppen dort zu treffen, wo es sie am stärksten schmerzt: bei ihrem Geld. Cyberkriminelle wandeln die Lösegelder auf Krypto-Währungsbörsen in harte Währungen um. Die Einführung strengerer Vorschriften für diese Krypto-Börsen würde es Ransomware-Gruppen erschweren, von ihrer Arbeit zu profitieren. Im Inland könnten Krypto-Währungsvorschriften und Anti-Geldwäsche-Richtlinien verhindern, dass Krypto-Unternehmen als Währungsumtausch für Ransomware-Angreifer genutzt werden.

Auch hier hilft eine internationale Zusammenarbeit mit festgelegten Richtlinien. Nationalstaaten wie Russland und China haben einen Anreiz, diese Art von Krypto-Währungsvorschriften für ihre eigenen Krypto-Händler einzuführen, vor allem deshalb, weil sie dadurch gezwungen sind, die Kryptowährung in ihre Währung umzuwandeln. Dies stärkt ihre eigene Finanzkraft und eröffnet eine neue Quelle für Steuereinnahmen. Wenn Ransomware-Gruppen feststellen, dass es nur wenige Länder gibt, in denen sie ihre Lösegeldzahlungen sicher auszahlen können, wird das Geschäftsmodell schlichtweg unattraktiv.

3. IT-Hygiene und Offenlegung von Sicherheitsverletzungen vorschreiben
Es gibt einige grundlegende IT-Hygienemaßnahmen, die viele Unternehmen immer noch nicht ergreifen: Aufklärung der Mitarbeiter über Spear-Phishing, Einführung von Zwei- und Mehrfaktor-Authentifizierung, ein grundlegender Endpoint-Schutz und die Sicherung von Daten auf netzwerk- und standortfernen Speichern. Regierungen könnten hier unterstützen, indem sie die Einhaltung von Zertifizierungen empfehlen, statt diese Anforderungen in Gesetze fließen zu lassen. Ein weiterer Vorteil: Zertifizierungen lassen sich im Gegensatz zu Gesetzen relativ leicht aktualisieren, so dass auch die Einhaltung der Vorschriften durch die Anbieter auf dem neuesten Stand bleiben würde.

Es muss Standard werden, Sicherheitsvorfälle zu melden. Dabei sollte die Berichtspflicht aber keine Strafmaßnahme sein. (außer vielleicht in Fällen, in denen die Vorschriften nicht eingehalten werden). Vielmehr sind sie als Sensibilisierungsmaßnahme zu behandeln. Je mehr Unternehmen oder Behörden verpflichtet sind, Datenschutzverletzungen sofort nach ihrem Auftreten zu melden, desto eher können ihre Partner und Anbieter sensibilisiert werden und sofortige Maßnahmen zum eigenen Schutz ergreifen. Eine bundesweite Meldepflicht für Datenschutzverletzungen ermöglicht zudem ein umfassenderes Verständnis dafür, wie häufig diese Angriffe vorkommen. Ransomware vollständig in den Griff zu bekommen gelingt erst dann, wenn ein Gefühl für das wahre Ausmaß, die Menge und die Häufigkeit dieser Angriffe besteht. Die Pflicht zur Offenlegung von Datenschutzverletzungen und Cyberangriffen trägt dazu bei, dies zu erreichen.

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