http://www.cio.com.br

OPINIÃO

Já pensou em usar mídia social para a segurança da informação?

(http://cio.com.br/opiniao/2015/09/22/ja-pensou-em-usar-midia-social-para-a-seguranca-da-informacao)

Mav Turner *
Publicada em 22 de setembro de 2015 às 07h26

É... Princípios por trás das redes sociais podem ser usados para aumentar a segurança organizacional. Veja como

Como os invasores podem obter, com maior facilidade, informações privilegiadas sobre seu alvo?

Acredite ou não, no LinkedIn. Pense bem, por que fazer uma varredura às cegas tentando obter as digitais dos alvos quando basta consultar os perfis de seus administradores de rede e de sistema no LinkedIn para ver em quais sistemas estão trabalhando?

A mídia social é uma potente ferramenta para as empresas, mas, como você pode ver, também pode representar uma grande ameaça. Como resultado, muitas empresas estão aplicando políticas que exigem que os funcionários removam detalhes específicos sobre seus cargos. Ao mesmo tempo, contudo, os princípios por trás da mídia social podem, na verdade, ser usados para aumentar a segurança organizacional.

Tudo se resume à ideia de compartilhar informações, que representa o foco da mídia social. Compartilhando programaticamente informações sobre ameaças, os defensores podem criar uma defesa mútua muito mais forte do que fariam individualmente.

Reconheço que isso é mais fácil falar do que fazer. Quando a questão é segurança, nós, profissionais de TI, temos sido tradicionalmente cautelosos quanto a compartilhar informações, já que isso poderia representar uma vantagem para os invasores. Embora ainda seja importante considerar quais informações são compartilhadas, enquanto setor, devemos encarar o fato de que fazer tudo sozinho não é mais uma opção. Devemos avançar além do compartilhamento de definições básicas de vírus ou assinaturas de IDS.

Como?

Para variar, precisamos arrancar uma página do manual de estratégia dos invasores. A realidade é que os invasores estão muito à frente dos defensores há um bom tempo. Em geral, eles também são muito sociáveis e compartilham informações sobre vulnerabilidades e táticas de forma muito mais eficiente do que os defensores. Esqueça a imagem do lobo solitário criminoso cibernético – embora eles ainda existam por aí, a maioria dos invasores faz parte de uma comunidade secreta muito ativa que compartilha ferramentas e táticas mais rápido do que qualquer empresa consegue acompanhar. Por isso, precisamos mudar as regras do jogo: tornarmo-nos melhores em compartilhar mais informações de modo mais eficiente.

Recentemente, isso se manifestou na forma de feeds de ameaças. Feeds de ameaças são uma tecnologia bastante proclamada para compartilhar rapidamente informações sobre ataques e permitir que sua infraestrutura detecte e responda dinamicamente a novas ameaças. Alguns desses feeds podem ser simples listas de endereços IP ou blocos de rede associados a atividades mal-intencionadas, enquanto outros podem conter análises comportamentais mais complexas.

A ideia de compartilhar padrões ou assinaturas de ataques não é nova, mas nos últimos anos, testemunhamos uma integração mais profunda na infraestrutura de detecção e proteção. Feeds de ameaças não garantem a segurança – na verdade, é bom ser cético com relação a qualquer coisa que alegue garantir a segurança – mas representam um passo na direção certa, rumo à criação de arranjos de defesa coletivos. Ainda assim, a maior parte dos dados nos feeds de ameaça de hoje é enviada anonimamente e, portanto, não se trata de uma aliança identificada – mas é um começo.

Alguns fornecedores de tecnologia de proteção, como os que oferecem antivírus e firewalls, criaram seus próprios feeds e os oferecem aos clientes como serviços de assinatura premium. Ainda que sejam bons, esses feeds normalmente funcionam somente com a tecnologia de um fornecedor específico, além de estarem limitados com relação à profundidade com que podem ser aproveitados em toda a sua organização de TI. O problema é que, para serem mais eficazes, seria melhor incorporar esses dados em outros locais em sua infraestrutura. Às vezes, é relativamente fácil conseguir isso com os dados brutos desses feeds, mas nem sempre. Também existem fontes de feeds de ameaças agnósticas com relação ao fornecedor que valem a pena conferir. Por exemplo, algumas ferramentas de gerenciamento de informações e eventos de segurança (SIEM) incluem tais recursos.

Também é possível obter e compartilhar informações sobre ameaças de outras maneiras.

Por exemplo, o Internet Storm Center também é uma excelente fonte de informações sobre ataques ativos. Eles publicam informações sobre as principais portas mal-intencionadas que estão sendo usadas por invasores e os endereços IP dos invasores. Se você vir qualquer servidor em seu data center se comunicando com esses IPs ou por essas portas, vale a pena investigar. Embora possa revelar-se benigno, esses são bons sinalizadores para ajudar a orientar suas investigações.

Melhorar o compartilhamento de dados entre as equipes internas é outra maneira. Menos da metade dos profissionais de TI que responderam a uma recente pesquisa da SolarWinds disseram que suas organizações têm segurança e outros processos de TI altamente integrados, mas fazer isso pode ajudar a detectar ataques e comportamentos que, de outra forma, passariam despercebidos.

Uma boa maneira de começar é contar com ferramentas ou painéis unificados que contenham informações sobre o estado de suas redes e sistemas. Com frequência, dados de desempenho podem ser usados para detectar incidentes de segurança, seja um súbito aumento no tráfego de saída, indicando que alguém está exfiltrando dados, ou uma CPU em um servidor de banco de dados apresentando um pico devido a um ataque.

A melhor maneira de começar a trilhar esse caminho é incluir outros membros da TI nos relatórios pós-ação de respostas a incidentes. Quanto mais eles compreenderem sobre como as ameaças foram descobertas, mais vigilantes ficarão quanto à detecção de anomalias em seus sistemas e à sua respectiva sinalização.

(*) Mav Turner *é diretor de marketing de produtos de segurança da SolarWinds*