Kurzfassung

Warum Angriff die beste Verteidigung ist: Missverhältnisse bei Anreizen – der Finanzsektor im Blickpunkt

Cyber-Kriminelle haben seit Langem die Vorteile auf ihrer Seite und finden immer neue Möglichkeiten zur Kompromittierung von Daten und Unterbrechung von Diensten sowie Informationsflüssen – und zwar nicht, weil sie besser sind, sondern weil sie von der Diskrepanz zwischen den Anreizen bei Angreifern und Verteidigern profitieren. Um diese Missverhältnisse besser zu verstehen, befragten wir 200 IT-Experten aus der Finanzdienstleistungsbranche und verglichen ihre Antworten mit denen von 600 IT-Experten aus anderen globalen Branchen. Der **Bericht** stellt drei wichtige Missverhältnisse bei Anreizen vor: zwischen festen Unternehmensstrukturen und flexiblen kriminellen Unternehmungen, zwischen Strategie und Umsetzung sowie zwischen der Führungsetage und den Implementierern.

Drei Ebenen des Missverhältnisses bei Anreizen bedingen Nachteile für die Verteidiger

Angreifer gegen Verteidiger	Die Anreize für die Angreifer entstehen aus einem fließenden, dezentralisierten Markt, wodurch sie flexibler und anpassungsfähiger sind. Im Gegensatz dazu werden die Verteidiger von Bürokratie und Entscheidungen übergeordneter Stellen eingeschränkt.
Strategie gegen Umsetzung	Obwohl 90 % aller Unternehmen über eine Cyber-Sicherheits-strategie verfügen, setzt nur die Hälfte diese Strategie vollständig um.
Führungsetage gegen Implementierer	Hochrangige Führungskräfte, die Cyber-Sicherheitsstrategien entwickeln, messen deren Erfolg anders als die Implementierer, die diese Strategien umsetzen, wodurch die Effektivität leidet.

intel Security

Unternehmensstruktur gegen kriminelle Unternehmung

Die Finanzdienstleistungsbranche versteht seit Langem die Auswirkungen klarer und direkter Anreize. Cyber-Kriminelle agieren in einer heimlichen, aber offenen Welt mit selbständigen Akteuren sowie klaren Motiven und fördern den dynamischen Wettbewerb sowie schnelle Innovationen. Dies führt zu einer starken Spezialisierung, sodass die besten Akteure einen reichen Erfahrungsschatz anhäufen und ein umfangreiches Netz aus Lieferanten sowie Kunden spinnen. Informationen werden über vielfältige Kanäle ausgetauscht, und neue Schwachstellen werden sehr schnell ausgenutzt. Aktive Märkte erleichtern die Suche nach interessierten Kunden und bestimmen den Preis für neue Informationen und neuen Code.

Laut unseren Untersuchungen gelingt es den Finanzdienstleistern unter den Befragten am ehesten, einen offenen Informationsmarkt für Cyber-Schutzmaßnahmen zu betreiben. Sie teilen am häufigsten Informationen mit anderen Unternehmen, einschließlich Partnern (63 % gegenüber 52 % der Befragten aus nicht zum Finanzsektor gehörenden Branchen), externen Beratern (49 % gegenüber 39 %) und sogar Mitbewerbern (26 % gegenüber 19 %). Nur 7 % der Befragten gaben an, dass sie keine Cyber-Bedrohungsinformationen austauschen (im Vergleich zu 14 % der Befragten aus anderen Branchen).

Diese Einstellung zum Austausch beeinflusst die Quellen, die Finanzdienstleister bei Entscheidungen über Cyber-Sicherheit heranziehen. Sie verwenden etwas häufiger Informationen aus externen Quellen als Befragte anderer Branchen. Dazu gehören Informationen von Sicherheitsanbietern (63 % gegenüber 57 %), externen Beratern (51 % gegenüber 46 %) und Branchengruppen (26 % gegenüber 22 %). Möglicherweise werden diese Informationen von Mitarbeitern analysiert und zusammengefasst, da die Experten aus der Finanzdienstleistungsbranche auch häufiger interne Briefings abhalten als Experten anderer Branchen (70 % gegenüber 61 %).

Die Unterstützung offener Cyber-Sicherheitsmärkte in der Finanzdienstleistungsbranche betrifft nicht nur Informationen, sondern auch Dienstleistungen und Berater. Sie wenden am häufigsten einen signifikanten Teil ihres Cyber-Sicherheitsbudgets für Berater auf (49 % gegenüber 40 % der Unternehmen anderer Branchen) und investieren etwas häufiger in Professional Services-Angebote für Überwachung und Reaktion auf Zwischenfälle (38 % gegenüber 34 %). Diese Offenheit für externe Informationen und Spezialisten hat positive Auswirkungen auf die Effektivität der Sicherheitsmaßnahmen.

Missverhältnisse zwischen Strategie und Umsetzung

Laut einem Großteil der Befragten stellt Cyber-Sicherheit jetzt das größte Risiko für Unternehmen aller Branchen dar. Fast 80 % der Finanzdienstleister informieren ihre Führungskräfte bei allen oder fast allen Meetings über Cyber-Sicherheitsrisiken (im Vergleich zu nur 70 % der Befragten in anderen Sektoren). Während fast alle Umfrageteilnehmer aus der Finanzbranche (95 %) angaben, dass ihr Unternehmen über eine Cyber-Sicherheitsstrategie zur Abwehr neuer und vorhandener Bedrohungen verfügt, ergeben sich die Herausforderungen meist bei der Umsetzung. Nur etwas mehr als die Hälfte (51 %) der Unternehmen gab an, dass sie ihre Cyber-Sicherheitsstrategie vollständig umgesetzt haben, und 8 % haben die Strategie überhaupt nicht umgesetzt.

Ein Teil der Diskrepanz bei der Umsetzung der Sicherheitsstrategien ist möglicherweise auf eine Fehleinschätzung der Risiken für das Unternehmen zurückzuführen. Im Durchschnitt gilt die Sorge der Führungskräfte dieser Finanzdienstleister eher Schäden für den Ruf des Unternehmens (67 %) als Umsatz- oder Gewinnverlusten (50 %). Angesichts der aktuellen Zunahme bei direktem Diebstahl in der Finanzbranche im Gegensatz zu Verlusten durch Betrug im Zusammenhang mit gestohlenen Kreditkartennummern kann diese Haltung zu einem falschen Gefühl der Sicherheit führen.

Die Unternehmen, die ihre Sicherheitsstrategie umsetzen, scheinen über einen überdurchschnittlich hohen **Sicherheitsreifegrad** zu verfügen. Die größte Bedeutung messen diese Sicherheitsteams präventiven Schutzmaßnahmen bei, gefolgt von der Untersuchung neuer Strategien sowie Lösungen und dann reaktiven Schutzmaßnahmen. Möglicherweise noch wichtiger: Sie wenden die wenigste Zeit für nicht im Zusammenhang mit der Cyber-Sicherheit stehende Aufgaben auf (8 % im Vergleich zu 14 % in anderen Branchen).

Da die Branche schon seit Langem Ziel von Cyber-Angriffen ist, überraschend es nicht, dass 73 % der Sicherheitsexperten bei Finanzdienstleistern ihr Budget für die Umsetzung ihrer Strategie als angemessen einschätzen (im Vergleich zu nur 58 % bei den anderen Branchen). Nur ein kleiner Teil der Unternehmen in der Finanzbranche war der Meinung, dass ihr Budget (4 %) oder ihr Personalbestand (9 %) unzureichend ist und Probleme bei der Umsetzung ihrer Strategie verursacht.

Eine weitere Diskrepanz zwischen Strategie und Umsetzung betrifft die Methoden, mit denen sichergestellt wird, dass Cyber-Schutzmaßnahmen nicht zu neuen Risiken für das Unternehmen führen. Obwohl die Mehrheit der Finanzunternehmen (73 %) eine Sicherheitsplattform zur Integration vorhandener und neuer Technologien betreibt, gaben etwa genau so viele Unternehmen (70 %) an, dass sie überlappende Sicherheitstechnologien angeschafft hätten. Das klingt zwar im ersten Moment nach einer guten Strategie, doch unzureichend integrierte, sich überschneidende Sicherheitstechnologien können zu Sicherheitslücken führen, da unterschiedliche Konfigurationen und Überwachungssysteme die Erstellung sowie Durchsetzung konsistenter Sicherheitsrichtlinien erschweren.

Unterschiedliche Anreize für Führungskräfte und Implementierer

Cyber-Kriminelle erhalten von ihren Aktivitäten einen direkten Anreiz – in Form von Geld, öffentlicher Aufmerksamkeit und Blamage aufseiten ihrer Opfer. Cyber-Sicherheitsteams bei Finanzdienstleistern erhalten am häufigsten Anreize wie Anerkennung (55 % gegenüber 48 % in anderen Sektoren) und Boni (53 % gegenüber 43 %). Nur 9 % der Befragten gaben an, dass zurzeit keine Anreize existieren. In anderen Branchen lag dieser Anteil bei 21 %. Der Hauptanreiz für die Vermeidung von riskantem Verhalten im Zusammenhang mit Cyber-Sicherheit besteht für Mitarbeiter in drohenden rechtlichen Schritten (69 % gegenüber 59 %). Außerdem nannten 56 % der IT-Experten in der Finanzbranche die Umsetzung von Strategien als Bestandteil ihrer persönlichen Leistungsbewertungen (im Vergleich zu nur 46 % in anderen Branchen).

Für die Ermittlung, ob eine Strategie den Zielsetzungen entspricht, sind ausreichend detaillierte Kennzahlen erforderlich. Nur 1 % der Befragten aus der Finanzdienstleistungsbranche gab an, dass sie nicht ermitteln können, ob sie die Ziele erreichen (im Vergleich zu 7 % in anderen Branchen). Auch wenn es sich nicht um eine signifikante Mehrheit handelt, nannten mehr der Cyber-Sicherheitsteams aus der Finanzbranche geeignete Methoden für die Strategiebewertung als andere Branchen, beispielsweise Risikoverwaltungsaktivitäten (66 % gegenüber 57 %) und durchschnittliche Behebungsdauer (52 % gegenüber 45 %).

Von Cyber-Kriminellen lernen

Bei Finanzdienstleistern, die seit langer Zeit in verschiedenen Arten von Märkten tätig sind, scheint das Missverhältnis bei den Anreizen im Cyber-Sicherheitsbereich am geringsten zu sein. Sie machen bereits den stärksten Gebrauch von Beratern und externen Sicherheits-Services, könnten aber möglicherweise externe Bedrohungsdaten und Sicherheitsinformationen stärker gewichten als ihre internen Briefings. Die Sicherheitsprozesse in diesen Teams scheinen gut heranzureifen, und sie sollten sich weiter auf integrierte Lösungen konzentrieren, anstatt auf überlappende Sicherheitsprodukte zu setzen. Möglicherweise müssen sie auch den Schwerpunkt von der Rufschädigung auf neue Bedrohungen und das Risiko tatsächlicher finanzieller Verluste verlagern, da Angreifer immer häufiger versuchen, direkt Gelder zu stehlen (z. B. Steigerung bei Mobile-Banking-Trojanern, Angriff auf die Zentralbank von Bangladesch über SWIFT, Kompromittierung von Konten der Tesco-Bank).

Kurzfassung

Lektionen aus dem kriminellen Markt	Krimineller Markt	Vorteile der Verteidiger
	Crime-as-a-Service	**Security-as-a-Service**
Marktkräfte nutzen	Der offene und dezentrale kriminelle Markt nutzt den Wettbewerb und die Marktpreise, um Einstiegshürden zu minimieren, Innovation zu fördern und erfolgreiche Projekte schnell zu skalieren.	Durch die intensivere Nutzung von Outsourcing und Open Contracting können die Kosten gesenkt, der Wettbewerb erhöht und die Einführung effektiver Sicherheitstechnologien sowie Vorgehensweisen gefördert werden.
	Konzentration auf veröffentlichte Schwachstellen	**Patch-Verfahren verbessern**
Offenlegung nutzen	Durch die Ausnutzung veröffentlichter Schwachstellen lassen sich kostenintensive Schwachstellenforschung und Exploit-Entwicklungen vermeiden. Wenn diese neu veröffentlichten Schwachstellen schnell in Angriffe integriert werden, können Angreifer ihre Gewinne maximieren, bis die gefährdeten Systeme gepatcht werden.	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.
	Offene Foren und Online-Werbung	**Informationsaustausch und Zusammenarbeit**
Transparenz erhöhen	Offene Foren und öffentliche Werbung erleichtern die Verbreitung erfolgreicher neuer Angriffe und krimineller Geschäftsmodelle sowie die breite Umsetzung empfohlener Vorgehensweisen.	Durch stärkeren Informationsaustausch und die damit verbundene Reduzierung doppelter Informationen lassen sich die Kosten für die Verteidiger senken. Zudem werden neue Technologien und Verfahren bekannt gemacht, mit deren Hilfe die Sicherheitslage erheblich verbessert wird.
	„Jeder mit Computer-Grundkenntnissen“	**Den weltweiten Fachkräftepool anzapfen**
Eintrittsbarrieren senken	Da formale Qualifikationen oder geografische Beschränkungen fehlen, können unterschätzte Fachkräfte aus der legitimen Wirtschaft vom kriminellen Ökosystem profitieren.	Durch die Nutzung eines breiteren Fachkräftepools – einschließlich junger und ausländischer Experten, können Unternehmen ihren Fachkräftemangel ausgleichen und Fachkräfte vom kriminellen Markt abziehen.
	Freiberuflermärkte belohnen Leistung	**Leistungsanreize**
Anreize anpassen	Auf dem kriminellen Freiberuflermarkt werden Beteiligte auf allen Ebenen und in allen Phasen der Angriffskette für hervorragende Leistung vom Markt belohnt und für schlechte Leistung bestraft.	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.

Wenn Sie weitere Informationen zur Diskrepanz der Anreize im Cyber-Sicherheitsbereich erhalten möchten (z. B. Aufschlüsselungen nach Land und Branche), laden Sie den vollständigen Bericht **Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity** (Manipulation des Spielfelds: Wie falsche Anreize gegen die Cyber-Sicherheit arbeiten) herunter.

intel Security

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/de