Wer war`s? Über die unnötige Zuordnung von Cyberangriffen

China, Nordkorea, Russland, Iran – Cyberattacken werden gern einem Land zugeordnet. Dabei spielt die Schuldzuweisung laut SophosLabs für die Sicherheitslage von Organisationen kaum eine relevante Rolle.

Nachrichten, die bestimmte kriminelle Gruppierungen mit Cyberangriffen in Verbindung bringen, fördern das (menschliche) Bedürfnis nach Schuldzuweisung. Und sie veranlassen Menschen zu glauben, dass es wichtig sei, *wer* die Attacke ausgelöst hat. Die Ransomware WannaCry Nordkorea anzulasten oder NotPetya an Russland zu adressieren, dient vielleicht der korrekten Strafverfolgung, aber für Unternehmen, die sich in einer Bedrohungslage befinden, ist diese Information wenig hilfreich.
Der Versuch Cyberangriffe bestimmten Urhebern zuzuordnen, kann sowohl Security-Teams als auch Führungskräfte unnötig ablenken. Der Fokus muss vielmehr darauf liegen, eine Attacke von vornherein zu verhindern, Bedrohungen zu neutralisieren und Maßnahmen zu ergreifen, damit eine Bedrohungssituation in Zukunft nicht noch einmal eintritt – egal von wem oder von wo.

Die Lösung der Gefahrenlage ist wichtiger, als die Identifikation des Gefährders
Angriffe bestimmten Gruppen zuzuschreiben und ihnen griffige Namen wie „Putrig Goshawk 623“ geben, ist en vogue, aber diese Zuordnung birgt die Möglichkeit zahlreicher Fehler. Ein Beispiel: Enthüllt eine Untersuchung als Quelle einer Attacke eine spezifische IP-Adresse oder in diesem Fall TTPs (**T**aktik, **T**echnik und **P**rozedur), bedeutet das noch lange nicht, dass der Besitzer der IP-Adresse für die Attacke verantwortlich ist oder diese ausgerollt hat. Es sind sozusagen nur die digitalen Brotkrümel, die am virtuellen Tatort zurückbleiben. Vorausgesetzt etwa, es lässt sich eine Verbindung zwischen einer IP-Adresse und einer Person herstellen, die just im Moment einer Attacke ein an die IP-Adresse gekoppeltes Gerät verwendet hat, dann weiß man zwar wo der Angriff ausgeführt wurde, aber nicht, wer es getan hat.
In den meisten Fällen hat diese Jagd nach dem Schuldigen für Unternehmen daher keinen Nutzen. Die Täter-Fixierung lenkt den Fokus auf das, was spannend klingt, aber nicht darauf, woraus es wirklich ankommt: Festlegen der Vorgehensweise, um auf Attacken zu antworten und entschlossen zu handeln. Ein weiteres Beispiel: Ein Unternehmen ist Opfer einer Ransomware-Attacke geworden, das IT-Team ist seit ein paar Tagen mit den Nachwirkungen beschäftigt. Angesichts der drohenden Frist zur Lösegeldzahlung ist es an der Zeit zu entscheiden, ob die angeforderte Zahlung von 100.000 Euro Sinn macht.
Bis hierhin war das IT-Team nicht in der Lage, die Ransomware zu identifizieren und herauszufinden, wie sie ins Unternehmen kam. Es existiert die Vermutung, dass es sich um die Hackergruppe „Putrid Goshawk 623“ aus Nordkorea handelt. Gleichzeitig versucht das IT-Team, seine Backups einzuspielen, die jedoch kontinuierlich neu infiziert werden.
Sich zu diesem Zeitpunkt über einen nationalstaatlichen Angriff Gedanken zu machen, ist Zeitverschwendung, denn es ändert nichts. Für das Unternehmen gilt jetzt, wieder gefahrlos „online“ zu gehen und klar abzuwägen, ob die Kosten für den Verlust von Daten, die Bereinigung und die Neu-Installation inklusive direkter und indirekter Betriebserhaltungskosten geringer sind als das Lösegeld.

Jetzt kommt es nicht nur auf die IT an, sondern auch auf die Führungsebene
Die Rolle der Führungskräfte ist ebenso entscheidend, wie die der IT-Spezialisten. In der Riege der Unternehmensleitung sitzen zumeist keine Spezialisten für IT-Sicherheit – müssen sie auch nicht sein. Wichtig ist, dass sie in der Lage sind, die richtigen Fragen vor, während

und nach einem Vorfall zu stellen:

- *Vorher:* „Kennen wir die Präventiv- und Erkennungskapazitäten unserer Sicherheit, und deren Begrenzungen inklusive Restrisiko?“

- *Währenddessen:* „Was wissen wir? Welche Vermutungen machen wir? Haben wir die Symptome der Bedrohung aufgespürt, um die eigentliche Ursache zu identifizieren und haben wir die Schwachstellen beseitigt, die ausgenutzt wurden?“

- *Nachher:* „Welche Maßnahmen sollten wir zukünftig ergreifen, damit so eine Situation sich nicht wiederholt?“

Unternehmen sollten hohe Priorität auf die Prävention, Erkennung und Reaktion bei Bedrohungen legen. Sie sollten sich in ihrer Strategie und in Bedrohungslagen nicht von Schuldzuweisungen beeinflussen lassen. Mit einem lösungsorientierten Ansatz sind Organisationen besser in der Lage, ihren Betrieb wiederherzustellen und ihre Cyberabwehr zu verbessern – und das ohne exaktes Wissen darüber, wer es denn genau war.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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