Whitepaper

mimecast

10 maneiras de prevenir ataques de ransomware

Os ataques de ransomware têm sido uma realidade para organizações de todos os tamanhos há algum tempo. Nos últimos meses, no entanto, o volume e a sofisticação dos ataques, bem como as consequências, têm vindo a aumentar.

As empresas vítimas encontram-se numa situação impossível. Ninguém quer pagar – prevenir completamente o ransomware é o objetivo – mas muitos sentem que não têm escolha. Pior ainda, não há garantias. Em uma pesquisa recente do Mimecast, 61% dos entrevistados em uma pesquisa anual State of Email Security 2021 disseram ter sofrido um ataque de ransomware nos últimos 12 meses. Desses entrevistados, 52% pagaram o ransomware, mas mais de um terço nunca recuperou seus dados.

Então, como você mantém sua organização segura? Trata-se de mais do que apenas segurança. Vamos dar uma olhada em dez estratégias que podem reduzir riscos, criar resiliência e ajudar a obter agressores fora do banco do motorista.

01.

Proteja seu perímetro de e-mail

Como as equipes de TI e segurança sabem muito bem, o e-mail ainda é o principal vetor de ataque. A melhor maneira de evitar que os funcionários caiam em ataques é bloquear o maior número possível de e-mails maliciosos o mais próximo possível da fonte. Usar um gateway de e-mail seguro maduro e baseado em nuvem com varredura avançada de entrada e saída continua sendo a maneira mais eficaz de fazer isso. Para os usuários do Microsoft 365, uma abordagem de segurança de e-mail em camadas também é essencial para reduzir o risco, à medida que os invasores buscam cada vez mais colher os benefícios de explorar a plataforma de produtividade empresarial mais adotada do mundo.

02.

Arquivar em um ambiente independente e protegido separadamente

A capacidade de proteger e preservar dados corporativos pode fornecer um maior grau de controle no pior cenário de um ataque de ransomware bem-sucedido, enquanto seguir as melhores práticas de manter uma quantidade enxuta de dados pode reduzir sua exposição e superfície de ataque.

O arquivamento em um ambiente seguro de forma independente permite que você atinja esses dois objetivos.

03.

Construa resiliência com capacidades de recuperação integradas

A capacidade de restaurar rapidamente e com facilidade as contas de e-mail para um ponto no tempo pode manter sua organização em funcionamento e mitigar os danos de um ataque de ransomware. Isso também pode evitar que suas equipes de TI e segurança dediquem semanas ou meses aos esforços de recuperação. Essa capacidade é particularmente crítica para os usuários do M365, que frequentemente descobrem tarde demais as lacunas de recuperação de dados na plataforma.

04.

Estabelecer um plano de continuidade de e-mail

A interrupção do fluxo de e-mails é uma realidade que todas as organizações devem enfrentar e planejar, e pode ocorrer por diversos motivos. O ransomware é, sem dúvida, um deles. A necessidade de aplicar patches urgentes, remediar um incidente ou até reconstruir completamente usando uma infraestrutura limpa são outros. Como o e-mail ainda é a espinha dorsal da grande maioria dos negócios, a capacidade de mantê-lo funcional durante eventos disruptivos é fundamental para uma estratégia de resiliência cibernética. Uma solução de continuidade pode garantir que, quando o e-mail ficar fora do ar, seu negócio não caia junto.

05.

Limitar a capacidade dos invasores de criar ataques altamente direcionados

Ataques altamente direcionados que imitam uma marca ou usam informações pessoais são difíceis de detectar até mesmo para os usuários mais sofisticados; e quando se trata de alvos lucrativos, os invasores estão dispostos a investir tempo para criá-los.Táticas mais recentes, como o uso de rastreadores de e-mail incorporados, podem revelar a localização física de um alvo, sistema operacional, nível de envolvimento com o e-mail malicioso e muito mais. Combine essas informações com a capacidade de enviar e-mails falsos de domínios de e-mail confiáveis ou imitar facilmente uma presença digital e você terá uma séria ameaça em suas mãos. Protocolos e tecnologias, como DMARC e gráficos de identidade, que complementam os recursos de segurança de e-mail podem proteger os usuários desses ataques direcionados e fornecer camadas adicionais de proteção para você, seus clientes e seus parceiros.

06.

Empregar novas tecnologias para melhorar a detecção de ataques sofisticados

A IA, e especialmente o aprendizado de máquina, estão desempenhando um papel cada vez maior nas tecnologias de segurança cibernética e podem ser um meio altamente eficaz de reforçar os recursos das soluções que as utilizam.

A aplicação mais comum até o momento é o reconhecimento de padrões e a capacidade de desenvolver esse "conhecimento" ao longo do tempo, permitindo que as taxas de detecção melhorem. Não há dúvida de que os casos de uso crescerão, mas também é essencial reconhecer a IA pelo que ela é — um complemento para uma forte estratégia de resiliência cibernética, em vez de uma bala de prata. Tecnologias que a incorporam de forma integrada, com um plano de longo prazo de como o uso da IA evoluirá, podem tornar sua estratégia de segurança mais eficaz hoje e ajudá-la a resistir ao teste do tempo a longo prazo.

07.

Cercar os usuários finais com suporte

Quando as ameaças surgem, as equipes de segurança não têm escolha a não ser confiar na forma mais imprevisível de proteção de todas: seres humanos. Há pouca discussão sobre se dar a eles o conhecimento e as ferramentas para tomar melhores decisões deve ser uma parte fundamental da estratégia de segurança de qualquer organização. Os benefícios de um programa de treinamento de conscientização sobre segurança cibernética são muitos, mas eles são mais efetivamente implantados como parte de uma estratégia geral. Soluções que incorporam recursos detalhados de rastreamento e pontuação de risco podem ajudar as equipes de segurança a identificar os funcionários com maior risco, enquanto os relatórios de sistemas de segurança de e-mail também podem revelar aqueles que estão sendo alvos com mais frequência. Fatores como esses podem ser usados para fornecer suporte adicional quando necessário.

IAlém disso, ferramentas como banners de aviso e alertas personalizáveis — quando aplicadas de forma seletiva e dinâmica — podem ajudar muito os funcionários a tomar melhores decisões. A contribuição dos funcionários também pode alimentar seu quadro de ameaças maior para melhorar ainda mais as taxas de detecção. Saiba mais.

08.

Manter boas práticas de atualização

Nem é preciso dizer — mas ainda vale a pena repetir — que uma boa higiene de patches é essencial para reduzir o risco de todos os tipos de ataques cibernéticos.

Manter um inventário de seus ativos, monitorar patches e estabelecer processos claros depriorização são todos passos fundamentais. Ter um backup de dados separadamente protegido também é uma proteção importante.

09.

Proteger contra infecções por downloads automáticos

Downloads de arquivos maliciosos podem abrir a porta para ataques de ransomware que são difíceis de detectar. A tecnologia conhecida como isolamento do navegador pode reduzir esse risco executando arquivos remotamente — em um contêiner ou na nuvem — para manter infecções por malware longe dos computadores, dispositivos e redes dos usuários. Também pode ajudar a eliminar o problema do paciente zero.

10.

Monitorar e controlar a TI oculta

O novo local de trabalho digital confundiu as linhas entre profissional e pessoal e reduziu a capacidade das equipes de TI e segurança de manter o controle. Sites inseguros, Wi-Fi mal protegido e serviços de compartilhamento de arquivos não seguros aumentam o risco. Os recursos de visibilidade e controle de aplicativos podem ajudar. Projetados para ajudar as equipes de TI e segurança a lidar com o problema de "TI sombra", eles revelam quais aplicativos estão sendo usados, por quem e com que frequência. As equipes podem então bloquear ou monitorar o uso conforme necessário.

Além dessas dez etapas principais, nenhuma discussão sobre ransomware estaria completa sem uma menção ao seguro cibernético. O debate continua acirrado, com autoridades governamentais começando a opinar, e não há uma resposta clara. Cada organização deve tomar suas próprias decisões baseadas em risco; mas, segurada ou não, a melhor estratégia é aquela que torna o risco de precisar pagar um resgate o mais baixo possível.

A missão da Mimecast é prevenir que eventos negativos afetem boas organizações.

Para obter mais informações sobre como podemos ajudar a defender contra ransomware e outros ataques sofisticados, solicite uma demonstração personalizada ou visite Mimecast.com.