Prepare-se para uma nova era de segurança

Empregue experiência, análise e uma abordagem sistemática com as soluções de segurança IBM

Definindo estratégias de segurança

O principal desafio dos líderes de segurança com relação aos dispositivos móveis é pensar menos em tecnologia e mais em política e estratégia.[1] Entretanto, de acordo com um estudo recente, mais de um terço dos executivos de segurança não tem *nenhum tipo* de estratégia de risco em vigor.[2]

Vivemos uma nova realidade de segurança

Atualmente, os ataques à segurança são bem financiados e realizados com uma precisão semelhante à com que negócios são conduzidos. E à medida que tecnologias como as de nuvem, dispositivos móveis, big data e mídias sociais são mais difundidas, os ataques a empresas se tornam mais sofisticados e custosos. De fato, o Ponemon Institute estima que o custo de apenas uma violação chegue a inacreditáveis US$ 11 milhões.[3]

As novas ameaças representadas pelas tecnologias emergentes configuram uma prioridade, em especial atualmente, em um mundo mais inteligente no qual empresas instrumentadas, interconectadas e inteligentes coletam, processam, utilizam e armazenam mais informações do que nunca. Líderes de segurança indicam que a segurança de dispositivos móveis é a tecnologia implantada mais recentemente, e 76% deles implementaram algum tipo de serviços de segurança para nuvem.[1] Mas o perímetro de rede da forma que o conhecemos está desaparecendo, e a tecnologia que as organizações vinham utilizando para proteger essas fronteiras está se tornando obsoleta. Os negócios deixaram de ser conduzidos dentro dos limites físicos da organização. Conforme os perímetros de rede tradicionais se dissolvem permanentemente e os pontos de extremidade continuam se proliferando, os ambientes de segurança se tornam mais complexos - fazendo com que seja mais difícil defender dados contra falhas de segurança e proteger os usuários que acessam esses dados.

A chave para superar esses desafios é adotar uma estratégia de proteção dinâmica que possa evoluir conforme as mudanças no panorama de ameaças e encontrar um parceiro de segurança capaz de fornecer a tecnologia, a especialização e a experiência para ajudar a assumir o controle da nova realidade da segurança.

As organizações devem se preparar hoje

Todas as empresas e todos os setores são vulneráveis a ataques. Ainda assim, frequentemente se passam meses antes que muitas delas sequer saibam que foram invadidas.
Organizações despreparadas para a nova era da segurança estão assumindo riscos perigosos que podem levar a danos caros e permanentes.

Veja os novos aspectos fundamentais:

- **Proteger os negócios -** Riscos de segurança representam uma ameaça cara e persistente para os negócios em termos de vendas, perda de confiança do cliente e, algumas vezes, um duradouro desgaste da marca. Líderes de negócios esperam que os CISOs forneçam uma muralha de proteção.
- **Adotar as tecnologias disruptivas** — Mesmo com tecnologias disruptivas como as de nuvem, dispositivos móveis, big data e mídias sociais assumindo residência permanente no mundo dos negócios, há maneiras de utilizá-las para fortalecer sua postura de segurança.
- **Abandonar medidas tradicionais** — A abordagem tradicional de implantar uma nova ferramenta de segurança para lidar com cada novo risco deixou muitas organizações com uma rede fragmentada que é cara, complexa e privada de uma visibilidade integral do cenário de segurança.
- **Parar de gerenciar a segurança sozinho** — Com os ataques evoluindo em velocidades alarmantes e novos métodos de ataque aparecendo com maior frequência, a maioria das organizações simplesmente não tem as habilidades e o pessoal necessários para estar à frente da próxima onda de ataques.
- **Preparar-se hoje —** Ao adotar uma nova estratégia de segurança - e compreender as habilidades que conferem eficácia a essa estratégia —, você pode se posicionar estrategicamente hoje para enfrentar ameaças que ainda serão criadas.

Prepare-se para o inevitável ataque

Para evitar violações de segurança, sua equipe deve estar treinada para pensar como um invasor. Comece identificando os ativos de maior importância para seus negócios - sejam eles funcionários, dados ou transações - e proteja-os colocando em prática robustas tecnologias de inteligência em segurança capazes de:

- Monitorar o acesso a dados
- Ajudar a evitar fraudes
- Identificar anomalias e acessos não autorizados
- Aplicar análise em tempo real para detectar indicadores de ataques.

Oitenta e três por cento das empresas consideram de relativamente a extremamente difícil recrutar e contratar profissionais de segurança.[4]

Para estar preparado para as inevitáveis violações de segurança, sua estratégia de segurança deve capacitá-lo a:

- **Limitar o impacto de uma violação** com um plano e uma equipe de resposta a incidentes.
- **Certificar-se de que as tecnologias de nuvem, dispositivos móveis, mídias sociais e big data sejam ainda mais seguras** do que as tecnologias localizadas nas instalações.
- **Empregar alternativas baseadas em riscos** onde for possível.
- **Testar incansavelmente a conformidade** com padrões do setor.
- **Implementar prontamente mudanças** de controles e políticas.
- **Aplicar inteligência e automação** para reduzir surpresas e facilitar tarefas rotineiras.

Por fim, lidar com as lacunas nas habilidades de segurança estabelecendo parcerias com consultores, utilizando serviços gerenciados e compreendendo pesquisas avançadas em segurança.

Soluções IBM para proteger seus negócios

A IBM oferece tecnologias testadas e comprovadas, criadas para proteger contra uma gama de ameaças à segurança. A IBM pode ajudá-lo a:

- **Transformar big data em inteligência de segurança acionável,** com as soluções de inteligência em segurança da IBM e os serviços de gerenciamento e monitoramento de ameaças da IBM
- **Proteger ativos sensíveis** com o Programa de Proteção "Crown Jewels" da IBM, os Serviços de Gestão de Acesso e Identidade da IBM, e o IBM Application and Data Security
- **Implementar defesas de última geração** utilizando os Serviços de Respostas a Emergências da IBM, os dispositivos do IBM Security Network Protection e as soluções da Trusteer[5] contra crimes cibernéticos
- **Manter o controle da nuvem** com as soluções de segurança de nuvem da IBM
- **Garantir a segurança de dispositivos móveis** com as soluções de segurança IBM MobileFirst, as soluções contra fraudes em dispositivos móveis da Trusteer e as soluções de segurança para dispositivos móveis da IBM Fiberlink[6]
- **Alavancar a inteligência proveniente de diversas fontes** utilizando a segurança como serviço, incluindo os serviços de segurança baseados em nuvem da IBM, o serviço de proteção de presença na web da IBM e a Proteção Avançada contra Fraudes da Trusteer
- **Realizar um benchmarking da maturidade com relação a seus pares** e definir um roadmap de transformação com o benchmarking de maturidade de segurança da IBM e a Avaliação de Riscos de Segurança da IBM
- **Integrar sua plataforma de segurança** com o IBM Security Framework de soluções e os Serviços de Otimização de Operações de Segurança da IBM
- **Tirar proveito da profunda experiência em segurança** com os serviços de Consultoria de Segurança da IBM, o IBM® X-Force® e as pesquisas da Trusteer

Por que a IBM?

Os controles de segurança tradicionais são insuficientes para lidar com os ataques sofisticados da atualidade. Por isso, a IBM oferece uma estratégia multifacetada que incorpora:

- Uma profunda inteligência em segurança e um amplo portfólio de segurança empresarial
- Amplos controles e visibilidade
- Atualizações de segurança e análise em tempo real
- Integração de recursos novos e existentes
- As mais recentes pesquisas sobre as ameaças emergentes e os métodos de segurança

Para obter mais informações

Para saber mais sobre as Soluções IBM Security, entre em contato com seu representante de vendas IBM ou Parceiro Comercial IBM, ou visite:
ibm.com/security

Sobre as Soluções de Segurança IBM

A divisão de Segurança IBM oferece um dos mais avançados e integrados portfólios de produtos e serviços de segurança. O portfólio, com suporte do desenvolvimento e pesquisa X-Force, de renome mundial, fornece inteligência em segurança para ajudar as organizações a protegerem de maneira holística seu pessoal, infraestruturas, dados e aplicativos, oferecendo soluções para gerenciamento de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de riscos, gerenciamento de endpoints, segurança de rede e outros. Essas soluções permitem que as organizações gerenciem os riscos de maneira eficaz e implementem uma segurança integrada para arquiteturas móveis, de nuvem, de mídias sociais e outras arquiteturas de negócios empresariais.
A IBM opera uma das mais abrangentes organizações de pesquisa, desenvolvimento e fornecimento de segurança do mundo, monitora 15 bilhões de eventos de segurança por dia em mais de 130 países e detém mais de 3.000 patentes de segurança.

Além disso, a IBM Global Financing pode ajudá-lo a adquirir os recursos de software de que seus negócios precisam da maneira mais econômica e estratégica possível. Nós trabalharemos junto com clientes com qualificação de crédito para customizar uma solução de financiamento adequada aos seus objetivos de negócios e de desenvolvimento, ativar um gerenciamento monetário efetivo e melhorar seu custo total de propriedade.
Financie seus investimentos críticos em TI e impulsione seus negócios com a IBM Global Financing. Para obter mais informações, visite: **ibm.com**/financing

[1] "A new standard for security leaders: Insights from the 2013 IBM Chief Information Security Officer Assessment," *IBM Corp*., outubro de 2013. http://public.dhe.ibm.com/common/ssi/ecm/en/ciw03087usen/CIW03087USEN.PDF

[2] IBM Global Technology Services, "Understanding the economics of IT risk and reputation: Making the business case for business continuity and IT security," *IBM Corp*., novembro de 2013. http://www-935.ibm.com/services/us/gbs/bus/html/risk_study.html

[3] "2013 Cost of Cyber Crime Study," *Ponemon Institute*, outubro de 2013. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[4] Jon Oltsik, Kristine Kao e Jennifer Gahm, "Security Management and Operations: Changes on the Horizon," *ESG Research*, 23 de julho de 2012. http://www.esg-global.com/research-reports/security-management-and-operations/

[5] A Trusteer, Ltd. foi adquirida pela IBM em setembro de 2013.

[6] A Fiberlink Communications foi adquirida pela IBM em dezembro de 2013.

IBM Corporation
Software Group
Route 100
Somers,
NY 10589

Produzido nos Estados Unidos da América em Março de 2014

WGF12347-BRPT-00