A necessidade de um novo avanço em Cibersegurança

Por: Ricardo Villadiego

Índice

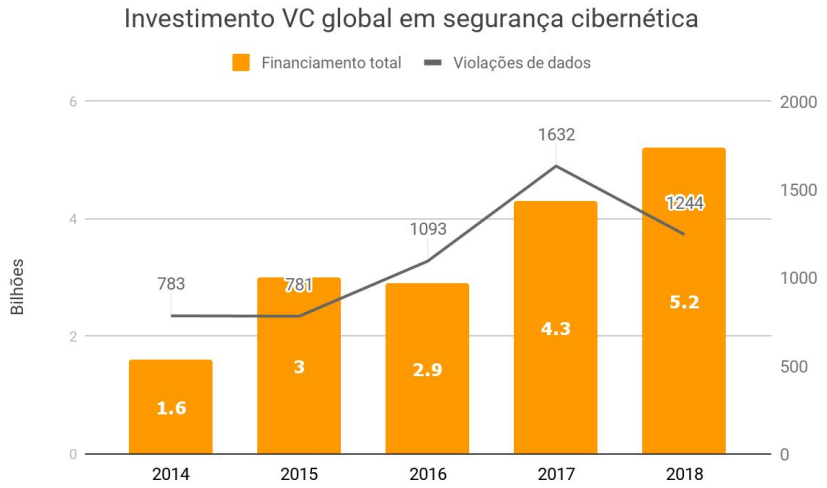
Sumário Executivo

Este documento compara o nível de investimento de capital de risco (VC) na indústria de segurança cibernética e as violações registradas nos Estados Unidos. O resultado desta comparação encoraja os profissionais de segurança a analisar as razões para o baixo desempenho do setor no que diz respeito à proteção, apesar do alto investimento. O presente artigo avalia a natureza reativa da indústria, a complexidade do processo de tomada de decisões e as consequências desses elementos para as organizações. A falta de um ciclo de feedback nas arquiteturas de segurança cibernética também é analisada. Finalmente, discute-se um novo avanço em Cibersegurança que o conceito de **continuous compromise assessment™** (análise contínua de comprometimentos) representa, ao implementar um ciclo de feedback extremamente necessário nas arquiteturas de segurança corporativas.

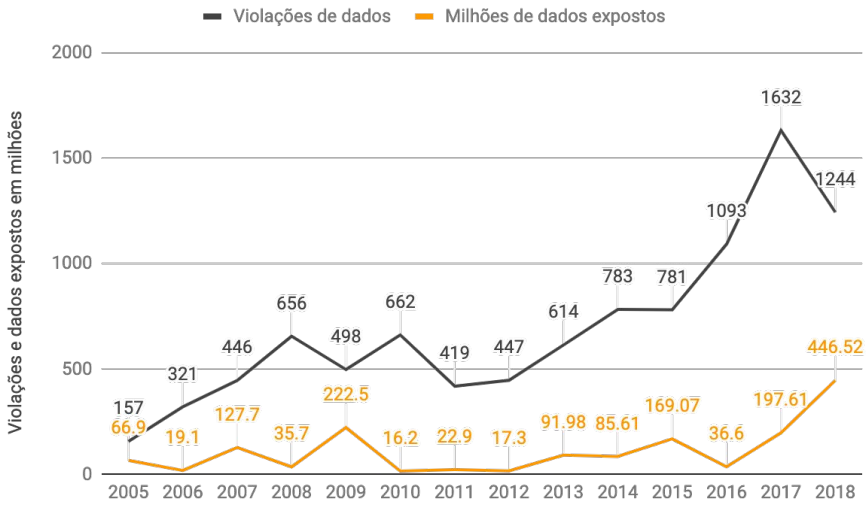
O estado da segurança cibernética

A indústria de segurança cibernética está super aquecida. Para começar, os investidores de capital de risco têm investido um volume sem precedentes de capital no crescimento e no financiamento de novos empreendimentos. Entre 2014 e 2018, foram investidos assombrosos US$ 17,1 bilhões, de acordo com a strategic cyber ventures[1].

Entre 2014 e 2018, a indústria de CR empregou assombrosos US$ 17,1 bilhões



Ainda assim, durante o mesmo período, o número de violações de segurança e a quantidade de dados expostos aumentou exponencialmente em uma crise de escala global. De acordo com o Centro de Recursos relativos a Roubo de Identidade dos EUA[2], o número de violações de dados cresceu de 783 em 2014 (o que já é assustador) para um pico de 1.632 em 2017.



[1] Investimento de Capital de Risco em Segurança Cibernética 2018: https://scvgroup.net/2018-cybersecurity-venture-capital-investment/
[2] Relatório de Violação de Dados do Centro de Recursos para Roubo de Identidade 2018

O mesmo estudo aponta que o problema afeta todos os setores.

Número de violações de dados nos EUA

Ano	Bancário/ Créditos/ Financeiro	Corporativo	Acadêmico	Governamental/ Militar	Médico/ Saúde	Total
2013	35	194	54	60	271	614
2014	38	263	57	91	332	781
2015	71	312	58	63	275	779
2016	51	497	97	72	373	1090
2017	134	907	128	79	384	1632
2018	135	572	77	100	367	1251

Investimento não significa necessaria-mente proteção

É falso afirmar que organizações submetidas a normas mais rigorosas - como no setor bancário - têm um melhor desempenho em segurança cibernética do que outras menos regulamentadas, ou que as indústrias que investem mais fortemente em segurança sofrem menos violações de dados. É hora de aceitar que investimento não se traduz necessariamente em proteção.

Durante anos, fomos condicionados a definir sucesso em termos de investimento de tempo e dinheiro. Em segurança cibernética, esta fórmula bem comprovada não está produzindo os resultados que deveríamos esperar de uma indústria que recebe um volume tão elevado de investimentos.

A fórmula universal (sucesso = tempo + dinheiro) funciona na maioria das áreas da vida, dos esportes à chegada do homem à lua. Ela tem produzido resultados impressionantes na área saúde. Em agosto de 2019, a OMS e o Instituto Nacional de Alergias e Doenças Infecciosas dos EUA anunciaram a cura para o vírus Ebola, e tem havido um progresso significativo em direção a uma cura para o vírus HIV, uma doença que significava sentença de morte há 20 anos.

No entanto, a perspectiva da segurança cibernética é decepcionante, e a guerra cibernética pode acabar sendo perdida. Outra indicação disto é uma marca icônica como a Capital One anunciar ser vítima de uma violação massiva. O caminho que nos levou a este ponto merece ser explorado.

Como chegamos aqui?

Há quatro fatores principais que trouxeram a indústria ao seu estado atual de comprometimento e incerteza:

a. **Ameaças em constante evolução** geram um número infinito de vulnerabilidades que as empresas devem tentar remediar. As tecnologias de segurança cibernética continuam a ser, em sua maioria, reativas, o que leva a um "ciclo cibernético" vicioso de atacantes que varrem redes, desenvolvem exploits e atacam sistemas e defensores que detectam ataques, analisam exploits e consertam sistemas.

b. **O capital ilimitado** que jorra na indústria alimenta fornecedores de soluções que adotam a abordagem “detectar para depois mitigar”. Os resultados são tecnologias no mercado que não estão prontas para o “horário nobre”, inerentemente instáveis e que se tornam obsoletas logo após a implantação sem nunca comprovar se cumpriram a sua promessa original.

c. Como resultado de a.) e b.), as arquiteturas de defesa cibernética **tornaram-se mais complexas**, empilhando uma avalanche de fornecedores negligentes quanto às capacidades de gestão e monitoramento e que acrescentam pouca proteção progressiva ao sistema. A complexidade e o custo a ela associados criam uma falsa sensação de segurança, especialmente nos níveis superiores na organização.

d. A sociedade atual está psicologicamente fixada em promessas de gratificação instantânea. Na hora de lidar com problemas, isso se traduz na **busca pela solução mágica** que vá resolver tudo. Este comportamento e a incapacidade de cogitar a ideia de sofrer uma violação de dados têm levado profissionais e tomadores de decisão a aceitar a conduta atual da inovação em segurança cibernética: detectar para então mitigar.

A complexidade e os custos envolvidos criam uma falsa sensação de segurança

Para piorar a situação, muitas das soluções e arquiteturas de segurança cibernética atuais funcionam basicamente como um sistema de circuito aberto. Isto significa que os sistemas não consideram os aspectos positivos dos sistemas de circuito fechado, em que o resultado ideal (neste caso, comprometimento zero) é medido continuamente para garantir que alterações sejam aplicadas ao sistema (a arquitetura de segurança cibernética).

É impossível obter resultados diferentes fazendo sempre a mesma coisa. Para interromper o ciclo cibernético, a cibersegurança precisa de uma mudança fundamental no sentido de aplicar a teoria de controle para medir continuamente o valor de referência. Para uma determinada organização, é necessário que este valor seja **“comprometimento zero”**. Qualquer desvio do valor de referência deve ser prontamente identificado e mitigado por meio do ajuste da arquitetura de segurança cibernética.

Tomando as decisões certas

As organizações devem decidir pela estratégia de defesa correta para seu modelo de negócios, setor e stakeholders. Isso significa adotar uma abordagem eficiente, efetiva e proativa e manter as taxas de falhas em ordem. No entanto, à luz do aumento significativo das violações na última década, será que estamos tomando as decisões corretas?

Um estudo recente[3] afirmou que os desafios para construir capacidades de segurança cibernética nas organizações têm origem em concepções erradas sobre dois aspectos complexos que têm recebido pouca atenção:

- **A incerteza em torno dos incidentes cibernéticos:** É um desafio para os profissionais de segurança e risco aplicar teorias convencionais de tomada de decisões a investimentos em segurança cibernética devido à dificuldade de medir o impacto de um incidente cibernético hipotético. Consequentemente, eles acabam tomando decisões e fazendo julgamentos com base na sua experiência e nos seus conhecimentos sobre a probabilidade de acontecimentos incertos.

  A incerteza e a gravidade das ameaças cibernéticas, combinadas com mudanças frequentes nas tecnologias adquiridas e a introdução de novas vulnerabilidades torna difícil para os tomadores de decisão alocar recursos para investimentos em segurança cibernética de maneira eficiente. A presença crescente de ameaças cibernéticas criou um ambiente que foca em defesas técnicas, mas negligencia o senso econômico dos investimentos. Se uma empresa não sofre ataques cibernéticos — mais precisamente, não detecta ataques cibernéticos — a motivação para investir em segurança cibernética é baixa. Por esta razão, muitos profissionais da indústria com frequência não conseguem prever corretamente os riscos cibernéticos. Não surpreende o fato de haver uma distância enorme entre a percepção que as organizações têm do estado da sua segurança cibernética e o quadro real. Como resultado, elas podem acabar subestimando a frequência com a qual os incidentes ocorrem e o tempo que as soluções de segurança cibernética levam para trabalhar, prever, detectar e responder a um incidente.

- **Atrasos na formação de capacidades de segurança cibernéticas:** A cibersegurança torna-se cada vez mais complexa. Como outros modelos complexos, seus sistemas incluem potenciais atrasos. Numa organização reativa, em que os gestores só começam a investir no desenvolvimento de capacidades de segurança cibernética após a detecção de um ataque, os sistemas de informação não conseguirão se recuperar devidamente a tempo e ficarão vulneráveis. Como o Rei Henrique VIII da Inglaterra disse uma vez: "De todas as perdas, o tempo é a mais irrecuperável, pois jamais pode ser resgatado". Se as organizações pudessem evitar esta abordagem reativa, combater o impulso de cair na armadilha do curto prazo e agir de forma decisiva para implementar as capacidades de segurança cibernética de que precisam, elas estariam numa posição melhor.

Se uma empresa não sofre ataques cibernéticos — mais precisamente, não detecta ataques cibernéticos — a motivação para investir em segurança cibernética é baixa.

[3] Tomada de decisões e preconceitos no desenvolvimento de capacidades de segurança cibernética: resultados de um experimento de jogo de simulação.

Um novo avanço em Cibersegurança

A crise global da segurança cibernética é um problema que deve ser resolvido ou melhorar significativamente no curto prazo. Os investidores de capital de risco continuam (corretamente) a injetar capital no setor. Com um cenário de ameaças que pode - e irá - evoluir infinitamente, abordar o problema é cada vez mais vital.

As organizações devem considerar que os criminosos digitais já conseguiram entrar

O foco deve estar na formação de capacidades de segurança cibernética que revolucionem fundamentalmente o estado atual do setor. Precisamos repensar o nosso paradigma de segurança, nos afastando do antigo modelo baseado em tentar manter os adversários fora das redes. As organizações devem considerar que os criminosos digitais já conseguiram entrar. Isto é conhecido nos círculos governamentais dos EUA como assumption of breach (presunção de violação). Deborah Hayden, da Direção de Garantia de Informação da NSA, afirmou isso já em dezembro de 2010.[4]

A indústria carece de um processo real que proporcione certeza em torno dos incidentes - um dos dois motores para tomar as decisões corretas em matéria de cibersegurança. Na Lumu, chamamos este processo de ***continuous compromise assessment™*** (avaliação contínua de comprometimentos).

Para entender melhor este conceito, é interessante revisar a Cyber Kill Chain[5], um modelo para identificação e prevenção de atividades de intrusão cibernética. Ele aponta as etapas que os adversários devem concluir para alcançar seus objetivos, como apresentado no gráfico abaixo.

Um olhar mais atento sobre as diferentes fases das diversas variantes da Cyber Kill Chain revela um denominador comum que possibilita as ações dos adversários: **o acesso à rede**. O tráfego na rede é o ponto de partida para iluminar as ameaças. Quase todas elas devem primeiro ser baixadas e depois comunicam-se de volta com o seu C&C (comando e controle) para fornecer dados de valor para os atacantes.

A habilidade de coletar tráfego de rede para iluminar ameaças pode ser o **ciclo de feedback** que muitos pesquisadores e acadêmicos de segurança cibernética têm idealizado há décadas

A habilidade de coletar tráfego de rede para iluminar ameaças pode ser o **ciclo de feedback** que muitos pesquisadores e acadêmicos de segurança cibernética têm idealizado há décadas. Mesmo com os avanços em largura de banda e armazenamento, a coleta do tráfego de rede pode representar custos proibitivos para as organizações. O problema evolui para a questão de como coletar sinais do tráfego de rede de maneira que represente com precisão o resumo das "conversas" dentro de uma organização.

[4] Presunção de violação: O novo paradigma da segurança por Jeffrey Carr
[5] Desenvolvido por Lockheed Martin
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Em seu livro *Secrets and Lies*, *("Segurança. Com - Segredos e Mentiras Sobre a Proteção na Vida Digital")*, Bruce Schneier afirma que "muitas vezes, os padrões de comunicação são tão importantes quanto o conteúdo da comunicação." Por exemplo, o simples fato de Alice telefonar todas as semanas para um terrorista conhecido é mais importante do que os detalhes da sua conversa. Juntando isso aos passos associados à Cyber Kill Chain, podemos perceber facilmente que o processo envolvido no comprometimento de um dispositivo e uma rede fará com que esse dispositivo e essa rede se comportem de forma diferente. Aqui estão alguns passos para ilustrar o processo:

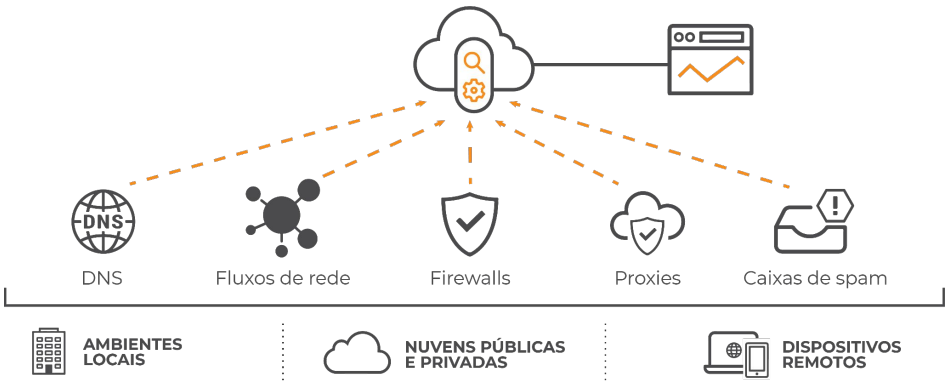
- O usuário final que o adversário está querendo atacar apontará o seu dispositivo para um novo **host**.
- Se o ataque for bem-sucedido, o dispositivo tentará conectar-se à infraestrutura do adversário **(C&C)** procurando instruções e/ou exfiltrando informações.
- Em ataques mais sofisticados, o adversário precisará conseguir privilégios de acesso. Para isso, o dispositivo comprometido tentará comunicar-se com dispositivos próximos e/ou com alvos valiosos dentro da organização, agora comprometida. Isto é um claro sinal de **movimentação lateral.**
- À medida que o adversário for conquistando novas vítimas, mais dispositivos tentarão conectar-se com a sua infraestrutura.

Uma análise mais aprofundada dos passos descritos leva aos elementos-chave dos metadados do tráfego de rede para uma representação precisa do resumo das conversas dentro da organização, tal como descrito na tabela seguinte:

Metadado de rede	Por que é importante
Consultas DNS	A coleta de consultas DNS fornece o contexto das tentativas de conexões dos dispositivos da organização com a infraestrutura adversária.
Fluxos de rede	Entre outros comportamentos maliciosos, os fluxos de rede fornecem informações esclarecedoras sobre os dispositivos de uma organização que estão sob controle de adversários e tentam movimentar-se lateralmente.
Logs de acesso de proxies do perímetro ou firewalls	Nos casos em que os ataques evitam a resolução do domínio, os vestígios do contato do adversário estarão nos logs de acesso de firewalls ou proxies, dependendo da configuração da rede da organização.
Caixa de spam	O correio eletrônico é o método preferido pelos atacantes para distribuir exploits entre os usuários finais da organização[6]. A análise da caixa de spam fornece informações sobre o tipo de ataque que a organização está recebendo, mas, ainda mais importante, se os usuários finais estão acessando esses ataques e se a organização está com um alto risco de comprometimento.

[6] Relatório de Violações de Dados da Verizon de 2019.

Sinalizar o tráfego desta maneira em vez de fazer uma captura completa é ideal, pois envolve apenas uma fração minúscula do total do tráfego de rede. Mesmo assim, ainda é possível identificar o nível de comprometimento da organização.



Técnicas específicas foram desenvolvidas para facilitar a coleta de dados e minimizar o atrito nos diversos ambientes que compreendem uma rede hoje em dia.

Um outro problema a ser resolvido é como tornar esse processo contínuo. A coleta e o processamento destes logs para um período específico são viáveis, mas desafiadores. As organizações podem ficar decepcionadas rapidamente com a alta complexidade na coleta e no processamento de dados, ainda que usem ferramentas que prometem tratar pelo menos alguns destes logs-chave, como SIEM ou coletores de fluxos de rede.

Para resolver esta última questão, é necessário um processo preciso, contínuo e confiável, desde a coleta até a iluminação, como mostrado na imagem a seguir.

Somente após a implementação de um processo contínuo podemos dizer que o ciclo de feedback foi estabelecido - e isto pode ser considerado um novo avanço em Cibersegurança na atualidade. Um processo contínuo de avaliação de comprometimento não só simplificará a tomada de decisões para gestores e profissionais, como também transformará completamente a dinâmica do ecossistema de segurança cibernética e o ciclo cibernético de atacantes versus defensores.

Conclusão

A segurança cibernética é complexa. O sucesso em cenários complexos reside na capacidade do sistema de se regular frente a distúrbios. Na prática, isto é feito por meio de sistemas de ciclo fechado ou "sistemas controlados por erros", definindo erro como estado de comprometimento para um determinado incidente de segurança cibernética. Quanto mais rapidamente a indústria avançar para o desenvolvimento das capacidades de cibersegurança necessárias, que ajudem as organizações a avaliar continuamente seu estado de comprometimento, mais rapidamente a resiliência cibernética poderá ser alcançada. Com alterações pequenas mas calculadas na arquitetura de segurança cibernética, a distância entre o incidente cibernético e a detecção da violação pode ser dramaticamente reduzida.

Iluminando ameaças e adversários

www.lumu.io

Lumu Technologies Inc. | 8600 NW 36th St., Suite 150 Doral, FL 33166 | info@lumu.io | +1 (877) 909-5868