ManageEngine
M365 Manager Plus

Sete Melhores Práticas para asegurar seu Microsoft 365

Introdução

Com mais de 135 milhões de usuários ativos por mês mundialmente, o Microsoft 365 é o conjunto de aplicações na nuvem mais utilizado. Para muitas organizações, ele é o ponto de entrada para a computação em nuvem. À medida que que se começa a migrar dados sensíveis e críticos de negócios para plataformas na nuvem como o Microsoft 365, várias preocupações de segurança podem estar na sua mente: os dados estão seguros? Quem possui acesso? E se um usuário não autorizado comprometer contas privilegiadas? E quanto ao cumprimento dos requisitos de conformidade?

Quando se trata do Microsoft 365, você pode aproveitar os recursos fornecidos pela Microsoft e outras ferramentas de administração do Microsoft 365, como o M365 Manager Plus, para simplificar o seu monitoramento de segurança.

Neste white paper, analisaremos as práticas recomendadas de monitoramento de segurança para o Microsoft 365, incluindo os tipos de atividades que você deve monitorar, ameaças a serem procuraradas e quais ferramentas você pode usar para fazer tudo isso.

Atividades do Microsoft 365 que você deve monitorar

Saber por onde começar com o monitoramento de segurança do Microsoft 365 pode ser um desafio. Para começar, você precisa saber quais atividades monitorar e o que elas podem dizer sobre sua segurança de TI. No geral, os tipos de atividades do Microsoft 365 que devem ser monitoradas, se você já não estiver fazendo isso, são:

Acesso do usuário: Saiba quem está assessando sua assinatura do Microsoft 365, quando e de onde. Estabeleça um padrão para o comportamento normal de acesso do usuário e detecte quaisquer desvios para saber de tentativas de ataque. Por exemplo, se um usuário tentar logar de uma localização não usual, com certeza é uma atividade suspeita e justifica uma análise.

Ações do administrador: uma vez que invasores possuem acesso a seu ambiente, eles frequentemente tentam aumentar seus privilégios para tentar acessar seus dados sensíveis, tal como fazem os infiltrados maliciosos. O monitoramento de mudanças nas funções de administrador, a forma como suas atividades são registadas e os direitos de acesso podem ajudá-lo a detectar potenciais ameaças externas e internas nas suas fases iniciais.

Permissões de mudanças: Monitorar as mudanças de permissões e políticas de compartilhamento de arquivos no One Drive for Business pode ajudá-lo a detectar os primeiros sinais de uma potencial violação de dados. Além disso, monitorar as atividades de arquivos por usuário, incluindo quando eles são carregados, deletados, editados e restaurados, pode ajudá-lo a detectar e investigar atividades anômalas.

Mudanças nas políticas do Microsoft 365: As políticas do Microsoft 365 definem os direitos de acesso dos usuários aos recursos, assim como as atividades que eles podem executar no seu ambiente do Microsoft 365. Quaisquer alterações indesejadas resultarão em uma lacuna na segurança. Por isso, é necessário monitorar continuamente as mudanças nas políticas, incluindo as de malware e filtragem de conteúdos do Exchange. Mudanças a estas políticas podem permitir que os spammers enviem e-mails de phishing e anexos maliciosos. Você também deve estar atento a quaisquer alterações que enfraqueçam as políticas de senhas da sua organização.

Atividades com agentes mal-intencionados conhecidos: O monitoramento de suas atividades do Microsoft 365 em contexto de vetores de ataque conhecidos ajuda a mitigar os ataques nas suas fases iniciais. A identificação de atividades, como o compartilhamento de arquivos com anfitriões maliciosos e o carregamento de vários uploads com extensões de arquivos de ransomware conhecidas pode alertá-lo para possíveis ameaças segurança.

Melhores práticas para monitorar a segurança do Microsoft 365

Existem várias medidas que podem ser tomadas para proteger o seu ambiente Microsoft 365.

Abaixo, discutiremos sete práticas recomendadas que sua organização deve seguir para o monitoramento abrangente de sua segurança.

Melhor prática 1:
Configure políticas de senhas e autenticação multi-fator (MFA)

No Centro de Administração do Microsoft 365, você pode fortalecer a segurança do Azure AD configurando políticas para senhas fortes, expiração de senha e MFA para acesso. Essas são boas práticas de segurança, mas sozinhas, não são suficientes. É necessário também monitorizar continuamente as atividades de início de sessão dos usuários para procurar sinais de credenciais comprometidas.

Melhor prática 2:
Monitore todas as atividades de sign-in dos usuários do Azure AD

Quando um usuário anômalo faz login no seu ambiente do Microsoft 365, você precisa conhecer todos os detalhes associados a esse incidente para interromper a violação em seu caminho. Por exemplo, se o seu CFO estiver em Nova York, mas se conectar da China, você deve saber imediatamente. Monitore toda a atividade de login do usuário no Azure AD para estabelecer uma linha de base de atividade padrão. Assim, você pode identificar anomalias, como entradas incomuns com base em horário, frequência ou local. Monitore se há picos repentinos de tentativas ou falhas repetidas de login, pois podem ser indicações de um ataque de força bruta. Você pode monitorar as atividades de entrada do usuário com os relatórios do Azure AD ou uma solução de monitoramento de segurança do Microsoft 365 de terceiros, como o M365 Manager Plus.

Melhor prática 3:
Estabeleça uma política de privilégio mínimo

Talvez você já esteja familiarizado com esta prática recomendada de segurança universal, mas, dada a importância no contexto de segurança do Microsoft 365, vale a pena reavaliar as políticas atuais de sua organização. Em geral, você deve conceder privilégios o mínimo possível aos seus administradores - o suficiente para que eles realizem seu trabalho e nada mais. Mudanças de privilégios podem indicar um agente mal-intencionado em seu ambiente que está tentando obter acesso aos dados confidenciais de sua empresa, por isso é importante monitorar continuamente essas atividades por meio dos logs de auditoria administrativa.

Melhor prática 5:
Monitore os registros de auditoria do administrador do Microsoft 365

Por padrão, os administradores têm direitos e permissões para acessar os registros de auditoria, monitorar atividades dos usuários e detectar anomalias. Mas sempre há a chance de um insider mal-intencionado com privilégios de administrador tentar adulterar os logs de auditoria para ocultar seus rastros. Esse é o motivo, para além das mudanças nas funções e permissões, que você deve monitorar todas as atividades do administrador.

Você pode auditar essas atividades com o recurso de auditoria de log administrativa do Microsoft 365:

- Atividades de arquivos e páginas
- Atividades de arquivos
- Atividades de compartilhamento e solicitação de acesso
- Sincronização de atividades
- Atividades de administração do site
- Atividades da caixa de correio do Exchange
- Atividades de balanço
- Atividades de administração de usuários
- Atividades de administração de grupos do Azure AD
- Atividades de administração de aplicativos
- Atividades de administração de funções
- Atividades de administração do Directory
- Atividades do eDiscover
- Atividades do Power BI
- Atividades do Microsoft Teams
- Atividades do Yammer
- Atividades administrativas do Exchange

Melhor prática 5:
Monitore todas as atividades do usuário no OneDrive for Business

É importante monitorar todos os acessos e atividades dos usuários (excluir, carregar, editar, restaurar, etc.) para os dados críticos para negócios armazenados no OneDrive for Business. Ao estabelecer uma linha padrão da atividade regular do usuário, é possível detectar anomalias que justifiquem uma investigação. Por exemplo, um usuário que esteja restaurando vários arquivos excluídos no OneDrive for Business pode ser um agente mal-intencionado tentando recuperar dados históricos. É claro que sempre há a possibilidade de um funcionário simplesmente excluir alguns arquivos importantes por acidente, mas, de qualquer forma, vale a pena investigar.

Além disso, a manutenção de logs de todas as atividades de arquivos de usuários pode ajudá-lo não apenas a atender aos requisitos de conformidade, como o PCI DSS, mas também a realizar investigações forenses após uma violação de dados.

Melhor prática 6:

Monitore mudanças nas permissões de compartilhamento do OneDrive for Business e de arquivos com entidades externas

Quando seus usuários compartilham arquivos com entidades fora de sua organização, você precisa saber disso. É por isso que você precisa monitorar as mudanças no OneDrive for Business que habilitam as permissões de compartilhamento externo. Com ferramentas avançadas, como o M365 Manager Plus, você pode criar seus próprios perfis de auditoria e configurar alertas de e-mail em tempo real para serem enviados a você sempre que as permissões de compartilhamento de arquivos forem modificadas.

Melhor prática 7:

Monitore mudanças nas políticas de filtragem do Exchange Online

No Microsoft Exchange Admin Center (EAC), você pode definir suas políticas de filtragem de conteúdo (spam) e malware, entre outras configurações. No entanto, a definição dessas políticas não é uma atividade do tipo "configure e esqueça". Em vez disso, você deve monitorar continuamente as mudanças nessas políticas que indiquem um ataque ou violação. Se elas enfraquecem suas políticas de filtragem de conteúdo ou malware, remetentes poderão enviar spam, inclusive e-mails de phishing ou anexos carregados de malware.

Quais ferramentas devem ser usadas para monitorar o Microsoft 365?

Há muitas ferramentas e recursos disponíveis para ajudá-lo a proteger e monitorar seu ambiente do Microsoft 365. De fato, pode ser muito difícil tentar descobrir por onde começar.

Centro de Segurança e Conformidade do Microsoft 365

A Microsoft chama o seu Microsoft 365 Security & Compliance Center de portal único para proteger seus dados no Microsoft 365. Ele oferece funções úteis, como arquivamento de caixas de correio, prevenção de perda de dados, pesquisa de conteúdo e atividades do usuário, gerenciamento de dispositivos, permissões de assinatura e retenção de documentos.

Microsoft 365 Cloud App Security

A Microsoft oferece o Microsoft 365 Cloud App Security, anteriormente conhecido como Microsoft 365 Advanced Security Management, que fornece informações sobre atividades suspeitas no Microsoft 365 para que você possa investigar situações potencialmente problemáticas e tomar medidas para resolver problemas de segurança quando eles surgirem. Com ele, você pode receber notificações de alertas acionados para atividades atípicas ou suspeitas, ver como os dados da sua organização no Microsoft 365 são acessados e usados, suspender contas de usuários que exibem atividades suspeitas e exigir que os usuários façam login novamente nos aplicativos do Microsoft 365 depois que um alerta for acionado.

No momento em que este artigo foi escrito, o Microsoft 365 Advanced Security Management estava disponível no Microsoft 365 Enterprises E5 e como um complemento para outros planos do Microsoft 365 Enterprise.

API de gerenciamento do Microsoft 365 e gerenciamento de segurança unificado

A API de gerenciamento do Microsoft 365 amplia os recursos de segurança e conformidade para soluções dedicadas de gerenciamento de segurança, incluindo o M365 Manager Plus. Por meio da RESTful API, as aplicações externas podem obter informações sobre ações e eventos de usuários, administradores, sistemas e políticas dos logs de atividades do Microsoft 365 e do Azure Active Directory. Isso significa que você pode gerenciar o monitoramento de segurança do Microsoft 365 em sua plataforma que for existente, se ela for compatível com a API.

Por que você deve considerar o uso de uma ferramenta de monitoramento de segurança de terceiros

Embora a Microsoft ofereça muitas ferramentas, capacidades e recursos para segurança e conformidade, encontrar onde provisionar, configurar e usar cada serviço pode ser tremendamente desafiador. Embora a experiência do usuário seja apenas um fator a ser considerado, há muitos outros motivos pelos quais você pode querer considerar o uso de uma solução de monitoramento de segurança de terceiros para o Microsoft 365.

Uma camada adicional de monitoramento de segurança

Uma solução de monitoramento de segurança dedicada pode fornecer uma camada adicional de garantia de segurança e recursos críticos de detecção de ameaças para seu ambiente do Microsoft 365, incluindo regras, alarmes e análises pré-criados..

Visibilidade centralizada de toda a sua postura de segurança

Quando você analiza as atividades dos usuários no Centro de Conformidade e Segurança do Microsoft, você precisa procurar por informações de segurança relacionadas em várias ferramentas e registros para obter todo o contexto da ameaça durante a investigação e resposta. Uma solução de gerenciamento de segurança unificado desmonta os silos de dados, agregando todos aqueles que são relacionados à segurança em um único lugar. Estes dados incluem informações sobre seus ativos, vulnerabilidades conhecidas, atividades de usuários e mais, o que torna uma investigação de incidente muito mais eficiente.

Retenha auditorias de log por mais de 90 dias

A partir de hoje, Microsoft elimina qualquer log do Microsoft 365 com duração maior de 90 dias. Se você está procurando por uma retenção de períodos de log melhor para cumprir os regulamentos, você pode aproveitar uma solução como o M365 Manager Plus para coletar logs do Microsoft 365 e os armazer indefinidamente.