SOPHOS
Cybersecurity made simple.

Angriff Lila: So stellt man ein Sicherheitsunternehmen sicher auf

Ross McKerchar ist der neu ernannte CISO, Chief Information Security Officer bei Sophos. In einem Interview gibt er tiefe Einblicke in seine Arbeit und gibt Tipps zur besseren Sicherheit.

Was bedeutet es heutzutage CISO bei einem Sicherheitsunternehmen zu sein?
Der CISO hat eine sehr breit aufgestellte Rolle. Letztlich ist man derjenige, der auf die Cybersicherheit in der gesamten Organisation achten und sich dafür verantworten muss. Bei der Beschreibung meiner Teamstruktur wird das deutlich – verschiedene Teams arbeiten Hand in Hand für die Sicherheit:

Team eins ist das **Risiko- und Strategie-Team**: Seine Rolle ist es, Möglichkeiten zu evaluieren und jegliche Probleme an erster Stelle zu verhindern. Das tut das Team, indem es sicherstellt, dass wir unsere Ressourcen auf die richtigen Bereiche fokussieren, unsere Systeme sicher aufbauen und diese am Laufen halten. Und das alles wiederum linientreu mit unseren Grundsätzen.

Ein weiteres Team ist das **Sicherheits-Vertrauens-Team**. Diese Mitarbeiter sollen aktiv prüfen, ob unsere Kontrollen auch wirklich greifen. Sie tun dies sowohl durch individuelles Testing als auch durch Simulation echter Attacken. Wir nennen es Lila Teambuilding, in Anlehnung an den Begriff des Rotes Teams, der für eine unabhängige Gruppe steht, die als Gegner auftritt, um für eine bessere Effektivität zu sorgen. Das Lila Team operiert ähnlich, aber es wird in enger Zusammenarbeit mit den Verteidigern (Blaues Team) geführt. Das Ziel ist nicht einfach nur in das System einzubrechen, sondern zu gewährleisten, dass das Blaue Team lernt, wie man jegliche identifizierte Schwachstelle auffindet und bekämpft.
Bei Sophos nimmt das Security Operations Centre (SOC) die Rolle des Blauen Teams ein. Seine Aufgabe ist die aktive Abwehr von Angriffen mithilfe von eng überwachten Alarmen und Metriken unserer Infrastruktur, plus: Suchen nach möglichen Problemen und ein wachsames Auge auf entstehende externe Bedrohungen.

Zuletzt gibt es noch das Team der **Sicherheits-Technik-Abteilung**. Sie installiert und spielt mit neuen Sicherheitstools und -Produkten quer durch unser Umfeld. Damit haben diese Mitarbeiter eine besonders wichtige Rolle, denn ihre Arbeit fließt bedeutend in die Entwicklung und das Testen der Effektivität unserer Produkte ein. Das reicht von der Zusammenarbeit mit unserem R&D Teams zum Testen der Machbarkeit von Programmen und Techniken in einem sehr frühen Stadium bis zur Sicherstellung, dass wir auch intern über eine starke Verbreitung unserer Produkte verfügen.

Alls das macht meinen Job sehr spannend: dass wir Produkte verkaufen, die mit echten Anwendern von Sicherheitssoftware zusammen entwickelt und getestet

werden. Meine Aufgabe ist es, diese Mitarbeiter in mein Team zu holen und sicherzustellen, dass sie gut zusammenarbeiten.

Wie schützt man seine Mitarbeiter gut?
Ich bin ein großer Verfechter von Grundlagen: mit Basis-Sicherheit und guter Hygiene kommt man sehr weit, besonders wenn man kein spezifisches Ziel ist. Ein großes Problem von Handys und alten Computern ist ihre Eigenschaft, irgendwann keine aktuellen Updates mehr aufzuzeigen. Man muss hier also selbst für die neuesten Versionen sorgen. Außerdem sollte man darauf achten, zumindest irgendeine Art von Endpoint-Sicherheitssoftware zu verwenden. Starke Passwörter sind ein Muss und insbesondere mobile Geräte wie Laptops und Smartphones sollten über Verschlüsselungen verfügen.
Schließlich sollte man auch sicherstellen, dass die Mitarbeiter umsichtig mit Emails, Texten, Anrufen etc. sind. Das lässt sich in Workshops und Trainings vermitteln. Einfach zu handhabende IT-Systeme und simple Regeln statt komplexer Anweisungen helfen den Mitarbeitern. Auch eine Multi-Faktor-Authentifizierung ist ein Muss heutzutage.

Ein letzter Tipp für die Sicherheit Zuhause:
Natürlich wäre ein Smart Home-Sicherheitssystem ideal. Aber, darüber hinaus sollte man sich einfach immer bewusst sein, dass jedes einzelne Kommunikationsmedium ein potentielles Opfer für Cyberkriminelle ist. In einem durchschnittlichen Haushalt leben Laptops, Smartphones, Tablets etc. Alle sollten Software-seits auf dem neuesten Stand seien.
Jeder hat zudem Bereiche, die für Betrüger von Interesse sind. Wer sagt, „Macht nichts, bei mir gibt es nichts von Wert“, da muss ich gleich eingreifen: wenigstens hat man die Pflicht, die Daten seiner Familie und Freunde zu schützen!

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