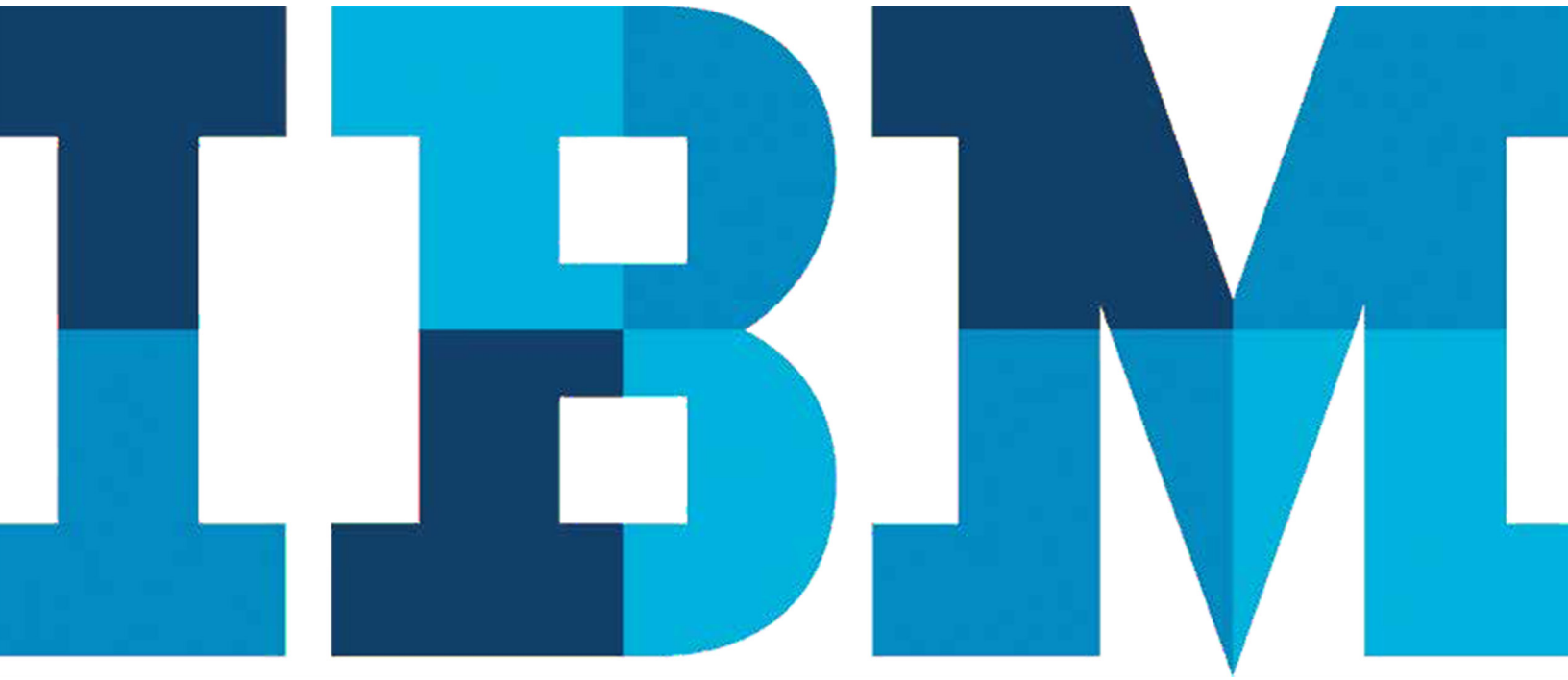
IBM Security
White Paper de Liderança de Ideias

Abril de 2015

IBM Security: Uma nova era

A IBM fornece milhares de especialistas em segurança e um portfolio integrado de soluções de segurança para ajudar a detectar e prevenir ameaças avançadas



IBM

Introdução

Vivemos em uma era de ouro da informação. Avanços em ciência de dados, análise de dados e redes inteligentes estão ajudando a vencer grande número de desafios—como médicos tratam doenças, estudantes aprendem e empresas inovam, para citar apenas alguns.

Mas uma nova espécie de criminosos—os invasores cibernéticos—está "envenenando a fonte". Invisíveis, pacientes e deliberados, estes intrusos invadem eletronicamente a rede e os computadores de uma organização, infiltrando-se no ambiente de forma que eles não sejam notados. Então, no momento certo, eles roubam dados sensíveis como números de cartão de crédito, segredos comerciais e informações pessoais. Eles causam danos enormes—uma estimativa indica o custo anual de cibercrime em mais de 400 bilhões de dólares.[1]

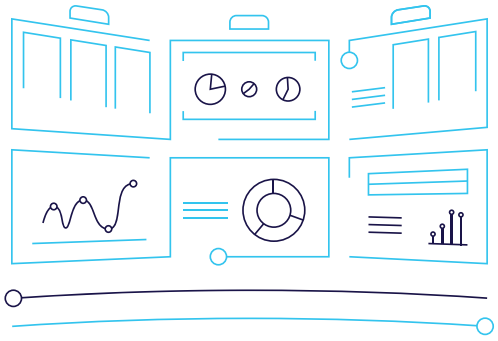
Eles são mais do que um simples grupo de hackers amadores. Esta é uma mudança fundamental na natureza do crime organizado que poderia destruir o progresso obtido a partir da revolução na computação, software e conectividade. É um novo tipo de ameaça que demanda pensamento inovador com relação à segurança.

Modernize a segurança com uma abordagem inteligente de ponta a ponta

Hoje em dia, para lutar contra ameaças cibernéticas, você precisa deixar para trás os "fossos e firewall" e as abordagens orientadas por conformidade das práticas de segurança tradicionais. Em vez disso, é necessário fortalecer a análise adaptativa, as defesas inteligentes e os controles integrados para descobrir e interromper ataques em tempo real.

Mas a tecnologia por si só não é a "bala de prata". Na verdade, nenhuma solução é única. São necessários políticas e sistemas de gerenciamento rigorosos também—programas que protejam proativamente todas as partes da organização, através de seus usuários, dados, aplicativos e infraestrutura.

Para fazer isto da forma correta, é necessário dar foco em quatro resultados principais: otimizar seus programas de segurança, parar ameaças avançadas, proteger ativos críticos e proteger ambientes de nuvem e de dispositivos móveis.



Como você está otimizando seu programa de segurança?

Um programa de segurança otimizado significa políticas e estratégias definidas claramente, programas rigorosos e uma equipe forte e coesa para implementá-los. Ainda assim os desafios podem ser enormes. Alguns dos problemas mais comuns incluem:

- **Nenhuma estratégia clara**: Você ainda não criou um inventário cuidadoso de sua estratégia de segurança. Você está abordando desafios críticos sem nenhum roadmap para o futuro—e nenhuma orientação geral.

- **Problemas de fragmentação**: Sua equipe precisa desempenhar tarefas repetitivas — respondendo às questões de segurança com uma nova ferramenta para cada risco que surge. E agora você tem uma confusão de soluções distintas com visões limitadas do cenário. Isto pode ser dispendioso, complexo e ineficaz para parar os sofisticados ataques de hoje em dia.

- **Falta de skill adequados**: Poucos profissionais no mercado com conhecimento adequado de segurança. E como a batalha para proteger a sua empresa evolui constantemente à medida que novas ameaças surgem, o déficit de competências inevitavelmente aumenta. Se você não pode medir adequadamente a efetividade da segurança de sua organização, você não saberá por onde começar — tendo uma estratégia efetiva definida ou não.

- **Prioridade nível C**: Manchetes sobre violações de segurança têm aumentado a preocupação do nível executivo a respeito das violações de dados em potencial. Agora estão solicitando que você se apresente ao CEO e ao conselho pelo menos uma vez ao ano, e possivelmente com muito mais frequência. Como você comunica suas prioridades e resultados de uma maneira—livre de "jargões de segurança"—que explique claramente suas ideias?

O passo à frente

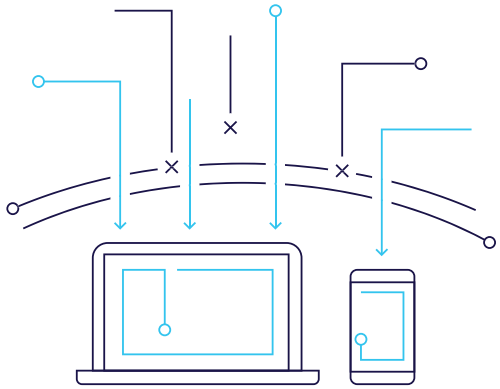
A IBM pode ajudá-lo a projetar um roadmap de segurança para o futuro. Trabalharemos com você para avaliar e testar sua capacidade de segurança com relação à sua concorrência. Em seguida, poderemos aplicar nosso conhecimento e soluções de segurança para ajudá-lo a mover em direção a uma abordagem de segurança integrada.

Uma nova abordagem para otimizar a segurança:

- **Avalie e transforme sua postura de segurança**: Você precisa classificar a maturidade de sua segurança com relação aos seus parceiros e testar implacavelmente para conformidade com os padrões de mercado. Podemos ajudá-lo a analisar a efetividade de seus controles e desenvolver um roadmap para reduzir riscos futuros. O mais importante, nós mostraremos a você como direcionar a conversa conforme você trabalha com as principais partes interessadas e os principais executivos para implementar rapidamente a mudança.

- **Construa operações de segurança da próxima geração**: Você está tratando a segurança como um caminho para reduzir o risco e aumentar seus negócios? Se não, comece agora. Seja sistemático. Defina os recursos de que sua organização precisa para permanecer segura. Em seguida, aplique inteligência e automação para minimizar surpresas e facilitar as tarefas rotineiras. Nós temos excelência nisto. Estamos ansiosos para ajudar.

- **Obtenha ajuda de especialistas no mundo todo 24x7x365**: Contrate "caçadores cibernéticos" profissionais para ajudar a detectar invasores, implementar novas soluções ou executar operações. A equipe de consultoria e serviços gerenciados da IBM está pronta para ajudar sua equipe de segurança a corrigir déficits de competências e a entender ameaças complexas. Fazemos isto usando nosso conhecimento e acesso avançado a informações de ameaças no mundo todo. Desejamos construir uma parceria valiosa com você e sua equipe.



Você pode parar as ameaças avançadas?

Ameaças cibernéticas sofisticadas estão em alta. Mais de 95 por cento dos chief information security officers (CISOs) acreditam que experimentarão um ataque avançado nos próximos 12 meses.[2] E quase 90 por cento dos CISOs acreditam que as ameaças de segurança avançadas atuais causam substancialmente mais danos do que ameaças tradicionais.[3]

O que é uma ameaça avançada? Um ataque sofisticado, direcionado, em um sistema, executado por invasores cibernéticos organizados motivados por ganho financeiro, políticas ou fama. Diferente dos worms, cavalos de troia ou vírus — que podem ser bloqueados facilmente por defesas de segurança de rede e endpoint — as ameaças avançadas são introduzidas silenciosamente, podem permanecer em um sistema por meses ou até mesmo anos, e são muito mais difíceis de detectar. Uma vez implantadas, elas coletam informações e maximizam o dano em sua organização.

Na IBM, nossos especialistas usam pesquisa extensiva e trabalho de detetive para entender totalmente as origens e recursos característicos dos invasores. Isto nos permite identificá-los, superá-los e impedi-los.

Se um cliente é violado, temos equipes de "socorristas" que podem diagnosticar e corrigir o problema.

O passo à frente

A inteligência é construída com relação a cada aspecto do nosso portfolio de soluções de segurança. Juntamente com a integração, ela é o caminho para uma postura de segurança forte. Use análitica e insight para parar ameaças avançadas e crie uma defesa unificada. Ao mesmo tempo, mova em direção a um design de sistema totalmente integrado.

As principais maneiras de parar ameaças avançadas:

- **Evite ataques direcionados em tempo real**: Podemos ajudá-lo a parar ameaças sofisticadas com defesas da próxima geração. Armados com nossas soluções de cibercrime mais recentes, você poderá detectar ameaças mais rápido e tomar decisões com base em informações correlacionadas de conjuntos de dados pesados em tempo real.

- **Detecte ameaças avançadas com inteligência em segurança**: É possível responder a violações mais rapidamente e parar de fato ameaças sofisticadas em tempo real com a análise de big data da IBM.

- **Defenda-se contra fraude na web e cibercrime**: Integração é a chave para parar ameaças avançadas. Manter a visibilidade e a coordenação entre domínios de segurança é vital. Nós o ajudaremos a reduzir os custos operacionais e a complexidade da infraestrutura com controles integrados e serviços gerenciados.

O quão seguros estão seus ativos críticos?

Não faz muito tempo, sua organização precisava apenas se preocupar com o acesso dos funcionários a poucos aplicativos altamente controlados dentro de sua rede. Tudo isso mudou. Tudo e todos estão interconectados. Como resultado, você pode estar enfrentando qualquer um destes desafios:

- Sua empresa possui potencialmente milhões de clientes, parceiros, fornecedores e outros usuários entrando em seu sistema buscando acesso a registros.
- O uso de dados aumentou exponencialmente, e a taxa de novos aplicativos sendo desenvolvidos no mundo dos aplicativos móveis é surpreendente. Esta velocidade e volume explosivos provavelmente está estressando seus sistemas de segurança.
- Invasores cibernéticos bem financiados e altamente eficazes estão trabalhando noite e dia para localizar vulnerabilidades nestas novas plataformas. Pior, agora eles usam a mídia social para rastrear seus usuários autorizados para roubar suas credenciais e explorar vulnerabilidades.
- A Internet das Coisas, com potencialmente bilhões de dispositivos conectados e novos aplicativos, introduz um novo nível de vulnerabilidade. Suas políticas de segurança atuais podem não abordar comunicações entre máquinas, e dispositivos conectados podem não estar protegidos por soluções de segurança tradicionais.
- Novos aplicativos podem apresentar vulnerabilidades e ter grandes falhas de segurança.

Não é surpresa que violações de segurança estejam ocorrendo com cada vez mais frequência. Para proteger seus dados sensíveis, você deve adotar uma nova abordagem baseada em risco.

O passo à frente

A IBM oferece uma variedade de software e serviços para ajudá-lo a proteger ativos críticos—desde controles e análise de segurança avançados até métodos comuns para reforçar seu programa de proteção de dados.

Como proteger ativos críticos:

- **Controle e administre usuários e seus acessos**: Valide "quem é quem" na empresa e na nuvem, e use controles focados no contexto e baseados em função para ajudar a evitar acessos não autorizado. Estes controles são inteligentes o suficiente para saber onde os usuários estão, o que eles desejam fazer e qual deve ser seu comportamento normal—tudo isso antes que eles tenham o acesso concedido. Procure por violações coletando dados relevantes para a segurança oriundos de toda a empresa. Implemente tecnologias de inteligência de segurança para análise em tempo real, prevenção contra a fraude e detecção de anomalias. Expanda sua perícia em segurança com inteligência de ameaça externa.

- **Identifique e proteja dados sensíveis**: Descubra e classifique ativos de dados críticos. Proteja estas informações com controles inteligentes que monitorem quem está acessando esses dados e a partir de onde. Detecte anomalias e acesso não autorizado. Procure por indicadores de ataque sutis usando recursos analíticos de segurança detalhados.
- **Gerencie o risco de segurança do aplicativo**: Analise as vulnerabilidades de segurança dos aplicativos antes que eles entrem em produção—evitando os custos de corrigi-los posteriormente e os danos em potencial de reparar as perdas das vítimas. Aborde a segurança desde o primeiro dia.

- **Gerencie e proteja sua rede e endpoints**: Imponha conformidade, bloqueie ameaças e corrija vulnerabilidades com visibilidade quase em tempo real.

Você está protegendo efetivamente a nuvem e os dispositivos móveis?

Sua organização adotou uma plataforma móvel, lançou iniciativas de mídia social ou adotou a computação em nuvem? Em caso afirmativo, você sabe que cada vez mais transações de negócios estão sendo levadas para fora da empresa. Um exemplo: conforme plataformas em nuvem continuam sendo adotadas, o perímetro tradicional em torno do datacenter está se dissolvendo, tornando difícil proteger dados críticos contra o aumento de brechas na segurança.

Além da nuvem, muitas empresas estão adotando políticas traga seu próprio dispositivo (BYOD) – bring your own device e outras iniciativas de mobilidade para engajar melhor funcionários e clientes. Mas, como as linhas entre vida pessoal e profissional se confundem, a segurança móvel está pagando o preço.

Se sua equipe de segurança foi surpreendida com estes desafios, você não está sozinho.

Os executivos de segurança têm várias preocupações com relação a estas novas iniciativas. Manter dados privados e seguros em um ambiente em nuvem agora é a preocupação principal dos CISOs.[4] Eles também temem o perigo do roubo e da perda de dispositivos móveis. De fato, 76 por cento dos CISOs vêem o roubo de dispositivo ou a perda de dados sensíveis em um dispositivo com grande preocupação.[4] Além disso, menos da metade dos líderes de segurança sentem que possuem uma abordagem efetiva de gerenciamento de dispositivos móveis. Existe uma lacuna clara entre as demandas de negócios e as realidades de segurança.[5]

O passo à frente

A IBM pode ajudar a sua empresa a evitar essa exposição. Temos especialistas que podem trabalhar com sua equipe de segurança para construir uma nova postura de segurança, mais forte, desenhada para iniciativas de nuvem e de dispositivos móveis. Lembre-se, é vital abordar a segurança no início da implementação das tecnologias de nuvem e de dispositivo móvel.

Maneiras de proteger a nuvem e dispositivos móveis:

- **Ganhe visibilidade e controle em nuvem**: Fortaleça cargas de trabalho e monitore a atividade de ataque enquanto suporta a conformidade na nuvem. O portfolio de soluções de segurança da IBM está preparado para nuvem. Isso significa que podemos ajudar a proteger os funcionários e clientes, dados, aplicativos e infraestrutura de sua empresa conforme você constrói sua nuvem privada. Trabalhamos com vários provedores de serviços de nuvem para construir segurança para suas ofertas.
- **Ajude a proteger a empresa móvel**: Proteja dispositivos, conteúdo, aplicativos e transações. Estes são os recursos mais solicitados por nossos clientes hoje para segurança móvel. Comprometa-se com a abordagem da segurança móvel desde o primeiro momento.
- **Adote um modelo de segurança de infraestrutura como serviço**: Aproveite a facilidade de uso, a disponibilidade global e a flexibilidade da segurança baseada em nuvem. Soluções hospedadas podem ajudar a reduzir os custos da manutenção de sua própria infraestrutura de segurança, enquanto também tratam da falta crescente de equipe de segurança qualificada.

A diferença da IBM Security

Ciberinvasores não são a ameaça número um para a segurança de uma empresa. Complacência e procrastinação são.

Atrasar uma auditoria de programa de segurança, postergar um upgrade importante para seu sistema de proteção contra ameaças, confundir conformidade regulatória com uma postura de segurança rígida—tudo isso é sinal de que você poderia se tornar vulnerável a um ataque que causaria danos à receita, reputação e sucesso de sua empresa. Você deve tratar questões de segurança o mais rápido possível, e é valioso ter um pioneiro no segmento de mercado mundial ao seu lado.

Na IBM, nossa nova abordagem de segurança é centralizada em três áreas principais:

- **Inteligência**: A inteligência em segurança é o elemento central do portfolio de soluções de segurança da IBM. A Segurança da IBM fornecer a análise e visibilidade detalhadas de que empresas como a sua precisam para ajudar a repelir uma ampla gama de ameaças.
- **Integração**: As soluções e serviços de Segurança IBM integram recursos de segurança novos e existentes entre domínios. Isto fornece visibilidade crítica, controles abrangentes e ajuda a reduzir a complexidade.
- **Conhecimento**: O conhecimento da IBM origina-se de mais de 6,000 profissionais e pesquisadores experientes que suportam clientes em mais de 130 países. Nosso insight profundo vem do monitoramento de mais de 270 milhões de endpoints e do gerenciamento de 15 bilhões de eventos todos os dias—e é construído acerca de produtos e serviços IBM, fornecidos via feeds de clientes em tempo real e integrados em compromissos profissionais.

Obtenha a defesa forte de que precisa contra ameaças novas e desconhecidas realizando parcerias com a IBM, um líder comprovado em segurança corporativa. Estamos comprometidos—por meio de investimentos em pesquisa e desenvolvimento, contratação e retenção dos melhores talentos, e liderança de ideias extensiva—em ajudá-lo a proteger sua organização. Nossa nova abordagem para segurança pode permitir que organizações como a sua inovem enquanto reduz o risco. Podemos fornecer um caminho para crescimento de seus negócios—enquanto ajudamos a proteger seus dados e processos mais críticos.

Para obter maiores informações

Para saber mais sobre o portfolio de soluções de Segurança IBM, entre em contato com seu representante da IBM ou Parceiro Comercial IBM, ou visite: **ibm.com**/security

[1] "Perdas de Lucro Líquido: Estimando o Custo Global do Cibercrime", Centro para Estudos Internacionais e Estratégicos/McAfee, Junho de 2014. http://www.mcafee.com/us/resources/reports/ rp-economic-impact-cybercrime2.pdf

[2] CEB Information Risk Leadership Council, "Previsão de Segurança 2015 - Dez Imperativos para a Função de Segurança da Informação," Novembro de 2014.

[3] Conselho Executivo Corporativo, "Respondendo a Ameaças Avançadas," Fevereiro de 2014.

[4] IBM MDI, "Pesquisa de Opinião do Chief Information Security Officer," 2013.

[5] IBM Center para Insights Aplicados, "Fortificando para o futuro: Insights da Avaliação do IBM Chief Information Security Officer 2014," 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

Recicle

IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Abril 2015

WGW03118-USEN-00