Missverhältnisse bei Anreizen

Angetrieben von den Marktkräften überholen Cyber-Kriminelle die Verteidiger.

Drei Beispiele für die Missverhältnisse

Die Missverhältnisse zwischen Cyber-Kriminalität und Verteidigung besteht auf mehreren Ebenen, z. B. zwischen Angreifern und Verteidigern, zwischen Strategie und Umsetzung sowie zwischen Führungsetage und Implementierern eines Unternehmens.

Angreifer

Flexibel und schnell

Die Anreize der Angreifer sind durch einen fließenden, dezentralen Markt geprägt, an den sie sich flexibel und schnell anpassen.

gegen

Verteidiger

Durch Bürokratie eingeschränkt

Die Verteidiger werden durch Bürokratie und Entscheidungen übergeordneter Stellen eingeschränkt.

Strategie

90 %

Über 90 Prozent der Unternehmen verfügen über eine Cyber-Sicherheitsstrategie.

gegen

Umsetzung

Weniger als 50 %

Weniger als die Hälfte der Unternehmen haben ihre Strategien vollständig implementiert.

Führungsetage

Unterschiedliche Erfolgsmessung

Führungskräfte, die die Cyber-Strategien entwickeln, messen den Erfolg anders als die Implementierer.

gegen

Implementierer

Begrenzte Effektivität

Implementierer, die die Strategien umsetzen, werden von Führungskräften eingeschränkt.

Das Ausmaß der Missverhältnisse

Obwohl Cyber-Sicherheitsrisiken für Unternehmen immer mehr zur Herausforderung werden, liegen die Unzulänglichkeiten nicht nur bei Risikoverwaltung und Teamanreizen, sondern auch bei der Vorgehensweise von Angreifern und Verteidigern.

76 %

76 Prozent der Befragten gaben an, dass das Cyber-Sicherheitsrisiko jetzt zu den drei wichtigsten Risikofaktoren gehört.

54 %

54 Prozent der befragten Führungskräfte sorgen sich mehr um die Auswirkungen auf den Ruf des Unternehmens als um die tatsächlichen Folgen eines Cyber-Sicherheitsangriffs.

83 %

83 Prozent der Umfrageteilnehmer melden auch weiterhin Schäden aufgrund von Kompromittierungen der Cyber-Sicherheit.

5× wahrscheinlicher

Betreiber gaben mit einer 5 Mal höheren Wahrscheinlichkeit an, dass keine Anreize für Cyber-Sicherheit existieren.

Ideen/Geld

Cyber-Kriminelle der Oberklasse stehlen Ideen, während einfachere Kriminelle Geld stehlen.

51 %

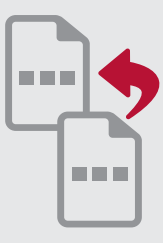
Nur 51 Prozent der befragten IT-Experten in Russland haben Arbeit im legalen IT-Sektor gefunden.

42 %

42 Prozent der Schwachstellen werden innerhalb von 30 Tagen nach ihrer Entdeckung von Kriminellen ausgenutzt.

Lektionen aus dem kriminellen Markt

Vergleich zwischen dem kriminellen Markt und den IT-Abteilungen



Transparenz erhöhen

Durch stärkeren Informationsaustausch und die damit verbundene Reduzierung doppelter Informationen lassen sich die Kosten für Verteidiger senken. Zudem werden neue Technologien und Verfahren bekannt gemacht, mit deren Hilfe die Sicherheitslage erheblich verbessert wird.

Anreize anpassen

Um Anreize von der Führungsetage bis hin zur Mitarbeiterebene anzupassen, müssen zum Beispiel Auszeichnungen und Boni für Mitarbeiter sowie Manager geschaffen werden, die gute Sicherheitsergebnisse erzielen.

Marktkräfte nutzen

Durch Outsourcing und Open Contracting können die Kosten gesenkt, der Wettbewerb erhöht und die Weitergabe innovativer Empfehlungen gefördert werden.

Eintrittsbarrieren senken

Durch die Nutzung eines breiteren Fachkräftepools – einschließlich junger und ausländischer ICT-Experten, die oft von Cyber-Kriminalität angezogen werden – können Unternehmen ihren Mangel an Cyber-Experten ausgleichen und Fachkräfte vom kriminellen Markt abziehen.

Offenlegung nutzen

Wenn Unternehmen nach der Offenlegung von Schwachstellen schneller reagieren (z. B. bessere Patch-Verfahren anwenden sowie veraltete Systeme zügig austauschen), können die Sicherheitslage verbessert und die Kosten für die Angreifer erhöht werden.

Sich abstimmen. Von Angreifern lernen. Mit Anpassung zum Erfolg.

Den vollständigen Bericht finden Sie unter www.mcafee.com/misaligned.

2504_0217_info-misaligned-incentives-cybercriminals-defenders