Desequilibrando o jogo: como incentivos divergentes prejudicam a segurança cibernética

Há tempos os criminosos cibernéticos têm a vantagem. Eles estão sempre encontrando novas maneiras de roubar dados, prejudicar o funcionamento de serviços e interromper o fluxo legítimo de informações. Porém, isso não se deve a uma suposta superioridade desses atacantes, mas sim à divergência dos incentivos que motivam atacantes e defensores. Para entender melhor essas divergências, entrevistamos 800 profissionais de segurança cibernética nos cinco setores mais importantes do mercado. 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 divergências de incentivos deixam os defensores em desvantagem

Atacantes versus defensores	Os incentivos para os atacantes derivam de um mercado fluido e descentralizado, que confere a eles agilidade e rapidez de adaptação, enquanto os defensores se veem presos à burocracia e à cadeia vertical de comando.
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 criam as estratégias cibernéticas e os responsáveis por implementá-las na prática têm métricas diferentes para avaliar o sucesso, o que acaba limitando sua eficácia.

Estrutura corporativa versus organização criminosa

Enquanto o alvo da maioria dos ataques cibernéticos é algum tipo de organização com hierarquia e burocracia, os criminosos cibernéticos operam em um mundo sombrio, porém aberto, de freelancers e incentivos claramente definidos. O mercado de crime cibernético faz uma "leitura de preços" e responde com novos produtos e serviços diariamente. Quando recursos antigos perdem a eficácia, outros são rapidamente disponibilizados on-line. Isso permite uma competição dinâmica e acelera a inovação entre os diversos componentes do mercado de crime cibernético, que abrange desde criminosos altamente sofisticados e bem equipados (por vezes até patrocinados por países) até hacktivistas e consumidores de crime cibernético como serviço. Neste estudo, entrevistamos especialistas técnicos em segurança cibernética e autoridades policiais para entender melhor esses mercados.

O mercado cibernético é altamente especializado, e seus integrantes mais dedicados podem desenvolver grandes habilidades em suas respectivas áreas. Os especialistas encontrados com mais frequência são programadores de malware, designers de sites maliciosos, especialistas em infraestrutura, hackers de explorações e vulnerabilidades e farsantes que esquematizam golpes de engenharia social. Os lucros são distribuídos entre os especialistas de acordo com suas contribuições. O dinamismo da concorrência e a reputação conquistada regulam continuamente esse mercado, rebaixando os criminosos menos talentosos e elevando os melhores ao topo.

Um dos principais efeitos desse modelo de concorrência direta e compensação é a velocidade com que novas vulnerabilidades e explorações são utilizadas. 42% das vulnerabilidades são exploradas por criminosos em até 30 dias da data de sua divulgação. Um exemplo é o kit de exploração Angler. Segundo estimativas, ele chegou a dominar o mercado, respondendo por 82% da atividade de kits de exploração. Quando seus desenvolvedores foram presos, bastaram algumas semanas para que os atacantes que o utilizavam adotassem um substituto, o kit de exploração Neutrino, como veículo para suas cargas virais. A maioria dos criminosos investe pouco em pesquisa ou não realiza pesquisa alguma. Eles se aproveitam do trabalho de criminosos de elite, distribuído rapidamente nos mercados negros da Web, e da grande quantidade de sistemas que demoram muito para receber correções. Essa abordagem tem a vantagem de ser de baixo custo.

Alguns casos notórios de crimes cibernéticos podem deixar a impressão de que muitos criminosos vêm da Rússia e do Leste Europeu. Isso não deixa de ser verdade, especialmente devido aos programas avançados de matemática e ciência da computação disponíveis e à falta de oportunidades legítimas de emprego. Mesmo funcionários legítimos de empresas de TI e telecomunicações nessas regiões muitas vezes levam uma vida dupla como criminosos. Em alguns casos, eles chegam a postar abertamente suas identidades do mercado negro da Web em seus perfis do Facebook. As equipes corporativas de defesa e segurança cibernética podem aprender muito com esses mercados negros. Um conjunto bem definido de incentivos e a recompensa na forma de reputação podem ter um efeito positivo e considerável sobre a atitude e a eficácia de alguém.

Falta de sintonia entre estratégia e implementação

De acordo com a maioria dos entrevistados, a segurança cibernética é o maior risco enfrentado pelas organizações. Mais de 70% dos diretores recebem informações sobre os riscos à segurança cibernética nas reuniões de conselho, com destaque particular para desafios que sequer figuravam entre os dez maiores há apenas seis anos. Quase todos (93%) afirmam que suas organizações têm uma estratégia de segurança cibernética para lidar com ameaças novas e existentes.

É nesse ponto que surge a primeira divergência. Muitos executivos acreditam que sua estratégia foi totalmente implementada na organização inteira, mas apenas 30% dos operadores corroboram essa declaração. Para ambos os grupos, a métrica principal da eficácia da segurança cibernética é a quantidade de violações, mas além disso não há consenso. Os executivos seniores se apoiam mais nas métricas de desempenho, como o custo de recuperação de uma violação ou o retorno dos gastos em segurança cibernética. Já os operadores recorrem às medidas técnicas, como varreduras de vulnerabilidades e testes de penetração. Mais da metade (54%) dos executivos entrevistados estão mais preocupados com o impacto sobre a reputação do que com os efeitos práticos de um incidente de segurança cibernética. Um fato preocupante: menos de um terço (32%) desses profissionais acreditam que um incidente de segurança cibernética resulte em perda de receita ou lucro, o que pode transmitir uma falsa sensação de segurança.

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 dos entrevistados (71%) afirmem manter uma plataforma de segurança que integra tecnologias novas e existentes, 64% reconhecem que também adquirem tecnologias de segurança que se sobrepõem. 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: dinheiro, publicidade ou o constrangimento de seus alvos. De acordo com nossa pesquisa, os profissionais de segurança cibernética precisam de mais incentivos, mas o grau de confiança dos executivos nos incentivos que oferecem atualmente não condiz com a satisfação da equipe operacional que eles estão tentando motivar.

Quase metade dos operadores entrevistados afirmam que suas organizações não oferecem incentivos. Esse número é cinco vezes maior que a quantidade de profissionais em posição de liderança que afirmam oferecer esses incentivos. Talvez os funcionários mais próximos à base da estrutura da organização desconheçam a existência dos incentivos que recompensam o desempenho, ou talvez não os considerem eficazes. Felizmente, 65% dos profissionais entrevistados afirmam estar pessoalmente motivados a fortalecer a defesa e a segurança cibernética da organização.

Os executivos que afirmam oferecer incentivos para seus profissionais de segurança cibernética se mostraram mais propensos a identificar ofertas de compensação financeira (60%) ou reconhecimento (58%). Porém, a quantidade de profissionais não executivos que reconhecem esses mesmos incentivos é de 15 a 25% inferior. Quando perguntados sobre quais incentivos gostariam de receber, os operadores deram quase a mesma importância à compensação financeira (63%) e a reconhecimento ou prêmios (62%). Esse resultado comprova o que outros estudos já indicavam: que as oportunidades de desenvolvimento profissional são tão ou mais valiosas do que os bônus.

A escola do crime cibernético

As organizações podem aprender a eliminar essas divergências com o exemplo da comunidade de criminosos. A segurança como serviço pode oferecer a flexibilidade de que você precisa para combater as operações do crime cibernético como serviço. Consultores especializados podem capacitar suas equipes internas com experiência e recursos direcionados quando necessário. Os incentivos de desempenho e reconhecimento podem contribuir para defesas mais fortes e acelerar os ciclos de correções. É necessário experimentar para definir a combinação ideal de métricas e incentivos para cada organização, mas é possível aumentar a velocidade e o foco das defesas e obter resultados de segurança melhores.

Resumo executivo

Lições do mercado do crime	Mercado do crime	Contraparte dos defensores
Aproveitamento das forças do mercado	**Crime 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.	**Segurança como serviço** 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.
Uso da divulgação pública de vulnerabilidades	**Ataque às vulnerabilidade divulgadas publicamente** 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.	**Melhores práticas de aplicação de 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.
Mais transparência	**Fóruns abertos e publicidade on-line** Os fóruns abertos e a publicidade on-line facilitam o sucesso e a proliferação de novos ataques e modelos de negócios criminosos, além de disseminarem a ampla adoção de melhores práticas.	**Compartilhamento de informações e colaboração** Expandir o compartilhamento de informações pode ajudar a reduzir os custos para os defensores. Dessa forma, é possível evitar trabalho duplicado e espalhar notícias sobre novas tecnologias e práticas que ofereçam melhorias de segurança consideráveis.
Barreiras de entrada menores	**"Qualquer usuário de computador"** 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.	**Uso de um pool global de pessoal qualificado** Recorrer a um amplo pool de indivíduos qualificados, incluindo jovens e estrangeiros especializados em TIC (que muitas vezes são atraídos pelo crime cibernético), pode ajudar as empresas a preencher lacunas de habilidades e retirar talentos do mercado do crime.
Convergência de incentivos	**Mercados de freelancers premiam 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.	**Incentivos ao desempenho** 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.

Para obter mais detalhes sobre a divergência de incentivos na segurança cibernética, incluindo análises separadas por país e mercado vertical, faça download do relatório completo: Desequilibrando o jogo: como incentivos divergentes prejudicam a segurança cibernética, Center for Strategic and International Studies (CSIS), março de 2017.

intel Security

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16º andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com