DOCUMENTAÇÃO TÉCNICA | OUTUBRO DE 2014

Ameaças persistentes avançadas: como se defender de dentro para fora

Russel Miller
Gerenciamento de segurança da CA Technologies

ca technologies

Sumário

Resumo executivo

Desafio

Proteger uma organização é um desafio cada vez mais difícil. A complexidade dos ataques está aumentando, e o surgimento das ameaças persistentes avançadas, um tipo de ataque direcionado, fez as organizações ficarem mais cientes de sua vulnerabilidade ao ataque. Empresas como RSA Security, Google e Northrup Grumman se viram na mira das ameaças persistentes avançadas. Não ter sido vítima de uma violação significativa no passado não é garantia de segurança no futuro, pois as organizações que estão especificamente na mira das ameaças persistentes avançadas enfrentam desafios com os quais os administradores de segurança não estão habituados a lidar, como o espaçamento das ações no decorrer de vários meses ou anos para evitar a detecção. O dano causado por uma violação também está se agravando e se tornando motivo de preocupação para os executivos de nível sênior.

Oportunidade

Não há "bala de prata" quando se trata de se defender contra as ameaças persistentes avançadas. Várias camadas de proteção devem ser empregadas e combinadas para reduzir o potencial de violação e atenuar o dano, caso ele venha a ocorrer.

A abordagem inicial para se defender contra os ataques direcionados era proteger o perímetro usando firewalls e sistemas de detecção de invasões para detectar e bloquear comportamentos anômalos. Essa abordagem pode ser eficaz para se defender contra determinados tipos de ataques, mas não consegue oferecer proteção contra todos os vetores, como "spear phishing" e "engenharia social".

Embora não haja um único produto de segurança — com base em tecnologia ou outro recurso — que possa proteger totalmente uma organização contra ameaças persistentes avançadas, a disponibilidade atual de soluções de segurança entre domínios pode ajudar as organizações a se protegerem melhor do que nunca. Gerenciamento de identidades com privilégios, controle e proteção de informações e segurança da infraestrutura interna são áreas que tradicionalmente foram tratadas de forma isolada, mas que agora podem ser combinadas para permitir que as organizações protejam sua infraestrutura de TI e seus datacenters de maneiras complementares. A CA Technologies chama isso de inteligência de dados e identidades.

Benefícios

Ao compreender as ameaças persistentes avançadas e se proteger contra elas, as organizações reduzem seu risco, caso se tornem alvos específicos de um ataque. O risco reduzido não é apenas financeiro, mas também de reputação, operacional, legal e regulatório.

Ao adotar uma visão holística da segurança que possa ser usada contra as ameaças persistentes avançadas, a organização também está se protegendo contra ataques menos avançados, automatizados e até internos. Uma abordagem abrangente para a segurança tem muitas outras vantagens, incluindo melhorar a conformidade, viabilizar serviços com base na nuvem, melhorar a segurança da virtualização e economizar custos.

Seção 1: Desafio

Ameaças persistentes avançadas: não se trata dos negócios do dia a dia

Ameaças persistentes avançadas apresentam desafios diferentes dos riscos à segurança tradicionais. A ameaça persistente avançada consiste em um ataque duradouro e sofisticado a uma entidade-alvo específica. O invasor é frequentemente patrocinado pelo governo e busca obter informações valiosas de inteligência de outros governos, mas os ataques também podem ser originados em e destinados a organizações privadas. Esse termo foi usado pela primeira vez pela Força Aérea dos EUA em 2006.[1] O NIST (National Institute of Standards and Technology) define as ameaças persistentes avançadas da seguinte maneira:[2]

"A ameaça persistente avançada é um adversário com níveis sofisticados de conhecimento e recursos significativos, o que lhe permite, por meio do uso de vários vetores de ataque (por exemplo, ataques online, físicos e de ludibriação), gerar oportunidades para atingir seus objetivos que, geralmente, são estabelecer e ampliar sua presença dentro da infraestrutura de tecnologia da informação das organizações com a finalidade de vazar informações continuamente e/ou sabotar ou impedir aspectos cruciais de uma missão, programa ou organização ou, ainda, se colocar em uma posição para fazer isso no futuro. Além disso, a ameaça persistente avançada persegue seus objetivos repetidamente por um período prolongado, adaptando-se aos esforços do defensor de resistir a ela, com o propósito de manter o nível de interação necessário para executar seus objetivos."

Embora haja outras definições, três palavras ajudam a esclarecer o que é uma ameaça persistente avançada:[3]

- **Avançada:** o invasor tem recursos técnicos significativos para conseguir explorar vulnerabilidades no alvo. Isso pode incluir acesso a grandes bancos de dados de vulnerabilidades, explorações e habilidades de codificação, mas também a capacidade de descobrir e tirar proveito de vulnerabilidades até então desconhecidas.
- **Persistente:** as ameaças persistentes avançadas frequentemente ocorrem por um período prolongado. Diferentemente dos ataques de curta duração que tiram proveito de oportunidades temporárias, as ameaças persistentes avançadas podem durar anos. Vários vetores de ataque podem ser usados, desde ataques com base na internet até engenharia social. Pequenas violações de segurança podem ser combinadas com o tempo para obtenção de acesso a dados mais significativos.
- **Ameaça:** para haver uma ameaça, deve haver um invasor com motivação e capacidade para realizar um ataque bem-sucedido.

Ferramentas puramente automatizadas não são consideradas ameaças persistentes avançadas em si, embora possam ser usadas por um grupo organizado e coordenado como parte de um ataque maior.

Estágios

Uma típica ameaça persistente avançada pode ser composta pelos quatro estágios a seguir:

Figura A.

Quatro estágios de uma ameaça persistente avançada

1. **Reconhecimento:** investigação das vulnerabilidades de uma organização. Isso pode incluir desde uma pesquisa básica, inclusive consultas de domínio, até verificações de portas e vulnerabilidades.
2. **Entrada inicial:** exploração de pontos fracos para estabelecer a presença na rede-alvo. Isso pode ser feito usando métodos técnicos sofisticados ou técnicas como "spear phishing" (ataques de phishing direcionados), que resultam na obtenção de acesso de um usuário normal a um único sistema. "Engenharia social", ou a exploração de pessoas, é também um método comum para se obter acesso.
3. **Elevação de privilégios e expansão do controle:** quando um invasor penetra no perímetro da rede, ele tenta obter privilégios e controle adicionais sobre sistemas essenciais. Essa etapa também pode envolver a instalação de ferramentas de backdoor ("porta dos fundos") para simplificar o acesso futuro à rede.
4. **Exploração contínua:** uma vez estabelecido o controle, o invasor pode exportar dados confidenciais continuamente.

O terceiro e quarto estágios podem acontecer no decorrer de vários anos, a fim de reduzir o risco de detecção.

O que torna as ameaças persistentes avançadas diferentes?

A principal diferença entre as ameaças persistentes avançadas e as ameaças "normais" é o fato de terem uma organização específica como alvo. Embora a defesa do perímetro e o uso de controles de segurança padrão possam proteger a organização contra ataques comuns, essas técnicas podem não ser suficientes ao enfrentar ameaças persistentes avançadas. Invasores pacientes podem aguardar que novas vulnerabilidades revelem um ponto fraco ou podem combinar vulnerabilidades aparentemente pequenas para formar um ataque prejudicial em larga escala.

Quando se enfrenta uma ameaça como essa, as regras normais não valem. No passado, muitas organizações precisavam simplesmente ter uma segurança melhor do que outras empresas e organizações conectadas à internet, pois muitos invasores escolhiam os alvos mais fáceis. Mas com as ameaças persistentes avançadas, as organizações precisam ser capazes de derrotar um inimigo motivado que vai se concentrar em procurar pontos fracos, em vez de sair à caça de outro alvo.

O espaço de tempo das ameaças persistentes avançadas também pode tornar a detecção particularmente difícil. Em uma violação de segurança padrão, volumes significativos de dados podem ser exportados em um curto espaço de tempo, possibilitando que firewalls e dispositivos de detecção de invasões descubram a violação. Um invasor em uma ameaça persistente avançada pode levar meses e até anos parar exportar os dados desejados, passando despercebido até mesmo por sistemas bem configurados com recursos completos.

Objetivos	Alvos
Devido à sua natureza direcionada, os executores de ameaças persistentes avançadas muitas vezes têm objetivos diferentes dos hackers de internet comuns, incluindo um foco maior nos seguintes objetivos, em vez de roubos simples e molecagens: ▪ Manipulação política ▪ Espionagem militar ▪ Espionagem econômica ▪ Espionagem técnica ▪ Extorsão financeira	Tipos específicos de organizações se encaixam mais no perfil de risco das ações de ameaças persistentes avançadas devido à natureza política e com patrocínio do governo da ameaça: ▪ Órgãos governamentais ▪ Organizações de defesa e prestadores de serviços ▪ Sistemas essenciais de infraestrutura (por exemplo, concessionárias de serviços públicos, sistemas de comunicações e transporte) ▪ Organizações políticas ▪ Instituições financeiras ▪ Empresas de tecnologia

Exemplos

RSA

Em 2011, a RSA Security anunciou ter sido vítima do que definiu como uma ameaça persistente avançada[4]. Os invasores conseguiram acesso inicial enganando um usuário interno, que abriu um email com um anexo de planilha que explorava uma vulnerabilidade de dia zero no Adobe Flash. A partir daí, os invasores escalonaram privilégios, instalaram backdoors e obtiveram o controle de outros sistemas.

Eles conseguiram obter acesso aos sistemas da RSA que mantinham informações relacionadas a seus tokens de autenticação de dois fatores, conhecidos como SecurID. Essas informações potencialmente incluíam valores capital, que a RSA usa com seus tokens para gerar senhas de uso único que mudam a cada 60 segundos. Se o código-fonte em si fosse roubado, os invasores poderiam procurar vulnerabilidades na implementação do SecurID ou até na própria criptografia.

Operação Aurora

Operação Aurora foi uma ameaça persistente avançada direcionada a diversas empresas de grande porte, como Google, Adobe, Rackspace e Juniper Networks. Os relatórios da mídia sugerem que muitas outras empresas estavam na mira, incluindo Yahoo, Northrup Grumman, Morgan Stanley, Symantec e Dow Chemical.[5] Acredita-se que o Politburo chinês tenha direcionado os ataques como parte de uma campanha coordenada de larga escala contra os Estados Unidos e outros países ocidentais.[6]

Seção 2: Oportunidade

Defesa em profundidade

O segredo para se defender de ameaças persistentes avançadas é uma defesa em profundidade. Se tiver tempo suficiente, um invasor determinado conseguirá violar a maioria dos perímetros de rede. Uma defesa bem-sucedida irá:

1. Dificultar a penetração inicial.
2. Reduzir o potencial de escalonamento de privilégios, caso uma conta seja comprometida.
3. Limitar o dano que pode ser infligido por uma conta comprometida, mesmo que ela tenha privilégios.
4. Detectar contas comprometidas e atividades suspeitas logo no início do processo.
5. Reunir informações úteis para uma investigação forense, de forma que seja possível determinar que danos ocorreram, quando e por quem.

Proteger o perímetro com firewalls e sistemas de detecção de invasões na borda da rede só ajuda na primeira e na quarta defesa. É necessário contar com uma estratégia de proteção mais ativa.

Detecção precoce

Frequentemente, as violações são detectadas depois que o invasor conseguiu acesso a uma rede interna e provocou danos ou roubou grandes quantidades de dados. Nesse ponto, a "defesa" contra a ameaça persistente avançada envolve um caro processo de controle de danos, limpeza e monitoramento contínuo. A chave para ter uma proteção acessível e gerenciável contra as ameaças persistentes avançadas está em detectá-las o quanto antes. Na fase inicial de um ataque, quando o invasor ganha acesso à rede pela primeira vez, a organização pode usar várias técnicas para detectar uma violação, incluindo desvincular e externalizar a segurança do sistema da administração do sistema, evitar e detectar tentativas de escalonamento de privilégios e de uso não autorizado do privilégio e auditar e registrar atividades dos usuários fora dos logs do sistema operacional (esse tipo de auditoria e registro pode ser desconhecido para o invasor).

O gerenciamento de identidades com privilégios, a proteção e o controle das informações e a segurança da infraestrutura interna formam o núcleo de uma estratégia de defesa em profundidade contra ameaças persistentes avançadas, juntamente com a detecção precoce. Essas técnicas estão detalhadas nas seções a seguir.

Gerenciamento de identidades com privilégios

As ferramentas de PIM (Privileged Identity Management - Gerenciamento de identidades com privilégios) gerenciam e monitoram contas administrativas, como "Administrador" no Windows e "raiz" no UNIX e Linux. Os sistemas de PIM:

- Implementam o princípio de "menos privilégios", mesmo para contas administrativas.
- Gerenciam o acesso às contas compartilhadas por meio de recursos de gerenciamento de senhas de usuários com privilégios.
- Monitoram as atividades dos usuários para ajudar a assegurar a responsabilização e auxiliar em uma investigação de violação de segurança.

Acesso com menos privilégios

Todas as pessoas devem ter os privilégios mínimos necessários para fazer seu trabalho. Embora esse conceito seja compreendido por muitas organizações, elas frequentemente falham ao implementá-lo na prática, particularmente para contas administrativas. Os indivíduos que precisam de algum nível de acesso com privilégios geralmente recebem a senha da conta administrativa relevante, que é compartilhada por várias pessoas.

O que as organizações devem perceber com o aumento da prevalência das ameaças persistentes avançadas é que o acesso com privilégios não precisa ser uma decisão do tipo "tudo ou nada". Os indivíduos podem receber privilégios elevados que lhes permitam executar apenas uma tarefa muito específica. No passado, isso era feito nos sistemas UNIX e Linux usando a ferramenta "sudo", mas ferramentas modernas de controle de acesso podem conceder e negar acesso de forma centralizada tanto para sistemas UNIX como Windows®.

Modelo de segurança: desvinculando a segurança da administração de sistemas

Um sistema operacional típico tem um modelo de segurança de duas camadas: usuários com privilégios e usuários comuns. Entretanto, para se proteger contra ameaças persistentes avançadas, é necessário um modelo mais sofisticado. Esse modelo baseia-se nos princípios de segurança padrão de "menos privilégios" e "segregação de tarefas". No mínimo, três funções administrativas principais devem ser definidas:

- **Administrador de sistemas:** o próprio administrador do sistema deve ter os privilégios necessários para fazer atualizações no software do servidor, alterações de configuração e instalações de software. Os administradores de sistemas não devem ser capazes de alterar configurações importantes de segurança ou ver logs relacionados à segurança.
- **Administrador de segurança:** esses administradores devem ser capazes de atualizar e alterar configurações de segurança e ver arquivos de log relacionados à segurança. Os administradores de segurança não devem ser capazes de instalar software ou acessar dados confidenciais em um sistema.
- **Auditor:** os auditores precisam ser capazes de verificar as configurações de segurança e ver arquivos de log, mas não devem ter a capacidade de fazer alterações em um sistema. Embora o acesso a arquivos confidenciais possa ser necessário, todos os acessos devem ser somente leitura.

Tipos de administrador adicionais devem ser criados quando apropriado, como administradores de banco de dados ou de outros aplicativos particularmente confidenciais.

O uso de um modelo de segurança com várias camadas cumpre duas metas simultaneamente: protege contra ameaças internas provenientes de contas de administrador, limitando o que cada indivíduo pode fazer, e também dificulta a ação das ameaças persistentes avançadas de invasores externos. Em vez de ter de comprometer uma conta de "superusuário", os invasores agora precisarão obter acesso a várias contas para ter acesso total a um sistema.

Controles refinados

Os controles refinados, além de constituírem uma boa prática de segurança, são particularmente úteis para atenuar os danos provocados por uma ameaça persistente avançada. Quando os invasores obtêm privilégios administrativos, eles geralmente instalam "rootkits" de backdoor e começam a exportar dados confidenciais. Com os controles de acesso adequados, mesmo um invasor com acesso privilegiado é limitado naquilo que consegue fazer, podendo ser impedido de acessar arquivos confidenciais, executar comandos mal-intencionados, instalar programas, interromper ou iniciar serviços ou alterar arquivos de log. Em um sistema no qual controles refinados são implementados, o invasor pode ser forçado a comprometer várias contas para fazer o que antes era possível com uma única conta.

A implementação de controles de acesso refinados também pode atenuar o risco de um dos maiores pontos fracos de segurança em uma organização: as pessoas. Usando o que se chama de técnicas de "engenharia social", os invasores costumam enganar os funcionários e outras pessoas de dentro da empresa para que forneçam informações que poderão ser usadas para obter acesso às suas contas ou revelar outros pontos fracos de segurança. Ao limitar o acesso a importantes sistemas e dados dos funcionários, os danos que podem ser causados por um invasor que obtenha acesso às contas por meio de engenharia social são reduzidos.

Gerenciamento de contas compartilhadas

O gerenciamento de contas compartilhadas (ou "gerenciamento de senhas de usuários com privilégios") é uma defesa importante contra as ameaças persistentes avançadas. A obtenção de acesso a identidades com privilégios (frequentemente, por meio de escalonamento de privilégios) é um passo intermediário importante em quase todos os ataques bem-sucedidos. As ferramentas de gerenciamento de senhas de usuários com privilégios devem ser capazes de:

- Armazenar senhas criptografadas com segurança.
- Gerenciar a complexidade das senhas e alterações automatizadas regulares de acordo com diretivas.
- Restringir o acesso a contas administrativas exigindo que todos os acessos passem por um portal centralizado.
- Usar a funcionalidade de "logon automático" para evitar que até usuários autorizados saibam as senhas de contas com privilégios.
- Fornecer acesso de emergência a contas com controles adicionais e aprovações exigidas.
- Eliminar o uso de senhas embutidas em código nos scripts (que são frequentemente armazenadas em texto não criptografado e podem ser roubadas por um usuário mal-intencionado).

Esses recursos não só impedem o compartilhamento das senhas, mas também evitam que sejam roubadas de arquivos de senhas pessoais ou por captura da digitação. Ao exigir que todos os logons de contas com privilégios passem por um proxy central, a organização pode rastrear todos os acessos e atividades em caso de violação, ajudando no trabalho investigativo e potencialmente atenuando os danos.

Relatório das atividades do usuário

Compreender quais ações estão sendo executadas pelas contas com privilégios é um componente importante para detectar ameaças persistentes avançadas e atenuar os danos em caso de um ataque inicial bem-sucedido. Por sua natureza, as ameaças persistentes avançadas geralmente envolvem a exportação de volumes significativos de dados, que pode ser detectada pelas ferramentas certas. Os logs de atividades dos usuários comprovam quais atividades estão ocorrendo em um sistema ou dispositivo de rede, podendo ser usados para identificar descumprimentos de diretiva e investigar violações de segurança.

Regulamentações como HIPAA, CA SB 1386 e inúmeras leis estaduais de notificação de violação exigem que uma organização divulgue a violação de segurança à pessoa ou organização afetada. Os logs de atividades dos usuários podem ser usados para investigar a violação de segurança e descobrir não só quem fez o que, mas também como aconteceu, a fim de que os controles internos possam ser corrigidos e os processos possam ser aprimorados.

As ferramentas de geração de relatórios de atividades de usuários devem ser capazes de:

- Monitorar tudo:
  - Logons, especialmente de contas compartilhadas e com privilégios, incluindo o IP de origem, a identificação do usuário original que acessa uma conta compartilhada, a data e a hora do logon e do logoff
  - Atividades de contas compartilhadas, indo até a ID do usuário original
  - Comandos, sejam inseridos por meio de linha de comando ou interface gráfica do usuário

- Detectar comportamento anômalo:
    - Identificar atividades suspeitas e gerar alertas.
    - Fornecer capacidade de correlação de logs, concentrando-se em vincular a atividade do usuário ao indivíduo que a executou por meio de análise de padrões complexos de logs de auditoria.
- Investigar violações:
    - Provar "quem fez o que" em um ambiente de contas compartilhadas.
    - Fornecer ferramentas de análise visual de logs com recursos de detalhamento que podem agilizar a investigação das atividades de usuários e recursos, bem como a identificação de violações de diretivas.

Na ocorrência de uma violação, essas capacidades ajudarão a organização a entender:

- Como um invasor conseguiu obter acesso a uma conta
- O que ele fez enquanto estava usando essa conta e qual foi o dano causado
- Como evitar ataques futuros usando métodos iguais ou semelhantes
- Potencialmente quem era o invasor e de onde ele veio
- Que informações relatar aos órgãos de regulamentação

É fundamental lembrar que os próprios logs devem ser protegidos dos administradores. Usuários com privilégios podem determinar onde os logs são armazenados localmente nos sistemas e descobrir as diretivas de auditoria usadas dentro da organização. Eles podem encobrir seus próprios rastros excluindo registros dentro de arquivos de log locais, já que possuem acesso completo aos sistemas (se controles refinados adequados não tiverem sido implementados). As organizações devem armazenar os logs em um local remoto que não possa ser acessado por esses usuários com privilégios e, também, monitorar se forem feitas tentativas de excluir os arquivos de log locais dos sistemas.

Proteção e controle das informações

Em uma ameaça persistente avançada, o objetivo final do ataque é roubar informações confidenciais; portanto, ter controle sobre os dados é um componente essencial para uma defesa bem-sucedida. Para proteger os dados confidenciais de uma ameaça persistente avançada, a organização deve proteger e controlar os dados em quatro estados:

- **Dados no acesso.** Informações confidenciais que estejam sofrendo tentativas de acesso por uma função inapropriada.
- **Dados em uso.** Informações confidenciais manipuladas na estação de trabalho local ou no laptop.
- **Dados em movimento.** Informações confidenciais transmitidas pela rede.
- **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 quais são as informações 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.

Segurança da infraestrutura interna

Embora a proteção do perímetro da rede, de identidades com privilégios e de dados seja um componente essencial de uma defesa em profundidade contra ameaças persistentes avançadas, também é importante proteger a infraestrutura de TI interna. Além da arquitetura e da segmentação de rede apropriadas, isso inclui configurar e proteger servidores e dispositivos individuais corretamente, bem como seus ambientes.

Segurança inesperada e externalizada

Os invasores criam estratégias e empregam táticas contra defesas de segurança conhecidas. Também usam comandos, funções e utilitários comuns do sistema operacional para reunir informações, monitorar o sistema e realizar ações para expandir seu controle. Os profissionais de segurança podem usar as pressuposições básicas dos invasores contra eles, adicionando elementos inesperados a um sistema. Por exemplo, arquivos e comandos que parecem não estar protegidos nem ser monitorados por logs do sistema podem estar protegidos e ser monitorados por uma ferramenta externa. Na verdade, as permissões que um invasor vê não são necessariamente as permissões que estão sendo aplicadas. Isso permite que a organização detecte quando um invasor verifica as permissões do sistema operacional e viola diretivas externas ao testar os limites das permissões.

Esse é um motivo importante pelo qual a administração da segurança deve ser externalizada e separada da administração do sistema operacional. Após obter acesso inicial a um sistema, um invasor típico tentará escalonar os privilégios a fim de ignorar os controles do sistema operacional. Com esse acesso, ele pressupõe que poderá passar por cima de mecanismos de segurança e "esconder seus rastros" de forma eficaz. Com uma função de segurança externa, frequentemente é possível detectar e conter os invasores com mais antecedência no processo da ameaça persistente avançada, quando o invasor tenta escalonar seus privilégios, alterar os controles de segurança dos sistemas ou exercer privilégios que não foram concedidos. Embora o invasor possa ignorar controles e logs tradicionais no nível do sistema operacional com êxito, processos de detecção externos podem pegá-lo desprevenido. Na essência, a organização pode implementar uma diretiva de controle de acesso nos bastidores, de forma poderosa e inesperada.

Além disso, os comandos padrão do sistema podem ser modificados. Se os administradores renomearem funções como "sudo", todas as tentativas de usar o comando sudo original poderão disparar um alerta e levar à detecção precoce de uma violação.

Proteção do servidor

Todos os servidores que hospedam informações confidenciais devem ser configurados de maneira a minimizar o potencial de comprometimento e a disseminação dos dados, caso o comprometimento venha a ocorrer. Isso inclui:

- Usar um firewall de software para controlar as comunicações de entrada e saída, restringir pacotes por IP de origem, protocolo (por exemplo, SSH, TELNET etc.) e porta TCP; bloquear protocolos não seguros (por exemplo, serviços não criptografados, como FTP).
- Bloquear todas as execuções e instalações de aplicativos, exceto quando explicitamente especificadas ("aplicativos aprovados"), evitando explorações de execução de código e a instalação de software de "backdoor".
- "Confinar" aplicativos. Definir e permitir ações aceitas para aplicativos de alto risco e restringir qualquer comportamento que exceda esses limites. Por exemplo, uma ACL pode ser criada com base em uma ID lógica que possua processos e serviços da Oracle®; dessa maneira, seu comportamento confinado não permite nenhuma ação além de iniciar serviços do Oracle DBMS.
- Impedir alterações em arquivos de log.
- Habilitar o monitoramento da integridade do arquivo para detectar alterações em arquivos importantes, como as feitas por "rootkits".
- Controlar o acesso a arquivos de diretório de aplicativos confidenciais (por exemplo, somente o aplicativo de folha de pagamento pode abrir arquivos de folha de pagamento).
- Detectar alterações em arquivos confidenciais em tempo real.

Segurança uniforme

Um problema comum na computação distribuída é a diversidade de recursos e a disponibilidade de controles de segurança nas plataformas (por exemplo, os controles de diretório/arquivo do UNIX são significativamente diferentes dos controles do Windows). Isso pode levar a vários problemas exploráveis:

- Diretivas de segurança voltadas para um modelo de sistema, em vez de um modelo de segurança de negócios
- As diretivas de segurança devem acomodar as limitações do sistema
- Erros e omissões causados pela complexidade adicional do gerenciamento de segurança

Para fornecer uma defesa abrangente contra as ameaças persistentes avançadas, as configurações de segurança devem ser aplicadas da maneira mais uniforme possível em todas as plataformas. Todas as limitações e inconsistências devem ser compreendidas e monitoradas.

Esse é outro motivo pelo qual as organizações não devem depender exclusivamente da segurança do sistema operacional. Ferramentas externas podem fornecer uma plataforma universal para aplicar um paradigma de segurança em todos os ambientes, possibilitando uma abordagem para a segurança que seja centralizada, simplificada e voltada para os negócios.

Segurança da virtualização

O número de sistemas virtualizados disparou, fazendo com que os ambientes virtuais sejam um alvo importante dos invasores em uma ameaça persistente avançada. O hypervisor também é um alvo crucial, por causa do nível de acesso que pode proporcionar. Se um invasor comprometer o hypervisor, poderá obter acesso quase completo a todas as máquinas virtuais executadas nele. Embora a segurança do sistema operacional possa impedir logons diretos e a criptografia possa proteger dados confidenciais, essas medidas não resistirão a um invasor determinado. Alguém

com controle administrativo sobre um hypervisor pode copiar máquinas virtuais inteiras para um ambiente externo, além de se ignorar a segurança com base no host usando métodos de força bruta ou substituindo arquivos-chave.

Para proteger os ambientes virtuais, as organizações devem novamente se concentrar nos administradores e aplicar o princípio de menos privilégio. Primeiro, o acesso a contas de hypervisor com privilégios deve ser rigorosamente controlado, com todas as ações monitoradas e registradas em log. Segundo, da mesma maneira que nos ambientes físicos, as identidades de hypervisor com privilégios devem ser restritas à execução apenas das ações necessárias. Por exemplo, um administrador financeiro deve ser capaz de acessar apenas máquinas virtuais pertencentes ao departamento financeiro, e não os sistemas de RH.

Juntando tudo

Nenhuma ferramenta de segurança vai proteger uma organização de uma ameaça persistente avançada empreendida por um invasor determinado, capacitado, persistente e dotado de recursos. O objetivo de qualquer estratégia de defesa contra ameaças persistentes avançadas está em dificultar ao máximo a penetração na rede, limitar o dano que pode ser causado e a quantidade de informações que pode ser roubada caso a violação seja bem-sucedida, e detectar uma violação o mais rapidamente possível.

Embora a segurança do perímetro seja um componente necessário para impedir a violação inicial, ela não é absolutamente suficiente e de pouco serve para reduzir os danos depois que a violação ocorreu. O segredo para a atenuação está em uma combinação inteligente de gerenciamento de identidades com privilégios, classificação e controle de dados e segurança da infraestrutura.

Ferramentas padrão de gerenciamento de identidades com privilégios podem restringir ou conceder acesso com base em um conjunto de regras. Embora esse recurso possa fornecer uma segregação apropriada das tarefas, trata-se de uma solução inerentemente rígida. Os privilégios podem ser modificados com o tempo à medida que as funções mudarem, mas essa é essencialmente uma solução passiva.

"Reconhecimento de conteúdo" é o que é necessário para orientar uma nova geração de recursos de defesa ativa contra ameaças persistentes avançadas. Significa integrar a inteligência de dados em cada decisão tomada ao determinar se uma solicitação deve ser atendida. Isso deve ser feito reconhecendo e compreendendo os padrões de acesso e uso dos dados. Por exemplo, deve-se observar o seguinte:

- **Alterações no tipo dos dados acessados.** Um administrador acessa consistentemente dados de um tipo específico (por exemplo, registros operacionais) e, então, solicita acesso a informações financeiras confidenciais ou dados de clientes.
- **Alterações no uso dos dados.** Um administrador que geralmente acessa dados confidenciais por meio de um aplicativo específico com acesso somente leitura solicita a exportação dos dados para um disco rígido externo, um pen drive ou por email.
- **Alterações na quantidade de dados.** Um administrador acessa 100 MB de dados confidenciais semanalmente e solicita acesso para 500 GB no mesmo período.
- **Alterações na frequência do acesso aos dados.** Um administrador acessa dados altamente confidenciais uma vez por mês e, repentinamente, começa a acessar os mesmos dados diariamente.

Nenhuma dessas alterações pode por si só indicar que ocorreu uma violação; entretanto, elas representam uma alteração no comportamento. Um sistema que controla o acesso de usuários com privilégios de forma inteligente deve levar todos esses fatores em consideração ao examinar uma solicitação de acesso. Essa inteligência de dados pode ser usada para negar o acesso a recursos em tempo real ou para permitir o acesso, mas criar um alerta indicando atividade suspeita.

Seção 3: Benefícios

Reduza seus riscos!

As organizações que estão na mira de uma ameaça persistente avançada enfrentam vários tipos de danos. Os invasores podem roubar documentos de propriedade intelectual e estratégia, afetando potencialmente a competitividade. O roubo de dados de clientes pode levar a reações dos clientes, danos à reputação e ações judiciais. O roubo de informações particulares de saúde ou registros financeiros pode levar a problemas de conformidade regulamentar.

Um benefício secundário de um programa holístico para se defender contra ameaças persistentes avançadas é o fato de ele ajudar a proteger a organização contra outras ameaças, desde ataques externos automáticos até ameaças internas. Muitas das técnicas empregadas para atenuar os danos das ameaças persistentes avançadas também limitam o acesso concedido a contas internas, incluindo os administradores. Ao limitar o acesso e segregar tarefas até dos usuários com privilégios, a organização está se protegendo contra um administrador inidôneo ou outro usuário interno mal-intencionado.

Uma característica única dessa abordagem é o fato de ela não exigir conhecimentos específicos sobre vulnerabilidades e novas explorações e não depender da defesa do perímetro. Usando essas técnicas, as organizações podem aplicar um modelo de segurança e permitir ou negar ações com base em regras de negócios, na confidencialidade dos dados e em comportamento anômalo. Como esse modelo pode ser aplicado uniformemente em todas as plataformas e ser separado da segurança do sistema operacional, ele pode proporcionar um meio eficaz de se defender contra as ameaças persistentes avançadas e detectar ataques no início do processo.

Seção 4:

Conclusões

Os ataques direcionados estão crescendo em prevalência. Violações ocorridas em empresas como a RSA foram altamente divulgadas e terão consequências de longo alcance, tanto para a reputação quanto para os lucros.

A ideia de defesa em profundidade não é nova. Trata-se de um aspecto fundamental de qualquer programa de segurança. A novidade está no foco em proteger as identidades com privilégios internas a fim de evitar danos causados por pessoas de fora da empresa. Com o perímetro da rede deixando de ser o bastião da segurança, a identidade tornou-se ainda mais importante. Essencialmente, "a identidade é o novo perímetro".

Ao usar a identidade para proteger contra ameaças internas e externas, como as ameaças persistentes avançadas, o "reconhecimento de conteúdo" deve ser um requisito importante. Ao usar a inteligência de dados como parte de todas as decisões de acesso, as organizações de hoje podem entender melhor os riscos associados a cada ação adotada por um usuário. Solicitações de acesso a dados confidenciais podem ser analisadas e compreendidas com muito mais contexto do que antes. Em vez de contar com regras fixas para permitir ou bloquear determinadas ações, você pode usar os dados para ter uma ideia mais clara da atividade do usuário.

Para ajudar sua organização a sair na frente quando se trata de defesa contra ataques direcionados, adote o gerenciamento de identidades com privilégios e o reconhecimento de conteúdo como pilares do seu programa de segurança.

Seção 5:

Referências

1 http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

2 NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

3 "Advanced Persistent Threat", Wikipedia, http://en.wikipedia.org/wiki/Advanced_persistent_threat

4 http://www.rsa.com/node.aspx?id=3872

5 http://en.wikipedia.org/wiki/Operation_Aurora

6 http://www.nytimes.com/2010/11/29/world/29cables.html?_r=2&hp

Seção 6:

Sobre o autor

Russell Miller passou mais de oito 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 produtos na CA Technologies, com foco em gerenciamento de identidades com privilégios e proteção de dados. Russell é bacharel em Ciências da Computação pela Middlebury College e fez mestrado em Administração de Empresas na MIT Sloan School of Management.