Jäger der verlorenen Daten: Das Sophos Incident Response Team sucht und eliminiert Cyberbedrohungen. Fast so spektakulär wie auf der Leinwand.

Wenn sich nachts um zwei plötzlich Sicherheits-Alerts häufen, rückt es an: das Sophos Incident Response Team analysiert, deckt auf und stoppt Cyberbedrohungen auf der ganzen Welt, rund um die Uhr. Klingt wie ein Superhelden-Job.

Peter Mackenzie, Direktor Incident Response bei Sophos, ist so etwas wie der Indiana Jones der Cyberlandschaft: Unermüdlich scannt er mit seinem Team Computersysteme auf der Suche nach Auffälligkeiten, die Hinweise auf eine Cyberbedrohung geben. In den meisten Fällen rufen Geschädigte die Experten zu sich, weil sie Opfer zum Beispiel einer Ransomware-Attacke wurden oder noch mittendrin sind. Die Crux: wenn ein derartiger Erpresser-Vorfall die Rechner lahmlegt, ist das nicht der Anfang eines Cyberangriffs, sondern das aggressive Finale. „Ich beschreibe Ransomware oft als Quittung, die die Kriminellen zum Schluss dalassen. Viele der Opfer, die wir befragen, wann was passiert ist, geben an, dass die Verschlüsselung um ein Uhr nachts startete und sie daraufhin Alarme erhielten. Wenn wir dann die Systeme untersuchen, finden wir oft heraus, dass die Betrüger bereits seit zwei Wochen im Netzwerk sind und ihre Vorbereitungen getroffen haben“, so Peter Mackenzie.

Cybercrime ist längst professionalisiert

Wer jetzt denkt, dass eine Person oder ein Grüppchen Tag und Nacht auf die Tastatur hackt, die verschlüsselten Daten fein aufbewahrt und d’accord zur Ganovenehre nach erpresster Zahlung zurückgibt, um sich mit der erbeuteten Kohle ein schönes Leben an der Copacabana zu machen, hat zu viele Filme der 80er Jahre gesehen. In Wirklichkeit sind Cyberangriffe längst professionalisiert. Es gibt für jeden Bereich einer Attacke spezialisierte Anbieter, die von „Wir bringen Sie in jedes Netzwerk“ (hier gibt es bereits die Profession des Initial Access Brokers….), über „Wir kaufen gestohlene Daten“ bis zu „Wir übernehmen die Erpressung“ reichen. Expertenwissen ist nicht nötig, und auch wer den Zugang zum Dark Web scheut, wird via Google und How-To-Video bei Youtube zum Cybercrook-Lehrling.
Zuviel Enthusiasmus kann dabei auch schiefgehen, wie der kürzlich beschriebene Fall multipler Angreifer belegt, die als konkurrierende Ransomware-Gruppen das zufällig gemeinsame Opfer in einer Art Schichtwechsel attackierten und sich dabei gegenseitig sabotierten.

Schludrigkeit bei der Gerätepflege wird zur Achillesverse

Das Incident Response Team stoppt nicht nur die Attacke, sondern analysiert auch die Prozesse in den Systemen, was die Cyberganoven getan haben und wozu. Auch ob sie sich Hintertüren für ein späteres Zurückkehren eingebaut haben.
Für die Betrüger ist nach Eintritt in das Netzwerk nach Angaben von Mackenzie ein Aspekt immens wichtig: wozu habe ich Zugang. Dazu scannen sie das Netzwerk, gar nicht mal konkret nach etwas Bestimmtem, sondern eher wie ein Dieb im Büroflur, der jeden Türknauf drückt, irgendwann öffnet sich eine Tür.
Die Möglichkeiten für clevere Betrüger sind heutzutage immens. Wenn sich also ein verdächtiger Impuls auf einem System befindet, Sicherheits-Software diese erkennt und eliminiert, heißt das noch lange nicht, dass das Problem damit gelöst ist. Zumeist ist ein schludriger Umgang mit Aktualisierungen, Patches und Ausstattung jedes einzelnen Geräts der kleine Beginn einer großen Katastrophe.

Moderne Cyberabwehr nur mit aktueller Software und menschlichen Expertise
Peter Mackenzie rät nach all seiner Erfahrung im täglichen Umgang mit Cybergefahren in großen und kleinen Betrieben zur Prävention. Folgende Fragen helfen, die Schwachstellen im Betrieb ausfindig zu machen und Vorkehrungen (Tools, Experten, Services etc.) dazu zu treffen. Und zwar am besten sofort, um im Ernstfall rasch reagieren zu können.

1. Was passiert, wenn wir eine Ransomware-Attacke haben?
2. Was geschieht, wenn unsere Backups gelöscht werden?
3. Was passiert, wenn uns jemand mitteilt, wir hätten einen Angreifer in unserem Netzwerk?

Sicherheit ist ein umfassender und zeitaufwändiger Prozess, der kontinuierlich der Pflege und Korrektur bedarf. Software, die initial Auffälligkeiten erkennt und MDR (Managed Detection and Response)-Experten, die rund um die Uhr Angriffe identifizieren und stoppen sowie den Schaden für die Systeme begrenzen sind essenzielle Grundlage einer modernen Prävention und Abwehr von Cyberangriffen.

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