„Wir dürfen Unvollkommenheit nicht mit Sinnlosigkeit verwechseln“

Erfolgreiche Cybersecurity muss Prävention und Detektion ausbalancieren
Von Joe Levy, CTO bei Sophos

In ihrer bisherigen Historie konzentrierten sich Cybersicherheitsprodukte hauptsächlich darauf, bösartigen Code daran zu hindern, auf Computer zu gelangen und diesen auszuführen. Was als Hobbyprojekte zur Beseitigung lästiger Viren auf Disketten begann, hat sich zu einer milliardenschweren Cybersicherheitsindustrie mit dem Ziel entwickelt, die moderne und onlineabhängige Welt zu schützen. Mit zunehmender Reife lässt sich allerdings ein gefährlicher Trend beobachten: Die anwachsende Gewissheit, dass Prävention nicht perfekt ist, verwandelt sich in eine Art provokative Kapitulation, die Unvollkommenheit mit Sinnlosigkeit verwechselt.

In der Folge hat das Cybersecurity-Pendel in den letzten zehn Jahren stark in Richtung Detektion geschwungen und damit die dringend benötigte, schnelle Verbesserung der Erkennungsfähigkeiten stimuliert – mit dieser Entwicklung sind wir alle besser dran. Aber nachdem diese Evolution mittlerweile sehr weit fortgeschritten ist, müssen wir nun eine Überkorrektur verhindern und einen Gleichgewichtszustand zwischen modernem Erkennungs- und klassischem Vorbeugungsschutz anstreben. Wir haben es weder mit einem reinen Malware- noch mit einem reinen Gegnerproblem zu tun, sondern müssen uns mit beidem auseinandersetzen. Dennoch ist das Sprichwort „Vorbeugen ist besser als heilen“ in der IT-Sicherheitswelt so wichtig wie nie – insbesondere in einer Zeit, in der ein einzelner kompromittierter Rechner Kriminellen das nötige Einfallstor bieten kann, um ganze Industrien mit Lösegeldforderungen zu überziehen.

Da moderne Angreifer bei ihren virtuellen Beutezügen gefühlt mit dem Supersportwagen unterwegs sind, ist es enorm wichtig, frühzeitig automatisierte Straßensperren zu errichten, die die Attacke stoppen. Denn ein System, das zum effektiven Schutz 24 Stunden am Tag und 365 Tage im Jahr einen sekundenschnellen menschlichen Eingriff an der Tastatur erfordert, versagt zwangsläufig irgendwann. Wenn wir gegenüber den Kriminellen keinen Boden verlieren wollen, müssen wir sowohl Tools zur Eliminierung von Malware ständig verbessern und uns gleichzeitig auf den Weg machen, eine Plattform zu schaffen, die uns Echtzeiteinblicke in die Aktivitäten der Angreifer bietet. Bei der schieren Menge und Variantenvielfalt an Angriffen ist Prävention entscheidend, um knappe IT-Security-Ressourcen in den Unternehmen zu schonen, damit sie verfügbar sind, um sich auf größere, verheerendere Angriffe zu konzentrieren, die eine menschliche Reaktion erfordern. Ein verbesserter Schutz hilft dabei, den Heuhaufen niederzubrennen und die Nadel freizulegen, die besondere Aufmerksamkeit erfordert.

Essenziell und in den kommenden Monaten unabdingbar für eine effektive Cybersecurity ist in diesem Zusammenhang der in der Technologiebranche häufig verwendete Begriff „Shift Left“. Gemeint ist damit die Strategie, ein Problem frühzeitig anzugehen, sich nicht auf vermeintlichen Lorbeeren auszuruhen und damit viel Zeit und Geld zu sparen. Konkret: Eine Anwendung lässt sich nicht effektiv absichern, indem die Sicherheit erst am Ende des Entwicklungsprozesses berücksichtigt wird. Genauso wenig ist es möglich Systeme oder Netzwerke effektiv abzusichern, wenn die Verantwortlichen der Vorstellung erliegen, dass eine bessere Prävention nicht mehr erreichbar ist, oder wenn diese glauben, dass entweder

Prävention oder Erkennung allein die Probleme der modernen Informationssicherheit lösen kann.

Wir werden einen entscheidenden Schritt nach vorne kommen, wenn wir diesen „Shift Left“ mit einem industrieübergreifenden Teamwork kombinieren. Es geht darum, die massenhaft gesammelten Daten über Cyberangriffe zu kuratieren und gemeinsam eine Engine für Sicherheitsoperationen zu schulen. „Empfehlungs-Engines“ funktionieren bereits vielfach in unserem täglichen Leben und führen uns zu Produkten, die wir vielleicht kaufen möchten, oder zu Fernsehsendungen, die wir sehen möchten. Sie verbessern unser Leben auf vielfältige Weise. Eine Engine für Sicherheitsempfehlungen hat ein ähnliches Ziel: sie ersetzt nicht die aktiven Personen, die unsere Netzwerke und Computer schützen, aber sie hilft ihnen bei der Priorisierung, Triage und Reaktion auf Vorfälle. All das mit dem übergreifenden Ziel, die Verschiebung des zur Verfügung stehenden Zeitrahmens bei der Angriffsabwehr von Wochen auf Tage und von Tagen auf Minuten zu senken. Das kann uns nur unter Anleitung von KI-verstärkten Sicherheitsoperationen gelingen und im Erfolgsfall die Sicherheitsbranche neu definieren – und damit dafür sorgen, dass Cyberkriminelle auch weiterhin das Nachsehen haben.

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