Umfrage zeigt: Cyberkriminelle schalten den Turbo ein und bringen Unternehmen an ihre Grenzen

Joe Levy, President der Sophos Technology Group (STG), ordnet die Ergebnisse der jüngsten Studie "The State of Cybersecurity 2023: The Business Impact of Adversaries on Defenders" ein.

Die Lage der Cybersicherheit in Unternehmen kann in einem Satz beschrieben werden: Während die Cyberkriminellen mit dem Supersportwagen unterwegs sind, versuchen Unternehmen oftmals, mit der der getunten Mittelklasselimousine mitzuhalten. Sprich: Die Angreifer werden immer schneller, und die angegriffenen Unternehmen können nicht mithalten.

Die aktuelle Studie "The State of Cybersecurity 2023: The Business Impact of Adversaries on Defenders" zeigt, dass die heutige Realität ein Cybersicherheitssystem der zwei Geschwindigkeiten ist, in dem sich Angreifer und Verteidiger mit unterschiedlichem Tempo bewegen. Die Angreifer beschleunigen und erweitern durch Maßnahmen wie Automatisierung, "as-a-Service"-Modelle für Cyberkriminalität, verdeckte Identitätswechsel und weitere Anpassungen stetig ihren Aktionsradius und können eine breite Palette ausgeklügelter Angriffe in großem Umfang durchführen.

Reaktionszeiten von bis zu 15 Stunden plus Fehlkonfigurationen sind Hauptrisiken
Auf der anderen Seite können die Verteidiger – gehandicapt durch einen Mangel an Fachwissen, eine überwältigende Anzahl von Warnungen und zu viel Zeit, die für die Reaktion auf Vorfälle aufgewendet werden muss – nicht mithalten.

Die meisten Unternehmen haben Schwierigkeiten bei der Erkennung von und Reaktion auf Bedrohungen. 93 % der Befragten bewerten die Durchführung grundlegender Sicherheitsaufgaben als schwierig. Die Aufarbeitung von Sicherheitswarnungen ist dabei ein weit verbreitetes Problem. Im Durchschnitt wird nur knapp die Hälfte (48 %) aller Warnmeldungen untersucht, um festzustellen, ob es sich um Anzeichen für bösartige Aktivitäten handelt.
Die meisten Unternehmen tun sich außerdem schwer, die zu untersuchenden Warnmeldungen bzw. Ereignisse zu identifizieren und zu priorisieren (71 %).

Bei Unternehmen mit 100 bis 3.000 Mitarbeitern dauert der gesamte Erkennungs-, Untersuchungs- und Reaktionsprozess im Durchschnitt neun Stunden, bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sogar 15 Stunden.
In operativer Hinsicht fehlt es den Verteidigern an Vertrauen in ihre Prozesse, wobei die Fehlkonfiguration von Sicherheitstools als das am häufigsten benannte Sicherheitsrisiko im Jahr 2023 gilt.
Mehr als die Hälfte (52 %) der IT-Fachleute gibt an, dass Cyberbedrohungen für ihr Unternehmen inzwischen zu weit fortgeschritten sind, um sie allein bewältigen zu können. Bei kleinen Unternehmen (100-250 Mitarbeiter) sind es sogar 64 %.

Schlaflose Nächte und zu viel Zeit für die Bewältigung von Bedrohungen
Diese Situation bedeutet für Firmen finanzielle, betriebliche und ressourcenbezogene Folgen, wobei die Auswirkungen des Systems der zwei Geschwindigkeiten erheblich sind und das gesamte Unternehmen betreffen. So sind die direkten finanziellen Auswirkungen eines Cybervorfalls enorm und bereits gut bekannt: Die durchschnittlichen Kosten für ein kleines

oder mittelgroßes Unternehmen zur Behebung eines Ransomware-Angriffs belaufen sich auf 1,4 Millionen US-Dollar. Diese Kosten für die Beseitigung von Vorfällen sind jedoch nur ein Teil der gesamten Wahrheit.

Denn auch die Kapazität für die Bereitstellung anderer IT-Programme ist eingeschränkt: 55 % der Befragten gaben an, dass die Bewältigung von Cyberbedrohungen die Arbeit des IT-Teams an anderen Projekten beeinträchtigt hat. Auch den geschäftsorientierten Bemühungen steht die Cybersicherheit durch ihre Dringlichkeit und Unvorhersehbarkeit im Weg: 64 % wünschen sich, dass das IT-Team mehr Zeit für strategische Fragen und weniger Zeit für die Bekämpfung von Vorfällen aufwenden könnte.
Die lange Zeit, die für die Erkennung, Untersuchung und Behebung von Sicherheitswarnungen aufgewendet wird, hat zudem beträchtliche finanzielle Auswirkungen in Bezug auf die Ressourcenkosten.

Und es zeigt sich, dass diese Situation auch für die Mitarbeiter eine große Belastung darstellt. 57 % der IT-Fachleute geben an, dass die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, sie manchmal nachts wachhält. Bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sind es sogar 65 %.

Angesichts der hohen Kosten für die Rekrutierung, Schulung und Bindung von Mitarbeitern in diesem Bereich stellen all diese Auswirkungen zusätzliche Herausforderungen und Kosten für das Unternehmen dar.

Zum vollständigen Report mit Grafiken geht es hier:
https://assets.sophos.com/X24WTUEQ/at/f8t5qgvm44h5s39br4pkcjt/sophos-the-state-of-cybersecurity-2023-wp.pdf

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