DOCUMENTAÇÃO TÉCNICA | Janeiro de 2015

Preciso confiar *em alguém.* ...Não?

Lidando com ameaças internas à segurança cibernética

Russell Miller

Merritt Maxim

Gerenciamento de segurança da CA Technologies

ca technologies

Sumário

Resumo executivo

"Quando você ocupa posições que têm acesso com privilégios, como a de um administrador de sistemas desse tipo de agência de comunidade de inteligência, está exposto a muito mais informações em uma escala mais ampla do que o funcionário mediano."

– Edward Snowden

Desafio

Embora muitas organizações concentrem seus esforços de segurança na borda da rede, é o interior que talvez represente o maior risco à segurança cibernética. Dos executivos aos administradores de TI e parceiros, muitas pessoas têm acesso a dados confidenciais que, se forem expostos publicamente, podem ter ramificações significativas para os negócios de uma organização ou mesmo para a sua existência.

A segurança cibernética geralmente é considerada como um campo técnico, com defensores altamente habilitados que procuram lograr os invasores em uma competição de intelecto e vontade. Embora haja alguma verdade nessa caracterização, falta o aspecto talvez mais importante da segurança: o elemento humano. As pessoas tendem a confiar nos conhecidos, o que as leva a compartilhar senhas ou outras informações que não deveriam compartilhar.

A confiança é um elemento essencial para operar qualquer tipo de organização. As pessoas precisam acessar informações confidenciais e sistemas essenciais por muitas razões, e um nível de confiança precisa estar associado a esse acesso. Compreender e gerenciar essa confiança é o desafio mais crucial e difícil ao lidar com ameaças internas.

Oportunidade

"Confiar" não significa conceder aos funcionários acesso irrestrito e desnecessário às informações. Com os controles de segurança corretos, as organizações podem reduzir significativamente sua exposição ao risco de ameaças internas. A chave é encontrar o equilíbrio correto entre a autorização do funcionário e o controle e, ao mesmo tempo, manter a responsabilidade dos funcionários sobre suas ações. Isso requer uma abordagem ampla para permitir que uma organização gerencie cuidadosamente suas identidades, seu acesso e seus dados, desde o gerenciamento de identidades até a governança, o gerenciamento de identidades com privilégios e a proteção de dados.

A fraude interna é uma ocorrência comum. Em média, as organizações tiveram, aproximadamente, 55 incidentes de fraude relacionados a funcionários nos últimos 12 meses.[1]

– The Ponemon Institute

Benefícios

Os controles de segurança fortes, além de reduzirem o risco, também permitem o compartilhamento de informações em uma organização. O acesso a informações altamente confidenciais é frequentemente muito restrito, devido ao risco de exposição dos dados. Com os controles de segurança adequados, os dados podem ser compartilhados com um grupo maior de pessoas, que podem ser mais eficientes e inovadoras.

"No mundo atual, a coisa mais valiosa que alguém possui é a tecnologia. A ação mais importante que este país pode realizar é proteger seus segredos comerciais."[3]

– Juiz distrital dos EUA Ruben Castillo

Seção 1:

Desafio

Os usuários internos podem roubar, apagar ou expor dados confidenciais de forma maliciosa ou involuntária por vários motivos. Ao mesmo tempo, é necessário que eles tenham um certo nível de acesso para permitir o funcionamento da empresa ou a operação da organização. É imprescindível entender as ameaças internas em vários níveis, desde as motivações até os exemplos de danos e a maneira como a ameaça evoluiu, para que seja possível abordar de forma inteligente as estratégias de redução do risco.

Tipos de ameaças internas

As ameaças internas não são todas iguais. Existem três tipos de ameaças internas: usuários internos mal-intencionados que roubam informações ou causam danos deliberadamente, usuários internos que são explorados inadvertidamente por terceiros externos e usuários internos que são descuidados e cometem erros não intencionais.

- Os **usuários internos mal-intencionados** são os menos frequentes, mas têm o potencial de provocar danos significativos devido a seu acesso interno. Administradores com identidades com privilégios são especialmente arriscados. De acordo com o Ponemon Institute, "as violações de dados resultantes de ataques mal-intencionados são as mais caras".[2]
- Os **usuários internos explorados** podem ser "enganados" por terceiros externos para fornecer dados ou senhas que não deveriam fornecer.
- Os **usuários internos descuidados** podem simplesmente pressionar a tecla errada e excluir ou modificar acidentalmente informações cruciais.

As ameaças internas também podem vir de usuários com privilégios (administradores) ou de usuários regulares com acesso a dados confidenciais. Os administradores geralmente possuem privilégios completos para executar praticamente qualquer operação em vários sistemas essenciais. Pessoas de todos os tipos frequentemente acumulam mais direitos do que o necessário para seu cargo, o que gera um aumento no risco que é totalmente possível de ser prevenido.

O que mudou?

A aposta. À medida que nos tornarmos cada vez mais uma economia com base em informações, a propriedade intelectual e os segredos comerciais são mais importantes do que nunca para a sobrevivência de uma organização. A ascensão da análise de "Big Data" aumentou o problema. As empresas agora estão armazenando vastas quantidades de dados para revelar padrões e perspectivas que seriam impossíveis há alguns anos. Embora sejam potencialmente um importante diferencial de negócios, esses dados, em alguns casos, são altamente confidenciais, contendo informações como dados pessoais dos clientes, números de cartões de crédito, transações, comunicações e até mesmo localizações. Uma violação de segurança do armazenamento de dados de um cliente pode resultar em violação de leis de privacidade, ações coletivas e danos à reputação que podem levar à perda do negócio.

A equipe CERT (Computer Emergency Response Team) da Carnegie-Mellon University definiu um usuário interno mal-intencionado como "um funcionário, um prestador de serviços ou um parceiro de negócios atual ou antigo que tem ou teve acesso autorizado à rede, ao sistema ou a dados de uma organização e intencionalmente excedeu ou utilizou incorretamente esse acesso de uma maneira que afetou negativamente a confidencialidade, a integridade ou a disponibilidade das informações ou dos sistemas de informação da organização".[4] Historicamente, o usuário interno era um funcionário, mas, conforme observado pela CERT, o escopo das ameaças internas se expandiu para além dos funcionários, incluindo o conluio com usuários externos, parceiros de negócios "confiáveis" e outras pessoas. Esse desenvolvimento, combinado à natureza altamente distribuída e móvel da força de trabalho atual, significa que a ameaça interna está mais severa do nunca.

Fatores de risco internos

Todas as organizações enfrentam desafios comuns ao tentar reduzir o risco de violações de segurança internas:

Gerenciamento ineficiente de usuários com privilégios. Todos os ambientes de TI possuem usuários com privilégios (administrador, raiz) que têm acesso total a importantes sistemas, aplicativos e informações. Isso não é apenas um risco de segurança, também pode tornar a conformidade muito mais difícil. O compartilhamento de senhas de administrador é outro problema comum que pode levar ao acesso inadequado a sistemas e informações, além da incapacidade de identificar especificamente quem executou qual ação em cada sistema.

Atribuição inapropriada de funções e direitos. O gerenciamento de funções e direitos de usuários é um dos maiores desafios enfrentados por muitas organizações de TI. A sobreposição de funções e a duplicação ou a inconsistência de direitos são problemas comuns que podem levar ao acesso e ao uso inadequado de informações confidenciais. Além disso, a falta de desprovisionamento automatizado pode levar a direitos excessivos ou contas órfãs, o que pode fornecer aberturas pelas quais usuários internos descontentes podem iniciar um ataque.

Governança de identidades em geral inadequada. A proteção efetiva contra o acesso ou o uso inadequado de informações exige um controle robusto das identidades dos usuários, dos acessos e do uso de informações. A maioria das organizações possui alguns controles nessas áreas, mas não tem uma abordagem unificada e robusta para proteger de verdade seus ativos de informações.

Classificação de informações e aplicação de diretivas inadequadas. Muitas organizações nem mesmo sabem onde estão todas as suas informações confidenciais e, geralmente, possuem diretivas definidas e comunicadas de maneira inadequada em relação à maneira como essas informações confidenciais devem ser tratadas. Mas o mais importante é que muitas organizações não têm nenhum controle em vigor para detectar e impedir a transmissão ou a divulgação inapropriada de informações confidenciais.

Auditoria e análise inadequadas. Muitas empresas não têm nenhuma maneira de fazer a auditoria contínua de acessos a fim de ajudar a garantir que apenas os indivíduos com autorização adequada estejam obtendo acesso e que o uso de informações por eles esteja de acordo com a diretiva estabelecida. Mesmo que elas tenham ferramentas de auditoria em vigor, o volume absoluto de dados de log gerados torna muito difícil para as organizações analisar os dados e identificar violações ou ameaças.

Complexidade do log de auditoria. O volume absoluto dos dados de auditoria e log impede a investigação forense e a detecção. O log de todas as atividades de TI é uma importante etapa inicial no combate a ataques internos, e os atuais ambientes de TI altamente distribuídos e complexos geram volumes massivos de dados de log, mas o volume absoluto de dados é muito difícil de gerenciar.

Resposta reativa. A maioria das abordagens atuais para resolver as ameaças internas é reativa, não preditiva. Embora isso possa ajudar imensamente nas investigações forenses, o problema é que o ataque ou o roubo já ocorreu. Portanto, as organizações devem procurar soluções que possam fornecer recursos mais analíticos e preditivos que, se não conseguirem impedir os ataques internos, ainda poderão identificar os "usuários internos sob risco" e, em seguida, implementar registros em log mais detalhados sobre esses indivíduos em resposta.

Nenhuma diretiva de uso aceitável abrangente por escrito. Todas as organizações devem ter diretivas de uso aceitável detalhadas para todos os funcionários e devem fazer com que os funcionários revisem e assinem as diretivas anualmente. Essa é uma etapa básica, mas que as organizações frequentemente negligenciam. Ter uma diretiva de segurança por escrito não impede necessariamente os ataques internos, mas pode ser útil para fornecer uma linha de base a toda a organização sobre o que é um uso aceitável e os métodos apropriados para lidar com dados confidenciais.

Cerca de 65% dos funcionários que cometem roubo de IP interno já tinham aceitado cargos em uma empresa concorrente ou tinham aberto sua própria empresa quando cometeram o roubo. Cerca de 20% tinham sido recrutados por uma parte externa que visava os dados. Mais de metade rouba os dados no período de um mês antes de sair.

Behavioral Risk Indicators of Malicious Insider IP Theft: Misreading the Writing on the Wall,

– Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D.

Por que é difícil: redução do risco vs. viabilização dos negócios

A confiança é imprescindível para a operação de qualquer organização. Para que uma organização se beneficie com as informações confidenciais, as pessoas e os sistemas certos precisam conseguir acessá-las, e as diretivas excessivamente restritivas prejudicam a capacidade de resposta, a inovação e até mesmo o funcionamento da organização. Ao mesmo tempo, a confiança desnecessária leva a riscos desnecessários. Por exemplo, as pessoas que geralmente são mais confiáveis têm a capacidade de causar o maior dano: são os usuários com privilégios em uma organização. Normalmente, esses administradores possuem privilégios para realizar essencialmente qualquer operação em sistemas cruciais, e os usuários normalmente acumulam mais direitos do que precisam para sua função atual. Outro risco desnecessário associado às identidades com privilégios é o uso de contas compartilhadas. O acesso de várias pessoas à mesma conta leva a uma falta de responsabilidade.

O gerenciamento do elemento humano é o aspecto mais desafiador do gerenciamento de ameaças internas. Muitas pessoas sentem a necessidade de acreditar que sua empresa confia nelas e se sentem menosprezadas em novos controles que removem o acesso a informações às quais elas tinham acesso anteriormente. Além disso, o acesso é frequentemente considerado como uma forma de status, principalmente com os administradores de TI, e as tentativas de refrear o acesso geralmente encontram resistência.

Exemplos de violações de segurança internas

Muitas violações de segurança cometidas por usuários internos nunca são tornadas públicas. As organizações preferem manter a confidencialidade dessas violações para evitar os danos à sua reputação e as preocupações dos clientes sobre a sua segurança. No entanto, muitas violações de usuários internos altamente danosas foram divulgadas. Aqui estão algumas das mais conhecidas:

Violações de segurança internas bastante conhecidas

Agência de Segurança Nacional dos EUA	São Francisco	Motorola
Edward Snowden, trabalhando para a Booz Allen Hamilton como terceirizado da NSA, forneceu documentos altamente secretos para os jornalistas sobre os programas chamados "Prism" e "Boundless Informant". As informações de Snowden expuseram detalhes do armazenamento e processamento de comunicações da NSA, inclusive ligações telefônicas e emails.[5]	Um funcionário descontente em São Francisco bloqueou o acesso da cidade à sua própria rede FiberWAN, que continha documentos confidenciais, inclusive registros policiais. O pior é que os emails ficaram inacessíveis e os cheques da folha de pagamento não puderam ser emitidos. A cidade gastou mais de um milhão de dólares em uma tentativa infrutífera de obter acesso à rede.[6]	Hanjuan Jin, que trabalhou como engenheiro de software da Motorola durante nove anos, foi pego pelos agentes da alfândega dos EUA entrando em um avião para Pequim com 30.000 dólares em dinheiro, juntamente com mais de 1.000 documentos marcados como "informações confidenciais e proprietárias", representando 10 a 15 milhões de dólares em segredos comerciais. Jin foi considerado culpado de roubo de segredos comerciais em uma corte federal dos EUA e condenado a quatro anos de prisão.[7]

Seção 2:

Oportunidade

As organizações precisam enfrentar a realidade de que os ataques internos são uma ameaça significativa e que estão cada vez mais complexos. Uma vez que grande parte dos ativos e informações de uma organização está online e acessível, as organizações precisam de uma abordagem proativa para se defender desses ataques internos. Essa abordagem deve envolver uma variedade de soluções que abranjam o gerenciamento de identidades e acesso e a proteção das informações. Nada pode impedir completamente todos os ataques internos, mas a adoção de uma abordagem proativa agressiva pode ajudar a reduzir os riscos, melhorar a conformidade e permitir que a organização de TI ofereça suporte aprimorado a iniciativas de negócios.

Encontrando o equilíbrio

Ferramentas para gerenciar identidades, acesso e dados podem permitir que a organização encontre o equilíbrio adequado entre a capacitação e o compartilhamento de dados confidenciais, com os controles necessários para reduzir os riscos de violações de segurança internas. As organizações podem reduzir o risco de todos os três tipos de ameaças internas (mal-intencionadas, exploradoras e por descuido), permitindo a responsabilização, implementando acesso com menos privilégios e controlando dados confidenciais. A responsabilização fará com que os usuários internos mal-intencionados pensem duas vezes antes de agir, ajudará a identificar usuários internos explorados e tornará os usuários mais atentos em suas ações. O acesso com menos privilégios negará ações e limitará o dano resultante de todos os tipos de ataques internos, inclusive de ações inadvertidas, porém danosas. Com o controle direto de dados confidenciais, as empresas podem impedir que eles sejam exportados para fora de sua rede usando ferramentas, como unidades USB ou, até mesmo, email.

"Confiar" não significa conceder aos funcionários acesso irrestrito a informações que não são relevantes para seus cargos. As organizações têm um certo grau de confiança em qualquer funcionário que acesse dados ou sistemas confidenciais. A concessão de acesso além do necessário é um risco supérfluo que não significa que a organização não confie em seus funcionários. É apenas uma empresa inteligente.

Para oferecer suporte a novos controles de segurança, é imprescindível estabelecer uma norma cultural em torno do acesso com menos privilégios aplicando controles de uma maneira padrão em toda a organização. Dessa maneira, os indivíduos percebem a segurança de dados como uma prioridade organizacional e não uma falta de confiança em uma determinada pessoa. Isso reduz os sentimentos negativos associados a uma abordagem cuidadosamente controlada do acesso a dados.

Uma abordagem aprofundada para reduzir ameaças internas

Os recursos de segurança atuais podem reduzir os danos de uma violação de segurança interna, identificar uma violação após o fato a fim de permitir uma resposta eficaz ou mesmo evitar que uma violação chegue a ocorrer. Os recursos mais importantes incluem:

Gerenciamento de identidades com privilégios

O gerenciamento de identidades com privilégios está no centro de qualquer defesa cibernética contra ameaças internas. As contas com privilégios têm o acesso necessário para que uma pessoa visualize e roube as informações mais confidenciais de uma organização ou cause um grande dano aos sistemas de TI essenciais. Geralmente, elas também são compartilhadas, com o acesso de várias pessoas às mesmas contas e senhas, resultando em falta de responsabilização.

Para gerenciar identidades com privilégios é necessário uma abordagem com várias partes. Além do gerenciamento de contas compartilhadas, controles adicionais permitem a responsabilização dos usuários internos e podem limitar os danos gerados por um invasor externo que obtenha acesso a uma conta administrativa.

56%. "Porcentagem de executivos que dizem que sua fraude mais grave ocorreu devido a um usuário com privilégios."[8]

– Pricewaterhouse Coopers

Principal recurso	Necessidade	Descrição	Benefício
Gerenciamento de senhas de contas compartilhadas	As contas com privilégios, como 'raiz' no UNIX e 'Administrador' no Windows, geralmente são compartilhadas, o que reduz a responsabilidade.	Controlar o acesso a contas administrativas com privilégios usando recursos de armazenamento de senhas e logon automático. Este é o ponto de partida da maioria das soluções de gerenciamento de identidades com privilégios.	Reduz o risco de usuários não autorizados obterem acesso a contas com privilégios. Evita o compartilhamento de senhas.
Controles de acesso refinados	O acesso a contas com privilégios geralmente é "tudo ou nada", um risco de segurança desnecessário que leva a usuários com mais privilégios do que precisam.	Gerenciar o acesso de usuários com privilégios após o logon. Controlar qual acesso os usuários têm com base em sua identidade individual, mesmo ao usar uma conta administrativa compartilhada.	Reduz o risco ao fornecer aos administradores apenas o mínimo de privilégios necessários para suas funções.
Relatório de atividades do usuário/gravação de vídeo da sessão	Acompanhar todas as ações do usuário para determinar o que ocorreu e "quem fez o que" em uma investigação. Nem todas as atividades do usuário são gravadas e muitos aplicativos não geram logs, o que reduz a responsabilidade e dificulta as investigações forenses.	Registrar todas as ações do usuário, rastreando todos os registros por indivíduo, mesmo quando uma conta compartilhada é usada. O ideal é acompanhar um sistema de TI em um formato semelhante a vídeo.	Simplifica a descoberta de "quem fez o que" em uma investigação forense, usando um vídeo compreensível, em vez de pesquisas de arquivos de log incompreensíveis. Permite a responsabilização dos usuários de sistemas de TI. Cria logs para aplicativos que originalmente não os produzem.
Segurança da virtualização	A virtualização adiciona uma nova camada de infraestrutura que deve ser protegida: o hypervisor.	Gerenciar usuários com privilégios no VMware e, ao mesmo tempo, fornecer automação orientada à virtualização de controles de segurança em máquinas virtuais.	Reduz os riscos da virtualização, desde os administradores do VMware até as máquinas virtuais.
Ponte de autenticação do UNIX	O gerenciamento de contas e acesso de usuários em servidores individuais UNIX e Linux é uma carga administrativa que pode levar a erros e omissões.	Autenticar os usuários nos sistemas UNIX e Linux para o Microsoft Active Directory.	Consolida informações de autenticação e contas no Active Directory, em oposição ao gerenciamento de credenciais do UNIX localmente em cada sistema. Reduz a sobrecarga administrativa.

"Se você não implementar controles adequados para os usuários com privilégios, correrá o risco de degradação no nível do serviço, custos de medidas corretivas na auditoria, desenvolvedores acessando dados (confidenciais) de produção e funcionários descontentes derrubando a sua infraestrutura ou fazendo você de refém."[9]

– Forrester Research, Inc.

Gerenciamento de identidades e governança

Uma causa significativa de violações de segurança são os direitos inadequados. Isso pode ser provocado por configurações iniciais incorretas de direitos de acesso, acúmulo de direitos ao longo do tempo ou mesmo direitos de acesso incorretos de um usuário, que foram definidos intencionalmente por um administrador colaborador não autorizado. O acúmulo de direitos pode ser o resultado da falta de manutenção quando o funcionário muda de cargo e mantém todos os seus direitos de acesso. Embora os direitos incorretos do usuário aumentem principalmente o risco de ameaças internas, os usuários externos também podem obter acesso a essas contas ou encontrar contas não utilizadas que tornam mais fácil ocultar suas atividades. Um erro frequente que muitas organizações cometem é não desprovisionar as contas e remover todos os direitos de acesso imediatamente ao demitir os administradores.

Uma solução de melhor prática é um processo abrangente e contínuo para reconhecer quais usuários devem ter acesso a quais recursos e, então, validar os direitos de acesso apropriados de cada usuário regularmente. A Governança de identidades, segmentada em um alto nível como gerenciamento de funções e conformidade de identidades, envolve vários processos relacionados a identidades, incluindo a verificação e limpeza de direitos de usuários existentes, a criação de modelos de função precisos e a aprovação de diretivas e processos que ajudem a garantir a atribuição adequada de privilégios aos usuários. As soluções de Governança de identidades podem fornecer vários benefícios, incluindo:

- Aumento da segurança por meio da automação dos processos necessários para ajudar a atender às auditorias de conformidade e do estabelecimento de diretivas de segurança de identidades entre sistemas.
- Redução de custos de gerenciamento de identidades com a simplificação das etapas envolvidas nos projetos, como detecção de funções, limpeza de privilégios e certificação.
- Menor tempo para valorização e maior aderência às diretivas do IAM por meio do fornecimento mais rápido de uma base de função e segurança consistente e precisa.

Controles de dados

O objetivo final de todos os ataques cibernéticos é roubar informações confidenciais ou causar danos; portanto, ter controle sobre os dados é um componente essencial para uma defesa bem-sucedida. Da mesma forma, muitas violações de segurança internas são o resultado de download de dados valiosos de propriedade intelectual (como código-fonte) por um funcionário. Para proteger os dados confidenciais, uma organização deve proteger e controlar os dados em quatro estados:

1. **Dados no acesso.** Tentativa de acesso a informações confidenciais por um indivíduo que ocupa uma função inadequada.
2. **Dados em uso.** Informações confidenciais manipuladas na estação de trabalho local ou no laptop.
3. **Dados em movimento.** Informações confidenciais transmitidas pela rede.
4. **Dados em descanso.** Informações confidenciais armazenadas em repositórios como bancos de dados, servidores de arquivos ou sistemas de colaboração.

Para conseguir isso, as organizações devem definir diretivas para aplicar controle, caso seja detectado acesso ou uso inadequado dos dados. Caso ocorra uma violação de diretiva (como uma tentativa de acessar propriedade intelectual, copiar informações para uma unidade USB ou tentar enviá-las por email), a solução deverá atenuar o comprometimento e gerar um alerta.

A classificação das informações é o elemento central de qualquer iniciativa de segurança de dados. Sem compreender o contexto das informações, inclusive o que são e onde estão localizadas, é impossível implementar um programa abrangente de proteção de dados. Uma organização deve detectar e classificar as informações confidenciais de forma precisa, com base em seu nível de confidencialidade para a organização. Isso inclui propriedade intelectual, mas também informações de identificação pessoal, informações particulares sobre saúde e outras informações não públicas.

Uma vez que as informações tenham sido classificadas corretamente, diretivas tenham sido definidas e controles tenham sido implantados, a organização poderá monitorar e controlar o acesso e a manipulação de todas as informações confidenciais. Isso inclui ações do usuário que vão desde a simples tentativa de acessar e ler dados confidenciais até copiar para um dispositivo removível ou imprimir, enviar por email para fora da rede e detectar dados armazenados em um repositório como o SharePoint.

"Apenas os amadores atacam máquinas; os profissionais têm como objetivo as pessoas."[10]

– Bruce Schneier

Autenticação avançada

Embora os métodos de autenticação geralmente não sejam considerados quando se discute ameaças internas, eles são muito relevantes em caso de um usuário externo explorar um usuário interno para que forneça suas credenciais. As senhas não fornecem segurança adequada para as informações e os aplicativos importantes atuais. Quando esses invasores se autenticam no sistema, sempre há fatores contextuais que podem, se reconhecidos, gerar um aviso sobre a validade da autenticação. Por exemplo, se alguém de Finanças que trabalha em Nova York, de repente, efetuar logon na Rússia ou se alguém efetuar logon em Roma duas horas depois de efetuar logoff em Nova York, estará claro que uma autenticação fraudulenta está em andamento.

As soluções de autenticação com base em risco fornecem uma pontuação de risco de cada tentativa de autenticação, o que pode ajudar a determinar se uma tentativa de violação pode estar em andamento. Nesses casos, outros métodos de "autenticação adicional" podem ser necessários, a tentativa pode ser simplesmente rejeitada ou um alarme pode ser gerado.

Segurança da virtualização

O potencial de dano das ameaças dos usuários internos aumentou recentemente com a explosão de dados confidenciais e as ferramentas de administração mais poderosas. A ascensão da virtualização, em particular, deu margem a novos riscos. Em primeiro lugar, existe uma nova classe de administradores no hypervisor, que deve ser gerenciada, monitorada e controlada. Em segundo lugar, esses administradores do hypervisor podem alterar, copiar ou excluir dezenas de máquinas virtuais apenas com alguns cliques do mouse, o que torna o roubo e os danos mais simples, rápidos, prejudiciais e difíceis de serem detectados.

Para superar os desafios à segurança em um ambiente virtualizado, as organizações precisam adotar uma abordagem proativa, e não reativa, para impedir ameaças e omissões. Um ponto de partida é aplicar na camada do hypervisor os fundamentos de segurança já incorporados em uma infraestrutura tradicional.

Essas ações permitem o estabelecimento de uma base de segurança sólida; porém, por si só, não conseguem lidar com todas as alterações dinâmicas que tornam os servidores virtuais menos seguros do que os servidores físicos. A infraestrutura virtual deve ser ainda mais protegida implementando, também, recursos específicos à virtualização. A automação orientada à virtualização oferece recursos inovadores para gerenciar os riscos associados à segurança do hypervisor. Aplicada em conjunto com os fundamentos de segurança, ela protege o ambiente virtual e, ao mesmo tempo, oferece suporte às rápidas demandas de seus negócios.

Seção 3: Benefícios

Controle a ser ativado

Utilizando controles de segurança com base em identidades e dados, as organizações reduzem o risco de violações internas e melhoram os programas de conformidade. Os recursos automatizados e gerenciados centralmente ajudam a reduzir os custos e fortalecem os controles de segurança de TI. Com auditoria robusta, os desafios de conformidade se tornam menos assustadores, permitindo que as organizações forneçam comprovação de controles e demonstrem para os auditores a operação efetiva dos controles de segurança estabelecidos.

A defesa contra usuários internos de qualquer tipo é um problema fundamentalmente desafiador. O fluxo de informações é essencial para o funcionamento de uma empresa. As restrições podem levar a problemas operacionais ou impedir que os funcionários tenham acesso às informações necessárias para que possam ser eficientes ou inovadores.

Tendo os controles ***certos***, no entanto, uma organização pode compartilhar informações com várias pessoas. Esses controles permitem que a organização opere com ***confiança limitada***. Sem a restrição da concessão de privilégios apenas do tipo "tudo ou nada", as organizações podem compartilhar informações específicas com pessoas às quais anteriormente esse acesso teria sido negado! As organizações que utilizam controles dessa maneira estão fazendo da segurança uma ferramenta para capacitar a empresa.

As organizações também devem lembrar que, ao se protegerem contra as ameaças internas, elas também estão se protegendo contra os invasores externos. As identidades, inclusive identidades com privilégios, são frequentemente usadas por usuários externos após o invasor violar o perímetro da rede. Ao empregar um núcleo robusto de controles de segurança interna, uma organização terá criado uma base sólida para evitar ou reduzir os danos dos ataques externos.

Seção 4:

Conclusões

A ameaça de usuários internos é real e crescente. As organizações devem acordar para a realidade de que as ameaças internas não são mais um conceito abstrato, mas algo que pode ocorrer a qualquer momento. Em vez de adotar uma mentalidade fechada e aceitar a inevitabilidade de um ataque interno, as organizações devem adotar uma postura mais agressiva no combate à ameaça interna. Uma parte central dessa postura agressiva deve ser o Gerenciamento de identidades e acesso, juntamente com a Prevenção de perda de dados.

A ameaça interna nunca pode ser totalmente removida, mas os controles com base em identidade são a base de um programa de prevenção de ameaças internas bem-sucedido. As organizações preocupadas com o combate de ameaças internas devem implantar alguns ou todos esses recursos porque fazer isso é um mecanismo eficiente e comprovado para manter os ataques internos sob controle.

Seção 5:

Referências

1 The Ponemon Institute, "The Risk of Insider Fraud: Second Annual Study." Fevereiro de 2013

2 The Ponemon Institute, "The Risk of Insider Fraud: Second Annual Study." Fevereiro de 2013

3 bigstory.ap.org/article/sentencing-set-corporate-espionage-suspect

4 cert.org/insider_threat

5 newyorker.com/online/blogs/closeread/2013/06/edward-snowden-the-nsa-leaker-comes-forward

6 slate.com/articles/technology/future_tense/2013/02/fiberwan_terry_childs_gavin_newsom_on_why_governments_should_outsource_technology.single

7 articles.chicagotribune.com/2012-08-31/business/ct-biz-0830-moto-theft--20120831_1_trade-secret-case-hanjuan-jin-trade-secrets

8 online.wsj.com/article/SB10001424052970203753704577255723326557672

9 Forrester Research Inc., "Assess Your Identity And Access Management Maturity". 26 de setembro de 2012

10 schneier.com/crypto-gram-0010

Seção 6:

Sobre os autores

Russell Miller passou mais de seis anos trabalhando com segurança de rede em várias funções, desde a de hacker ético até marketing de produto. Atualmente, ele é diretor de marketing de soluções na CA Technologies, com foco em gerenciamento de identidades com privilégios e segurança da virtualização. Russell é bacharel em ciências da computação pelo Middlebury College e cursou seu MBA na MIT Sloan School of Management.

Merritt Maxim tem 15 anos de experiência em gerenciamento e marketing de produtos no setor de segurança de informações, incluindo cargos na RSA Security, na Netegrity e na CA Technologies. Em sua função atual na CA Technologies, Merritt cuida do marketing de produtos para iniciativas de gerenciamento de identidades e segurança na nuvem. Coautor de "Wireless Security", Merritt participa de blogs sobre vários tópicos de segurança de TI e pode ser seguido no Twitter em www.twitter.com/merrittmaxim. Merritt é bacharel cum laude em ciências humanas pela Colgate University e cursou seu MBA na MIT Sloan School of Management, além de ser o autor de "Wireless Security".

Conecte-se com a CA Technologies em ca.com/br

A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da era dos aplicativos. O software está no cerne de todas as empresas, em todos os setores. Do planejamento ao desenvolvimento e do gerenciamento à segurança, a CA está trabalhando com empresas de todo o mundo para mudar a maneira como vivemos, fazemos negócios e nos comunicamos – usando dispositivos móveis, as nuvens privada e pública e os ambientes distribuídos e de mainframe. Obtenha mais informações em **ca.com/br**.