Uma Abordagem Abrangente sobre Segurança

Uma publicação do
IBM® Redbooks® Point-of-View
da IBM Academy of Technology

Por Chung-Sheng Li, Ph. D., Director IBM Research, **Katsumi Ohnishi**, IBM Executive Architect, e **Josuyla R. Rao**, Director IBM Research

Destaques

Adote uma abordagem de segurança ampla que antecipe e pare invasores antes de se infiltrarem em seu sistema:

- Altere o paradigma de segurança de uma defesa de perímetro tradicional para uma sequência contínua de segurança de baixa granularidade em um microperímetro.
- Empregue a defesa de microperímetro e inteligência de segurança, que são as chaves para tratar de ameaças emergentes em modelos de tendência de computação remota, social e em nuvem.
- Altere sua solução de produtos para uma abordagem de inteligência de segurança integrada e abrangente.
- Implemente a inteligência de segurança para minimizar riscos provenientes de um volume de dados em crescimento, proliferação de nuvens e usuários remotos e tecnologias da web.

O contexto atual de segurança

O ícone de segurança da área de trabalho de seu computador, normalmente com a forma de um escudo, representa um firewall pessoal. Ele protege contra ameaças e ataques e procura intrusos que violem a barreira. Embora essa proteção seja um bom exemplo de segurança de baixa granularidade, as organizações nem sempre estabelecem proteções semelhantes dentro dos limites de sua empresa. Como resultado, muitos servidores que são críticos aos negócios continuam confiando apenas em proteções de alta granularidade de firewalls corporativos e mecanismos de detecção e prevenção de intrusos.

Os negócios e governos de hoje devem assumir uma abordagem mais ampla para proteger as informações contra invasores ou infiltrados maliciosos. Essa tarefa não é fácil quando os usuários demandam acesso rápido e conveniente às informações que esperam que estejam protegidas. Como consequência, as organizações precisam cada vez mais de uma abordagem mais inteligente que confie em controle de baixa granularidade de privilégios de acesso e detecção de campo distante de ameaças potenciais e aparentemente não relacionadas. Tal abordagem deve também confiar em métodos de restrição de multicamada para isolar as intrusões e minimizar o dano.

O dilema dos negócios é que eles devem permitir acesso aos seus sistemas para possibilitar tarefas e serviços ao mesmo tempo em que protegem recurso de informações. No entanto, os riscos continuam crescendo. Por exemplo, os volumes de dados estão constantemente crescendo. Os usuários de nuvem, dispositivo móvel e de telecomutação acessam redes com diversos dispositivos a partir de vários locais. Os aplicativos cada vez mais usam a Internet para colaborarem e se comunicarem. E, usando tecnologias da Web 2.0, os usuários de fora dos negócios podem acessar dados e controles. Todos esses riscos ilustram que a violação de segurança pode ocorrer em qualquer lugar e potencialmente criar um efeito cascata com reverberações globais.

A resposta a tais riscos foi construir grandes firewalls para proteger toda a empresa. No entanto, agora a tendência é proteger todos os recursos dentro da rede. Tais recursos incluem servidores, middleware, armazenamento, arquitetura orientada a serviços, aplicativos e informações, cada um deles pode ter valores estratégicos diferentes.

Reagir a violações de segurança não é o suficiente para proteger as informações, redes e o corporativo de um negócio. Você deve antecipar e se proteger contra ataques maliciosos antes de eles ocorrerem. Para estar preparado, você precisa ver a segurança como uma consequência que se correlaciona entre eventos físicos e virtuais, entre eventos aparentemente

inofensivos e suspeitos e entre atividades locais e globais. Você deve adotar o conhecimento de segurança usado por comunidades de inteligência e aplicação da lei. Nessas comunidades, as pistas para impedir eventos, como um diálogo de um terrorista online antes de uma taque, são escrupulosamente reunidas e analisadas.

Persistência de ameaças em diferentes níveis

Os negócios estão em risco de ameaças internas e externas, conforme mostrado em Figura 1.

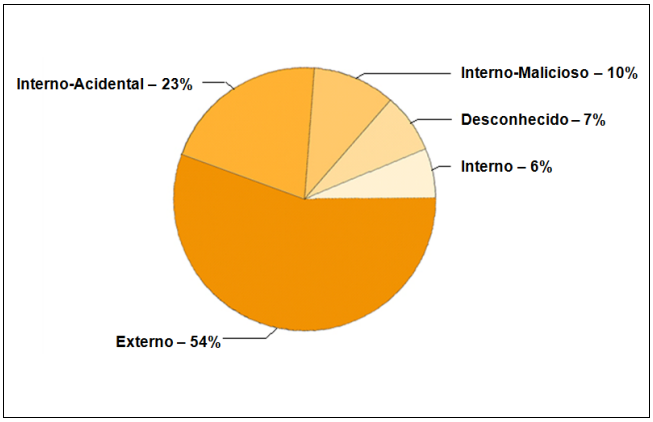

Figura 1 Porcentagens de incidente de ataque

As ameaças internas incluem tentativas maliciosas de pessoas internas e tentativas não intencionais de violar a segurança com malcode, vazamento de dados ou roubo de dados valiosos, entrando por meio dos pontos vulneráveis do sistema. As ameaças externas incluem negação de serviço (DoS), vandalismo e propaganda na web, botnets (grupos de computadores comprometidos que executam software de ataque) e interrupção de equipamento. Também incluem ataques à infraestrutura crítica, como grades de energia e sistemas de combustível, comunicação e transporte.

As medidas de segurança para evitar ameaças incluem a verificação de antecedentes dos usuários, acesso restrito, monitoramento físico, monitoramento de integridade da plataforma, controles da área de trabalho e a definição de perfis e auditoria das interações dos usuários. Essas medidas também incluem a detecção e prevenção de transferência de dados sensíveis para um site externo desautorizado.

Outras ameaças incluem injeção de SQL, phishing e ameaças persistentes avançadas (APT), que têm sido experienciadas por muitas empresas famosas. Uma APT é o ataque mais grave aos ativos de negócios, devido à sua progressão em estágios ao longo do tempo.

O progresso de um APT acontece da seguinte forma:

1. Os invasores usam a mídia social para enviar emails aparentemente inocentes. Essa técnica é conhecida como *phishing*. Os emails contêm anexos ou aplicativos ocultos que entram pela segurança. Esses aplicativos são chamados de *malware*.
2. O malware instala ferramentas que permitem que o invasor tenha acesso remoto para controlar os servidores e computadores por trás do firewall.
3. O malware coleta as credenciais do usuário. Então, ele vai para os usuários privilegiados e, finalmente, para os destinos de alto valor.
4. O malware estabelece acesso a servidores de temporariedade em pontos principais.
5. O invasor transfere dados sensíveis para um servidor de temporariedade externo, em uma máquina comprometida externa.

Tradicionalmente, os negócios respondem a tais ameaças reforçando o perímetro de defesa nos limites da organização. Essa abordagem tem se tornado cada vez menos efetiva devido à necessidade de conduzir os negócios além do perímetro. Além disso, ela não resolve as ameaças de violadores internos.

Em 2008, pela primeira vez, um violador interno superou as violações externas, desafiando uma defesa tradicional baseada em perímetro em segurança cibernética.

Como você se prepara e gerencia riscos afeta de forma crítica seus resultados, por exemplo, em termos de custos, sucesso e efetividade. A escolha da melhor proteção para seus ativos de dados pode ser confusa considerando a proliferação de abordagens e produtos de segurança.

A necessidade de uma solução de maior alcance

Por décadas, os negócios confiaram na IBM com suas redes, dados e sistemas, esperando qualidade, desempenho e tecnologia de ponta. Agora, esperam o mesmo para a segurança de ativos. Para atender a esta demanda de mercado, a IBM muda de uma abordagem de produto para uma abordagem corporativa integrada para a inteligência da segurança. Esta abordagem está baseada nos principais elementos que permitem um gerenciamento ativo, informações em tempo real, correlação analítica e gerenciamento de ameaça previsível.

O modelo de inteligência de segurança da IBM abrange todo o escopo de preocupações com a segurança, desde a conformidade até a infraestrutura. A estrutura do modelo ajuda a identificar, prever e remediar ameaças de TI e riscos corporativos e atingir a conformidade. Os recursos de segurança da estrutura usam ciclos de planejar-executar- verificar-agir (PDCA). Esses ciclos se baseiam no princípio de *defesa em profundidade*, que é uma abordagem estruturada em camadas de educação, prevenção, detecção e remediação de segurança. A solução da IBM foi construída por milhares de pesquisadores, desenvolvedores, consultores e especialistas no assunto em iniciativas de segurança. E mais, a IBM ofereceu consultoria e implementou milhares de projetos de segurança, o que resultou em conhecimento prático nas melhores práticas e processos.

A estrutura de segurança

A inteligência de segurança, que é a arte e ciência de antecipar, monitorar e analisar riscos antes de eles ocorrerem, é uma tendência do mercado atual. A inteligência de segurança fornece visibilidade unificada e analítica em tempo real a partir de dispositivos de rede e de segurança para sistemas operacionais, aplicativos, terminais e recursos de infraestrutura de servidores. A inteligência de segurança envolve os seguintes aspectos principais, cada um deles envolvendo um nível básico e um nível ideal, ou de uma posição reativa para uma reação proativa:

- *Pessoas*, que vão de um diretório centralizado para provisionamento de usuário com forte autenticação, para analítica baseada em função, governança de identidade e controles de usuário privilegiado.
- *Dados*, que desenvolvem de criptografia, controles de acesso, monitoramento de acesso e prevenção de perda de dados até analítica de fluxo de dados e governança de dados. O cálculo social é cada vez mais importante na interceptação de vazamentos de dados e ataques de phishing.
- *Aplicativos*, que vão de varredura, firewall e varredura de código-fonte de aplicativo até processos de engenharia de aplicativo seguro e detecção de fraudes.
- *Infraestrutura*, que abrange desde defesa de perímetro por antivírus alta granularidade e gerenciamento de segurança de terminal e rede (detecção e prevenção de intrusão e inspeção profunda de pacotes) até monitoramento, perícia e mineração de dados de rede avançados.

Pontos principais da solução para inteligência de segurança

A IBM foca em quatro áreas principais na entrega de inteligência de segurança: ameaças avançadas, computação em nuvem, computação remota, regulamentação e conformidade.

As ameaças avançadas, ou APTs, são ataques direcionados sofisticados que são projetados para obter acesso contínuo a informações críticas. Essas ameaças estão se tornando mais graves e mais frequentes. A solução é uma forte camada de rede que integre segurança, analítica e inteligência de ameaça, além de fatores humanos e sociais, pois ataques avançados normalmente começam como ataques phishing.

Ao consolidar dados massivos, as soluções de inteligência de segurança fornecem insight mais profundo para defender contra diversas ameaças, incluindo APT. A solução de gerenciamento de informações de segurança e eventos IBM (SIEM) ajuda a distinguir ameaças reais de “barulho.” Ela também ajuda a reduzir alertas de positivo falso usando dados mais contextuais e análise mais inteligente.

A maioria dos negócios entendem que precisam aproveitar a computação em nuvem, mas ainda se preocupam com os riscos em potencial. Como provedor de serviços e de segurança, a IBM está bem posicionada para fornecer uma infraestrutura segura na nuvem e em plataformas para isolar as informações em datacenters e nuvens seguros.

De acordo com a Gartner, Inc., 90% dos negócios suportarão aplicativos corporativos em dispositivos remotos até 2014.[1] Para acompanhar este ambiente de trabalho expandido, a principal preocupação da maioria dos CIOs é fornecer aos funcionários acesso amplo e, ao mesmo tempo, proteger seus dispositivos remotos. A IBM foca em acesso seguro a dados corporativos enquanto suporta a privacidade e oferece recursos de segurança abrangentes entre terminal, gateway e desenvolvimento de aplicativos. A IBM também oferece produtos para integrar e entregar gerenciamento de dispositivo remoto e fornece controle de acesso e identidade federada aos aplicativos e sistemas do usuário.

É necessária uma abordagem expansiva que antecipe, monitore e analise riscos antes que eles ocorram.

Os negócios investem muitos esforços na conformidade com requisitos regulamentares do governo e do segmento de mercado, normalmente por preços cada vez maiores. Com a ajuda da IBM, os negócios podem mapear os regulamentos em sua infraestrutura de TI e de negócios, o que pode reduzir custos, simplificar a complexidade do sistema, automatizar a configuração e simplificar o monitoramento, auditoria e geração de relatórios. A IBM oferece produtos que fornecem criação de log e correlação confiáveis e que executam funções de orquestração, analítica e de painel.

Mais sobre a inteligência de segurança

Apenas construir suas defesas de perímetro não protege seus negócios. Usando os produtos e serviços na estrutura de segurança da IBM, ilustrada em Figura 2, a IBM pode ajudar a prever, identificar e remediar ameaças e atingir a conformidade. Para alcançar esses objetivos, a IBM oferece produtos e serviços os domínios de infraestrutura de TI de pessoas, dados, aplicativos e infraestrutura, além de serviços de conformidade e segurança.

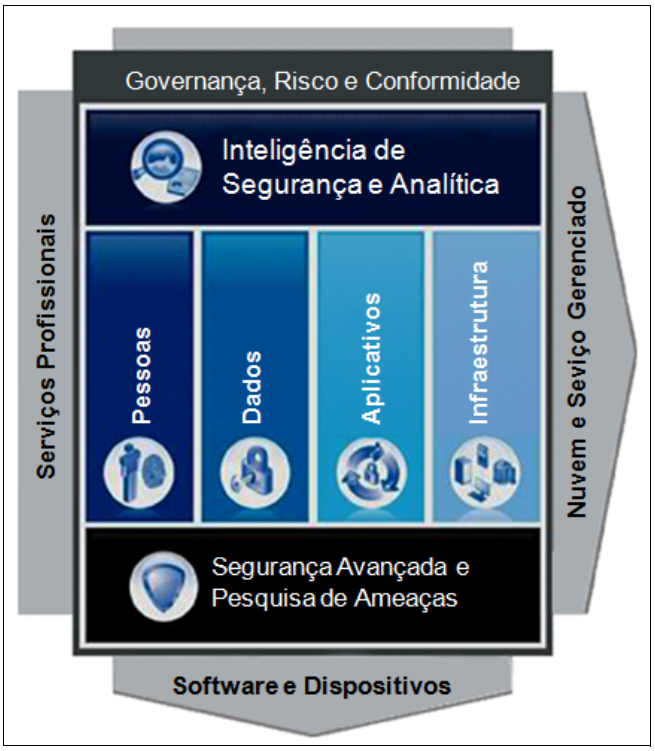

Figura 2 Estrutura de segurança da IBM

A IBM oferece inteligência de segurança completa com um leque completo de serviços e produtos para os principais domínios de negócios:

- Pessoas. A IBM fornece serviços para avaliação de identidade, analítica baseada em função, controles de usuário, implementação e hospedagem usando os produtos a seguir:
  - IBM Tivoli Identity and Access
  - IBM Tivoli Federated ID
  - IBM Tivoli Single Sign-on
- Dados. A IBM fornece serviços para avaliação, criptografia, implementação de prevenção de perda de dados (DLP), analítica de fluxo e governança usando os produtos a seguir:
  - IBM InfoSphere® Guardium®
  - IBM InfoSphere Optim™ Data Masking
  - Criptografia de fita e disco
  - IBM Tivoli® Key Manager
- Aplicativos. A IBM fornece serviços para avaliação, processos de engenharia segura e detecção de fraude usando os produtos a seguir:
  - IBM Rational® AppScan® Source Edition
  - IBM Rational AppScan Standard Edition
  - IBM Tivoli Security Policy Manager

[1] Gartner Newsroom
http://www.gartner.com/it/page.jsp?id=1480514

- Infraestrutura. A IBM fornece serviços para segurança de rede (detecção e prevenção de intrusão e inspeção profunda de pacote), perícia, mineração de dados, teste de penetração, firewall, sistemas de prevenção de intrusão, serviços d e gerente de vulnerabilidade e proteção remota gerenciada, usando os produtos a seguir:
  - IBM Tivoli Network Intrusion Prevention
  - IBM WebSphere® DataPower® XML Gateway
  - IBM Tivoli Endpoint Manager (antivírus usando Trend Micro)
  - IBM Security zSecure™ segurança de mainframe

O que está por vir: Como a IBM pode ajudar

Para ajudá-lo a implementar a inteligência de segurança, a IBM oferece os serviços da equipe do IBM X-Force® Research and Development, que é uma das equipes de pesquisa e desenvolvimento de segurança comercial mais reconhecidas do mundo. Essa equipe estuda e monitora as tendências de ameaça mais recentes, incluindo vulnerabilidades, explorações e ataques ativos, vírus e outro malware, spam, phishing e conteúdo da web malicioso. Além de avisar os clientes e o público geral sobre como responder a ameaças emergenciais e críticas, a equipe do X-Force também oferece conteúdo de segurança para proteger clientes da IBM dessas ameaças.

A equipe do X-Force publica, bianualmente, o IBM X-Force Trend and Risk Report, que ajuda os clientes, pesquisadores e o público a entender os riscos de segurança mais frequentes e ficar à frente de ameaças emergentes. O relatório explorar minuciosamente os desafios mais significativos que são enfrentados pelos profissionais de segurança de hoje. Para obter o IBM X-Force Trend and Risk Reports, acesse:

ibm.com/security/xforce/downloads.html

Além da equipe do IBM X-Force, os serviços e produtos IBM oferecem uma solução completa que pode ajudar a defender seus dados, aplicativos e infraestrutura contra ataques, proteger seus recursos de informações e permitir acesso seguro aos usuários.

Recursos para Obter Mais Informações

Para obter mais informações sobre os conceitos destacados neste documento, consulte os recursos a seguir:

- Publicações de IBM Redbooks sobre segurança

  http://www.redbooks.ibm.com/Redbooks.nsf/portals/Security?Open&count=20

- IBM X-Force Trend and Risk Reports

  ibm.com/security/xforce/downloads.html

- IBM Institute for Advanced Security

  http://instituteforadvancedsecurity.com/default.aspx•

- *Security in Development: The IBM Secure Engineering Framework*, REDP-4641

  http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf

Avisos

Essas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do usuário.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses Web sites não fazem parte dos materiais deste produto IBM e a utilização desses Web sites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o cliente.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente aos seus fornecedores.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas.

O documento REDP-4944-00, foi criado ou atualizado em November 21, 2013.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Estes e outros termos de marca registrada IBM são marcados em sua primeira ocorrência nessas informações com o símbolo apropriado (ou), que indica marca registrada de direito comum ou marca registrada nos Estados Unidos de propriedade da IBM no momento em que as informações foram publicadas. Tais marcas registradas também podem ser marcas registradas ou de direito comum em outros países. Uma lista atual das marcas registradas IBM está disponível na Web, no endereço
`ibm.com/legal/copytrade.shtml`

Os termos a seguir são marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AppScan®
DataPower®
Guardium®
IBM®
InfoSphere®
Optim™
Rational®
Redbooks®
Redbooks (logotipo) ®
Tivoli®
WebSphere®
X-Force®
zSecure™

Os termos a seguir são marcas registradas de outras empresas:

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviço de terceiros.