DOCUMENTAÇÃO TÉCNICA | ABRIL DE 2016

Fechando backdoors da rede

Cinco principais melhores práticas para controlar riscos de fornecedores terceiros

Dale R. Gardner
Gerenciamento de segurança da CA

ca technologies

Sumário

Resumo executivo

Desafio

As maiores violações ocorridas na Target, na Home Depot, no eBay, no Departamento de Administração de Pessoal dos EUA e em outros locais foram possíveis devido ao roubo ou comprometimento de credenciais de usuário, que pertenciam a um usuário com privilégios com amplo acesso a sistemas confidenciais. Em quase dois terços dos casos, a violação inicial foi facilitada por práticas de segurança inadequadas de um terceiro — um fornecedor ou um parceiro de negócios que tinha acesso a uma rede interna. Usando as credenciais dos parceiros que foram roubadas, os invasores exploraram a infraestrutura de TI violada em busca de contas com privilégios, as quais foram utilizadas para obter acesso não autorizado a sistemas essenciais e causar grandes prejuízos para as empresas.

Oportunidade

De maneira semelhante às empresas que sofreram violações, muitas organizações estão diante de uma combinação complexa e frustrante de fornecedores terceiros, prestadores de serviços e parceiros de negócios que têm acesso de rede à sua infraestrutura de TI e a uma grande variedade de contas com privilégios usadas na execução de aplicativos essenciais. No atual trabalho interconectado, não é possível bloquear o acesso e eliminar as contas com privilégios completamente. Por esse motivo, a única opção é proteger melhor as contas com privilégios contra usuários não autorizados, aumentando, assim, a proteção dos ativos de informações confidenciais.

Benefícios

Com a empresa interconectada, é possível obter economia com o outsourcing, melhorias na qualidade e aumento da eficiência. Restringir o acesso de rede no firewall para todos já não é mais uma opção. Recursos relevantes devem estar disponíveis para os parceiros de negócios, de modo que seja possível desfrutar dos benefícios. É necessário utilizar melhores práticas relacionadas à segurança das informações para bloquear as violações e permitir a realização de atividades de negócios legítimas.

Seção 1

Riscos criados pelo acesso de terceiros

Atualmente, na maioria das organizações, há inúmeros não funcionários com algum nível de acesso com privilégios a sistemas e redes internas. Frequentemente, a equipe de segurança da informação da empresa sabe pouco ou nada sobre essas pessoas; a única coisa que se sabe é que elas trabalham para fornecedores da empresa, são prestadores de serviços terceirizados ou parceiros de negócios. Geralmente, esses usuários terceiros representam o maior risco para a empresa, pois suas contas são frequentemente o caminho mais fácil para prejudicar a empresa. Exemplos desses tipos de violações podem ser vistos nas notícias sobre a Target, a Home Depot e outras empresas. O comprometimento do acesso de usuário de um terceiro relativamente pequeno pode ser utilizado para obter acesso mais amplo às redes e aos sistemas da organização e causar enormes prejuízos. Essas violações não são algo anormal. De acordo com Troy Leach, da PCI Council, cerca de 65% das violações podem ser causadas por um terceiro.

Os órgãos reguladores estão cientes desses riscos e estão trabalhando com o setor para desenvolver regulamentos e controles apropriados para lidar com esse desafio. Por exemplo, o PCI versão 3 do Padrão de segurança de dados introduziu novos controles destinados a lidar com os riscos de terceiros. Benjamin Lawsky, Superintendente de serviços financeiros do estado de Nova York, declarou: **"A segurança cibernética de um banco geralmente depende da segurança cibernética de seus fornecedores. Infelizmente, essas empresas terceiras podem fornecer uma entrada de backdoor para hackers que desejam roubar dados confidenciais dos clientes dos bancos."** Como resultado, reguladores da área de serviços financeiros, da saúde e de outros setores estão desenvolvendo novos requisitos de conformidade para reduzir os riscos e aumentar a segurança.

> "A segurança cibernética de um banco geralmente depende da segurança cibernética de seus fornecedores. Infelizmente, essas empresas terceiras podem fornecer uma entrada de backdoor para hackers que desejam roubar dados confidenciais dos clientes dos bancos"
>
> – Benjamin Lawsky, Superintendente de serviços financeiros do estado de Nova York

---

Seção 2

Cinco principais melhores práticas para controlar riscos de fornecedores terceiros

Daqui para frente, controlar e gerenciar o acesso de terceiros a redes e sistemas estão se tornando requisitos cada vez mais importantes tanto para o gerenciamento de riscos da segurança das informações quanto para a conformidade com regulamentos.

> "Os hackers acessaram as redes da OPM usando as credenciais roubadas da empresa contratada KeyPoint Government Solutions."
>
> Exclusive: The OPM breach details you haven't seen, 21 de agosto de 2015

Melhor prática 1: implementar controles e processos auxiliares

Um bom ponto de partida é definir processos e controles que ajudam a gerenciar os riscos, algo semelhante ao que acontece com a maioria dos problemas de segurança das informações. Isso é muito importante para gerenciar os riscos de terceiros, pois grande parte das atividades ocorre fora do alcance e controle diretos da equipe de segurança das informações. Como é possível estabelecer relações de negócios e fornecer acesso sem o conhecimento ou a análise por parte da equipe de segurança das informações, é necessário que haja o envolvimento dessa equipe nas negociações contratuais para que as diretivas apropriadas sejam desenvolvidas e aplicadas como parte da estrutura geral de gerenciamento de identidades e acesso.

A parte simples do processo é provisionar, desprovisionar e definir as diretivas apropriadas para os usuários com privilégios que não são funcionários. Da mesma forma como acontece com outros usuários com privilégios, os seguintes aspectos precisam ser esclarecidos:

- Definição e treinamento dos usuários
- Sistemas e recursos aos quais o acesso é necessário
- Nível de privilégios necessário para a execução das tarefas
- Todas as restrições a serem aplicadas
- Frequência de monitoramento, de gravação de sessões, de alertas e de análise de sessões

A maioria das organizações já conta com essas diretivas para usuários com privilégios. Se essas diretivas não existirem, será necessário criá-las. Os mesmos processos e controles que se aplicam aos usuários com privilégios que são funcionários devem ser aplicáveis aos não funcionários. Geralmente, o gerenciamento desses processos fica por conta da equipe de operações de TI, dos indivíduos responsáveis pelo gerenciamento de identidades ou de um grupo contratado. Esses grupos devem estar cientes e estar de acordo com os processos de treinamento, provisionamento, monitoramento e desprovisionamento de usuários terceiros com privilégios.

Padrões de segurança

De maneira geral, sua segurança é tão forte quanto seu elo mais fraco. Por meio de um usuário com privilégios que trabalha para um parceiro, os processos e a infraestrutura desse parceiro se tornam parte da própria infraestrutura de TI da organização. Um único parceiro com controles ineficazes ou segurança inadequada pode ser um canal para que hackers violem a proteção da organização, conforme comprovado pela violação do Departamento de Administração de Pessoal dos EUA, que ocorreu por meio de credenciais que foram roubadas da empresa contratada KeyPoint Government Solutions. Desse modo, sob um ponto de vista de gerenciamento de riscos, a avaliação da segurança de cada parceiro com relação aos padrões organizacionais já estabelecidos é de extrema importância. Em um número cada vez maior de casos, a PCI, a HIPAA e outras normas de conformidade exigem a realização de avaliações dos fornecedores terceiros e a descrição dos requisitos específicos.

A maioria das organizações já conta com padrões estabelecidos de segurança das informações. Esses padrões devem ser aplicados aos fornecedores terceiros. Inúmeras fontes estão disponíveis para o desenvolvimento de novos padrões de segurança das informações:

- A Shared Assessments publica um documento SIG (Standard Information Gathering - Coleta Padrão de Informações) para ajudar a padronizar o processo de avaliação e coleta de informações de segurança
- O OCC (Office of the Comptroller of the Currency) publica orientações amplas sobre o gerenciamento de riscos, com seções específicas à área de TI que podem ser utilizadas
- O FFIEC (Federal Financial Institutions Examination Council) publica documentos com padrões relevantes
- Ferramenta de avaliação de riscos de segurança do Departamento de Saúde e Serviços Humanos
- Controles de segurança e privacidade 800-53 da NIST para sistemas de informações federais

- Autoridades estaduais regulamentares
- Estruturas de controles e diretivas ISO 27002 ou COBIT

Além disso, as normas de conformidade específicas do setor podem incluir requisitos para trabalhar com terceiros:

- Padrão de segurança de dados PCI
- HIPAA HITECH

Implementação, treinamento e aplicação

Após a avaliação e o estabelecimento dos processos, é necessário que eles sejam implementados e aplicados pelas áreas Jurídica, de TI e de Finanças e pelas unidades de negócios que tiverem relacionamento com fornecedores como parte integrante da definição e implementação de contratos com terceiros. Estes são os elementos básicos que devem ser incluídos nos contratos com terceiros:

- Garantias: referências às diretivas e aos procedimentos reais que um fornecedor se compromete a aplicar, incluindo verificações de histórico e treinamento dos funcionários do fornecedor com acesso aos sistemas da organização.
- Medidas corretivas: multas por processos de correção e não conformidade.
- Provisões de auditoria: verificações e ajustes disponíveis para validar a conformidade e frequência das auditorias.

Essas cláusulas fundamentais de gerenciamento de riscos devem ser incorporadas às partes relevantes do processo de contrato e implementação. A natureza detalhada da diretiva e da aplicação varia conforme a área de negócios, equilibrando os riscos e os custos.

Melhor prática 2: melhorar a autenticação dos usuários

A maior oportunidade de mitigação de riscos, em que o mínimo de custo e esforço pode proporcionar o máximo de redução de riscos, está na identificação e autenticação dos usuários. Conforme já mencionado, cerca de dois terços das violações podem ser causados pelo processo inadequado de identificação e autenticação dos usuários terceiros, incluindo o gerenciamento de credenciais (ou a ausência dele). Em geral, as organizações de terceiros tendem a ser empresas menores, que não contam com a maturidade de segurança e a experiência das organizações maiores. Geralmente, isso gera inúmeros problemas. As credenciais dos usuários podem ser comprometidas de duas maneiras: credenciais fracas e gerenciadas de maneira inadequada ou divulgação não intencional das credenciais à pessoa errada.

- **Credenciais fracas:** mesmo diante da escolha de uma senha forte, a aplicação da duração e das regras de senha pode ser um processo entediante. As pessoas, principalmente os fornecedores menores, não praticam esse processo. Por exemplo, vamos supor que um fornecedor terceiro use as mesmas credenciais de senha e ID de usuário para todos os clientes. Assim que os invasores conseguissem comprometer um conjunto de credenciais de um cliente, eles simplesmente poderiam ter acesso à lista de clientes do fornecedor (que foi criteriosamente publicada no site do fornecedor) e invadir o restante das organizações, uma a uma.
- **Divulgação equivocada:** de acordo com estatísticas recentes, o índice de sucesso em tentativas recorrentes de phishing está próximo dos 100% após apenas de cinco a sete tentativas. Isso é um reflexo do nível de sofisticação que esses esforços passaram a ter e da natureza humana dos usuários mais experientes e sofisticados. Um único erro pode levar a prejuízos, como visto no caso da violação que ocorreu na rede de energia elétrica da Ucrânia em dezembro de 2015. Isso significa que até mesmo os parceiros de negócios mais experientes podem estar sujeitos a ataques de phishing.

A melhor forma de proteger as credenciais usadas para acessar os sistemas é gerenciá-las e controlá-las proativamente por meio da definição e da aplicação de diretivas, incluindo:

- Complexidade
- Frequência de alterações
- Autenticação de vários fatores

Uma melhor prática para o gerenciamento de credenciais é a autenticação de vários fatores para todos os terceiros (e usuários internos com privilégios). Assim que uma organização torna-se o alvo, é apenas uma questão de tempo para que as credenciais usadas por um fornecedor terceiro sejam comprometidas. Por exemplo, na violação que ocorreu na rede de energia elétrica da Ucrânia, o malware BlackEnergy foi entregue a um usuário confiável e com privilégios por meio de um anexo do Microsoft Office infectado e usado como um vetor de acesso inicial para obter as credenciais legítimas. A melhor maneira de impedir que isso aconteça é adicionando outro fator ao processo de autenticação. Inúmeras opções de autenticação de vários fatores estão disponíveis. A opção específica mais eficaz dependerá de uma combinação de fatores econômicos e regulamentos ou normas de conformidade. Por exemplo, no governo federal dos EUA, há requisitos específicos para o uso de cartões PIV/CAC para usuários administrativos e com privilégios. Em outros ambientes, estão disponíveis outras opções, incluindo certificados, tokens com base em hardware e em software, além de processos de verificação que utilizam o telefone celular de uma pessoa. A economia da autenticação de vários fatores é muito favorável, facilitando a criação do caso de negócio.

A eficácia do gerenciamento de credenciais de terceiros depende do fato de cada um dos usuários do fornecedor ter credenciais individuais, algo que não é consistente com as atuais práticas de negócios em muitas organizações. Em muitos casos, em vez de criar uma conta para um usuário, é criada uma conta para um fornecedor, considerando que qualquer um dos funcionários do fornecedor poderá usar a mesma conta e as mesmas credenciais. Isso pode ser muito mais fácil em termos administrativos. Entretanto, os seguintes problemas ocorrerão quando várias pessoas compartilharem uma conta:

- A autenticação de vários fatores é mais complicada.
- A capacidade de controlar o acesso às credenciais e o uso delas é mais complicada, principalmente em casos quando alguém sair da organização ou mudar de função. É muito mais fácil ocorrer o roubo ou a divulgação de credenciais compartilhadas.
- A atribuição, a capacidade de determinar as ações específicas que cada um desses indivíduos realizou na rede, é perdida. Se uma conta for compartilhada entre várias pessoas, não haverá uma forma de saber qual dessas pessoas realizou a ação que gerou problemas.

Implementar um processo em que as credenciais sejam emitidas a indivíduos, e não a um fornecedor, elimina significativamente esses problemas e simplifica o processo de incluir e excluir usuários. Quando alguém passa a fazer parte da organização do parceiro de negócios, uma conta é criada, e o acesso é fornecido. Essa conta e esse acesso poderão ser encerrados com a mesma rapidez e facilidade quando esse indivíduo sair da empresa ou mudar de função. O sucesso na autenticação de usuários e no gerenciamento de acesso não é apenas uma questão tecnológica, mas também uma questão que envolve pessoas, processos e treinamento que precisa ser tratada ao negociar contratos com o fornecedor e estabelecer processos. Os fornecedores precisam fornecer notificações sobre mudanças no quadro de funcionários, um trabalho extra para eles. Além disso, é necessário que existam procedimentos para facilitar a comunicação desses eventos por parte do fornecedor. De modo geral, esse esforço administrativo adicional vale a pena devido às melhorias na segurança e no controle que essas abordagens oferecem. Na verdade, as normas regulamentares exigem o controle de acesso e a autenticação em nível individual, pois eles são muito eficazes.

A última área, que talvez seja menos comum nas organizações, é o requisito das verificações de histórico e da comprovação de identidades de terceiros que acessam os sistemas da organização. Mais uma vez, essa é uma questão de gerenciamento de riscos — o custo envolvido (tanto financeiro quanto administrativo) geralmente é justificado, principalmente em ambientes confidenciais.

O armazenamento de credenciais é uma tecnologia que centraliza e automatiza as regras de complexidade de senhas, as alterações de senha e a integração de sistemas de autenticação de vários fatores. A próxima opção mais acessível depois do gerenciamento de credenciais é a separação da autenticação do controle de acesso.

Melhor prática 3: separar a autenticação do controle de acesso

Na maioria das redes, assim que uma pessoa obtém acesso à rede, ela passa a ter visibilidade de uma ampla variedade de dispositivos e sistemas e, possivelmente, acesso a eles. Entre os resultados dessa arquitetura de rede estão as violações como as que ocorreram na Target, na Home Depot, na rede de energia elétrica da Ucrânia e em muitas outras empresas. Todas elas ocorreram com o uso de uma cadeia de destruição de violação. Com a cadeia de destruição de violação, os invasores concluem uma série de etapas — muitas vezes, de maneira iterativa — para executar uma violação. O ataque inicia com a obtenção de acesso inicial a uma rede, geralmente por meio do comprometimento das credenciais do terceiro ou do fornecedor. Depois disso, o invasor pode vasculhar a rede violada para encontrar vulnerabilidades ou credenciais adicionais que possam ser exploradas para obter ainda mais acesso com níveis ainda maiores de privilégios, até finalmente atingir seu alvo final, como foi o caso da rede de energia elétrica da Ucrânia.

> "Todas as três empresas afirmaram que os invasores limparam alguns sistemas executando o malware KillDisk na conclusão do ataque cibernético. O malware KillDisk apaga arquivos selecionados nos sistemas de destino e corrompe o registro de inicialização mestre, tornando os sistemas inoperáveis. Também foi relatado que, em pelo menos uma instância, as HMIs (Human-Machine Interfaces – Interfaces Homem-Máquina) com base em Windows integradas a unidades de terminal remotas também foram sobrescritas pelo KillDisk. Os invasores também tornaram os dispositivos de conversão serial para Ethernet em subestações inoperáveis, corrompendo o firmware. Além disso, os invasores supostamente programaram desconexões para o no-break do servidor por meio da interface de gerenciamento remoto do no-break. A equipe avalia que essas ações foram realizadas como uma tentativa de interferir nos esforços de restauração."
>
> Ataque cibernético contra infraestrutura essencial da Ucrânia
> Data de publicação original: 25 de fevereiro de 2016

Conforme mencionado na Melhor prática 2, uma forma de acabar com essa cadeia de destruição é controlando o acesso à rede e dificultando a entrada de um invasor com o uso da autenticação de vários fatores. Outra camada de defesa é limitar a visibilidade e o acesso aos recursos na rede. A maioria dos fornecedores precisa de acesso somente a sistemas muito específicos. Não é necessário que eles tenham acesso nem visibilidade de toda a rede nem mesmo de uma sub-rede.

É possível limitar o acesso e a visibilidade com o uso de uma segmentação de rede física. Geralmente, isso é feito para cumprir uma norma regulamentar. Ao segmentar a rede e controlar o acesso, é possível limitar o escopo dos recursos disponíveis. Embora essa abordagem possa ser eficaz, ela apresenta deficiências:

- Despesas administrativas gerais necessárias para configurar e manter essa arquitetura de rede
- Vulnerabilidade das conexões entre as diferentes partes da rede - um invasor pode encontrar uma forma de passar pelas conexões de rede a fim de obter acesso a seu alvo

A melhor alternativa é usar a segmentação lógica com uma solução de gerenciamento de identidades com privilégios, como o CA Privileged Access Manager, que pode limitar o acesso aos recursos. Essa solução funciona por meio da implementação de um "ponto de contenção" pelo qual um usuário terceiro deve passar para obter acesso a recursos protegidos. Essa abordagem proporciona inúmeros benefícios:

- **Controle de acesso com confiança zero:** um logon bem-sucedido não fornece acesso a toda a rede. Em vez disso, o sistema aplica diretivas que especificam quais recursos estão disponíveis a um usuário, o que limita um indivíduo a apenas esses sistemas. Essa abordagem permite um controle rigoroso quanto à visibilidade e ao acesso — um indivíduo nunca verá os recursos aos quais ele não tem permissão de acesso. O usuário vê apenas uma lista predefinida dos sistemas aos quais ele tem permissão de visualização e acesso.
- **Prevenção contra leapfrog:** para controlar o movimento lateral dentro de uma rede, o sistema intercepta uma variedade de comandos de rede, como TELNET ou SSH, e impede a execução deles. Esse recurso limita o acesso de terceiros a somente sistemas especificados previamente, eliminando as formas de obter visibilidade do restante da rede e as tentativas de acessar outros sistemas.

É importante padronizar e consolidar os métodos de acesso com um ponto de contenção, usando uma solução de gerenciamento de acesso com privilégios, uma VPN ou qualquer outra solução que direcione o acesso por meio de caminhos conhecidos. Ao definir caminhos aceitáveis para o acesso externo aos recursos, o processo de monitoramento torna-se mais fácil. Ao conter protocolos não aprovados e direcionar sessões aprovadas para um caminho predefinido, fica mais fácil identificar as irregularidades para uma investigação mais detalhada, em que o SIEM e as ferramentas de geração de registros podem ajudar a sinalizar eventos anormais.

Melhor prática 4: impedir erros e comandos não autorizados

As permissões e os direitos de acesso podem ser usados para limitar o acesso a recursos da tecnologia da informação. Muitas vezes, essa abordagem não oferece o nível de precisão necessário para realmente controlar as ações de um usuário em um sistema. Por exemplo, um administrador de sistema terceiro talvez precise fazer logon em um servidor usando uma conta de superusuário altamente privilegiada, como root ou admin. Motivos técnicos ou administrativos podem garantir essa abordagem de acesso, gerando uma situação arriscada. Com esse nível de autoridade, o indivíduo pode fazer tudo o que quiser no sistema, incluindo a exclusão completa dele, o que é um risco inaceitável para a maioria das organizações, mesmo se esse indivíduo for um funcionário dentro da empresa.

O uso de uma solução de gerenciamento de acesso com privilégios fornece uma abordagem mais aceitável habilitando o controle de permissões refinado para gerenciar melhor esse tipo de usuário. O sistema de gerenciamento de acesso com privilégios permite que um usuário tenha sessões mediadas em nome dele para vários sistemas de destino usando inúmeras contas diferentes (por exemplo, uma conta root), cada uma com níveis de permissão diferentes.

Também é possível usar filtros de comandos, listas negras e listas brancas para limitar os comandos que um usuário específico pode realizar. Uma lista negra contém os comandos não permitidos, enquanto uma lista branca contém os comandos que podem ser executados. Quando usadas em conjunto, essas listas fornecem um alto nível de controle e flexibilidade. Desse modo, esse usuário com privilégios pode manter o recurso de computação sem causar danos inaceitáveis. Um benefício inesperado resultante do filtro de comandos é a prevenção de erros não intencionais. No exemplo anterior, o superusuário conseguirá mover arquivos, mas não conseguirá reformatar o disco.

Combinados com a geração de registros, os filtros de comando facilitam o processo de monitoramento e envio de alertas para que o sistema responda de maneira adequada quando alguém tentar violar um dos filtros, seja enviando um aviso ou encerrando uma sessão ofensiva. Por exemplo, um usuário pode tentar fazer alguns experimentos antes de atingir os limites reforçados pelos filtros de comando — quando os limites são acionados, o sistema pode gerar um alerta que solicita uma investigação sobre as ações desse usuário. Aqui estão algumas das possíveis respostas:

- Bloquear e avisar o usuário
- Encerrar a sessão
- Desativar a conta de usuário
- Gerar alertas/alarmes para o SOC

Melhor prática 5: monitorar e investigar

É necessário sempre um certo nível de monitoramento. O nível específico e o escopo de monitoramento dependem das considerações de gerenciamento de riscos e conformidade.

Mesmo em casos com pouco risco inerente, a geração de registros em log ajuda a solucionar problemas e investigar atividades suspeitas. A geração básica de registros em log consiste em uma simples gravação do que ocorreu e é muito útil para analisar atividades inadequadas ou não autorizadas. Ela inclui:

- Horários de logon e logoff
- Sistemas acessados
- Comandos executados
- Respostas recebidas

Em qualquer tipo de situação confidencial, o monitoramento utiliza logs para aplicar diretivas estabelecidas de acesso ao sistema, pois os esforços de violação dessas diretivas requerem atenção. Inúmeras ações podem ser realizadas como resposta a uma tentativa de violação de diretiva — em um nível básico, as tentativas de violação de diretivas requerem uma investigação para descobrir o que aconteceu. Talvez seja necessário treinamento adicional para ajudar os usuários a compreenderem as tarefas que eles devem executar e como elas devem ser executadas. Uma violação pode ser um erro simples ou uma indicação de tentativa de comportamento mal-intencionado. O monitoramento ajuda a capturar eventos suspeitos para que estes sejam investigados.

As investigações são muito importantes, conforme visto no caso da JPMorgan Chase, em que os funcionários descobriram que tinham ocorrido violações após investigar um de seus fornecedores.

"A JPMorgan notou a presença de hackers em seus sistemas em agosto, depois de descobrir que o mesmo grupo de hackers tinha invadido o site destinado a uma corrida beneficente patrocinada pelo banco. Só depois de descobrir que o site Corporate Challenge tinha sido violado é que a JPMorgan detectou que sua própria rede tinha sido atacada pelos mesmos hackers."

"Neglected Server Provided Entry for JPMorgan Hackers"
The New York Times, 22 de dezembro de 2014

Em situações ainda mais confidenciais, a captura ou gravação de sessões talvez seja necessária para fornecer informações completas sobre o que aconteceu em uma determinada sessão e auxiliar em possíveis investigações futuras. Um caso de uso comum é capturar a gravação em tela inteira das sessões confidenciais. Em casos de violações de diretivas conhecidas ou problemas subsequentes com um sistema, essa gravação poderá ser analisada posteriormente com o objetivo de avaliar o que aconteceu na sessão original. Dependendo da confidencialidade do ambiente, poderão ser realizadas verificações por amostragem. Um dos desafios geralmente associados à gravação de sessões é que os arquivos de gravação podem ser extensos e as despesas gerais do sistema podem ser altas. O outro desafio é que deve haver um plano de ação para analisar as sessões gravadas. Como os custos relacionados ao tempo e à tecnologia aumentam para a gravação de sessões, a análise de custo e benefício ajudará a identificar as situações apropriadas para esse nível de investimento. Como ponto de partida, é recomendável identificar o seguinte:

- Quando é necessário fazer a gravação e por quanto tempo
- Quando será necessário analisar as gravações e com que frequência isso será feito
- Qual é a diretiva de retenção das gravações

Se você optar por implantar as técnicas de gravação de sessões, é importante considerar diversos recursos importantes:

- Fácil acesso aos metadados sobre a sessão — quando ela foi iniciada e encerrada.
- Capacidade de passar rapidamente pelas sessões e ir a um ponto específico de uma gravação.
- Capacidade de destacar atividades "interessantes", como violações de diretiva e atividades confidenciais.

As situações que representam riscos mais elevados podem exigir monitoramento específico ("over the shoulder") ou acesso de duas partes, que exige que outro indivíduo veja o que um usuário com privilégios faz em tempo real. Geralmente, essas situações de risco extremo não ocorrem com terceiros ou outros usuários externos. O monitoramento específico apresenta alguns desafios técnicos. Entretanto, além disso, o responsável pelo monitoramento deve ser altamente experiente para que consiga entender as ações realizadas e suas ramificações no ambiente mais amplo. Sob uma perspectiva de gerenciamento de riscos, o monitoramento específico pode ser apropriado para um número muito pequeno de situações.

O monitoramento típico inclui um processo composto por duas etapas:

- **Resposta em tempo real para as violações de diretiva:** várias ações podem ocorrer: aviso ao usuário, geração de um alerta para a central de operações de segurança ou encerramento de uma conta ou sessão.
- **Pesquisa e análise após o fato:** uma análise dos registros ou das gravações de sessões para auxiliar na solução de problemas ou em investigações forenses.

A pesquisa e análise após o fato podem incluir esforços para correlacionar registros e alertas gerados por um sistema de gerenciamento de acesso com privilégios a outras ferramentas de segurança e rede para a detecção de eventos inesperados. Por exemplo, em organizações em que há uma solução de gerenciamento de acesso com privilégios, toda a atividade administrativa é centralizada nesse tipo de sistema. Se as solicitações de sessão SSH ou TELNET vierem de outras partes da rede, elas serão vistas como alertas imediatos de que algo está errado e serão investigadas. Ao eliminar ou banir ferramentas administrativas não autorizadas, fica relativamente fácil identificar as atividades suspeitas. Um firewall de última geração pode auxiliar na sinalização de aplicativos ou protocolos não permitidos. Outras atividades suspeitas podem incluir acesso em horários inesperados ou comportamentos incomuns, como downloads de arquivos.

Com o passar do tempo, as análises e as auditorias manuais contínuas ajudam a refinar as ferramentas e diretivas para ignorar falsos positivos e automatizar gatilhos e alertas para que sejam mais eficazes.

Seção 3:

Benefícios do gerenciamento de riscos de terceiros

Nenhuma organização moderna pode ficar isolada e desconectada da internet. As relações de negócios exigem a colaboração eletrônica, na qual ocorre a troca de informações confidenciais entre parceiros. Atualmente, as empresas usam provedores terceiros para serviços de contabilidade, processamento de cartões de crédito, assessoria jurídica, administração de planos de previdência, serviços de marketing, manufatura e centenas de outras tarefas. A colaboração eletrônica entre parceiros de negócios economiza tempo e dinheiro e possibilita a utilização de sistemas e processos automatizados que aumentam a precisão, a qualidade e a eficiência. Restringir o acesso de terceiros à rede no firewall não é uma opção. Recursos relevantes devem estar disponíveis para os parceiros de negócios, de modo que seja possível desfrutar dos benefícios. Ao mesmo tempo, as empresas enfrentam riscos reais ao se conectarem com terceiros.

As violações de segurança são dispendiosas. De acordo com a revista Fortune, após o roubo de 40 milhões de cartões de pagamento e 70 milhões de outros registros no final de 2013, a Target estimou custos de US$ 162 milhões após o reembolso dos seguros. A Sony estimou gastos de US$ 35 milhões na "restauração de sistemas financeiros e de TI" após uma violação em 2014. A Home Depot registrou US$ 28 milhões em despesas líquidas antes da cobrança de impostos. Os custos acima mencionados não incluem danos à reputação nem o aumento dos prêmios de seguro. Além desses custos "desagradáveis", a vida das pessoas mudou totalmente. Muitas pessoas perderam seus empregos, e aquelas que continuaram na empresa tiveram de trabalhar arduamente na investigação e atenuação das violações.

> "Independentemente do modo como avaliamos tudo isso ou se pensamos no que aconteceu ou no que ainda pode acontecer, concordamos com o fato de que as empresas precisam investir na segurança das informações."
>
> Benjamin Dean, membro da School of International and Public Affairs da Columbia University - revista Fortune, 27 de março de 2015

Obviamente, nenhuma empresa quer ser capa do The Wall Street Journal como exemplo de outra grande violação. As cinco principais melhores práticas de segurança das informações podem bloquear as violações e possibilitar atividades de negócios legítimas, mantendo a segurança da reputação e dos ativos de informação de sua organização.

Seção 4:

Conclusões

De acordo com o DBIR (Data Breach Investigations Report - Relatório de Investigações de Violações de Dados) de 2015 da Verizon, o comprometimento de 700 milhões de registros resultou em uma perda financeira estimada de US$ 400 milhões. As 70 organizações que contribuíram para a conclusão desse relatório documentaram 79.790 incidentes de segurança, sendo que 2.122 deles foram violações confirmadas em 61 países, com dois terços dos incidentes ocorrendo nos EUA. Embora a grande maioria das ameaças ainda venha de fontes externas, as ameaças internas e de parceiros aumentaram um pouco entre 2013 e 2014. Os riscos são reais, conforme evidenciado pela enorme violação no Departamento de Administração de Pessoal dos EUA.

O método de ataque ao OPM seguiu uma fórmula: ter como alvo um prestador de serviços em um ataque de engenharia social e roubar as credenciais para obter acesso à rede. Implantar o malware em um sistema e criar uma backdoor. Vazar dados durante muitos meses, sem nenhum tipo de detecção.

A violação do OPM também enfatizou a vulnerabilidade das organizações quanto à engenharia social. Prestadores de serviços e funcionários do governo agora passam por programas de treinamento para obter conscientização sobre segurança e conhecer os perigos do spear phishing e de outras ameaças de mídia social.

> "The most innovative and damaging hacks of 2015",
> Revista CSO, 28 de dezembro de 2015

Muitos riscos podem ser atenuados com o uso das cinco melhores práticas descritas neste documento que trabalham juntas para criar uma defesa de segurança das informações mais eficiente, flexível, robusta e em camadas. Essas práticas incluem:

- Implementar controles e processos auxiliares que definam e apliquem diretivas para usuários terceiros com privilégios.
- Melhorar a autenticação dos usuários usando tecnologia de autenticação de vários fatores para que seja mais difícil afetar as credenciais com privilégios, mesmo com ataques de phishing e engenharia social.
- Separar a autenticação do controle de acesso para que os usuários com privilégios tenham visibilidade limitada das redes internas, o que limita os possíveis danos que um usuário ou um conjunto de credenciais roubadas podem causar.
- Impedir erros e comandos não autorizados para que os gatilhos em tempo real sejam a primeira linha de defesa, protegendo a infraestrutura contra erros não intencionais e tentativas mal-intencionadas.
- Monitorar e investigar atividades suspeitas para rapidamente identificar violações, aprimorar o treinamento quando necessário e aperfeiçoar continuamente a automação e os processos para a eliminação de falsos positivos.

Os sistemas de gerenciamento de acesso com privilégios têm recursos automatizados que ajudam a definir, automatizar e aplicar as cinco melhores práticas, descritas neste documento, por toda a empresa, em ambientes físicos, virtuais e na nuvem, ajudando as organizações a implementarem processos consistentes em sistemas, aplicativos e dispositivos.

Seção 5

Referências

https://www.brighttalk.com/webcast/9017/156931

http://www.xceedium.com/solutions/privileged-identity-management/432-2

http://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233/op-1

http://www.bankinfosecurity.com/banks-vendor-monitoring-comes-up-short-a-8103

Relatório do Departamento de Serviços Financeiros do estado de Nova York, 9 de abril, "Update on Cyber Security in the Banking Sector: Third Party Service Providers"
http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?emc=edit_tu_20160301&nl=bits&nlid=59970007

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html

How Much do Data Breaches Cost Big Companies? Shockingly Little
http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ 27 de março de 2015

http://fortune.com/tag/data-breach 2 de março de 2016

http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10?itc=refresh 27 de julho de 2015

https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx 21 de agosto de 2015

http://www.csoonline.com/article/3018343/security/the-most-innovative-and-damaging-hacks-of-2015.html

Seção 6:

Sobre o autor

Dale R. Gardner trabalhou na área de software corporativo durante mais de duas décadas, concentrando-se nas áreas de gerenciamento de redes e sistemas e em vários segmentos de segurança, incluindo gerenciamento de identidades, segurança de aplicativos, gerenciamento de vulnerabilidades, conformidade e segurança de rede. Anteriormente escritor e analista de pesquisas, ele definiu, compilou e comercializou várias soluções de gerenciamento e segurança que melhoram as operações e ajudam a garantir a integridade e confiabilidade da infraestrutura de tecnologia da informação corporativa. Atualmente, ele é responsável pelo marketing global do portfólio de produtos de gerenciamento de acesso com privilégios da CA Technologies.