Resumo de solução

Evite que os dados saiam da sua organização

Os dados estão escapando da maioria das organizações. Às vezes eles saem com pessoas de dentro da organização, mas na maioria das vezes são roubadas por pessoas de fora. Eles estão saindo de várias formas e por vários canais. As organizações estão tentando deter esse fluxo, por diversos motivos e com graus variados de êxito. A Intel Security encomendou o *Intel Security 2016 Data Protection Benchmark Study* (Estudo de referência da Intel Security sobre proteção de dados em 2016) para ter uma compreensão mais profunda sobre as pessoas por trás desses roubos, os tipos de dados roubados e as maneiras pelas quais esses dados saem das organizações.

No *Relatório do McAfee Labs sobre ameaças: setembro de 2016*, analisamos os dados da pesquisa e detalhamos nossas descobertas. Entre outras coisas, descobrimos que:

- O intervalo entre a perda de dados e a descoberta da violação está ficando maior.
- Fornecedores de serviços de saúde e fabricantes são alvos fáceis.
- A abordagem típica de prevenção de perda de dados é cada vez mais ineficaz contra novos alvos de roubo.
- A maioria das empresas não vigia o segundo método mais comum de perda de dados.
- A prevenção de perda de dados é implementada pelas razões certas.
- A visibilidade é vital.

Políticas e procedimentos recomendados para uma prevenção de perda de dados eficaz

É fundamental que as organizações criem políticas e procedimentos de prevenção de perda de dados para evitar transferências acidentais ou deliberadas de dados confidenciais para pessoas não autorizadas. Uma iniciativa bem-sucedida de prevenção de perda de dados começa no estágio de planejamento, quando os requisitos do negócio são definidos. Por exemplo, as políticas de classificação e de perda de dados devem ser alinhadas com as políticas de privacidade e com os padrões de compartilhamento de dados da organização no estágio de planejamento. O estabelecimento de requisitos razoáveis de negócios ajuda a manter o foco na iniciativa de prevenção de perda de dados e protege contra a ampliação excessiva do escopo.

intel Security

Uma próxima etapa importante em uma iniciativa de prevenção de perda de dados é identificar dados confidenciais dentro da organização. Tecnologias de varredura de servidores e endpoints permitem a classificação dos arquivos com base em expressões regulares, dicionários e tipos de dados não estruturados. Os produtos de prevenção de perda de dados frequentemente oferecem classificações incorporadas para categorias típicas de dados confidenciais, como dados de cartões de pagamento ou informações pessoais de saúde, que podem acelerar o processo de descoberta. Classificações personalizadas também podem ser criadas para identificar tipos de dados específicos da organização.

Um fator complicador nessa etapa são os aplicativos, aprovados ou não pelo departamento de TI, e seus dados de suporte na nuvem. Quanto a dados aprovados pelo departamento de TI, a identificação de dados confidenciais pode e deve ser parte do processo, quando da assinatura do serviço na nuvem. Nesse caso, pode ser relativamente simples classificar esse tipo de dado.

No entanto, grupos funcionais dentro das organizações frequentemente ignoram o departamento de TI para atingir objetivos de negócios próprios ao fazer, eles próprios, assinaturas de serviços na nuvem. Se o departamento de TI não estiver ciente desses serviços e dos dados correspondentes, haverá um potencial maior para perda de dados. Consequentemente, é importante trabalhar com esses grupos funcionais durante essa etapa para identificar as localizações dos dados na nuvem e utilizar o processo precedente para classificar esses dados.

Após a conclusão do processo de descoberta de dados confidenciais, implementar produtos de prevenção de perda de dados dentro da rede confiável e em todos os endpoints pode proporcionar visibilidade e controle sobre dados importantes, tanto estacionários quanto em trânsito. Políticas devem ser implementadas para detectar acesso ou movimentação inesperada de dados confidenciais. Eventos como dados confidenciais sendo transferidos para dispositivos USB ou pela rede para um local externo podem ser parte de um processo de negócios normal ou podem ser uma ação deliberada ou acidental que resulte em perda de dados.

Um treinamento bem desenvolvido de conscientização em segurança pode reduzir a probabilidade de violações de dados. Telas de justificação podem orientar os usuários quanto às ações apropriadas relacionadas a transferências de dados confidenciais e permitir que os usuários sejam instruídos sobre políticas de proteção de dados durante seu cotidiano de trabalho. Por exemplo, uma tela de justificação pode notificar os usuários de que sua transferência de dados confidenciais é contra a política da empresa e oferecer alternativas à realização da transferência, como editar os dados confidenciais antes de tentar a transferência novamente.

Os donos dos dados costumam compreender melhor do que outros grupos da organização como seus dados são utilizados. Os donos dos dados devem ser designados e empoderados para fazer uma triagem dos incidentes de perda de dados. A separação de atribuições entre os donos dos dados e a equipe de segurança reduz a possibilidade de que uma única equipe burle políticas de proteção de dados.

Uma vez que os movimentos aprovados dos dados tenham sido estabelecidos e as políticas que governam esses movimentos tenham sido incorporadas nos produtos de prevenção de perda de dados, as políticas para bloquear transferências não aprovadas de dados confidenciais podem ser ativadas. Com o bloqueio ativado, os usuários são impedidos de realizar ações contrárias à política. As políticas podem ser ajustadas para proporcionar flexibilidade, dependendo dos requisitos do negócio, para assegurar que os usuários possam desempenhar suas funções e ainda estarem protegidos.

Conforme a iniciativa de prevenção de perda de dados avança, é importante validar e ajustar as políticas a intervalos regulares. Às vezes as políticas são demasiadamente restritivas ou muito permissivas, afetando a produtividade ou representando um risco de segurança.

Como a Intel Security pode ajudá-lo a se proteger contra vazamento de dados

McAfee DLP Discover

A primeira etapa para proteger adequadamente os dados é compreender onde residem as informações e o que são exatamente esses dados. O McAfee DLP Discover protege contra vazamento de dados simplificando essa primeira etapa através das seguintes capacidades:

- Identificar as classificações a serem detectadas dentro do ambiente confiável utilizando classificações predefinidas (por exemplo, HIPAA, PCI, SOX) ou criando classificações personalizadas.
- Realizar uma varredura de inventário e examinar utilizando as classificações identificadas para compreender onde e quais tipos de dados residem dentro do ambiente confiável. Examinar violações da política existente na interface de McAfee DLP Discover.
- Realizar uma varredura de correção para localizar dados armazenados em locais não autorizados e movê-los para um local autorizado.
- Varreduras de inventário e correção podem ser realizadas em recursos locais, como compartilhamentos de rede ou recursos na nuvem, como Box.
- Criar novas políticas de proteção de dados com base nos resultados das varreduras do McAfee DLP Discover.

McAfee DLP Endpoint

O McAfee DLP Endpoint monitora e evita o vazamento de dados nas dependências da empresa, fora dela e na nuvem. Monitore rapidamente eventos em tempo real, aplique políticas de segurança com gerenciamento centralizado e gere relatórios de proliferação e forenses detalhados sem prejudicar as operações do dia a dia.

- Após a conclusão da fase de descoberta, crie políticas de proteção de dados para relatar violações de políticas. Isso provê os dados necessários para uma melhor compreensão da movimentação dos dados dentro da organização, além de permitir a imposição de regras de bloqueio. O McAfee DLP inclui classificações predefinidas (por exemplo, HIPAA, SOX, PCI e ITAR) que podem ser utilizadas para identificar dados dentro da organização.
- Crie telas de orientação para os usuários compreenderem melhor as políticas de proteção de dados enquanto realizam suas transferências de dados cotidianas. Esses pop-ups educacionais personalizáveis são extremamente úteis e reduzem transferências de dados arriscadas por parte dos funcionários.
- Confira o gerenciador de incidentes para identificar as propriedades dos dados sendo transferidos para locais não autorizados, por exemplo, a maneira pela qual as transferências são feitas e quem as está fazendo.
- Depois que políticas de proteção de dados forem criadas e ajustadas conforme os requisitos organizacionais, ative o bloqueio de transferências de dados não autorizadas.
- Ative as classificações manuais para que os usuários possam classificar os documentos que criarem. Como donos dos dados, eles provavelmente compreendem melhor a confidencialidade dos documentos, caso o mecanismo de classificação automática não consiga detectar dados estruturados. Isso já está incorporado no McAfee DLP Endpoint, dispensando quaisquer ferramentas adicionais de terceiros.
- Para proteção adicional, crie e implemente uma regra de proteção a acesso de aplicativo que utilize o McAfee Threat Intelligence Exchange para evitar que aplicativos desconhecidos acessem dados confidenciais. Isso permite que aplicativos autorizados transfiram dados confidenciais, mas restringe o acesso a esses dados por parte de aplicativos não verificados ou maliciosos.

McAfee DLP Monitor

O McAfee DLP Monitor coleta, rastreia e gera relatórios sobre dados transmitidos em toda a rede. Revele facilmente ameaças desconhecidas aos dados e tome providências para protegê-los.

- Ative as políticas e regras predefinidas relevantes para detectar possíveis violações dentro da rede.
- Crie políticas e regras personalizadas adicionais, por exemplo, para monitoramento de transferências de dados confidenciais para a nuvem.
- Realize análises forenses para correlacionar eventos de risco atuais e passados, detectar tendências de risco e identificar ameaças. O McAfee DLP Monitor permite que especialistas em segurança entendam a situação rapidamente e desenvolvam regras e políticas para lidar com o problema.
- Crie filtros de captura adicionais para excluir dados irrelevantes e ajuste regras para reduzir os falsos positivos.
- Configure alertas para enviar notificações para remetentes, destinatários, donos de dados e administradores de sistemas quando ocorrerem violações de políticas.

McAfee DLP Prevent

O McAfee DLP Prevent protege contra a perda de dados assegurando que os dados só deixem a rede quando for apropriado, seja por e-mail, webmail, mensagens instantâneas, wikis, blogs, portais, HTTP/HTTPS ou transferências FTP. Identificar e mitigar tentativas de vazamento com rapidez é a diferença entre manter seus valiosos dados seguros e fazer parte do próximo grande escândalo.

- Integre o McAfee DLP Prevent com proxies de Web ou agentes de transferência de mensagens utilizando políticas predefinidas para impedir transferências de dados não autorizadas através de gateways de e-mail ou proxies de Web.
- Crie regras do McAfee DLP Prevent para permitir ou bloquear documentos confidenciais com base no percentual de correspondência.
- Use modelos predefinidos de DLP para evitar que dados confidenciais sejam transferidos para a nuvem.
- Examine relatórios de incidentes de segurança e ajuste políticas para reduzir os falsos positivos e maximizar a continuidade dos negócios.
- Configure alertas para enviar notificações para remetentes, destinatários, donos de dados e administradores de sistemas quando ocorrerem violações de políticas.

Leitura adicional

Comunidade do Intel Security Expert Center

- McAfee Data Loss Prevention

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com