Respondendo a — e recuperando-se de — ataques de segurança sofisticados

As quatro coisas que você pode fazer para ajudar a manter sua organização segura

IBM

Índice

Introdução

Como tantas outras coisas no mundo de hoje, os ataques cibernéticos — assim como aqueles que os cometem — estão se tornando mais sofisticados a cada ano. Ao mesmo tempo, os recursos de TI estão movendo-se além do firewall e as empresas estão distribuindo seus aplicativos e dados em diversos dispositivos. Agora está claro que simplesmente proteger o perímetro de uma organização não é suficiente. Esses ataques sofisticados — que incluem ameaças persistentes avançadas, as APTs — estão ignorando as defesas tradicionais.

Sabemos muito bem como os principais incidentes de segurança podem afetar dados, redes e a brand corporativa da empresa. Sabemos também que ataques sofisticados, desenvolvidos para ter acesso contínuo a informações críticas ou causar danos em infraestruturas críticas, estão se tornando mais graves, mais frequentes e mais onerosos.

Qual a gravidade? Os ataques sofisticados podem incluir:

- Roubo de propriedade intelectual
- Confisco de contas bancárias e outros ativos financeiros
- Distribuição de malware em computadores individuais e através de sistemas
- Exposição de informações comerciais confidenciais e/ou de clientes online
- Danos às infraestruturas críticas

Qual a frequência? Um estudo realizado com 2.618 líderes empresariais e profissionais de segurança em 2012 nos Estados Unidos, Reino Unido, Alemanha, Hong Kong e Brasil constatou que eles experimentaram uma média de 66 ataques por semana, sendo os números mais altos informados por organizações na Alemanha e nos EUA: 82 e 79 por semana, respectivamente. Em seus relatórios de meados de 2012, equipes de desenvolvimento e pesquisa da IBM X - Force observaram uma tendência crescente nas vulnerabilidades gerais, prevendo um possível índice mais alto até o final do ano.[2]

Qual o custo? O custo médio de recuperação de um simples ataque cibernético foi estimado em quase US$300.000 pelas organizações acima mencionadas no estudo de 2012.[3] Esse custo podia atingir quase 1 bilhão de dólares ao longo de um ano.

Além do mais, sabemos que as pessoas por trás destes ataques sofisticados são pacientes e fazem planos em longo prazo. Elas reconhecem e apontam vulnerabilidades específicas, estão mudando seu foco da exploração para a destruição.

Neste documento, iremos discutir as quatro etapas proativas que você pode — e deve — realizar agora para ajudar a manter sua organização segura:

- **Priorizar** seus objetivos de negócios e definir sua tolerância de risco
- **Proteger** sua organização com um plano de segurança proativo
- **Preparar** sua resposta ao inevitável: um ataque sofisticado
- **Promover** e apoiar uma cultura de conscientização de segurança.

Etapa 1: Priorizar seus objetivos de negócio e definir sua tolerância de risco

A experiência ao longo dos últimos anos deixou claro que "segurança" é um termo relativo. Não importa o quanto desejamos criar uma empresa completa e permanentemente segura e o que se deve fazer, a realidade é outra. Ainda assim, a crescente ameaça de ataques sofisticados exige que levemos a sério a segurança de nossas informações e a proteção de nosso pessoal e infraestrutura. Para isto, começamos com o estabelecimento de prioridades.

Determinar o que é mais importante para a segurança de seu negócio e por quê

Isso parece óbvio. Mas, pensar sobre seus objetivos de negócios e discutir o que é mais importante – e os riscos que você está disposto a tolerar – ajudará a estabelecer uma base sólida para uma estratégia de segurança que atenda às necessidades exclusivas de toda sua organização. Uma vez estabelecida uma base de referência, você terá dado um grande passo na direção certa.

Identificar as áreas mais vulneráveis ao ataque

Assim como há algumas coisas que são mais importantes que outras para a segurança do seu negócio, existem também algumas áreas que são mais vulneráveis do que outras. Nossa intenção não é apontar culpados. Em vez disso, é uma oportunidade de ver as coisas como elas são — assim você pode criar um ambiente mais seguro no geral.

Identificar os tipos específicos de ataques que representa a maior ameaça

Os ataques sofisticados são desenvolvidos para causar o máximo de destruição possível — geralmente resultando em perda ou uso indevido de dados críticos e/ou interrupção de infraestrutura crítica. Por esse motivo, é preciso olhar para as informações de sua empresa e sistemas críticos de negócios a partir do ponto de vista do invasor. E então pergunte a si mesmo como um invasor poderia causar mais danos.

Identificar as áreas que incorreriam na maior perda em caso de ataque

É aqui que nos defrontamos com nosso maior pesadelo. Ao desenvolver um plano de sucesso, há a necessidade de prever quanta devastação ocorreria no caso de um ataque na área mais vulnerável de sua empresa.

É preciso olhar para as informações de sua empresa e sistemas críticos de negócios a partir do ponto de vista do invasor.

Jogos online / sites de entretenimento hackeados, 100 milhões de registros de clientes comprometidos

Custos estimados: US$ 3,6 bilhões

Vítima: Comunidade de jogos online e sites de entretenimento

O que aconteceu: Uma "intrusão externa" a uma rede de jogos resultou no comprometimento das contas de 70 milhões de clientes, colocando dados pessoais e de cartão de crédito em risco. A empresa foi forçada a "desativar" os serviços online durante a investigação, gerando reação pública e imprensa negativa generalizada. Uma segunda invasão na divisão de entretenimento comprometeu dados adicionais do cliente.

Por que aconteceu: Os invasores supostamente foram capazes de invadir a segurança da rede e obter acesso a contas não codificadas e dados de usuários, e possivelmente alguns dados de cartão de crédito.

Dano causado: Além do sentimento público negativo generalizado, a empresa supostamente enfrentou custos superiores a US$171 milhões em perdas comerciais e despesa de resposta. A capitalização de mercado relatada da empresa caiu em aproximadamente US$ 3,6 bilhões, enquanto o preço das ações caiu 12 por cento.

Lições aprendidas: Foi relatado que uma das vulnerabilidades exploradas era conhecida pela empresa. Empresas devem utilizar uma estrutura para gerenciar o risco associado a ativos de informações, bem como estabelecer mecanismos fortes de governo para oferecer suporte a essa estrutura.

Apenas para efeitos ilustrativos. Os fatos reais e danos associados a esses cenários podem ser diferentes dos exemplos fornecidos. *São estimados, com base em informações financeiras publicamente disponíveis, assim como em artigos publicados.*

Etapa 2: Proteger sua organização com um plano de segurança proativo

Agora que você estabeleceu suas prioridades, é o momento de fazer seus planos, obter a tecnologia certa no lugar e colocar tudo em prática. É neste momento que você toma medidas para garantir que sua empresa está ciente das ameaças potenciais e trabalhando de forma proativa a fim de se defender contra elas — de forma contínua.

Criar uma abordagem proativa e informada à segurança de TI

Desenvolva uma estratégia de segurança com políticas e tecnologias destinadas a proteger proativamente os ativos e informações que você identificou como prioridades na Etapa 1. Preparar sua organização para gerenciar com êxito em relação a vulnerabilidades é uma parte essencial ao assumir uma postura proativa quanto à segurança. As políticas de segurança desenvolvidas irão estabelecer as bases de sua estratégia de gerenciamento de segurança das informações. Essas políticas devem documentar seus requisitos de segurança, processos e padrões de tecnologia. Isso oferece vantagens: além de lhe ajudar a detectar e eliminar as vulnerabilidades, uma estratégia inteligente de segurança também pode melhorar as operações empresariais, reduzindo riscos e diminuindo os custos de gerenciamento de segurança de TI.

Identificar e corrigir as vulnerabilidades existentes

Isso poderia envolver um processo tão simples (mas de uso intensivo de recursos) quanto certificar-se de que cada sistema operacional em cada computador esteja atualizado em relação às correções de segurança — e irão continuar assim. Outras vulnerabilidades são mais difíceis de detectar e corrigir, como os pontos fracos em aplicativos empresariais.

Mediar contra quaisquer ameaças existentes

Você está confiante de que já não é vítima de um ataque sofisticado? Ataques particularmente perniciosos, como as ameaças persistentes avançadas ou APTs, são desenvolvidos para permanecer invisíveis o maior tempo possível, passando de um host comprometido para o próximo, sem gerar tráfego de rede identificável. No "núcleo" de cada APT, encontra-se uma função de controle remoto, que permite que criminosos naveguem para hosts específicos nas organizações de destino, manipulem sistemas locais e tenham acesso contínuo a informações críticas. Para se proteger, são necessárias ferramentas desenvolvidas para detectar comunicações de controle remoto entre seu sistema e o invasor criminoso.

Tornou-se mais importante do que nunca direcionarmos nossa atenção ao teste de eficácia de políticas de segurança, procedimentos e tecnologias.

Testar, testar e testar mais ainda

Com o surgimento dos ataques sofisticados, deparamo-nos com a realidade de que sua organização será vítima disso. É apenas uma questão de tempo. Por esse motivo, tornou-se mais importante do que nunca que direcionemos nossa atenção aos testes de eficácia de políticas de segurança, procedimentos e tecnologias — especialmente porque eles são o elemento principal das exigências legais e regulatórias para o cuidado e diligência devidos. Não fazer isso pode significar que os funcionários das empresas serão responsabilizados pelos resultados de uma violação de segurança.

Além disso, como o cenário da segurança continuar a mudar a um ritmo crescente, é igualmente importante que políticas de testes e revisões regulares sejam implementadas.

Adotar uma abordagem inteligente para inteligência de segurança

Como manter o controle da situação — sem deixar seu departamento de TI em estado contínuo de pânico? Ferramentas de inteligência e análise de segurança podem monitorar e correlacionar a atividade de dados através de várias tecnologias de segurança, oferecendo-lhe visibilidade e insight sobre o que está acontecendo em seu ambiente — para ajudá-lo a detectar e investigar os tipos de atividades suspeitas que possam indiciar um ataque em andamento. Elas ajudam a reduzir a complexidade comunicando-se em uma linguagem comum através de ambientes de vários fornecedores, enquanto diminui a pressão sobre seu departamento de TI, proporcionando potencialmente tempo e economia de custos.

Desenvolver procedimentos de controle e atribuir propriedades de risco

Assim como tudo na vida, seus programas de segurança e políticas de defesa contra ameaças como ataques sofisticados são apenas tão bons quanto a capacidade de sua organização de garantir que todos estejam obedecendo a regras. É necessário um plano para se manter em controle da situação em longo prazo. Isso inclui decidir quem vai monitorar e gerenciar suas políticas de segurança e como comprovar que sua postura de risco está sendo mantida. Certifique-se de que seu programa de segurança tenha a propriedade e liderança atribuídas em todas as áreas empresariais críticas. Ao expandir a conscientização e responsabilidade às principais áreas de risco, você criará uma maior compreensão e execução dos controles de segurança já estabelecidos. E isto, por sua vez, permitirá a criação de um ambiente empresarial mais seguro.

Demonstrar e documentar o valor de seus investimentos em segurança

Não há como contornar o fato de que sua organização terá que encontrar o espaço necessário em seu orçamento para a criação e manutenção de um programa de segurança eficaz. Como é muito difícil quantificar valores em termos de ataques que não ocorreram, é uma boa ideia manter comunicações contínuas sobre o que você está fazendo e por que isso é importante. Ao relatar atividades significativas que causaram ou poderiam causar invasões em sistemas críticos e dados, por exemplo, é possível demonstrar o valor dos investimentos em tecnologia de segurança, identificar lacunas, interromper ataques em andamento, descobrir oportunidades de aperfeiçoamento e inspirar confiança em sua abordagem.

49%

dos executivos de TI sentem-se confrontados pela incapacidade de medir a eficácia de seus atuais esforços em relação à segurança.[4]

Rever tudo para garantir que não haja lacunas ou sobreposições desnecessárias

Quando se trabalha em grupo, mas assumindo responsabilidades individuais em aspectos específicos de um plano, é fácil cometer o erro de supor que alguém cumpra uma tarefa que você não tenha cumprido. Da mesma forma, é possível que mais de uma pessoa realize a mesma tarefa. Por isso, faça uma verificação final para a clareza e completude — certificando-se de que você incluiu provisões para inteligência de segurança, análise e monitoramento, por exemplo — a fim de reduzir a complexidade e gastos desnecessários, e procurar oportunidades para simplificar o monitoramento contínuo, o gerenciamento e a tomada de decisão em tempo real nas tecnologias.

Dados de clientes roubados do varejista por mais de 18 meses; pelo menos 45 milhões de registros levantados

Custos estimados: Até US$ 900 milhões

Vítima: Varejista de desconto nacional

O que aconteceu: Aparentemente 45 milhões de números de cartões de débito e crédito de clientes foram roubados dos sistemas da empresa, embora o número real de registros roubados seja difícil de determinar, em decorrência da duração e da natureza do incidente. Esses dados foram vendidos para criminosos e, em seguida, utilizados para fazer compras fraudulentas.

Por que aconteceu: A empresa supostamente recolheu e armazenou quantidades excessivas e desnecessárias de informação pessoal por muito tempo e dependia da tecnologia de criptografia desatualizada para proteger os dados. Os invasores, aparentemente obtiveram acesso inicial ao banco de dados central através de conexões inseguras sem fio em lojas de varejo. A empresa posteriormente foi considerada infratora das normas do segmento de mercado de pagamento.

Dano causado: Parece ter sido a maior violação deste tipo que obteve cobertura generalizada da mídia. Além de ações judiciais, multas e custos de reparação altos, o dano à reputação e outros custos indiretos são imensuráveis.

Lições aprendidas: A reavaliação periódica e regular dos riscos de infraestrutura e informações é necessária conforme as ameaças e tecnologias em constante mudança podem tornar obsoletas as proteções anteriormente aceitáveis.

Apenas para efeitos ilustrativos. Os fatos reais e danos associados a esses cenários podem ser diferentes dos exemplos fornecidos. *São estimados, com base em informações financeiras publicamente disponíveis, assim como em artigos publicados.*

Etapa 3: Preparar sua resposta ao inevitável: um ataque sofisticado

Uma vez que suas políticas de segurança, procedimentos e tecnologias tenham sido implementados da melhor forma possível, é hora de resolver como lidar com uma violação se e quando ela ocorrer. De fato, como um analista observou recentemente: "A maioria dos administradores de segurança e diretores de segurança da informação de grandes empresas compreendem que não é uma questão de "se", mas sim de "quando" a sua organização irá experimentar uma violação."[5]

Desenvolver um plano detalhado e coordenado

Uma organização necessita de uma política e processo entre empresas unificado a fim de gerenciar suas respostas a incidentes. Se você já tem um plano em prática, você já o testou e determinou sua eficácia recentemente?

Seu plano de resposta a incidentes deve especificar de que forma um ataque será evitado, identificar o que foi comprometido (se for o caso), e calcular o impacto financeiro e de reputacional. Deve também oferecer diretrizes para a comunicação com os funcionários, com quaisquer indivíduos cuja informação possa ter sido comprometida e com os meios de comunicação.

Verificar se você tem acesso aos recursos e ferramentas necessários para uma resposta imediata

Quanto maior o tempo levado para identificar e responder a um ataque, maior o dano provável e custo de reparação. Além disso, cerca de 78 por cento dos executivos que responderam a uma pesquisa recente patrocinada pela IBM sobre o risco reputacional alegaram que se recuperam de incidentes considerados relativamente pequenos (como queda de website) em menos de seis meses. O tempo necessário para se recuperar de danos à reputação devido ao cibercrime é muito maior — em parte, porque pode ser mais difícil divulgar a ideia de que o problema foi inteiramente resolvido.[6]

Munir-se dos recursos ou habilidades necessários para responder ativamente e investigar incidentes de segurança é fundamental para reduzir seus impactos.

É claro que ter acesso aos recursos ou habilidades necessárias para ativamente responder e investigar incidentes de segurança é fundamental para reduzir o seu impacto. Se sua reputação influencia diretamente sua capacidade de conduzir seus negócios, ou se e a natureza do seu negócio pode aumentar o risco de ataques sofisticados, considere a implementação de um sistema permanente de acompanhamento e gerenciamento contra ameaças e riscos. Esta abordagem utiliza tecnologia elaborada para melhorar a defesa, automatizar a resposta a incidentes e realizar análises investigativas em uma ampla gama de ameaças.

Munir-se de uma abordagem consistente para atribuir responsabilidades em toda a organização

Aceite o fato de que praticamente todas as organizações serão vítimas de um ataque sofisticado de algum tipo, em algum momento. Certifique-se de que seu plano de resposta a incidentes especifica quem terá que fazer o que e como todos irão compartilhar informações. Coordenação em toda a empresa é a chave para a detecção, solução e contenção eficazes. É importante que todos os envolvidos exerçam um função relevante — e saibam que função é esta. Determinar quais os passos que cada parte interessada terá que implementar em sua área para ajudar a reduzir a ocorrência — e limitar a amplitude — de ataques sofisticados.

Processadores de pagamento no núcleo dos negócios sofrem intrusões que afetam 130 milhões de clientes

Custos estimados: Até US$ 500 milhões

Vítima: Processador de pagamento

O que aconteceu: Cerca de 130 milhões de números de cartão de crédito e débito de clientes foram roubados de um sistema de processamento de pagamentos, resultando em transações fraudulentas.

Por que aconteceu: Um software malicioso foi aparentemente inserido no sistema de processamento e utilizado para coletar dados não criptografados de pagamentos em andamento, enquanto estava sendo processado pela empresa durante o processo de autorização da transação. Os dados do cartão incluíam números dos cartões, datas de validade e outras informações determinadas a partir da tarja magnética no verso do cartão de pagamento.

Dano causado: Esta foi uma violação visível e enorme, que também recebeu ampla cobertura da mídia. A empresa teria pagado mais de US$140 milhões em custos diretos relacionados a decisões judiciais, acordos e taxas. E a capitalização de mercado da empresa supostamente caiu quase meio bilhão de dólares nos três meses após o evento.

Lições aprendidas: Uma resposta direta e sincera a tal crise minimizou a deserção de clientes. As informações compartilhadas e aproveitadas pelos padrões associados do setor de mercado reforçaram a postura de segurança da empresa permitindo-lhe, eventualmente, recuperar a sua perda de valor de mercado.

Apenas para efeitos ilustrativos. Os fatos reais e danos associados a esses cenários podem ser diferentes dos exemplos fornecidos. *São estimados, com base em informações financeiras publicamente disponíveis, assim como em artigos publicados.*

Etapa 4: Promover e apoiar uma cultura de conscientização de segurança

A tarefa referente à segurança da rede de uma empresa continua tornando-se infinitamente mais complexa à medida que as informações trafegam por milhares de dispositivos, assim como através dos inúmeros serviços públicos baseados na web. Um estudo relatou que 91 por cento dos usuários de smartphones corporativos conectam-se a emails corporativos, mas exige-se que apenas um em três instale softwares de segurança para celulares.[7] Em um ambiente assim, o acesso torna-se fácil para todos os envolvidos — inclusive criminosos.

Criar e apoiar uma cultura de conscientização sobre os riscos em toda a organização

É hora de expandir a missão de segurança da empresa; da equipe de tecnologia e suas máquinas a cada pessoa dentro da empresa, assim como a todos os parceiros de negócios. Já que cada pessoa apresenta um perigo potencial, cada um deve representar também uma parte da solução. Afinal, o sucesso depende sobretudo de se promover e apoiar uma cultura consciente sobre riscos, em que a importância da segurança informa todas as decisões e procedimentos em todos os níveis da empresa. Isso significa que os procedimentos pertinentes à segurança de dados precisa se tornar algo relevante, tal como trancar a porta ao sair de casa.

Garantir que cada funcionário saiba o que fazer

O processo de mudança de cultura de uma empresa pode ser extremamente desafiador. Mas se as medidas necessárias forem tomadas para se comunicar a real importância da ajuda a fim de melhorar a segurança, assim como para ensinar a todos como reconhecer e reportar possíveis problemas, você estará tomando as medidas corretas e cabíveis.

Nossos fundamentos em segurança

Na IBM, estamos sempre nos esforçando para encontrar o equilíbrio entre o aperfeiçoamento de como fazemos negócios e a necessidade de controlar riscos. A resposta abrangente da companhia inclui tecnologia, processos e medidas políticas. Trata-se de 10 práticas essenciais.

1. Desenvolver uma cultura de conscientização sobre os riscos — onde haja tolerância zero na empresa quando os funcionários forem descuidados quanto à segurança. Os gerentes precisam implementar continuamente essa mudança em todos os níveis da empresa, assim como ferramentas para acompanhar seu progresso.

2. Gerenciar incidentes e respostas — É essencial um esforço de toda a empresa para implementar análises inteligentes e recursos de resposta automática. A criação de um sistema automatizado e unificado permitirá que a empresa monitore suas operações — ofereça respostas rapidamente.

3. Proteger o local de trabalho — Cada estação de trabalho, laptop ou smartphone oferece uma abertura potencial a ataques maliciosos. As configurações de cada dispositivo devem se submeter a um gerenciamento e execução centralizados. E os fluxos de dados dentro de uma empresa têm que ser classificados e encaminhados exclusivamente para o seu círculo de usuários.

4. Segurança no design — Uma das maiores vulnerabilidades em sistemas de informação surge do fato de que implementamos os serviços primeiramente e, em seguida, implementamos a segurança. A única solução é integrar a segurança desde o início e realizar testes regulares para acompanhar seu cumprimento.

5. Manter a organização — Gerenciar atualizações em uma variedade de softwares pode ser impossível. Em um sistema seguro, os administradores podem acompanhar cada programa em execução, confirmar que são atuais, e dispor de um sistema para instalar as atualizações e correções à medida que forem liberados.

6. Controlar o acesso à rede — Empresas que filtram dados registrados através de pontos de acesso monitorados têm mais facilidade em detectar e isolar o malware.

7. Segurança nas nuvens — Se uma empresa estiver migrando determinados serviços de TI para um ambiente em nuvem, ela estará mais próxima de outros usuários — incluindo estelionatários. Por isso, é importante ter as ferramentas e os procedimentos para isolar-se dos outros, e para monitorar possíveis ameaças.

8. Patrulhar a vizinhança — A cultura de segurança existente em uma empresa deve ir além dos limites da empresa e estabelecer as melhores práticas entre os seus contratados e fornecedores. Isto é um processo semelhante a controles de qualidade já existentes no passado.

9. Proteger as riquezas da empresa — Cada empresa deve realizar um inventário de seus ativos críticos — sejam eles referentes a dados científicos ou técnicos, documentos confidenciais ou informações particulares de clientes — e garantir que eles recebam tratamento especial. Cada item prioritário deve ser vigiado, controlado e codificado como se a sobrevivência empresa de dependesse dele.

10. Identificar quem é quem — Empresas que falham no gerenciamento do "ciclo de vida da identidade" estão operando "às cegas" e podem estar vulneráveis às intrusões. Você pode enfrentar este risco através da implementação de sistemas meticulosos para identificar pessoas, gerenciar suas permissões, e revogá-las quando necessário.

Figura 1. ***Dez práticas essenciais:*** *Um programa de segurança bem-sucedido define um equilíbrio que permite flexibilidade e inovação, mantendo as garantias consistentes a serem compreendidas e praticadas por toda a organização.*

Comece agora — antes que sua empresa se torna uma vítima

Recentemente, a IBM X- Force relatou mais de 4.400 novas vulnerabilidades de segurança apenas no primeiro semestre de 2012. Presumindo que essa tendência tenha se estendido até o fim do ano, as vulnerabilidades totais previstas provavelmente iriam superar o recorde de quase 9.000, registrado em 2010. Além disso, a taxa de vulnerabilidades não corrigidas do primeiro semestre de 2012 foi a mais alta que a IBM X- Force observou desde 2008.

Muitas organizações tiveram que lidar com as consequências causadas por vazamento de senha e de dados pessoais. E esses ataques têm se tornado cada vez mais sofisticados. Por exemplo, através da obtenção de pequenas quantidades de dados pessoais importantes a partir de sites de mídia social, os invasores foram capazes de utilizar "truques" inteligentes de engenharia social para ter acesso irrestrito a contas específicas. Eles têm até mesmo ignorado a autenticação de dois fatores, convencendo fornecedores de telefonia celular a realocar o serviço de caixa postal de usuários. Portanto, não se trata apenas da possibilidade de sua empresa se tornar uma vítima, mas de quando isso irá acontecer. Na realidade, 61 por cento dos executivos que participaram do recente estudo da IBM sobre o risco reputacional e TI afirmaram que as violações de dados, roubo de dados e cibercrime representa a maior ameaça à reputação de suas empresas.[8]

Não se trata apenas da possibilidade de sua empresa se tornar uma vítima, mas de quando isso irá acontecer.

É compreensível procurar ajuda

É fácil sentir-se sobrecarregado quando você considera o que é preciso para proteger sua organização contra ataques sofisticados. Há muito sobre o que discutir, pensar e sobre o que se preocupar. Mas você só precisa dar um passo de cada vez. E não precisa fazê-lo sozinho.

Os consultores da IBM Security Services podem ajudá-lo a planejar, implementar e gerenciar virtualmente todos os aspectos de sua estratégia de segurança. Eles são profissionais de segurança experientes que aperfeiçoaram suas habilidades nos setores público e privado, trabalhando na liderança e consultoria de segurança corporativa, agências de investigação do governo, aplicação da lei e pesquisa e desenvolvimento.

Além de oferecer serviços de consultoria, a IBM ajudou a definir o padrão de confiabilidade, responsabilidade e proteção em serviços gerenciados de segurança desde 1995. Estes serviços são desenvolvidos para ajudá-lo a melhorar sua postura em relação à segurança da informação, reduzir o custo total de propriedade e demonstrar a conformidade com a terceirização do monitoramento e gerenciamento de operações de segurança da IBM, independentemente do tipo de dispositivo ou de fornecedor, 24 horas por dia durante o ano todo ou quando necessário.

O IBM Managed Security Services pode oferecer a inteligência de segurança, o conhecimento, as ferramentas e a infraestrutura necessários para ajudá-lo a proteger seus ativos de informação contra ataques oriundos da Internet muitas vezes a uma fração do custo interno destinada a recursos de segurança.

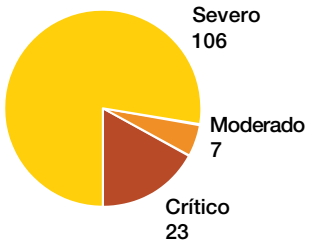
Comece com um Security Health Scan gratuito

Provavelmente, você já está pensando sobre o quanto sua empresa está vulnerável. É possível ter uma ideia dessa vulnerabilidade com o Security Health Scan gratuito oferecido pelo IBM Security Services. Veja como funciona: A IBM realizará uma varredura de até 10 endereços de IP ou um domínio web de sua escolha, uma vez por semana por três semanas, sem nenhum custo. Você receberá uma análise detalhada da vulnerabilidades encontradas — classificadas pelo seu grau de gravidade — juntamente com as instruções passo a passo sobre como remediá-las. Além disso, durante o período de varredura, você terá acesso ao portal do IBM Managed Security Services Virtual Security Operations Center e a todas as informações de inteligência e ameaças fornecidas por ele.

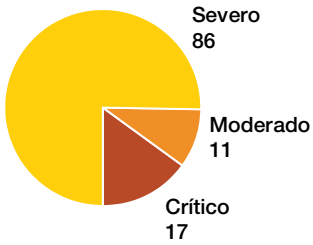
O que um Security Health Scan encontraria na sua empresa?

Observam-se aqui exemplos de descobertas feitas através de Security Health Scan em vários tipos de organizações, mostrando a média de vulnerabilidades encontradas após apenas uma das três varreduras consecutivas e semanais. Não é surpresa que até mesmo as empresas mais seguras podem ser expostas significativamente, por vezes, em vários setores. No ambiente corporativo dinâmico atual, onde fronteiras já não existem, é mais provável que se encontre, pelo menos, algumas vulnerabilidades e exposições.

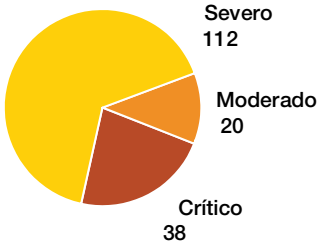
Universidade



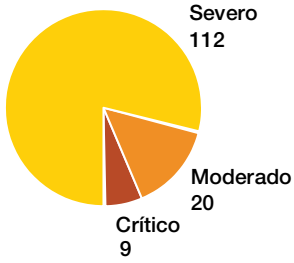
Companhia de seguros



Hosting virtual/ provedor de hosting da web



Governo da cidade



Para obter mais informações

Para saber mais sobre como o IBM Security Services pode ajudá-lo a reduzir custos e aumentar sua proteção contra ameaças sofisticadas, entre em contato com seu representante IBM ou Parceiro de Negócios IBM, ou visite o seguinte website:
ibm.com/services/security

Para inscrever-se a fim de obter um Security Health Scan gratuito, visite:
ibm.com/security-scan

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produzido nos Estados Unidos da América
Fevereiro de 2013

[1] Ponem on Institute LLC, *The Impact of Cybercrime on Business: Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil sponsored by Check Point Software Technologies*, Maio de 2012.
[2] Relatório Semestral de Riscos de Tendências da IBM X-Force 2012, Setembro de 2012.
[3] Consultar nota 1 acima.
[4] *Security Intelligence Can Deliver Value Beyond Expectations And Needs To Be Prioritized*, a commissioned study conducted by Forrester Consulting on behalf of IBM Global Technology Services, Maio de 2012.
[5] Postagem em blog: *"Okay, Breaches Are Inevitable: So Now What Do We Do?"* por Paula Musich, Current Analysis, 20 de julho de 2012.
[6] IBM Global Technology Services, Risco Reputacional e TI, Setembro de 2012.
[7] Kaspersky Labs, Enterprise Mobile Security Survey, Dezembro de 2010.
[8] Consultar nota 6 acima.

Recicle

SEW03029-USEN-00