RESUMO EXECUTIVO

# Vantagem do ataque sobre a defesa: Incentivos divergentes — foco no setor de serviços financeiros

Há tempos os criminosos cibernéticos levam vantagem. Eles estão sempre encontrando novas maneiras de roubar dados, prejudicar o funcionamento de serviços e interromper o fluxo legítimo de informações. Não porque eles são melhores, mas devido a uma divergência nos incentivos que motivam atacantes e defensores. Para compreender melhor essa divergência de incentivos, consultamos 200 profissionais de TI no setor de serviços financeiros e comparamos suas respostas com as de 600 profissionais de TI de outros setores globais. O **relatório** identificou três divergências importantes de incentivos: entre as estruturas corporativas e o fluxo livre das organizações criminosas; entre a estratégia e a implementação; e entre executivos seniores e os encarregados pela implementação.

**Três níveis de incentivos divergentes colocam os defensores em desvantagem**

| | |
|---|---|
| Atacantes versus defensores | Os incentivos dos atacantes são determinados por um mercado fluido e descentralizado, o que os torna ágeis e de rápida adaptação, enquanto os defensores enfrentam restrições burocráticas e decorrentes de decisões tomadas de cima para baixo. |
| Estratégia versus implementação | Ainda que mais de 90% das organizações tenham uma estratégia de segurança cibernética, menos da metade delas implementaram completamente essas estratégias. |
| Executivos versus implementadores | Os executivos seniores que desenvolvem estratégias cibernéticas medem o sucesso de maneira diferente dos que implementam essas estratégias, o que limita a eficácia geral. |

## Estrutura corporativa versus organização criminosa

O setor de serviços financeiros há muito compreende os efeitos de incentivos claros e diretos. Os criminosos cibernéticos operam em um mundo obscuro, mas aberto, de livre iniciativa e motivações claras, e que promove competição dinâmica e inovação rápida. Isso leva a um alto grau de especialização, permitindo que os profissionais do crime cibernético se tornem muito bons em seu ofício e criando uma ampla rede de fornecedores e clientes. Informações são compartilhadas por uma ampla variedade de canais e novas vulnerabilidades são exploradas muito rapidamente. Mercados ativos tornam fácil encontrar clientes interessados e determinar o preço de novas informações e código.

Segundo essa pesquisa, as organizações de serviços financeiros são, dentre as consultadas, as mais adeptas a administrar um mercado aberto de informações de defesa cibernética. Elas são as mais propensas a compartilhar informações com outras organizações, incluindo parceiros (63% contra 52% dos entrevistados de setores não financeiros), consultores externos (49% contra 39%) e até mesmo concorrentes (26% contra 19%). Somente 7% dos consultados afirmaram não compartilhar quaisquer informações sobre ameaças cibernéticas, contra 14% em outros setores.

Essa atitude quanto ao compartilhamento influencia as fontes que as organizações de serviços financeiros utilizam ao tomar decisões sobre segurança cibernética. Elas são levemente mais propensas a utilizar informações compartilhadas por fontes externas do que organizações de outros setores. Isso inclui inteligência de fornecedores de segurança (63% contra 57%), consultores externos (51% contra 46%) e grupos setoriais (26% contra 22%). Talvez essas informações estejam sendo analisadas e resumidas por operadores, visto que os profissionais de serviços financeiros são muito mais propensos a utilizar instruções internas do que os profissionais de outras organizações (70% contra 61%).

O suporte a mercados abertos de segurança cibernética no setor de serviços financeiros vai além de informações sobre serviços e consultores. Eles são os mais propensos a aplicar uma parte significativa de seus orçamentos de segurança cibernética em consultores (49% contra 40% em organizações não financeiras) e um pouco mais propensos a aplicar dinheiro em serviços profissionais de monitoramento e resposta a incidentes (38% contra 34%). Essa abertura a informações e especialistas externos tem apresentado um impacto positivo sobre a eficácia da segurança.

## Falta de sintonia entre estratégia e implementação

De acordo com a maioria dos entrevistados, em todos os setores, a segurança cibernética é o maior risco enfrentado pelas organizações. Quase 80% das organizações de serviços financeiros estão informando seus diretores sobre os riscos de segurança cibernética na maioria ou em todas as reuniões de diretoria, contra 70% em outros setores. Embora quase todos (95%) os entrevistados do setor financeiro afirmem que suas organizações possuem uma estratégia de segurança cibernética para lidar com ameaças atuais e novas, os desafios surgem principalmente na implementação. Pouco mais da metade (51%) das organizações afirmam ter implementado plenamente sua estratégia de segurança cibernética, enquanto 8% nada implementaram.

Parte da divergência na implementação de estratégias de segurança pode ser decorrente de uma preocupação equivocada quanto à natureza dos riscos para os negócios. Na média, as lideranças e as diretorias dessas organizações de serviços financeiros estiveram mais preocupadas com danos à reputação da empresa (67%) do que com perdas de receita ou de lucros (50%). Considerando-se o surto recente em roubos diretos no setor financeiro, diferentes de perdas por fraude ligadas a números de cartões de crédito roubados, essa atitude pode estar proporcionando uma falsa sensação de segurança.

As organizações que estão implementando suas estratégias de segurança parecem ter um nível de maturidade de segurança acima da média. A tarefa mais prioritária dessas equipes de segurança foi a defesa proativa, seguida pela investigação de novas estratégias e soluções e, então, pela defesa reativa. Provavelmente mais importante é que elas dispenderam menos tempo em tarefas não relacionadas à segurança cibernética: apenas 8%, contra 14% em outros setores.

Em um setor que há muito é alvo de ataques cibernéticos, não surpreende que 73% dos profissionais de segurança de serviços financeiros tenham afirmado que seus orçamentos são adequados para a implementação de sua estratégia, contra apenas 58% nos outros setores. Somente um pequeno número de empresas do setor financeiro considerou que seu orçamento (4%) ou pessoal (9%) era insuficiente e que isso causaria problemas para a implementação de sua estratégia.

Outra divergência entre estratégia e implementação são os métodos usados para garantir que as medidas de defesa cibernética não exponham a organização a novos riscos. Embora a maioria das empresas financeiras (73%) afirme manter uma plataforma de segurança que integra tecnologias novas e existentes, um percentual semelhante (70%) reconhece que também adquire tecnologias de segurança sobrepostas. Essa pode parecer uma sólida estratégia de implementação, mas adotar tecnologias de segurança sobrepostas sem a devida integração pode criar lacunas de segurança. A diversidade de configurações e sistemas de monitoramento acabam dificultando a criação e a imposição de políticas de segurança consistentes.

## Divergências de incentivos entre executivos seniores e implementadores

As empreitadas dos criminosos cibernéticos rendem incentivos diretos, na forma de dinheiro, publicidade ou constrangimento de seus alvos. As equipes de segurança cibernética de serviços financeiros são as mais propensas a ter incentivos como reconhecimento (55% contra 48% em outros setores) e bônus (53% contra 43%). Somente 9% dos entrevistados afirmaram não haver incentivos no momento, em comparação com 21% em outros setores. O principal desestímulo contra comportamentos arriscados para a segurança cibernética por parte de funcionários é a ameaça de processos jurídicos (69% contra 59%). Além disso, 56% dos profissionais de TI do setor financeiro afirmam que a implementação da estratégia está incorporada em suas análises de desempenho individuais, contra 46% dos profissionais de outros setores.

Determinar se a estratégia está atingindo os objetivos requer um conjunto de parâmetros suficientemente detalhados. Somente 1% dos entrevistados de serviços financeiros afirmaram que não puderam determinar se estavam atingindo os objetivos, contra 7% em outros setores. Embora não sejam uma maioria significativa, mais equipes de segurança cibernética disseram ter métodos apropriados para avaliação de estratégias no setor financeiro do que em outros setores, como atividades de gerenciamento de risco (66% contra 57%) e tempo médio até a resolução (52% contra 45%).

## A escola do crime cibernético

As empresas de serviços financeiros, com seu longo histórico de operar em vários tipos de mercados, parecem ter a menor divergência de incentivos em segurança cibernética. Elas já são as que mais utilizam consultores e serviços de segurança externos, mas poderiam dar ainda mais prioridade a inteligência contra ameaças e informações de segurança externas em relação a suas instruções internas. Os processos de segurança dessas equipes parecem estar amadurecendo bem e devem continuar a se concentrar em soluções integradas em vez de depender de produtos de segurança sobrepostos. Elas talvez precisem também aumentar seu foco em novas ameaças e no risco de perda financeira real em vez de perda de reputação, pois os atacantes estão, cada vez mais, tentando roubar fundos diretamente (como demonstra o aumento em cavalos de Troia nos serviços bancários móveis, o roubo SWIFT/Bangladesh e as contas comprometidas do Tesco Bank).

| Lições do mercado do crime | Mercado do crime | Vantagem dos defensores |
|---|---|---|
| **Aproveitamento das forças do mercado** | **Crime como serviço** | **Segurança como serviço** |
| | A natureza aberta e descentralizada do mercado do crime se aproveita da concorrência e dos preços do mercado para minimizar barreiras de entrada, promover a inovação e ajudar a ampliar rapidamente a escala de suas empreitadas. | Um maior uso de terceirização e contratos abertos pode ajudar a reduzir custos, aumentar a concorrência e facilitar a ampla adoção de tecnologias e práticas eficazes de segurança. |
| **Divulgação pública de vulnerabilidades** | **Visar vulnerabilidades divulgadas publicamente** | **Melhorar as práticas de aplicação de correções** |
| | A exploração de vulnerabilidades divulgadas evita o alto custo da pesquisa de vulnerabilidades e do desenvolvimento de explorações. As novas vulnerabilidades divulgadas são rapidamente incorporadas aos ataques para maximizar seu valor antes que os defensores apliquem correções. | Responder com mais rapidez à divulgação de vulnerabilidades públicas através de práticas aprimoradas de aplicação de correções e da substituição mais veloz de sistemas legados pode aumentar a segurança e elevar os custos para os atacantes. |
| **Aumento da transparência** | **Fóruns abertos e publicidade on-line** | **Compartilhamento de informações e colaboração** |
| | Os fóruns abertos e a publicidade propiciam a proliferação de modelos de negócios criminosos e novos ataques bem-sucedidos, bem como a ampla adoção das melhores práticas. | Expandir o compartilhamento de informações pode ajudar a reduzir os custos para os defensores ao evitar o trabalho duplicado, além de divulgar novas tecnologias e práticas que proporcionem melhorias significativas na segurança. |
| **Redução dos obstáculos à entrada** | **"Qualquer usuário de computador"** | **Aproveitar de uma reserva global de talentos** |
| | O ecossistema criminoso dispensa qualificações formais e ignora limites geográficos. Nesse ecossistema, indivíduos qualificados e pouco valorizados no sistema econômico legítimo podem ter seu valor maximizado. | Recorrer a uma reserva mais ampla, multinacional e demograficamente diversificada de pessoas qualificadas pode ajudar as empresas a preencher lacunas de habilidades cibernéticas e a retirar talentos do mercado do crime. |
| **Convergência de incentivos** | **Mercados de freelancers premiam o desempenho** | **Incentivos para o desempenho** |
| | No mercado freelancer do crime, operadores de todos os níveis e áreas funcionais da cadeia de ataque são premiados pelo mercado por sua excelência e penalizados por um desempenho ruim. | Para promover a convergência dos incentivos desde a equipe de liderança até os operadores, incentivos como prêmios e bônus devem ser oferecidos aos funcionários e gerentes que apresentarem bons resultados de segurança. |

## Saiba Mais

Para obter mais detalhes sobre a divergência de incentivos na segurança cibernética, incluindo análises separadas por país e mercado vertical, faça o download do relatório completo: **Vantagem do ataque sobre a defesa: Divergência de incentivos**.

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br