X-Force

Relatório de ameaças de segurança internas IBM Security X-Force 2021

IBM Security X-Force Threat Intelligence

Relatório de inteligência especial 2º trimestre 2021

IBM

Índice

Introdução 03
Principais resultados da pesquisa 04

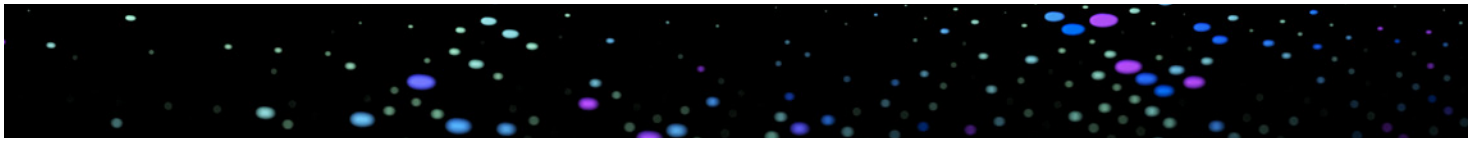
Seção 1
Como são descobertos os ataques provenientes de ameaças internas 05

Seção 2
Ausência de evidências e incógnitas na pesquisa do X-Force 07

Seção 3
Acesso privilegiado *versus* acesso administrativo 08

Seção 4
Quem vigia os vigilantes? 09

Seção 5
Recomendações 13



Introdução

O cenário de ameaças cibernéticas está em constante mudança, pois tanto os invasores quanto os defensores investem em novas tecnologias e processos. As organizações gastam um valor global aproximado de US$ 60 bilhões por ano para defender seus ativos e recrutar talentos para prevenir e reagir a ataques, ao passo que os gastos com segurança aumentaram 10% em 2021.[1]

Enquanto grande parte do foco e dos gastos de uma organização destina-se a impedir ataques provenientes de fora da própria empresa, muitas vezes as ameaças internas são negligenciadas: aquelas que vêm de dentro da organização. As ameaças internas, frequentemente acidentais ou não maliciosas, têm o potencial de causar danos devastadores na forma de furto de dados, perda financeira, furto de propriedade intelectual e danos à reputação. Em uma pesquisa de 2020, o Ponemon Institute estimou que as organizações gastam, em média, US$ 644.852 para se recuperar de um incidente oriundo de uma ameaça interna, independentemente da origem do incidente.[2] Isto inclui o custo de monitoramento e investigação de suspeitas de ocorrências internas e a resposta ao incidente, contenção, erradicação e remediação de um incidente interno.

No âmbito deste documento, o IBM Security X-Force define o usuário interno (insider) como:

— O usuário interno acidental: um funcionário ou fornecedor/prestador de serviços terceirizado negligente.[3]

— O usuário interno malicioso: um funcionário ou fornecedor/prestador de serviços terceirizado criminoso ou malicioso.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. Define-se o usuário interno negligente como um usuário que involuntariamente causa um incidente que afeta a confidencialidade, integridade ou disponibilidade de dados ou sistemas dentro de uma organização. Isto não inclui incidentes de phishing/engenharia social.

Usando dados proprietários exclusivos adquiridos a partir de investigações reais de resposta a incidentes, o X-Force analisou suspeitas de incidentes com ameaças internas — tanto acidentais como maliciosas — que afetaram as organizações de 2018 a 2020. Juntamente com os relatórios de código aberto dos mais proeminentes ataques perpetrados por membros internos, este documento examinará as descobertas críticas a partir desses dados, tais como:

— Como é descoberta a maioria dos ataques dos usuários internos.

— O papel desempenhado pelo nível de acesso nos ataques de usuários internos.

— Melhores práticas para atenuar as ameaças internas.

Principais resultados da pesquisa

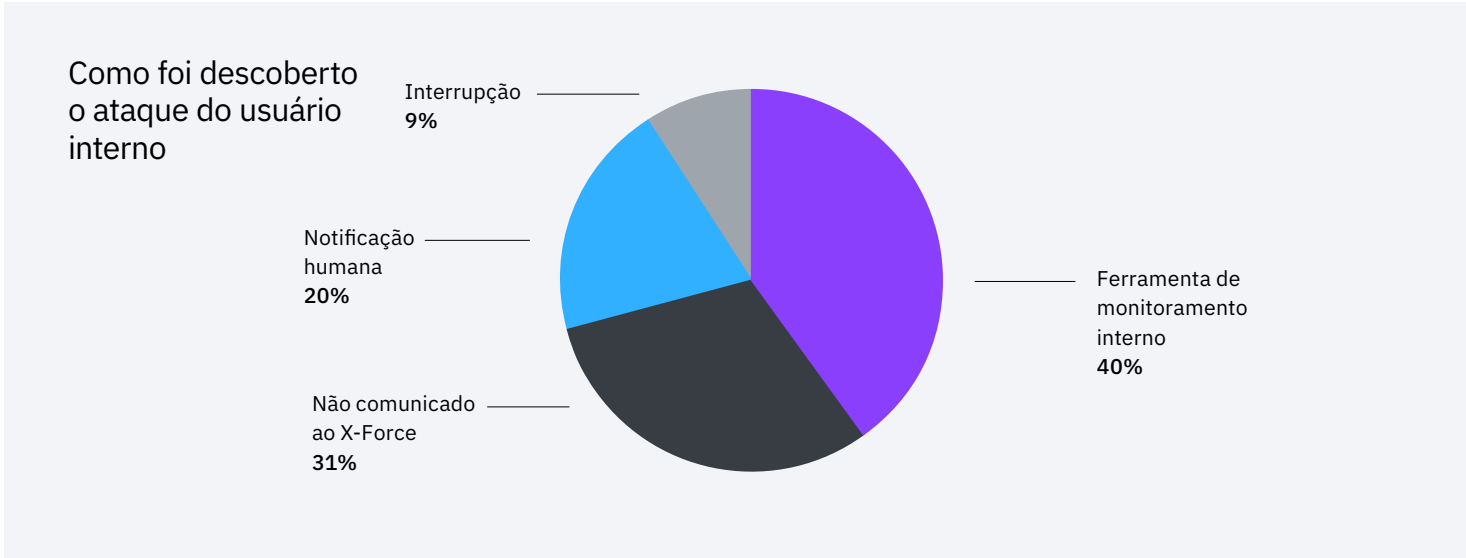
40% dos incidentes foram detectados por meio de alertas gerados por uma ferramenta de monitoramento interno.

40% dos incidentes envolveram um funcionário com acesso privilegiado aos ativos da empresa.

Em 100% dos incidentes nos quais o usuário interno foi confirmado ou provavelmente teve acesso administrativo, esse nível elevado de acesso contribuiu para o incidente.

Como são descobertos os ataques provenientes de ameaças internas

Ameaças internas geralmente são definidas como ataques nos quais usuários legítimos com algum nível de acesso aos ativos da empresa aproveitam esse acesso, de forma maliciosa ou acidental e acabam causando danos à organização. Esta ameaça pode vir de um funcionário atual ou antigo, bem como de um prestador de serviços terceirizado ou fornecedor que tenha acesso para exercer uma função comercial específica.



Uma análise das ameaças internas às quais o X-Force tem respondido desde 2018 revela que 40% desses incidentes foram detectados por meio de alertas gerados por uma ferramenta de monitoramento interno. Notificações humanas, por exemplo de funcionários que alertam a organização sobre atividades anômalas, representaram 20% das detecções, e uma interrupção do sistema alertou as equipes de segurança em 9% dos casos.

No 2020 Cost of Insider Threats: Global Report gerado pelo Ponemon Institute, patrocinado pela ObserveIT e pela IBM, estima-se que ferramentas como a análise comportamental do usuário (UBA), Gerenciamento de acesso privilegiado (PAM), Informações de segurança e gestão de eventos (SIEM) e programas como o compartilhamento de informações sobre ameaças e o treinamento e conscientização dos usuários pouparam às organizações uma média de 3 milhões de dólares em termos de redução ou eliminação de riscos internos.[4]

Economia de custos de 3 milhões de dólares

Estima-se que ferramentas como UBA, PAM, SIEMs e programas como o compartilhamento de informações sobre ameaças e o treinamento e conscientização dos usuários pouparam às organizações uma média de 3 milhões de dólares em termos de redução ou eliminação de riscos internos.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

Ausência de evidências e incógnitas na pesquisa do X-Force

Com relação aos incidentes internos nos quais o método de descoberta não foi "relatado ao X-Force" ou "ausência de evidências", as equipes de resposta aos incidentes do X-Force não receberam informações suficientes para tomar uma decisão sobre a descoberta. Isto se deve muitas vezes à falta de visibilidade de muitas organizações sobre como é seu ambiente padrão e como ele funciona. Para detectar atividade anômala dentro de qualquer sistema, é fundamental entender como é a atividade normal para que essas atividades anormais possam ser mais facilmente detectadas com confiança. Em 2019, a IBM patrocinou um relatório SANS[5] analisando o cenário de ameaças avançadas às organizações. Essa pesquisa demonstrou que:

— 48% das organizações consideraram a falta de visibilidade em sua infraestrutura como a principal lacuna em termos de segurança.

— 35% sentiram que lhes faltava a capacidade de detectar o uso indevido por parte de usuários internos da empresa.

— 47% das organizações admitiram não ter a capacidade de entender como era a atividade normal de referência dentro de suas redes.

5. https://www.ibm.com/account/reg/br-pt/signup?formid=urx-39989

Acesso privilegiado *versus* acesso administrativo

O X-Force classificou dois tipos diferentes de usuários ao analisar incidentes relacionados a ameaças internas.

Define-se um **usuário privilegiado** como alguém dentro da organização com acesso a dados sigilosos. Esses dados podem ser propriedade intelectual, dados de clientes ou informações de RH. Estes usuários também podem ser aqueles com acesso a informações corporativas sigilosas, como dados de fusões e aquisições ou outras informações legais.

Define-se usuários com **acesso administrativo**, também conhecidos como administradores ou admins, como pessoas com acesso elevado aos sistemas de TI dentro da rede. Teoricamente, esse tipo de acesso não deve se sobrepor. Entretanto, o X-Force descobriu que os usuários finais podem geralmente ser excessivamente provisionados em seus ambientes de TI.

Os membros internos com acesso administrativo são diferentes daqueles com acesso confidencial a um ambiente corporativo. Estes incluem funcionários, prestadores de serviços/fornecedores com acesso ao ambiente de TI da organização e apresentam um risco único para uma organização com base em seus elevados privilégios de rede.

Exemplos de funções com acesso privilegiado

- Funções de RH
- Executivos seniores
- Funções financeiras
- Funções jurídicas
- Cargos de pesquisa
- Outras funções com acesso à propriedade intelectual de uma organização ou "joias da coroa" ou dados dos clientes

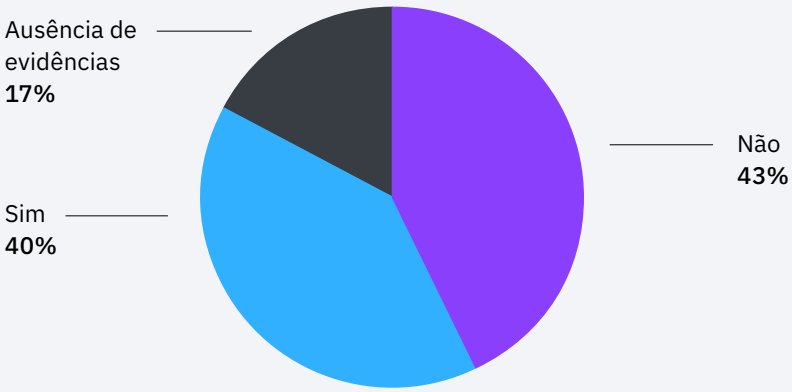
Exemplos de funções com acesso administrativo

- Administradores do servidor
- Administradores de TI
- Helpdesk (suporte)
- Fornecedores de TI externos
- Outras funções que são capazes de modificar configurações/parâmetros em sistemas de TI

Quem vigia os vigilantes?

Os usuários internos que causam incidentes costumam ter acesso privilegiado? A resposta em uma palavra é sim.

O usuário interno teve acesso privilegiado aos dados?



A análise dos dados do X-Force mostra que 40% dos incidentes provocados por membros internos envolveram um funcionário com acesso privilegiado a ativos sigilosos da empresa. Para esta pesquisa, o X-Force classificou o acesso privilegiado como pessoas que trabalham em áreas que incluem o departamento de TI, recursos humanos, finanças, segurança ou cargos executivos.

Nos outros 17% dos dados, não ficou claro se o usuário interno tinha ou não acesso privilegiado a dados sensíveis, o que significa que o número de incidentes causados por usuários com acesso privilegiado poderia ter sido substancialmente maior.

Os indivíduos com acesso elevado a ativos críticos, tais como ações de rede, dispositivos de segurança, sistemas de e-mail, informações pessoais identificáveis de funcionários ou clientes (PII), propriedade intelectual ou dados financeiros, podem representar um risco consideravelmente maior do que os que possuem privilégios mais limitados.

Faz sentido, então, que incidentes causados por usuários internos acidentais com acesso privilegiado acabem custando mais às organizações do que aqueles causados por usuários internos acidentais com um menor nível de acesso. Os incidentes envolvendo usuários internos mal-intencionados com maior nível de acesso privilegiado têm um preço ainda mais alto, e os ataques envolvendo esses usuários podem evoluir para uma violação de dados em larga escala. Por exemplo, em 2018, um corretor de imóveis australiano que trabalhava para uma agência local de grande porte foi considerado culpado de acessar bancos de dados confidenciais antes de se desligar da agência. O corretor manipulou o status das potenciais vendas no sistema, diminuindo o interesse dos potenciais clientes. Além disso, o corretor admitiu ter levado mais de 200 cadastros de clientes para propor negócios em uma nova agência. Estima-se que esse ataque interno tenha custado à agência afetada 30 milhões de dólares em vendas potenciais de propriedades.[6]

Um dos melhores métodos para prevenir incidentes com informações privilegiadas relacionadas ao acesso é aderir aos princípios de privilégios mínimos e garantir que os usuários tenham o nível mais baixo de acesso necessário para o desempenho de suas funções na organização. Isso pode ser feito através de uma solução de gerenciamento de acesso privilegiado (PAM, na sigla em inglês) que pode ser construída em torno de um modelo de confiança zero.[7,8] Neste modelo, o objetivo é que todos com uma conta de usuário tenham o menor privilégio possível, diminuindo a probabilidade de um usuário interno obter acesso não intencional a dados ou ativos. Este conceito se torna ainda mais crítico na nuvem, onde residem mais dados e os usuários que os solicitam, tanto humanos quanto não humanos, devem acessá-los para operar.

O 2020 Cost of Insider Threats: Global Report mostrou que apenas 39% das organizações adotaram alguma forma de gerenciamento de acesso privilegiado em suas organizações.[9] Além disso, mostra que a adoção de um PAM resultou em uma economia de custos de 3,1 milhões de dólares, destacando a eficácia dessas medidas.

39%

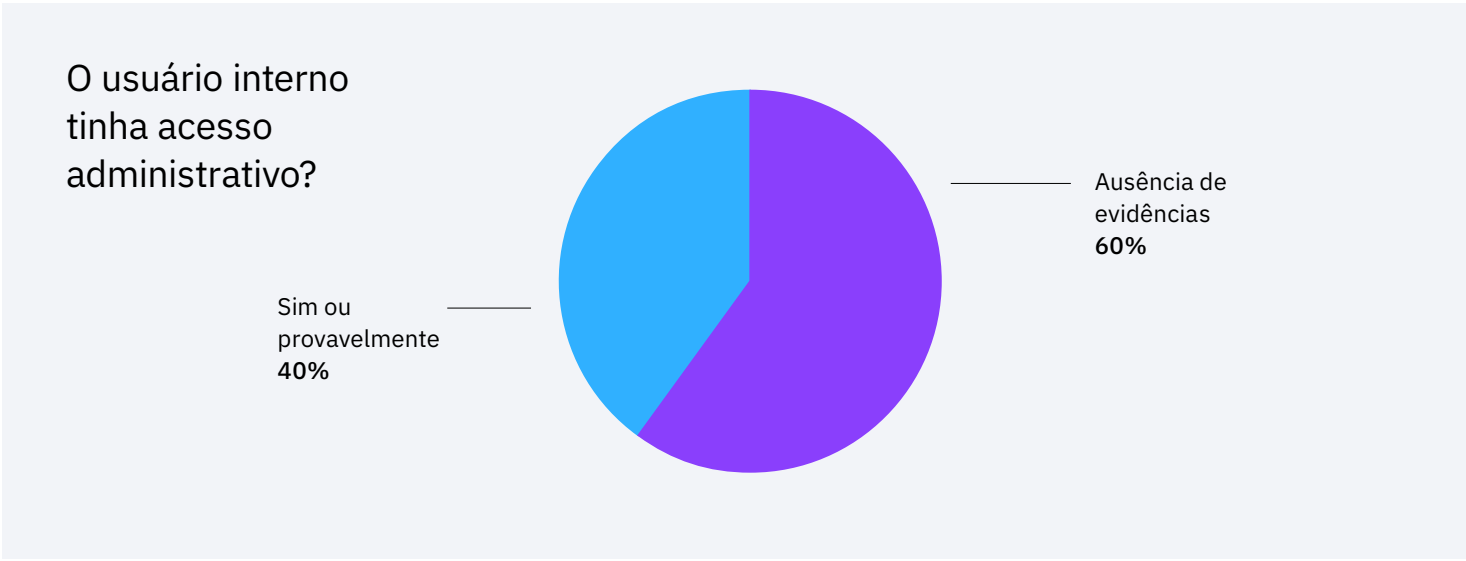
39% das organizações adotaram alguma forma de PAM em suas organizações.[9] Esta adoção resultou em uma economia de custos de 3,1 milhões de dólares.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/br-pt/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/br-pt/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

O abuso do acesso administrativo é um problema extremamente dispendioso

Já houve inúmeras ocorrências públicas de usuários internos abusando de seu poder como administradores em organizações para fins nefastos, incluindo vingança, ganho monetário ou outras más intenções. Em fevereiro de 2020, o antigo engenheiro da Microsoft, Volodymyr Kvashuk, foi considerado culpado de usar seu acesso privilegiado para roubar mais de 10 milhões de dólares em ativos digitais da empresa.[10] O furto foi possibilitado pelo acesso administrativo de Kvashuk na plataforma de vendas a varejo por cuja gestão era o responsável.[11] Mais especificamente, Kvashuk usou os endereços de e-mail de seus colegas e contas de teste válidas no sistema para encobrir sua atividade, incluindo a exfiltração de vales-presente digitais. Estes e outros bens furtados foram revendidos na Internet para lucro pessoal que o engenheiro usou mais tarde para comprar uma casa de 1,6 milhões de dólares e um carro Tesla de 160.000 dólares.[12]

Abuso de acesso administrativo em números

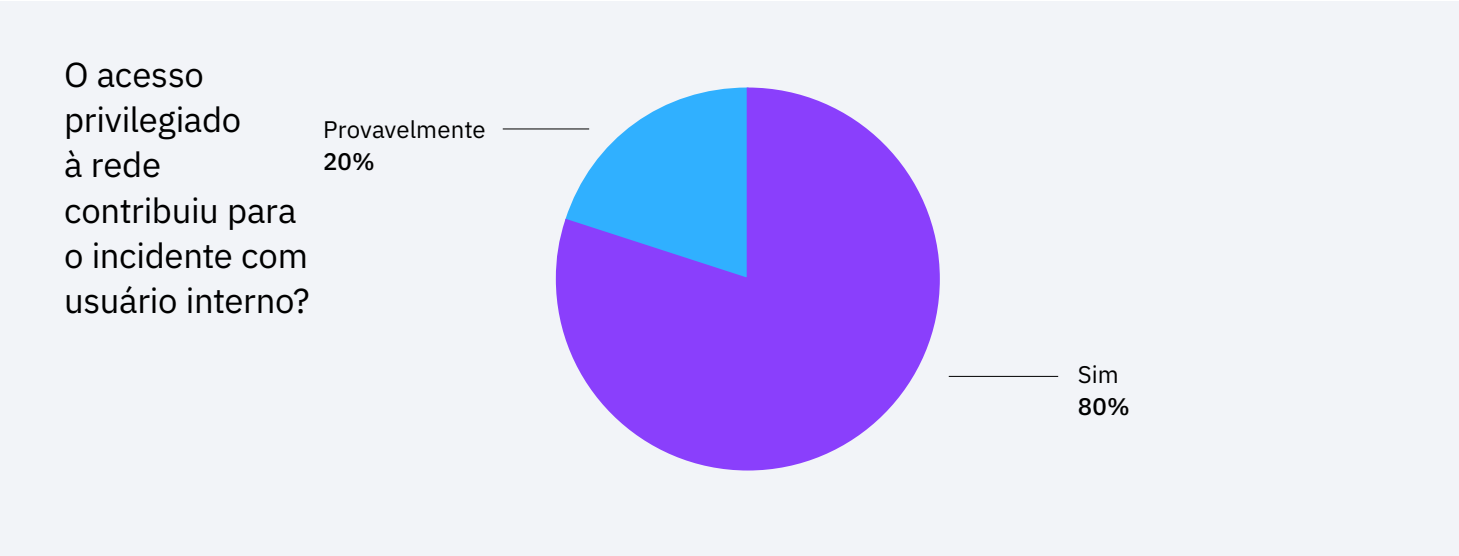


Em 40% dos incidentes aos quais o X-Force respondeu de 2018 a 2020, foi confirmado que o usuário interno certamente (ou provavelmente) teve acesso administrativo à rede. Os analistas do X-Force determinaram o tipo de acesso interno baseado nos detalhes do incidente quando o papel específico do usuário não foi fornecido pelo cliente.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

Esses incidentes envolveram a exfiltração de dados, exposição e exclusão de dados sensíveis, e instalação de software não autorizado, entre outros. Concretamente, algumas organizações perderam petabytes de logs, apagados dos servidores, sofreram vazamentos intencionais de código-fonte ou sofreram interrupções dispendiosas nas mãos de um usuário interno com acesso administrativo.

Mais interessante ainda, em 100% dos incidentes em que o usuário interno certamente (ou provavelmente) teve acesso administrativo, este acesso elevado contribuiu para o incidente. (Veja o gráfico abaixo)



Para explicar este aspecto de outra maneira, se o usuário interno não tivesse acesso administrativo, é provável que o incidente tivesse provocado muito menos impacto para a organização ou, em muitos casos, ele poderia não ter ocorrido. O X-Force respondeu a vários incidentes internos nos quais bancos de dados e logs críticos foram excluídos dos servidores. Se o usuário interno não tivesse tido acesso administrativo a esses sistemas, o evento não teria acontecido.

Recomendações

O X-Force acredita que a quantidade de incidentes internos está sub-representada nos dados de terceiros. É provável que haja muito mais incidentes dessa natureza tratados internamente pelas organizações e provavelmente não divulgados devido ao medo de responsabilização ou danos à reputação da organização.[13]

A pesquisa e os dados do X-Force destacam a necessidade de que as potenciais ameaças internas sejam um componente relevante de um programa de segurança da informação baseado no impacto que esses incidentes podem ter sobre uma organização. Particularmente, a IBM Security recomenda o seguinte em relação às ameaças internas:

As estratégias de defesa em profundidade funcionam bem para detectar ameaças internas.

Tradicionalmente, acredita-se que uma abordagem de várias camadas das tecnologias e processos implementados pelas organizações faça frente às ameaças externas. Entretanto, a pesquisa do X-Force indica que muitas dessas ferramentas, incluindo as soluções de informações de segurança e gestão de eventos (SIEM), foram cruciais para detectar também a atividade de ameaças internas.

Entenda o que é normal em seu ambiente.

A melhor maneira de detectar atividades suspeitas de qualquer tipo de invasor é compreender que tipo de atividade é considerada normal dentro de sua rede. A construção de uma compreensão sólida da atividade de referência facilita a detecção e resposta a comportamentos anômalos de forma rápida e eficaz. Uma solução robusta de análise comportamental do usuário (UBA) pode proporcionar essa funcionalidade e adaptar-se às mudanças em seu ambiente ao longo do tempo.

Reavalie o acesso administrativo regularmente.

O X-Force encontrou vários incidentes internos envolvendo administradores que provavelmente se deveram a usuários com privilégios de acesso excessivos. Um controle rigoroso de mudanças e processos deve ser implementado junto ao acesso administrativo, particularmente em servidores de missão crítica. Considere soluções tecnológicas que registram e concedem acesso administrativo temporário a sistemas e funções sensíveis.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

Separe suas equipes de segurança da informação e administrativas de TI.

A experiência do X-Force demonstrou que uma abordagem equilibrada para gerenciar a independência e a governança das equipes de segurança e administrativas ajuda a permitir uma segurança maior. Isso também permite que as equipes administrativas tenham a flexibilidade e a criatividade necessárias para otimizar sua exploração e descoberta de ameaças, ao mesmo tempo em que proporciona à empresa supervisão e controle suficientes para minimizar os riscos dentro da equipe.

Estabeleça perfis de risco para funções organizacionais sensíveis.

Como o acesso privilegiado contribuiu para muitos dos incidentes internos aos quais o X-Force respondeu, recomendamos que as organizações considerem a elaboração de perfis de risco para cargos dentro da organização que tenham acesso sensível ou administrativo a sistemas ou dados. A implementação de uma solução de gestão de acesso privilegiado (PAM) baseada em um modelo de confiança zero cria menos privilégios de acesso para os usuários e pode minimizar o impacto de incidentes com informações privilegiadas.

Atualize seu manual de resposta a incidentes para incluir ameaças internas.

Um treinamento genérico não é suficiente para esses incidentes. Embora a maioria dos manuais de resposta leve em conta os ataques de adversários externos, as organizações devem considerar a inclusão de cenários de ameaças que levem em conta usuários internos acidentais ou mal-intencionados. Considere um parceiro que possa ajudar você a desenvolver Planos de Resposta a Incidentes e manuais de ataque específicos para melhor preparar e responder a ataques cibernéticos.

Continue treinando seus funcionários.

As práticas empresariais éticas estão incluídas nos programas anuais de treinamento de inúmeras organizações, juntamente com o treinamento em engenharia social. Muitos dos incidentes internos aos quais o X-Force respondeu foram descobertos por outros funcionários e não pela tecnologia. As organizações devem incluir a forma de comunicar uma suspeita de incidente interno nas iniciativas anuais de ética empresarial ou de treinamento em engenharia social. Além disso, o treinamento baseado em funções para funcionários com acesso privilegiado pode ajudá-los a se manter conscientes dos sinais de que algo ao seu redor não está certo.

Aproveite os serviços de inteligência contra ameaças conceituados.

Muitas vezes, os clientes são desafiados pela criação, gerenciamento e operacionalização da inteligência de ameaças. Busque uma solução que proporcione a agregação, automação e integrações necessárias para operacionalizar a inteligência de ameaças em escala.

Os serviços de Detecção e Resposta Gerenciada fornecem proteção 24 horas por dia.

Os serviços de segurança de Detecção e Resposta Gerenciada (MDR) são essenciais para proporcionar prevenção, detecção e resposta rápida a ameaças internas. São fundamentais as soluções que vão além da prevenção tradicional, utilizando AV de última geração para bloqueio baseado em comportamento, investigações e gerenciamento contínuo de políticas.

Descubra como a IBM Security ajuda os clientes a proteger os ambientes mais complexos e críticos contra ameaças externas e internas.

Saiba mais sobre a IBM Security

IBM Security

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

Produzido nos Estados Unidos da América
Maio de 2021

IBM