A base da segurança:

Qual é o nível necessário de segurança?

CISCO

Conteúdo

Introdução: a base da segurança

Quando as empresas instalam dezenas de produtos de segurança cibernética e, mesmo assim, ainda são violadas, surge a questão: *qual é o nível de segurança necessário?* De quantos produtos uma empresa precisa? Quais são necessários? Quanto deve ser gasto com este tipo de tecnologia? Em outras palavras, *onde está a base da segurança da informação?*

A segurança é algo com que as empresas podem gastar infinitamente tentando conter os invasores. Mas quanto elas ***precisam*** gastar e o que ***precisam*** fazer para permanecerem seguras?

Isso vai muito além do dinheiro. Talvez a empresa tenha um orçamento considerável para a segurança, mas não contratou os especialistas certos para colocar o projeto em prática. Ou talvez a empresa tenha um orçamento de segurança reduzido, mas investiu com sabedoria nas pessoas certas e na tecnologia adequada, e em seus ativos mais vulneráveis ou essenciais. Às vezes, grande parte da segurança de uma empresa é gerenciada por terceiros, que não têm como influenciar as mudanças ou as atualizações necessárias.

Portanto, sim, o orçamento é importante em se tratando de segurança cibernética. Mas não é tudo. Em que situação sua empresa se encontra em relação à segurança? Você conta com funcionários, processos e tecnologia especializados para defender proativamente sua empresa? Você está abaixo ou acima de um nível mínimo de proteção?

Neste relatório, vamos descrever os principais fatores para o sucesso da estratégia de segurança da informação de uma empresa, segundo uma pesquisa, de metodologia duplo cega, realizada com aproximadamente 80 profissionais de segurança da informação pela Cisco.

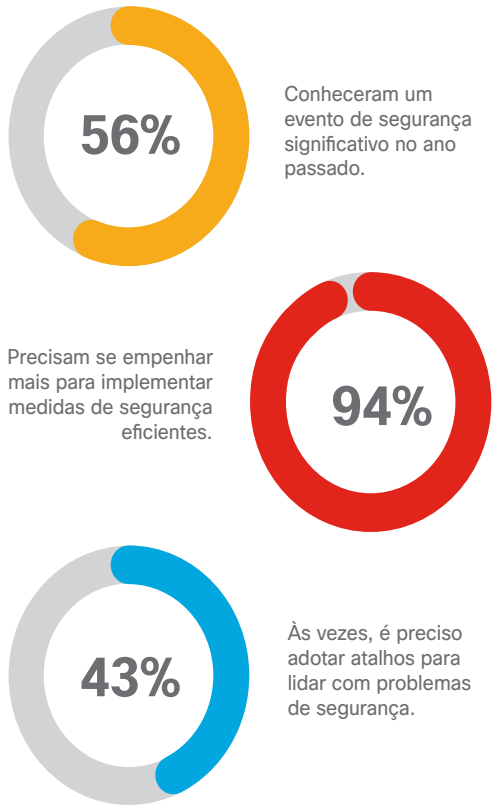
"Existem muitas dinâmicas para os desafios de segurança, além do dinheiro apenas."

Wendy Nather, diretora de CISOs de consultoria, Cisco

Os números não mentem

Foi revelador constatar em nossa pesquisa recente que 56% dos entrevistados (mais da metade) enfrentaram um evento de segurança cibernética considerável (violação, invasão, infecção por malware etc.) no ano passado. Cerca de 94% dos entrevistados disseram que precisam se empenhar mais para implementar medidas de segurança eficientes. E 43% admitem que, às vezes, precisam pegar atalhos para lidar com problemas de segurança, como limpar completamente um endpoint infectado em vez de remover o malware com precisão. (Consulte a Figura 1).

Figura 1 Como as empresas atuais estão fazendo com a segurança?
Porcentagem de entrevistados, N=79



Fonte: pesquisa sobre a base da segurança da Cisco de 2019

Mas nem tudo é má notícia. Cerca de 95% dos entrevistados disseram que podem identificar com eficiência quais dados e sistemas da empresa exigem os mais altos níveis de proteção, o que é um bom começo. Então, por que eles ainda estão com dificuldades? É por causa de dinheiro? Ou há outros fatores em jogo?

A diretora de CISOs de consultoria da Cisco, Wendy Nather, destaca os quatro fatores que podem afetar a segurança:

- Orçamento
- Conhecimento
- Recursos
- Influência

Nather inventou o famoso termo "linha de pobreza da segurança" há vários anos para iniciar essa discussão. Ela também escreveu dois relatórios sobre o tema quando atuou como diretora de pesquisa na **451 Research**: "A vida abaixo da linha de pobreza da segurança" em 2011 e "O verdadeiro custo da segurança" em 2013.

"Com base na minha experiência anterior como CISO nos setores público e privado, sei que há muitas empresas com dificuldades no assunto de segurança cibernética", diz Nather.
"Existem muitas dinâmicas para estes desafios, que vão além do dinheiro da questão financeira., Isto significa que uma empresa que gaste milhões pode ter problemas de segurança, enquanto uma empresa com um orçamento menor pode ter defesas suficientes de acordo com suas necessidades específicas."

Fatores que determinam o sucesso da segurança

Orçamento à parte, há outros fatores que podem afetar a base da segurança. Além do orçamento, também há conhecimento, recursos e influência.

Orçamento

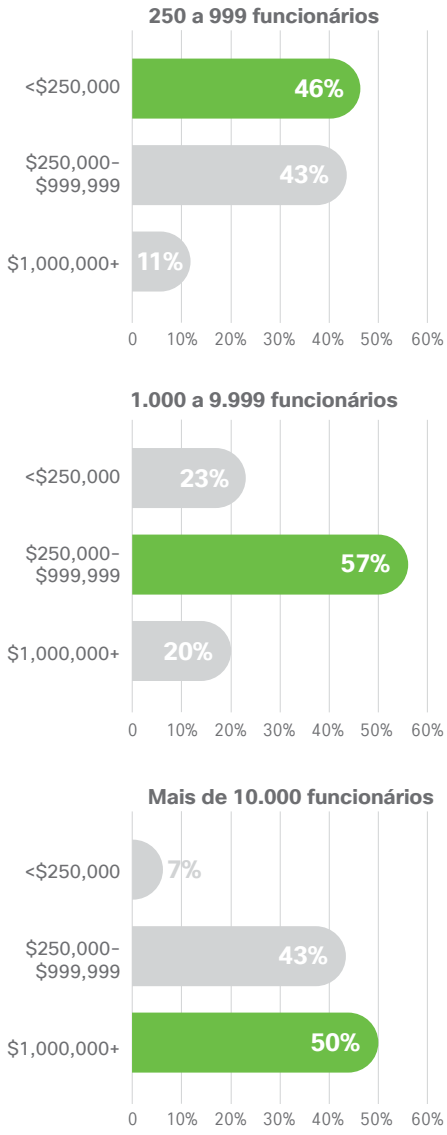
Quanto as empresas estão gastando com segurança?

Não existe um número mágico quando se trata de gastos com segurança. O montante que determinada empresa deve gastar com segurança depende de vários fatores, como: porte, setor, risco e postura e assim por diante. No entanto, dividimos os gastos anuais com segurança dos entrevistados da pesquisa (com base no porte da empresa) para servir como referência aproximada para outras empresas. Como ilustra a Figura 2:

- Entre as **empresas de médio porte (250 a 999 funcionários)**, 46% estão gastando menos de US$ 250.000 em segurança por ano e 43% estão gastando entre US$ 250.000 e US$ 999.999. (Apenas 11% estão gastando US$ 1 milhão por ano.)
- A maioria (57%) das **empresas (1.000 a 9.999 funcionários)** está gastando entre US$ 250.000 e US$ 999.999 em segurança por ano. (Apenas 20% estão gastando US$ 1 milhão por ano, enquanto 23% estão gastando menos de US$ 250.000.)
- Cerca de 50% das **grandes empresas (com mais de 10.000 funcionários)** estão gastando US$ 1 milhão ou mais em segurança por ano, sendo que 43% gastam entre US$ 250.000 e US$ 999.999 e apenas 7% gastam menos de US$ 250.000.

Embora esses números forneçam algumas informações básicas sobre a proporção entre o porte da empresa e as despesas com segurança, é importante observar que o porte não é o único aspecto a ser considerado em se tratando de gastos com segurança. O número de funcionários não está correlacionado necessariamente com o montante da receita ou do financiamento disponível, ou até mesmo com o risco que a empresa enfrenta. Por exemplo, um fundo de cobertura pode estar gerenciando bilhões de dólares com uma pequena equipe, enquanto uma grande agência estatal com muitos funcionários pode ter um orçamento limitado e flutuante.

Figura 2 Quanto a empresa gasta por ano com segurança?



Fonte: pesquisa sobre a base da segurança da Cisco de 2019

Outro critério bastante usado para aferir os gastos com segurança é analisar uma porcentagem do orçamento de TI. No entanto, as porcentagens não ajudam quando os números envolvidos são muito grandes ou muito pequenos. Se puder gastar 10% de um orçamento de TI de bilhões de dólares em segurança, um banco pode comprar muito mais do que uma startup que representa 10% de um orçamento de TI de US$ 50.000 para gastar em segurança. Quando as empresas estão definindo os níveis de gastos em segurança, é melhor determinar os recursos de segurança específicos necessários, em vez de simplesmente escolher uma porcentagem do orçamento de TI aleatoriamente.

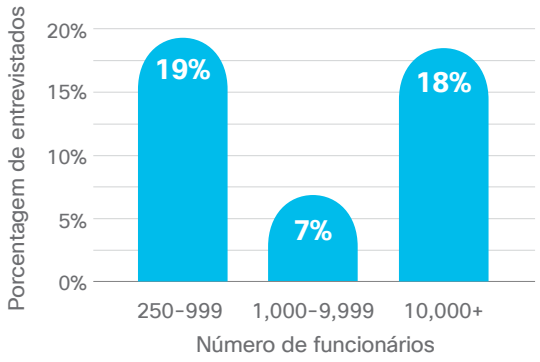
As empresas podem arcar com a segurança necessária?

Surpreendentemente, 84% dos entrevistados da pesquisa disseram que podem pagar uma parte, mas não toda a segurança *mínima* necessária para defender a infraestrutura. Curiosamente, descobrimos que as empresas com 1.000 a 9.999 funcionários têm mais dificuldades de assumir as despesas com a segurança, sendo que apenas 7% dessas empresas afirmam que podem arcar com a segurança mínima necessária. (Consulte a Figura 3).

Em comparação, 19% das empresas menores (250 a 999 funcionários) e 18% das empresas maiores (mais de 10.000 funcionários) disseram que podem arcar com toda a segurança *mínima* necessária. Parece que os orçamentos de segurança nem sempre acompanham proporcionalmente a expansão das empresas (até que um grande número de funcionários seja atingido).

"A questão é por que as empresas menores não se classificam como incapazes de arcar com a segurança mínima necessária", diz Nather. "É porque elas acham que não representam um alvo e, portanto, não precisam de tanta segurança? O risco de segurança aumenta em relação a outros fatores de crescimento de uma empresa? Ou uma empresa entra no radar dos invasores após atingir determinado perfil, apenas quando percebe que não cumpriu um determinado requisito de segurança?"

Figura 3 Minha empresa pode proporcionar toda a segurança mínima necessária.
Porcentagem de entrevistados que concordam



Fonte: pesquisa sobre a base da segurança da Cisco de 2019

Um orçamento maior aumenta a confiança e os recurso de segurança?

Cerca de 27% das empresas que gastam US$ 1 milhão ou mais em segurança por ano disseram que podem arcar com toda a segurança mínima necessária, em relação a apenas 9% das que gastam entre US$ 250.000 e US$ 999.999. Parece lógico que o aumento dos gastos faz alguma diferença nos recursos de segurança.

No entanto, as empresas de todos os portes ainda acham que precisam se empenhar mais para implementar uma estratégia de segurança eficiente. Cerca de 94% das empresas que gastam US$ 1 milhão ou mais por ano disseram que precisam se empenhar mais, assim como 95% das que gastam entre US$ 250.000 e US$ 999.999 e 92% das que gastam menos de US$ 250.000.

Por isso, embora seja uma grande ajuda, o orçamento não é tudo quando se trata de segurança. Quais são os outros fatores que entram em jogo?

Entre as empresas com 1.000 a 9.999 funcionários, apenas 23% disseram que dependem mais da equipe interna para obter conhecimentos de segurança. Mais uma vez, os números mostram que as empresas desse porte específico têm mais dificuldades quando se trata de arcar com os recursos de segurança necessários.

Conhecimento

As empresas têm a equipe e as qualificações adequadas para proteger os ambientes com eficiência?

Ao perguntar em quem *mais* confiam quanto ao conhecimento de segurança, apenas 37% disseram que confiam na equipe interna. Quase a mesma quantidade de entrevistados (28%) disseram que confiam mais nas redes profissionais. Esses números representam a escassez generalizada de habilidades em segurança cibernética. De acordo com a **pesquisa realizada pela (ISC)²**, temos uma escassez de quase 3 milhões de profissionais de segurança cibernética em todo o mundo.

Embora seja bom poder recorrer a recursos externos para obter conhecimentos de segurança, as empresas também devem contar com o valioso conhecimento da equipe de segurança interna, que engloba conhecimento sobre a experiência do usuário e o design do processo, a análise de risco e a resposta a incidentes.

"Há muitas chamadas de risco de segurança que precisam ser feitas e muito trabalho de resposta a incidentes que só pode ser feito se você tiver conhecimento institucional da empresa", disse Nather. "Por isso, mesmo contando com o auxílio de unidades externas de resposta a incidentes, você ainda precisa contar com profissionais internos que sabem o que está acontecendo na rede."

Também descobrimos que 34% dos entrevistados estão aprendendo com a mídia sobre as vulnerabilidades e os incidentes de segurança que afetam a empresa. Esse número destaca a necessidade de jornalistas confiáveis e blogueiros especializados para preencher a lacuna de conscientização situacional da segurança cibernética para muitas empresas.

Recursos

Quais outros fatores impedem as empresas de ter uma estratégia de segurança sólida?

Mesmo que a empresa tenha o conhecimento necessário para saber o que incluir no programa de segurança, não significa necessariamente que ela tenha os recursos para executá-lo. Por exemplo, a sabedoria convencional afirma que a segmentação de rede é um controle de segurança cibernética importante, mas pode ser muito difícil e caro proteger uma rede antiga e complexa administrada por vários provedores com os recursos disponíveis.

Além disso, as equipes de segurança nem sempre podem impor seus requisitos em empresas ou grupos externos. Por exemplo, quando um fabricante precisa atender a dezenas de normas e regulamentos operacionais específicos do país, pode levar anos para liberar e distribuir uma atualização de software para os sistemas de controle.

Os recursos são fatores importantes na base. Às vezes, também conhecidos como "maturidade de segurança", os recursos dependem das funcionalidades básicas necessárias da empresa antes de avançar em projetos mais sofisticados. Isso inclui (consulte a Figura 4):

Figura 4 Pirâmide de maturidade da segurança

1. **Saber o que você tem e o que está fazendo.** A manutenção de um inventário de recursos atualizado não é tão fácil quanto parece no ambiente dinâmico de hoje em dia. Muitos ecossistemas de aplicações são tão complexos que ninguém sabe quais dados estão sendo compartilhados, para quais fins e por meios de quais interfaces. As auditorias de usuários geralmente descobrem contas essenciais, mas que não são documentadas.
2. **Ser capaz de iniciar (e evitar) mudanças nos recursos.** Caso não tenha o controle de um recurso, você precisa fazer com que o proprietário o altere rapidamente para corrigir uma vulnerabilidade. Da mesma forma, você precisa ter certeza de que as mudanças só aconteçam quando são aprovadas e que também levem em conta as dependências tecnológicas.
3. **Entender os riscos de segurança.** Quais são os recursos mais importantes e quanto eles valem para os criminosos? Você deve saber quais tipos de ameaças têm mais probabilidade de visar a os recursos, como reconhecê-las e bloqueá-las. Caso contrário, você pode gastar tempo e dinheiro em recursos não importantes e ignorar os valiosos.
4. **Ser capaz de instalar e operar a tecnologia de segurança.** Depois de dominar os três primeiros recursos, você será capaz de usar os produtos e serviços com eficiência.

Quais tecnologias são usadas com mais frequência nos programas de segurança?

Essas são as 15 melhores tecnologias de segurança que estão sendo usadas pelos entrevistados da pesquisa:

1. **Gerenciamento de firewalls/políticas de segurança**
2. **Segurança de e-mail**
3. **Proteção contra malware de rede**
4. **Ameaças à nuvem e detecção/proteção da carga de trabalho**
5. **Prevenção contra perda de dados**
6. **Criptografia**
7. **VPN**
8. **Internet segura/gateway da Web**
9. **Segurança das informações e gerenciamento de eventos (SIEM)**
10. **Controle de acesso de rede**
11. **Agente do Cloud Access Security**
12. **Segurança de endpoint/EDR**
13. **Firewall para aplicativos na Web**
14. **Detecção de ameaças à rede/Análise de tráfego na rede**
15. **Plataformas de inteligência de ameaças**

"Quanto mais produtos você tiver, mais trabalho terá para conectar todas essas informações. Ao pensar em segurança, você precisa adotar uma abordagem holística e não apenas uma estratégia de pilar a pilar... Com a automação integrada, você pode começar a agir sem ter que expandir muito a equipe."

Marisa Chancellor, diretora sênior, segurança da informação, Cisco

As 15 principais tecnologias listadas acima compõem um portfólio substancial e exigem um grande número de pessoas com bastante conhecimento para configurar, manter e monitorar tudo. A implicação é que o custo do pessoal da base de segurança é maior do que muitas empresas imaginam quando estão tentando planejar os itens necessários.

"Na minha função anterior como analista do setor, eu perguntava aos profissionais de segurança quais tecnologias eles achavam que CISOs precisavam comprar para proteger adequadamente as empresas", disse Nather. "As respostas que obtive foram muito genéricas, indicando que não há um projeto padrão. Alguns indicaram apenas quatro tecnologias, enquanto outros citavam mais de 31 ferramentas diferentes."

"Muitos entrevistados dessa pesquisa simplesmente disseram que o que é necessário para uma empresa depende de vários fatores, incluindo o tipo de dados que ela tem, em qual setor ela atua, se ela está dispersa geograficamente e assim por diante", continuou Nather. "Se não conseguimos criar uma resposta única para o CISO (e o mais próximo disso que temos é um padrão de conformidade para um caso de risco bem definido, como o PCI-DSS), não podemos esperar que toda empresa saiba com confiança o que realmente precisa. Se ela não souber do que precisa, também não saberá se pode arcar com a segurança."

Embora algumas tecnologias, como firewalls e segurança de endpoint, sejam escolhidas com frequência, as demais realmente dependem da situação específica da empresa, o que pode exigir uma ampla pesquisa e uma auditoria de segurança digital para determinar o que cabe no orçamento e é realmente necessário.

Kelley Misata, PhD, é fundadora e CEO da Sightline Security. A Sightline é uma nova empresa de segurança digital e 501(c)(3) sem fins lucrativos que firmou uma parceria com outras organizações sem fins lucrativos para avaliar, priorizar e melhorar a segurança.

Segurança cibernética para organizações sem fins lucrativos

Por que uma empresa como a Sightline é necessária hoje em dia?

Misata: Por vários motivos, mas aqui estão os três principais. Primeiro, as organizações sem fins lucrativos ainda não sabem do que precisam. Estão navegando pela segurança digital sem um mapa. Com todas as dificuldades da segurança, fica muito difícil, principalmente quando tempo, equipe e orçamento são limitados. E justamente quando você está concentrado 200% em sua missão de ajudar os outros!

Segundo, as soluções de segurança comercial não foram criadas para organizações sem fins lucrativos. Sim, as organizações sem fins lucrativos têm funções comerciais semelhantes, mas também têm nuances que diferenciam a maneira como gerenciam a segurança.

Terceiro, as organizações sem fins lucrativos não têm um conhecimento mais aprofundado sobre segurança. Na verdade, as pessoas que não são do setor de segurança não entendem o que estamos falando porque os profissionais de segurança às vezes não são muito claros. As organizações sem fins lucrativos participam de conferências de segurança e acham que não conseguem reconciliar o que está sendo dito ou alinhar as soluções oferecidas aos negócios. A missão da Sightline é ser a ponte, o tradutor e o defensor dessas organizações. Estamos construindo ferramentas de avaliação e uma comunidade de segurança unicamente para organizações sem fins lucrativos.

Influência

As empresas podem influenciar fornecedores, parceiros e terceiros para fornecer a segurança de que precisam?

Atualmente, a segurança da cadeia de suprimentos de terceiros é uma das principais preocupações dos CISOs. Com serviços, hardware e software provenientes de dezenas ou centenas de fontes diferentes, as empresas não conseguem controlar totalmente a segurança.

Não é surpresa que quanto mais funcionários e orçamento as empresas tiverem, maior a probabilidade de influenciarem fornecedores e parceiros para ajudá-las com a segurança. Por exemplo, 86% das empresas com mais de 10.000 funcionários estão aprendendo sobre as vulnerabilidades e os incidentes de segurança com os fornecedores/parceiros afetados antes que os casos se tornem públicos, em relação a apenas 60% das empresas com menos de 1.000 funcionários.

E 38% das empresas que gastam US$ 1 milhão ou mais em segurança por ano disseram que sempre puderam adicionar termos e condições relacionados à segurança a um contrato de fornecedor/parceiro, em relação a apenas 17% das empresas que gastam menos do que US$ 250.000 em segurança por ano. Isso indica que as empresas maiores com mais poder aquisitivo estão mais bem posicionadas para negociar com as partes externas.

Como ficam as empresas menores, que podem ser ainda mais dependentes de parceiros externos? "A melhor opção pode ser unir-se aos colegas para exercer mais influência sobre provedores e fornecedores compartilhados", diz Nather. "Por exemplo, as associações do setor, os fóruns de segurança digital regionais ou o compartilhamento de informações e os centros de análise (ISACs) permitem que os membros organizem solicitações e respostas a problemas de segurança. Encontrar ou criar essa influência faz parte do trabalho do CISO hoje, o que torna a rede ainda mais importante".

(Segurança cibernética para organizações sem fins lucrativos, continuação)

Quais são alguns dos desafios de segurança específicos que as organizações sem fins lucrativos enfrentam?

Misata: Em primeiro lugar, as organizações sem fins lucrativos são muito simples, o que significa que elas não têm tempo ou dinheiro para desperdiçar em nada que não esteja diretamente relacionado à sua missão. Para muitas organizações sem fins lucrativos, a segurança cibernética é vista como cara, complexa e desnecessária até que algo ruim aconteça.

Em segundo lugar, muitas organizações sem fins lucrativos não identificaram quais dos seus recursos podem ser atraentes para os invasores. Então, como elas podem saber o que proteger? Hoje, muitas organizações sem fins lucrativos são levadas a gastar dinheiro em soluções antes de entender o que precisam.

Em terceiro lugar, um dos maiores desafios para as organizações sem fins lucrativos é que ninguém na empresa se concentra diretamente na segurança. Embora estejam muito energizados e saibam que a segurança (principalmente a segurança digital) é importante, a atenção é direcionada em várias direções.

A grande notícia é que, apesar de tudo isso, as organizações sem fins lucrativos estão avançando e não se consideram mais imunes a um ataque; elas reconhecem que têm recursos e dados de valor. Porém, muitas vezes, elas têm influência mínima sobre fornecedores e provedores de serviços; estão muito atrás da curva. Por meio do nosso trabalho com os membros da Sightline, podemos coletar dados e ideias sobre o estado de segurança das organizações sem fins lucrativos, para que possamos começar a trazê-las para o mundo.

Pontos principais

Em geral, as empresas não acham que podem arcar com a segurança necessária, independentemente do tamanho ou do quanto estão gastando atualmente.

Empresas intermediárias com 1.000 a 9.999 funcionários têm mais dificuldade para proteger os ambientes de forma adequada.

Não há resposta única quando se trata de quais produtos de segurança uma empresa deve usar ou quanto deve ser gasto com segurança. Depende muito do tamanho e do tipo de empresa, da importância de seus recursos e do que ela realmente pode pagar. Isso torna mais difícil para as empresas descobrirem o que os programas de segurança devem incluir.

O aumento dos gastos nem sempre se traduz em mais recursos/maior confiança de segurança. Outros fatores devem ser considerados, como o conhecimento e a influência.

As empresas devem ter certeza de que a equipe interna continua desenvolvendo conhecimento em segurança geral e no perfil específico de ambiente e risco. Há alguns aspectos da segurança que podem ser abordados apenas por especialistas internos.

Os recursos desempenham um papel importante na base da segurança. Fatores como a possibilidade de uma equipe de segurança ter controle sobre determinados recursos podem afetar muito a capacidade de executar uma estratégia de defesa, mesmo com o orçamento e o conhecimento necessários à disposição.

Quanto maior for a empresa, mais fácil será influenciar terceiros que afetam a postura de segurança. Talvez as empresas menores precisem aproveitar o poder das associações para obter a mesma influência e economia de escala.

Recomendações para aumentar a segurança

Independentemente de onde a empresa se enquadra em relação à base da segurança, estas são algumas recomendações para resolver os principais desafios abordados nesse relatório.

1. Descubra o que é certo para sua empresa

As empresas devem analisar detalhadamente para onde estão indo os gastos com segurança. Nesse setor, há muita pressão para acompanhar os colegas. *"O que todos os outros estão comprando? Preciso dessa nova tecnologia?"* Claro que é sempre bom ficar de olho no setor e avaliar o que os outros estão fazendo para aumentar as defesas. No entanto, como confirmamos nesse relatório, a segurança nunca é igual para todos.

Antes de comprar mais tecnologia, analise o conhecimento em relação à pirâmide de maturidade da segurança em nossa seção de recursos. Como diz o velho ditado, "você não pode proteger o que não sabe que tem." Um scanner de vulnerabilidade não será útil se você não conseguir corrigir o que ele encontrar.

Saber quais ameaças não são apenas possíveis, mas *prováveis*, vai ajudar você a se concentrar nas prioridades certas quando não for possível proteger tudo. Considere fazer uma **avaliação de risco cibernética** interna ou por meio de terceiros para começar com o pé direito.

2. Aproveite melhor os investimentos

Uma tendência desastrosa é sempre buscar os produtos de segurança mais recentes e maiores. Isso é bom em teoria para ter certeza de que você está protegido contra ameaças em constante evolução. No entanto, para muitas empresas, criou-se uma confusão de produtos desarticulados que são difíceis de gerenciar, se não impossíveis. Se você estiver recebendo muitos alertas de tecnologias diferentes e tiver que passar o dia todo indo e voltando entre diferentes aplicações para descobrir o que está acontecendo no ambiente, a segurança será comprometida.

Em vez disso, é hora de investir em tecnologias de segurança que trabalham para você, e não o contrário. A Cisco adota uma **abordagem de plataforma para a segurança**, o que significa que não vendemos apenas firewalls, segurança de e-mail ou tecnologia antimalware. Oferecemos um portfólio aberto e amplo de tecnologias de segurança que trabalham em conjunto para proteger a rede. Se uma ameaça for encontrada em uma área, podemos bloqueá-la automaticamente em qualquer outro lugar. A automação e a integração podem percorrer um longo caminho para minimizar a complexidade e garantir que você aproveite ao máximo as tecnologias de segurança e os funcionários.

"Vejo a segurança como um ecossistema. Quanto mais as coisas funcionarem juntas, melhor. Se eu tiver que gastar tempo e energia integrando as tecnologias por conta própria, terei menos tempo para gastar realmente com a segurança."

Steve Martino, vice-presidente sênior/ CISO, Cisco

Em se tratando de fornecedores, não se esqueça de aproveitar tudo o que eles oferecem, muitas vezes a um baixo custo ou de graça. Participe dos webinars gratuitos. Ligue para o suporte técnico. Participe dos eventos do fornecedor. Participe dos grupos de consultoria do cliente. Participe dos treinamentos do fornecedor. Definitivamente, se você investiu em tecnologia, a equipe de segurança deve saber como usá-la de forma eficiente.

3. Adote uma abordagem de segurança de Zero Trust

As ameaças estão atingindo sua empresa por todos os lados. Elas têm como alvo usuários, aplicativos, a rede, a nuvem, dispositivos de IoT, etc. Essa superfície de ataque expandida torna essencial que as empresas sigam uma **abordagem de segurança de tolerância zero**.

Zero Trust exige que as empresas:

- Obtenham visibilidade em todas as áreas da rede
- Adotem controles para garantir que apenas as pessoas, os dispositivos e as aplicações certas possam operar no ambiente da empresa
- Tenham um meio eficaz de bloquear comportamentos suspeitos para evitar a propagação de ataques

Com essas etapas, as empresas podem proteger com mais eficiência os funcionários, a carga e o local de trabalho.

Ao ir além das medidas de segurança básicas e adotar uma abordagem de segurança mais abrangente e holística, você pode tornar mais difícil e mais caro para os invasores comprometerem os recursos, o que certamente ajuda na segurança!

4. Intensifique o treinamento

Como muitos de nossos entrevistados contam com fontes externas para obter conhecimento em segurança, mais treinamento é necessário. Após contratar talentos, você deve continuar investindo nas habilidades deles e na compreensão do ambiente.

Permita que eles participem de conferências e workshops. Promova sessões de treinamento interno. Incentive-os a acessar recursos gratuitos, como o **Cisco Security Blog** e a **página da inteligência de ameaças do Cisco Talos**, para se manterem atualizados sobre as ameaças mais recentes. Incentive que eles conquistem mais certificações. Em suma, assegure que eles não estejam simplesmente fazendo o trabalho deles, mas se tornando verdadeiros especialistas nas demandas de segurança cibernética da sua empresa, e não apenas especialistas em segurança, mas também especialistas na empresa. Terceiros nunca entenderão as necessidades e restrições de segurança específicas tão bem quanto seus próprios funcionários.

5. Considere a terceirização

Se você estiver administrando vários sistemas antigos, é provável que a equipe de TI esteja gastando muito tempo com gerenciamento e atualização, além de receber uma segurança ineficiente em troca. Migrar de sistemas antigos complexos para aplicativos SaaS terceirizados para funções comerciais bem conhecidas e não essenciais, como e-mail, aplicativos de escritório, folha de pagamento e outros, pode ajudar muito na segurança nessas áreas para que você possa se concentrar na proteção dos principais processos e ativos.

Para os produtos de segurança que exigem uma equipe mais dedicada do que você tem disponível (devido ao custo), a terceirização do gerenciamento dessas tecnologias por meio de um MSSP também é uma opção. Perceba que às vezes é melhor, e mais econômico, obter ajuda do que tentar fazer tudo sozinho.

6. Una forças

Como indicado em nossa seção sobre influência, certamente os números não mentem em se tratando de segurança. Se a empresa for muito pequena para exercer influência sobre os fornecedores, considere se unir a outras empresas por meio de redes profissionais ou grupos do setor. Corrigir bugs em tempo hábil e obter atualizações de fornecedores e parceiros é fundamental para ter uma segurança eficiente. E é mais difícil para eles dizer não a 50 pequenas empresas do que apenas uma.

Acesse cisco.com/br/security para descobrir como podemos ajudar a proteger SEU ambiente.

Metodologia

Os dados desse relatório são baseados em um estudo duplo-cego online com aproximadamente 80 tomadores de decisão de TI localizados nos EUA, que responderam a perguntas sobre orçamento e planejamento. Os entrevistados são funcionários em tempo integral de empresas de pequeno porte (250-999 funcionários), médio porte (1000-9999 funcionários) e grande porte (mais de 10.000 funcionários), que trabalham para uma organização com fins lucrativos, governo ou instituição de ensino superior com um departamento de TI formal. Eles conhecem bem os procedimentos e as políticas, participam da criação da estratégia de segurança e gastam pelo menos 40% do tempo com a segurança.

O Cisco Cybersecurity Series

Ao longo da última década, a Cisco publicou uma série de informações sobre inteligência de ameaças para profissionais de segurança interessados no status global da segurança digital. Estes relatórios abrangentes têm fornecido detalhes dos cenários de ameaças e as implicações para as empresas, bem como as melhores práticas para se defenderem contra os impactos das violações de dados.

Na nova abordagem da nossa liderança de pensamento, a Cisco Security está publicando vários artigos baseados em pesquisas e orientados por dados sob o banner Cisco Cybersecurity Series. Ampliamos o número de títulos para incluir relatórios diferentes para profissionais de segurança com interesses diferentes. Apelando para a profundidade e amplitude da experiência de pesquisadores de ameaças e inovadores no setor de segurança, a coleção anterior de relatórios da série 2019 inclui o Relatório de Privacidade de Dados, o Relatório de Ameaças, o Relatório de Referência do CISO, o Relatório de Segurança de e-mail, Threat Hunting e outros ainda virão ao longo do ano.

Para obter mais informações e todos os relatórios e cópias arquivadas, acesse www.cisco.com/br/securityreports.

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

Sede - região da Ásia Pacífico
Cisco Systems (USA), Pte. Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdã,
Holanda

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

Publicado em outubro de 2019

BTTM_01_1019