Vier kritische Fragen, die Unternehmen ihrem Anbieter von Managed Security Services stellen sollten

Die Landschaft der Cybersicherheitsbedrohungen ist unglaublich volatil. Cyberkriminelle gehen immer professioneller vor, spezialisieren sich zunehmend und treten sogar in Konkurrenz zu anderen Gruppierungen. In der Folge sind Unternehmen innerhalb von Monaten, Wochen oder Tagen – manchmal sogar gleichzeitig – nicht nur einmal sondern immer wieder Angriffen ausgesetzt.

Der weltweite Arbeitskräftemangel im Bereich Cybersicherheit verschärft diese Herausforderungen. Weltweit hat sich die Personallücke im Bereich Cybersicherheit im Jahr 2022 nach Angaben der „2022 Cybersecurity Workforce Study by (ISC)²“ um 26,2 % erhöht, mit insgesamt mehr als drei Millionen offenen Stellen. Während einige Regionen besser abschneiden als andere – wie beispielsweise Lateinamerika, das die Lücke um 26,4 % schloss – bergen die verbleibenden Engpässe immer noch nationale Sicherheitsrisiken.

Cyberkriminelle sind immer aktiv, und Sicherheitsteams müssen es auch sein. Viele Organisationen, die nicht über die erforderlichen Ressourcen verfügen, um selbst immer komplexere Cyberbedrohungen zu erkennen und darauf zu reagieren, entscheiden sich für die Nutzung von Cybersecurity-as-a-Service (CSaaS), um proaktive Abwehrmaßnahmen zu implementieren. Beim CSaaS-Modell setzen Unternehmen externe Spezialisten ein, um kritische Cybersicherheitsanforderungen zu erfüllen, wie z. B. Bedrohungsüberwachung rund um die Uhr. Durch die Auslagerung oder Erweiterung von IT-Teams mit Managed Detection and Response (MDR)-Services als zentrales CSaaS-Angebot können Unternehmen dazu beitragen, Angriffe abzuschwächen, bevor sie auftreten.

Jedes Unternehmen, das erwägt, den Sicherheitsbetrieb auszulagern, sollte Sicherheitsdienstpartnern diese vier Fragen stellen:

1.Welche Erfahrung haben sie in der Zusammenarbeit mit anderen Unternehmen in unserer Branche und Region?
Wenn der Anbieter mit anderen Organisationen in ihrer Branche und Region zusammenarbeitet, sollten diese über Erfahrungen aus erster Hand bei der Verteidigung gegen die spezifischen Bedrohungen verfügen, denen sie ausgesetzt sind.

2. Können sie unsere bestehenden Technologien verwalten und unterstützen?
Fragen sie, ob der CaaS-Anbieter auf ihren vorhandenen Sicherheitstechnologien aufbauen kann, oder ob sie das, was sie bereits im Einsatz haben, entfernen und ersetzen müssen. Der ideale Anbieter sollte in der Lage sein, mit den vorhandenen Technologielösungen zu arbeiten.

3. Wie ausgereift ist ihr Verständnis von neu auftretenden Cyberbedrohungen?
Kriminelle entwickeln sich häufig in den Taktiken, Techniken und Verfahren (TTPs) weiter, die sie verwenden, um Angriffe möglichst unbemerkt durchzuführen. Unternehmen sollten sehr sorgfältig darauf achten, dass ein potenzieller Anbieter die entsprechenden Ressourcen vorweisen kann, mit denen er eine qualitativ hochwertige Bedrohungsanalyse sowie schnelle Reaktion gewährleisten kann.

4. Kann die Lösung eines potenziellen Partners mit unserem Unternehmen skalieren und sich mit unseren Anforderungen weiterentwickeln?
Es ist von entscheidender Bedeutung, dass jeder potenzielle Partner in der Lage ist, den individuell wachsenden und sich entwickelnden Anforderungen gerecht zu werden und die Unternehmenssicherheit zusammen mit sich ändernden Anforderungen effektiv zu optimieren.

Mit einem starken CSaaS-Anbieter sind Unternehmen in der Lage, eine vollständig etablierte Sicherheitsstruktur mit proaktiven Abwehrmaßnahmen und 24/7-Unterstützung zur realisieren. Dies gibt Unternehmen die Möglichkeit, ihre IT-Operationen kontinuierlich zu verbessern und Organisationsmodelle zu verfeinern, wodurch sie in einer äußerst volatilen Bedrohungslandschaft nicht nur überleben, sondern auch wachsen können.

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