SEGURANÇA DE NÍVEL CORPORATIVO AO ALCANCE DE PEQUENAS E MÉDIAS EMPRESAS

VISÃO GERAL

A maioria das organizações depende de protocolos de e-mail e Web para realizar seus negócios. Por isso mesmo a maioria dos ataques cibernéticos começa com esses protocolos. Uma proteção efetiva detecta e previne ataques padronizados conhecidos, bem como ataques avançados e desconhecidos. As tecnologias premiadas da FireEye ajudam a detectar e a deter ataques avançados de múltiplos estágios e múltiplos vetores, com precisão. Elas conferem às equipes de segurança ferramentas eficazes que viabilizam a eficiência operacional ao emitir bem menos alertas falsos positivos. Essas soluções valiosas são desenvolvidas para serem de fácil acesso e uso, além de permitir que as organizações se concentrem na expansão de seus negócios.

A FireEye é pioneira nessa tecnologia para detecção de ataques avançados desconhecidos, mas inicialmente a distribuiu apenas em grandes corporações. No entanto, os atacantes cibernéticos visam organizações de qualquer porte. As pequenas e médias empresas (PMEs) reconhecem que não estão imunes e que uma proteção contra ameaças avançadas é fundamental para sua estrutura de trabalho de segurança.

DESAFIOS DA SEGURANÇA

As pequenas e médias empresas enfrentam muitos desafios de segurança, parcialmente devido à natureza dinâmica do cenário de ameaças cibernéticas e também devido à maneira como as PMEs tentam operacionalizar o gerenciamento de segurança dentro de suas organizações.

Os desafios relacionados ao cenário de ameaças geralmente decorrem de uma falta de visibilidade sobre toda a organização. As tecnologias tradicionais de detecção e prevenção em perímetro, dependentes de assinaturas de ataque, têm dificuldades para identificar as ameaças de hoje. Os atacantes usam técnicas para alterar a assinatura característica do malware para que a mesma apareça apenas uma vez em cada organização. Em muitos casos, o malware nem ao menos tem relação com os ataques.

Os desafios relacionados às operações de segurança estão centrados no fato de que as PMEs frequentemente recebem alertas demais, os quais exigem providências por parte de recursos humanos escassos. Muitos alertas são falsos positivos e o tempo dos analistas é desperdiçado com a investigação de problemas não relacionados à segurança. O excesso de falsos positivos também pode ocultar os verdadeiros positivos que exigem interação imediata para que sejam evitados impactos adicionais.

Existem ainda outras complicações. Para investigar alertas, as PMEs precisam contratar pessoal com qualificação adequada em segurança. Na maioria das organizações, o recurso de segurança é parte do departamento de TI, o que gera conflitos de interesses. As PMEs que aplicam uma abordagem de defesa profunda em camadas podem se ver diante de várias ferramentas de tecnologia de segurança frequentemente mal gerenciadas, gerenciadas por provedores de serviços de segurança ou simplesmente não gerenciadas. Na melhor das hipóteses, isso pode resultar em custo excessivo; na pior, pode constituir uma exposição significativa a riscos. Esses desafios estão todos conectados: as PMEs precisam controlar os custos enquanto utilizam poucos recursos humanos para gerenciar muitas ferramentas de segurança que geram alertas demais.

FireEye

A SOLUÇÃO

A solução da FireEye combina o Network Security Essentials (NXE) com o Email Threat Prevention Cloud (ETP) para proteger as organizações contra ameaças baseadas em Web e e-mail.[1] Esses dois vetores representam 90% dos ataques cibernéticos. A solução ajuda a otimizar o seu orçamento de segurança ao identificar problemas críticos de segurança sem a distração de falsos positivos que sobrecarregam e retardam desnecessariamente a resposta a incidentes.

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

A correlação de URLs maliciosos com e-mails de spearphishing é fundamental para a identificação da saraivada inicial de muitos ataques multivetoriais. O mecanismo Cloud MVX proporciona visibilidade sobre esses vínculos, possibilitando às organizações ver como os dois eventos estão relacionados e bloquear automaticamente estágios subsequentes dos ataques, como tentativas, por parte dos atacantes, de transferir dados roubados pela Web. Assim também são identificados e bloqueados ataques subsequentes que aproveitem táticas, ferramentas e procedimentos (TTPs) semelhantes.

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

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 para minimizar o risco de violações onerosas.

Além do mecanismo Cloud MVX patenteado e sem assinaturas, o Network Security Essentials inclui a tecnologia Intelligence-Driven Analysis (IDA) que identifica e bloqueia ameaças conhecidas e desconhecidas. A tecnologia IDA é uma coletânea de mecanismos contextuais e baseados em regras que detectam e bloqueiam atividades maliciosas com base na inteligência mais recente obtida de máquinas, atacantes e vítimas. Um sistema de prevenção de intrusões (IPS) detecta ataques comuns com correspondência de assinatura convencional e proporciona proteção contra riskware para bloquear spyware e adware. Diferentemente de software 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 (zero-day), gerando baixas taxas de falsos positivos e liberando as equipes de segurança para que se concentrem nos alertas que importam.

Opções de distribuição versáteis

O Network Security Essentials requer um appliance virtual ou físico no local que possa ser distribuído no modo em linha ou somente monitoramento. O appliance no local, chamado de nó de rede inteligente, pode ser distribuído em vários locais, do perímetro de rede primário a escritórios remotos e filiais — ou seja, qualquer lugar que tenha acesso direto à Internet. A imagem de máquina virtual transferível por download (figura 1) é preferida por ser econômica e de rápida distribuição. Os nós de rede inteligentes utilizam a tecnologia Intelligence-Driven Analysis (IDA) e detecção de IPS com base em assinaturas para identificação e proteção contra atividades suspeitas. Eles usam uma conexão criptografada para enviar objetos suspeitos, que exigem análises adicionais, para o serviço Cloud MVX, na nuvem privada da FireEye. O nó de rede inteligente e o serviço Cloud MVX também estão disponíveis como um appliance de hardware integrado (figura 2). A FireEye recomenda a opção de 50 Mbps para empresas pequenas e a de 100 Mbps para empresas médias.

Segurança de e-mail: Email Threat Protection Cloud

O e-mail é frequentemente utilizado para iniciar grandes violações. O ETP é uma oferta de software como serviço (SaaS), com base na nuvem, que analisa o e-mail quanto a indícios de spearphishing, bem como vírus comoditizados ou ameaças de spam. O ETP utiliza a tecnologia patenteada Cloud MVX para prevenir proativamente ataques avançados via e-mail. Ele também oferece proteção antispam e antivírus em linha. O ETP pode proteger caixas de correio situadas no local ou baseadas na nuvem, com distribuição em linha ou somente monitoramento.

Inteligência sobre ameaças

A inteligência sobre ameaças com base na nuvem da FireEye acompanha os alertas da solução da FireEye. Essa inteligência, atualizada a cada 60 minutos, inclui informações sobre novos perfis de malware, informações de inteligência obtidas de adversários e vitimas, exploits de vulnerabilidades e descobertas de ameaças. Ela complementa o mecanismo Cloud MVX com análises com base na nuvem e tecnologias de autoaprendizagem para detectar ameaças avançadas. Consequentemente, os alertas da FireEye podem incluir informações contextuais críticas, como a possível identidade do perpetrador da ameaça, prováveis motivações e detalhes do malware, para ajudar os profissionais de segurança a detectar e a deter ataques de zero-day altamente direcionados e malware conhecido.

[1] Relatório de investigações sobre violações de dados da Verizon de 2015

EXEMPLOS DE CONFIGURAÇÃO

Fatores a serem levados em consideração ao montar uma solução: o número de caixas de e-mail a monitorar, o volume de tráfego de rede que passa pelo sistema, o ambiente virtualizado ou físico, a adoção de serviços oferecidos pela nuvem e o nível de conscientização quanto à segurança por parte dos líderes executivos seniores e da diretoria. A FireEye e seus parceiros podem ajudá-lo a escolher ou desenvolver uma solução que satisfaça as suas necessidades, nos moldes desses exemplos de configuração.

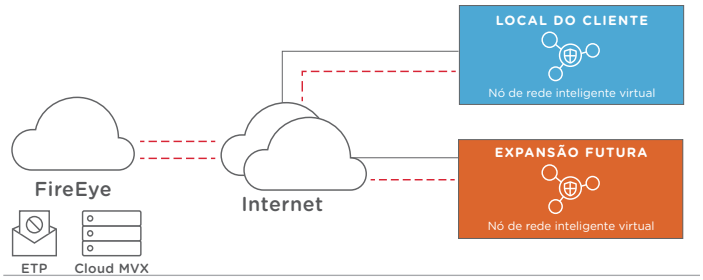

FIGURA 1 — ETP CLOUD E CLOUD MVX COM APPLIANCES VIRTUAIS

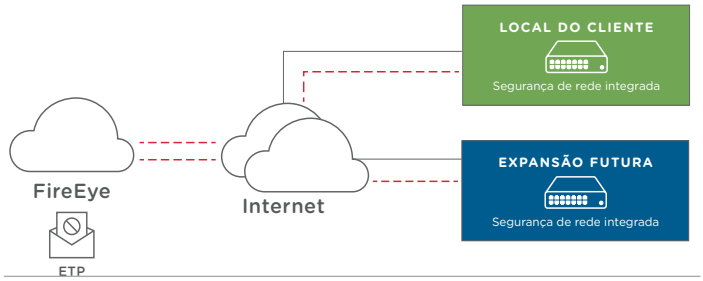

FIGURA 2 — ETP CLOUD E APPLIANCES FÍSICOS DE SEGURANÇA DE REDE INTEGRADA

	PEQUENA 1	PEQUENA 2	MÉDIA 1	MÉDIA 2
TIPO DE DISTRIBUIÇÃO	**VIRTUAL/NUVEM**	**APPLIANCE FÍSICO**	**VIRTUAL/NUVEM**	**APPLIANCE FÍSICO**
Número de funcionários	200 - 250	200 - 250	450 - 550	450 - 550
Tráfego de rede	50 Mbps	50 Mbps	100 Mbps	100 Mbps
Exemplo de solução proposto	ETP com 200 a 250 licenças Virtual NX1500 Cloud MVX	ETP com 200 a 250 licenças 2500NXE1 integrado	ETP com 450 a 550 licenças Virtual NX2500 Cloud MVX	ETP com 450 a 550 licenças 2500NXE2 integrado

PRÓXIMOS PASSOS

As PMEs são um alvo preferencial ou uma oportunidade para atacantes avançados porque frequentemente têm medidas de segurança deficientes, em grande parte devido a recursos limitados e pouca conscientização. Para ampliar os negócios e reduzir os riscos, é fundamental manter um nível básico de segurança. Isso exige confiança no estado da segurança, bem como no programa, nas ferramentas e nos processos de segurança.

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

SOBRE A FIREEYE, INC.

A FireEye® é líder em segurança como serviço (SaaS) orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência sobre ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. A empresa tem mais de 5.000 clientes em 67 países, dos quais mais de 940 constam na lista Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
+1 408.321.6300 / 877.FIREEYE (347.3393) / LATAM@FireEye.com

www.FireEye.com