Symantec + BLUE COAT
Defining the Future of Cyber Security

DOCUMENTO TÉCNICO

Adoção segura do Office 365

UM GUIA EXECUTIVO

AUTORA
Deena Thomchick
DIRETORA SÊNIOR DO SETOR DE NUVEM DA BLUE COAT

Symantec + BLUE COAT
Defining the Future of Cyber Security

Adoção segura do Office 365

UM GUIA EXECUTIVO

Introdução

O recado está dado. Mais cedo ou mais tarde, praticamente todas as empresas migrarão para o Office 365. É só uma questão de tempo até irmos das vantagens comerciais de produtividade e colaboração ao modelo econômico de licenciamento de despesas operacionais e, por fim, à realidade fundamental do objetivo da Microsoft quando desenvolveu o Office 365. O Office 365 já é a aplicação em nuvem mais implementada, e 78% das empresas a utilizam ou pretendem utilizá-la.

A maioria das empresas começou a adotar o Office 365 com a migração para o Exchange Online para e-mail e calendário, fazendo do Exchange Online o plano mais vendido do Office 365. O Exchange Online é seguido pelo OneDrive, para compartilhamento de arquivos, em segundo lugar, e pelo ProPlus, para uma grande variedade de aplicações da Microsoft, em terceiro lugar.

Considerações principais

O compartilhamento e a movimentação de dados são elementos importantes em toda adoção do Office 365, desde um plano do Exchange Online que vem com uma caixa de correio de 50 GB, a aplicação Outlook e o OneDrive até os pacotes ProPlus completos. Desde a primeira etapa, a migração ao mundo do Office 365 traz diversas questões que devem ser consideradas.

1. Uma grande quantidade de dados corporativos agora serão armazenados na nuvem da Microsoft, acessíveis por diversos usuários e estarão fora do controle do departamento de TI tradicional da empresa. Com isso, é preciso fazer algumas considerações sobre privacidade, segurança e conformidade.
2. Os dados serão transmitidos entre a nuvem e os terminais, que podem ou não estar localizados dentro do perímetro da empresa e podem ou não ser gerenciados por ela. Isso gera grandes oportunidades para passar pelas defesas da empresa, o que pode ser explorado pelas ameaças.
3. Sua infraestrutura terá um número muito maior de conexões abertas e simultâneas à Internet e volumes maiores de dados em movimento no seu perímetro. Portanto, será necessário acomodar e gerenciar um tráfego de rede maior para manter os níveis de serviço de desempenho.

A Gartner identificou a segurança e o desempenho como as principais questões a serem resolvidas ao adotar o Office 365. Muitas empresas não consideram nenhuma delas em seus planos iniciais de adoção e acabam tendo dificuldades para conseguir verba e tempo para implementar esses itens.

Quem é o responsável pela segurança no Office 365?

Você é o responsável por proteger seus usuários e o seu conteúdo nas suas contas do Office 365. A Microsoft prestará serviços de infraestrutura para garantir que os hackers não obtenham acesso aos seus servidores e que seus funcionários sejam avaliados para confirmar que são de confiança e não utilizarão seus dados. No entanto, a Microsoft não se responsabiliza por controlar o quê, como e com quem os seus funcionários e outros usuários compartilham os dados em suas contas do Office 365. Além disso, eles não assumirão a responsabilidade pelo tipo de conteúdo que os usuários enviarem para a nuvem. Ou seja, eles não controlam como os seus usuários utilizarão o serviço.

O mau uso acidental, ataques de hackers e malware normalmente acontecem entrando pela porta da frente das suas contas do Office 365. Provavelmente, é por isso que a Gartner previu, em 2016, que "95% das falhas de segurança em nuvem acontecerão por culpa do cliente".

A adoção do Office 365 trará uma série de benefícios à sua empresa, mas saiba que será necessário ajustar o seu provisionamento de segurança para controlar o compartilhamento de conteúdos confidenciais na nuvem e proteger sua empresa contra ameaças, invasões e erros de usuários trazidos pelo uso do Office 365.

Comece o planejamento estratégico e financeiro agora mesmo

Muitas empresas priorizam o planejamento estratégico e financeiro de sua implementação do Exchange Online ou de amplos planos do Office 365 sem prever as exigências adicionais de segurança e desempenho.

Custo e planejamento para os serviços da Microsoft

Você vai simplesmente migrar para o Exchange Online ou adotará uma abordagem mais ampla do Office 365? Qual plano é o mais adequado para a sua empresa? Com que velocidade você migrará os usuários? Quais são as dimensões da sua adoção? Uma pesquisa da Gartner sugere que a adoção pode ser lenta e constante, e muitas empresas executam operações do Exchange Online e do Exchange tradicional simultaneamente por algum tempo.

Planejamento estratégico e financeiro para proporcionar maior segurança

Será necessário oferecer controle e proteção de dados em nuvem, DLP, controle de acesso e proteção contra ameaças. Realize uma análise crítica das opções de segurança da própria Microsoft e decida o que é e o que não é bom o suficiente para você, em se tratando da proteção da sua empresa. Considere as exigências de conformidade e realize uma análise de risco para a sua empresa. Tente ser realista em relação à mão de obra que pode ser necessária para determinados sistemas de segurança. A Gartner prevê que, "Em 2018, 40% das implementações do Office 365 dependerão de ferramentas de terceiros para preencher lacunas de segurança e conformidade...". (FONTE: GARTNER, "COMO AUMENTAR A SEGURANÇA DO OFFICE 365") É possível que a Gartner esteja sendo conservadora com essa previsão; a adoção pode ser muito maior em empresas de médio e grande porte.

- Planeje-se para incluir soluções de segurança de terceiros, como o Agente de segurança de acesso à nuvem (CASB, Cloud Access Security Broker) e a proteção contra ameaças avançadas (ATP, Advanced Threat Protection).
- Aumente a cobertura de segurança de suas soluções existentes de DLP e proteção contra ameaças para acomodar os dados em nuvem.
- Avalie o seu gerenciamento de acesso. Pode ser necessário adicionar ou aumentar as soluções de login único e autenticação multifator (MFA, multi-factor authentication).

Preveja o desempenho

Avalie a capacidade de sua segurança de perímetro e seus serviços de rede para acomodar grandes aumentos no volume de dados e no número de conexões simultâneas à Internet: roteadores e switches de rede, gateways da Web, firewalls, IPS e outros sistemas e serviços de proteção do perímetro e de rede. Por exemplo: um usuário comum do Exchange Online manterá seis ou mais conexões simultâneas à Internet e exigirá mais 200 MB de largura de banda de Internet. Ao acrescentar mais aplicações do Office 365, as conexões simultâneas necessárias podem aumentar para mais de 40, e a largura de banda, para 300 MB ou mais. Provavelmente, isso exigirá um dimensionamento para aproveitar as funcionalidades desses sistemas e otimizar o tratamento de tráfego para obter um melhor desempenho.

Proteja-se contra atividades não autorizadas dos usuários

A Microsoft protegerá o back-end de sua nuvem do Office 365, mas você é o responsável por proteger suas contas do Office 365 como se elas fossem um de seus sistemas internos, porque é exatamente isso que elas são. É preciso estar atento ao acesso e às atividades dos usuários e implementar proteções para evitar o acesso não autorizado e identificar e reduzir as atividades não autorizadas em suas contas. Ataques, violações e roubo de dados exigem ações, e elas são realizadas pelos usuários (ou entidades que se passam por usuários).

Proteja o acesso às contas do Office 365

Implemente proteções para evitar o acesso não autorizado às suas contas.

Adote uma solução de login único (SSO, Single Sign On), caso não possua uma. Provavelmente, o Office 365 não será seu único sistema que necessitará de acesso seguro, então, busque uma solução que seja capaz de lidar com diversas aplicações, e não apenas com o Office 365. Caso já possua SSO, basta adicionar o Office 365 à sua solução existente. Caso não possua uma solução de SSO, há diversas opções de SSO disponíveis, inclusive uma da Symantec.

Adicione autenticação multifator às suas exigências de acesso para o Office 365. Considerando o cenário de ameaças atual, sozinhas, as senhas não são seguras o suficiente. Os hackers usam ataques de força bruta para descobrir as senhas e os usuários normalmente usam a mesma senha ou uma variação dela para diversas contas. Assim, mesmo que os seus sistemas estejam seguros, uma violação de dados de outro lugar pode expor as senhas que podem ser usadas para obter acesso às suas contas.

Identificar e reduzir as atividades suspeitas do usuário

Há várias formas para seus dados e suas contas serem expostos. Os usuários que realmente têm acesso a eles podem expor suas contas acidentalmente em virtude da interceptação de sessões causada por malwares. Você também pode ser uma das empresas que, infelizmente, possuem um conhecido malicioso. Porém, na maioria das vezes, as informações confidenciais são expostas por meio do mau uso acidental dos usuários, que simplesmente cometem erros.

Implemente uma boa solução de CASB. Busque um CASB que possua um sistema de análise de comportamento do usuário capaz de identificar comportamentos anormais e suspeitos do usuário na nuvem, além de oferecer controles de políticas automatizados para reduzir os possíveis danos resultantes. Recomendamos que ele ofereça visibilidade detalhada da atividade do usuário e facilite a identificação precisa, agindo quando houver comportamentos suspeitos.

Evite a exposição de dados

Defina uma estratégia para monitorar e controlar os dados sigilosos na nuvem do Office 365

Você terá conteúdo confidencial e relacionado à conformidade nas suas contas do Office 365. Considerando que erros diversos e mau uso por conhecidos são a primeira e a segunda causas mais comuns de um incidente de segurança que envolve uma violação de dados (FONTE: DATA BREACH INVESTIGATIONS REPORT DE 2016 DA VERIZON), será necessário ter uma forma de controlar e proteger seus dados em nuvem.

O compartilhamento de arquivos em nuvem facilita a colaboração, mas também acaba facilitando o compartilhamento excessivo de dados sigilosos. 23% dos arquivos em nuvem são amplamente compartilhados e 12% deles contêm dados sigilosos ou relacionados à conformidade. (FONTE: ELASTICA SHADOW DATA REPORT DE 2016)

O amplo compartilhamento pode levar à exposição acidental, que normalmente envolve o compartilhamento público acidental ou o compartilhamento com grandes grupos de pessoas. Isso pode acontecer facilmente por conta de permissões herdadas de compartilhamento de arquivos e pastas ou um compartilhamento antigo com pessoas que não estão que não estão mais ligadas à empresa.

Identifique e classifique o conteúdo confidencial

A capacidade de identificar e classificar os dados confidenciais ou relacionados à conformidade é fundamental, principalmente quando estão em uma nuvem em que o compartilhamento excessivo ocorre com muita frequência. Essa é uma funcionalidade essencial para uma solução de DLP útil e eficiente. Desenvolver e manter um sistema próprio de identificação e classificação demanda muito tempo. Você economizará muita mão de obra se aproveitar uma solução de DLP que ajude a classificar seus dados.

Evite e corrija o compartilhamento excessivo de conteúdo confidencial em nuvem

Defina controles automatizados de políticas para evitar a exposição de seus dados sigilosos. Para isso, é preciso ter visibilidade e controle sobre todos os seus dados na nuvem do Office 365, incluindo a capacidade de:

- Monitorar e controlar os dados sigilosos que chegam ao Office 365 e saem dele, usando gateways e controles preventivos de terminais;
- Monitorar e controlar os dados armazenados e/ou criados na nuvem do Office 365 não importando quem, como ou de onde esses dados foram enviados à nuvem;
- Monitorar e controlar o compartilhamento de nuvem para nuvem entre o Office 365 e outras aplicações em nuvem

Adicione um CASB para obter visibilidade e controle

Um bom CASB alertará quando seus dados sigilosos estiverem em risco na nuvem e oferecerão prevenção e correção automatizadas caso haja exposição de informações confidenciais. Além da visibilidade e dos controles de política excelentes, um bom CASB pode oferecer DLP com base em dicionários, análise científica

de conteúdo de dados e sistemas personalizados de aprendizado de conteúdo. Um CASB melhor ainda se integrará com sua solução mais ampla de DLP, se você tiver um. Caso tenha decidido permitir dados confidenciais na nuvem, é possível usar os sistemas do CASB para criptografar automaticamente os dados sigilosos na nuvem, oferecendo uma proteção adicional contra a violação de dados.

Adicione DLP em nuvem para uma ampla identificação, classificação e proteção

Identifique e proteja os dados confidenciais em toda a sua empresa com uma solução de DLP que protege suas contas em nuvem e seus sistemas do local. É provável que você tenha dados confidenciais em diversas aplicações, e uma solução de DLP robusta e de alta qualidade oferecerá uma proteção consistente, ao mesmo tempo que reduz a mão de obra associada à perda de dados.

Caso já possua uma solução de DLP implementada, será necessário descobrir como expandir essa proteção para identificar e classificar todos os seus dados na nuvem do Office 365. Existem algumas opções de CASB para integração com DLP no local para você escolher. No entanto, a única solução de CASB integrado de nuvem para nuvem + DLP em nuvem atualmente disponível vem com uma combinação da DLP da Symantec e Elastica CloudSOC.

Mantenha a conformidade

As penalidades relacionadas à conformidade aumentaram nos últimos anos, por isso, manter a conformidade com as exigências regulamentares é mais importante do que nunca, principalmente para os setores financeiro, de assistência médica, varejo e telecomunicações. A maioria dos regimes de conformidade se resume a duas exigências principais: é preciso realizar uma avaliação de risco e agir com responsabilidade para proteger tipos de dados específicos.

A visibilidade é fundamental para avaliações de risco

Veja as opções de visibilidade nativas do Office 365 e de uma solução de CASB. Você deve ter a capacidade de enxergar diretamente suas contas do Office 365, além de inspecionar o tráfego in-line. A visibilidade direta do Office 365 garante que você não deixe de notar os dados em suas contas do Office 365 enviados por dispositivos remotos não gerenciados, por meio de transferências diretas de nuvem para nuvem ou criados de forma nativa no Office 365. Também é preciso ter visibilidade e controle sobre o tráfego in-line, para que seja possível evitar ações arriscadas e monitorar o comportamento dos usuários com um alto nível de detalhes, associados às suas aplicações do Office 365 e outras aplicações em nuvem.

Proteja os dados relacionados à conformidade

Use o controle de dados, a criptografia e a DLP para evitar que sua empresa exponha PII, PHI, PCI e outros dados controlados por regulamentações de privacidade de dados. Alguns regimes de conformidade exigirão a criptografia de arquivos e dados transferidos para a nuvem; outros, que sua empresa mantenha o controle sobre suas chaves de criptografia (nesses casos, não será possível usar uma solução de criptografia que exija que a Microsoft ou o fornecedor do seu CASB mantenha suas chaves de criptografia na nuvem deles). Analise as regras de PII, HIPAA e GDPR para garantir que a sua empresa esteja pronta para cumprir essas normas.

Impeça o roubo e destruição

Implemente proteções para se defender de ataques em suas contas do Office 365, sejam malwares que buscam uma forma de invadir sua empresa, ransomware ou malfeitores determinados a destruir dados, ataques que buscam uma forma de vazar dados de dentro do seu perímetro organizacional ou ameaças que procuram roubar dados valiosos. É fundamental ter defesas ativas para proteger sua empresa contra as contas comprometidas. As empresas possuem milhares de credenciais em uso por seus funcionários que dão acesso a dados valiosos. Basta uma delas ser comprometida para abrir uma porta que pode causar um grande prejuízo.

Identificar atividades maliciosas

Há uma série de tecnologias que podem ajudá-lo a identificar automaticamente as ameaças em suas contas em nuvem, desde a identificação de malwares conhecidos, atividade maliciosa e ameaças, que podem ser induzidas a se expor. Veja como é possível aplicar uma abordagem em camadas usando todos os itens mencionados acima para diminuir o risco à sua empresa.

Identificar e controlar as contas comprometidas

Implementar um CASB ou outra solução com funcionalidades eficientes de análise de comportamento do usuário (UBA, user behavior analysis) é uma excelente forma de identificar e reduzir os prejuízos causados pelas contas do Office 365 comprometidas. Esse método é capaz de encontrar ameaças difíceis ou impossíveis de serem identificadas usando outros métodos de proteção contra ameaças.

Automatize o antimalware em sua nuvem

Adicione soluções antimalware que verificam e corrigem infecções por malware nas suas contas em nuvem. Essa é uma camada de proteção eficiente e fácil de ser automatizada. Aproveite para proteger quantos terminais você conseguir: um terminal infectado é uma ótima oportunidade para as ameaças invadirem a sua nuvem.

Adicione proteção contra ameaças avançadas

Considere acrescentar uma camada de proteção contra ameaças avançadas para analisar os arquivos transferidos em suas contas em nuvem (incluindo, entre outros, o Office 365). Essas correções estão disponíveis como serviços em nuvem e/ou soluções locais e aproveitam o sandboxing e a emulação de códigos para induzir os malwares não identificados a se expor. Essa é uma camada de proteção importante no cenário atual de malware, que é polimórfico e altamente direcionado.

Prepare-se

Em algum momento, você terá um incidente de segurança. Quando isso acontecer, é preciso ser capaz de responder rapidamente para reparar os danos e evitar futuros incidentes.

O segredo da resposta a incidentes é a capacidade de identificar uma área de interesse e encontrar os dados relacionados em detalhes utilizáveis para analisar o que aconteceu. É preciso ter um sistema que seja capaz de identificar, com agilidade, se há alguma área de interesse que necessite de investigação. Também é necessário encontrar exatamente a informação relacionada ao problema investigado. Em seguida, devemos ter informações com detalhes suficientes para realizar uma análise eficiente. E, por fim, é possível analisar os dados de diversas fontes com uma solução de gerenciamento de incidentes e eventos de segurança (SIEM, Security Event and Incident Management).

Pode ser difícil obter o nível correto de visibilidade e registrar os dados das atividades nas contas em nuvem. Busque CASB, ATP, SWG e outras soluções de segurança que oferecem relatórios de alta qualidade e possuem fácil integração com seus sistemas de análise central.

Tenha uma visão panorâmica

Hoje, é possível que você esteja pensando apenas na adoção do Office 365, mas, provavelmente, essa não é a única aplicação em nuvem que a sua empresa utilizará. Inclusive, você já deve usar diversas outras soluções em nuvem para ativação de negócios. Ao considerar a implementação de segurança para o Office 365 ou qualquer outra aplicação em nuvem, lembre-se de avaliar os benefícios de soluções de segurança consolidadas de terceiros e da segurança nativa oferecida pelos fornecedores individuais de aplicações em nuvem. Nenhuma aplicação em nuvem fica isolada. Cada nuvem utilizada faz parte da infraestrutura integrada e da propriedade intelectual de sua empresa. A Gartner prevê que 40% das empresas optarão por proteger o Office 365 com soluções de terceiros. Uma solução de terceiros compatível com todos os tipos de nuvem pode oferecer uma visibilidade mais ampla, funcionalidades consistentes de segurança e, normalmente, maior eficiência para diversas aplicações em nuvem, sendo mais fácil de usar pelo seu departamento de TI.

Em resumo...

Parabéns por dar um passo à frente em sua adoção do Office 365. Você perceberá uma série de benefícios comerciais com essa migração. No entanto, para adotar o Office 365, também é preciso realizar um planejamento financeiro e estratégico em relação a medidas de segurança adicionais. Provavelmente, você precisará prever e acomodar maiores volumes de tráfego de Internet.

Para adotar o Office 365 com segurança, é necessário atender às exigências a seguir:

- Proteger o acesso às suas contas do Office 365 com SSO e MFA;
- Proteger-se contra comportamentos suspeitos de usuários nas contas do Office 365 utilizando análises de comportamento do usuário e CASB;
- Proteger seus dados sigilosos na nuvem contra perda com o CASB e DLP;
- Planejar a implementação do Office 365 para conformidade regulamentar com análise de risco e visibilidade da nuvem e controles de segurança excelentes;
- Proteger-se contra malware e ameaças avançadas em sua nuvem do Office 365 com UBA, antimalware e ATP;
- Preparar-se para ter uma resposta eficiente a incidentes se ou quando houver um problema de segurança com registros e relatórios excelentes de todas as suas soluções de segurança; e
- Planejar sua infraestrutura organizacional prevendo um aumento no tráfego de Internet e nas conexões. Talvez seja preciso dimensionar ou otimizar o desempenho de toda a sua rede e das soluções de segurança que lidam com o tráfego de Internet.

Sobre a autora

Deena Thomchick é diretora sênior do setor de nuvem da Blue Coat. Ela possui mais de 25 anos de experiência na área de tecnologia, com ênfase em segurança. Alguns de seus trabalhos estão relacionados à criptografia, proteção contra ameaças avançadas, segurança de rede e segurança de terminais.

Sobre a segurança em nuvem da Blue Coat e da Elastica

A Blue Coat, Inc. é fornecedora líder em soluções avançadas de Web Security para empresas internacionais e governos, protegendo 15 mil organizações por dia, incluindo mais de 70% das empresas na lista global da Fortune 500. Com sua plataforma de segurança, a Blue Coat combina a rede, a segurança e a nuvem, protegendo empresas e seus usuários contra ameaças virtuais, sejam na rede, na Web, na nuvem ou em dispositivos móveis. A Blue Coat foi adquirida pela Bain Capital em maio de 2015. Em 12 de junho de 2016, a Symantec e a Blue Coat, Inc. anunciaram a celebração de um contrato definitivo pelo qual a Symantec comprará a Blue Coat à vista, por aproximadamente US$ 4,65 bilhões. A operação foi aprovada pela diretoria das duas empresas e sua conclusão é esperada para o terceiro trimestre de 2016.

A Elastica, adquirida pela Blue Coat em novembro de 2015, é líder em segurança de acesso à nuvem Data Science Powered™. Sua plataforma CloudSOC™ proporciona autonomia às empresas para aproveitar aplicações e serviços em nuvem enquanto permanecem seguras, protegidas e em conformidade. Uma série de aplicações de segurança da Elastica implementadas na plataforma ampliável CloudSOC fornecem o ciclo de vida completo de segurança de aplicações em nuvem, incluindo auditoria de shadow IT, detecção em tempo real de invasões e ameaças, proteção contra invasões e violações à conformidade e investigação do histórico de atividades de conta para análise pós-incidente.

Para obter mais informações, acesse bluecoat.com e elastica.net.