MARSH & McLENNAN INSIGHTS

Cyber Handbook 2019 da MMC

Perspectivas sobre risco cibernético na era digital

MARSH GUY CARPENTER MERCER OLIVER WYMAN

PREFÁCIO

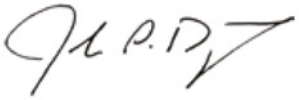
O risco cibernético é uma enorme preocupação para os líderes empresariais. De acordo com a Pesquisa Executive Opinion 2018 do Fórum Econômico Mundial (WEF) com mais de 12.500 executivos, os grandes ciberataques são classificados como o risco n° 1 ao se fazer negócio virtualmente por todas as economias avançadas. À medida que as empresas desenvolvem a sua abordagem a esta ameaça dinâmica e desafiadora em 2019, surgem algumas tendências que devem ser levadas em consideração.

Primeiro, o uso cada vez maior de tecnologias como inteligência artificial, a Internet das Coisas (IoT) e a robótica estão ampliando a área de atuação dos ciberataques. Embora estas tecnologias tenham potencial significativo para melhorar a produtividade e a eficiência de uma empresa, elas em geral estão sendo implantadas sem plena consideração quanto ao nível possível de aumento da exposição ao risco cibernético da empresa. As decisões sobre a implantação de novas tecnologias devem levar em conta o risco cibernético aumentado como uma parte importante da análise custo/benefício.

Segundo, para muitas empresas, o risco a si própria (não o risco a terceiros) é hoje a principal preocupação cibernética. A perda financeira potencial derivada do roubo de informações de terceiros em um ciberataque permanece uma questão crítica. Contudo, à medida que as organizações se tornam cada vez mais dependentes da tecnologia para os seus principais processos comerciais, os cenários de ciberataque que criam os maiores danos para muitas empresas são aqueles voltados para as vulnerabilidades dentro de sua própria infraestrutura digital e que podem resultar em transtorno comercial significativo ou danos materiais. O planejamento do risco cibernético deve abordar totalmente os cenários da empresa e de terceiros.

Em terceiro lugar, em uma atitude de abordagem do planejamento do risco cibernético, as organizações devem internalizar que não se trata de uma questão de "se", mas de "quando" elas vivenciarão um importante evento cibernético. Isso reequilibrará a forma pela qual as empresas investem e alocam os seus recursos de gestão de risco cibernético. As empresas não só devem continuar a instalar processos e infraestrutura para detectar e conter potenciais ciberataques, mas também devem investir em processos que as ajudem a responder e a reabilitar-se depois da ocorrência de um evento. Para muitas organizações, vemos a realocação dos recursos de prevenção para resposta como uma orientação construtiva.

No contexto dessas tendências, a edição de 2019 do Manual Cibernético da MMC inclui as nossas perspectivas sobre os principais desenvolvimentos, as implicações específicas do setor e as estratégias para aumentar a resiliência. Ele dá destaque a artigos de líderes empresariais das Marsh & McLennan Companies, assim como especialistas da Microsoft, CyberCube, Cisco e FireEye. Esperamos que este manual ajude a lhe fornecer algumas novas perspectivas sobre como aumentar a sua resiliência cibernética face a esta ameaça cada vez maior.



John Drzik

President, Global Risk and Digital
Marsh & McLennan Companies

ÍNDICE

RELÓGIO DE TENDÊNCIA

ANÁLISE DETALHADA DO SETOR

RELÓGIO DE TENDÊNCIA

SUBESTIMANDO A VOLATILIDADE NO MERCADO DE SEGURO CIBERNÉTICO

Ashwin Kashyap
cofundador e chefe de Produtos
e Analytics, CyberCube

O seguro cibernético é a linha de negócio de crescimento mais rápido na história moderna, permeando as linhas de negócio mais tradicionais com margens de lucro bem atraentes. O que começou como uma cobertura para a proteção das empresas contra o hacking (invasões) agora foi ampliado para cobrir interrupção do negócio, extorsão, fraude financeira, responsabilidade legal e falha do sistema decorrentes de ciberataques.

Mas enquanto as equipes de seguro cibernético desfrutavam dos benefícios de prêmios mais altos e lucros resultantes, o mercado mais amplo subestima de modo sistemático a volatilidade da perda subjacente da distribuição.

DESCONTANDO VARIÁVEIS PROSPECTIVAS

As abordagens tradicionais da quantificação da volatilidade incluem a coleta e a análise de informações de sinistro durante décadas em um mundo relativamente estacionário. Para a maioria das empresas, contudo, o modelo para a volatilidade está longe de ser robusto devido à transparência limitada nos riscos cibernéticos modelados e não modelados. As estimativas da volatilidade normalmente pressupõem o conhecimento derivado do espaço dos agentes da ameaça conhecidos e dos vetores do ataque conhecidos, junto com eventos efetivos e de quase acidentes históricos. Uma perspectiva desta natureza sofre de predisposição à recenticidade e tende a fornecer um falso sentido de conforto para os tomadores de decisão.

As variáveis prospectivas exerceram um papel relativamente limitado nas decisões de negócio quanto a preços, alocação de capital e transferência de risco de resseguro. O que está normalmente excluído é o espaço dos desenvolvimentos da tecnologia, vetores de ameaça desconhecida, grupos emergentes de agentes da ameaça que tornam obsoletas as medidas preventivas existentes. A volatilidade implícita nos sinistros decorrentes dos ciberataques é mais bem estimada por meio de um entendimento sólido e fundamental dos desenvolvimentos na tecnologia e as ameaças emergentes pertinentes.

Alguns exemplos estão relacionados abaixo:

CAMPANHAS DE RANSOMWARE (código malicioso de resgate) EM ESCALA

O ransomware tem sido usado com sucesso desde 2005 visando um ganho financeiro relativamente pequeno por grupos de agentes da ameaça. Historicamente, a escala de uma campanha de ransomware tem sido mínima, e somente no último ano foram observados padrões que demonstravam a que levaria uma campanha de ransomware sem alvo e indiscriminada. Embora a maioria dos modelos considerara o ransomware como um vetor do ataque, a escala foi grandemente subestimada. O aumento na volatilidade originado da dimensão da escala em um padrão de ataque existente como o ransomware não era levado em conta na precificação das apólices de seguro cibernético.

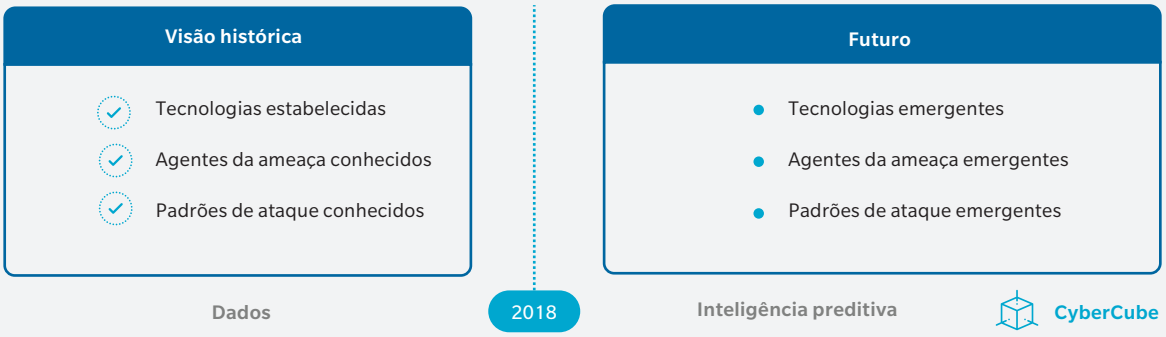
ANEXO 1: O RISCO CIBERNÉTICO SE ESPALHA PELA MAIORIA DAS LINHAS DE SEGURO TRADICIONAIS

COMPUTAÇÃO QUÂNTICA

Outro exemplo de uma tendência de tecnologia prospectiva não trivial é a computação quântica.

Vamos observar o vínculo entre computação quântica e criptografia. O princípio mais importante na criptografia é que grandes números primos são relativamente fáceis de gerar e multiplicar. Entretanto, a fatoração de um grande número gerado usando este método em dois números primos é difícil quando se usa as capacidades existentes de computação. Caso as capacidades de computação quântica em escala se tornem disponíveis para os agentes da ameaça no país, os sistemas que são construídos e protegidos com o uso de padrões de criptografia correntes estarão vulneráveis. Os métodos de criptografia que não podem ser quebrados usando a computação quântica estão tendo o seu desenvolvimento retardado com relação à proliferação das capacidades da computação quântica. Isso apresenta um risco existencial aos padrões de criptografia correntes.

ANEXO 2: INTELIGÊNCIA PREDITIVA
Alavancando novas variáveis para aprimorar as decisões da transferência de risco



INTERNET DAS COISAS (IOT)

Quando aparelhos do uso diário em um mundo conectado têm travas físicas sendo substituídas por travas digitais, e quando surgem exemplos de aparelhos domésticos transformados em armas, o perfil de exposição das empresas seguradas muda quase drasticamente. Se as apólices dos segurados residenciais têm cobertura ampliada para incluir o risco cibernético, o preço existente e as diretrizes de reserva não são mantidos. Está comprovado no mercado que as apólices residenciais oferecem a opção de se escolher segurar o risco cibernético, mas não está claro se tais exposições sistêmicas são consideradas em termos de decisão quanto ao preço.

NOTIFICAÇÃO MASSIVA DE INCIDENTES DE VIOLAÇÃO

Os produtos de seguro que ofereciam cobertura contra privacidade, disponibilidade e integridade de dados já viram índices mais baixos de sinistro e índices combinados quando comparados a outras linhas de negócio bem estabelecidas na maior parte das participantes do mercado. Um dos motivos para isso é que uma maioria significativa de empresas que sofreram violação decide não divulgar publicamente que sofreram violação temendo danos na reputação, responsabilidade legal e fiscalização aumentada de seus clientes e do público. Uma exceção a isso se dá quando há uma exigência legal de divulgação.

A real frequência de violações e a volatilidade associada têm sido então subestimadas na maioria dos modelos usados hoje em dia.

Esta observação levou muitas seguradoras a oferecer cobertura cibernética com um desconto significativo para os detentores de apólices existentes de outras linhas de negócio com o objetivo de ganhar participação no mercado. Por esses motivos, os níveis de preço são determinados quase inteiramente pela dinâmica concorrencial, ao contrário do risco técnico associado às apólices.

FALTA DE SINISTROS DE EVENTOS DE ACUMULAÇÃO CIBERNÉTICA DE GRANDE ESCALA

Têm ocorrido inúmeros quase acidentes de uma perspectiva de acumulação nos últimos cinco anos no mercado de seguro cibernético. A ausência de um sinistro de grande escala em todo o setor até 2017 resultou na subestimação da volatilidade com a expectativa de que as defesas de segurança e os planos de continuidade dos negócios das empresas estejam equipados para lidar com a interrupção do negócio decorrente de um ciberataque.

Esta hipótese agora foi completamente descartada. Meses de paralisação foram observados pelas empresas que sofreram

impacto com o NotPetya, o evento que expôs o impacto significativo da acumulação com as reivindicações sendo apresentadas contra apólices de bens patrimoniais.

Este resultado foi inesperado e não foi cobrado nas apólices que cobriam este risco, por acidente ou de outra forma. Tais exposições silenciosas existem para muitas seguradoras, levando a uma volatilidade aumentada no perfil de risco das operadoras que dirigem negócios de P&C em grande escala.

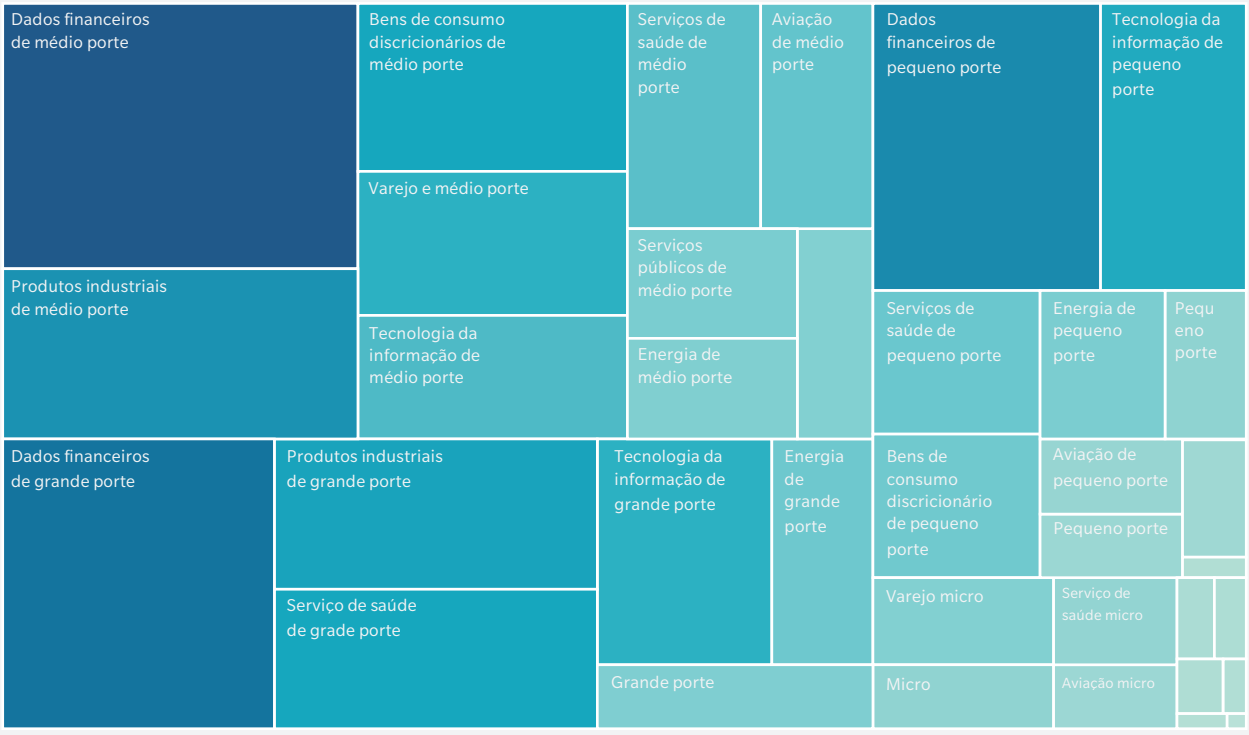
INTRODUÇÃO DAS CARGAS APROPRIADAS DE CATÁSTROFE CIBERNÉTICA

Temos bastante inteligência emergente sobre como as necessidades de precificação e gestão de acumulação são impactadas em decorrência do risco cibernético incorporado em todas as linhas de negócio.

As seguradoras resolveram determinar cargas apropriadas de catástrofe cibernética nos planos de classificação. Quando determinam as cargas da catástrofe, nem todos os riscos segurados são parecidos e a capacidade de compreender as relatividades nesses riscos é primordial para as decisões sobre preços. Uma grande empresa de serviços financeiros com centenas de fornecedores, centenas de milhões em receitas e milhares de colaboradores tem um perfil de risco diferente quando comparada com um pequeno negócio de serviços profissionais com pouca receita, poucos colaboradores e poucas dependências.

Existe um consenso direcional no mercado sobre a necessidade do ajuste das estimativas da volatilidade para responder pelas incertezas prospectivas. As seguradoras e resseguradoras estão usando modelos e parcerias de tecnologia para ampliar o seu horizonte com relação a este risco complexo.

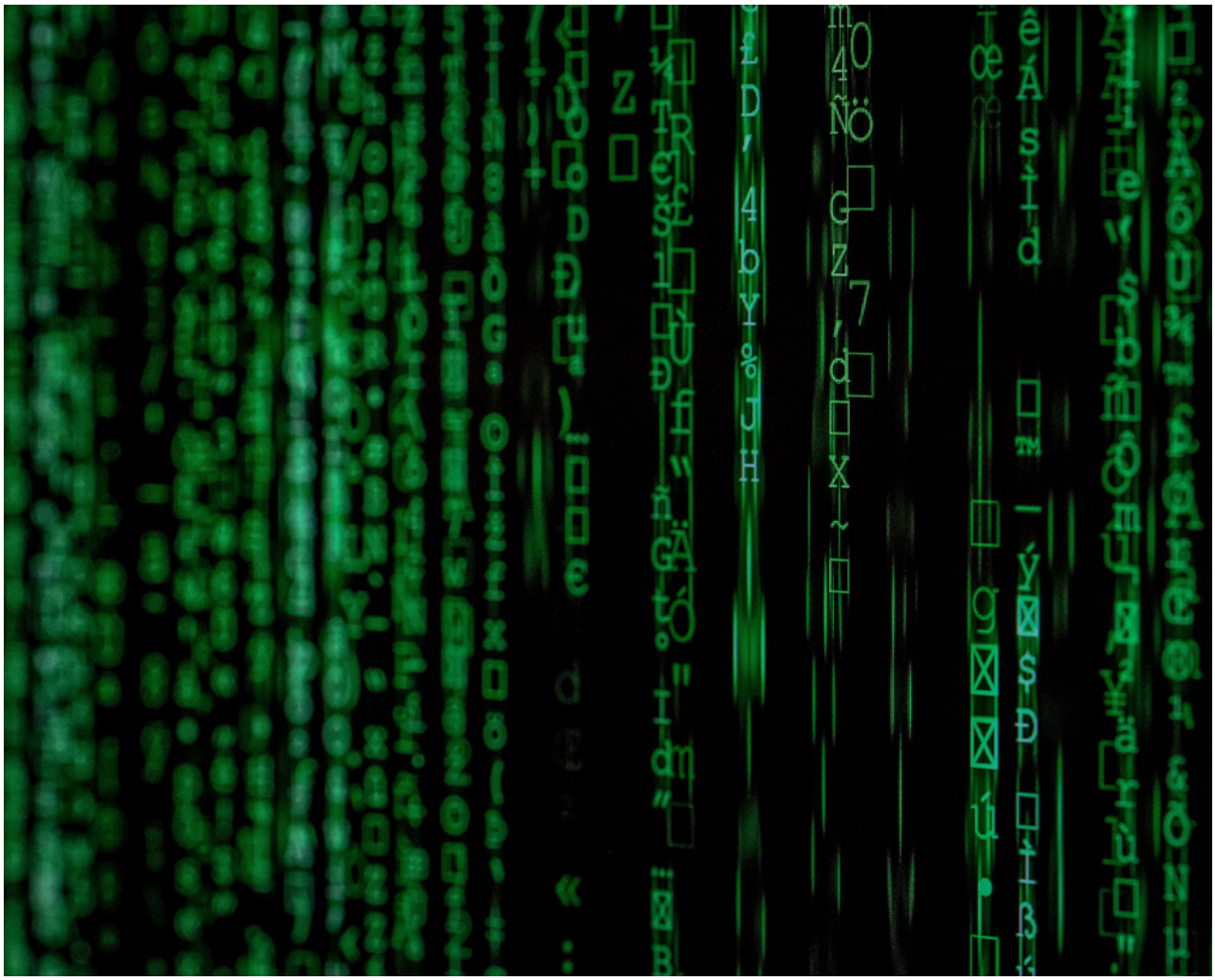
ANEXO 3: MAPA DE RELATIVIDADE DO RISCO CIBERNÉTICO



RELÓGIO DE TENDÊNCIA

SPECTRE E MELTDOWN

O SINAL DE ALERTA PARA A INOVAÇÃO DIGITAL?



Paul Mee
Sócio e chefe de cibernética, Oliver Wyman

Chris DeBrusk
Sócio em Finanças, Risco e Digital, Oliver Wyman

Inúmeros comunicados à imprensa esta semana deram destaque à Spectre e à Meltdown, duas falhas de cibersegurança recentemente descobertas. O que torna estas falhas diferentes de outros "furos" de segurança é que elas são falhas de hardware, não de software – e se manifestam em microprocessadores que funcionam na maioria dos computadores e telefones do mundo. As falhas de segurança de software podem ser virtualmente corrigidas; as falhas de hardware em geral exigem substituição da peça física, como um recall de airbag das fabricantes de automóvel.

O QUE SÃO SPECTRE E MELTDOWN?

Em geral, ambas as falhas Spectre e Meltdown permitem que um invasor acesse áreas da memória do computador que deveriam ser inacessíveis. Os hackers ganham acesso ao tirar vantagem de aspectos do design do microprocessador que é usado para melhorar o desempenho, inclusive a leitura antecipada da memória e a execução de instrução de defeito. Se um programa pode acessar a memória que deve estar protegida, um intruso poderia potencialmente acessar as informações sensíveis. Essas informações sensíveis poderiam ser senhas ou outras informações de acesso que abririam a porta para uma violação de dados bem maior.

Como estas falhas foram identificadas, uma correção (patch) foi emitida para os principais sistemas operacionais que analisam a vulnerabilidade Meltdown, embora potencialmente em um impacto bastante relevante no desempenho. Atualmente não existe correção para a Spectre, mas especula-se que ela não pode ser totalmente consertada sem a substituição física do processador em todos os computadores e servidores afetados.

Há duas maneiras principais pelas quais um invasor poderia tirar vantagem destas falhas para obter acesso a dados confidenciais ou sensíveis. A primeira seria rodar um programa de ataque em uma nuvem pública que tentasse roubar as informações que estão rodando simultaneamente nos mesmos servidores físicos, uma vez que a nuvem pública é um ambiente compartilhado e virtual. Embora seja teoricamente possível, este tipo de ataque seria altamente especulativo, como uma pescaria no meio do oceano sem se ter ideia do que existe abaixo. Além disso, os grandes provedores de nuvem já corrigiram a sua infraestrutura ou acrescentaram proteções para impedir o vazamento desse tipo de informação.

A segunda é muito mais provável. Ao enganar alguém para que rode um malware em uma máquina específica, provavelmente através de um ataque de phishing, as outras informações que rodam nessa mesma máquina podem ser comprometidas. Dito isso, não há ataques comprovados deste tipo e os fornecedores de sistemas operacionais vêm divulgando correções e proteções para reduzir a probabilidade de isso ocorrer.

Qual a importância desta distinção da perspectiva do risco cibernético e inovação digital? Consideramos isso muito importante e provavelmente sinaliza o início de uma nova era em design de tecnologia.

OS HARDWARE NÃO SÃO MAIS SEGUROS (E DE FATO NUNCA FORAM)

As pessoas em geral acham que o software é normalmente cheio de vírus e exposto aos hackers, mas que o hardware físico é seguro. A Spectre e a Meltdown ressaltaram a falácia nesta suposição. De uma perspectiva prática, isto significa que as pilhas de hardware em data centers cativos e em laptops, telefones e dispositivos do cliente precisam ser tratadas como potencialmente comprometidas (e geralmente não passíveis de correção). As situações de segurança devem ser ajustadas de forma condizente.

Esta materialização reforça a noção de que a abordagem de castelo murado à cibersegurança é fundamentalmente deficiente e que as empresas devem usar uma abordagem por níveis à segurança que aumente o controle (e provavelmente o atrito do usuário) à medida que os ativos se tornam mais sensíveis. Todo o núcleo desta filosofia está na suposição de que você será invadido e agirá para limitar qualquer dano.

OS DISPOSITIVOS SÃO O PRÓXIMO VETOR DE ATAQUE

Durante os últimos cinco anos, houve um avanço continuado para conectar praticamente tudo em nossas vidas diárias. Desde termostatos inteligentes até controles remotos para abertura da porta da garagem, lâmpadas, brinquedos infantis e até aquários – tudo está sendo conectado ao ponto de acesso Wi-Fi local de modo que possa ser controlado remotamente e atualizar os dados na nuvem. Aparentemente, isso é uma coisa boa – os dispositivos inteligentes são mais fáceis de serem usados, economizam energia e certificam que os peixes permaneçam vivos.

Infelizmente, todos esses dispositivos em rede também permitem aos hackers milhões de novos pontos de ataque que normalmente não são fortalecidos de modo eficaz. Pior ainda, os fabricantes de dispositivos raramente instalam programas de atualização e patch necessários para a identificação e o fechamento das falhas de segurança que são descobertas. Além disso, esses dispositivos são cheios de microprocessadores e outros hardware que podem criar risco adicional.

Como é provável que a disseminação do networking e da Internet das Coisas continue acelerada, é absolutamente imprescindível que os compradores de dispositivos (tantos os consumidores quanto as empresas) demandem proteção para os seus dados. Afinal, o seu aquário não deve permitir que os hackers roubem todos os seus dados.

A SEGURANÇA DEVE SER A PRIMEIRA LIMITAÇÃO DO DESIGN, NÃO A ÚLTIMA

Uma vez que as invasões já estão difundidas e provavelmente ficarão piores, a segurança deve ser um ponto focal, e não uma reflexão tardia, no design do dispositivo – começando na etapa da elaboração de diagramas. A prática corrente de fazer uma análise superficial da segurança pouco antes de lançar a v.1.0, e então rapidamente corrigir os problemas de segurança que são descobertos (em geral depois das primeiras invasões), é simplesmente inaceitável no ambiente cibernético dos dias de hoje.

Da mesma forma, esta suposição básica de que o aumento de atrito do usuário para melhorar a segurança é inaceitável também deve ser contestada de modo direto e continuado. Os usuários devem ser treinados para aceitar alguma complexidade adicional em troca pela proteção – e aqueles que projetam a experiência do usuário deverão ser criativos sobre como inserir naturalmente a segurança na experiência do usuário.

Spectre e Meldown parecem ser tão somente o início quando se trata de falhas de segurança nos hardware. Essas falhas ocorreram porque os engenheiros comprometeram a segurança para obter desempenho, o que poderia fazer sentido há 20 anos. No ambiente atual totalmente conectado em rede e sempre ligado, esse tipo de compensação só cria caminhos a serem explorados pelos hackers.

RELÓGIO DE TENDÊNCIA

APRENDIZADO DE MÁQUINA E SEGURANÇA

HOPE OU HYPE?

TK Keanini
Distinguished Engineer,
Cisco

Existe uma atração em aclamar os avanços importantes em tecnologia como uma panaceia para os desafios enfrentados pelas organizações e pela sociedade nos dias atuais. A fanfarra geralmente termina em desapontamento, quando a última tecnologia fantástica não corresponde às expectativas. Não surpreende que o aprendizado de máquina, um domínio que faz parte do amplo espectro da inteligência artificial, tenha sido aclamado como a atual resposta essencial em cibersegurança. Consequentemente, ele está hoje no topo das expectativas inflacionadas no mais recente Hype Cycle for Emerging Technologies da Gartner.

O QUE É APRENDIZADO DE MÁQUINA... E O QUE NÃO É

Arthur Samuel definiu aprendizado de máquina em 1959 como "o campo de estudo que dá aos computadores a capacidade de aprender sem serem programados explicitamente". Em outras palavras, o aprendizado de máquina ensina os computadores a fazer o que as pessoas fazem: aprender com a experiência e melhorar ao longo do tempo.

Uma distinção importante é que o aprendizado de máquina é um domínio que faz parte do amplo espectro da inteligência artificial. Os dois termos não são totalmente sinônimos, embora sejam geralmente usados de modo intercambiável.

O aprendizado de máquina consiste principalmente em três categorias de alto nível:

- **Aprendizado supervisionado:** Quando você sabe a pergunta que deseja fazer e tem exemplos disso sendo perguntado e respondido corretamente
- **Aprendizado não supervisionado:** Você não tem respostas e pode não saber totalmente as perguntas
- **Aprendizado por reforço:** Comportamento de ensaio e erro eficaz em cenários de jogo

ANEXO 4: APRENDIZADO DE MÁQUINA: TERMOS COMUNS

Inteligência Artificial (IA) é um campo científico dentro da Ciência da Computação voltado para o estudo dos sistemas de computação que podem executar tarefas e resolver problemas que exigem a inteligência humana

Aprendizado de Máquina (ML) é o campo da IA que focaliza uma classe específica de algoritmos que podem aprender com os dados sem ser programados explicitamente

Há três formas principais pelas quais uma máquina pode aprender com os dados: aprendizado supervisionado, não supervisionado e por reforço

Cada categoria do aprendizado de máquina é eficaz na resolução de tipos específicos de tarefas e problemas

Aprendizado de máquina supervisionado	Aprendizado de máquina não supervisionado	Aprendizado por reforço
Mapear dados de entrada em saídas rotuladas	Encontrar padrões em dados de entrada não rotulados	Executar ações para maximizar as recompensas
Usado habitualmente em problemas de classificação e regressão como: • Processamento de linguagem natural • Reconhecimento de imagem • Previsão financeira	Usado habitualmente em problemas de segmentação e clustering como: • Reconhecimento de padrão e tendência • Segmentação do cliente • Monitoramento da transação	Como ocorre no aprendizado supervisionado, mas com mecanismo de recompensa instalado em vez de resultado rotulado: • Jogos de tabuleiro e vídeo • Robótica

COMO FUNCIONA O APRENDIZADO DE MÁQUINA SUPERVISIONADO

Os detalhes e os termos do aprendizado de máquina podem parecer intimidantes para cientistas sem dados, então vamos analisar alguns termos importantes.

O aprendizado supervisionado requer dados de treinamento, conjuntos de pares de pergunta e resposta corretas, chamados de "verdade absoluta". Este treinamento faz com que os classificadores – os burros de carga do aprendizado de máquina que categorizam as observações –, e os algoritmos – as técnicas que organizam e orientam os classificadores – façam um ótimo trabalho quando analisam novos dados no mundo real.

Um exemplo comum é o reconhecimento facial.

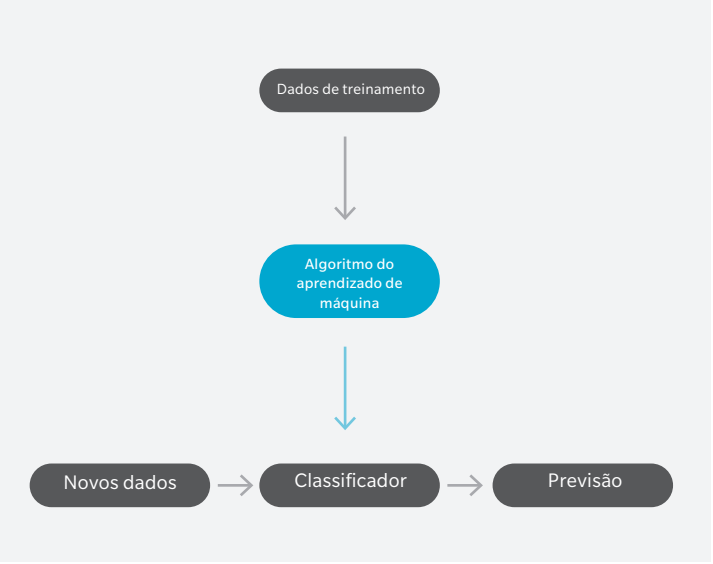
Os classificadores analisam padrões específicos de dados que estão treinados para reconhecer – não o nariz ou os olhos – para marcar com precisão um rosto específico entre milhões de fotos.

APRENDIZADO DE MÁQUINA NA CIBERSEGURANÇA

O panorama das ameaças cibernéticas hoje força as organizações a monitorar constantemente e a correlacionar milhões de pontos de dados externos e internos por uma série de pontos de extremidade. Simplesmente não é viável administrar este volume de informações continuamente com uma equipe de pessoas.

O aprendizado de máquina se projeta aqui porque pode reconhecer padrões e prever ameaças em grandes conjuntos de dados, tudo na velocidade da máquina. Com a automação da análise, as equipes de cibernética podem rapidamente detectar ameaças e isolar as situações que precisam de uma análise humana mais a fundo. As técnicas do aprendizado de máquina podem proteger melhor as organizações de várias formas:

ANEXO 5: APRENDIZADO DE MÁQUINA
Principais termos



1. **Detectando invasores sub-reptícios nas redes:**
   O aprendizado de máquina pode detectar anomalias de comportamento para encontrar invasores internos ou registrados com credenciais roubadas
2. **Prevendo "vizinhanças ruins" on-line:**
   Ao aprender com os padrões de atividade da internet, o aprendizado de máquina pode identificar automaticamente a infraestrutura do invasor configurada para lançar a próxima ameaça
3. **Detectando ataques por meio de novidades e exceções:**
   O aprendizado de máquina detecta padrões de ataque que os seres humanos não conseguem detectar prontamente, como um novo relacionamento entre colegas na rede com hosts comunicando que não pode ou que não deveria
4. **Detectando comportamento suspeito de usuário da nuvem:**
   As técnicas analíticas revelam comportamentos suspeitos do usuário, indicativos de comprometimento da conta na nuvem, para extrair dados ou executar operações mal-intencionadas
5. **Detecção de malware modernos:**
   O aprendizado de máquina é valioso na detecção de malware polimórfico, decompondo os atributos da ameaça para interromper com mais sucesso ameaças polimórficas novas e de reengenharia

CUIDADO COM AS ARMADILHAS

Embora o aprendizado de máquina represente uma tremenda promessa para a cibersegurança, ele tem a sua parcela de falhas que precisam ser reconhecidas visando o seu uso apropriado.

1. Lidando com más recomendações: Caso um aplicativo usando aprendizado de máquina sugira uma recomendação de filme incorreta, ele é em geral ignorado. Contudo, caso o aprendizado de máquina incorretamente não detecte uma ameaça ou falsamente condene um arquivo sem defeito, isso teria potencial para interromper as operações comerciais. O aprendizado de máquina tenta dar conta do custo dos erros no mundo real, mas isso mostra como a segurança é desafiadora para o aprendizado de máquina, de forma que não deixe passar as ameaças, nem bloqueie o negócio legítimo
2. Responsabilidade pela mudança: Como o aprendizado de máquina pode ser responsável pelas mudanças ocorridas no mundo à sua volta? Por exemplo, se ele opera em um ambiente no qual dois países são inimigos, como ele pode se responsabilizar por um tratado de paz entre os antigos adversários? Isso torna vital o novo treinamento periódico, para que ele permaneça correto à medida que o mundo evolui
3. Lidando com a "explicabilidade": Quando o aprendizado de máquina detecta alguma coisa ruim, ele geralmente explica para si próprio com lógica matemática, em vez de contexto de segurança pertinente. Por exemplo, digamos que um sistema de aprendizado de máquina detectou um dispositivo infectado em um escritório da área financeira. Antes de potencialmente arrancar o CFO da rede, um especialista em segurança deve confirmar os detalhes da infecção pertinentes do evento de segurança – como o computador foi infectado, se existe um aplicativo vulnerável no laptop, qual foi o arquivo que tornou-se mal-intencionado, etc., para entender melhor como responder.

A lógica matemática não ajuda aqui, mas sim as informações do evento relacionadas à segurança que observamos que o aprendizado de máquina nem sempre compartilha. Este problema de "explicabilidade" é um desafio legítimo

FAZENDO COM QUE O APRENDIZADO DE MÁQUINA FUNCIONE PARA A SUA ORGANIZAÇÃO

O aprendizado de máquina não é uma panaceia para aumentar a resiliência cibernética. Pelo contrário, ele é uma camada de segurança adicional e útil para aumentar as outras técnicas instaladas. Em vez de ser usado isoladamente, ele precisa estar combinado com outras técnicas de cibersegurança, desde regras de prevenção de invasão e assinaturas antivírus, até whitelists (listas de remetentes seguros), envio para áreas restritas e técnicas comportamentais. Com respeito ao aprendizado de máquina, nenhuma outra técnica ou método bastará, de modo que devemos convocar um pipeline de centenas de algoritmos trabalhando em conjunto visando resultados bem sucedidos.

Em segundo lugar, nenhuma abordagem de segurança é eficaz sem uma equipe de seres humanos conduzindo pesquisa de inteligência de ameaça, confirmando que tudo está funcionando como deveria e dedicando-se às mudanças no contexto (lembra daquele tratado de paz?).

Finalmente, mas não menos importante, o aprendizado de máquina tem muitas medidas técnicas de sucesso, mas nem todas são úteis para um profissional da área de segurança. Para que o aprendizado de máquina tenha mais sucesso e seja adotado mais plenamente, ele deve gerar resultados compreensíveis e geralmente "mostrar o seu trabalho" com contexto de segurança.

RELÓGIO DE TENDÊNCIA

NOTPETYA NÃO FOI UMA “GUERRA” CIBERNÉTICA

Thomas Reagan
líder de prática de Cibernética dos EUA, Marsh

Matthew McCabe
assessor jurídico assistente para Política Cibernética, Marsh

Este verão marcou o aniversário do ciberataque mais dispendioso da história. O NotPetya causou estrago em algumas grandes empresas, custando a elas bilhões de dólares em receita perdida, danificando sistemas de computação e exigindo despesa significativa para a restauração das operações globais. Em sua vigília, indústrias inteiras reavaliaram as suas práticas de patching, continuidade dos negócios, interrupção da cadeia de abastecimento, e mais.

No mesmo ano desde o NotPetya, aprendemos muito sobre o ataque, mas muitos detalhes permanecem vagos. Uma discussão constante para o setor de seguro, entretanto, é se o NotPetya era "belicoso" – e, mais especificamente, se a exclusão de guerra onipresente encontrada nas apólices de seguro cibernético poderiam ter impedido a cobertura. Um artigo recente do Wall Street Journal descreveu essa como uma "pergunta de muitos milhões de dólares para as empresas que compram seguro cibernético".

Confundir a exclusão de guerra com um evento cibernético não físico como o NotPetya decorre de dois fatores: (1) o NotPetya infligiu um dano econômico significativo em inúmeras empresas, e (2) os governos dos EUA e do Reino Unido atribuíram o ataque do NotPetya aos militares russos. Apenas esses dois fatores, entretanto, não são suficientes para levar este ciberataque não físico para a categoria de guerra ou atividade "hostil e belicosa". Esses termos que têm sido considerados pelos tribunais, e pelas sentenças resultantes, e que hoje fazem parte da Lei do Conflito Armado, deixam claro que é preciso haver muito mais para que se chegue à conclusão de uma ação "belicosa".

Primeiro: Quais foram os efeitos do ataque? Para que um ciberataque chegue ao nível de uma atividade belicosa, as suas consequências devem ir além das perdas econômicas, até mesmo as grandes. Anos antes do NotPetya, quando foi pedido ao presidente Obama que caracterizasse um ciberataque similar no país que não infligisse dano físico, mas que se comprovasse "bastante dispendioso" para uma empresa norte-americana, o presidente habilmente descreveu o incidente como "um ato de vandalismo cibernético". Os seus comentários estavam embasados em uma história legal de conflito armado em que a atividade belicosa sempre acarretava baixas ou destroços. Para que um ciberataque fosse considerado dentro do escopo da exclusão de guerra, deveria haver um resultado comparável, equivalente a um uso de força militar.

Segundo: Quem foram as vítimas e onde estavam localizadas? As vítimas serviam a um fim militar e residiam próximo ao conflito efetivo ou "em locais bem distantes do local ou do objeto de alguma guerra".

As vítimas mais importantes do NotPetya operavam longe de qualquer área de conflito e trabalhavam em tarefas meramente civis como entregando pacotes, produzindo produtos farmacêuticos, fabricando desinfetantes e biscoitos.

Terceiro: Qual foi o objetivo do ataque? O NotPetya não era uma arma que suportava um uso de força militar. O ataque ocorreu bem antes do Dia da Constituição, quando a Ucrânia celebra a sua independência. O caos resultante fez com que o NotPetya apresentasse maior semelhança com um esforço de propaganda, não com uma ação militar que pretendesse "coação ou conquista", fato que a exclusão de guerra deveria abordar.

Como os ciberataques continuam a crescer em gravidade, as seguradoras e os compradores de seguro reverão se a questão da exclusão de guerra será aplicável a um incidente cibernético. Para essas situações, chegar ao limite da atividade "belicosa" exigirá mais do que uma intenção mal-intencionada agindo em todo o país. Como demonstrado nas recentes condenações de autoridades da inteligência militar estrangeira por interferência nas eleições dos EUA, a maioria das invasões em todo o país ainda faz parte da categoria de atividade criminal.

O debate sobre se a exclusão de guerra poderia ser aplicada ao NotPetya demonstra que, caso as seguradoras continuem a incluir a exclusão de guerra nas apólices de seguro cibernético, o texto deverá ser emendado para deixar claras as circunstâncias necessárias para a sua ativação. Na ausência desse esclarecimento, seguradoras e compradores de seguro devem seguir a Lei do Conflito Armado, incluindo decisões que poderiam ter mais de um século, para discernir entre as categorias de atividade criminal e ações belicosas. Quanto às últimas, todos os precedentes indicam que o NotPetya simplesmente não atingiu esse nível.

RELÓGIO DE TENDÊNCIA

MINERANDO O OURO VIRTUAL

COMPREENDENDO A AMEAÇA DO CRYPTOJACKING

Stephen Viña
vice-presidente sênior, Marsh

Paula R. Miller
vice-presidente sênior, Marsh

Em vez de roubar dados da empresa ou pedir pelo seu resgate, os cibercriminosos dominavam uma nova forma de atacar as empresas. Por meio do cryptojacking, um dos tipos de ciberataques de crescimento mais rápido globalmente, os criminosos podem desviar a capacidade de processamento de uma organização para fazerem a mineração de criptomoedas, abrindo a porta para novas fontes de receita ilícita às custas da empresa. E a sua organização pode já ser uma vítima e nem saber disso.

O QUE É CRYPTOJACKING?

Milhares de criptomoedas ou "moedas" existem hoje em dia, todas com finalidades variadas. Algumas, como o Bitcoin e o Monero, servem como uma moeda digital e podem reter considerável valor monetário. O sempre alto valor de um único Bitcoin, por exemplo, chegou a cerca de US$ 20.000 em dezembro de 2017; o valor flutua diariamente com base na disponibilidade e na movimentação da moeda. A criação de determinadas criptomoedas, inclusive o Bitcoin e o Monero, requer a conclusão de um quebra-cabeça criptográfico complexo que é registrado em um blockchain, um processo conhecido por criptomineração (cryptomining). A realização desses cálculos pode ser dispendiosa, exigindo considerável processamento e energia elétrica e, em alguns casos, equipamentos especializados. Pelos seus esforços, os mineradores são recompensados com unidades recentemente criadas da criptomoeda minerada, proporcionando um pagamento potencialmente lucrativo dependendo do valor e da quantidade da moeda.

Como o valor das criptomoedas aumentou, muitas organizações se voltaram para a mineração de moedas como uma nova fonte de receita. Algumas empresas perguntaram aos usuários on-line se eles permitiriam a mineração de criptomoedas em seus computadores em troca da eliminação da publicidade. Contudo, um número crescente de mineradores hoje estão simplesmente roubando, ou sequestrando, a capacidade de processamento necessária de consumidores e empresas desavisados. O que já fora um processo complicado tornou-se relativamente fácil com o advento de scripts de mineração no navegador, que permitem que os fraudadores usem a capacidade de processamento de alguém que visita um site infectado. O malware de criptomineração também pode ser espalhado por links mal-intencionados, publicidades, anexos de e-mail, Wi-Fi público, aplicativos falsos e backdoors do sistema.

As infecções foram agressivas, afetando cerca de 30% das empresas monitoradas pela firma de cibersegurança Fortinet no primeiro trimestre de 2018, dobrando os números de registro de 2017.

Em fevereiro de 2018, por exemplo, os hackers expuseram a risco um plug-in de leitura de tela para os cegos, afetando mais de 4.000 sites em todo o mundo, inclusive o Serviço Nacional de Saúde britânico.

Algumas empresas representam especialmente alvos sólidos para o cryptojacking. Elas incluem:

- Empresas de infraestrutura crítica, que consomem quantidades significativas de energia e em geral têm sistemas de controle industrial vulneráveis
- Empresas que confiam cegamente nos serviços na nuvem, que apresentam a oportunidade de "mineração de alto nível"

O cryptojacking também está frequentemente vinculado a dispositivos da Internet das Coisas (IoT), como telefones celulares, que podem permitir que os mineradores juntem rapidamente exércitos de dispositivos sequestrados para minerar criptomoedas em larga escala.

COMO O CRYPTOJACKING PODE AFETAR AS EMPRESAS

O roubo da capacidade de processamento de uma empresa por meio do cryptojacking pode trazer consequências financeiras efetivas ao longo do tempo. A captura correta dos custos diretos do cryptojacking, entretanto, pode ser difícil, uma vez que a maioria das vítimas pode não notar uma infecção ou reconhecer o culpado.

Mas a ameaça é real. O desempenho de um sistema de computador infectado poderia se tornar lento devido às operações complexas e continuadas necessárias para a execução dos cálculos de mineração. Computadores sobrecarregados de trabalho poderiam levar ao travamento de funções necessárias e, em alguns casos, ao superaquecimento e à falha definitiva das unidades de processamento central. Isso pode parecer como um

inconveniente temporário ou isolado, mas espalhado por toda uma empresa, poderia ter implicações destruidoras e caras para as empresas. Além da potencial degradação no serviço e da resultante perda de produtividade e de receita, as empresas podem incorrer em custos por maior consumo de energia ou uso da nuvem.

Uma organização também poderia incorrer em despesas extras para substituir hardware mais cedo ou com mais frequência do que o planejado, e para suporte adicional de TI visando ajudar a lidar com problemas de desempenho do sistema.

As empresas que transferem software de criptomineração para terceiros desavisados também se tornam objeto de litígio e fiscalização regulatória. A Federal Trade Commission, por exemplo, lançou recentemente um sistema para os clientes protocolarem reclamações caso se tornem vítimas de cryptojacking, e realizaram ações de execução contra empresas que sequestraram os dispositivos móveis dos clientes com malware para minerar moeda virtual.

É claro que, se os mineradores são capazes de comprometer a rede corporativa para roubar a capacidade de processamento da empresa, é possível que as mesmas pessoas acessem dados, instalem malware ou explorem outras vulnerabilidades para causar danos. Assim como o anuncio de qualquer tipo de violação importante de dados pode trazer danos reputacionais, a divulgação pública de um evento de cryptojacking também pode danificar a posição da empresa junto a clientes e terceiros.

UM SEGURO CIBERNÉTICO PODE AJUDAR?

As apólices de seguro cibernético são projetadas para cobrir perdas e responsabilidades diretas causadas por um evento cibernético. As apólices cibernéticas podem cobrir as despesas incorridas diretamente pelos detentores da apólice para TI forense, recriação ou restauração de ativos de dados, resposta à violação de dados, perda de receita comercial e dano reputacional. A cobertura também se estende a sinistros de responsabilidade civil contra terceiros por violações da privacidade e falhas de segurança, como a transferência de malware para um terceiro ou a divulgação não autorizada de dados sensíveis do cliente.

Um incidente de cryptojacking poderia resultar em vários tipos de sinistros que são cobertos pelas apólices de seguro cibernético. Por exemplo, um incidente de cryptojacking poderia interromper importantes sistemas de controle ou a rede de uma empresa, ativando a cobertura de interrupção de negócio, ou poderia resultar na perda de informações sensíveis, ativando a cobertura de recuperação de ativo de dados. O seguro cibernético também pode ajudar a cobrir os custos das investigações para a determinação da causa, da fonte e do escopo de um evento de cryptojacking e para os serviços de contabilidade forense para preparações de sinistro. As empresas que inadvertidamente transferem malware de cryptojacking para terceiros também podem procurar uma apólice de seguro cibernético para reparação de quaisquer sinistros relacionados para indenização.

A resposta do seguro cibernético dependerá dos termos e condições específicos de uma determinada apólice. As empresas devem considerar a análise cuidadosa das disposições de cobertura específicas para determinar se e como as suas apólices reagirão às perdas por cryptojacking. As empresas também devem trabalhar com os seus consultores de risco para assegurar que as suas apólices de seguro cibernético incluam gatilhos de sinistro específicos e definições amplas de sinistro visando capturar todos os cenários possíveis para os quais um segurado esperaria recuperar a perda.

RECOMENDAÇÕES

Enquanto houver muito dinheiro, é provável que os participantes cibernéticos continuem a sequestrar os sistemas de computação para minerar criptomoedas, evoluindo os seus métodos ao longo do tempo. Como ocorre com outros ciberataques, as empresas devem procurar detectar e impedir esta ameaça em crescimento e evolução, olhando de perto os sinais de infecção.

Para proteger mais a sua empresa do cryptojacking, trabalhe com o seu consultor de seguro para avaliar o seu potencial para exposição ao cryptojacking e determinar como a sua apólice de seguro cibernético pode responder. O momento para avaliar as suas apólices de seguro cibernético quanto à cobertura potencial é antes da sua organização ser atacada.

RELÓGIO DE TENDÊNCIA

SIGA O DINHEIRO

UM OLHAR MINUCIOSO NO IMENSO CARTEL DE HACKING DE CARTÃO DE CRÉDITO, FIN7

Nick Carr
gerente sênior, FireEye

Barry Vengerik
diretor técnico, FireEye

O agente de ameaça financeira FIN7 esteve nas manchetes em agosto de 2018, quando a Vara de Justiça Federal dos Estados Unidos indiciou três de seus membros por invasão. O grupo escolheu cuidadosamente as suas vítimas, ao se voltar para o roubo de dados de cartão de pagamento em larga escala usando técnicas de nível nacional e um ciclo de desenvolvimento rápido e inovador. Estes agentes mal-intencionados são membros de um dos mais prolíficos grupos de ameaças financeiras desta década, tendo elaborado com astúcia ataques voltados para mais de 100 organizações. O FIN7 é denominado por muitos fornecedores como o "Grupo Carbanak".

O grupo de ameaças se caracteriza por seu roubo persistente e em grande escala de dados de cartão de pagamento dos sistemas da vítima, mas as operações financeiras do FIN7 iam além do roubo das informações de crédito. Em certas ocasiões, quando encontravam, mas não obtinham, dados do cartão de pagamento dos sistemas de ponto de vendas protegidos com criptografia de ponta a ponta ou de extremidade a extremidade, o FIN7 se articulava para se voltar para os departamentos financeiros dentro das organizações das suas vítimas.

A FireEye seguiu o FIN7 desde 2015, observando a sua movimentação desde macros do Microsoft Office como armas para não serem descobertos. O FIN7 evoluiu, usando iscas de phishing com arquivos de atalho ocultos para infectar os alvos e os expor. Durante as campanhas em que a FireEye se associou ao FIN7, o grupo focalizava vítimas dentro dos seguintes setores nos Estados Unidos e na Europa: restaurantes, serviços de hospitalidade, cassinos e jogos, energia, finanças, tecnologia de ponta, software, viagem, educação, construção, varejo, telecomunicações, governo e serviços comerciais.

Em abril de 2017, o FIN7 enviou e-mails de phishing para o pessoal envolvido com os arquivamentos da SEC (Securities and Exchange Commission) dos EUA em várias organizações, tendo como alvo as pessoas que teriam um provável acesso a informações privilegiadas relevantes que os agentes do FIN7 poderiam usar para obter vantagem competitiva no mercado de ações.

Com os seus ataques mais recentes, o FIN7 em geral instalava malware de ponto de venda dentro das organizações alvo. O grupo enviava e-mails de phishing e então ligava para os alvos, encorajando-os a abrir os e-mails com malware, dando início ao processo de infecção. O resultado? Mais de US$ 1 bilhão de perdas para as vítimas.

As pessoas que compravam alguma coisa em mais de 3.000 locais afetados viam as suas carteiras levarem prejuízo. O FIN7 roubou digitalmente 15 milhões de números de cartão de crédito, e então os vendeu no mercado paralelo para uso de outros criminosos.

A FireEye conversou com Nick Carr e Barry Vengerik, dois analistas que tinham rastreado o FIN7 durante anos, sobre os alvos do grupo, e como e o que poderia vir a seguir para o imenso cartel de hacking diante das recentes prisões de três de seus líderes.

O FIN7 parecia de fato estar concentrado em restaurantes, serviços de hospitalidade, cassinos e jogos. Por que estes setores de modo específico?

Barry Vengerik: Estes setores estão totalmente voltados para os serviços ao consumidor. Com os hotéis em que haviam se infiltrado antes, o FIN7 se comunicaria como se estivesse tentando reservar grandes eventos corporativos, com salão de festas e várias salas. Isso é uma isca tentadora para qualquer um que estivesse encarregado de reservas nesses hotéis.

Da mesma forma, para os restaurantes o FIN7 usava temas de serviço de alimentação ou grandes pedidos, mas também temas de reclamações sobre o restaurante, como “A comida me deixou enjoado” ou “Deixei minha bolsa no restaurante”. O FIN7 de fato tentava capitalizar sobre o aspecto de serviço do cliente, assim como se voltava para usuários específicos dentro da organização cujas tarefas regulares eram abrir anexos não solicitados – o que vai diretamente de encontro aos conselhos sobre phishing que geralmente damos aos clientes. O pessoal alvo nestas organizações não estava em uma posição de evitar a interação com estes anexos não solicitados.

Que tipos de conteúdo o FIN7 usava para entrar nos ambientes da vítima?

Barry: Durante os primeiros dois anos, o grupo usava consistentemente um backdoor do Java Script que chamamos de "mal concebido" e acrescentava novos recursos a ele com cada vítima. Uma vez estabelecido o acesso inicial, percebemos um conjunto interessante de conteúdo secundário, inclusive o famoso backdoor CARBANAK. Era um misto de um backdoor mais simples na frente que recebia muito do desenvolvimento ativo, e então eles rapidamente passavam para ferramentas e técnicas bem diferentes com base no ambiente do cliente.

Com tal variedade de ferramentas e constantes mudanças, fica mais difícil encontrar o FIN7 no ambiente de um cliente? É possível continuar a rastreá-los por todas essas mudanças?

Nick Carr: A resposta da FireEye está voltada para a proteção dos nossos clientes com respeito a esses e-mails de phishing iniciais. Ao mesmo tempo, arrumamos uma enorme quantidade de conflitos de resposta de incidente nas invasões do FIN7, em geral nos clientes que não têm os nossos produtos. O simples fato de sermos capazes de detectar a aparência deles quando estão tentando entrar na rede não é suficiente – temos que detectar alguns desses métodos mencionados pelo Barry, nos misturando e parecendo bons administradores de sistema. É bem interessante.

Alguns membros do FIN7 foram presos em agosto. Vocês perceberam algumas mudanças no grupo depois das prisões?

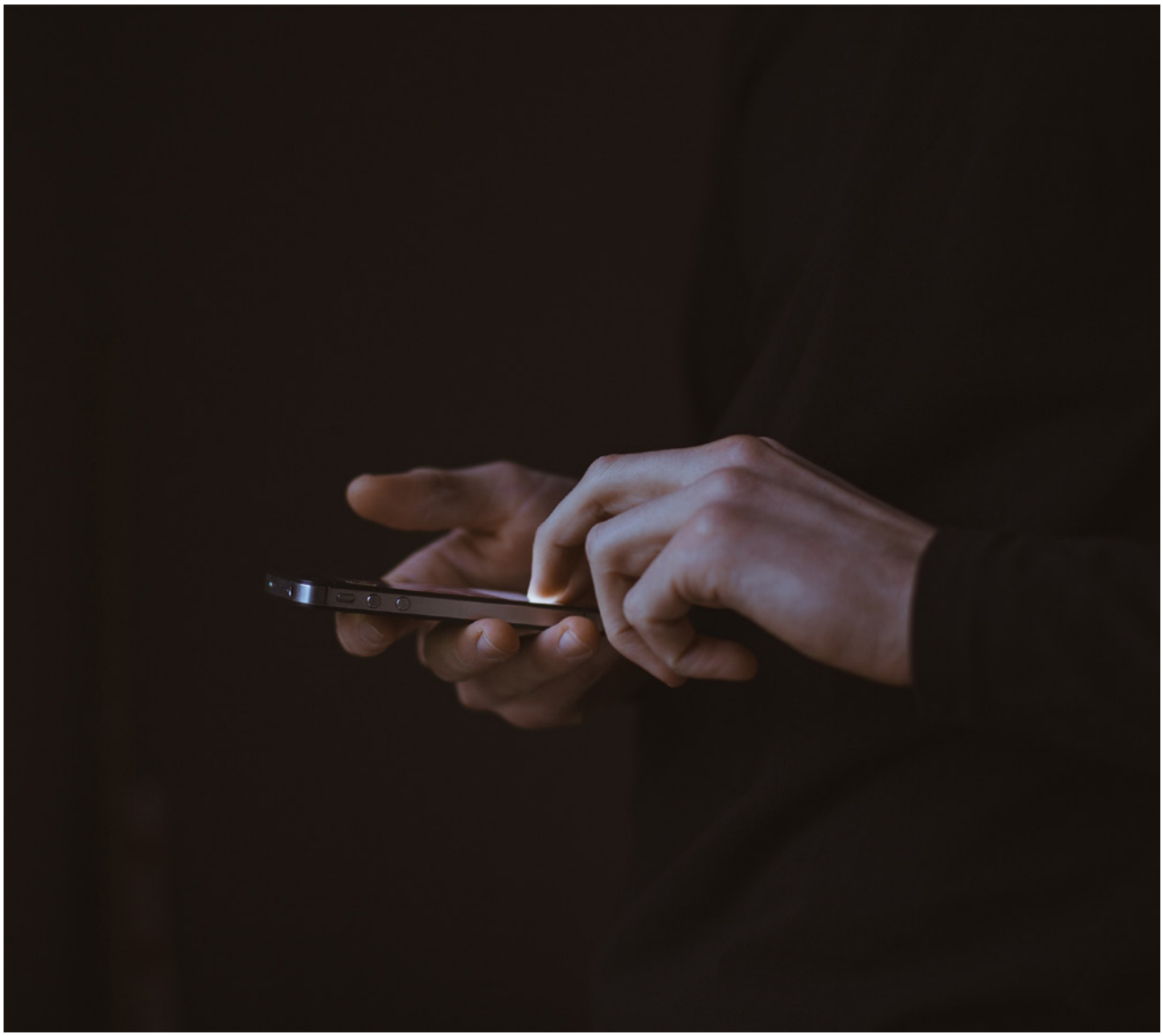
Barry: A partir do último verão, percebemos um novo backdoor de vetor inicial chamado BATELEUR, voltado para o mesmo conjunto de vítimas. Era um backdoor de Java Script diferente, mas bem similar na funcionalidade do backdoor que tínhamos visto do FIN7 no passado. Percebemos que a atividade de backdoor mal planejada tradicional do FIN7 estava mais lenta e que a atividade do BATELEUR aumentara. Assim, estamos bem confiantes de que isso é um aspecto mais novo do FIN7. Dado o tamanho aparente da organização por trás disso, pode ficar realmente difícil identificar o que é de fato controlado pela mesma organização, ou talvez seja um desenvolvedor que se afastou e está começando o seu próprio lance, ou um terceiro fornecendo infraestrutura ou malware para esta organização.

Você espera alguma mudança ocorrendo como resultado das prisões de alguns membros do FIN7?

Nick: O que vemos são as pessoas continuando a operar. Enquanto houver países sem extradição em que esses caras estejam, a maioria da atividade irá continuar.

RELÓGIO DE TENDÊNCIA

INCIDENTES GLOBAIS DE TERRORISMO CIBERNÉTICO EM ALTA



Jeremy Platt
diretor executivo, Guy Carpenter

Emil Metropoulos
vice-presidente sênior, Guy Carpenter

A natureza da ameaça terrorista que afronta a sociedade mudou consideravelmente nos últimos 20 anos. Antes, os governos e as (re)seguradoras estruturavam as suas estratégias de mitigação e respostas para lidar com ataques que eram de grande escala.

Recentemente, entretanto, vimos uma série de pequenos, menos sofisticados, mas não menos aterrorizantes atos de terrorismo pelas áreas geográficas que envolvem baixas em massa e eventos geradores de medo. E o tipo de ameaça continuará a mudar à medida que novas tecnologias e oportunidades se revelem para as organizações terroristas – o ciberterrorismo é um exemplo de uma fronteira recentemente em desenvolvimento do perigo.

Tradicionalmente, a maioria dos ciberataques tem sido realizada por organizações criminosas, com grande parte dos incidentes não sendo registrados em uma escala de risco empresarial de empresas que enfrentaram contratempos significativos. Em 2017, esta dinâmica foi mudada com os incidentes WannaCry e NotPetya. Estes dois ataques afetaram organizações em mais de 150 países, levaram à interrupção dos negócios e outras perdas estimadas em bem mais de US$ 300 milhões por algumas empresas, geraram danos reputacionais e resultaram em perda de dados dos clientes.

Em dezembro de 2017, o governo dos EUA tomou uma atitude inusitada e atribuiu o ataque WannaCry aos hackers com apoio da Coreia do Norte. O WannaCry e o NotPetya expuseram um risco sistêmico e afetaram uma ampla quantidade de empresas sem alvo específico, demonstrando o potencial de agravamento na ameaça de ciberterrorismo.

Nesse contexto, poucas tendências estão emergindo:

O panorama para os pontos de ataque está se expandindo

Os processos físicos tradicionais realizados pelos sistemas de controle industrial – inclusive setores de infraestrutura crítica como serviços públicos de energia, serviços de tratamento da água, e sistemas de saúde e emergência – estão se tornando on-line.

A Guy Carpenter, coligada da Oliver Wyman, prevê que 30 bilhões de dispositivos conectados estarão em uso em 2030, criando mais ativos suscetíveis a ataques e agregando mais vulnerabilidades a explorar.

Os ciberataques estão se tornando mais avançados

O aumento de hackers altamente capacitados, em geral com apoio de países, está coincidindo com o desenvolvimento de ferramentas mais sofisticadas que parecem estar penetrando no ambiente mais amplo por meio de um mercado paralelo em franca expansão.

As consequências são muitas

As empresas estão agora profundamente dependentes de seus sistemas e dados, e a interferência com esses ativos pode afetar significativamente a capitalização do mercado e colocar em perigo a liderança executiva, as reputações, vendas e lucros. As falhas em cibersegurança têm o potencial para desestabilizar um empreendimento da noite para o dia.

Começou a ocorrer uma mudança na natureza dos incidentes cibernéticos: desde afetar principalmente os consumidores até causar um impacto nos sistemas políticos e econômicos globais como um todo

Exemplos desta tendência em mudança são as recentes manchetes cobrindo o setor bancário. Ciberataques em grande escala no setor bancário podem resultar em dinheiro e informações pessoais roubados confiados pelos clientes a estas instituições e também, em um cenário bem pior, gerar uma “corrida” ao sistema bancário global. Os grupos terroristas têm metas ambiciosas para os ataques cibernéticos induzidos. Os sistemas de controle industrial que dão suporte ao setor de eletricidade são totalmente fechados para ameaças externas. Contudo, as proteções que vêm com o isolamento enfraqueceram a introdução de controles automatizados administrados pelos sistemas de rede interconectados.

À medida que cresce a automação, assim também aumenta a oportunidade de manipulação de um sistema de controle industrial por meio de um ciberataque.

Para serviços públicos e outras instalações de infraestrutura, os custos potencias de uma interrupção em uma malha de transmissão como resultado de um ciberataque podem incluir:

- Receita perdida;
- Despesas adicionais para restaurar as operações e melhorar as defesas de cibersegurança;
- Multas regulatórias e fiscalização adicional; e
- Danos reputacionais

Esses ataques, embora raramente tornados públicos, estão ocorrendo com mais frequência. Os autores potenciais de atos de ciberterrorismo podem ser separados em cinco categorias: crime organizado, hacktivismo, grupos terroristas não estatais, lobos solitários e estados nacionais. Embora as motivações, capacidades e prioridades variem entre os grupos, cada um deles pode causar estragos em uma escala global; com financiamento em ritmo acelerado de crescimento, esses ataques podem se tornar mais catastróficos.

Com a convergência desses fatores, a oportunidade poderia combinar com os motivos existentes para infligir às empresas perdas catastróficas pelo ciberterrorismo. Ao longo do tempo, as apólices de seguro cibernético evoluíram para cobrir a falha da tecnologia e a interrupção resultante ou a perda da receita. As seguradoras também estão reconhecendo cada vez mais a interdependência dos negócios, em especial por meio da tecnologia.

Muitas apólices de seguro cibernético agora contêm disposições para interrupção de negócio e interrupção de negócio contingente, inclusive aquelas que envolvem pane na cadeia de abastecimento de uma organização a partir de uma violação de dados.

A cobertura da interrupção do negócio tornou-se um componente mais comum de cobertura nas apólices de seguro cibernético nos últimos 24 meses. As soluções de resseguro no ciberespaço tendem a seguir a cobertura de segurança e privacidade oferecida no mercado de seguros. Embora o texto dos contratos de resseguro varie, o seguro cibernético geralmente cobre incidentes de segurança de rede, não obstante as crenças políticas ou ideológicas de um agente não estatal.

O Cyber Solutions Specialty Practice and Global Cyber Center of Excellence dedicado da Guy Carpenter trabalha com profissionais pelo mundo para fornecer soluções de transferência de risco visando ajudar as empresas a quantificar cenários potencialmente catastróficos e identificar o caminho certo para administrar, afastar e transferir os riscos associados. Estruturamos uma ampla gama de soluções customizadas de resseguro utilizando nossas capacidades de modelização internas combinadas com nosso investimento em modelos terceirizados para criarmos a nossa própria visão de risco cibernético holística e da melhor categoria para os nossos clientes.

ANÁLISE DETALHADA DO SETOR

COMO UM CIBERATAQUE PODERIA CAUSAR A PRÓXIMA CRISE FINANCEIRA

Paul Mee
sócio e chefe de cibernética, Oliver Wyman

Til Schuermann
sócio, Serviços Financeiros, Oliver Wyman

Este artigo foi inicialmente publicado na Harvard Business Review

Desde que a falência forçada do banco de investimento Lehman Brothers desencadeou a crise financeira há 10 anos, os reguladores, gestores de risco e presidentes de banco central pelo mundo passaram a reforçar a capacidade dos bancos de tolerar impactos financeiros.

Mas a próxima crise pode não vir de um choque financeiro. O culpado mais provável: um ciberataque que cause interrupção nas capacidades dos serviços financeiros, em especial nos sistemas de pagamento, por todo o mundo.

Os criminosos sempre buscaram formas de se infiltrar nos sistemas de tecnologia financeira. Agora, o sistema financeiro enfrenta o risco adicional de tornar-se dano colateral em um ataque mais amplo à crítica infraestrutura nacional. Esse ataque poderia abalar a confiança no sistema global de serviços financeiros, fazendo com que bancos, empresas e clientes ficassem frustrados, confusos ou em pânico, o que, por sua vez, poderia causar um grande impacto negativo sobre a atividade econômica.

Somente o crime cibernético custa aos países mais de US$ 1 trilhão globalmente, bem mais do que o recorde de US$ 300 bilhões de danos devido a desastres naturais em 2017, de acordo com uma análise recente realizada pela nossa empresa. Classificamos os ciberataques como a maior ameaça enfrentada pelas empresas no mundo atual – bem à frente do terrorismo, das bolhas especulativas e outros riscos.

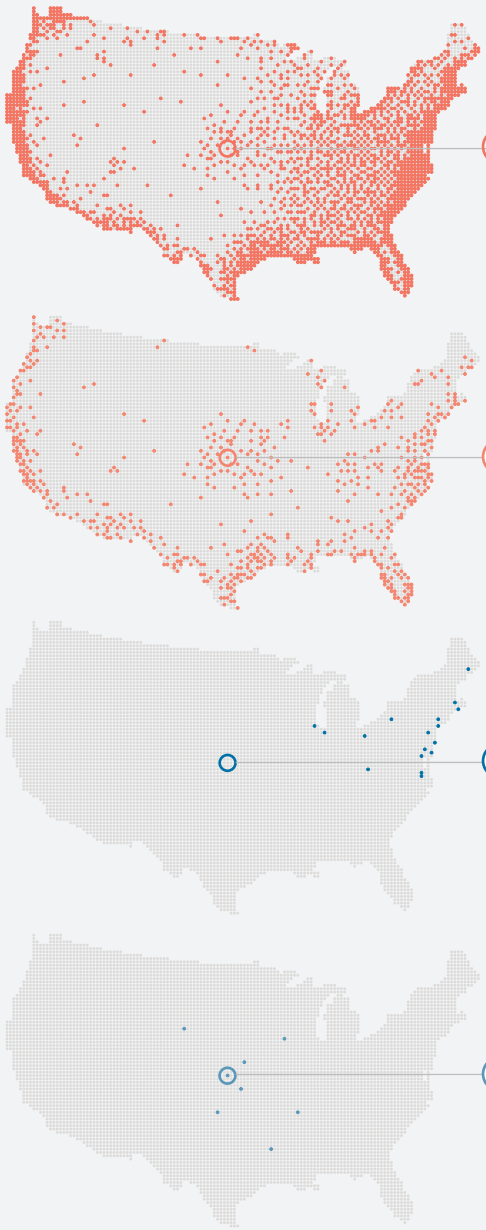
Um ataque no processamento de um computador ou na rede de comunicações poderia causar danos econômicos de US$ 50 bilhões a US$ 120 bilhões, um nível de perda entre aquela dos furacões Sandy e Katrina, de acordo com as estimativas recentes. Mas não é improvável um ataque tão mais amplo e debilitante. Só no mês passado, o FBI emitiu uma advertência para os bancos sobre um ataque em grande escala pendente conhecido como um ataque de saques de dinheiro dos caixas automáticos, em que ondas de saques fraudulentos sincronizados esvaziam as contas bancárias. Enquanto isso, em julho foi revelado que hackers trabalhando para a Rússia penetraram facilmente nas salas de controle dos serviços públicos de eletricidade dos EUA e poderiam ter causado blecautes.

“Somente o crime cibernético custa aos países mais de US$ 1 trilhão globalmente, um múltiplo do recorde de US $ 300 bilhões de danos devido a desastres naturais em 2017, de acordo com uma análise recente realizada pela nossa empresa”

Como seria possível explicar uma crise financeira detonada por um ciberataque? Um cenário provável seria um ataque por uma nação criminosa ou grupo terrorista em instituições financeiras ou importante infraestrutura. Na Coreia do Norte, por exemplo, o Grupo Lazarus, também conhecido como Hidden Cobra, rotineiramente busca formas de expor bancos e explorar criptomoedas. Um ataque a um banco, fundo de investimento, empresa custodiante, rede de caixas automáticos, a rede de mensagens entre bancos conhecida como SWIFT, ou o próprio Federal Reserve (Banco Central dos EUA) representaria um ataque direto ao sistema de serviços financeiros.

Como seria possível explicar uma crise financeira detonada por um ciberataque? Um cenário provável seria um ataque por uma nação criminosa ou grupo terrorista em instituições financeiras ou importante infraestrutura. Na Coreia do Norte, por exemplo, o Grupo Lazarus, também conhecido como Hidden Cobra, rotineiramente busca formas de expor bancos e explorar

ANEXO 9: COMO UM CIBERATAQUE SE ESPALHA
A rapidez da disseminação dos ciberataques depende dos controles instalados para impedir isso. A seguir, exploramos até onde um vírus de ciberataque poderia se espalhar em 60 horas em quatro cenários diferentes



SEM CONTROLES
O vírus se espalha rapidamente por todas as áreas povoadas dos Estados Unidos

CONTROLES DE DETECÇÃO
O vírus se espalha em um ritmo mais lento

CONTROLES DE PROTEÇÃO
O vírus se espalha no máximo para a metade do país, na 52ª hora a disseminação diminui e o vírus é eliminado de algumas áreas

CONTROLES DE IDENTIFICAÇÃO
O vírus se espalha em um ritmo mais lento e fica próximo ao ponto de origem

SESSENTA HORAS

Quatro possíveis cenários de disseminação do vírus depois de 60 horas

PONTO DE ORIGEM DO VÍRUS
Um vírus se espalha pelo uso de um dispositivo de ponto de venda

Fonte: Análise da Oliver Wyman

criptomoedas. Um ataque a um banco, fundo de investimento, empresa custodiante, rede de caixas automáticos, a rede de mensagens entre bancos conhecida como SWIFT, ou o próprio Federal Reserve (Banco Central dos EUA) representaria um ataque direto ao sistema de serviços financeiros.

Outra possibilidade seria se um professo hacktivista ou amador "script kiddy" resolvesse usar programas mal-intencionados para lançar um ciberataque sem a devida consideração quanto às consequências. Esse ataque poderia causar uma reação em cadeia, com danos bem além do pretendido originalmente, devido a regras, normas de batalha e princípios que são de conhecimento convencional na maior parte das situações de guerra, mas que não existem de forma significativa na arena digital.

Por exemplo, em 2016 um "script kiddie" realizou uma negação de serviço congestionando Twitter, Spotify e outros serviços de internet de renome à medida que amadores aderiam a título de brincadeira. O dano poderia ser significativo, fosse o grande ciberataque deliberado ou mesmo acidental. A maioria das redes de caixas automáticos pela América do Norte poderia ser interrompida. Os sistemas de cartão de crédito e outros pagamentos poderiam falhar por nações inteiras, como aconteceu com a rede VISA no Reino Unido em junho. Os bancos on-line poderiam tornar-se inacessíveis: nada de dinheiro, pagamentos, ou informações confiáveis sobre as contas bancárias. Os bancos perderiam a capacidade de negociar entre si durante um período crítico de incerteza. Poderia haver pânico generalizado, embora temporário.

Esse resultado poderia não causar o tipo de crise financeira de longa inquietação ocorrida na Grande Recessão, pois o dinheiro seria provavelmente restituído aos bancos e aos provedores de serviços de pagamento assim que os sistemas voltassem a ficar on-line. Ao mesmo tempo, não está claro como um banco central, o tradicional bombeiro das crises financeiras, poderia responder a este tipo de crise no curto prazo. Depois que o problema fosse resolvido e a crise fosse suspensa, uma tarefa dificílima de recuperação despontaria. Seria bem mais difícil se os dados forem corrompidos, manipulados ou tornados inacessíveis.

Como impedir esse cenário? As empresas devem implantar sistemas que permitam que elas interrompam a disseminação de um contágio de ciberataque, e que retomem as operações do modo mais rápido e suave possível. O setor de serviços financeiros precisa concordar inteiramente, e estar preparado para colocar em prática, quanto a estratégias de resposta coordenada e recuperação para evitar danos sistêmicos. Os reguladores em muitos países vêm trabalhando diligentemente na preparação para os ciberataques e na sua redução, mas precisam olhar além das próprias fronteiras e introduzir regulamentações, leis e estruturas empresariais em uníssono, como a Network and Information Security Directive da União Europeia, que é projetada para proteger uma lista sempre crescente de infraestrutura crítica de sistemas bancários e de assistência à saúde para mercados on-line e serviços na nuvem.

Muitas destas medidas estão sendo tomadas em vários níveis. Mas é preciso fazer muito mais. Um ataque que abale a confiança naquelas máquinas poderia gerar consequências debilitantes sobre o fluxo do dinheiro entre clientes, empresas e instituições financeiras pelo mundo.

ANÁLISE DETALHADA DO SETOR

O SETOR DE AVIAÇÃO PODE ESTAR VULNERÁVEL AO CIBERATAQUE POR MEIO DE SUA CADEIA DE ABASTECIMENTO GLOBAL

Paul Mee
sócio e chefe de cibernética, Oliver Wyman

Brian Prentice
sócio, Aviação, Oliver Wyman

Publicado na Forbes.com em abril de 2018

Em março, o Departamento de Segurança Interna dos EUA e o FBI emitiram um alerta preocupante: A partir do mesmo mês dois anos antes, hackers russos patrocinados pelo estado vêm se infiltrando na rede de eletricidade do país e em vários setores da infraestrutura, incluindo aviação, coleta de informações sobre como as redes foram organizada e quais controles dos sistemas estão instalados. Embora não pareça ter sido perpetrada uma sabotagem, permanece a questão – o que os russos pretendem fazer com os dados coletados?

Embora todos esses setores, em especial os seus maiores participantes, tendam a ter instalada uma ampla cibersegurança, ela pode não ser tão abrangente quanto o país esperaria. Nesse caso, em vez de obter acesso pela porta da frente, onde o sistema de alarme era mais robusto, esses hackers simplesmente davam a volta e entravam pelas redes mais vulneráveis de operações de terceiros e fornecedores, contando com uma infinidade de técnicas que incluíam o uso de e-mails de phishing infectados com malware e o roubo de credenciais.

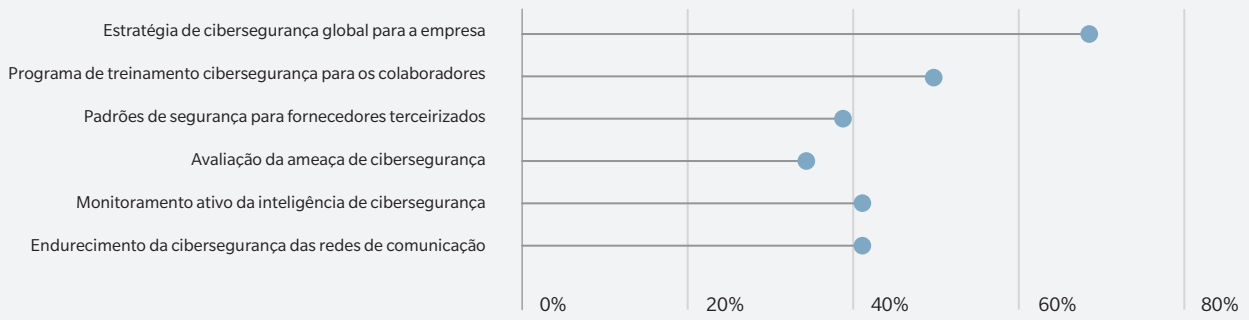
Desnecessário dizer que o cenário causaria arrepios nos setores de aviação e aeroespacial. Enquanto as principais fabricantes de aeronaves e as linhas aéreas são alvos óbvios devido ao potencial que representam de interromper visivelmente o comércio internacional, elas também se classificam no topo das listas de vítimas dos hackers porque mantêm cadeias de abastecimento globais e altamente conectadas que, nos últimos anos, vêm ativamente tornando digitais as operações. Quanto mais digitais, maior a superfície de ataque para os hackers. Os vários links sobre cadeia de abastecimento da aviação e aeroespacial – algumas de grande porte, muitas de pequeno a médio portes – se tornaram todos vulnerabilidades potenciais, dada a difícil tarefa de assegurar que todos os fornecedores com acesso insistam no mesmo nível de rigor tanto na cibersegurança quanto no treinamento de seus colaboradores.

VULNERABILIDADES NA CADEIA DE ABASTECIMENTO

As maiores organizações dentro de um setor podem ter cibersegurança avançada; o mesmo nem sempre pode ser dito da vasta rede de provedores de serviço e fornecedores, muitos dos quais são membros do setor de MRO (manutenção, reparo e reformas) que presta serviços às aeronaves do país.

Em 2018, na pesquisa da Oliver Wyman sobre o setor de MRO, as respostas revelaram brechas potenciais na proteção. Por exemplo, enquanto 67% das pessoas pesquisadas afirmaram que a sua empresa estava preparada para um ciberataque, menos da metade foi capaz de dizer se tinham conduzido uma análise de cibersegurança em 2017. Somente 9% dos provedores independentes de MRO, 50% dos fabricantes de estruturas e revestimentos de aeronaves e fabricantes de componentes, e 41% das linhas aéreas confirmaram que tinham criado padrões de segurança para os fornecedores terceirizados. Isso deixa, potencialmente, muitas empresas sem uma visão clara da segurança digital dos fornecedores – quase todos eles mantêm credenciais para fazer logon nos seus sistemas.

ANEXO 9: QUAIS AS SALVAGUARDAS DE CIBERSEGURANÇA IMPLANTADAS PELA SUA EMPRESA?
% do total das pessoas pesquisadas que selecionaram cada resposta



Fonte: Análise da Oliver Wyman

E essa falta de conhecimento pode levar ao desastre, como as principais empresas descobriram nos últimos cinco anos. Em 2013, por exemplo, os hackers usaram credenciais roubadas de um fornecedor de aquecimento, ventilação e ar condicionado para penetrar na rede da gigante varejista Target, roubando dados de 70 milhões de clientes e informações sobre 40 milhões de cartões de pagamento. O custo para a Target: perto de US$ 300 milhões.

Enquanto os cibercriminosos de décadas atrás pareciam motivados pelo dinheiro que poderiam ganhar com os dados roubados, as recentes brechas parecem mais ter a intenção de criar o caos organizacional. Em junho de 2017, os hackers – provavelmente do setor militar russo, conforme acreditavam a CIA e a inteligência britânica – atacaram a Ucrânia com software que literalmente destruía os dados e desarticulava as operações no sistema bancário daquele país, nos ministérios governamentais e no metrô, assim como na antiga central elétrica de Chernobyl.

UMA EMERGÊNCIA GLOBAL

De lá, o ransomware arrasador chamado NotPetya infectou sistemas de computador pelo mundo, inclusive aqueles do conglomerado de despacho dinamarquês Maersk. Isso levou a graves atrasos nos principais portos como Roterdã, Bombaim e o Porto de Nova York e New Jersey, e a paralisação temporária do maior terminal no porto de Los Angeles. É sobre ataques assim que se deve instigar as empresas de transporte para que reavaliem o seu nível de preparo cibernético.

Globalmente, o hacking tornou-se um setor em crescimento, custando às economias pelo mundo mais de meio trilhão de dólares dos EUA anualmente – uma quantia que vem crescendo a cada ano. Em alguns países, os hackers trabalham fora de escritórios regulares e recebem para passar o dia de trabalho procurando vulnerabilidades nas redes digitais das organizações, ficando à espera de brechas para desenvolver pelas quais possam penetrar e roubar informações ou pior.

Os especialistas imaginam que haja mais de 300.000 hackers profissionais em todo o mundo. Em lugares como Rússia, China, Leste Europeu e Coreia do Norte, o hacking tornou-se um setor em crescimento.

Para montar uma estratégia abrangente e unificada de cibersegurança e gestão de risco para o setor, os provedores de MRO devem considerar seriamente a prática de diversas ações. Primeiro, as empresas do setor devem conduzir auditorias independentes dos programas de cibersegurança existentes. Isso inclui verificar tudo, desde o entendimento de quem e do que tem acesso à rede de computadores de uma empresa, até se um processo de detecção em tempo real e um mecanismo de resposta foram delineados, pelos quais os gerentes são responsáveis em cada etapa da execução do protocolo de cibersegurança, até se existe um processo de supervisão para garantir que os procedimentos sejam seguidos e documentados.

PADRÃO DO SETOR

O setor como um too também deve desenvolver uma estrutura clara para mitigação e gestão dos riscos cibernéticos. O National Institute of Standards and Technology (NIST) desenvolveu um conjunto de padrões e melhores práticas específicos do setor para serem aproveitados no projeto de uma estrutura de cibersegurança.

Por fim, o setor deve trabalhar nas empresas visando fortificar os seus sistemas de tecnologia da informação – tanto a infraestrutura quanto a conservação – e criar uma cultura atenta à segurança. Enquanto não existe solução garantida para impedir todos e quaisquer ataques, o desenvolvimento de uma abordagem holística à gestão de risco de cibersegurança a ser compartilhada pelo setor – e atualizada regularmente – pode dar às empresas um certo fôlego. Os cibercriminosos certamente não estão parados.

ANÁLISE DETALHADA DO SETOR

O BLOCKCHAIN PODE AJUDAR A REDUZIR O RISCO CIBERNÉTICO DO SETOR FINANCEIRO?

Erin English
estrategista de segurança sênior,
Microsoft

Dada a frequência aumentada dos ciberataques, os reguladores financeiros identificam a cibersegurança como um dos riscos mais prementes ao setor de serviços financeiros. Mais ainda, devido à interconexão do sistema financeiro global, um ciberataque em um banco pode afetar outros bancos e instituições financeiras.

Estas considerações se aplicam com igual força aos permissioned blockchains, que contam com interconexões em curso. Enquanto o setor de serviços financeiros explora o uso dos permissioned blockchains – que limitam o acesso a uma determinada planilha para determinadas partes conhecidas ou fidedignas em um consórcio – para melhorar serviços e operações, os participantes do setor devem reconhecer e levar em conta uma série de capacidades de cibersegurança – bem como os riscos – referentes a esta tecnologia.

VANTAGENS DO BLOCKCHAIN...

Um dos benefícios do blockchain é a sua resiliência inerente na mitigação de riscos e ataques cibernéticos, em particular aqueles direcionados às instituições financeiras. Embora não seja imune a todas as formas de risco cibernético, a estrutura única do blockchain fornece capacidades de cibersegurança que não estão presentes em outras tecnologias herdadas. A seguir, temos algumas das vantagens da tecnologia no combate ao risco cibernético:

- A arquitetura distribuída de um blockchain aumenta a resiliência de toda a rede ser exposta para ficar comprometida a partir de um único ponto de acesso ou ponto de falha
- Os mecanismos de consenso – um importante recurso dos blockchains – melhoram a robustez global e a integridade de registros compartilhados, pois o consenso entre os participantes da rede é um pré-requisito para a validação de novos blocos de dados e mitiga a possibilidade de que um hacker ou um ou mais participante comprometido da rede possa corromper ou manipular um registro específico
- Os blockchains também fornecem aos participantes uma maior transparência, tornando bem mais difícil corromper os blockchains por malware ou ações manipulativas. Mais ainda, os blockchains podem conter vários níveis de segurança – tanto na rede quanto instalados em cada participante
- Por fim, os blockchains hospedados em uma plataforma na nuvem, como o Microsoft Azure, oferecem proteções de cibersegurança até maiores devido aos controles de acesso da plataforma e muitas outras proteções

...E RISCOS

A despeito de muitos benefícios da cibersegurança inerentes aos blockchains, esta tecnologia, como qualquer outra, permanece sujeita a riscos de cibersegurança inerentes que exigem uma gestão de risco equilibrada e proativa.

Muitos desses riscos envolvem um elemento humano, como a manutenção da confidencialidade, integridade e disponibilidade de chaves privadas; erros humanos de codificação que podem introduzir o risco de cibersegurança dos aplicativos fora da cadeia; dados não seguros que podem ser ingeridos de fontes externas; ataques baseados na identidade que pretendem corromper o mecanismo de consenso de um blockchain; e ameaças avançadas que podem corromper os processos de tomada de decisão do blockchain. Por conseguinte, um programa robusto de cibersegurança permanece vital para a proteção da rede e das organizações participantes com respeito a ameaças cibernéticas, em especial à medida que os hackers desenvolvem mais conhecimento sobre os permissioned blockchains e suas vulnerabilidades.

Uma série de importantes considerações estruturais deve ser levada em conta por ocasião da construção de programas de cibersegurança para blockchains. Por exemplo, os registros adicionados a um blockchain em geral são imutáveis. Esta imutabilidade impede a intervenção indevida e cria um registro auditável, mas pode exigir um ajuste especial na programação para restaurar a integridade de um blockchain caso sejam introduzidas transações fraudulentas ou mal-intencionadas no registro. Além disso, os papéis e responsabilidades dos participantes do blockchain exigem uma estrutura zelosa de governança para alcançar um equilíbrio eficaz entre acesso e segurança.

NECESSIDADE DE UMA ESTRUTURA EFICAZ

Ao levar em consideração as ferramentas de política pública para melhorar a segurança dos blockchains, os princípios e controles de cibersegurança das leis, regulamentações e diretrizes existentes do setor permanecem componentes críticos para um programa eficaz

de cibersegurança para implantações de blockchain. Sem dúvida, a maior parte dos provedores de serviço na nuvem, em especial aqueles que dão suporte ao setor de serviços financeiros, já deve ter instalados estes controles.

A Microsoft e a Câmara de Comércio Digital recentemente publicaram um informativo, Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry, para aprofundar o diálogo da política de cibersegurança entre os provedores da tecnologia de blockchains, como a Microsoft, e as organizações de serviços financeiros usando blockchain e suas reguladoras.

Embora seja encorajador para as instituições financeiras que as diretrizes e regulamentações familiares para a cibersegurança sejam tão pertinentes quanto o são para os blockchains, o processo de aplicação desses padrões exigirá novas abordagens de múltiplas partes interessadas para o setor e o governo.

PRÓXIMAS ETAPAS

Ademais, a eficácia destas regras existentes – que não foram projetadas para a tecnologia do blockchain especificamente – é em geral suficientemente ampla para cobrir esta nova tecnologia. Com isto em mente, defendemos que as seguintes recomendações para os formuladores de políticas e participantes do setor fornecem uma estrutura para uma abordagem inteligente e coordenada visando a promoção do desenvolvimento de aplicativos seguros de blockchain através de padrões de cibersegurança viáveis.

- Solicita uma versão sob medida da estrutura de cibersegurança do NIST para as atividades dos permissioned blockchain. Os participantes do setor de serviços financeiros devem otimizar a estrutura para os permissioned blockchains, levando o foco da cibersegurança da organização ou da empresa para a cibersegurança da rede

- Encorajar o diálogo entre regulador e setor, inclusive por meio de áreas restritas regulatórias. Para que os reguladores entendam o risco de cibersegurança nos permissioned blockchains, devem primeiro ter um entendimento detalhado sobre as tecnologias e como elas funcionam. Os participantes do setor podem ajudar a fornecer este entendimento ao manter um diálogo franco com os reguladores com relação aos permissioned blockchains, suas oportunidades e seus riscos.

- Encorajar os formuladores de políticas a reconhecer os benefícios únicos de cibersegurança das tecnologias dos blockchains. Enquanto as tecnologias dos blockchains continuam a evoluir para uma gama ampliada de aplicativos e setores, os formuladores de políticas estão antenados com os benefícios únicos destas tecnologias, incluindo os benefícios da cibersegurança

- Estimular a harmonização entre padrões de cibersegurança aplicados aos permissioned blockchains. . A convocação de conselhos colegiados e órgãos regentes do setor público-privado é uma etapa útil para certificar se a orientação de cibersegurança aplicável à tecnologia do blockchain é compatível e não impede a inovação

PROTEGENDO AS INFORMAÇÕES DOS CLIENTES

O setor de serviços financeiros se beneficia de forma extraordinária do crescimento do blockchain devido às aplicações dos muitos serviços financeiros da tecnologia. À medida que as ameaças cibernéticas continuam a evoluir em complexidade e intensidade, as tecnologias emergentes, como os permissioned blockchains, podem contribuir para os importantes objetivos de redução do risco de cibersegurança e proteger de modo adequado as informações financeiras dos clientes e a integridade do sistema financeiro global.

Os permissioned blockchains oferecem capacidades de cibersegurança significativas, compartilham alguns dos mesmos riscos cibernéticos que afetam outros sistemas de TI, e têm características únicas, tudo isso digno de mais consideração e avaliação por governos e indústrias.

ANÁLISE DETALHADA DO SETOR

O SETOR DE ASSISTÊNCIA À SAÚDE ASIÁTICO ESTÁ DEBILITADO PELOS CIBERATAQUES

Jayant Raman
sócio, Prática Financeira e de Risco, Oliver Wyman

Prashansa Daga
chefe de prática de Saúde e Ciências da Vida, Marsh

Kitty Lee
diretora, Prática de Saúde e Ciência da Vida, Oliver Wyman

A assistência à saúde é um dos setores mais vulneráveis para os ciberataques, com mais de uma em quatro (27%) organizações de assistência à saúde comunicando terem sido uma vítima de um ciberataque nos últimos 12 meses. Isso é mais do que nas instituições financeiras (20%) e cerca de duas vezes a incidência no setor de comunicações, mídias e tecnologia (14%). A despeito disso, as pessoas pesquisadas do setor de assistência à saúde subestimam a probabilidade de um ciberataque.

Como os impactos potenciais dos ciberataques são transfronteiriços, nenhum país está totalmente imune a este fenômeno. Ataques de ransomware, como o WannaCry e o Petya, tiveram um alcance global que afetou os negócios de assistência à saúde e as seguradoras na região. Em comparação com seus equivalentes globais, leva-se cinco vezes mais tempo para detectar um invasor para as empresas da Ásia-Pacífico.

AMEAÇAS OBSERVADAS

Os participantes da última Pesquisa de Percepção do Risco Cibernético Global da Marsh-Microsoft foram perguntados sobre a sua percepção dos cenários de perda cibernética que poderiam causar o maior impacto.

A interrupção do negócio foi destacada como a principal preocupação de risco cibernético no setor de assistência à saúde (69%), como ocorre em outros setores. Em 2017, o ataque global WannaCry teve sucesso no desligamento temporário dos sistemas de TI dos hospitais em todo o mundo. Em situações com mais ameaças à vida, os hackers cibernéticos podiam comprometer dispositivos médicos, como máquinas de MRI (ressonância magnética) ligadas à rede de saúde, como pontos de entrada para redes Wi-Fi não seguras, causando graves danos aos dispositivos médicos.

Violação de informações dos clientes é um cenário mais assustador em assistência à saúde (67%) do que nos outros setores. Um registro médico contém dados imensos sobre uma pessoa e, quando comprometido, não pode ser reemitido ou suspenso, como no caso de um cartão de crédito. Os cibercriminosos podem usar, e até mesmo manipular, esses dados para causar sérios aborrecimentos, danos à reputação dos usuários ou comprometimento das contas da empresa, ou para monetizar os dados roubados.

GRAVES CONSEQUÊNCIAS FINANCEIRAS

O setor de assistência à saúde está mais preocupado com agentes da ameaça motivados financeiramente: 45% das pessoas

ANEXO 6: PRINCIPAIS CENÁRIOS DE PERDA CIBERNÉTICA COM O MAIOR IMPACTO POTENCIAL OBSERVADO

Fonte: Mantendo os cuidados com a saúde sob resgate: Perspectivas do setor sobre riscos cibernéticos. Centro Global de Riscos da Marsh and McLennan Companies

pesquisadas do setor de assistência à saúde indicaram os grupos de crime organizado ou hacktivismo como a sua principal fonte de preocupação.

Mais ainda, observamos que os ciberataques causam impactos financeiros mais graves dentro do setor de assistência à saúde. Mais de 70% das pessoas pesquisadas de assistência à saúde imaginam que cada cenário de violação cibernética no setor custe mais de US$ 1 milhão, em comparação com uma média entre setores de 65% que se sentem da mesma forma. De fato, um custo total médio de violações de dados no exercício fiscal de 2017 foi de US$ 3,6 milhões por empresa pelos setores, de acordo com o Ponemon Institute.

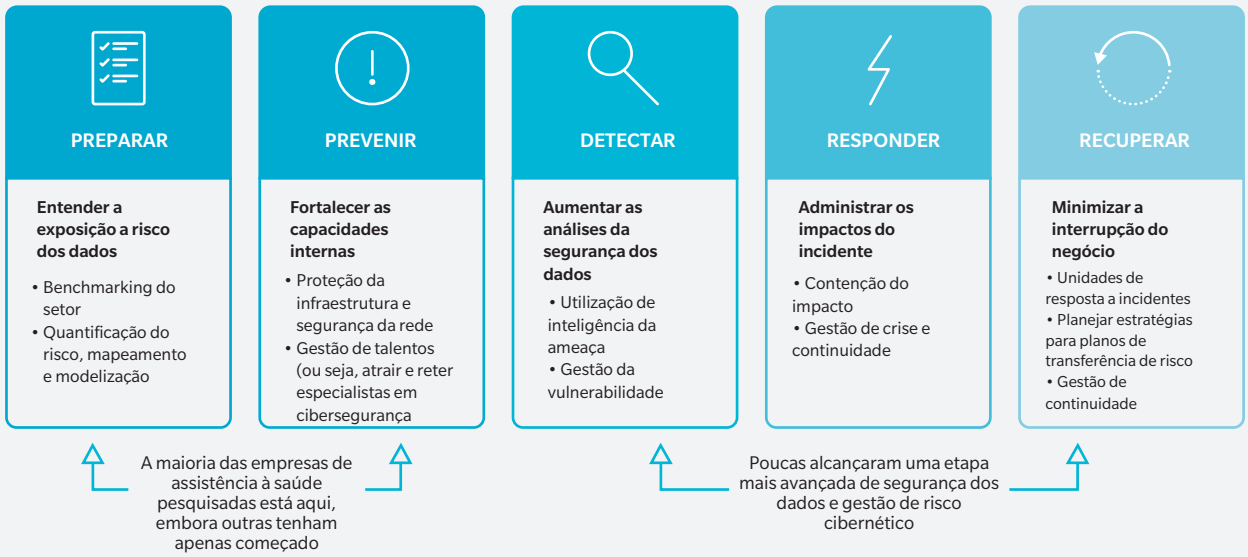
ABORDAGEM 360

Uma estratégia totalmente inclusiva de dados e risco cibernético se baseia em uma análise de risco minuciosa, um apetite por risco definido e na quantificação da exposição a risco. Assim, a estratégia de gestão de risco determina a governança correta, identifica ameaças e ações corretivas, e quantifica o valor do investimento necessário para preencher lacunas e vulnerabilidades. Como parte das expectativas da administração, dos acionistas, reguladores e agências de classificação, serão projetados mecanismos específicos do setor para salvaguardar contra incidentes, bem como para implantar um manual de estratégias atualizado e documentado sobre incidente cibernético no caso de violações.

PREPARAR E PREVENIR

Um diagnóstico de grave risco interno, logo de início, é necessário para avaliar os riscos cibernéticos de uma empresa em comparação com as colegas do setor. 40% das organizações de assistência à saúde ainda não conduziram uma avaliação de lacuna de cibersegurança nos últimos dois anos, e há espaço para melhorias no entendimento e na administração de sua exposição ao risco global. As organizações de assistência à saúde precisam identificar, definir e mapear as ameaças e os cenários específicos de ataques cibernéticos aos seus ativos tangíveis e intangíveis. Essas práticas customizadas devem se tornar um procedimento operacional padrão no setor de assistência à saúde.

ANEXO 7: CINCO FUNÇÕES IMPORTANTES DA ESTRUTURA DA CIBERSEGURANÇA E AÇÕES RECOMENDADAS



Fonte: Mantendo os cuidados com a saúde sob resgate: Perspectivas do setor sobre riscos cibernéticos. Centro Global de Riscos da Marsh and McLennan Companies

Uma força de trabalho instruída e uma cultura de cibersegurança são imperativas no combate aos ciberataques cada vez mais complexos e frequentes. Muitos incidentes cibernéticos tentados e bem sucedidos nas organizações de assistência à saúde foram atribuídos a erro humano.

A necessidade de mudar de uma estratégia de proteção cibernética induzida pela TI para uma disciplina madura de gestão de risco requer uma abordagem ascendente, como a criação de uma força de trabalho mais especializada em cibernética e o fortalecimento de uma cultura de cibersegurança no local de trabalho.

O fortalecimento de segurança de rede deve ser uma prioridade dada a proliferação da Internet das Coisas (IoT) e dos dispositivos móveis com acesso às redes corporativas. As organizações de assistência à saúde devem dar ênfase às práticas comprovadas de higiene da cibersegurança – que não estão presentes na metade do setor de assistência à saúde hoje em dia. As pessoas pesquisadas admitem não ter criptografia de hardware (47%) e autenticação multifator para as redes corporativas (50%) Apenas a metade das pessoas pesquisadas do setor de assistência à saúde melhoraram a vulnerabilidade e a administração de patches no ano passado.

DETECTAR E RESPONDER

Os departamentos de TI são os principais proprietários e tomadores de decisão de gestão de risco pelo setor de assistência à saúde globalmente. Em geral, os riscos cibernéticos parecem como um melhoramento, não como parte de uma avaliação holística de gestão de risco. Ao assumir uma abordagem mais proativa para melhorar a cibersegurança, as organizações são encorajadas a entender mais o retorno sobre o risco, por meio da quantificação, e a elaborar capacidades internas pelas múltiplas áreas funcionais interconectadas alinhadas com a sua estratégia cibernética. Uma abordagem liderada pela administração para determinar o apetite por risco cibernético é uma primeira etapa para o reconhecimento de que o risco cibernético é um risco para toda a empresa.

O apoio a estruturas avançadas de resiliência de dados é um ótimo mecanismo de detecção e plano de resposta a incidente holístico. Quase dois terços das organizações de assistência à saúde não desenvolveram um plano de resposta a incidente cibernético.

E mais alarmante, 37% das pessoas pesquisadas não estão certas quanto aos motivos por trás da falta de um plano de resposta cibernético, enquanto apenas 22% estão confiantes de que a cibersegurança e os firewalls da sua organização são adequados.

RECUPERAR

Os principais riscos enfrentados pelas organizações de assistência à saúde hoje em dia incluem exposição de dados dos pacientes, sistema compartilhado de exposição de dados e exposição do colaborador. Com o reconhecimento de que os riscos cibernéticos não podem ser eliminados, as organizações de assistência à saúde estão começando a ver o seguro ou os programas de transferência de risco cibernético como uma forma de mudar os riscos, como uma solução para a proteção do balanço patrimonial e para comprovação e conformidade contratuais. Instigados pela onda de ataques de alto nível e novas regras de proteção de dados, os prêmios anuais brutos de seguro cibernético cresceram em 34% ao ano durante os últimos sete anos. A European Union Agency for Network and Information Security também descobriu uma correlação positiva entre a diminuição do seguro cibernético e o nível de preparação – e as organizações de assistência à saúde apenas estão começando a reconhecer isso.

Enquanto menos da metade das organizações que responderam à pesquisa de assistência à saúde (49%) tem cobertura de seguro cibernético, o número é consideravelmente maior do que a média de 34% entre os setores, mas fica marginalmente atrás das instituições financeiras (52%).

A falta de concordância interna quanto à necessidade de seguro cibernético e orçamentos e recursos insuficientes são também grandes impedimentos (com 22% de

ANEXO 8: SITUAÇÃO DO SEGURO CIBERNÉTICO DAS ORGANIZAÇÕES DE ASSISTÊNCIA À SAÚDE

Fonte: Mantendo os cuidados com a saúde sob resgate: Perspectivas do setor sobre riscos cibernéticos. Centro Global de Riscos da Marsh and McLennan Companies

pessoas pesquisadas mencionando isso como motivo) na penetração do seguro cibernético no setor de assistência à saúde.

Esses números ainda sustentam a observação de que o orçamento nas organizações de assistência à saúde está mal-alinhado e que a modernização da tecnologia deve ser priorizada.

O SETOR DE ASSISTÊNCIA À SAÚDE PRECISA FAZER MAIS

Enquanto as empresas nos principais mercados da região Ásia-Pacífico como China, Singapura, Hong Kong, Austrália e Coreia do Sul estão reavaliando e melhorando a sua cobertura de seguro cibernético no setor de assistência à saúde, deve-se reconhecer que o seguro cibernético não é uma solução direta e deve ser aumentado com estratégia robusta de risco e gestão continuada.

O setor de assistência à saúde tem praticado mais ações na média do que os outros setores nos últimos 12-24 meses visando impedir e se preparar para os ciberataques. Por exemplo, 60% das pessoas pesquisadas do setor de assistência à saúde – em comparação com 51% das pessoas pesquisadas pelos setores – indicaram que estão avaliando a lacuna de cibersegurança para descobrir que outras necessidades devem ser observadas para que se protejam contra futuras ameaças. Mesmo assim, a maioria das organizações de assistência à saúde continua a focalizar mais sobre a prevenção ou a preparação, e não suficientemente sobre a detecção e a resposta.

CIBERNÉTICA EM CMT

PROTEGENDO-SE E AOS SEUS CLIENTES

Tom Quigley
Comunicações, Mídias e Tecnologia, chefe de prática, Marsh

Saahil Malik
diretor, Comunicações, Mídias e Tecnologia, Oliver Wyman

Na qualidade de um habilitador da digitalização rápida, o setor de Comunicações, Mídias e Tecnologia (CMT), incluindo o setor de Telecomunicações, está exposto a um amplo conjunto de ameaças de cibersegurança. De acordo com a última Pesquisa de Percepção de Risco Cibernético Global da Marsh-Microsoft, 13,5% das empresas de CMT comunicaram ter sido vítimas de ciberataques nos últimos 12 meses. As instituições neste espaço têm uma infraestrutura crítica e geralmente agem como condutos para fluxos de informações e transações críticas – para si mesmas e para os outros setores.

Ademais, a evolução da tecnologia (como a crescente adoção da nuvem e a implantação da inteligência artificial) está superando em crescimento a capacidade das empresas de CMT de administrar, responder a ciberataques e recuperar-se deles. Em alguns casos, os modelos de negócio estão evoluindo mais rapidamente do que as capacidades técnicas e de cibersegurança correspondentes das empresas. Embora as empresas de CMT tenham sido observadas como mais confiantes quanto ao entendimento e a mitigação dos riscos cibernéticos do que os outros setores na média, quando se tratava de recuperação dos incidentes cibernéticos, o setor de CMT se mostrava tão inseguro quanto os outros.

Assim, é imperativo que este setor compreenda as ameaças, as fontes e o impacto, e desenvolva uma abordagem 360 referente à cibernética para comprovação futura de sua infraestrutura subjacente, operações e por fim as informações do cliente.

AMEAÇAS OBSERVADAS

Os participantes da última Pesquisa de Percepção do Risco Cibernético Global da Marsh-Microsoft forneceram insights sobre as suas percepções dos cenários de perda cibernética que poderiam causar o maior impacto. As pessoas pesquisadas destacaram que a interrupção do negócio e o dano reputacional são os dois principais cenários de perda com o impacto mais significativo.

ANEXO 9: PRINCIPAIS CENÁRIOS DE PERDA CIBERNÉTICA COM O MAIOR IMPACTO POTENCIAL OBSERVADO

Fonte: Pesquisa de Percepção de Risco Cibernético Global de 2017 da Marsh-Microsoft

A interrupção do negócio foi destacada como o principal risco cibernético no setor de CMT (77%), como ocorre em outros setores.

Os provedores de serviços de comunicação em geral têm contratos rígidos de nível de serviço e espera-se que forneçam alto desempenho e níveis de serviço ininterruptos para atender às demandas dos clientes. Assim, a conectividade comprometida ou uma "falha no desempenho" poderia levar a uma grave interrupção, efeitos em cascata e sérios eventos de perda.

Junto com a interrupção do negócio, o dano reputacional era visto como sendo extremamente nocivo para a saúde de longo prazo do setor de CMT (77%, significativamente mais alto do que a média intersetorial de 59%). Para o setor de CMT, e em especial o setor de telecomunicações, clientes, investidores e governo podem avaliar o histórico dos provedores potenciais à medida que se tornam mais conscientes sobre a segurança.

FONTES DE AMEAÇA MULTIDIMENSIONAL E IMPACTOS

Os modelos de negócio cada vez mais complexos das empresas de CMT, junto com o potencial de impacto dos eventos cibernéticos sobre os clientes que atendem, chama a atenção para a vulnerabilidade do setor de CMT quanto ao fator de ameaça humana. Empresas no setor de CMT marcaram os agentes da ameaça motivados financeiramente (33%), os erros humanos e os colaboradores desonestos (34% no total) como as suas maiores preocupações de ameaça. Eles são difíceis de serem previstos e antecipados – e derivam de uma série de fatores, inclusive, entre outros, a perspectiva de ganhos financeiros e coerção, a manipulação deliberada de dados ou a mera negligência.

Em consequência disso, o impacto financeiro percebido de uma violação cibernética no setor de CMT foi um dos maiores entre os setores.

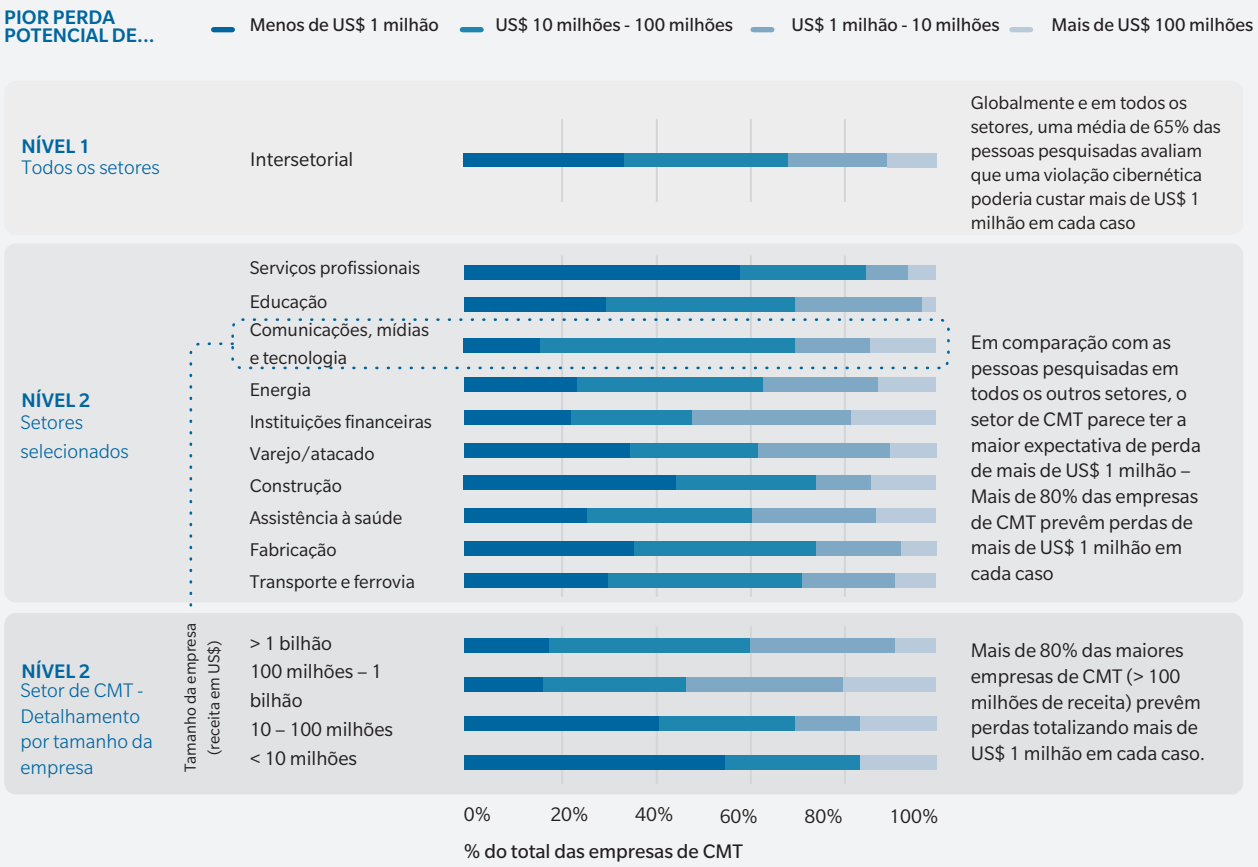
Mais de 80% das empresas de CMT previram perdas diretas de mais de US$ 1 milhão por incidente, em comparação com aquelas dos setores de assistência à saúde (75%), energia (76%) e as instituições financeiras (77%).

REGULAMENTOS AMPLIADOS

O risco de mudança reguladora aumentou de modo significativo e a crescente atenção às questões reguladoras, como o acesso transfronteiriço a dados e a revogação da neutralidade de rede nos Estados Unidos, refletiram a crescente responsabilidade colocada sobre as empresas de telecomunicações pelos reguladores. Empresas em determinadas jurisdições são legalmente obrigadas a notificar violações de dados aos seus clientes e não podem mais jogar tudo para baixo do tapete, enquanto outras devem agora exercer um papel autorregulador maior no tratamento das transmissões de dados. Por exemplo, o Código de Comunicações Eletrônicas promulgado pela Comissão Europeia delineou novos objetivos reguladores para o setor de telecomunicações. Ele dá suporte à agenda do Mercado Único Digital da UE e será necessário um investimento significativo para observar de modo eficaz as regulamentações múltiplas e algumas vezes conflitantes.

A Associação GSM (um órgão comercial originalmente europeu que representa os interesses das operadoras da rede móvel por todo o mundo) começou a trabalhar em uma estrutura intersetorial para gestão do risco cibernético. As regulamentações específicas do mercado, como o Regulamento Geral de Proteção de Dados da UE, a Lei de Cibersegurança da China, a Lei de Cibersegurança de Singapura, a Lei de Privacidade do Consumidor da Califórnia e o proposto Regulamento da Privacidade Eletrônica continuarão a causar problemas; e as regulamentações sobre normas e metas de conformidade, por exemplo, ainda podem complicar o ambiente operacional carregado de risco.

ANEXO 10: IMPACTO FINANCEIRO ESTIMADO DE CADA CASO DE INCIDENTE CIBERNÉTICO A PARTIR DE UMA ANÁLISE TOP-DOWN



Fonte: Pesquisa de Percepção de Risco Cibernético Global de 2017 da Marsh-Microsoft

CIBER-RESILIÊNCIA AVANÇADA EM CMT

Várias empresas neste setor já deram início a diversas iniciativas estratégicas para melhorar a cibersegurança. Por exemplo, no caso das operadoras de telecomunicações, as iniciativas variam desde o uso de tecnologias de inteligência artificial/aprendizado de máquina, aquisição de seguro de cibersegurança, foco na governança interna (pela nomeação de CISOs) e colaborações externas sobre o compartilhamento de melhores práticas, entre outras.

Como parte das expectativas da administração, dos acionistas, reguladores e agências de classificação, os mecanismos específicos do setor são projetados para salvaguardar contra incidentes, bem como para implantar um manual de estratégias atualizado e documentado sobre casos de violação.

A maioria das empresas de CMT ainda está colocando mais ênfase na prevenção ou na preparação, e não focalizam suficientemente a detecção e a resposta. Só pouco mais de um terço das pessoas pesquisadas do setor de CMT comunicaram ter instalado um plano de

resposta a incidente cibernético (39%) ou ter investido em melhorias na detecção de eventos cibernéticos (37%).

Uma estratégia totalmente inclusiva de dados e risco cibernético se baseia em uma avaliação de risco minuciosa, um apetite por risco definido e na quantificação da exposição a risco. Esta estratégia de gestão de risco então determina a governança correta, identifica ameaças e ações corretivas, e quantifica o valor do investimento necessário para preencher lacunas e vulnerabilidades.

Um diagnóstico rigoroso de risco interno, logo de início, é necessário para avaliar os riscos cibernéticos de uma empresa em comparação com as colegas do setor. De acordo com a Pesquisa de Percepção de Risco Cibernético Global da Marsh-Microsoft, 42% das empresas de CMT não conduziram uma avaliação de lacuna de cibersegurança nos últimos 12 meses. As empresas de CMT precisam identificar, definir e mapear as ameaças cibernéticas específicas aos seus ativos tangíveis e intangíveis.

Instruir a força de trabalho e construir uma cultura de cibersegurança para combater os ciberataques cada vez mais complexos e frequentes. Só em 2017, por exemplo, o erro humano era considerado como aumentando os ciberataques relacionados à nuvem em 424% globalmente, e a atividade não intencional como a infraestrutura de nuvem mal configurada era responsável por quase três entre quatro registros comprometidos. Dado o volume e a velocidade dos dados dentro do setor de CMT, é importante o treinamento de todos os colaboradores e não apenas dos especialistas em cibernética quanto ao manuseio de dados do cliente e apólices associadas à segurança de dados sensíveis.

A expansão do programa de cibersegurança deve ser uma prioridade dada a proliferação da Internet das Coisas (IoT), dos dispositivos móveis com acesso às redes corporativas, e da crescente digitalização das redes físicas no setor de CMT. As empresas devem dar ênfase às práticas comprovadas de higiene da cibersegurança, que não estão presentes na metade das empresas de CMT hoje em dia. As pessoas pesquisadas do setor de CMT admitiram não ter criptografia de hardware (42%) e autenticação multifator para as redes corporativas (44%).

Incorporar a cibernética aos planos de gestão de risco da empresa. Os departamentos de TI são vistos como os principais proprietários e tomadores de decisão de gestão de risco cibernético pelo setor de CMT globalmente. As empresas são encorajadas a entender mais o retorno sobre o risco, por meio da quantificação, e a elaborar capacidades internas pelas múltiplas áreas funcionais interconectadas alinhadas com a sua estratégia cibernética. Passar para uma percepção mais "voltada para o risco" significará tornar a gestão de risco cibernético uma responsabilidade de cima a baixo de toda a empresa que é distribuída pelos departamentos.

O apoio a estruturas avançadas de resiliência de dados. O apoio a estruturas avançadas de resiliência de dados.

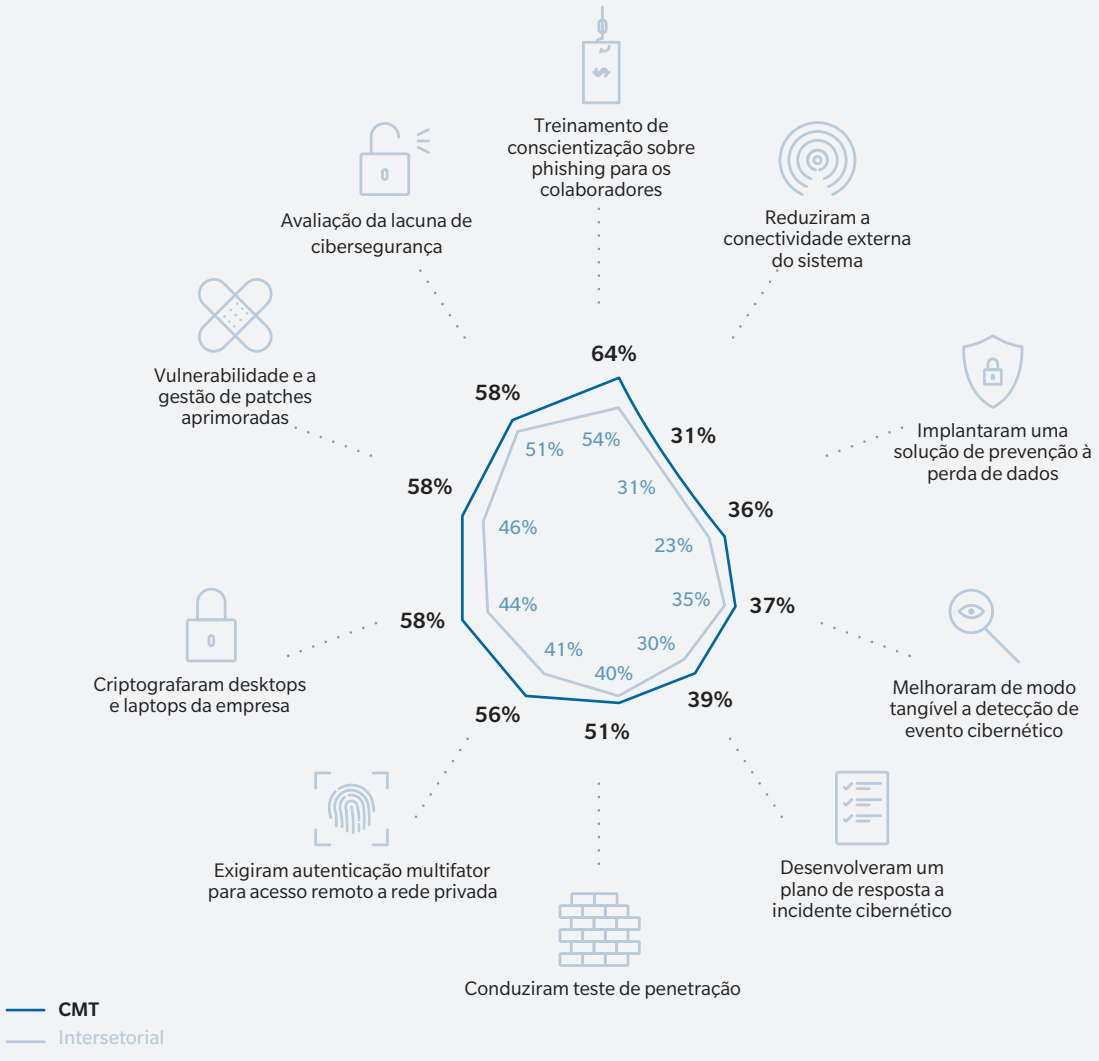
Explorar um conjunto abrangente de soluções de transferência de risco. Dada a complexidade dos riscos cibernéticos para as empresas de CMT, somente uma parcela compra seguro cibernético independente. Historicamente, a maioria foi solicitada a comprar apólices de Erros e Omissões de Tecnologia (E&O Tech) que contêm algumas coberturas cibernéticas.

Contudo, com o aumento da gravidade dos eventos cibernéticos, e como buscam proteger investimentos massivos de pesquisa e desenvolvimento (P&D), as empresas de CMT procuram uma série de soluções de transferência de risco. Desde o acréscimo de mais seguros cibernéticos independentes até a exploração de soluções mais complexas como risco integrado, capital de risco alternativo, soluções de risco paramétricas e cativas, existe um reconhecimento de que, a despeito dos seus melhores esforços, haverá eventos de perda para financiar.

CONVOCAÇÃO

Na corrida em alta velocidade pela liderança em tecnologia e as incertezas relacionadas, as empresas precisam considerar com atenção a abordagem global à segurança para a obtenção do equilíbrio certo entre segurança e flexibilidade de uso. Somente com uma posição mais rigorosa na gestão de risco cibernético, com a cibernética incorporada aos seus casos de negócio, as empresas de CMT podem diferenciar-se potencialmente e trazer maior valor para os seus clientes e consumidores.

ANEXO 11: IMPACTO FINANCEIRO ESTIMADO DE CADA CASO DE INCIDENTE CIBERNÉTICO A PARTIR DE UMA ANÁLISE TOP-DOWN



RISCO CIBERNÉTICO NA ÁSIA

RAMIFICAÇÕES PARA OS SETORES IMOBILIÁRIO E DE HOSPITALIDADE

Jaclyn Yeo
gerente de pesquisa,
Marsh & McLennan Insights

Meghna Basu
analista de pesquisa,
Marsh & McLennan Insights

Globalmente, o setor de bens imobiliários e hospitalidade (RE&H) é o quarto setor mais frequentemente visado, responsável por cerca de 11% das violações de dados em 2016-2017. O setor de RE&H é suscetível a ciberataques e é um alvo conveniente para os criminosos já que contém tesouros de ativos financeiros, informações pessoais identificáveis (PII), pontuações de crédito externo e dados de propriedade intelectual (PI) interna.

Com a chegada da Quarta Revolução Industrial (4IR), as informações confidenciais de empresas e usuários finais também estão se tornando mais expostas à atividade criminosa, na medida que o setor de RE&H está se tornando mais conectado à internet do que antes. É crucial que as empresas observem como a adoção da sua tecnologia está ampliando a sua superfície de ataque, e que os gestores de risco identifiquem pontos de acesso vulneráveis que podem ser explorados por cibercriminosos.

AUMENTANDO OS PONTOS DE EXTREMIDADE VULNERÁVEIS

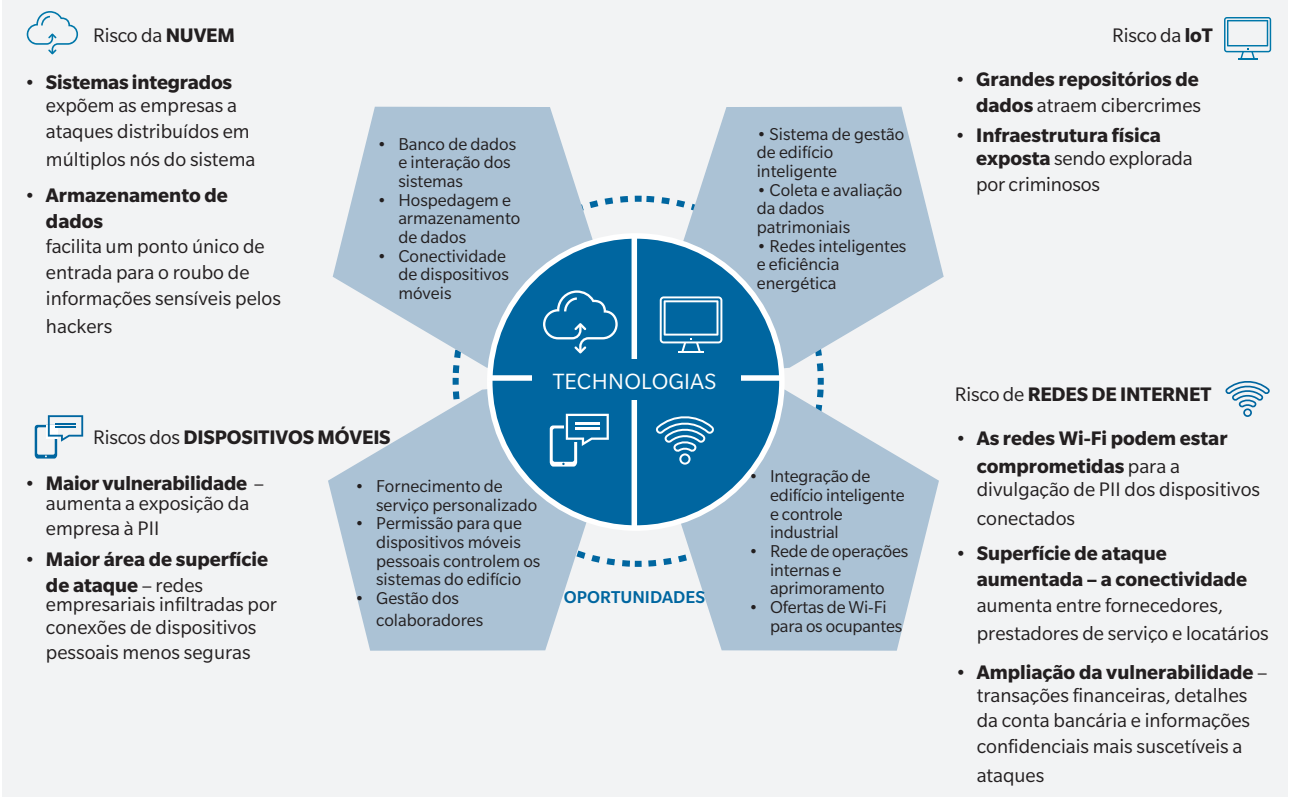
Complicações em termos de segurança adicional também podem ser criadas sem o conhecimento das empresas. Por exemplo, o desenvolvimento econômico e a urbanização pela Ásia estimulados por várias iniciativas inteligentes da cidade criaram rapidamente dados adicionais e conectaram esses dados ao ambiente construído. Da mesma forma, as empresas de RE&H na região estarão cada vez mais desenvolvendo, vendendo e usando edifícios que acumulam grandes quantidades de big data sensíveis e pessoais. Esses edifícios centralizam a coleta de dados pelos clientes, fornecedores e empresas, tornando-os alvos fundamentais para os ataques. Em decorrência disso, o aumento na conectividade entre os setores de RE&H e o ambiente construído acrescenta à responsabilidade das empresas o fortalecimento de suas medidas de cibersegurança e asseguram uma adequada proteção cliente-dados.

A adoção crescente de tecnologias emergentes permite que se acumulem e transmitam big data e informações financeiras, que representam alvos fundamentais para os ciberataques. Finalmente, isso levará a um aumento exponencial no número de pontos de extremidade para ataques potenciais.

EM DESTAQUE

A despeito das técnicas cada vez mais inovadoras usadas nos ciberataques, muitos invasores ainda fazem uso de táticas tradicionais para obter acesso. Eles também estão voltados para os executivos e outros colaboradores da linha de frente para enganá-los a ativar códigos de software maliciosos que forneçam acesso fácil ao sistema de rede de uma organização. Os exemplos a seguir ilustram algumas técnicas ultrapassadas usadas pelos invasores cibernéticos.

ANEXO 12: RISCOS E OPORTUNIDADES NA ADOÇÃO DE TECNOLOGIAS EMERGENTES NO SETOR DE RE&H



Fonte: Análise do APRC (Asia Pacific Risk Center)

Exemplo 1: Uma imobiliária sediada em Perth enfrentou um quase roubo em setembro de 2016, quando houve um pedido de retirada não autorizada de A$ 500.000 (~US$ 384.000) da conta de depósito da agência. Os cibercriminosos conseguiram instalar malware nos sistemas de computador da empresa, que acreditaram ter infiltrado o sistema quando os membros do quadro de pessoal, sem saber, clicaram nos links do website mal-intencionado dos e-mails de phishing. Uma vez instalado, o malware permitia que os criminosos registrassem pressionamentos de teclas e identificassem os detalhes de logon do banco da empresa.

Por sorte, como parte das melhores práticas da agência de bens imobiliários de reconciliar as contas de depósito diariamente, a retirada não autorizada foi descoberta a tempo por um membro do quadro de pessoal e o banco pertinente desfez a transferência de fundo antes que este chegasse aos criminosos17. Além de aprimorar programas de treinamento para aumentar a conscientização sobre cibersegurança e ensinar aos colaboradores como reconhecer e-mails de phishing mal-intencionados, a imobiliária logo introduziu uma conexão de rede mais segura com o seu banco, que incluía software anti-malware e recursos de autenticação multifator e multipartes.

Exemplo 2: Uma cadeia de hotéis de renome sofreu duas violações de dados em 2015 e em 2017, quando os seus sistemas de cibersegurança foram comprometidos, vazando as PIIs e as Informações do Setor de Cartões de Pagamento (PCI) de seus clientes por todo o mundo. Enquanto também sofriam um impacto considerável em 2015, o impacto na China e em Hong Kong na violação de 2017 foi significativamente maior, demonstrando que as ameaças cibernéticas estão no auge na Ásia e causando mais impacto na região do que antes. Ambas as invasões cibernéticas foram causadas por malware que infectou os sistemas de processamento de pagamentos da cadeia de hotéis, expondo o PCI, como nomes dos detentores dos cartões, números dos cartões, datas de validade e códigos de verificação interna – tudo isso sendo obtido dos cartões de crédito manualmente lançados ou passados nas recepções.

A violação do malware do PDV (ponto de venda) foi causada pela inserção de código de software mal-intencionado de um terceiro no sistema de TI de vários hotéis através do computador do PDV. Para os dois incidentes, a empresa não divulgou quantos clientes foram potencialmente afetados e não sabia exatamente os pormenores de quem tinham sido comprometidos.

ANEXO 13: RESUMO DAS ESTATÍSTICAS DO HACK DA CADEIA DE HOTÉIS

Fonte: Análise do APRC; arquivo de dados das pesquisas cibernéticas da Marsh Hong Kong e da Marsh/Microsoft

MUITO DESPREPARADA

De acordo com a última Pesquisa de Percepção de Risco Cibernético Global da Marsh-Microsoft e da Pesquisa de Risco Cibernético da Marsh Hong Kong, a falta de preparação cibernética do setor de RE&H pode ser atribuída ao que segue:

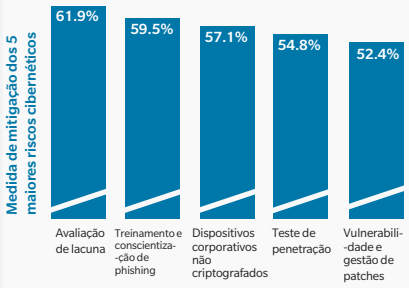
- Uma lacuna ampliada de percepção-realidade
- Defesa insuficiente contra a superfície de ataque ampliada
- Indiferença diante da compra de seguro cibernético

Existe um grande abismo entre como as empresas preparadas consideram estar diante de um ataque e o quão protegidas elas estão de fato. Por exemplo, uma grande maioria (65%) das pessoas pesquisadas do setor de RE&H na Ásia classificou a ameaça cibernética como uma das 5 maiores preocupações do risco empresarial; mas 85% das pessoas pesquisadas de RE&H em Hong Kong gastam menos de 10% do seu orçamento anual em cibersegurança. Mais ainda, as empresas do setor de RE&H parecem em geral confiantes (88%) de que entendem a sua exposição ao risco cibernético, mas 48% a ignoram ou não têm quaisquer métodos para medir a sua exposição ao risco cibernético.

ANEXO 14: ESTRATÉGIAS DE DEFESA DO ECYBER UTILIZADAS PELO SETOR DE RE&H

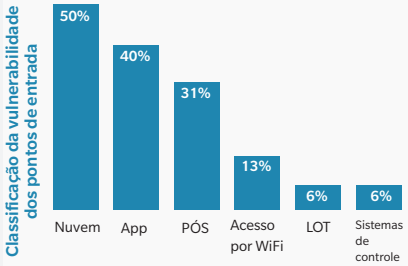
1 Identificar pontos de entrada vulneráveis

P: Quais destas etapas a sua organização percorreu nos últimos 12 a 24 meses?
Por percentual da seleção da pessoa pesquisada



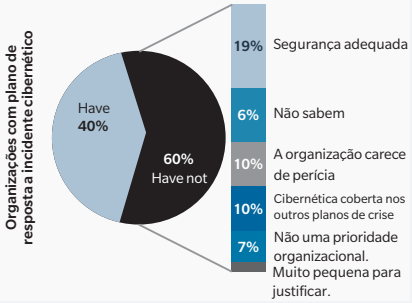
3 Plano de resposta a incidente cibernético

P: Quais dos seguintes pontos de entrada você considera que sejam os mais vulneráveis no setor de RE&H?
Por percentual da seleção da pessoa pesquisada



2 Medidas de mitigação praticadas

P: Caso a sua organização não tenha e/ou não planeje desenvolver um plano de resposta a incidente cibernético, qual o motivo?



As pessoas pesquisadas também supunham que as suas estruturas internas de cibersegurança eram suficientes para impedir a ocorrência de ciberataques. Seis dentre 10 empresas de RE&H não têm e não planejam desenvolver um plano de resposta a incidente cibernético, a despeito de uma dentre cinco ter respondido que já vivenciara um ciberataque só nos últimos 12 meses.

Apesar de haver uma grande chance de serem atacadas, a maioria das empresas não está preparada para responder a um ataque.

Embora sendo capazes de identificar os principais pontos de entrada e tendo instalado algum tipo de medidas de cibersegurança para se proteger contra ciberataques, a conscientização não condiz com o nível de defesa adequado. 60% das organizações pesquisadas estão sem planos de resposta a incidente adequados; 10% alegaram falta de perícia como um motivo para não ter um plano de resposta a incidente, enquanto outras 10% sugeriram que os incidentes cibernéticos sejam cobertos por outros planos de crise e, com isso, não precisem selecionar um plano de resposta a incidente independente.

Gigantescas perdas econômicas têm mais probabilidade de ocorrer devido à interrupção do negócio, já que as funções críticas, a proteção de dados e as soluções de backup de prevenção de perdas podem interromper as operações no caso de um ciberataque. Sem uma adequada gestão de crise e o engajamento das partes interessadas, as operações normais da empresa serão ainda retardadas quando as organizações se desdobram apressadamente para realizar investigações forenses após o incidente e notificar as pessoas afetadas.

Existe espaço para melhora no reconhecimento do significado do seguro cibernético no setor de RE&H. 31% indicaram que têm planos de comprar ou aumentar o seguro cibernético durante os próximos 12 meses, principalmente impulsionadas por planos de gestão de risco cibernético ou instigadas pelos ciberataques bem-sucedidos nas outras empresas.

Em contrapartida, uma entre 10 empresas de RE&H não tem e não pretende comprar cobertura de seguro cibernético, alegando como motivos principais as limitações na cobertura, considerações sobre o custo ou a crença de que o risco cibernético foi adequadamente coberto nas outras apólices.

É previsível que fatores reguladores, como legislações ou normas das agências de classificação, causem impacto insignificante sobre a decisão de comprar seguro na região Ásia-Pacífico, já que a legislação e as forças policiais estão atualmente lutando para manter a paz na região. Com o Regulamento Geral de Proteção de Dados (GDPR) da UE instalado, as leis de cibersegurança e as divulgações obrigatórias de violação de dados pela região estão aumentando. Mais ainda, a despeito da localização, qualquer organização que detenha dados pessoais de qualquer cidadão da UE será afetada pelo GDPR. Assim, as taxas de adoção do seguro cibernético pelos setores na Ásia podem crescer, com as empresas usando o processo de conformidade com o GDPR para fortalecer as suas práticas principais de risco cibernético.

TORNAR-SE "CYBER-READY"

As organizações no setor de RE&H na Ásia estão mais suscetíveis a ciberataques agora do que antes. A despeito do setor de bens imobiliários tradicionalmente se considerando um alvo desinteressante para os hackers, as principais tendências na região sugerem que o setor de bens imobiliários, assim como o de hospitalidade, estão cada vez mais expostos a vulnerabilidades cibernéticas.

REGULAMENTOS

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (GDPR)

A PORTA PARA O FUTURO?

Kaijia Gu
sócio, Preços, Vendas e Marketing,
Oliver Wyman

Em 25 de maio de 2018, cruzamos o tão esperado limite de ter o Regulamento Geral de Proteção de Dados (GDPR), à medida que uma nova legislação entra em vigor na Europa. Para as organizações, isso será uma mudança drástica pela região sobre como elas abordam a privacidade de dados – com consequências financeiras e reputacionais bastante grandes. Mas fora da conformidade, outras forças estão em jogo.

Até agora, as discussões sobre o GDPR estiveram grandemente voltadas para os requisitos de conformidade. Em se tratando de um setor consciente de risco, a maioria das grandes seguradoras e as maiores prestadoras de serviços financeiros vêm diligentemente realizando programas de prontidão do GDPR, assegurando que todas as "caixas" de conformidade foram firmemente marcadas. Para algumas, o GDPR é apenas um exercício de conformidade extremamente caro. Até agora, o tratamento do GDPR meramente como uma questão de governança não somente perderia em potencial oportunidades estratégicas significativas, mas também representaria uma ameaça, caso alguém mais fizesse melhor e mais rápido. A Oliver Wyman acredita que as empresas inteligentes aproveitarão esta oportunidade para abrir a porta para um futuro em que modelos de negócio novos e revolucionários possam abordar e resolver complexos desafios do cliente, fornecendo-lhe valor aumentado.

CAMPO DE ATUAÇÃO ESTABILIZADO

O GDPR fornece a propriedade e o controle do uso dos dados de volta para os clientes. Assim, empresas de grande porte que hoje capturam e usam os dados dos clientes não mais reivindicam estes dados como sendo parte de seu ativo. Decisivamente, mediante solicitação do cliente, as organizações devem permitir que os dados sejam transferidos para algum terceiro. Isso sem dúvida levará a uma equiparação drástica do campo de atuação entre aquelas empresas já estabelecidas e as novas participantes. Depois do GDPR, as maiores empresas já estabelecidas não mais têm um monopólio sobre os dados dos clientes, e deverão defender as suas posições de mercado com vantagens competitivas distintas. De um lado, é uma boa notícia para as novas participantes, em especial para as start-ups ambiciosas e engenhosas de seguro e tecnologia, para as quais, no passado, os dados eram dificilmente adquiridos e caros.

Vejamos o exemplo das renovações das apólices. Durante muitos anos, as seguradoras contavam com formulários enormes de cotação e processos desajeitados de comparação para deter os clientes de levar os seus negócios para outro lugar. Mas e se o preenchimento de questionários ineficientes pudesse ser logrado com um clique? Depois do GDPR, um divisor de águas significativo seria a "cotação com um clique", desde que os clientes dessem o seu consentimento para o transporte de seus dados de outro lugar.

Esse levantamento fácil dos dados pessoais de um fornecedor existente representa a principal ameaça dos níveis aumentados de atrito, e uma substancial erosão do lucro.

CONFIANÇA E RECOMPENSA

Com os dados não estando mais "cercados" por empresas já estabelecidas, as organizações deverão impor novos conceitos sobre como se diferenciar, assim gerando uma vantagem competitiva. Para os clientes cada vez mais perceptivos, uma experiência do consumidor sem alterações será vista como meramente básica.

Dois eminentes fatores adicionais estarão nas mentes dos clientes de seguro do futuro.

1. "OS MEUS DADOS ESTÃO SEGUROS?"

Violações de dados de alta visibilidade, fraude aumentada, uso questionável das mídias sociais e manchetes denunciando manipulação política em larga escala aumentaram a noção de segurança dos dados na consciência coletiva do público. A pesquisa de DNA Digital britânica da Oliver Wyman estabeleceu que o maior medo dos clientes com respeito ao mundo digital é a perda de privacidade. Mais da metade dos clientes pesquisados se preocupava com o compartilhamento das informações pessoais on-line. No futuro, os clientes estarão demandando maior transparência no uso dos dados; o GDPR torna obrigatório que as empresas façam isso.

2. "VOU GANHAR ALGUMA COISA SE COMPARTILHAR OS MEUS DADOS?"

Dados os consentimentos explícitos necessários para o uso e o compartilhamento dos dados dos clientes, estes cada vez mais perceberão que os seus dados têm bastante valor. Assim, estarão buscando obter mais valor do compartilhamento dos seus dados, seja em serviço excepcional ou experiências, produtos e ofertas personalizados, ou produtos e serviços com desconto. Estes incentivos tornar-se-ão a nova moeda em troca por se manter ou transmitir as informações pessoais.

Os pontos acima reforçam a necessidade de que os líderes empresariais do setor de seguro adotem uma estratégia centrada no cliente que se volte para o valor, tanto de uma perspectiva de confiança quanto comercial. Listamos aqui algumas das prováveis proposições de valor convincentes dos projetos de novos negócios e o placar das empresas já estabelecidas e das novas participantes com base no seu DNA comercial fundamental.

SEM ATITUDES DE ARREPENDIMENTO DAS EMPRESAS JÁ ESTABELECIDAS

Estrategicamente falando, parece que o GDPR traz mais ameaças do que oportunidades para as empresas já estabelecidas ao nivelar o campo de atuação. Contudo, no ecossistema de seguro cada vez mais dinâmico e em constante mudança, o limite entre as empresas já estabelecidas e as start-ups é bem fluido e há alguns benefícios duradouros para aquelas já existentes. As empresas já estabelecidas geralmente acumularam uma grande base de clientes ao longo do tempo e construíram uma marca confiável. Muitas estabeleceram um profundo entendimento sobre o comportamento e as necessidades do cliente. A questão principal é se elas ficaram cientes das implicações estratégicas e decidiram sair de sua zona de conforto, adotando uma abordagem inventiva e ágil no desenvolvimento de modelos de negócio. As empresas já estabelecidas também precisarão reconsiderar os seus ativos, capacidades, capital e talentos.

Ofensivas ou defensivas, percebemos várias atitudes sem arrependimento para as grandes empresas já estabelecidas à medida que a porta do GDPR se abre.

MAPEAMENTO ESTRATÉGICO

As empresas já estabelecidas devem se perguntar "Como quero ser conhecida nos próximos cinco anos, ou mesmo 10 anos?" Elas devem analisar para onde está se encaminhando o setor em um nível macro e alinhar a sua estratégia com uma cadeia de valor voltada para o futuro. Embora isso seja crítico com ou sem o GDPR, o regulamento iminente forneceu um bom gatilho para que as empresas embarquem nesta jornada – mesmo se ainda não tiverem começado.

AVALIAÇÃO DE ATIVOS DE DADOS

O futuro sucesso das empresas já estabelecidas pode depender de quão bem elas entendem de quais ativos de dados precisam para construir o negócio do futuro. Da mesma forma, elas devem compreender como proteger esses ativos de dados que já têm (de modo que os clientes não peçam que os seus dados sejam apagados) e obter aqueles que ainda não têm.

AGILIDADE

O ciclo de vida dos novos modelos de negócio está em ritmo acelerado na nossa era atual. A antiga abordagem de passar anos devotando um exército de pessoas a construir um modelo "perfeito" não funciona mais. Desenvolvimento ágil, desenvolvimento de software e ambientes de operações (DevOps), tecnologia sediada na nuvem e centricidade do cliente serão ingredientes essenciais para se arquitetar os novos modelos de negócio.

EXCELÊNCIA COMERCIAL

Isso pode parecer contraintuitivo mas, dadas as margens já existentes, uma empresa já estabelecida e bem-sucedida na reinvenção de seu modelo de negócio requer um investimento potencialmente significativo. A capacidade de otimizar o negócio existente para gerar caixa e avanço no financiamento do novo negócio é crucial para a maioria das empresas já estabelecidas.

UMA PALAVRA FINAL

Seguro é um negócio complexo e, desde 25 de maio em diante, o setor vivenciará uma transformação considerável. A inércia tornará este processo gradual, não súbito. Para aquelas empresas que escolheram não fazer planos e se contentar em simplesmente observar o GDPR, entretanto, os riscos de ser deixada para trás são bastante reais. É provável que fiquem à margem dos competidores ousados – as empresas já estabelecidas e as novas participantes igualmente – que desejam muito adotar a mudança e estão prontas para construir exatamente o tipo de negócio que desejam. A oportunidade está batendo à porta – estamos curiosos para ver quem vai abri-la.

EM UM EXAME REGULATÓRIO MINUCIOSO,

AS INSTITUIÇÕES FINANCEIRAS DEVEM MONITORAR O RISCO CIBERNÉTICO DE TERCEIROS

Alex deLaricheliere
diretor executivo – US Banking & Capital Markets, Marsh

A cibersegurança está classificada entre as principais preocupações de bancos, seguradoras e outras instituições financeiras que podem representar alvos importantes para os cibercriminosos e estar vulneráveis às interrupções potenciais graças aos seus sistemas de tecnologia geralmente complexos, ativos financeiros valiosos e os ricos dados dos clientes que podem deter.

Com o crescimento da conscientização sobre os riscos cibernéticos, muitas instituições financeiras desenvolveram capacidades internas robustas para deter ciberataques e impedir as interrupções da tecnologia. Mas talvez de igual importância – tanto para a organização quanto para os reguladores – sejam as práticas de gestão de risco cibernético dos seus fornecedores.

INVESTIGANDO O RISCO CIBERNÉTICO DE TERCEIRO

Desde a crise financeira do final dos anos 2000, o Federal Reserve, a Securities and Exchange Commission, o Escritório do Controlador da Moeda e outros reguladores esmiuçaram as práticas de gestão de risco das instituições financeiras. Uma das maiores áreas de atenção foi o risco de tecnologia.

Recentemente, tanto o setor quanto os reguladores estão afinados quanto aos riscos apresentados pelos fornecedores. Muitas instituições financeiras grandes desenvolveram escritórios de gestão do fornecedor com a missão explícita de policiar e fiscalizar o seu conjunto de fornecedores e de terceiros com quem trabalham. Embora os reguladores pareçam apreciar esta abordagem à gestão de risco, eles não abrandaram. Em vez disso, estão agora investigando mais fundo, olhando para fornecedores do segundo e do terceiro nível – aqueles em quem confiam os fornecedores das instituições financeiras.

Para as instituições financeiras, esses fornecedores representam vulnerabilidades potenciais de risco cibernético que poderiam custar milhões. Os fornecedores que detêm ou processam dados poderiam se tornar vítimas de ataques de hacking eles próprios, ou fornecer uma porta para os ataques às redes corporativas das instituições financeiras. As interrupções da tecnologia nos fornecedores também podem afetar as operações das instituições financeiras.

EXAMINANDO A SUA CADEIA DE VALOR

Assim como ocorre com as empresas que produzem ou vendem produtos físicos em geral e que fazem uma auditoria regular de suas cadeias de abastecimento para avaliar as vulnerabilidades a perigos naturais e outros riscos físicos, as instituições financeiras devem avaliar as suas cadeias de abastecimento, buscando obter insight quanto às práticas de mitigação do risco cibernético dos seus fornecedores de primeiro, segundo e terceiro níveis.

A sua organização pode já ter esse insight. Caso não tenha, ela deve:

- Avaliar processos existentes de gestão de terceiros e necessidades de dados, identificando todos os relacionamentos com fornecedores e terceiros e examinando minuciosamente a linguagem contratual relacionada à segurança dos dados
- Desenvolver uma estrutura de gestão de risco que inclua a exposição de cada fornecedor e o risco de violação ou interrupção do negócio, assim como as ações recomendadas
- Monitorar continuamente a postura de segurança da rede do seu fornecedor, identificando aquelas empresas que apresentam riscos que devem ser analisados mais de perto
- Estabelecer um protocolo de ação que permita que você sistematize a gestão do seu risco de terceiro

Também é importante quantificar o seu risco cibernético, incluindo as exposições de terceiros. Uma análise baseada no cenário do seu risco cibernético pode ajudar a avaliar a probabilidade e a gravidade potencial de um evento cibernético envolvendo um fornecedor – algo de grande interesse aos reguladores financeiros. A modelização do cenário também pode ajudar na identificação e na avaliação da mitigação do risco potencial e das opções de seguro.

Você já deve ter um programa de cibersegurança eficaz instalado na sua organização, mas esse pode não ser o caso para os seus fornecedores – ou os fornecedores com quem eles contam. Siga estas etapas para compreender e administrar melhor o seu risco cibernético de terceiro.

PROTEGENDO O SETOR PÚBLICO

SETE FORMAS PELAS QUAIS OS GOVERNOS ESTADUAIS PODEM AUMENTAR A SUA CIBERSEGURANÇA

Ryan Harkins
diretor de assuntos estaduais e política pública, U.S. Government Affairs da Microsoft

Erin English
estrategista de segurança sênior, Microsoft

Os hackers estão voltados, cada vez mais, para os governos estaduais e suas capacidades administrativas. Como o setor público pode se proteger contra essas ameaças?

Pelos Estados Unidos, os governos estaduais e locais estão fazendo investimentos significativos em tecnologia da informação, de modo que possam tirar vantagem das mesmas eficiências que capacitam a incumbência do setor privado rumo à Quarta Revolução Industrial. Isso está criando oportunidades adicionais, mas também novos riscos. Os governos estaduais dos EUA têm sido objeto, a uma taxa alarmante, de adversários que estão cada vez mais sofisticados e impulsionados por motivos mais amplos. Consequentemente, os governos estaduais se encontram nas linhas de frente, graças ao papel que exercem na prestação de serviços essenciais ou na administração da indústria e do comércio. Sem dúvida, as agências estaduais podem reter toneladas de dados pessoais vulneráveis, tornando-as alvos desejáveis para os ataques cibernéticos. Talvez a ameaça mais preocupante venha de invasores do país que estão ansiosos por explorar as redes do governo estadual.

Naturalmente, os formuladores de políticas do estado estão ansiosos para encontrar meios de proteger os seus sistemas. Eles enfrentam desafios à medida que adotam novas tecnologias, seguram-se a orçamentos limitados e se esforçam para acompanhar o ritmo das ameaças crescentes, tudo isso enquanto prestam serviços críticos para os seus eleitores. No intuito de abordar esses desafios, os estados devem pensar holisticamente e adotar estratégias de cibersegurança abrangentes e baseadas no risco, em vez de simplesmente responder ao mais recente incidente ou manchete de cibersegurança. Isso requer um pensamento a longo prazo e a sugestão de melhores práticas que sejam flexíveis e capazes de se adaptar a um panorama de ameaças em evolução.

Em julho de 2018, a Microsoft detalhou sete melhores práticas que cada estado deve implantar para proteger o seu governo e os eleitores das ameaças da cibersegurança. Esses princípios estão baseados na perícia e na experiência da Microsoft no combate a ameaças no ciberespaço globalmente.

1. POLÍTICA BÁSICA DE CIBERSEGURANÇA EM DIRETRIZES E NORMAS ESTABELECIDAS

Os governos estaduais devem adotar estruturas federais (como a Estrutura de Cibersegurança do NIST) para ajudar no trabalho preliminar para uma política estadual de cibersegurança forte e eficaz. A estrutura fornece uma visão estratégica de alto nível sobre o ciclo de vida do risco à cibersegurança visando ajudar a entender melhor o seu risco à cibersegurança, e permite a aplicação dos princípios e das melhores práticas da gestão de risco para melhorar a segurança e a resiliência da infraestrutura crítica e dos serviços.

2. ESTABELECER UM CONSELHO CONSULTIVO DE CIBERSEGURANÇA COM O SETOR E A COMUNIDADE ACADÊMICA

Em muitos estados, a maior parte da perícia em cibersegurança está localizada nos setores da indústria e nas disciplinas acadêmicas, e muitos destes especialistas provavelmente estariam ansiosos por contribuir para a política estadual de cibersegurança. Cada estado deve utilizar esses ativos e criar um conselho consultivo de cibersegurança. Esses conselhos podem reunir especialistas do setor, acadêmicos e líderes do setor público para que desenvolvam estratégias de cibersegurança para os governos estaduais e ajudem a responder às ameaças em curso.

3. CRIAR UMA CULTURA DE CIBERSEGURANÇA

Em muitos casos, o ponto mais frágil da segurança para uma organização, inclusive governos estaduais, é o seu pessoal. A reversão desse fenômeno requer a capacitação dos colaboradores com habilidades de que precisam para que fiquem à frente e estejam preparados para proteger contra ameaças cada vez mais sofisticadas. Contudo, somente oito estados atualmente exigem treinamento de cibersegurança para todos os seus colaboradores. Acreditamos ser essencial desenvolver uma força de trabalho especializada, perita em cibernética para reduzir os riscos cibernéticos do estado.

Para criar uma cultura de cibersegurança e reduzir os riscos de ciberataques, os governos estaduais devem implantar um programa robusto de treinamento em cibersegurança para todos os funcionários estaduais.

4. INCREMENTAR NOVOS RECURSOS PARA MELHORAR A INTEGRIDADE DA ELEIÇÃO

Desde 2016, novos recursos elaborados para melhorar a integridade das eleições foram disponibilizados para os estados. Entre eles, estão o financiamento federal para garantir as eleições, programas de segurança da eleição livre coordenados pelo Departamento de Segurança Interna (DHS), tecnologias que ajudam a proteger as campanhas políticas (por exemplo, Microsoft AccountGuard) e suporte a auditorias robustas após a eleição (como auditorias de limitação de risco, ou RLAs) e novos manuais de melhores práticas de segurança da eleição.

5. INTEGRAR A CIBER-RESILIÊNCIA A CADA ETAPA DO PLANEJAMENTO ESTRATÉGICO

À medida que os governos estaduais desenvolvem e implantam estratégias para a proteção de seus ativos de TI e dados das ameaças à cibersegurança e outros desastres, eles também devem tentar tornar resilientes os dados desses serviços. Em outras palavras, assegurar que as redes estaduais possam se adaptar, recuperar e continuar a operar se e quando ocorrer um ataque. A adoção da ciber-resiliência não somente ajuda que os estados sejam mais seguros; ela pode criar oportunidades para que os estados elaborem estratégias abrangentes e de longo prazo que os coloquem em um caminho rumo à transformação digital. Mais ainda, ela pode promover uma cultura de inovação, gerar novos caminhos para investimento e contribuir para um estado vibrante e economicamente competitivo.

6. CONSIDERAR O SEGURO CIBERNÉTICO PARA AJUDAR NA PROTEÇÃO DOS ATIVOS DO ESTADO

O seguro cibernético pode ajudar os estados a complementar o seu processo de gestão de risco cibernético, fornecendo proteção financeira contra os riscos que não podem ser totalmente mitigados. Os benefícios da cibersegurança não são somente financeiros – a cibersegurança, evidentemente, não é um substituto para uma estratégia de cibersegurança robusta e a sua prática. Para que se qualifiquem, as seguradoras geralmente exigem que os estados atendam a determinado conjunto de normas de cibersegurança como o treinamento regular do quadro de pessoal, a criptografia de dados sensíveis e a manutenção de servidores atualizados. Isso então força os governos estaduais a implantar sólidas práticas de cibersegurança, aumentando a saúde global de seus sistemas de tecnologia e a proteção de seus dados.

7. SÓLIDAS POLÍTICAS E CONFORMIDADES DE AQUISIÇÃO SÃO ESSENCIAIS

À medida que aumentavam os dados criados e armazenados pelos estados, isso também acarretava obrigações legais e regulatórias dos estados. Tornou-se cada vez mais importante que os estados analisem as suas políticas de conformidade e aquisição, e garantam que os seus fornecedores possam demonstrar que permitirão a conformidade por meio de suas ferramentas e serviços.

AVANÇANDO A CIBER-RESILIÊNCIA DO GOVERNO ESTADUAL

Os formuladores de políticas de hoje devem tomar decisões cuidadosas e multidisciplinares constantemente, para responder aos desafios de suas populações crescentes, interconectividade aumentada, expectativas volúveis dos serviços do governo e incertezas da segurança no ciberespaço. A implantação da cibersegurança e de estruturas da política para proteção maior dos governos estaduais pode ajudar a enfrentar esses desafios enquanto permite que os funcionários estaduais protejam melhor os seus sistemas. Seguir as recomendações e a abordagem estratégica contidas nesses sete princípios pode ajudar os estados a inovar, melhorar os seus objetivos de segurança e proteger mais os seus sistemas de tecnologia da informação e seus cidadãos.

ESTRATÉGIA DE CIBER-RESILIÊNCIA

QUANDO A SITUAÇÃO SE AGRAVA, OS FORTES REAGEM
VENCENDO O DESAFIO DO APETITE POR RISCO CIBERNÉTICO

Michael Duane
sócio, Finanças e Gestão de Risco,
Oliver Wyman

Rico Brandenburg
sócio, Risco e Política Pública,
Oliver Wyman

Matthew Gruber
gerente de engajamento,
Oliver Wyman

A escala dos ataques recentes e da resultante atenção das mídias, as pressões de supervisão para atualizar a gestão de risco cibernético e o ritmo da inovação tecnológica para prosseguir estão ocorrendo cada vez mais rapidamente. Esses fatores estão obrigando as instituições financeiras a ter um entendimento claro sobre os riscos cibernéticos que enfrentam, e a determinar o nível de risco cibernético que a instituição está disposta a aceitar.

Um apetite por risco cibernético eficaz, mensurável e pronto para uso (o conjunto de afirmativas e métricas que articulam os pontos de vista do Conselho de Administração e da alta administração sobre o escopo e o nível de risco cibernético que a instituição está disposta a aceitar) dá às instituições uma capacidade de gestão de risco para estabelecer e comunicar limites estratégicos para a assunção de risco cibernético pela instituição.

Em nossa experiência, a jornada do desenvolvimento de um apetite por risco cibernético é tão importante quanto o próprio apetite por risco cibernético. Assim, é essencial engajar a alta administração e o Conselho de Administração usando uma abordagem de projeto estruturado que combine a criação da conscientização e obtenha insumos. Fazendo isso, fica claro o motivo pelo qual o apetite zero simplesmente não é realista.

APETITE POR RISCO CIBERNÉTICO: UMA FERRAMENTA ESTRATÉGICA PARA ADMINISTRAR A EXPOSIÇÃO RAPIDAMENTE CRESCENTE

À medida que continuam a crescer a escala e a frequência de eventos cibernéticos publicamente comunicados – sem mencionar os eventos não públicos e quase incidentes –, o risco cibernético se torna um tópico continuamente importante para as partes interessadas seniores pelas principais instituições financeiras e seus supervisores. Em resposta, as partes interessadas internas e externas esperam que as instituições desenvolvam um apetite por risco cibernético eficaz, mensurável e pronto para ser usado, e o incorporem aos processos de tomada de decisão e à governança (por exemplo, gastos de TI).

Um apetite por risco cibernético bem elaborado é uma poderosa ferramenta de gestão de risco para uma instituição. Ele fornece às partes interessadas seniores (em especial aquelas não enterradas nas operações do dia a dia, como o Conselho de Administração e os supervisores) uma articulação concisa do nível e do tipo de riscos cibernéticos aceitáveis para a instituição, colocando o risco cibernético no nível de outros riscos mais familiares como risco de crédito, risco de mercado e risco operacional. Consequentemente, o apetite por risco cibernético de uma instituição pode ser melhorado como um ponto de ancoragem para priorizar os investimentos em cibersegurança, tanto dentro do risco cibernético quanto pelos outros tipos de risco, para alinhar a postura cibernética da instituição ao seu apetite por risco. Quando disseminado pela instituição, o apetite por risco cibernético se torna uma poderosa ferramenta de comunicação que permite que o risco cibernético seja mais tangível pelas empresas e suporte funções, aumentando a conscientização quanto ao risco cibernético e a necessidade de administrá-lo em cada nível organizacional.

É DIFÍCIL DEFINIR UM APETITE POR RISCO CIBERNÉTICO EFICIENTE

A elaboração cuidadosa de um apetite por risco cibernético eficiente não é um empreendimento trivial, e é difícil fazê-lo corretamente (a despeito da crença comum de que não é muito difícil "anotar algumas afirmações que caracterizam a capacidade de tomada de risco da instituição"). Mas as consequências de um apetite por risco cibernético pouco articulado podem ser significativas. Um apetite por risco cibernético compreende mais do que palavras e métricas. Apropriadamente adotado e comunicado por toda uma instituição, ele pode causar um impacto tangível na atividade e no comportamento da empresa. Afirmações pouco articuladas podem causar confusão e podem fazer com que os colaboradores pratiquem atos improdutivos ou potencialmente perigosos.

MAS É IMPORTANTE FAZER DIREITO

Dada a importância de um apetite por risco cibernético, os desafios na sua definição de forma significativa e as consequências caso as instituições estejam erradas, o emprego de uma abordagem estruturada é crítico, começando com um conjunto normalmente acordado de princípios do projeto.

Um apetite por risco cibernético eficaz, mensurável e pronto para uso começa com os temas relevantes do risco cibernético identificados por meio de um processo de identificação e avaliação do risco cibernético. Um tema (ou grupo de temas) específico é então vinculado a uma afirmativa, que é subsequentemente disseminada para os diferentes elementos da superfície de ataque (ou seja, trabalhadores, arquitetura de TI, terceiros, clientes). Nesse nível, a afirmativa é em geral suficientemente concreta para vincular métricas e começos projetados para medir a conformidade com a afirmativa. A métrica é agregada e acumulada ao nível do Conselho usando abordagens apropriadas de agregação (por exemplo, os mais prejudicados). O uso desta abordagem permite que as instituições obtenham afirmativas e métricas do apetite por risco que podem ser convertidas de modo eficaz em processos de decisão da empresa para assegurar que o apetite por risco esteja incorporado na instituição.

A vinculação da métrica quantitativa pertinente às afirmativas qualitativas bem elaboradas é importante para mensurar o nível de conformidade da instituição com a afirmativa de apetite por risco. Em geral, é necessário mais de um indicador para refletir adequadamente uma determinada afirmativa de apetite por risco. O processo de seleção da métrica deve assegurar que (a) a métrica tenha um vínculo claro com a afirmativa, (b) os dados necessários para a mensuração da métrica estejam disponíveis ou possam ser coletados em tempo hábil, (c) a métrica esteja medindo os riscos (e não o puro desempenho) e o projeto da métrica seja prospectivo sempre que possível, e (d) a métrica seja simples e de fácil interpretação para um público menos familiarizado com o tópico.

Mudanças no ambiente externo, a prontidão interna ou o modelo de negócio podem causar impacto significativo sobre o começo da métrica do risco cibernético.

Assim, os começos devem ser analisados e atualizados pelo menos anualmente, ou com mais frequência no caso de métricas que sejam impactadas de modo significativo por mudanças em fatores externos ou internos.

Mas a mensuração do alinhamento ao apetite por risco cibernético não é suficiente. Para incorporar o apetite por risco cibernético à instituição, é importante vincular ações tangíveis às violações do começo do apetite por risco cibernético. As ações devem incluir uma análise da causa raiz e um plano de reparação para abordar o problema subjacente que é discutido com a alta administração e o Conselho de Administração. A discussão na alta administração e nos comitês do Conselho de Administração criam a conscientização e asseguram que os planos de reparação abordem questões estruturais, e que a administração tenha os recursos pertinentes para tratar do problema.

PRINCIPAIS ETAPAS PARA A ELABORAÇÃO CUIDADOSA DE UM APETITE POR RISCO CIBERNÉTICO EFICAZ

A elaboração de um apetite por risco cibernético eficaz de uma instituição começa no nível do Conselho de Administração. Uma vez estabelecido o apetite por risco cibernético no nível do Conselho, as afirmativas e métricas podem ser disseminadas para os níveis mais baixos da instituição. A partir do Conselho de Administração, recomendamos o uso de uma abordagem estruturada para a elaboração da estrutura do apetite por risco cibernético de uma instituição.

A elaboração de um apetite por risco cibernético eficaz é crucial para qualquer instituição que tenha exposição à internet. Embora isso possa ser uma tarefa difícil, fazê-lo corretamente pode entregar valor real para a instituição. Um apetite por risco cibernético bem elaborado (incluindo afirmativas e métricas) serve como uma ferramenta poderosa para a priorização do investimento em cibersegurança, tomando boas decisões de gestão de risco cibernético e criando a conscientização do risco cibernético pela instituição.

ESTRATÉGIA DE CIBER-RESILIÊNCIA

PREPARANDO-SE PARA UM CIBERATAQUE

James Cummings
consultor sênior, Risco Cibernético, Oliver Wyman

Paul Mee
sócio e chefe de cibernética, Oliver Wyman

Os exercícios simulados ajudam a desenvolver uma "memória muscular" que sirva como defesa contra violações internas e externas do sistema.

A cibersegurança, em muitas organizações, tem sido exposta, nos últimos anos, a um tipo de solução de queijo suíço, uma vez que os cibercriminosos descobriram pontos de entrada vulneráveis para arrancar centenas de milhões de dólares das principais empresas vítimas de hacking. Em inúmeras situações, as empresas deixaram de construir defesas sólidas, ou deixaram de reconhecer e reagir rapidamente a um ataque. Obviamente, a cibersegurança deve ser alçada aos principais níveis de estratégia de mitigação de risco, junto com risco de moeda, desastre natural e ataques terroristas.

Em nosso ponto de vista, os exercícios simulados podem ser de enorme valia para muitas empresas, em especial aquelas com enormes receitas diárias e/ou milhares de transações. Os exercícios simulados podem começar com cenários simples e prosseguir com simulações mais sofisticadas com fatores agravantes. Um determinado exercício é estruturado para simular um ataque real, com as várias partes interessadas – executivos do alto escalão, chefes de unidades de negócio, ou ambos – respondendo com ações e reações potenciais, bem como suas suposições e expectativas por trás dessas ações.

Um moderador e uma equipe preparados facilitam as mudanças, colocando os defensores dentro da mente de um hacker/criminoso. O moderador aplica fatores complexos como informações falsas, distrações, eventos climáticos extremos ou o fator tempo.
Uma equipe de analistas observa a simulação e, na sua conclusão, facilita um "hot wash" (discussões e avaliações pós-exercício) – extraindo os defeitos, as falhas e as lacunas, e convertendo isso em um conjunto de recomendações práticas.

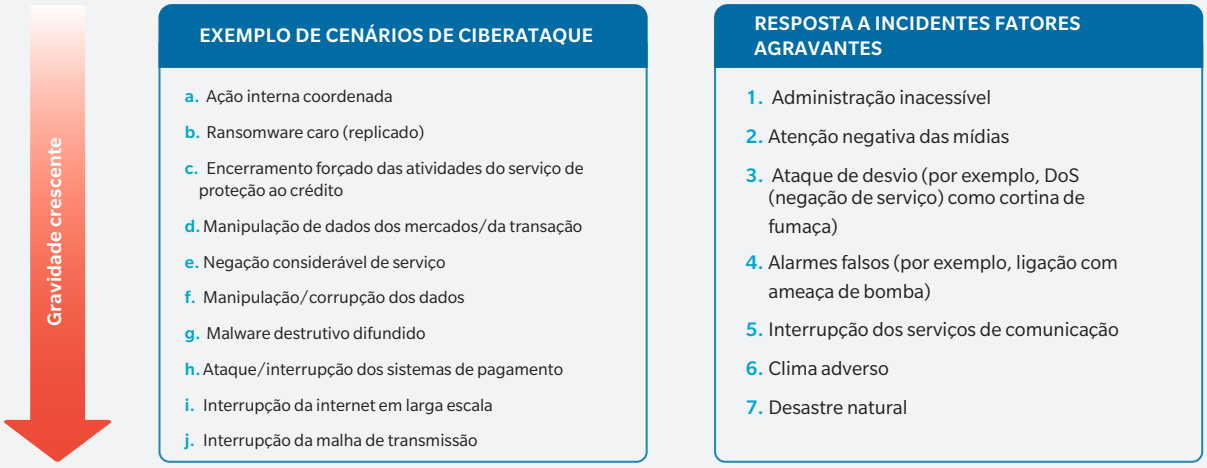
ROTEIRO PARA UM EXERCÍCIO SIMULADO CIBERNÉTICO

Uma empresa deve analisar o seu panorama e a sua perspectiva particular, com as metas ampliadas de identificação de lacunas na ciber-resiliência e otimização da governança de resposta (quem chama quem quando?). Com base nos recentes ataques do panorama de ameaças, em especial às organizações colegas – é possível customizar o exercício com riscos relacionados à cibernética específicos do ecossistema da sua organização. Desde o início, é essencial definir o que uma determinada organização ou comunidade deseja aprender de um exercício simulado de cibernética.

ANEXO 15: DEFINIR OS OBJETIVOS DO APRENDIZADO

1. Qual é o escopo completo das partes que estarão envolvidas em todo um importante incidente cibernético?
2. Que relacionamentos com o governo e outras agências, e a autoridade policial, devem estar instalados?
3. Que arranjos de liderança são necessários e como isso varia por tipo/gravidade de incidente?
   Por exemplo, quando o escritório do prefeito dará a resposta?
4. Onde os arranjos de governança e os direitos de decisão devem ser mais bem definidos?
5. Como as principais decisões serão tomadas, comunicadas e postas em prática com respeito a:
   - Determinação da gravidade do incidente
   - Contenção
   - Paralisação dos sistemas
   - Envio de mensagens ao público, às mídias e de supervisão
   - Declaração de "tudo OK"
6. Quais as decisões relacionadas à recuperação e à reparação coordenadas que devemos estar preparados para tomar?
7. Que planos de reparação, arranjos operacionais e recursos serão necessários após um importante incidente cibernético?
8. Qual é o escopo completo das partes que devem estar envolvidas na recuperação de um importante incidente cibernético?

ANEXO 16: CENÁRIOS DE CIBERATAQUE



CENÁRIOS

Usando estudos de caso de recentes eventos cibernéticos importantes, é possível selecionar os cenários com base na probabilidade de risco efetivo para a sua organização. Os cenários básicos podem ser preparados com variados graus de gravidade, idiossincrasias e surpresas, dependendo de seu atual nível de prontidão ou sofisticação.

O processo padrão é dar início com um caminho básico, linear, como uma Ação Interna Coordenada ou Negação de Serviço (DoS), com que as partes interessadas estão mais familiarizadas. O segundo caminho, mais dinâmico, acrescenta cenários de ataque mais grave, como Manipulação de Dados, Malware Destrutivo Difundido ou Parada grave da rede elétrica/internet. O terceiro caminho é como o anterior, mas acrescenta fatores agravantes – como Ataque de Cortina de Fumaça, Resposta Negativa das Mídias, Clima Adverso ou Ataque Terrorista (ver a figura no Anexo 16, "Cenários de Ciberataque").

EXERCÍCIO CIBERNÉTICO

O tamanho, o momento e a configuração do exercício simulado efetivo são no máximo determinados pelos objetivos – e pela disponibilidade dos executivos ou das principais partes interessadas.

A presença de todos não é totalmente necessária, mas proveitosa. Em teoria, o exercício é de um ou dois dias fora da unidade para aprimorar o engajamento ativo dos gerentes e executivos seniores responsáveis. Os especialistas e técnicos em cibernética também estão presentes como uma verificação da realidade e para contestar as suposições ou ações propostas.

Conduzir exercícios cibernéticos pelos cenários acordados:

- Caminho linear nº 1 — bem básico *(~60 minutos)*
- Caminho linear nº 2 — mais complexo *(~90 minutos)*
- Caminho dinâmico — fatores agravantes *(90 a 120 minutos)*

As respostas incluem a determinação da gravidade do incidente, a contenção, a paralisação dos sistemas e as comunicações das mídias. Uma vez detectado o ataque, a questão imediata é se devemos paralisar ou não todos os sistemas, apenas um segmento, ou nada. Você tenta conter um ataque visível ou aumentar as defesas para se proteger contra um ataque mais amplo? Parte do cálculo é uma função de determinar se você está lidando com um hacker de 14 anos ou com um hacker a serviço do estado.

O fundamental deste exercício cibernético é o mapeamento de quem faz o que, e quando. Quem faz a chamada? Como ela é feita então? Caso os principais participantes estejam fora da unidade, uma ação remota pode ser realizada facilmente? Quando se alerta a mídia ou a polícia local? O que é a "arvore de chamadas" – e há redundâncias caso um importante participante não possa ser localizado? Parte da elaboração de uma árvore de chamadas, além das informações básicas de contrato, é a preparação de um mapa de direitos de tomada de decisão – quem tem a autoridade em uma determinada organização/unidade ou área geográfica? E ainda há redundâncias quando uma determinada pessoa está indisponível?

Quanto ao final do jogo, quem dá o sinal de "tudo OK" mostrando que o ataque chegou ao fim e que os sistemas da empresa podem ser restaurados? Em todos os casos, o momento é importante – como finais de semana, feriados ou férias afetam a resposta? Existe uma equipe reserva, e ela está a par de tudo?

QUESTIONAMENTO DE "HOT WASH"

O "hot wash" post-mortem é um importante elemento do exercício global. As respostas propostas e a identificação de árvores de chamadas precisam ser totalmente analisadas e refinadas. As pessoas certas estavam tomando decisões? Onde estão as principais lacunas, que problemas surgem e se destacam, a governança está preparada para os ataques, qual o plano de comunicação interna e externa?

Refaça as notas do analista para determinar se houve de fato um plano preparado instalado, ou se as pessoas estavam agindo na correria. No último caso, fica claro que um livro de procedimentos deve ser redigido. Determine se a polícia deveria ter sido chamada – ou chamada anteriormente. Quando a Sony Pictures foi hackeada em 2014 – possivelmente pela Coreia do Norte – ela esperou uma semana antes de ligar para a polícia.

Em retrospectiva, parece que a notificação imediata teria tornado o evento menos penoso para a Sony.

Mesmo quando você decide não chamar a polícia, está bem claro que você tomou uma decisão consciente e que não se tratou de um descuido.

Este exercício "hot wash" naturalmente leva a um conjunto de recomendações para as pessoas, o grupo coletivo de importantes partes interessadas, e os pilares externos como a autoridade policial e a mídia.

Desenvolver uma longa lista de observações, lacunas e principais problemas, então extrair dali as recomendações. Produzir um pacote informativo e dividir informações sobre as conclusões.

REPITA A DOSE

A configuração do primeiro exercício simulado é geralmente aquela de um exercício de várias semanas. Os exercícios subsequentes podem ser organizados de maneira bem mais rápida. A configuração inclui entrevistar os principais participantes para estabelecer os objetivos e avaliar a disponibilidade. Uma vez decididos horário e local, a equipe central (moderador e analistas) realiza um ensaio final.

Fazer esse exercício não é um evento único. Dada a crescente sofisticação dos cibercriminosos, e a infraestrutura sediada na nuvem e em constante expansão, sempre há novas vulnerabilidades a evitar. De modo ideal, esses exercícios simulados são um evento trimestral ou semestral. Muitas organizações agora realizam exercícios trimestrais nas diferentes áreas da organização – finanças, risco, linhas de negócio. Uma cadência regular de exercícios desenvolverá uma "memória muscular" da organização para reagir e justificar o gasto na melhoria das defesas. Como ocorreu com a pintura da Golden Gate, quando você já passou por todas as partes da organização, precisa começar tudo de novo. Você está em uma corrida sem linha de chegada.

ESTRATÉGIA DE CIBER-RESILIÊNCIA

O ENCONTRO DA CURVA DE PERDA CIBERNÉTICA FURTIVA PODE PAGAR GRANDES DIVIDENDOS PARA AS INSTITUIÇÕES FINANCEIRAS

Kevin Richards
chefe global de consultoria de risco cibernético, Marsh

Thomas Fuhrman
Diretor executivo - consultor de cibersegurança, Marsh

Alex deLaricheliere
diretor executivo – US Banking & Capital Markets, Marsh

Qual é a probabilidade de sua organização vivenciar um evento cibernético relevante nos próximos 12 meses? O risco é maior do que 50%? Menor do que 25%? Estas perguntas estão sempre presentes nas mentes dos gestores de risco, que anseiam por uma resposta pelo menos prática – se não for precisa.

Os riscos cibernéticos estão entre os mais graves perigos enfrentados pelo setor financeiro. O crime cibernético não somente está crescendo na frequência, mas também na magnitude, custando ao mundo uma estimativa de US$ 600 bilhões, ou 0,8% do PIB global, de acordo com um relatório recente publicado pela McAfee e pelo Centro de Estudos Estratégicos e Internacionais. Mas enquanto as instituições financeiras se tornaram experientes na estimativa da maioria dos riscos operacionais e usando estes dados para desenvolver estratégias de capital de risco, elas em geral desenvolvem barreiras para a ampliação desses métodos para a cibernética.

UM ABISMO DE INFORMAÇÕES

Um problema importante orbita pela falta de dados. Diferentemente dos outros riscos, existe uma quantidade limitada de dados históricos sobre o crime cibernético, principalmente porque esta é uma área de risco relativamente nova devido à sua forma em constante mudança. A gestão de risco cibernético ainda não foi "colocada em prática" em uma ampla escala.

Tradicionalmente, as entidades financeiras usavam estruturas qualitativas – vermelho, amarelo, verde ou alta, média, baixa – para caracterizar as ameaças cibernéticas, um sistema também comumente usado em outros setores. Esta abordagem pode ser bastante útil, mas não é mais suficiente para o setor financeiro, que vem sentindo uma necessidade crescente de determinar quantidades para o risco cibernético, calculando tanto a gravidade quanto a probabilidade. Uma metodologia mais quantitativa é necessária tanto para melhorar a proteção de uma empresa quanto para observar os regulamentos cada vez mais rigorosos, inclusive a estrutura de Basileia III e as normas impostas pelos reguladores nacionais.

Embora isto possa ser um esforço complexo, um ponto de partida é levar em conta a análise do cenário. Esta abordagem permite apontar estimativas do custo financeiro – a gravidade – dos eventos cibernéticos com boa precisão. Bem mais difícil é a determinação da probabilidade de um evento. Ter estimativas quantitativas confiáveis para a gravidade e a probabilidade permitirá que os gestores de risco respondam à pergunta fundamental:

"Qual é a probabilidade de sua organização vivenciar um evento cibernético que cause uma perda maior, digamos, do que US$ 100 milhões nos próximos 12 meses?" Na maior parte das vezes, é a questão da probabilidade que inviabiliza muitas tentativas de quantificar o risco cibernético, devido à natureza imprevisível de uma ameaça iniciada por um ser humano. Contudo, a despeito das limitações, os profissionais do risco financeiro devem enfrentar este desafio seguindo o ditado de que todo risco pode ser modelizado.

Nos últimos anos, motivados pelas normas e diretrizes do Comitê de Supervisão Bancária da Basileia, os reguladores dos bancos dos EUA e globalmente deram ênfase à necessidade de que as instituições financeiras tivessem reservas de capital adequadas ao modelizar uma ampla gama de riscos. Mais ainda, as empresas financeiras nos EUA são solicitadas a realizar testes de estresse em seus balanços patrimoniais, abordando uma série de cenários de alto impacto e baixa probabilidade, inclusive eventos cibernéticos. E os examinadores dos bancos dos EUA realizam regularmente avaliações de cibersegurança de todos os bancos.

Em 2016, o Federal Reserve, o Controlador da Moeda e o Federal Deposit Insurance Corporation emitiram uma Notificação Prévia em Matéria de Regulamentação Proposta (ANPR) declarando a sua intenção de estabelecer padrões mais rigorosos sobre as instituições sistematicamente importantes. Entre outras propostas, a ANPR afirmava a sua pretensão de desenvolver "metodologia consistente e reproduzível" para medir o risco cibernético. Sua convocação para apresentação de metodologias potenciais para quantificar o risco cibernético inerente e residual enfatiza a necessidade de que o setor financeiro aplique esses procedimentos para medir meticulosamente o risco cibernético.

Além do impulso regulador, existe grande reconhecimento no setor de que as instituições financeiras devem envidar esforços robustos para identificar e estimar o risco cibernético e proteger as suas operações e clientes das repercussões perturbadoras e potencialmente dispendiosas dos ciberataques.

CALCULANDO A CURVA DE PERDAS

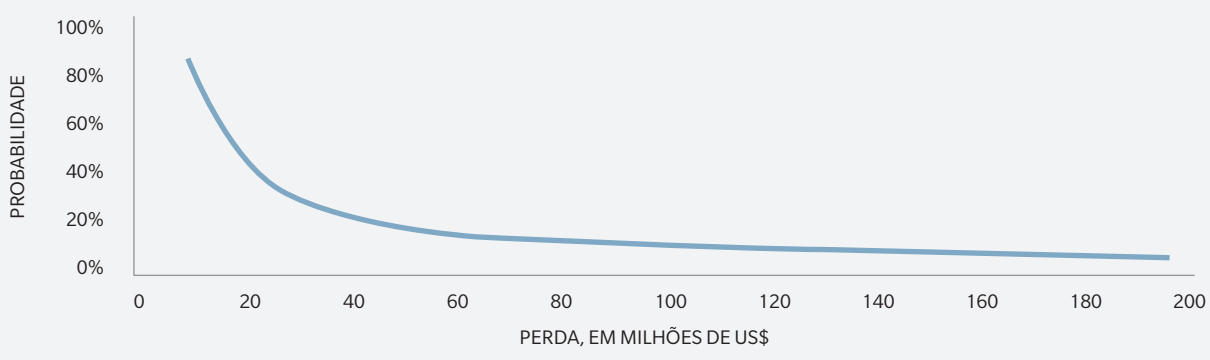
Quando se lida com eventos improváveis, a probabilidade e o impacto estão inextricavelmente vinculados; este é o que acontece em toda área de risco. Em geral, o relacionamento entre os dois pode ser expresso por uma curva de distribuição de perda não linear (ver o Anexo 17), que descreve uma situação em que o custo mais alto está associado à probabilidade mais baixa. Eventos muito dispendiosos são raros; eventos menos dispendiosos são mais comuns. Quando há suficientes dados históricos disponíveis, isso pode ser normalmente descrito com este tipo de curva característica. Se uma curva de perdas puder ser representada matematicamente com um grau adequado de confiança, ela pode abrir grandes oportunidades para a gestão do risco que representa. Isso permite que os profissionais de risco calculem o apetite por risco e a tolerância ao risco em suas organizações, e que consigam um bom entendimento sobre os riscos associados a eventos na "extremidade" (no lado direito) da curva. Nenhum modelo é perfeito, mas uma estimativa baseada nos dados da curva de perdas pode permitir que os líderes empresariais entendam melhor os riscos da cibernética e ajam no sentido de administrá-los.

A curva de perdas tem sido de fato usada como um pano de fundo para a modelização dos riscos operacionais durante algum tempo. Mas e sobre a cibernética? A cibernética em si é, afinal das contas, um risco operacional. A ideia da curva de perdas há tanto tempo estabelecida se aplica à cibernética? Certamente, a curva de perdas tradicional tem apelo intuitivo quando pensamos em risco cibernético. Parece que uma perda de, digamos, US$ 150 milhões devido a um ciberataque pelo menos é algo menos provável do que uma perda de US$ 50 milhões. Enquanto não existir certeza de que os riscos cibernéticos podem ser descritos de modo eficiente com a curva de perdas tradicional – poderiam os hackers causar eventos extremos mais dispendiosos para se tornarem eventos mais prováveis do que menos dispendiosos? – esta é uma abordagem de modelização atraente para se começar.

DESENVOLVENDO UMA CURVA DE PERDAS CIBERNÉTICA

A cibernética é hoje um dos mais desafiadores entre os riscos operacionais e pode passar muito tempo, se é que acontecerá um dia, antes de haver dados históricos suficientes para o desenvolvimento de uma curva de perdas específica da cibernética de uma organização com certeza. Mas a análise do cenário pode ajudar. Os profissionais de risco já estão familiarizados com a modelização do cenário para esboçar a curva de perdas para os riscos operacionais.

ANEXO 17: CURVA DE PERDAS REPRESENTATIVA



Esta abordagem também pode funcionar na cibernética. Poucas regras simples se aplicam ao desenvolvimento do cenário: foco nos riscos das extremidades; procurar eventos que sejam improváveis, mas plausíveis; e assegurar que os eventos são específicos da organização e do sistema com detalhes suficientes para analisar as perdas com precisão. Quando houver estimativas suficientes para impacto e probabilidade, mesmo com grandes intervalos de confiança, os "pontos dos pseudodados" podem ser plotados, e a curva de perdas começa a tomar forma.

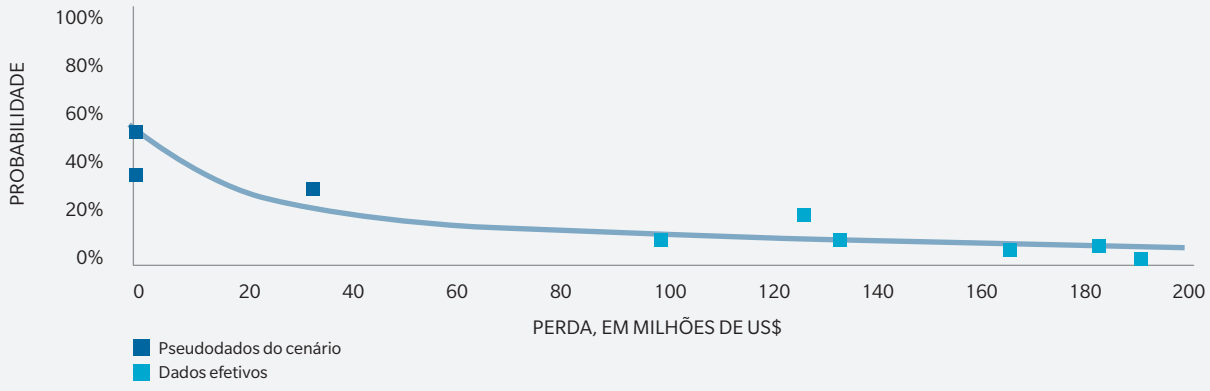
As estimativas de pseudodados do cenário podem ser combinadas com os dados efetivos dos eventos do mundo real, quando estes estiverem disponíveis (ver o Anexo 18). Através do ajustamento de curvas razoável com base em uma distribuição presumida – como log normal, Poisson, ou outra – uma instituição financeira pode desenvolver uma aproximação da curva de perdas para a cibernética imprecisa.

Este tipo de análise reúne a probabilidade e a gravidade em uma fórmula matemática, oferecendo insight para os gestores de risco e outras importantes figuras no risco de que a cibernética representa para as suas organizações. Em última análise, encontrar a curva de perdas na cibernética pode pagar grandes dividendos. As instituições financeiras podem usar este tipo de modelização como uma ajuda para o desenvolvimento de uma estrutura significativa de risco de capital para a cibernética que não pode apenas tratar dos requisitos reguladores, mas também elevar o papel da organização na gestão de risco cibernético.

QUE CENÁRIOS DE CIBERATAQUE AS INSTITUIÇÕES FINANCEIRAS DEVEM LEVAR EM CONTA?

1. Interrupção ou pane nas principais plataformas bancárias: Identificar as diferentes áreas que poderiam ser afetadas, e se poderia haver práticas alternativas de trabalho que possam ser usadas durante um período de paralisação.
2. Corrupção de bancos de dados: Considerar se é preciso ter cópias impressas para dar continuidade às operações no caso de um ciberataque.
3. Corrupção dos sistemas de back office: Determinar o custo dessa interrupção e criar um plano de backup robusto.
4. Interrupção das plataformas eletrônicas de negociação: Corretores, bancos de investimento, bolsas e terceiros envolvidos na compra e venda de ações, títulos e outros instrumentos financeiros devem ver se podem operar com conectividade perdida ou corrompida.
5. Interrupção estendida do serviço de internet: Determinar como a sua instituição será afetada se você e terceiros com quem você faz negócio forem forçados a ficar fora da internet durante um prazo não especificado. Considerar se algumas das operações, ou todas, podem continuar offline.

ANEXO 18: COMBINANDO DADOS ATUAIS E PSEUDODADOS PARA DETERMINAR A PERDA ESPECÍFICA DA CIBERNÉTICA



CONTATO

Para mais informações e outras consultas, entre em contato conosco conforme as instruções abaixo.

Tom Reagan
chefe de prática de Cibernética dos EUA, Marsh
Thomas.Reagan@marsh.com

Kevin Richards
chefe global de consultoria de risco cibernético, Marsh
Kevin.Richards@marsh.com

Paul Mee
sócio e chefe de cibernética, Oliver Wyman
Paul.Mee@oliverwyman.com

Jeremy Platt
chefe de prática de Soluções de Produtos Especializados Cibernéticos, Guy Carpenter
Jeremy.S.Platt@guycarp.com

Leslie Chacko
conselheira, Tecnologias Transformativas, Marsh & McLennan Insights
Leslie.Chacko@oliverwyman.com

Victoria Shirazi
diretora associada, Ciber-resiliência, Marsh & McLennan Solutions
Victoria.Shirazi@mmc.com

SOBRE A MARSH & MCLENNAN INSIGHTS

A Marsh & McLennan Insights usa a perícia única de nossa empresa e suas redes para identificar perspectivas e soluções inovadoras aos desafios mais complexos da sociedade. A Marsh & McLennan Insights exerce um papel crítico na entrega da abordagem única da MMC Advantage – Marsh & McLennan visando utilizar a força coletiva de nossos negócios para ajudar os clientes no tratamento de seus maiores desafios referentes a riscos, estratégia e pessoas.

SOBRE A MARSH & MCLENNAN COMPANIES

A Marsh & McLennan (na Bolsa de Nova York (NYSE): MMC) é a empresa líder na prestação de serviços profissionais nas áreas de risco, estratégia e pessoas. Os cerca de 65.000 colegas da empresa orientam clientes em mais de 130 países. Com uma receita anual de mais de US$ 14 bilhões, a Marsh & McLennan ajudam os clientes a navegar em um ambiente cada vez mais dinâmico e complexo através de quatro empresas líderes no mercado. A Marsh orienta clientes individuais e comerciais de todos os tamanhos sobre corretagem de seguro e soluções inovadoras de gestão de risco. A Guy Carpenter desenvolve estratégias avançadas de risco, resseguro e capital que ajudam os clientes a aumentar a lucratividade e buscar oportunidades emergentes. A Mercer fornece orientação e soluções voltadas para a tecnologia que ajudam as organizações a atender às necessidades de saúde, riqueza e carreira de uma força de trabalho em mudança. A Oliver Wyman atua como uma consultora crítica estratégica, econômica e de marca para o setor privado e para clientes governamentais. Para mais informações, visite mmc.com, siga-nos no LinkedIn e no Twitter @mmc_global ou subscreva o BRINK.