Microsoft

Seis etapas para criar uma estratégia de segurança holística

Essas informações são para você que

Se você for diretor de segurança da informação ou líder de segurança de TI que:

- Precisa de um guia rápido e útil para a estratégia de segurança geral.
- Quer se manter informado sobre as práticas mais recentes de segurança.

Tempo de leitura estimado: 9 minutos

Sumário

Enfrente o desafio

Proteger dados e sistemas é uma prioridade para as organizações. Mas enfrentar esse desafio fica mais difícil a cada dia, pois os ataques se tornam mais sofisticados, os funcionários usam uma gama mais ampla de dispositivos e aplicativos e os dados entram e saem da sua empresa de várias maneiras. Com a mudança em massa para o trabalho remoto, a segurança se torna ainda mais comprometida.

Os líderes têm de equilibrar esses desafios com a necessidade de colaborar, inovar e expandir um negócio. Você precisa de uma abordagem de segurança multifacetada que proteja constantemente todos os pontos finais, detecte sinais precoces de uma violação e responda antes que o dano ocorra. E não importa o quão fortes são suas defesas, as medidas preventivas não são mais suficientes, você também precisa adotar uma postura de "suposição de violação" que inclua medidas de detecção e resposta.

Os diretores de segurança da informação (CISOs) atuais precisam de estruturas de segurança ágeis que permitam a transformação digital e sejam apoiadas por estratégias holísticas inseridas em tecnologias, processos e programas de treinamento. Embora tudo isso esteja disponível para soluções na infraestrutura local, a verdade é que a migração para a nuvem melhora imediatamente os recursos de segurança em toda a organização.

Este e-book compartilha as seis práticas recomendadas de CISOs que fizeram da segurança a pedra angular do sucesso dos negócios. Essas práticas recomendadas se aplicam a um cenário na infraestrutura local, mas são infinitamente mais fáceis de alcançar em um cenário de nuvem.

1. Use produtos de segurança integrados para permitir uma resposta rápida

75

é o número de produtos de segurança que grandes organizações, em média, usam.[1]

Os atores de ameaças evoluíram de ataques de "smash-and-grab" para aqueles que comprometem os sistemas na esperança de manter uma presença persistente e de longo prazo. Os invasores agora usam uma variedade de vetores e uma variedade cada vez mais avançada de ferramentas e técnicas: roubar credenciais, instalar malware que se apaga para evitar a detecção, modificar processos internos e redirecionar dados de rede, fraudes de engenharia social e até mesmo segmentação de telefones celulares dos funcionários e dispositivos domésticos.

As organizações estão implantando cada vez mais ferramentas de segurança contra essas ameaças. Embora destinadas a abordar questões específicas, essas soluções raramente funcionam juntas. Muitos usam painéis, consoles e logs proprietários. A dificuldade de integração dificulta ter uma visão abrangente e priorizar ameaças rapidamente. Isso se torna um desafio ainda maior ao lidar com os recursos de nuvem e na infraestrutura local. Como resultado, os ataques podem passar despercebidos por mais de 140 dias.[2]

[1] "Symantec lança a nova era da proteção avançada contra ameaças", Businesswire, outubro de 2015.

[2] "Cenário de ameaças: por números." Mandiant, A FireEye Company, 2016.

Experimente

À medida que a rápida detecção e resposta se tornam mais importantes, estas práticas recomendadas surgiram:

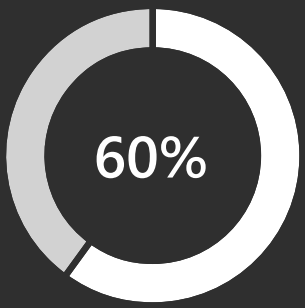
- Obtenha uma visão holística de segurança de toda a sua rede, incluindo ambientes híbridos e de nuvem.
- Crie um ecossistema de produtos e plataformas de segurança que se integram uns aos outros e fornecem insights.
- Faça parcerias com fornecedores de tecnologia que colaborem e compartilhem informações em toda a indústria de segurança.

Principais conclusões

A falta de integração entre produtos de segurança dificulta para as equipes de segurança visualizar e combater rapidamente as ameaças de modo holístico.

Procure produtos projetados para a integração com outros produtos.

2. Gerencie o acesso por meio de identidades, não pontos de extremidade



das violações são originadas em um ponto de extremidade comprometido.[3]

Uma violação de dados pode ter custos enormes. Estabelecer controles de segurança suficientes para obter visibilidade de ameaças e ataques é uma maneira de combater o alto custo. No entanto, as equipes de segurança também têm que dar suporte à TI consumida, onde os funcionários não trabalham mais exclusivamente em dispositivos rigidamente controlados e emitidos por empresas, e esperam trabalhar em qualquer lugar, em qualquer dispositivo ou em qualquer plataforma, independentemente de ter sido sancionado pela TI corporativa.

Neste mundo, as estratégias de segurança orientadas a identidade vinculam o acesso à identidade, não aos dispositivos. Aplique controles com base na função e na necessidade, independentemente de como o usuário se conecta. Esse foco na autenticação e gerenciamento de usuários à medida que acessam ativos corporativos também permite que as organizações protejam seus dados, independentemente de onde eles estejam armazenados, como são acessados ou com quem são compartilhados.

[3] "Cinco principais ameaças enfrentadas por seus negócios e como responder a elas", Microsoft Secure Blog, outubro de 2016.

Experimente

A mudança de uma estratégia de segurança que envolve apenas pontos de extremidade oferece uma abordagem mais robusta. Essas ferramentas podem ajudar:

- **Soluções de gerenciamento de identidade e acesso (IAM)** e **gerenciamento de aplicativos móveis com soluções de prevenção de perdas de dados** (DLP). Ambas ajudam a reduzir o risco, protegendo o acesso a aplicativos e dados em recursos corporativos e na nuvem. O IAM pode eliminar a necessidade de múltiplas credenciais, dando aos funcionários uma única identidade para acessar recursos de nuvem e na infraestrutura local. Os sistemas IAM baseados em nuvem também podem usar a inteligência e análise de ameaças do provedor de tecnologia para detectar melhor tentativas de acesso anormal e responder automaticamente de forma adequada.
- **A autenticação multifator (MFA)** oferece outra camada de proteção, exigindo que um usuário apresente algo que ele saiba (sua senha) e algo que ele tenha (autenticação secundária por meio de um dispositivo, impressão digital ou reconhecimento facial). Outras táticas robustas incluem basear o acesso no risco do usuário, no risco do dispositivo, no risco do aplicativo e até mesmo no risco da localização. Esses recursos podem permitir, bloquear ou exigir automaticamente o MFA de um usuário em tempo real com base nas políticas que você define, essencialmente permitindo que as organizações aumentem a proteção em sua própria porta da frente.

Principais conclusões

Uma estratégia de segurança orientada por identidade muda o foco de pontos de extremidade (dispositivos) para o gerenciamento de usuários que acessam os dados corporativos.

A proteção mais robusta do ponto de extremidade fornece insight pós-violação em técnicas adversárias.

3. Adote um modelo de confiança zero para derrotar ameaças

17.000
alertas de malware

precisam ser filtrados por semana, em média, pela empresas.[4]

Os hackers sabem que cada organização tem vários pontos de entrada. Eles usam golpes de phishing, ataques de malware e spyware, explorações de navegadores e software, acesso por meio de dispositivos perdidos e roubados, engenharia social e outras táticas para violar sua segurança. É preciso vigilância constante para manter a visibilidade entre as ameaças que você já conhece e para tomar consciência das vulnerabilidades emergentes.

Algumas ferramentas podem ajudar a manter uma abordagem de segurança sempre ativa, mas uma abordagem mais ampla faz mais sentido. As ferramentas tradicionais se concentram na prevenção, mas isso não é mais suficiente. As organizações devem assumir que uma violação já ocorreu ou que ocorrerá em breve. Isso é conhecido como confiança zero. Em seguida, elas devem encontrar maneiras de reduzir significativamente o tempo necessário para detectar e se recuperar da violação.

[4] "O custo da contenção de malware." Ponemon Institute, janeiro de 2015.

Experimente

Seja um especialista em segurança avançada. Ficar à frente das ameaças pode significar olhar para trás: aprender com incidentes, atividades e etapas passadas que os hackers tomaram.

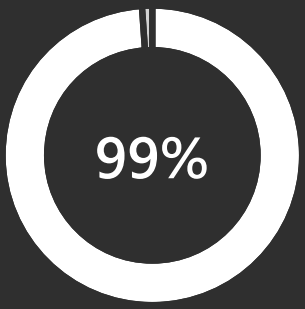
- Muitos aplicativos de segurança usam recursos de análise e aprendizado de máquina incorporados para analisar como um hacker obteve acesso. Mais soluções avançadas de segurança e análise usarão esses insights para agir automaticamente para prevenir e responder a violações semelhantes, o que ajuda a reduzir significativamente o tempo de mitigação.
- A amplitude e a profundidade tremendas do sinal e da inteligência estão por trás destas soluções, e quando combinadas com a experiência e o conhecimento de especialistas humanos, estas soluções podem ser ferramentas poderosas de encontro aos ágeis atores de ameaças.

Principais conclusões

Os aplicativos nativos de nuvem suportam um modelo de confiança zero mais facilmente do que os aplicativos herdados.

Os aplicativos herdados exigem modernização para oferecer suporte a acesso condicional baseado em identidade.

4. Migre para a nuvem com segurança



das falhas de segurança na nuvem serão falha do cliente até 2025.[5]

Cada organização está em um estágio diferente de sua jornada para a nuvem. Requisitos de conformidade, regulamentos locais e outros desafios migratórios significam que nem todas as organizações estão prontas para mover workloads críticos para a nuvem. As estratégias de nuvem híbrida são uma maneira de as organizações poderem entrar na nuvem, mantendo algumas cargas de trabalho na infraestrutura local e migrando outras.

Os modelos de serviços em nuvem afetam a forma como os provedores de serviços e os clientes compartilham responsabilidades. Isso levanta questões para os CISOs à medida que navegam pelos desafios de abrir mão de alguns dos controles de soluções na infraestrutura local para maior segurança que os fornecedores de nuvem podem oferecer.

A regra empírica para a segurança da nuvem é que ela é uma responsabilidade compartilhada. Os provedores de nuvem precisam ter segurança e criptografia de última geração, mas os clientes devem garantir que os serviços que compram sejam de fato seguros e que ampliem as políticas de segurança necessárias em seus novos recursos de nuvem.

[5] "A nuvem é segura?", Gartner, outubro de 2019.

Experimente

Faça as perguntas certas. Avaliar os provedores de nuvem não é apenas escolher um serviço, é escolher em quem confiar com seus dados. As perguntas críticas sobre segurança e controle de acesso que você deve fazer incluem:

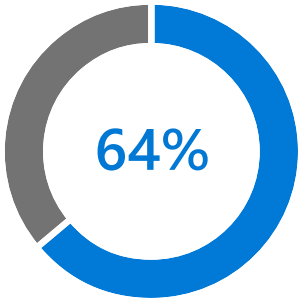
- Nossos dados estão protegidos por uma forte segurança e tecnologia de ponta?
- Você incorpora a privacidade por projeto e permite o controle dos nossos dados na nossa nuvem empresarial?
- Que tipo de investimentos você fez em processos de conformidade robustos e inovadores para nos ajudar a atender às nossas necessidades de conformidade?
- Onde nossos dados serão armazenados, quem tem acesso a eles e por quê?
- Você realiza revisões anuais de terceiros para garantir que os padrões de segurança e conformidade estejam sendo atendidos?
- Você rejeitará quaisquer solicitações de divulgação de dados pessoais dos clientes que não sejam juridicamente vinculativos?
- Você adere aos padrões regulatórios e de conformidade de diferentes países e locais e, em caso afirmativo, quais?

Principais conclusões

Ao avaliar provedores de serviços de nuvem, certifique-se de que eles cumpram os padrões internacionais.

Procure fornecedores que publiquem informações detalhadas sobre a operação de seus serviços e como eles lidam com dados.

5. Veja bem o Shadow IT



dos funcionários criaram pelo menos uma conta (inscrição em um site ou aplicativo relacionado ao trabalho) sem envolver o departamento de TI.[6]

Quando um funcionário cria uma conta baseada em nuvem sem a autorização ou o conhecimento de uma empresa, isso é conhecido como Shadow IT. As contas parecem completamente inofensivas: uma ferramenta para corrigir gramática, por exemplo. Mas essas contas criam vulnerabilidades mesmo na mais apertada das configurações de segurança.

As pessoas geralmente aceitam termos e condições sem ler e sem entender completamente ao que estão concedendo acesso. As soluções tradicionais de segurança de rede não foram projetadas para proteger os dados nos aplicativos SaaS e não podem dar visibilidade de TI sobre como os funcionários estão usando a nuvem.

Em última análise, não queremos diminuir as motivações por trás do Shadow IT. Permitir que pessoas e equipes finais usem os aplicativos de nuvem mais adequados para seu tipo de trabalho ajuda a impulsionar a produtividade e a inovação. Ganhar visibilidade, controle e proteção contra ameaças de aplicativos SaaS sombra são os primeiros passos na gestão de risco e facilitar a transformação digital que já começou em sua empresa.

[6] "Nova pesquisa demonstra o risco da Shadow IT", 1password, fevereiro de 2020.

Experimente

Obtenha as informações de que você precisa. Os CASBs (agentes de segurança de acesso à nuvem) fornecem às organizações uma visão detalhada de como seus funcionários estão usando a nuvem:

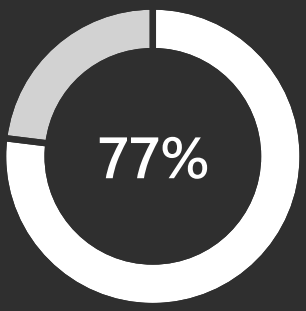
- Quais são os aplicativos de nuvem usados por seus funcionários?
- Que risco esses aplicativos representam para a organização?
- Como esses aplicativos estão sendo acessados?
- Que tipo de dados estão sendo enviados e compartilhados desses aplicativos?
- Como é o tráfego de upload/download?
- Existem anomalias no comportamento do usuário como viagens impossíveis, tentativas de logon com falha ou IPs suspeitos?

Principais conclusões

Os agentes de segurança de acesso à nuvem (CASBs) podem fornecer a você uma visão detalhada de como os funcionários estão usando a nuvem.

Com melhor visibilidade, é possível definir políticas que rastreiem e controlem como os funcionários usam esses aplicativos.

6. Torne a proteção e a produtividade perfeitas



dos CISOs dizem que se sentem na dúvida entre deixar as pessoas trabalharem livremente e manter a empresa segura.[7]

Os dados saem do seu controle agora mais do que nunca à medida que seus funcionários, parceiros e clientes os compartilham. Isso impulsiona a produtividade e a inovação, mas poderá ter consequências significativas se os dados altamente confidenciais caírem nas mãos erradas. Os líderes de segurança devem gerenciar e proteger os dados armazenados em vários locais e compartilhados através das fronteiras internacionais em conformidade com os regulamentos.

Os funcionários tolerarão muitos inconvenientes antes que sejam encontradas soluções alternativas de requisitos de segurança. Classificar e criptografar são as melhores maneiras de manter os dados seguros, ao mesmo tempo em que permitem o uso produtivo e o compartilhamento de informações. Você pode evitar o erro humano automatizando a classificação de dados. As ferramentas podem entender o contexto dos dados, como números de cartão de crédito dentro de um arquivo ou a confidencialidade dos dados com base na origem de dados. Uma vez rotulados, marcas visuais como cabeçalhos, rodapés e marcas d'água, bem como proteção, como criptografia, autenticação e direitos de uso, poderão ser aplicadas automaticamente a dados confidenciais.

[7] "Pesquisa mostra que a segurança de TI detém a produtividade e a inovação", ComputerWeekly.com, outubro de 2017.

Experimente

Fique à vontade com os detalhes. As equipes de segurança devem ser capazes de rastrear a atividade em arquivos compartilhados altamente confidenciais ou de alto impacto comercial e revogar o acesso, se necessário.

- Essa proteção persistente viaja com os dados e os protege em todos os momentos, independentemente de onde eles são armazenados ou com quem são compartilhados.
- Um sistema de gerenciamento de acesso de identidade facilita o fardo de rastrear arquivos altamente confidenciais.

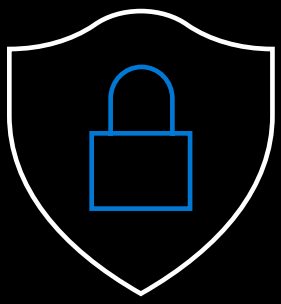
Principais conclusões

A segurança no nível dos dados é responsabilidade de todos.

A classificação e a rotulação de dados devem ocorrer no momento da criação, e as equipes de segurança devem poder monitorar atividades em arquivos e agir rapidamente.

Microsoft

Conclusão



A natureza multifacetada das ameaças cibernéticas significa que apenas resolver alguns de seus desafios de segurança não é mais suficiente. As necessidades de segurança de cada empresa são únicas, mas as empresas enfrentam os mesmos desafios e compartilham a mesma responsabilidade de proteger seus dados, pessoas e sistemas, incentivando a inovação e o crescimento. Você precisa de estruturas de segurança ágeis que promovam e apoiem a transformação digital, apoiadas por estratégias de segurança holísticas inseridas em tecnologias, processos e programas de treinamento.

Se você ainda não considerou uma migração para a nuvem, agora é um ótimo momento para explorar os maiores recursos de segurança encontrados lá. O Microsoft 365 oferece uma solução completa e inteligente para empresas de qualquer tamanho que suporta sua transformação digital com funcionalidades de segurança e conformidade incorporadas em todos os níveis.

Saiba mais nesta série de webinars gratuita e abrangente.

Assista à série >