IBM Security

Agente mal intencionado ou usuário legítimo? As ameaças que vêm de dentro são as mais difíceis de combater.

Os agressores são inteligentes, ágeis e com frequência aparentam ser quem não são, tornando os insights de segurança mais importantes que nunca.

IBM Security
White Paper

Seus usuários internos: Os negócios precisam de confiança. Mas a segurança exige cuidados.

Uma empresa precisa confiar em seus funcionários, parceiros e fornecedores. Os negócios simplesmente não acontecem sem eles. Mas quando esses usuários internos confiáveis acessam seus recursos digitais valiosos, você precisa saber quem eles são e o que estão fazendo, além de saber se recursos foram comprometidos. Sem esses insights, os riscos de roubo de dados ou comprometimento de aplicativos podem ser desnecessariamente altos.

Considere: A média de custo de uma violação de dados empresariais é de US$ 3,26 milhões.[1] Até 60% dos ataques são atribuídos a usuários internos.[2] Os números são impressionantes. Mas a redução desse perigo é ignorada por muitas empresas.

Isso acontece porque o estereótipo de um usuário interno que representa ameaça (um funcionário insatisfeito buscando vingança ou lucros) não é necessariamente verdadeiro. As pessoas podem ser descuidadas. Podem ser facilmente enganadas por esquemas de engenharia social bem executados. Enquanto trabalham para manter a produtividade, podem acabar comprometendo a segurança. No setor de serviços financeiros, por exemplo, o número de ameaças de ações involuntárias de usuários internos é 10 vezes maior que o de ações maliciosas de usuários internos.[3]

A configuração inadequada do servidor pelos administradores dos seus sistemas pode criar uma vulnerabilidade fácil de explorar. E ainda com mais frequência, o clique de seu contador em um e-mail de spear phishing pode resultar no roubo de credenciais. Isso pode abrir a porta para criminosos digitais entrarem livremente na sua infraestrutura e permanecer nela por um longo tempo, sem serem detectados, porque os agressores parecem ser usuários legítimos.

e simplesmente descuidados, ou ainda disfarçados e inteligentes. Será possível combatê-los apenas identificando o que fazem, ao analisar o comportamento para descobrir as ações que diferem da norma. Após ter esse insight, é possível identificar essas ameaças, tomar medidas para bloquear ações futuras e se recuperar dos danos que elas possam ter causado.

60%

dos ataques virtuais são atribuídos a usuários internos.[2]

Saiba mais no 2017 IBM® X-Force® Threat Intelligence Index

1 "2017 Cost of Data Breach Study: Global Overview," *Ponemon Institute*, junho de 2017.
2 "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," *IBM X-Force Research: 2016 Cyber Security Intelligence Index*, abril de 2016.
3 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, março de 2017.

Sinais de perigo: Fique atento a essas ações de usuários

Ameaças internas tratam menos de invadir a infraestrutura e mais de já estar dentro dela. É claro que a entrada aconteceu de alguma forma: seja simples como um erro por falta de treinamento de funcionários ou de forma sofisticada como uma campanha de spear phishing que rouba credenciais. Mas o que torna essas ameaças tão difíceis de descobrir e lidar é o fato de o agente já ter acesso e agir de forma despercebida.

O que você deve procurar? Existem três sinais reveladores:

Roubo e corrupção: Usuários internos apresentam um mau comportamento

- O acesso e os downloads de ativos de alto valor ocorrem com mais frequência que o normal
- Uso de uma conta pela primeira vez em muito tempo, ou de uma nova localização pela primeira vez
- Atividade de usuário muito diferente do normal por um período curto ou que muda gradativamente por um período estendido
- Padrões de atividade que são diferentes dos padrões de atividades dos colegas de um usuário

Erros prejudiciais: Usuários internos que agem de forma descuidada

- Configuração inadequada das ferramentas de segurança da organização
- Alterações nos atributos de outras pessoas sem solicitar permissão
- Usuários que abrem contas pessoais em servidores da empresa
- Usuários que compartilham credenciais de redes virtuais privadas
- Prestadores de serviços que verificam mensagens e e-mails por meio de um provedor terceirizado, especialmente de outros países
- Usuários que se conectam a um servidor em nuvem ou conta pessoal em um serviço de compartilhamento de arquivos

Brechas para usuários externos: Invasão dos criminosos digitais

- Números maiores de transferências de dados para e de servidores e/ou locais externos
- Números maiores que os esperados de logins de contas de máquinas
- Tentativas de alterar privilégios de uma conta existente ou de abrir novas contas

81%

dos ataques de usuários internos usaram credenciais de outra pessoa para evitar controles ou obter direitos elevados.[1]

Assista ao vídeo da IBM para saber mais sobre como identificar ameaças de usuários internos

1 "Ponemon Survey Indicates the Growing Threat of Insider Fraud Not a Top Security Priority for Organizations, Proves a Costly Mistake," *Ponemon Institute*, 28 de fevereiro de 2013

Ação necessária: Adicione ferramentas poderosas ao seu kit

O vazamento de dados comerciais sigilosos devido a ações involuntárias de usuários internos (agravado pela possibilidade de essas ações gerarem roubo em grande escala e uso inadequado de aplicativos por criminosos digitais que usam malware e bots) é uma enorme preocupação para as empresas atuais.

O desafio é que, sem as ferramentas analíticas certas, não há forma de diferenciar funcionários bem intencionados de agentes externos maliciosos que operam de forma disfarçada. Até que seja tarde demais. O número reduzido de funcionários nos centros de operações de segurança (SOCs) também agrava a situação. Embora a maioria das organizações implementem soluções de segurança, muitas dessas medidas se concentram em manter os invasores fora dos sistemas.

Como resultado, para lidar com ameaças que já estão dentro da organização, os SOCs precisam de uma nova abordagem. São necessários recursos que permitam a detecção de ameaças de usuários internos de forma mais rápida, contendo ataques com agilidade e limitando o impacto do incidente, e tudo isso enquanto equilibra a segurança com a confiança e privilégios de acesso oferecidos aos usuários legítimos.

Basicamente, combater ameaças de usuários internos exige três recursos fundamentais:

- **Recursos analíticos de segurança:** ferramentas que reúnam uma ampla variedade de dados de segurança e feeds de ameaças para automatizar a detecção de ameaças e facilitar a investigação e a resposta
- **Inteligência de ameaças:** feeds de dados de fontes externas confiáveis que fornecem insights globais constantemente atualizados de atividades de entidades maliciosas
- **Busca por ameaças:** investigações eficazes que estão constantemente procurando não apenas ataques, mas também vulnerabilidades que dão espaço a esses ataques

Com recursos fundamentais estabelecidos, os analistas dos SOCs podem realizar ações direcionadas contra ameaças de usuários internos, por exemplo, usando dados de fluxo para detectar anomalias no comportamento de usuários, estabelecer limites para o risco de cada usuário e bloquear acesso de usuários, se necessário. O SOC pode simplificar investigações, melhorar a visibilidade e responder de forma mais rápida a ameaças usando melhores práticas.

"(...) ataques de usuários internos voltados a serviços financeiros e de cuidados com a saúde foram em grande parte ações involuntárias (...) de usuários com uma maior probabilidade de sofrer ataques de phishing. As organizações (...) devem se concentrar em educar os funcionários sobre phishing e formas de evitar que sejam vítimas desses ataques (...)"[1]

Saiba mais na web sobre a abordagem integrada da IBM para combater ameaças de usuários internos.

1 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, março de 2017.

Por que a IBM? Uma abordagem integrada ajuda a manter sua segurança.

Para uma melhor detecção de ameaças internas, a IBM oferece uma abordagem desenvolvida para aprimorar a capacidade dos SOCs de monitorar usuários e investigar atividades suspeitas. Com base no IBM QRadar® Security Intelligence Platform, um mecanismo de análise de dados que coleta dados de segurança continuamente, esta abordagem cria uma linha de base de padrões de comportamento de usuários e perfis de atividades, e então usa algoritmos para detectar anomalias e desvios.

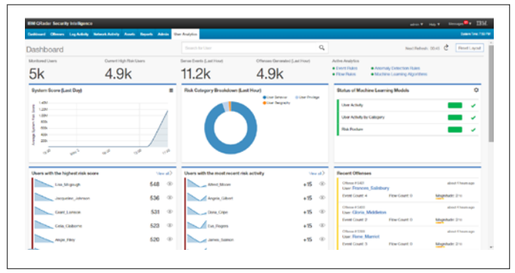
Para atender a demandas específicas de combate a ameaças internas, a plataforma do QRadar pode ser expandida com duas soluções de plug-in, ambas disponíveis para download no IBM Security App Exchange.

- O **IBM QRadar User Behavior Analytics** oferece uma abordagem fácil de usar que implementa aprendizado de máquina, análise de comportamento de usuários individuais e análise de comportamento de grupos de usuários para detectar atividades anômalas e atribuir pontuações de riscos para indivíduos com base em ações. Seu painel é integrado diretamente ao console do IBM QRadar SIEM e permite que analistas vejam usuários de alto risco a qualquer momento, determinando ações de segurança necessárias.

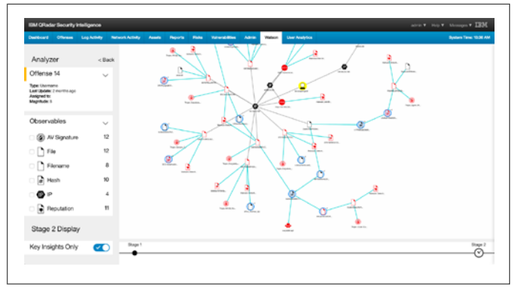
- O **IBM QRadar Advisor with Watson™** utiliza recursos cognitivos para investigar as informações recebidas do QRadar User Behavior Analytics, qualificar o incidente e identificar a causa-raiz. Operando com velocidade 60 vezes maior que as investigações manuais,[1] ele utiliza fontes estruturadas e não estruturadas para fornecer contexto e escopo para o ataque.

A solução também pode ser integrada ao IBM Security Identity Governance and Intelligence para revogar automaticamente o acesso de usuários quando uma atividade de alto risco for detectada. E pode ser integrada com o IBM i2® Analyze para permitir que equipes de segurança mapeiem visualmente dados relevantes para um incidente e compartilhem com facilidade análises de dados com membros da equipe

Clique na imagem para ampliá-la.
Clique novamente para ver no tamanho original.



IBM QRadar User Behavior Analytics



IBM QRadar Advisor with Watson

- Leia mais sobre como o IBM QRadar ajuda organizações a detectar e investigar ameaças de usuários internos.
- Faça o download do aplicativo QRadar User Behavior Analytics no IBM Security App Exchange.
- Faça o download de uma avaliação gratuita de 30 dias do QRadar Advisor with Watson.

1 Resultados observados por clientes que participaram do programa de teste beta do QRadar Advisor with Watson.

Para obter mais informações

Para saber mais sobre o QRadar, entre em contato com o representante da IBM ou o Parceiro Comercial IBM, ou visite: **ibm.com**/security/qradar/

Sobre as soluções do IBM Security

O IBM Security oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança corporativa. O portfólio, apoiado pela pesquisa e desenvolvimento de renome mundial X-Force, fornece inteligência de segurança para ajudar as organizações a proteger integralmente seus funcionários, infraestruturas, dados e aplicativos, oferecendo soluções para gerenciamento de identidade e de acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de risco, gerenciamento de endpoint, segurança de rede e muito mais. Essas soluções permitem que as organizações gerenciem efetivamente os riscos e implementem segurança integrada para dispositivos móveis, nuvem, redes sociais e outras arquiteturas empresariais de negócios. A IBM opera uma das organizações mais amplas 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, o IBM Global Financing oferece várias opções de pagamento para ajudá-lo a adquirir a tecnologia de que você precisa para expandir sua empresa. Nós fornecemos gerenciamento completo do ciclo de vida de produtos e de serviços de TI, desde a aquisição até o descarte. Para obter mais informações, acesse: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produzido nos Estados Unidos da América
Setembro de 2017

WGW03340-USEN-00