Segurança IBM
White Paper de Ideias Inovadoras

Janeiro de 2015

Uma nova era de segurança para uma nova era da computação

A IBM ajuda os clientes a otimizar seus programas de segurança, interromper ameaças avançadas, proteger ativos críticos e proteger a computação em nuvem e a computação móvel

IBM

Introdução

Com o passar dos anos, o jogo de gato e rato entre invasores cibernéticos e as pessoas que defendem as redes tem se tornado cada vez mais complexo. Novos avanços em tecnologias defensivas levaram os invasores a alterar suas táticas e novas técnicas de ataque produziram novas exigências de resposta que produtos pontuais não conseguem atender.

Enquanto muitas organizações permanecem em modo de resposta de crise, algumas deixaram a postura reativa para trás e estão adotando medidas para reduzir riscos futuros. Estão começando a entender que a segurança não é apenas uma coisa ou produto que pode ser comprado e instalado—é um processo contínuo que está na essência da própria empresa.

É necessário responder às ameaças—e a IBM tem as respostas

De acordo com um estudo recente, o custo médio de uma violação nos Estados Unidos durante o ano de 2014 foi superior a US$5,8 milhões[1]. Portanto, as organizações não podem se dar ao luxo de ignorar esse clima de segurança mutável e agressivo.

Além de salvar a organização de custos possivelmente devastadores, uma segurança eficaz pode ser uma ferramenta para realmente capacitar a empresa. Uma abordagem holística que combina os recursos compartilhados de sistemas, serviços e pesquisas IBM pode permitir que as organizações sigam em novas direções estratégicas. Com soluções integradas e abrangentes da IBM, as organizações podem:

- **Otimizar o programa de segurança—in**tegrando silos de segurança, reduzindo a complexidade e diminuindo os custos
- **Interromper ameaças avançadas—**com análise e insight para uma defesa integrada mais inteligente
- **Proteger ativos críticos**—usando controles de reconhecimento de contexto e baseados em funções para ajudar a evitar o acesso não autorizado
- **Proteger ambientes de nuvem e ambientes móveis**—para construir iniciativas de negócios e conectividade baseadas em uma postura de segurança mais forte

Otimizar o programa de segurança

Até o momento, as organizações geralmente responderam às preocupações de segurança implementando uma nova ferramenta para abordar cada risco novo. O resultado foi que precisaram instalar, configurar, gerenciar, corrigir, atualizar e pagar por dezenas de soluções diferentes com visualizações limitadas do cenário. Caros e complexos, esses recursos fragmentados de segurança não podem oferecer a visibilidade e a coordenação necessárias para interromper os ataques sofisticados da atualidade. Além disso, a qualificação e o conhecimento necessários para acompanhar um fluxo constante de novas ameaças nem sempre estão disponíveis.

Não raro, as empresas têm dificuldade para encontrar as qualificações de segurança de que precisam. À medida que novos riscos surgem, o meio ambiente deve se tornar mais complexo e o déficit de competências, mais amplo. Ademais, quase 50% dos executivos de TI dizem que enfrentam um desafio causado pela incapacidade de medir a eficácia dos esforços de segurança que têm[2]—e 31% dos profissionais de TI não têm uma estratégia de risco[3]. Muitas equipes de segurança simplesmente trabalham no escuro.

As organizações podem adotar várias medidas importantes para ter uma abordagem de segurança integrada—que elimine informações de segurança isoladas, melhore os insights sobre segurança e aprimore a proteção no contexto de segurança—incluindo:

- **Desenvolver uma estratégia de segurança com reconhecimento de riscos:** Classifique a maturidade da sua segurança em comparação com seus pares e teste implacavelmente o cumprimento das normas do mercado. Analise a eficácia dos seus controles e desenvolva um roteiro para ajudar a melhorar sua postura de segurança, bem como reduzir o risco. Trabalhe com as principais partes interessadas para implementar mudanças rapidamente.

- **Implementar uma abordagem sistemática:** Defina o sistema integrado de recursos concebidos para mantê-lo em segurança. Perceba o valor total dos seus investimentos existentes em segurança ao misturá-los nesse sistema. Aplique inteligência e automação para minimizar as surpresas e facilitar as tarefas de rotina.
- **Aproveitar o conhecimento de profissionais:** Para ajudar a fortalecer o déficit de competências e entender ameaças complexas, contrate profissionais de consultoria e serviços gerenciados que tenham um conhecimento avançado e acesso a informações sobre ameaças mundiais, assim como recursos avançados de pesquisa. Faça parcerias com fornecedores de segurança que possam ajudar a conceber, desenvolver, implementar e gerenciar sua estratégia de segurança em conformidade com seu estágio de maturidade e seus objetivos de segurança.

Interromper ameaças avançadas

Sem uma proteção dinâmica, uma organização poderá passar mais tempo se recuperando de um ataque do que o evitando. As pessoas que não se preparam para a mudança estão deixando suas organizações perigosamente expostas.

Para se preparar para a mudança e criar uma base para uma melhor proteção, as organizações podem:}

- **Analisar comportamentos em vez de assinaturas:** Utilize abordagens analíticas de última geração para identificar comportamentos ou atividades incomuns—ajudando a evitar ataques direcionados e fraudes criadas por ameaças avançadas persistentes e malwares sofisticados.
- **Transformar Big Data em inteligência de segurança acionável:** Correlacione enormes conjuntos de dados em tempo real, usando a análise preditiva para ajudá-lo a detectar ameaças mais rapidamente e a tomar decisões mais embasadas.
- **Preparar sua resposta para o inevitável:** Organize uma equipe de resposta a incidentes. Capacite sua equipe com uma "mentalidade de caçador" para pensar como um invasor. Elabore um plano de resposta coordenado usando as ferramentas, informações e qualificações certas para limitar o impacto de uma violação inevitável. Saiba quem chamar quando você precisar de ajuda.

Proteger ativos críticos

Criminosos organizados, hacktivistas, governos e adversários são motivados pelo ganho financeiro, pela política e pela notoriedade ao atacar seus ativos mais valiosos. Em uma pesquisa, 61% das organizações disseram que o roubo de dados e os crimes cibernéticos são as maiores ameaças à sua reputação[4] e que as violações causaram perda de receita e interrupção de negócios graves.

Enquanto isso, funcionários negligentes colocam o negócio em risco sem saber por meio dos erros humanos. Para aumentar o desafio, a "Internet das Coisas" está incluindo bilhões de dispositivos, novos aplicativos e usuários que precisam ser protegidos.

As operações dos invasores são bem financiadas e assemelham-se a operações de negócios—eles avaliam seus alvos pacientemente com base nos esforços e recompensas em potencial. Seus métodos são extremamente direcionados—eles utilizam a mídia social e outros pontos de entrada para rastrear pessoas com acesso, aproveitar-se de sua confiança e explorá-las na forma de vulnerabilidades.

Infelizmente, muitos investimentos em segurança do passado não conseguem proteger dos novos tipos e métodos de ataques. O resultado são violações de segurança mais graves que ocorrem em maior número e com mais frequência.

Para defesas mais inteligentes, porém, as organizações podem usar análise e insights para:

- **Impregnar inteligência e detecção de anomalias em todos os domínios:** Prepare sua equipe de segurança para procurar violações coletando dados relevantes sobre segurança em todos os lugares da empresa. Implemente tecnologias de inteligência de segurança que possibilitam análise em tempo real, prevenção de fraudes e detecção de anomalias. Utilize inteligência e conhecimento de ameaças externas para aumentar seu conhecimento prático.

- **Construir uma área segura de inteligência em torno das joias da coroa:** Descubra e classifique os ativos mais importantes da sua organização. Proteja esses dados, esses funcionários e essas transações com controles inteligentes. Monitore quem está acessando tais dados e a partir de onde. Detecte anomalias e acesso não autorizado. Procure indicadores sutis de um ataque usando análise de segurança profunda.
- **Otimizar a segurança para usuários, dados e aplicativos a fim de blindar ativos sensíveis:** Ajude a assegurar que suas informações estejam protegidas—em trânsito, em repouso e em uso, evitando o acesso por usuários não autorizados e desenvolvendo inteligência para identificar o uso indevido por parte das pessoas autorizadas a acessá-las.

Proteger a nuvem e os dispositivos móveis

As organizações estão adotando plataformas móveis, redes sociais, Big Data e computação em nuvem para analisar e compartilhar informações em taxas sem precedentes. Em uma pesquisa de opinião recente com líderes em segurança, 86% dos entrevistados disseram que adotaram a nuvem ou estão planejando iniciativas de nuvem[5].

Executivos de segurança expressam preocupação com a segurança das novas iniciativas, como o perigo de furto ou perda de dispositivos móveis, preocupações de privacidade associadas à computação em nuvem e compartilhamento acidental de dados sensíveis. Ao mesmo tempo, menos da metade dos líderes de segurança acham que têm uma abordagem eficaz de gerenciamento de dispositivos móveis, indicando uma diferença entre as demandas da empresa e a realidade da segurança[5].

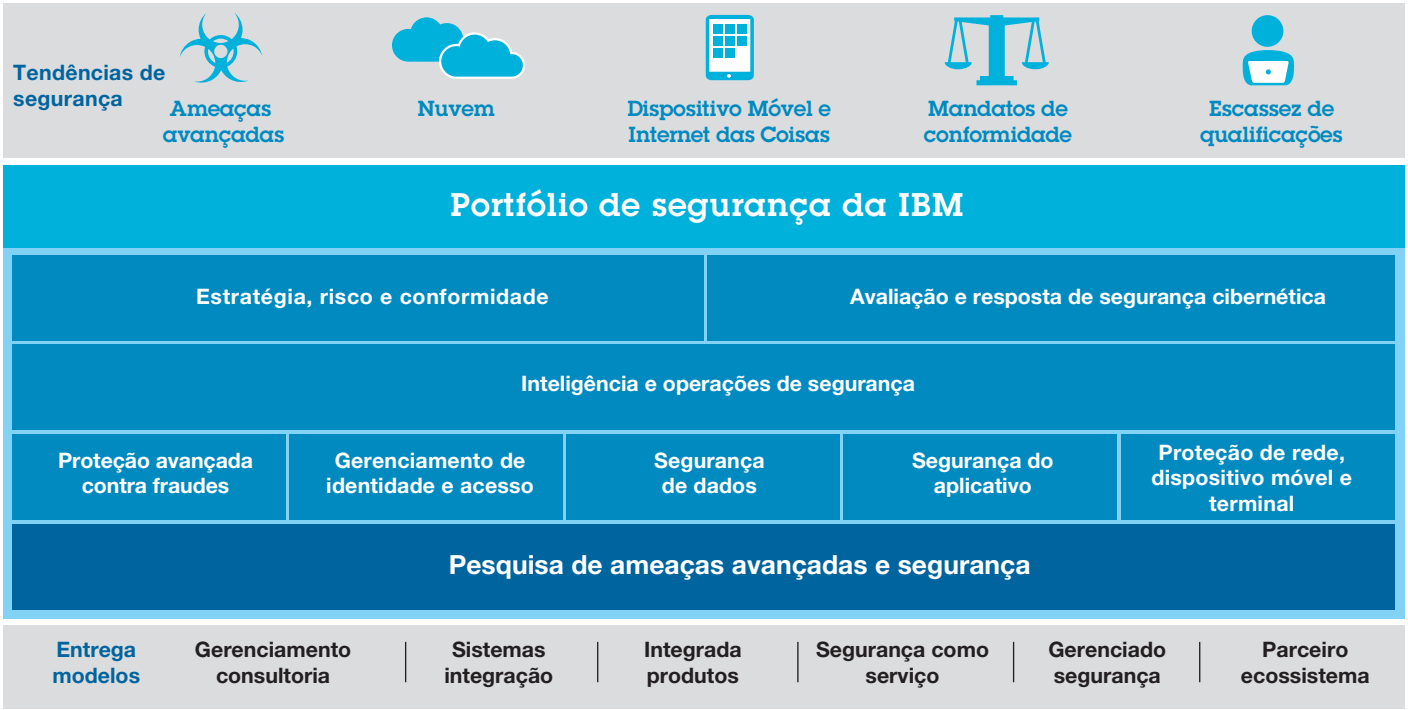
Para evitar uma exposição perigosa, as organizações devem implementar medidas tais como:

- **Controlar a agenda de segurança em busca de inovação:** Fique esperto agora em relação a como proteger iniciativas de dispositivo móvel, nuvem, Big Data e social. Entenda os imperativos estratégicos e trabalhe com a empresa para desenvolver alternativas baseadas em riscos. Recorra a especialistas para desenvolver um roteiro e implementar soluções seguras.
- **Integrar a segurança desde o primeiro dia:** Envolva-se no início e exija segurança em iniciativas de nuvem, dispositivo móvel, social e Big Data. Utilize as tecnologias mais recentes para tornar os dispositivos móveis mais seguros do que laptops, a nuvem mais segura do que datacenters, as redes sociais mais seguras do que email e Big Data mais seguros do que bancos de dados. Faça uma varredura dos aplicativos em busca de vulnerabilidades e corrija-as antes de implementar os aplicativos na web ou em uma loja de aplicativos online.
- **Use a nuvem, dispositivo móvel, social e Big Data para melhorar a segurança:** Use a segurança como serviço para implementação fácil e inteligência melhorada. Faça crowdsourcing em inteligência de ameaças para conseguir as dicas necessárias para ficar à frente dos ataques cibernéticos. Implemente ferramentas forenses de Big Data para detecção e recuperação de violações mais rápidas. Em um ambiente de Bring Your Own Device (BYOD), utilize contêineres de dados para proteger informações de negócios em qualquer lugar.

A diferença da Segurança IBM

A IBM é uma líder comprovada em segurança corporativa que ajuda as organizações na defesa contra ameaças novas e desconhecidas. Ela continua investindo substancialmente em pesquisa e desenvolvimento para construir um portfólio abrangente e integrado a fim de ajudar as organizações a inovar enquanto os riscos são reduzidos com:

- **Inteligência:** A inteligência de segurança está no centro do portfólio de Segurança IBM®. Com seus profissionais de campo especializados, a Segurança IBM pode oferecer a análise profunda e a visibilidade de que as organizações precisam para ajudar a enfrentar a grande variedade de ameaças.
- **Integração:** As soluções e serviços da Segurança IBM integram sistematicamente recursos de segurança novos e existentes em domínios de segurança, proporcionando visibilidade crítica, fornecendo controles abrangentes e ajudando a reduzir a complexidade.
- **Conhecimento:** O conhecimento da IBM através de mais de 6.000 profissionais e pesquisadores práticos que fornecem suporte aos clientes em mais de 130 países. Seu conhecimento, juntamente com os insights profundos reunidos a partir do monitoramento de mais de 270 milhões de endpoints e gerenciamento de 15 bilhões de eventos por dia, que são integrados aos produtos e serviços da IBM, fornecidos por meio de feeds de clientes em tempo real e integrados em contratos profissionais.



Para obter mais informações

Para saber mais sobre o portfólio de Segurança IBM, entre em contato com seu representante ou Parceiro de Negócios IBM ou acesse: **ibm.com**/security

Sobre a Segurança IBM

A Segurança IBM oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança corporativa. Recebendo suporte da pesquisa e do desenvolvimento mundialmente renomados da IBM X-Force®, o portfólio fornece inteligência de segurança para ajudar as organizações a proteger holisticamente seus funcionários, infraestruturas, dados e aplicativos, oferecendo soluções para gerenciamento de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de risco, gerenciamento de terminal e segurança de rede, entre outros. Essas soluções capacitam as organizações a gerenciar os riscos de forma eficiente e implementar segurança integrada para dispositivos móveis, nuvem, redes sociais e outras arquiteturas de negócio da empresa. A IBM administra uma das organizações de pesquisa, desenvolvimento e entrega de segurança mais amplas do mundo, monitora 15 bilhões de eventos de segurança por dia em mais de 130 países e possui mais de 3.000 patentes de segurança.

Além disso, a IBM Global Financing pode ajudá-lo a adquirir os recursos de software de que sua empresa precisa 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 eficaz e melhorar seu custo total de propriedade. Financie seus investimentos essenciais em TI e impulsione seus negócios com a IBM Global Financing. Para obter mais informações, acesse: **ibm.com**/financing

[1] "2014 Cost of a Data Breach Study", *Ponemon Institute*, maio de 2014. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

[2] Forrester Research, "Security Intelligence Can Deliver Value Beyond Expectations and Needs To Be Prioritized", maio de 2012. http://public.dhe.ibm.com/common/ssi/ecm/en/rll12348usen/ RLL12348USEN.PDF

[3] IBM Global Technical Services, "Understanding the economics of IT risk and reputation", *IBM Corp.*, novembro de 2013. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH& infotype=SA&appname=GTSE_RL_IH_USEN&htmlfid=RLW03024USEN& attachment=RLW03024USEN.PDF#loaded

[4] IBM Global Technical Services, "Reputational risk and IT", *IBM Corp.*, setembro de 2012. http://public.dhe.ibm.com/common/ssi/ ecm/en/rlw03009usen/RLW03009USEN.PDF

[5] IBM Center for Applied Insights, "Fortifying for the future; Insights from the 2014 IBM Chief Information Security Officer Assessment", *IBM Corp.*, dezembro de 2014. http://www-01.ibm.com/common/ssi/cgi-bin/ ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN& htmlfid=WGL03061USEN&attachment=WGL03061USEN.PDF#loaded

Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América – Janeiro de 2015

WGW03087-BRPT-00