ManageEngine
O365 Manager Plus

Checklist de auditoria do OIG para Office 365 e como se preparar para ela.

Introdução

Desde sua criação, a missão do Escritório do Inspetor-Geral (OIG) do Departamento de Saúde e Serviços Humanos dos EUA tem sido combater o desperdício, a fraude e o abuso. Com a ascensão do software como serviço (SaaS), plataforma como serviço (PaaS) e infraestrutura como serviço (IaaS), o OIG aumentou a fiscalização para garantir que as agências federais e os prestadores de serviço contratados pela esfera federal que transmitem informações não classificadas controladas (CUI) federais estejam seguindo as políticas estabelecidas pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA. As auditorias do OIG são uma forma de garantir que as organizações estejam em conformidade com essas políticas.

Mais de 80% das agências federais utilizam Microsoft Office 365, Azure AD e produtos de colaboração, como SharePoint, Yammer e Teams, para atender a milhares de funcionários e contratados. É de suma importância que eles protejam as informações confidenciais presentes nessas plataformas para cumprir as recomendações do NIST.

Neste e-book, discutiremos como configurar o Office 365 para garantir que seu locatário seja aprovado em uma auditoria do OIG.

O que será avaliado em uma auditoria do OIG

Os três aspectos de segurança que serão avaliados em uma auditoria do OIG incluem:

- **Segurança de informações de identificação pessoal (PII)**
- **Implementação de autenticação multifator (MFA)**
- **Políticas de retenção**

Informações de identificação pessoal (PII)

De acordo com o NIST, PII é qualquer informação sobre um indivíduo mantida por uma agência, incluindo **(1)** qualquer informação que possa ser usada para distinguir ou rastrear a identidade de um indivíduo, como nome, CPF, data e local de nascimento, nome de solteira da mãe ou registros biométricos; **(2)** qualquer outra informação vinculada ou vinculável a um indivíduo, como informações médicas, educacionais, financeiras e de trabalho.

Segurança de PII na Comissão de Valores Mobiliários dos EUA (SEC): Observações do OIG

A SEC dos EUA foi recentemente auditada pelo OIG, e descobriu-se que ela não armazenou corretamente as PII. Do relatório de auditoria:

"Além disso, em pelo menos cinco ocasiões, o pessoal desta agência não havia aplicado os requisitos contratuais relacionados com a proteção das PIIs, embora os especialistas pudessem acessá-las, e elas incluíam nome, endereço e data de nascimento de investidores e informações sobre contas de clientes. Também descobrimos que faltavam controles sobre os contratos em relação à liberação ou divulgação inadvertida de informações após a transmissão de informações a especialistas pela SEC. Como resultado, a agência não possuía a garantia de que os especialistas e seus sistemas de informação alcançavam níveis básicos de segurança que protegessem as informações confidenciais e não públicas da SEC, incluindo PIIs. Não identificamos ocasiões em que indivíduos não autorizados acessaram essas informações depois de elas terem sido fornecidas a especialistas. No entanto, a agência deve tomar medidas para minimizar o risco de divulgação, modificação e uso não autorizados de suas informações confidenciais e não públicas fornecidas aos especialistas."

Como proteger as PIIs no Office 365

Os recursos de gerenciamento de conformidade do Office 365 ajudarão você a monitorar e controlar quem pode acessar as PIIs afim de proteger o acesso às suas PIIs. No entanto, ele não tem alertas em tempo real. Então, qual é a solução? Uma ferramenta de administração, gerenciamento e auditoria do Office 365, como o O365 Manager Plus.

O e-mail continua a ser a via mais popular em comunicação de negócios e um meio simples pelo qual os funcionários podem compartilhar dados. O ManageEngine O365 Manager Plus identifica os e-mails com PIIs e outras informações privilegiadas. Depois de salvos os critérios a serem identificados nos e-mails, a ferramenta enviará os resultados da pesquisa em intervalos regulares diretamente para sua caixa de entrada.

Saiba como executar uma pesquisa de conteúdo no Office 365 usando o O365 Manager Plus.

Autenticação multifator (MFA)

De acordo com o NIST, MFA significa utilizar dois ou mais fatores diferentes para fazer a autenticação. Os fatores incluem: (i) algo que você sabe (como uma senha ou um PIN); (ii) algo que você tem (como um dispositivo de identificação criptográfica ou token); ou (iii) algo que você é (como biometria).

Configurações de MFA do Departamento de Energia dos Estados Unidos (DOE): Observações do OIG

O OIG é muito rigoroso com organizações que não protegem o acesso a seus dados com autenticação multifator. Em uma auditoria recente do sistema do Departamento de Energia dos Estados Unidos (DOE), o OIG declarou:

"Os pontos fracos identificados ocorriam, em parte, porque os funcionários não tinham planejado totalmente a implementação da autenticação multifator nos sistemas de informação. A orientação e os requisitos do departamento relacionados às tecnologias de autenticação multifator também nem sempre eram comunicados com eficiência. Sem o desenvolvimento e a implementação de um processo de autenticação multifator a nível de todo o Departamento, suas informações, incluindo dados sigilosos, continuarão sob um risco de segurança maior que o normal. Fizemos recomendações que, caso sejam implementadas em sua totalidade, devem ajudar o Departamento a melhorar sua segurança cibernética por meio da implementação eficaz da autenticação multifator. A gerência concordou com as recomendações do relatório e informou que haviam sido iniciadas ou planejadas ações corretivas para abordar os problemas identificados no relatório."

Como gerenciar as configurações de MFA no Office 365

O Admin Center do Microsoft Office 365 oferece aos administradores a opção de ativar ou desativar a MFA para vários usuários por vez. No entanto, a escolha de selecionar os métodos de verificação fica nas mãos dos usuários finais.

Por outro lado, o O365 Manager Plus permite que os administradores ativem, desativem e configurem os métodos de autenticação para vários usuários, sem a necessidade de privilégios especiais ou licenças premium adicionais. Os administradores podem até delegar o gerenciamento da MFA ao suporte técnico através de recursos de delegação personalizados, sem comprometer a segurança. O O365 Manager Plus também oferece um conjunto exclusivo de relatórios de auditoria integrados para monitorar de perto as atividades dos técnicos.

Aprenda a configurar a MFA para o Office 365 usando o O365 Manager Plus.

Políticas de retenção

As políticas de retenção ajudam a excluir itens desnecessários e/ou reter dados importantes para análise pericial. Elas podem ser aplicadas a uma organização inteira, a um grupo de usuários, a uma única caixa de correio ou a um site.

As políticas de retenção também são usadas para verificar e-mails e outros itens na pasta itens recuperáveis. Como padrão, se não for definida uma política de retenção, os dados são excluídos em 14 dias. Esse período de tempo pode ser estendido para um máximo de 30 dias. Após esse período, os itens são excluídos e não podem ser recuperados. Os próprios usuários podem excluir os arquivos, no entanto, com uma política de retenção, os administradores ainda poderão acessar esses dados usando eDiscovery ou Search-Mailbox.

Como essas políticas de retenção podem tanto preservar como excluir conteúdo, é importante saber o que acontece caso mais de uma política seja aplicada em um único item. Há uma prioridade definida nas regras de retenção: a regra mais importante é que a retenção sempre tem precedência sobre a exclusão e, se mais de uma retenção se aplicar a um item, a que tiver o período de retenção mais longo terá preferência.

Exemplo: Há uma política de retenção aplicada em toda a organização que protege os dados com menos de cinco anos de idade, e outra política do mesmo tipo que exclui os itens com mais de dois anos de idade. Os itens criados há três anos não serão excluídos por causa da primeira política, enquanto os itens com mais de cinco anos serão excluídos por causa da segunda política.

Somente usuários com permissão apropriada podem criar e gerenciar políticas de retenção. Há dois grupos padrão que têm permissão para gerenciar políticas de retenção: O administrador de conformidade e a gerência da organização.

Saiba como colocar as caixas de correio do Office 365 em retenção e aplicar políticas de retenção usando o O365 Manager Plus.

Como configurar políticas de retenção no Office 365

Dependendo das normas que uma organização precisa seguir, ela terá diferentes agendas de retenção para e-mails, demonstrativos financeiros, correios de voz e documentos. Isso pode ser um problema se os documentos e e-mails não tiverem sido marcados corretamente.

As etiquetas de retenção do Office 365 são usadas para especificar por quanto tempo uma mensagem permanece na caixa de correio e a ação a ser tomada quando a mensagem atinge a idade de retenção especificada. Quando uma mensagem atinge o período máximo de retenção, ela é movida para o arquivo local do usuário ou excluída. Para aplicar uma ou mais etiquetas de retenção a uma caixa de correio, você deve adicioná-las a uma política de retenção e, em seguida, aplicar a política às caixas de correio.

Com o O365 Manager Plus, os administradores podem colocar as caixas de correio dos usuários que entraram em férias em retenção, mantendo os itens excluídos da caixa de correio por um número especificado de dias, independentemente das políticas de retenção aplicadas aos itens da caixa de correio.

Saiba como colocar caixas de correio em retenção usando o O365 Manager Plus.

Conclusão

Preparar-se para uma auditoria do OIG, ou qualquer outra auditoria de conformidade, é um processo contínuo, demorado e que demanda intensos recursos. Na maioria dos casos, o OIG agendará uma visita de acompanhamento no local, para se certificar de que todas as violações foram corrigidas, portanto, busque entender claramente os requisitos.