Ambiente rico em destinos: por que o Microsoft 365 se tornou o maior risc

Data: 2025-09-18 17:23:24

Autor: Inteligência Against Invaders

O Microsoft 365 se tornou o sistema nervoso central dos negócios modernos – e os cibercriminosos sabem disso. Assim como o Windows se tornou o principal alvo dos invasores por causa de seu domínio de mercado nas décadas de 1990 e 2000,

O Microsoft 365 agora se encontra na mira por ter “vencido” a guerra de e-mail e colaboração.

Com mais de 400 milhões de licenças pagas do Office 365 em todo o mundo e inúmeras organizações que contam com seu conjunto integrado de aplicativos, o Microsoft 365 representa o melhor ambiente rico em alvos para agentes de ameaças.

A maldição do vencedor: o sucesso gera risco

O paralelo entre A jornada de segurança do Windows e a situação atual do Microsoft 365 é impressionante. O Windows se tornou o principal alvo de ataques em todo o mercado de sistemas operacionais, não porque era inerentemente menos seguro do que as alternativas, mas porque atacar o Windows significava acessar o maior grupo possível de vítimas em potencial.

Hoje, o Microsoft 365 enfrenta a mesma maldição do vencedor. Tendo consolidado com sucesso e-mail, compartilhamento de arquivos, colaboração e comunicação em um único ecossistema, O Microsoft 365 pintou um alvo enorme nas costas.

Esse domínio cria um efeito de multiplicação para os atacantes. Uma única campanha bem-sucedida direcionada ao Microsoft 365 pode impactar milhões de usuários em milhares de organizações. Para os cibercriminosos que operam em uma análise de custo-benefício, a matemática é simples:

Por que desenvolver vetores de ataque separados para várias plataformas quando você pode concentrar seus esforços na plataforma que atinge mais alvos?

Vetores de ameaças multisuperfície

O Microsoft 365 apresenta uma complexa rede de serviços interconectados que expandem drasticamente a superfície de ataque. Cada aplicativo — Outlook, SharePoint, Teams e OneDrive — representa um ponto de entrada em potencial, e sua forte integração significa que comprometer um serviço fornece caminhos para outros.

Isso cria “oportunidades de movimento lateral”. Um invasor que obtém acesso por meio de phishing no Outlook pode girar para exfiltrar dados do SharePoint, manipular documentos do OneDrive ou ingressar em reuniões confidenciais do Teams.

A experiência perfeita que atrai as empresas torna-se um cenário de sonho para os invasores que buscam maximizar o impacto.

Vulnerabilidades recentes do SharePoint destacam esse perigo. Em julho de 2025, Microsoft corrigiu vulnerabilidades de dia zero incluindo CVE-2025-53770, que foi explorado ativamente contra clientes locais do SharePoint desde 7 de julho, afetando mais de 75 servidores.

Esses ataques demonstram risco em cascata, em que o comprometimento do SharePoint fornece acesso a toda a infraestrutura colaborativa.

Escondido à vista de todos: o ponto cego de backup

Um dos riscos mais negligenciados nos ambientes do Microsoft 365 está nos sistemas de backup e recuperação. Muitas organizações assumem que as políticas de retenção internas e o histórico de versões da Microsoft fornecem proteção adequada, mas isso cria pontos cegos perigosos.

Os backups padrão do Microsoft 365 geralmente não têm as opções de recuperação granular necessárias para responder a ataques sofisticados e, pior, podem realmente armazenar e preservar conteúdo malicioso que se torna um vetor de ataque futuro.

Ao verificar URLs em backups de e-mail do Microsoft 365, os analistas descobriram que 40% continham links de phishing que foram devidamente preservados ao lado de comunicações comerciais legítimas.

Ainda mais alarmante, mais de 200.000 e-mails de backup continham anexos de malware. Essas descobertas expõem uma falha crítica nas abordagens tradicionais de backup: as organizações não estão apenas armazenando seus dados – elas estão criando arquivos permanentes das próprias ameaças projetadas para destruí-los.

Isso significa que a restauração do backup após um incidente de segurança pode reintroduzir os vetores de ataque originais de volta ao ambiente. Quando os agentes de ransomware criptografam bibliotecas do SharePoint ou corrompem caixas de correio do Exchange, ter backups robustos e isolados torna-se a diferença entre uma recuperação rápida e uma catástrofe que encerra os negócios.

No entanto, muitos MSPs e equipes de TI descobrem tarde demais que suas estratégias de backup têm lacunas críticas ao enfrentar ameaças modernas que visam especificamente plataformas de colaboração em nuvem.

Endurecimento sem dificultar

Os MSPs e as equipes de TI devem implementar controles de segurança robustos sem prejudicar os benefícios de produtividade do Microsoft 365. Isso requer defesas em camadas além dos recursos de segurança nativos.

A arquitetura Zero Trust torna-se essenciall, com verificação contínua das identidades do usuário e da integridade do dispositivo. A autenticação multifator não deve ser negociável, mas implementada para evitar o atrito do usuário que gera soluções alternativas.

A proteção avançada contra ameaças deve se estender a todos os aplicativos do Microsoft 365, desde a digitalização de documentos do SharePoint até o monitoramento do Teams e a análise de comportamento do OneDrive. As equipes de segurança precisam de visibilidade entre aplicativos para detectar padrões de acesso anômalos.

As avaliações regulares devem se concentrar nas configurações do Microsoft 365, incluindo permissões do Power Platform, integrações de terceiros e controles de acesso de convidados. A complexidade do ecossistema significa que configurações incorretas podem criar lacunas de segurança persistentes.

O caminho a seguir

O domínio do Microsoft 365 o torna um alvo inevitável. As organizações devem reconhecer que protegê-lo requer conhecimento especializado e ferramentas adaptadas às ameaças de colaboração na nuvem.

O objetivo não é abandonar o Microsoft 365 – seus benefícios são muito significativos. Em vez disso, as organizações devem reconhecer riscos elevados e implementar medidas proporcionais, tratando a segurança do Microsoft 365 como uma disciplina especializada, não um item de caixa de seleção.

As organizações que fortalecem proativamente as defesas mantêm uma vantagem competitiva enquanto protegem ativos confidenciais. Aqueles que não aprendem da maneira mais difícil por que ser o maior alvo traz os maiores riscos.

Sobre a TRU

O Unidade de Pesquisa de Ameaças da Acronis (TRU) é uma equipe de especialistas em segurança cibernética especializada em inteligência de ameaças, IA e gerenciamento de riscos.

A equipe da TRU pesquisa ameaças emergentes, fornece insights de segurança e oferece suporte às equipes de TI com diretrizes, resposta a incidentes e workshops educacionais.

Veja as últimas pesquisas da TRU.

Patrocinado e escrito por Acronis*.*