# Manipulation des Spielfelds: Wie falsche Anreize gegen die Cyber-Sicherheit arbeiten

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. Das liegt nicht daran, dass sie besser sind, sondern an der Diskrepanz zwischen den Anreizen bei Angreifern und Verteidigern. Um dieses Missverhältnis besser zu verstehen, befragten wir 800 Cyber-Sicherheitsexperten aus fünf großen 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

Während die meisten Cyber-Angriffe gegen Unternehmen mit Hierarchien und Bürokratie geführt werden, agieren Cyber-Kriminelle in einer heimlichen, aber offenen Welt mit selbständigen Akteuren und klaren Anreizen. Der Markt für Cyber-Kriminalität reagiert auf „Preissignale“ mit Innovation und neuen Produkten sowie Services, die rund um die Uhr angeboten werden. Wenn alte Funktionen unwirksam geworden sind, werden schon kurz darauf neue angeboten. Das fördert den dynamischen Wettbewerb sowie schnelle Innovationen auf den verschiedenen Bereichen des Cyber-kriminellen Marktes – von äußerst raffinierten, gut ausgestatteten Kriminellen und staatlich unterstützen Akteuren bis hin zu Hacktivisten und Cybercrime-as-a-Service-Käufern. Um diese Märkte besser zu verstehen, sprachen wir im Rahmen dieser Umfrage mit technischen Cyber-Sicherheitsexperten und Strafverfolgern.

Cyber-kriminelle Märkte sind stark spezialisiert, sodass die besten Akteure einen reichen Erfahrungsschatz anhäufen können. Die häufigsten Spezialisierungen sind Malware-Programmierer, Entwickler böswilliger Webseiten, Infrastrukturexperten, Exploit- und Schwachstellen-Hacker sowie Entwickler von Social-Engineering-Taktiken. Die Aufteilung der Gewinne unter diesen Spezialisten erfolgt entsprechend ihres Beitrags. Dynamischer Wettbewerb und Reputation verdrängen regelmäßig die weniger fähigen Kriminellen und lassen nur die besten an die Spitze.

Einer der stärksten Effekte dieses direkten Wettbewerbs- und Vergütungsmodells ist die Geschwindigkeit, mit der neue Schwachstellen oder Exploits genutzt werden: 42 % der Schwachstellen werden innerhalb von 30 Tagen nach ihrer Entdeckung von Kriminellen ausgenutzt. Als beispielsweise die Entwickler des einst dominierenden Exploit-Kits Angler (der laut einer Schätzung 82 % aller Exploit-Kit-Aktivitäten ausmachte) verhaftet wurden, wechselten dessen Nutzer innerhalb weniger Wochen zum Exploit-Kit Neutrino, um damit ihre Schaddaten zu verteilen. Die meisten Kriminellen betreiben wenig oder keine Forschung, sondern greifen auf die Arbeit der kriminellen Elite zurück, die häufig schnell über Untergrund-Webmärkte verbreitet wird. Außerdem profitieren sie von der großen Anzahl an Systemen, die erst nach langer Zeit gepatcht werden. Dies bietet den zusätzlichen Vorteil, dass die Kosten gering gehalten werden.

Geschichten aus der Welt der Cyber-Kriminalität implizieren, dass viele Hacker aus Russland und Osteuropa stammen würden. Das ist nicht ganz falsch und liegt vor allem an der hervorragenden Mathematik- und Informatik-Ausbildung, teilweise aber auch an fehlenden legitimen Berufschancen. Selbst Angestellte legitimer IT- und Telekommunikationsunternehmen in diesen Regionen arbeiten nebenberuflich als Hacker und werben auf ihren Facebook-Seiten offen mit ihren Dark Web-Identitäten. Die Cyber-Sicherheitsteams von Unternehmen können viel von diesen Untergrundmärkten lernen: Klare Anreize und Auszeichnungen können erhebliche positive Auswirkungen auf die Motivation sowie Effektivität haben.

## Diskrepanz zwischen Strategie und Umsetzung

Laut einem Großteil der Befragten stellt Cyber-Sicherheit jetzt das größte Risiko für Unternehmen dar. Mehr als 70 % aller Führungskräfte werden bei geschäftlichen Meetings über Cyber-Sicherheits-risiken informiert – insbesondere über Probleme, die noch vor sechs Jahren nicht einmal zu den Top 10 gezählt wurden. Fast alle (93 %) Umfrageteilnehmer gaben an, dass ihr Unternehmen über eine Cyber-Sicherheitsstrategie verfügt, die neue und vorhandene Bedrohungen abwehren soll.

An dieser Stelle tritt das erste Missverhältnis zutage. Viele Führungskräfte glauben, dass ihre Strategie im gesamten Unternehmen vollständig umgesetzt wurde, doch nur 30 % der Implementierer stimmen dieser Aussage zu. Für beide Gruppen ist die Anzahl der Kompromittierungen die wichtigste Kennzahl für die Effektivität der Cyber-Sicherheit – doch ab hier scheiden sich die Geister. Die Führungsetage setzt vielfach auf Wirksamkeitskennzahlen wie die Kosten für die Behebung einer Kompromittierung oder die Rendite von Cyber-Sicherheitsmaßnahmen. Die Implementierer konzentrieren sich mehr auf technische Maßnahmen wie Schwachstellen-Scans und Penetrationstests. Mehr als die Hälfte (54 %) der befragten Führungskräfte sorgt sich mehr um die Auswirkungen auf den Ruf des Unternehmens als um die tatsächlichen Folgen eines Cyber-Sicherheitsangriffs. Sorge bereitet die Tatsache, dass weniger als ein Drittel (32 %) dieser Experten glaubt, dass ein Cyber-Sicherheitszwischenfall zu Umsatz- oder Gewinnverlusten führt, was ihnen möglicherweise ein falsches Gefühl der Sicherheit verleiht.

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 (71 %) eine Sicherheitsplattform zur Integration vorhandener und neuer Technologien betreibt, gaben 64 % 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. Unsere Umfrage zeigt, dass es Cyber-Sicherheitsexperten nicht nur an Anreizen fehlt, sondern dass die Führungskräfte zudem stärker an die Effekte der bestehenden Anreize glauben als die Mitarbeiter, die sie damit motivieren möchten.

Fast die Hälfte der Implementierer berichtete, dass in ihrem Unternehmen keine Anreize geschaffen wurden. Von den Führungskräften gab nur ein Fünftel davon an, dass Anreize fehlen. Möglicherweise kennen die Mitarbeiter auf unteren Ebenen in der Organisationsstruktur die Leistungsanreize nicht, oder sie schätzen die Angebote als nicht effektiv ein. Erfreulicherweise bezeichneten sich 65 % der befragten Sicherheitsexperten als persönlich motiviert, die Cyber-Sicherheit ihres Unternehmens zu stärken.

Die Führungskräfte, die über vorhandene Anreize für Cyber-Sicherheitsexperten berichteten, nannten meist finanzielle Leistungen (60 %) oder Auszeichnungen (58 %). Bei den Nicht-Führungskräften berichteten 15 bis 25 % weniger Umfrageteilnehmer von solchen Anreizen. Auf die Frage nach den gewünschten Anreizen nannten die operativen Mitarbeiter fast genauso häufig finanzielle Leistungen (63 %) oder Auszeichnungen (62 %). Diese Zahlen passen zu anderen Studien, die zeigen, dass Weiterbildungsmöglichkeiten wertvoller sind als Boni.

## Von Cyber-Kriminellen lernen

Unternehmen können aus der Black Hat-Community lernen, um die bestehende Diskrepanz zu überwinden. Security-as-a-Service kann die zur Abwehr von Cybercrime-as-a-Service-Aktionen erforderliche Flexibilität bieten. Spezialisierte Berater können das interne Team bei Bedarf mit Fachwissen und speziellen Ressourcen unterstützen. Und Leistungsanreize sowie Auszeichnungen können Mitarbeiter zur Etablierung stärkerer Schutzmaßnahmen und kürzerer Patch-Zyklen motivieren. Sie müssen mit Experimenten herausfinden, welche Kennzahlen und Anreize für Ihr Unternehmen optimal sind. In jedem Fall kommen höhere Geschwindigkeit, mehr Schwerpunkt auf die Bedrohungsabwehr sowie bessere Sicherheit in greifbare Nähe.

## Kurzfassung

| Lektionen aus dem kriminellen Markt | Krimineller Markt | IT-Abteilungen |
|---|---|---|
| Marktkräfte nutzen | **Crime-as-a-Service**<br>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. | **Security-as-a-Service**<br>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. |
| Offenlegung nutzen | **Konzentration auf veröffentlichte Schwachstellen**<br>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. | **Patch-Verfahren verbessern**<br>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. |
| Transparenz erhöhen | **Offene Foren und Online-Werbung**<br>Offene Foren und öffentliche Werbung erleichtern die Verbreitung erfolgreicher neuer Angriffe und krimineller Geschäftsmodelle sowie die breite Umsetzung empfohlener Vorgehensweisen. | **Informationsaustausch und Zusammenarbeit**<br>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. |
| Eintrittsbarrieren senken | **„Jeder mit Computer-Grundkenntnissen“**<br>Da formale Qualifikationen oder geografische Beschränkungen fehlen, können unterschätzte Fachkräfte aus der legitimen Wirtschaft vom kriminellen Ökosystem profitieren. | **Den weltweiten Fachkräftepool anzapfen**<br>Durch die Nutzung eines breiteren Fachkräftepools – einschließlich junger und ausländischer ICT-Experten, die oft von Cyber-Kriminalität angezogen werden – können Unternehmen ihren Fachkräftemangel ausgleichen und Fachkräfte vom kriminellen Markt abziehen. |
| Anreize anpassen | **Freiberuflermärkte belohnen Leistung**<br>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. | **Leistungsanreize**<br>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 CSIS-Bericht (Center for Strategic and International Studies) vom März 2017 herunter: Manipulation des Spielfelds: Wie falsche Anreize gegen die Cyber-Sicherheit arbeiten.

intel Security

**McAfee. Part of Intel Security.**
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

 2480_0217_exe-misaligned-tilting-playing-field
März 2017