RELATÓRIO ESPECIAL DE SEGURANÇA CIBERNÉTICA

EMPRESAS DE PEQUENO E DE MÉDIO PORTE

Pequenas e poderosas

Como as empresas de pequeno e médio porte podem fortalecer suas defesas contra as ameaças atuais

CISCO

53% de empresas de médio porte sofreram uma violação

até

5000

Número médio de alertas de segurança

Empresas de médio porte investigam **55,6%** de alertas de segurança

Vinte e nove por cento das empresas de médio porte dizem que as violações custam, para eles, menos de US$ 100 mil. Vinte por cento afirmam que os custos são de US $1.000.000 a US $2.499.999

Muitas empresas de pequeno e médio porte aspiram práticas mais eficientes de segurança cibernética, como suas contrapartes maiores. As empresas de pequeno e médio porte são dinâmicas, o backbone da inovação e as garotas propagandas do trabalho duro. Elas correm ainda mais rápido e trabalham mais do que as outras empresas. E são expostas às mesmas ameaças digitais.

No cenário de ameaça digital de hoje, todas as empresas, grandes ou pequenas, estão em risco de um ataque. Mas, cada vez mais, empresas de pequeno/médio porte são o foco de ataques [1] e muitas vezes servem como uma plataforma de lançamento ou conduíte para campanhas maiores. Os criminosos veem as empresas de pequeno/médio porte como alvos fáceis que têm Infraestrutura e práticas de segurança menos sofisticada e um número inadequado de pessoal treinado para gerenciar e responder a ameaças. [1]

Muitas empresas de pequeno/médio porte estão apenas começando a perceber como são atraentes para os criminosos digitais. Muitas vezes, essa percepção vem tarde demais: depois de um ataque. A recuperação de um ataque cibernético pode ser difícil e cara, se não impossível, para essas empresas, dependendo da natureza e do escopo da campanha. Este relatório proporcionará um entendimento dos riscos que as empresas menores enfrentam, compartilhará um entendimento de como as pequenas empresas se preparam, em relação às outras empresas com relação à segurança e compartilhará um pouco de orientação para se considerar durante 2018 e além.

Considere estas descobertas do estudo comparativo de recursos de segurança de 2018 da Cisco: Mais da metade (54%) de todos os ataques digitais resultam em danos financeiros de mais de US$ 500.000, incluindo, mas não limitado, à perda de receita, clientes, oportunidades, e despesas. Esse valor é suficiente para tirar uma empresa de pequeno/médio de operação, permanentemente.

Um estudo recente da Better Business Bureau (BBB) [2] ajuda para enfatizar como as empresas de pequeno/médio porte podem lutar financeiramente para sobreviver depois de um ataque cibernético grave. A BBB perguntou a proprietários de pequenas empresas na América do Norte, “Por quanto tempo sua empresa permanece lucrativa se você tiver perdido, permanentemente, acesso a dados essenciais?” Apenas cerca de um terço (35%) disseram que poderiam permanecer lucrativos por mais de três meses. Mais da metade relatou que ficariam não lucrativas em menos de um mês.

A propósito, vemos empresas de pequeno e médio porte como empresas com menos de 250 funcionários e as definimos como empresas com 250 a 499 funcionários. Os dois segmentos estão incluídos neste relatório.

Analisamos os resultados dos entrevistados de empresas de pequeno e médio porte no nosso estudo comparativo sobre recursos de segurança de 2018, que chamaremos, simplesmente, de estudo comparativo. Esse estudo oferece informações práticas de segurança atualmente em uso e compara os resultados completos dos últimos três anos.

Nossos dados de empresas de pequeno/médio porte incluem 1816 respondentes em 26 países.

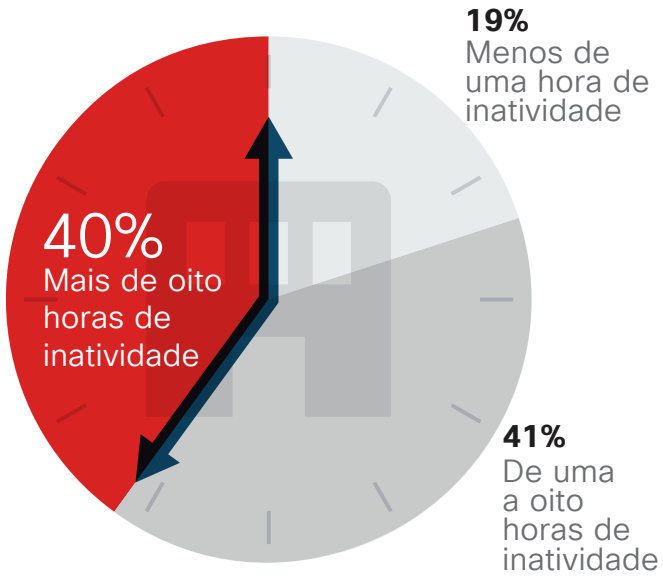
1 Ameaças digitais e soluções para empresas de pequeno e médio porte, Vistage Research Center, 2018. Desenvolvido em colaboração com a Cisco e o National Center for the Middle Market (Centro Nacional para o mercado de empresas de médio porte). Disponível em: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.
2 Estado de segurança cibernética entre as pequenas empresas na América do Norte, BBB, 2017: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

O que é um dia de negócios perdidos entre os colegas?

Disse nenhum administrador de TI jamais. Tempo de inatividade do sistema, que reduz a produtividade e a lucratividade, é um problema significativo para as empresas depois de um ataque digital. Pesquisa do estudo comparativo descobriu que 40% dos respondentes (250 a 499 funcionários) passaram por oito horas ou mais de tempo de inatividade do sistema, devido a uma violação de segurança grave no ano passado (Figura 1). A Cisco viu resultados semelhantes para empresas maiores na amostra de estudo (aquelas com 500 ou mais funcionários). A diferença, porém, é que empresas de grande porte tendem a ser mais resilientes do que empresas de pequeno/médio porte depois de um ataque, pois elas têm mais recursos para recuperação e resposta.

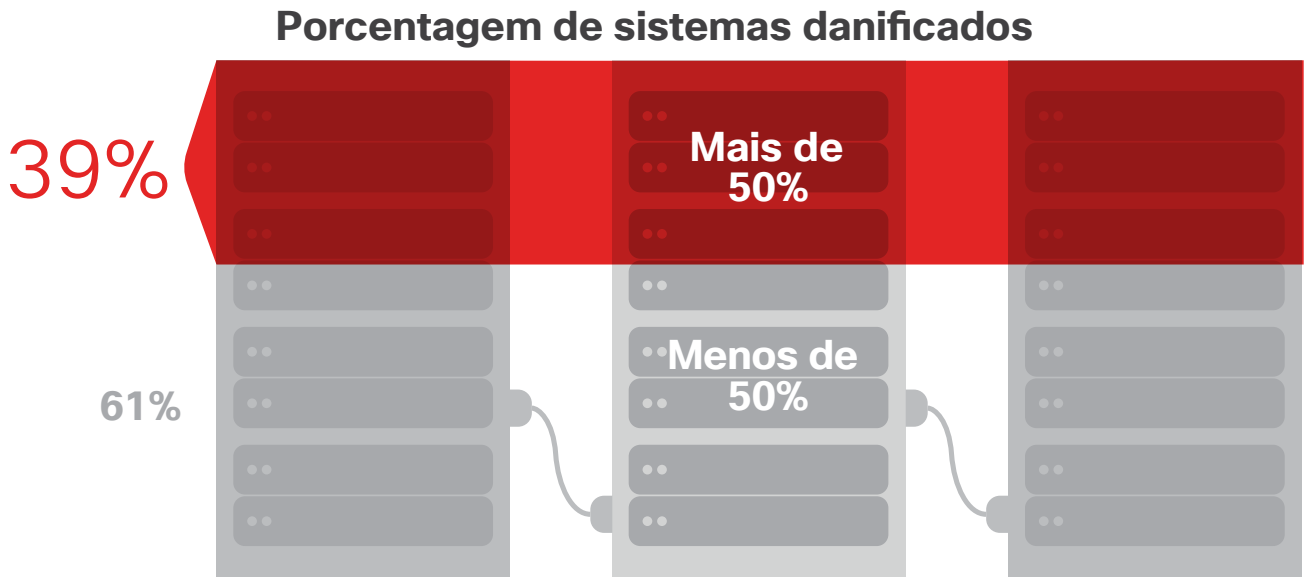
Além disso, 39% dos respondentes relataram que pelo menos metade dos seus sistemas tinham sido afetados por uma violação grave (Figura 2). Pequenas empresas apresentam menor probabilidade de ter vários locais ou segmentos de negócios e seus sistemas principais geralmente são mais interconectados. Quando essas empresas passam por um ataque, a ameaça pode se espalhar fácil e rapidamente da rede para outros sistemas.

Figura 1 Tempo de inatividade do sistema depois de uma violação grave



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Figura 2 Porcentagem dos sistemas afetados por uma violação grave



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

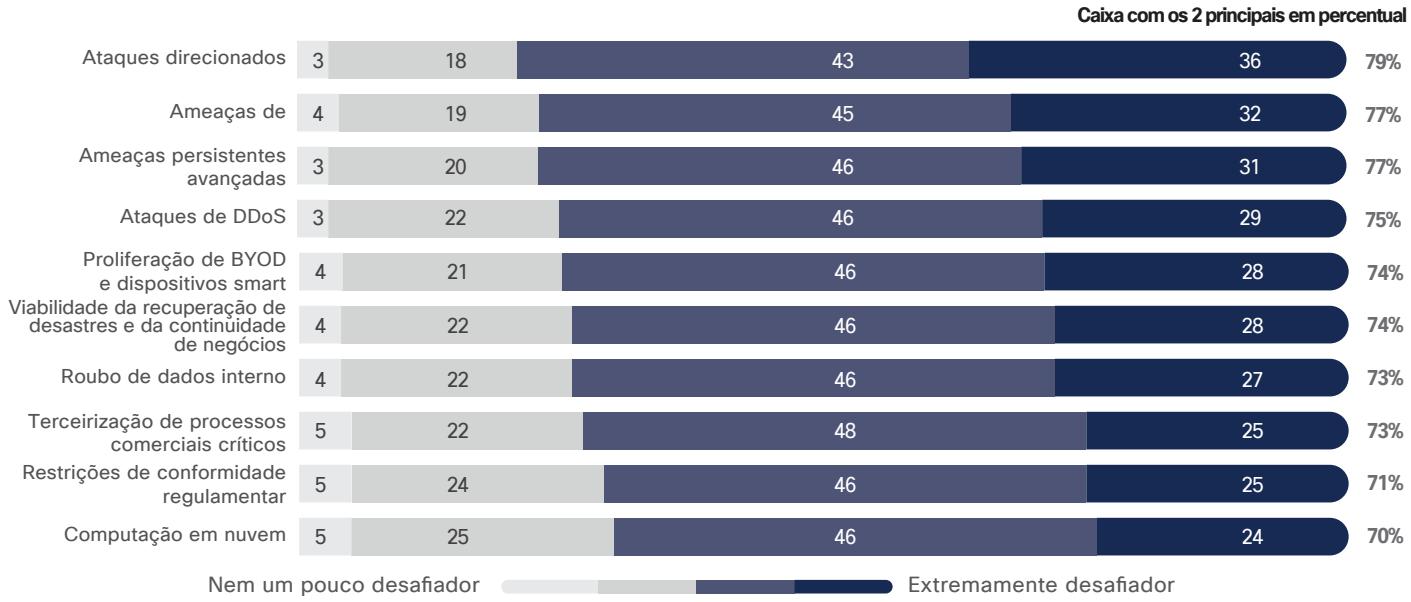
Noites de segurança sem sono

Quando perguntados sobre os maiores desafios de segurança que enfrentam, os respondentes estão mais preocupados com três coisas:

- Ataques direcionados contra funcionários (phishing bem pensado e bem projetado)
- Ameaças persistentes avançadas (malware avançado que o mundo nunca viu antes)
- Ransomware

O ransomware (é interessante, que não tenha sido citado como uma das "três principais" preocupações de grandes empresas) é, como sabemos, conhecido agora, como um malware que criptografa os dados, normalmente até que os usuários afetados paguem uma demanda de resgate e também pode criar interrupção grave e tempo de inatividade do sistema para empresas de pequeno/médio porte. O ransomware também é caro de forma diferente para essas empresas: especialistas em segurança da Cisco explicam que empresas de pequeno/médio porte são mais propensas a pagar resgates para os criminosos para que possam, rapidamente, retomar as operações normais. Elas simplesmente não podem pagar pelo tempo de inatividade e falta de acesso a dados essenciais, incluindo dados do cliente. (Consulte a Figura 3).

Figura 3 As principais preocupações de segurança das empresas de médio porte[5]



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Outras ameaças que as empresas de pequeno e médio porte não podem ignorar

Apesar das preocupações com o ransomware, os especialistas de segurança da Cisco sugerem que as ameaças estão diminuindo, pois mais criminosos estão mudando o foco para mineração de criptomoeda ("criptomineração"). O atrativo dessa atividade é triplo: pode ser altamente lucrativo, não podem ser rastreados pagamentos e os criminosos podem se preocupar menos com a possibilidade de responsabilidade criminal por suas ações. (Por exemplo, não há risco de os pacientes não terem o atendimento de que precisam porque os sistemas do hospital e os dados essenciais estão bloqueados pelo ransomware). Os criminosos também podem oferecer um software de mineração ("mineradores") por vários métodos, incluindo campanhas de spam de e-mail e kits de exploração. [3]

3 Resgate onde? Tomada do poder pelos mineradores de criptomoedas, gerando milhões", blog Cisco Talos, Janeiro 31, 2018: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Os pesquisadores de ameaças da Cisco explicam que os criminosos que usam o novo modelo de negócios de criptomineração ilícita "não estão mais penalizando as vítimas por abrir um anexo ou executar um script malicioso fazendo os sistemas reféns e exigindo um resgate. Agora [eles] estão usando, ativamente, os recursos de sistemas infectados."[4] Para empresas de pequeno/médio porte que não estão dispostas a ajudar nas operações de criptomineração ilícita, sistemas mais lentos podem ser o único sinal de que foram invadidas, a menos que tenham a tecnologia certa para detectar quando a atividade de criptomineração está presente.

A ameaça interna de 0,5%: 100% muito alto?

À medida que as empresas participantes movem mais dados e processos para a nuvem, também devem tomar medidas para gerenciar outra possível ameaça: pessoas desonestas dentro da própria empresa. Sem ferramentas para detectar atividades suspeitas (como o download de informações confidenciais do cliente), elas correm o risco de perda de propriedade intelectual, dados financeiros e confidenciais e dados dos clientes pelos sistemas da nuvem corporativa.

Uma investigação recente por pesquisadores de ameaças da Cisco destaca o risco: De janeiro a junho de 2017, examinaram tendências de extração de dados usando aprendizado de máquina para criar o perfil de 150.000 usuários em 34 países, que estavam usando a nuvem. Durante um mês e meio, os pesquisadores descobriram que 0,5% dos usuários fizeram downloads suspeitos. Meio por cento parece ruim? Dito de outra forma, isso significa que dois funcionários em uma empresa de 400 pessoas seriam ameaças internas. Isso é 100% muito alto. Especificamente, esses usuários baixaram, no total, mais de 3,9 milhões de documentos de sistemas da nuvem corporativa. É uma média de 5200 documentos por usuário durante um período de um mês e meio.[5]

Estudo comparativo de recursos de segurança da Cisco de 2018

Este relatório especial tem descobertas de dados selecionados do estudo comparativo de recursos de segurança 2018 da Cisco. A pesquisa envolveu mais de 3600 entrevistados em 26 países. Para obter mais informações sobre as práticas de segurança atualmente em uso por empresas de todos os tamanhos e uma comparação dos resultados de estudos anteriores da Cisco, baixe o *Relatório anual de segurança digital 2018 da Cisco* disponível em: https:// www.Cisco.com/c/en/US/products/Security/Security-Reports.html.

4 Ibid.
5 Para obter mais detalhes, consulte "Ameaças internas: aproveitando a nuvem" no Relatório anual de segurança cibernética 2018 da Cisco, disponível em: https://www.cisco.com/c/en/us/products/security/security-reports.html.

Desafios

A melhor defesa contra ameaças descritas anteriormente – exige coordenação e orquestração de recursos de TI. Esses recursos são mais comumente a pessoas, os processos e a tecnologia que as empresas podem acumular para impedir ataques.

No entanto, ainda mais que as empresas maiores, as empresas menores são desafiadas a coordenar esses recursos de forma que gerem dados sobre ameaças e parem ou mitiguem ataques, antes que eles causem danos. A falta perene de talentos de segurança que afeta as empresas causa impacto constante nas contrapartes menores ainda mais.

Tendências de tecnologia de segurança das empresas de pequeno e médio porte

Indo em frente, as empresas menores procuram, na realidade, abordar os desafios de segurança cibernética que ameaçam suas organizações com novas ferramentas para parar as ameaças.

Respondentes do estudo comparativo disseram que se recursos de pessoal estivessem disponíveis, estariam mais propensos a:

- Atualizar a segurança de endpoint para proteção avançada contra malware mais sofisticadas/EDR – a resposta mais comum em 19%.
- Considerar a melhor segurança de aplicativo da Web contra ataques na Web (18%)
- Implantar prevenção contra intrusões, ainda visto como uma tecnologia vital para interromper os ataques da rede e tentativas de exploração. Dezessete por cento (17%) (Veja a Figura 5).

À medida que as empresas consideram novas tecnologias, um desafio é determinar como os produtos operam entre eles para manter as empresas protegidas. Os encargos de gerenciamento de varredura por muitos consoles para responder a ameaças ou incidentes de segurança não devem ser subestimados.

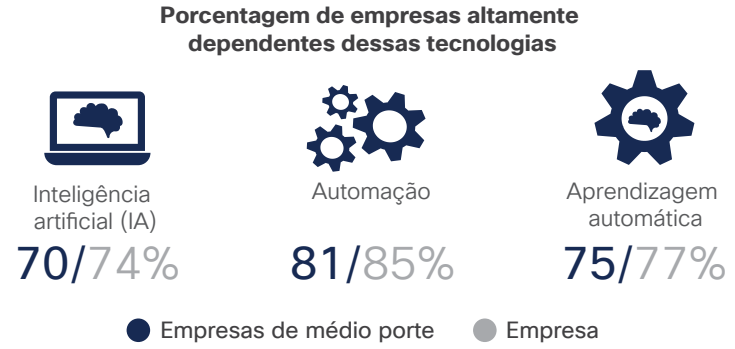
“Muitas pessoas pensam que se usarem uma abordagem de vários fornecedores, do melhor da categoria, isso as protegerá mais”, diz Ben M. Johnson, CEO da Cisco partner Liberty Technology em Griffin, Geórgia. “Mas o que vemos é que isso é mais difícil de gerenciar, pois custa mais e reduz a eficácia da segurança no geral”.

Aprendizado de máquina: Ajuda de segurança ou apenas campanha de marketing?

Ouvimos sobre o aprendizado de máquina devido à sua fama recente. Afinal, as empresas de médio porte contam com praticamente a mesma quantidade de aprendizado de máquina que as empresas maiores com relação a soluções analíticas que podem detectar, com eficácia, os ataques. Soluções que usam aprendizado de máquina e automação são usadas de forma menos intensa pelas empresas de médio porte, quando comparado a organizações com mais de 1.000 funcionários (Figura 4).

O aprendizado de máquina é mais eficaz quando é uma camada adicional de detecção em um produto já implantado, em oposição à compra de um produto separado para “fazer aprendizado de máquina”. Dessa forma, as equipes ganham o benefício do aprendizado de máquina para detectar anomalias e ameaças à velocidade da máquina, sem nenhuma despesa com novas equipes.

Figura 4 Empresas de médio porte contam menos com a automação e com as ferramentas de IA



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Empresas de médio porte móveis

As empresas também reconhecem que suas abordagens de segurança devem atender às demandas do ambiente de trabalho moderno e, em particular, à mudança para a mobilidade e a adoção de dispositivos móveis. Cinquenta e seis por cento (56%) dos respondentes disseram que defender dispositivos móveis de ataques digitais é considerado muito desafiador ou extremamente desafiador.

Empresas de médio porte e a nuvem

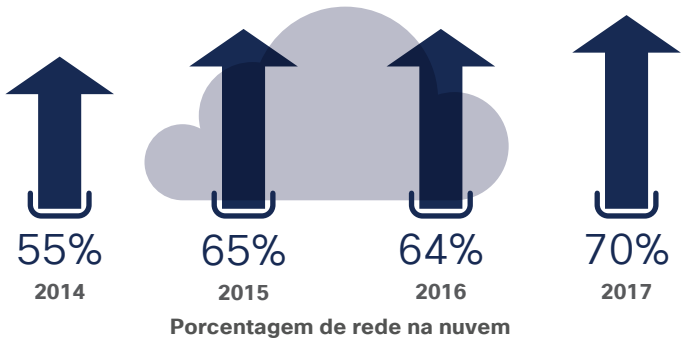
Reconhecendo os desafios de segurança, muitos respondentes estão buscando para a nuvem para reforçar as defesas sem contratar mais pessoas ou sobrecarregar os recursos atuais. A questão é se a mudança da segurança para a nuvem é uma estratégia suficiente para se proteger de ataques. Além disso, as empresas não podem simplesmente descarregar a responsabilidade migrando os dados para a nuvem : Elas ainda devem estar bem informadas sobre os controles de segurança impostos pelos provedores de nuvem, bem como sobre como possíveis violações na nuvem podem afetar os recursos no local.

A adoção de serviços na nuvem entre empresas de médio porte está claramente em ascensão, com base em pesquisa da Cisco. Em 2014, 55% dessas empresas disseram ter hospedado algumas das suas redes por uma forma de nuvem. Em 2017, esse número aumentou para 70% (Figura 5).

Muitos respondentes acreditam que a nuvem pode ajudar a fechar as lacunas nas suas defesas, além de resolver alguns problemas em sua infraestrutura e nas habilidades de seus funcionários. Na verdade, de acordo com a pesquisa da Cisco, o principal motivo das empresas de médio porte para hospedar redes na nuvem é a crença de que ela oferece melhor segurança aos dados (68%). O segundo motivo mais popular é que a empresa não tem trabalhadores internos suficientes (49%). (Consulte a Figura 6).

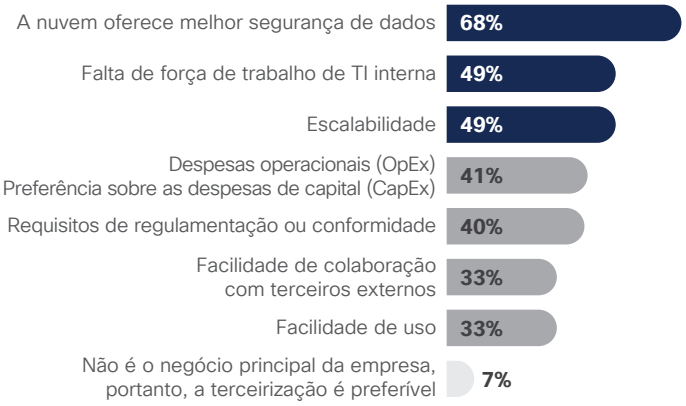
As empresas de médio porte também preferem a nuvem, devido à sua escalabilidade, ou seja, reduzindo a dependência da empresa em seus recursos internos – e a mudança flexível para as despesas operacionais, em vez de despesas de capital (Figura 6).

Figura 5 As empresas e médio porte mostram um aumento constante na adoção da nuvem



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Figura 6 As empresas de médio porte escolhem a nuvem para segurança e eficiência



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Pessoas: Como encontrar pessoal para reforçar a segurança

A boa notícia é que o estudo comparativo mostra que 92% das empresas de médio porte têm um executivo responsável pela segurança. (Consulte a Figura 7).

Considerando os recursos de equipe ampla, as empresas de médio porte estariam dispostas a acrescentar mais ferramentas de segurança, como firewalls de aplicativos da Web ou proteções avançadas de endpoint.

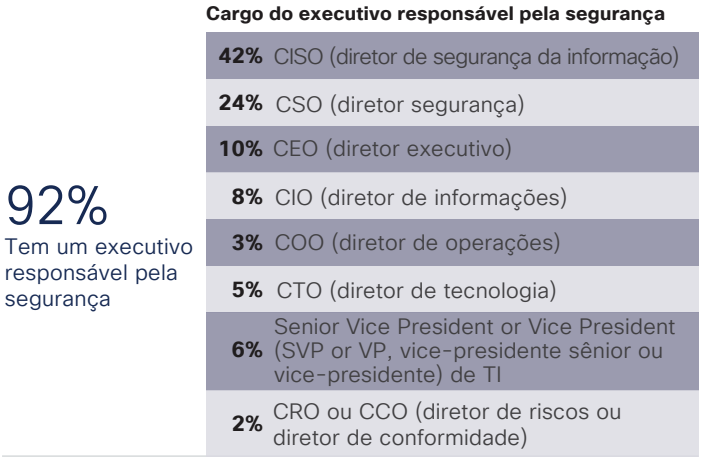
Empresas de médio porte têm algo em comum com empresas maiores: uma escassez de pessoal de TI, dificultando a capacidade de fortalecer as defesas. Simplesmente não há pessoas suficientes internamente para gerenciar ferramentas que podem melhorar a segurança, de acordo com a pesquisa da Cisco.

Por esse motivo, muitas empresas de pequeno/médio porte buscam ajuda terceirizada para reunir os talentos que precisam para aumentar seu conhecimento de ameaças, economizar dinheiro e responder a violações mais rapidamente. O desejo de informações independentes foi o motivo mais comum dado por empresas de médio porte para a terceirização de suas tarefas de segurança (Figura 8), seguido pela eficiência de custo e a necessidade de responder prontamente a incidentes de segurança.

Ajuda da terceirização é uma boa maneira de as empresas extraírem o máximo de recursos limitados. Mas essas empresas podem ter problemas, se presumirem que um provedor terceirizado ou um parceiro de nuvem fornecerá todos os recursos que elas não têm internamente.

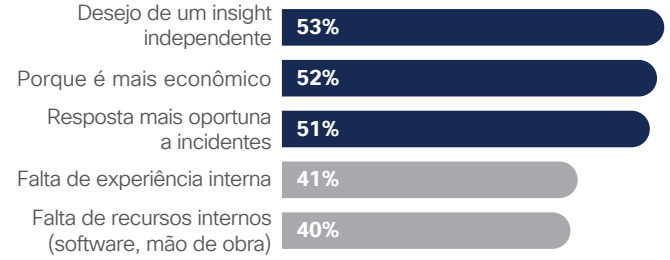
Chad Paalman, CEO da NuWave Technology Partners em Kalamazoo, Michigan, uma parceira da Cisco, acha que muitas empresas de pequeno e médio porte não sabem, exatamente, quanto (ou quão pouca) análise e monitoramento seus provedores de segurança terceirizados oferecem.

Figura 7 Executivos responsáveis pela segurança em empresas de médio porte



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Figura 8 As empresas de médio porte usam ajuda terceirizada para superar a falta de recursos internos



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

"Muitos líderes empresariais não são educados sobre suas redes. Eles presumem que se tiverem um firewall, então eles têm um cadeado na porta e ninguém pode entrar. Eles também pressupõem que se a segurança tiver sido terceirizada para um provedor de serviço gerenciado (MSP), monitoramento de log está acontecendo, ou o serviço inclui a detecção de intrusão."

Chad Paalman, CEO da NuWave Technology Partners

O resultado é, no entanto, que as empresas de pequeno/médio porte contam com seus parceiros terceirizados para fornecer:

- Serviços terceirizados de consultoria e aconselhamento (57%),
- Resposta a incidente (54%),
- Cinquenta e um por cento (51%) de monitoramento de segurança.

No entanto, elas têm menos probabilidade de terceirizar tarefas como inteligência de ameaças (39%). (Consulte a Figura 9).

A boa notícia é que as empresas de médio porte parecem estar separando alguns dos seus recursos limitados para compreender e responder a ameaças a coisas como aumento da inteligência de ameaças e resposta a incidente.

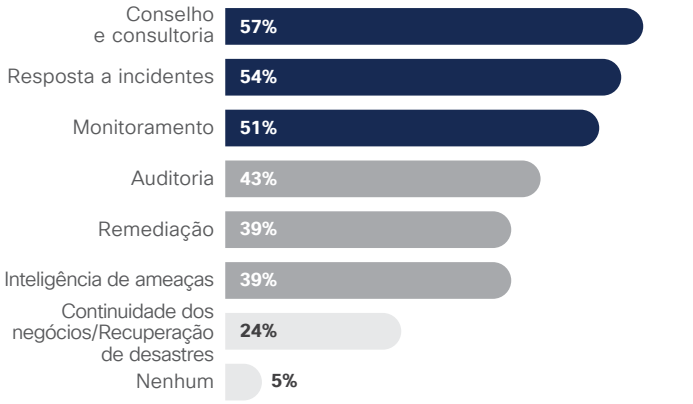
Processos: Check-ins regulares para o gerenciamento da segurança

Processos de segurança abrangentes e regulares, como controles para ativos de alto valor e análises de práticas de segurança, ajudam as empresas a identificar pontos fracos em suas defesas. Esses processos não são tão comuns em empresas de pequeno/médio porte como deveriam, talvez devido à falta de pessoal.

Por exemplo, de acordo com o estudo comparativo dos recursos de segurança de 2018 da Cisco, empresas de médio porte têm menos probabilidade do que organizações de grande porte em concordar em revisar práticas de segurança regularmente, que têm ferramentas para analisar os recursos de segurança e que rotineiramente investigam incidentes de segurança (Figura 10).

Uma observação positiva é que 91% das empresas de médio porte disseram realizar testes para avaliar seus planos de resposta a incidente pelo menos uma vez por ano. No entanto, como com sua dependência na nuvem e parceiros terceirizados, a pergunta é se esses planos de resposta a incidente são suficientes para evitar ataques cada vez mais sofisticados.

Figura 9 As empresas de médio porte terceirizam serviços de consultoria e aconselhamento, além de resposta a incidente



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Figura 10 As empresas de médio porte têm menos probabilidade de concordar totalmente com o uso de processos operacionais

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Conectando pessoas, processos e tecnologia: O desafio da orquestração

Se as empresas de pequeno/médio porte adicionarem mais fornecedores e produtos de segurança às suas defesas e transferirem recursos de TI para o gerenciamento desses produtos, suas empresas gerenciarão melhor a segurança? O oposto pode ser verdade, pelo menos em termos de compreensão e orquestração de alertas de segurança.

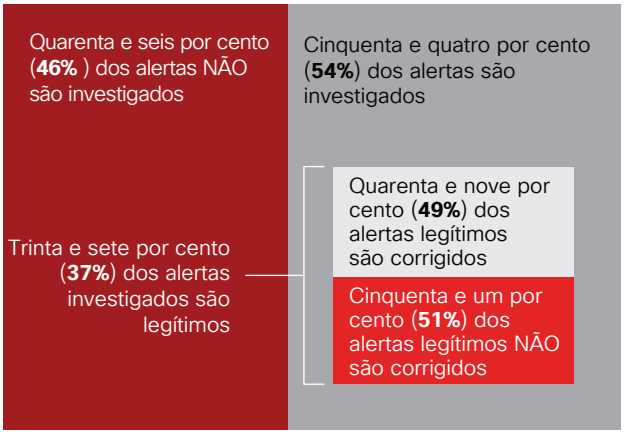
A maioria das empresas de pequeno/médio porte de hoje reconhecem que à medida que criam um ambiente de fornecedores e produtos mais complexos, suas responsabilidades aumentam. Por exemplo, 77% das empresas de médio porte descobriram ser um pouco desafiador ou muito desafiador orquestrar alertas dessas muitas soluções (Figura 11).

Quando as empresas tentam analisar esses alertas, os desafios combinados de pessoas, processos e tecnologia podem causar muitos alertas a serem investigados, como o estudo comparativo encontrado (Figura 12):

Figura 11 As empresas de médio porte têm menos probabilidade de concordar totalmente com o uso de processos operacionais

Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Figura 12 Porcentagem de alertas de segurança não investigados ou corrigidos



Fonte: Estudo comparativo de recursos de segurança da Cisco de 2018

Recomendações para o futuro

Tecnologia

À medida que as empresas consideram novas ferramentas, de forma ideal, elas podem evitar a adição de fornecedores e gerar ainda mais alertas.

Com isso em mente, são produtos desenvolvidos com mente aberta? Como eles se integração com outros em termos de compartilhamento de dados e inteligência de ameaças? Há integração de console de gerenciamento?

Se um fornecedor diz que os produtos foram projetados para atender e trabalhar com outros, isso acontece direto da fábrica ou o comprador terá que fazer um trabalho de API considerável?

Aprendizado de máquina, embora cercado por propaganda, tem seu lugar na segurança. No entanto, procure ver o aprendizado de máquina como uma camada de detecção dentro de produtos já implantados, com relação a um produto independente de outro fornecedor que adiciona outro produto para gerenciar.

Pessoas e processamento

Em poucas palavras, desenvolva, claramente, uma estratégia para melhorar a segurança cibernética. Apenas 38% das empresas de pequeno/médio porte têm uma estratégia de risco digital de ativos em vigor, de acordo com o Vistage Research Center, um centro de recursos para os líderes de empresas. [6]

Seu planejamento inclui o treinamento adequado dos usuários finais? As políticas de seguro cobrem a perda das empresas, decorrentes de um ataque digital? Que tal criar planos de continuidade dos negócios e de comunicação de crise para permitir recuperação mais rápida e ajudar a evitar danos à reputação?

Além disso, os líderes de TI devem explicar claramente o que a gerência das empresas realmente quer saber com relação a violações:

- Qual é o impacto para a empresa
- Quais medidas a equipe de segurança está tomando para conter e investigar a ameaça. Quanto tempo levará para retomar as operações normais. [7]

"Adotando um conjunto de plataformas e de ferramentas de segurança que trabalhem juntas, comparado a partes discrepantes que podem, na realidade, entrar em conflito entre si, você obtém uma maior eficácia da segurança, além de uma simplificação do gerenciamento."

Ben M. Johnson, CEO da Liberty Technology

"As empresas de pequeno/médio porte devem avaliar esses riscos e desenvolver os planos de resposta antes de uma violação, não depois."

Chad Paalman, NuWave Technology Partners

6 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. (Ameaças digitais e soluções para empresas de pequeno e médio porte) Desenvolvido em colaboração com a Cisco e o National Center for the Middle Market (Centro Nacional para o mercado de empresas de médio porte). Disponível em: https://www. vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Relatório semestral de segurança cibernética da Cisco 2017: https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ibid.

Conclusão

Uma recomendação final para as empresas de pequeno/médio porte promoverem melhorias na segurança cibernética é reconhecer que a mudança incremental é melhor que nenhuma alteração. Resumindo, elas não devem deixar um desejo de ser "perfeita" em sua abordagem de segurança atrapalhar o desejo de se tornar "melhor". Perfeito, como em todas as coisas, não existe.

Empresas de pequeno/médio porte também devem entender que não há nenhuma solução de tecnologia "bala de prata" para resolver todos os seus desafios de segurança cibernética. O cenário de ameaças é muito complexo e dinâmico. A superfície de ataque está sempre se expandindo e mudando. E, em resposta, estratégias e tecnologias de segurança devem também evoluir continuamente.

Para saber mais sobre a abordagem à segurança centrada em ameaças da Cisco, visite cisco.com/go/security.

Sede nas Américas
Cisco Systems, Inc.
San Jose, CA

Sede na Ásia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Singapura

Sede na Europa
Cisco Systems International BV Amsterdam,
Holanda

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefone e de fax estão disponíveis no site da Cisco, na página www.cisco.com/go/offices.

Publicado em julho de 2018