Prevention First

Preveção em primeiro lugar

Por que a proteção nativa do Microsoft 365 e do Google Workspace não é suficiente

Cybersecurity
Progress. Protected.

Lacunas na Proteção de E-mails

As organizações certamente estão entre os 3 bilhões de usuários do Google Workspace (incluindo 1,8 bilhão de usuários ativos do Gmail), 400 milhões de usuários do Outlook ou os 320 milhões de usuários do aplicativo de colaboração Microsoft Teams, todas ferramentas digitais essenciais para os negócios.

Após a implementação bem-sucedida e a configuração de algumas regras de segurança, em um cenário ideal, as equipes corporativas poderiam se concentrar em tarefas críticas para o negócio, trabalhando em ambientes de colaboração seguros.

No entanto, isso nem sempre acontece. Há **inúmeros agentes de ameaça que abusam de aplicativos legítimos na nuvem**, mas esse problema tem solução. Os gestores de TI precisam implementar camadas adicionais de segurança.

Com as ferramentas certas, os administradores podem minimizar a superfície de ataque originada nos serviços em nuvem, adotando uma abordagem de prevenção em primeiro lugar, que protege os aplicativos de colaboração corporativa e o e-mail contra ameaças antes que elas sejam executadas.

Entre os maiores desafios que as empresas enfrentam no campo da segurança de aplicações em nuvem estão, principalmente, as ameaças relacionadas ao e-mail:

PHISHING AND SPEAR-PHISHING

Os atacantes utilizam métodos inovadores, como o uso de QR Codes ou homoglifos, para induzir as pessoas a escanear e/ou clicar em links que aparentam ser legítimos.

IMPERSONAÇÃO E SPOOFING DE E-MAIL / COMPROMETIMENTO DE E-MAIL CORPORATIVO

Los correos electrónicos que intentan engañar a las personas para que crean que se están comunicando con un remitente legítimo son cada día mejores, especialmente con el uso creciente de tecnologías de IA.

FATOR HUMANO

Os colaboradores cometem erros, o que torna os gateways de e-mail especialmente atrativos para os atacantes. Treinamentos em cibersegurança continuam sendo fundamentais, pois o fator humano permanece como o elo mais fraco da cadeia, e nenhuma tecnologia funciona 100% se não for utilizada corretamente.

AMEAÇAS ZERO-DAY

A IA também está facilitando a criação de ameaças novas ou nunca vistas anteriormente por parte dos adversários.

E-mail: o playground favorito dos cibercriminosos

O e-mail continua sendo o principal vetor de ameaças cibernéticas. Nos últimos anos, a ESET detectou e bloqueou milhões de ameaças que contornaram as proteções nativas do Microsoft 365 e do Google Workspace.

A maioria dessas ameaças bloqueadas consistia em mensagens de phishing e spam. De acordo com a Verizon, o tempo médio para que os usuários caiam em e-mails fradulentos foi inferior a 60 segundos. O Relatório de Investigações de Violações de Dados de 2024 da empresa aponta que o pretexting é uma das técnicas de ataque mais utilizadas. O número de casos quase dobrou de 2022 para 2023 e, atualmente, o pretexting está envolvido em cerca de 20% de todos os ataques com motivação financeira. A maioria dos incidentes de pretexting resultou no comprometimento de e-mails corporativos, com um valor médio de transação em torno de US$ 50.000, segundo dados do FBI IC3. Os dados mais recentes indicam que essa tendência não dá sinais de desaceleração.

Segundo o ESET Threat Report H2 2024, a detecção de spam aumentou 19%, e arquivos HTML maliciosos que direcionam as vítimas para sites de phishing (trojan **HTML/Phishing.Agent**) continuam sendo, de longe, a ameaça mais prevalente por e-mail. No total, **esses ataques por e-mail representam quase um quarto (23,8%) de todas as ameaças cibernéticas detectadas pela ESET**. Outras ameaças em nuvem detectadas pela telemetria da ESET incluem diversos tipos de malware, como backdoors, spyware, infostealers e downloaders

Não tão seguro quanto parece

Embora a Microsoft e o Google tenham incorporado tecnologias avançadas de segurança diretamente em seus aplicativos em nuvem, que são protegidos e atualizados regularmente, isso não significa que estejam imunes a todas as ameaças existentes. Casos reais mostram que aplicativos e serviços legítimos em nuvem podem ser explorados para distribuir malware, ofuscar processos maliciosos e permitir acesso remoto a dispositivos corporativos:

- Pesquisadores da ESET identificaram, nos últimos anos, novas campanhas de phishing conduzidas por um agente de ameaça desconhecido, direcionadas a empresas em países europeus. Os e-mails continham anexos maliciosos protegidos pelo AceCryptor, um cryptor-as-a-service projetado para ocultar outros malwares de

ferramentas de cibersegurança. Caso o ataque fosse bem-sucedido, os invasores poderiam implantar o Remcos (também conhecido como Rescoms), uma ferramenta de acesso remoto e espionar as vítimas.

- No segundo semestre de 2024, o **Formbook**, um **infostealer** descoberto originalmente em 2016, apresentou um ressurgimento significativo, com aumento de mais de 200% nas detecções. Esse malware coleta, entre outros dados, informações da área de transferência, keystrokes, capturas de tela e dados em cache de navegadores. Trata-se de uma solução de malware-as-a-service (MaaS), comercializada em fóruns clandestinos, que se propaga por meio de anexos maliciosos em e-mails de phishing. Os produtos da ESET protegeram quase 34.000 usuários, principalmente na Europa Oriental e Central, além do Japão, Canadá e Espanha.
- Felizmente, na maioria dos casos, profissionais de cibersegurança identificam vulnerabilidades antes dos agentes de ameaça. Em junho de 2023, a equipe de testes de intrusão da empresa britânica de serviços de segurança Jumpsec descobriu e demonstrou uma forma de distribuir programas maliciosos por meio do Microsoft Teams, utilizando uma conta externa à organização-alvo. A equipe conseguiu **contornar as proteções integradas** e enganar o sistema, fazendo-o acreditar que um usuário externo era, na verdade, uma conta interna.

A ESET, fornecedora líder em cibersegurança, utiliza o ESET Cloud Office Security para proteger ambientes de colaboração baseados em nuvem.

Essa solução avançada aprimora os recursos de segurança nativos do Microsoft 365 e do Google Workspace ao realizar análises após os aplicativos classificarem e-mails ou arquivos como "seguros".

Os dados a seguir*, fornecidos pela ESET, mostram quantas ameaças conseguiram ultrapassar as defesas nativas.

920,000
ameaças de e-mail detectadas

813,000
e-mails de phishing bloqueados

110,000
ameaças não relacionadas a e-mail originadas no OneDrive, SharePoint e Google Drive

75,820,000
e-mails de spam capturados

Como aprimorar as defesas em *nuvem*?

É claro que, isoladamente, a segurança nativa dos aplicativos em nuvem não é suficiente. Para reduzir essa superfície de ataque crescente e prevenir ou mitigar ataques antes que causem danos, as empresas devem considerar o reforço dos controles nativos da Microsoft ou do Google com **camadas adicionais de proteção:**

Filtragem de spam

As mensagens de spam representaram mais de **46,8% dos 362 bilhões de e-mails** enviados e recebidos diariamente em todo o mundo em 2024. Com a solução de filtragem adequada, as empresas podem economizar um tempo significativo dos colaboradores e evitar problemas causados por spam malicioso.

Anti-phishing

Em 2024, o phishing foi identificado como o vetor inicial de ataque em 22% dos ciberataques enfrentados por empresas nos Estados Unidos. Contar com uma ferramenta automatizada que reconheça links de phishing anexados a e-mails é absolutamente essencial.

Verificação antimalware

Uma boa solução de segurança em nuvem deve realizar automaticamente a verificação de arquivos novos ou alterados em armazenamentos compartilhados, evitando que malwares sejam executados ou se espalhem.

Análise comportamental e ambiente de sandbox

Diante do surgimento contínuo de novas ameaças, ferramentas automatizadas de cibersegurança precisam estar preparadas para ataques nunca vistos anteriormente. Isso pode ser feito por meio de uma análise comportamental aprofundada de amostras suspeitas em um ambiente de sandbox isolado e seguro.

Anti-spoofing e mecanismo de regras

E-mails maliciosos que ocultam sua identidade ou se passam por remetentes legítimos precisam ser bloqueados. Com esse controle, apenas e-mails que aparentam vir de fontes confiáveis são realmente legítimos e permitidos.

Proteção contra homóglifos

Atacantes utilizam caracteres semelhantes para criar endereços de e-mail ou domínios enganosos que parecem legítimos. Detectar e bloquear ataques de homóglifos ajuda a prevenir phishing direcionado e outras atividades maliciosas, garantindo que as comunicações da organização permaneçam seguras.

Como a ESET ajuda

Ter tantas ferramentas à disposição e gerenciar um sistema de segurança robusto pode parecer mais um desafio. No entanto, adicionar camadas extras de segurança não precisa, necessariamente, aumentar a complexidade do trabalho dos administradores de TI.

O **ESET Cloud Office Security oferece proteção preventiva avançada para aplicativos do Microsoft 365 e do Google Workspace,** , com todos os recursos mencionados anteriormente. A solução aprimora a postura de segurança da organização por meio de proteção avançada contra ameaças, além de proporcionar visibilidade e controle sobre e-mails, compartilhamento de arquivos e ferramentas de dados e colaboração baseadas em nuvem. Além de operações mais eficientes e segurança aprimorada, o ESET Cloud Office Security contribui para a **redução da complexidade ao centralizar e automatizar processos rotineiros,** como:

- Novos usuários no ambiente corporativo não precisam ser adicionados manualmente por um administrador de TI em um console, eles passam a ser protegidos automaticamente após a criação da conta.
- Administradores de TI podem configurar intervalos de notificação para evitar a fadiga de alertas, garantindo ao mesmo tempo o recebimento dos avisos mais importantes.
- Arquivos suspeitos podem ser gerenciados facilmente em uma quarentena centralizada, com a possibilidade de liberação, exclusão ou investigação adicional, se necessário.

- A solução permite o gerenciamento multi-tenant para dezenas de milhares de usuários, abrangendo contas criadas nas duas plataformas mais utilizadas: Microsoft 365 e Google Workspace.

Com foco na prevenção e na proteção dos usuários finais e de seus dispositivos, o ESET Cloud Office Security assegura níveis mais elevados de proteção contra ameaças ao reduzir as superfícies de ataque relacionadas à nuvem, aliviando assim a carga de trabalho dos administradores de TI por meio de um console de gerenciamento em nuvem intuitivo.

Como solução independente ou como parte da ESET PROTECT Platform, ESET Cloud Office Security ajuda a proteger as organizações contra infecções, minimiza interrupções no trabalho causadas por mensagens não solicitadas e contribui para a prevenção de ataques direcionados e de ameaças inéditas, especialmente ransomware.

INTEGRAÇÃO

Por fim, o ESET Cloud Office Security conta com integração gratuita com o **ESET LiveGuard Advanced**, uma tecnologia baseada em nuvem que utiliza análise avançada, inteligência artificial de ponta, sandbox em nuvem e análise comportamental aprofundada para prevenir ataques direcionados, além de ameaças novas ou desconhecidas, incluindo *ransomware*.

Isso é ESET

Defesa proativa. Nosso negócio é minimizar a superfície de ataque.

Fique um passo à frente das ameaças cibernéticas conhecidas e emergentes com nossa abordagem de **prevenção em primeiro lugar**, impulsionada por **inteligência artificial** e **expertise humana**.

Experimente uma proteção de alto nível, sustentada por nossa **inteligência global de ameaças cibernéticas** desenvolvida internamente, compilada e analisada ao longo de mais de 30 anos, que impulsiona nossa ampla rede de pesquisa e desenvolvimento, liderada por **pesquisadores reconhecidos pelo setor**. A ESET protege o seu negócio para que ele possa desbloquear todo o potencial da tecnologia.

EXPLORAR

Proteção em múltiplas camadas, com foco em prevenção

Inteligência artificial de ponta aliada à expertise humana

Inteligência de ameaças reconhecida mundialmente

Suporte hiperlocal e personalizadol

eset
Cybersecurity
Progress. Protected.