Divergência de incentivos

Apoiados por forças do mercado, os criminosos cibernéticos estão à frente dos defensores.

Três dimensões de divergências

As divergências entre o crime cibernético e o trabalho das equipes de resposta são complexas. Elas ocorrem em vários níveis: entre atacantes e defensores, entre a estratégia e a implementação e entre executivos e implementadores de uma empresa.

Atacantes

Ágeis e rápidos

Os incentivos para os atacantes derivam de um mercado fluido e descentralizado, que confere a eles agilidade e rapidez de adaptação.

X

Defensores

Presos à burocracia

Os defensores se veem presos à burocracia e à cadeia vertical de comando.

Estratégia

90%

Mais de 90% das organizações têm uma estratégia de segurança cibernética.

X

Implementação

Menos de 50%

Menos da metade das organizações implementaram completamente suas estratégias.

Executivos

Métricas de sucesso diferentes

Os executivos seniores que criam estratégias cibernéticas têm métricas de sucesso diferentes dos implementadores.

X

Implementadores

Eficácia limitada

Os implementadores que põem a estratégia em prática sofrem com as limitações impostas pelos executivos seniores.

O estado de divergência

As empresas nunca se preocuparam tanto com o risco de segurança cibernética, mas há falhas no gerenciamento de riscos e nos incentivos à equipe, além de problemas inerentes à forma como os atacantes operam em oposição ao método de gerenciamento dos defensores.

76%

76 por cento dos entrevistados afirmam que o risco de segurança cibernética é um dos três maiores fatores de risco.

54%

54 por cento dos executivos entrevistados estão mais preocupados com o impacto sobre a reputação do que com os efeitos práticos de um incidente de segurança cibernética.

83%

83 por cento dos entrevistados continuam relatando danos causados por violações de segurança cibernética.

5× mais propensos

Os operadores se mostraram cinco vezes mais propensos a relatar que não existem incentivos à segurança cibernética.

Ideias/Dinheiro

Criminosos cibernéticos de alto nível roubam ideias; criminosos menores roubam dinheiro.

51%

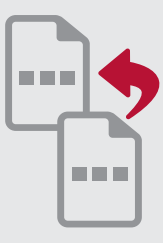
Apenas 51 por cento dos especialistas russos de TI entrevistados conseguiram emprego no setor legítimo de TI.

42%

42 por cento das vulnerabilidades são exploradas por criminosos em até 30 dias da data de sua divulgação.

Lições do mercado do crime

Mercado do crime versus contraparte dos defensores

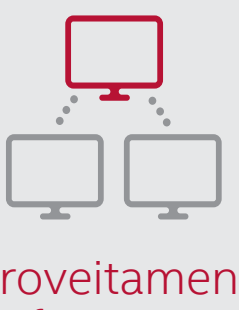


Mais transparência

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.

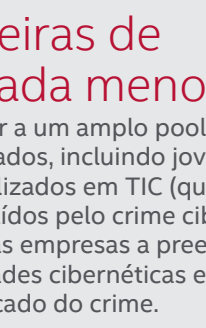
Convergência de incentivos

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.



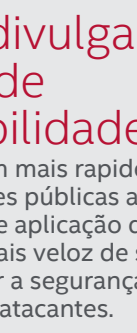
Aproveitamento das forças do mercado

A terceirização e os contratos abertos podem ajudar a reduzir custos, aumentar a concorrência e promover a adoção de melhores práticas inovadoras.



Barreiras de entrada menores

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 cibernéticas e retirar talentos do mercado do crime.



Uso da divulgação pública de vulnerabilidades

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.

Acabe com as divergências. Aprenda com os atacantes. Adapte-se e prospere.

Visite www.mcafee.com/misaligned para ler o relatório completo.

intel Security

2504_0217_info-misaligned-incentives-cybercriminals-defenders