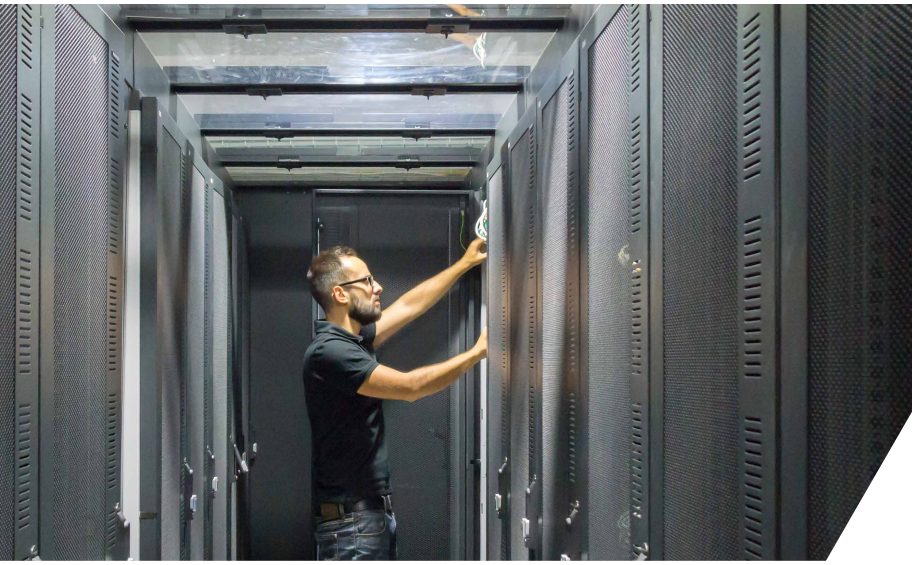
SEGURANÇA CIBERNÉTICA ESSENCIAL PARA EMPRESAS DE PEQUENO E MÉDIO PORTE



VISÃO GERAL

Muitos relatórios da indústria indicam que as empresas pequenas e médias (PMEs) estão particularmente sujeitas a riscos associados a atacantes cibernéticos sofisticados. De fato, 77% de todos os crimes cibernéticos visam PMEs. No entanto, restrições financeiras dificultam a obtenção dos recursos de que as PMEs necessitam para se protegerem contra ameaças avançadas.

Estabelecer uma linha de base essencial para a segurança exige uma estratégia de detecção e prevenção para proteger contra ameaças avançadas, com um plano de prontidão de resposta para incidentes não previstos. As tecnologias premiadas da FireEye ajudam a detectar e a deter ataques de múltiplos estágios e vetores. Elas municiam as equipes de segurança com insights precisos e contextuais para execução imediata de um plano de resposta próprio ou por intermédio de um parceiro. Os serviços da FireEye e de seus parceiros também complementam essas tecnologias proativas para ajudar as organizações na resposta a incidentes.

Essas soluções eficazes são desenvolvidas para serem de fácil acesso e uso por parte das PMEs, possibilitando que estas se concentrem na expansão de seus negócios.

O DESAFIO

Governos e grandes corporações, há muito cientes das ameaças avançadas, vêm implementando gradualmente estruturas de segurança e adotando tecnologias para reduzir o risco e o impacto de uma violação de dados. Essas organizações costumam ter orçamentos de segurança flexíveis ou possuem exigências jurídicas ou regulatórias para justificar o custo da segurança. O desafio das PMEs é que elas não dispõem das vantagens das grandes corporações, mas enfrentam riscos semelhantes.

Embora as notícias tendam a se concentrar em grandes violações, as PMEs costumam ser os principais alvos do cibercrime.[1] Por quê? Porque as PMEs possuem mais ativos (como números de cartões de crédito, informações de identidade, informações médicas e propriedade intelectual) do que indivíduos, mas menos segurança do que grandes corporações — o que as torna alvos ideais para os atacantes.

Muitas PMEs também são visadas por fornecerem terceirização de processos de negócios (BPO) ou serviços viabilizados por tecnologia da informação (ITES) para organizações maiores. Os atacantes exploram essa confiança, infiltram-se no elo mais fraco da corrente e, em seguida, movem-se lateralmente até um alvo mais significativo. Os atacantes tendem a seguir o caminho mais fácil para atingir seus objetivos.

As grandes corporações estão depurando cada vez mais sua cadeia de fornecimento para identificar fornecedores que possam demonstrar um alto grau de devida diligência em segurança cibernética. As PMEs precisarão implementar capacidades mais avançadas de prevenção e detecção para cumprir esses requisitos e ampliar seus negócios.

Ransomware e e-mails de spearphishing são riscos crescentes para as PMEs devido a uma segurança inadequada. As PMEs podem até não se considerar alvos, mas uma segurança deficiente as torna alvos fáceis para a abordagem rápida e inesperada do ransomware.

Tecnologias de segurança ultrapassadas, com base em assinaturas, são ineficazes contra essas ameaças porque estas frequentemente são polimórficas e intencionalmente desenvolvidas para evitar a exibição de qualquer assinatura prévia. Enfim, as PMEs precisam lidar com essas ameaças avançadas e com os riscos do ransomware. Estima-se que metade das pequenas empresas que sofrem um ataque cibernético encerram atividades no prazo de até seis meses.[2]

1 Symantec. "2015 Internet Security Threat Report". Abril de 2015
2 https://staysafeonline.org/

FireEye

A SOLUÇÃO

Defender-se contra os atacantes sofisticados de hoje requer uma solução de segurança que previna e detecte ameaças avançadas:

- Estando ciente dos principais vetores de ameaças e das atividades maliciosas nesses vetores.
- Detectando novas ameaças, inclusive ataques nunca antes vistos (zero-day) e ameaças comoditizadas e bem conhecidas.
- Identificando ataques avançados de múltiplos estágios e em múltiplos vetores.
- Utilizando inteligência de ponta para reconhecer rapidamente ameaças graves e perpetradores de ameaças.

O FireEye Essential Security combina o FireEye Network Security (NX) Essentials e o FireEye Email Threat Prevention Cloud (ETP) para proteger as organizações contra ameaças via e-mail e Web. Esses dois vetores de ameaças respondem por 90% dos ataques cibernéticos. A solução Essential Security ajuda a otimizar o seu orçamento de segurança ao identificar somente problemas críticos de segurança, sem a distração de falsos positivos que sobrecarregam e retardam a resposta a incidentes.

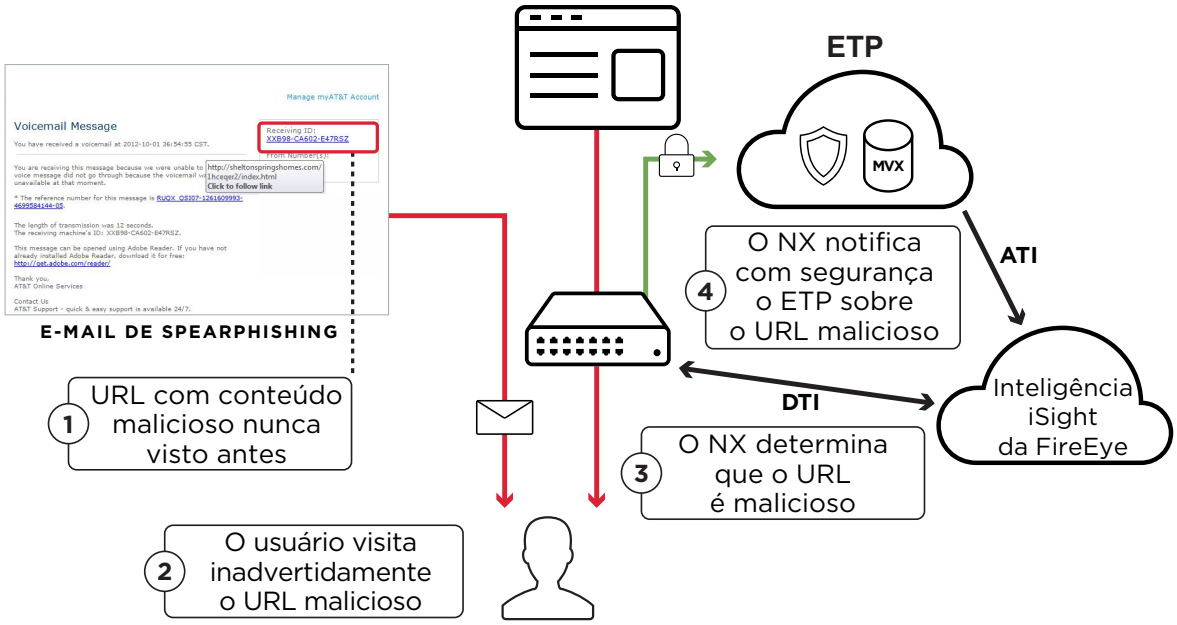
O poderoso mecanismo FireEye Multi-Vector Virtual Execution™ (MVX) está no centro das tecnologias da FireEye. Ele ajuda a identificar ataques avançados de múltiplos estágios e ameaças mistas que se estendem por várias superfícies de ataque, incluindo Web e e-mail, que podem não parecer maliciosas quando examinadas separadamente.

A correlação de URLs maliciosos com e-mails de spearphishing é fundamental para identificar a saraivada inicial de muitos ataques multivetoriais, conforme mostrado na figura 1. Enxergar essa conexão possibilita às organizações ver como os dois eventos estão relacionados e bloquear automaticamente estágios subsequentes do ataque, como tentativas, por parte dos atacantes, de transferir dados roubados pela Web. Assim também são identificados e bloqueados ataques subsequentes que utilizem táticas, ferramentas e procedimentos (TTPs) semelhantes.

A solução Essential Security ajuda as organizações a responder mais rapidamente às ameaças com uma inteligência contextual e decisiva. Ela também permite que as PMEs estiquem seus limitados orçamentos de segurança e reduzam a sobrecarga operacional, consolidando a distribuição de tecnologia, bloqueando automaticamente ataques críticos e gerando alertas de alta qualidade para minimizar o trabalho em vão.

Com um alto grau de automação, eficiência e eficácia, essa solução possibilita às organizações simplificar a distribuição e o gerenciamento cotidiano da segurança, tanto de rede quanto de e-mail, e melhorar sua postura de segurança.

FIGURA 1 — CORRELAÇÃO MULTIVETORIAL DO NETWORK SECURITY ESSENTIALS E DO EMAIL THREAT PREVENTION



TECNOLOGIA DE DETECÇÃO E PREVENÇÃO

Network Security Essentials

O FireEye Network Security Essentials é uma solução de segurança de rede econômica, pronta para usar e que pode ser distribuída em menos de 60 minutos. Ele minimiza o risco de violações onerosas ao detectar e deter ataques cibernéticos com base em rede, tanto conhecidos quanto desconhecidos. Ele utiliza o mecanismo MVX para analisar o tráfego da Web e detectar exploits, executáveis de malware e callbacks em múltiplos protocolos. Ele também inclui um sistema de prevenção de intrusões (IPS) com correspondência de assinatura convencional para detectar ataques comuns e proporcionar proteção contra riskware, bloqueando spyware e adware. Diferentemente de soluções antivírus (AV), de IPS isolado ou de firewall convencional ou de próxima geração, o Network Security Essentials detecta com alta precisão tanto os ataques conhecidos quanto os desconhecidos, de zero-day, gerando baixas taxas de falsos positivos.

Segurança de e-mail: Email Threat Protection Cloud (ETP)

O e-mail custuma receber a saraivada inicial das grandes violações. O FireEye ETP é uma oferta de software como serviço (SaaS) que analisa o e-mail quanto a indícios de spearphishing, bem como vírus comoditizados ou ameaças de spam.

Para simplificar a distribuição em uma oferta com base na nuvem, o ETP utiliza a tecnologia patenteada MVX para prevenir proativamente os ataques avançados via e-mail. Ele também oferece proteção antispam e antivírus internamente. O ETP pode proteger caixas de correio tanto na nuvem quanto no local.

Inteligência sobre ameaças

A inteligência sobre ameaças baseada na nuvem da FireEye aproveita o acesso que temos a dados de inteligência de sensores distribuídos globalmente e os alertas correspondentes da solução FireEye. Essa inteligência, atualizada a cada 60 minutos, inclui informações sobre novos perfis de malware, exploits de vulnerabilidades e descobertas de ameaças. Ela complementa o mecanismo MVX com análises com base na nuvem e tecnologias de autoaprendizagem para detectar ameaças avançadas.

O FireEye Dynamic Threat Intelligence (DTI) oferece atualizações hora a hora de dados intercambiados anonimamente sobre ameaças com base na Web, e-mail e arquivos pela rede global da FireEye na nuvem. Essas atualizações garantem que os ataques mais recentes vistos pela FireEye em sua rede global de clientes sejam encontrados e bloqueados. O DTI é disponibilizado com o Network Security Essentials.

O FireEye Advanced Threat Intelligence (ATI) oferece uma rica inteligência sobre adversários e vítimas, coletada por analistas de inteligência sobre ameaças e profissionais de resposta a incidentes. Como resultado, os alertas de ataque da FireEye podem incluir informações contextuais valiosas, como a identidade do possível perpetrador da ameaça, motivos prováveis e detalhes do malware. Isso torna a solução mais eficiente na detecção de malware conhecido e de ataques de zero-day altamente direcionados, além de ajudar os profissionais de segurança a se manter um passo à frente dos perpetradores de ameaças e a detê-los. O ATI é padrão com o ETP.

Opções de distribuição

A solução Essential Security pode ser distribuída internamente para maior controle e resposta em tempo real, interrompendo ataques em andamento conforme mostrado na figura 2.

FIGURA 2A. NETWORK SECURITY ESSENTIALS - DISTRIBUIÇÃO INTERNA

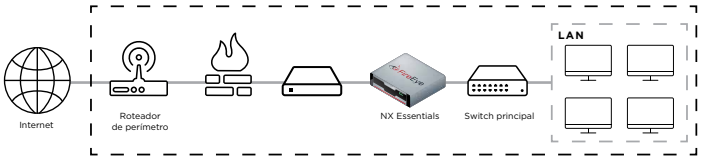
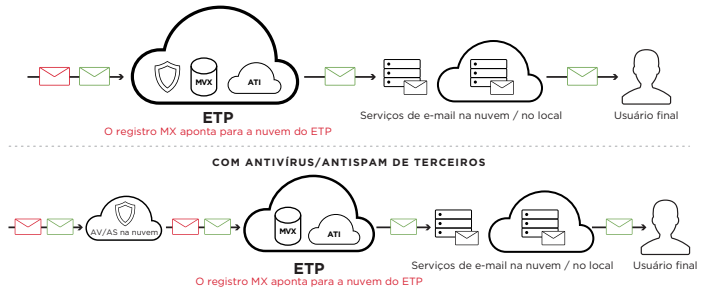


FIGURA 2B. EMAIL THREAT PREVENTION - DISTRIBUIÇÃO INTERNA



Algumas organizações preferem começar com uma abordagem mais conservadora, portanto, ela também pode ser distribuída nos modos fora de banda ou de apenas monitoramento (modo BCC no ETP), conforme mostrado na figura 3. Nessa distribuição, todo o tráfego é monitorado quanto a atividades maliciosas e um relatório é gerado, mas não há mecanismo de prevenção automatizado. A FireEye ou nossos parceiros podem ajudá-lo a determinar e a distribuir a opção mais adequada às suas necessidades.

FIGURA 3A. NETWORK SECURITY ESSENTIALS - DISTRIBUIÇÃO FORA DE BANDA (SPAN/TAP)

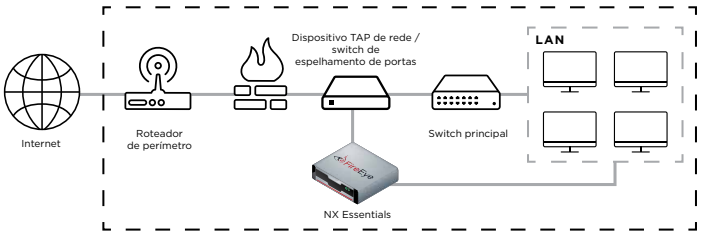
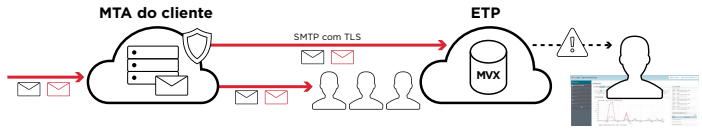


FIGURA 3B. EMAIL THREAT PREVENTION - MODO BCC



PREPARAÇÃO PARA VIOLAÇÕES

Lembre-se de que detecção e prevenção resolvem somente metade do problema. É igualmente crítico analisar e responder aos impactos técnico, jurídico, financeiro e de relações públicas de um incidente imprevisto. A FireEye recomenda enfaticamente o estabelecimento de um plano de resposta, de preferência com um parceiro de segurança. A FireEye e seus parceiros oferecem serviços para desenvolvimento do plano de resposta, validação do plano de resposta e investigação de incidentes.

PRÓXIMOS PASSOS

As PMEs são o alvo preferencial dos atacantes avançados porque frequentemente têm medidas de segurança deficientes, em grande parte devido a recursos limitados e à menor conscientização quanto às ameaças. Para manter o foco no crescimento dos seus negócios e para minimizar o risco, recomenda-se um nível essencial de segurança. Isso inclui processos e tecnologias de segurança desenvolvidos para defesa e resposta contra os atacantes cibernéticos sofisticados de hoje. Em última instância, isso lhe proporciona mais confiança no estado da sua segurança.

Para saber mais sobre as soluções de segurança da FireEye desenvolvidas para detectar e prevenir ataques avançados, bem como preparar um plano de resposta adequado no caso de um comprometimento, visite www.FireEye.com ou entre em contato com o representante de vendas local.

SOBRE A FIREEYE

A FireEye protege os ativos mais valiosos do mundo contra os atacantes cibernéticos atuais. Nossa combinação de tecnologia, inteligência e conhecimento ajuda a eliminar o impacto das violações. A comunidade global de defesa da FireEye conta com 4.400 clientes espalhados por 67 países, entre os quais mais de 250 despontam na lista Fortune 500.

Para mais informações sobre a FireEye, visite:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye