Relatório Lippis

Relatório técnico

Network Security 2.0

Uma abordagem de sistema para a redução das ameaças

Edição 1

por
Nicholas John Lippis III
Presidente, Lippis Consulting

Maio de 2008

Network Security 2.0: Uma abordagem de sistema para redução das ameaças

O procedimento convencional para combate às ameaças de TI é construir uma “defesa profunda” em camadas aplicando tecnologias de segurança como firewalls, IPS, controle de acesso à rede, software de cliente anti-x, agregação de alarme e correção de eventos, etc. E embora a abordagem de proteção em camadas seja uma estratégia útil para mitigação de ameaças, o cenário das ameaças mudou, forçando também uma mudança no procedimento convencional para uma abordagem de sistemas para proteger os ativos da empresa.

Network Security 2.0: Abordagem de sistemas ou segurança em camadas?

Ouvir o Podcast

Provedor de Conteúdo da Internet protege redes e serviços de clientes

Obter Relatório técnico:

A abordagem convencional em camadas baseava-se na instalação dos melhores produtos do mercado, que mantinham esse título apenas até o surgimento de novos produtos e depois eram relegados a uma posição de dispositivos autônomos e/ou silos de segurança mal integrados, como a conexão entre dispositivos de IPS e firewall. A abordagem de sistemas maximiza seus investimentos em segurança de TI integrando-os em uma Gestão de Sistemas que inclui política, reputação e identidades e que transcende a segurança de pontos terminais, redes, conteúdo e aplicativos. A abordagem de sistemas promete:

- Aplicar as políticas corporativas e proteger os ativos da empresa
- Reduzir a sobrecarga do departamento TI e de Operações de Segurança e o custo total de propriedade
- Diminuir os riscos à segurança de TI e a não-conformidade
- Proteger corporações da difusão de novas ameaças

Um Universo Complexo com um Novo Cenário de Ameaças

Importante Hospital Psiquiátrico Protege Dados de Saúde Importantes

Obter Relatório técnico:

Nós operamos em um mundo dos negócios complexo e permanentemente conectado. Novos aplicativos como comunicações unificadas, colaboração e conferências promovem níveis mais profundos de interação entre funcionários, parceiros, fornecedores e clientes. Funcionários móveis e em viagens conectam-se às redes de suas empresas de qualquer lugar do planeta. Os aplicativos da Web 2.0 permitem novas combinações de conteúdos diferentes que antes eram fornecidos separadamente, possibilitando formas inovadoras de comunicação e conexão. Todas essas tendências representam avanços fantásticos para a produtividade econômica, mas também geram novas ameaças e desafios à segurança.

Net Security 2.0: Quais são as novas ameaças?

O Network Security 1.0 infectou as ferramentas de comunicação e colaboração dominantes na época: email, mensagem instantânea, Web e infra-estrutura com malware, worms, vírus e outras explorações. Os hackers atacaram usando essas ferramentas de comunicação para provocar danos, e os líderes de TI reagiram criando uma proteção de perímetro com tecnologia de segurança de rede de firewall e IPS. Mas os hackers conseguiram ultrapassar essa proteção de perímetro atacando o comportamento dos funcionários ao usar os sistemas de mensagem instantânea, email, visitar websites ou usar outros aplicativos, que passaram a ser um excelente alvo para ataques de hackers através de spam, malware, etc. Em resumo, os hackers encontraram novas formas de atacar o comportamento e burlar as políticas e regras do firewall reduzindo o poder de defesa do perímetro. Então, surgiu o Network Security 2.0.

Os hackers já deixaram de ser um grupo inconseqüente em busca de emoção apenas para formar uma rede de criminosos cibernéticos que são a base do novo cenários de ameaças que chamamos de Network Security 2.0. Claramente, as explorações dos grupos do crime organizado on-line têm motivações financeiras. Os grupos criminosos on-line buscam formas de obter acesso a bancos de dados corporativos repletos de identidades, números de documentos e/ou cartões de crédito para vender ou explorar essas informações. Outros grupos de criminosos on-line tentam montar um escritório de serviços criando um imenso botnet para enviar spam ou participar de outras atividades ilegais.

Banco Comunitário Protege Dados e Simplifica Conformidade com Regulamentos
Obter Relatório técnico:

Da perspectiva das empresas, a principal preocupação com a segurança de TI é a perda e o roubo de dados, já que isso traz prejuízos à imagem da empresa e complica as relações comerciais com clientes, parceiros e fornecedores, sem mencionar as possíveis conseqüências regulatórias e jurídicas. Para os executivos, a perda e o roubo de dados é o pior dos cenários já que eles são obrigados a comunicar uma falha aos seus clientes e aos órgãos oficiais do governo através de meios de comunicação de massa, mesmo que simplesmente desconfiem que possa ter ocorrido uma perda de dados. Mesmo que os dados perdidos não sejam usados de forma mal-intencionada, o conselho de diretores é obrigado a comunicar a perda através de meios de comunicação, o que gera o mesmo risco de que se os dados perdidos tivessem realmente sido usados maliciosamente. Muitas vezes, a não-utilização mal-intencionada pode ser pior para as empresas já que os clientes ficam imaginando quando sua identidade será roubada devido à violação.

Em decorrência do novo tipo de ameaças à reputação e à marca que pode ser associado ao Network Security 2.0, a segurança da rede engloba agora uma edição corporativa avançada. Os executivos administrativos e de TI responderam com gestão de riscos e, em particular, com cargos de gestão de risco de TI dedicados à gestão de proteção, conformidade e segurança, financiados pelos orçamentos do departamento apropriado e de conformidade no nível do conselho. Em particular, os projetos da indústria de cartão de pagamento (PCI), que se referem ao Payment Card Industry Security Standards Council, são projetos do conselho administrativo que partem de um plano conceitual e ditam os requisitos específicos de segurança para proteger informações confidenciais, débito, crédito, caixa eletrônica, ponto de venda, etc.

Como Implementar uma Gestão Estadual mais Segura e Mais Inteligente

Obter Relatório técnico

A maioria dos conselhos em todo o mundo está preocupada com a conformidade, em especial com a conformidade com PCI, perda e roubo de dados e está perguntando a seus executivos de TI e administrativos o que está sendo feito para proteger contra essas explorações e para se manter em conformidade? Quais são nossas políticas, que tecnologias estamos usando ou precisamos adquirir para ampliar nossas defesas contra malware, spyware, botnets ou há algo dentro da nossa corporação que esteja potencialmente contribuindo para o vazamento de dados ou a não-conformidade?

A diferença no Network Security 2.0 é que as proteções dos anos 2000 não vão mais funcionar. No início de 2000, se uma corporação fosse infectada com um worm da Internet propagado através da sua rede, a TI simplesmente compraria um IPS com uma boa cobertura de assinatura e o instalaria. Ele bloquearia o worm e o problema estaria resolvido. Existem inúmeras ameaças no Network Security 2.0 com políticas incorporadas para burlar as proteções de finalidade única como firewalls, filtros de spam, dispositivos IPS, etc. Para proteger contra “ameaças inteligentes”, todos os dispositivos de segurança de rede precisam trabalhar de forma integrada. Para proteger contra ameaças inteligentes, é necessário adotar uma abordagem de sistema para a segurança que aproveite os investimentos anteriores em segurança. Em resumo, é preciso ter uma função de orquestração que use inteligência de defesa já existente na rede para minimizar essa nova classe de ameaças.

Filial inteligente, surge um novo modelo de criação de valor

DObter Relatório técnico:

Abordagem de sistemas para a segurança de TI

A segurança de ponto terminal, rede, conteúdo e aplicativos formam os quatro componentes arquitetônicos da abordagem de sistema para a segurança de rede. Cada um desses componentes faz parte de uma proteção de segurança em camadas. Os pontos terminais são protegidos por um software anti-x. As redes são protegidas por tecnologia de segurança de firewalls, IPS, NBAD, NAC e NAP. A rede também precisa ser protegida no nível do protocolo para analisar em profundidade os fluxos quanto à presença de comportamento anormal e reagir a ele.

A segurança do conteúdo é uma abordagem de proteção contra ameaças novas e emergentes, que protege os usuários de conteúdo em email, websites, sistemas de mensagens e etc., visto que esse é o fluxo de conteúdo que pode precisar de controle de ameaças. Os novos servidores de email conectam-se e desconectam-se com muita rapidez, e o mesmo ocorre com os servidores da Web que possuem malware.

Isso exige uma abordagem de proteção baseada na reputação em comparação a uma baseada em assinatura, e a capacidade de responder a uma enorme quantidade de variantes, já que os ataques costumam ser bastante direcionados, mas mudam rapidamente conforme os ambientes encontrados. Isso exige capacidade de combater vários ataques diferentes, porque um ataque é sempre diferente do outro. Os tempos dos ataques altamente disseminâveis com um único padrão como o NIMDA chegaram ao fim, e foram substituídos por ataques mutáveis que lhes permite mudar para burlar as defesas encontradas. Esses ataques a aplicativos de colaboração costumam vir de email, web, sistemas de mensagem ou outros aplicativos de comunicação emergentes. Como os hackers agora precisam dos usuários para propagar os ataques, que não são mais autopropagáveis, a segurança de conteúdo foca na inspeção do conteúdo para proteger os usuários de ações que possam permitir um ataque.
O aplicativo e os dados que eles acessam costumam ser os alvos escolhidos para os próximos ataques. Com o aumento do uso da Web 2.0 e SOA/Serviços da Web nas organizações, os hackers devem passar a direcionar os ataques a esses aplicativos, principalmente porque eles contêm um grande número de informações de clientes, dados corporativos e propriedade intelectual.

A abordagem de sistemas está voltada para orquestrar essas tecnologias de proteção contra ameaças para trabalharem de forma integrada como um único sistema, exatamente como o Tivoli faz para a TI. Para isso, os recursos de gestão de sistema precisam reunir todos os quatro componentes através de política, reputação, serviços e identidade. A gestão do sistema pode aplicar políticas comuns a todos os quatros componentes. Produtos como o Cisco MARS 6.0 agregam informações de alarme criando eventos correlacionados que forneçam sugestões de correção automatizadas ou que exijam ação do usuário para as operações da rede. Esses produtos de agregação de alarmes de segurança e correlação de eventos de segurança carregam informações de alarme de cada um desses quatro componentes e correlacionam os dados fornecendo os cenários das possíveis ameaças à rede e depois definindo proativamente uma política ou respondendo a uma ameaça.
A abordagem de sistema baseia-se na integração dos melhores produtos de segurança disponíveis no mercado já implementados na sua empresa através de um gerenciamento do sistema. A abordagem de sistema aplica políticas corporativas nos quatro componentes, protege os ativos críticos da TI e, ao mesmo tempo, diminui a sobrecarga e o custo operacional da TI. O resultado final é um menor risco para a segurança e de não-conformidade. Essa abordagem acaba com o dilema dos compradores de segurança: “devo comprar os melhores produtos disponíveis ou construir uma abordagem de sistema para a proteção de TI?”

Iniciantes não conseguem acompanhar

Cada nova onda de ameaças à segurança cria um mercado para empresas iniciantes desenvolverem produtos projetados especialmente para combater essas ameaças. Em geral, essas empresas são excelentes para criar uma proteção para uma ameaça em particular, mas não dispõem dos recursos necessários para combater a próxima onda de ameaças. Em resumo, essas novas empresas estão sempre em uma corrida contra os hackers, e como agora os hackers são criminosos cibernéticos com amplos recursos financeiros que superam em muito o orçamento das empresas iniciantes, fica impossível vencê-los. O resultado desse ciclo é que mesmo os melhores produtos do mercado acabam em um beco sem saída. Eles passam a atuar como um dispositivo/aparelho independente, como

um firewall, NBAD, IPS, dispositivo NAC, etc. e tentam expandir seu portfólio de mitigação de ameaças concentrando em uma pequena área através de desenvolvimento interno ou parcerias e constroem um silo de segurança mal integrado. Por exemplo, a parceria do 3Com IPS Tipping Point com o Lancope StealthWatch é um silo de segurança mal integrado de combate a ameaças com IPS e NBAD.

Combater ameaças emergentes ou ameaças difundidas?

Isso não quer dizer que os melhores produtos do mercado não sejam bons. Mas quando implementados como parte de uma abordagem de sistema completa, eles passam a ter uma maior durabilidade e contribuem para fortalecer a postura de segurança da sua empresa. Por exemplo, considere a Cisco. A Cisco oferece um dispositivo NAC que é o melhor produto do mercado, mas para aproveitar o máximo os recursos do dispositivo NAC, é preciso que ele faça parte de uma abordagem de sistema que lhe permita funcionar de forma integrada com outros produtos de segurança como o TrustSec da Cisco. Em uma abordagem de sistema, o dispositivo NAC inclui tudo o que está conectado à rede ampliando seu diâmetro e sua utilidade. Na Cisco, a estratégia de segurança é oferecer os melhores produtos do mercado que possam operar e migrar ao longo do tempo para uma abordagem de sistema integrado que ofereça maior valor aos clientes. Por exemplo, um cliente da Cisco pode implementar o Cisco IronPort, que pode não fazer parte da sua estrutura de gestão comum, ou o Cisco Security Manager pode não gerenciar o IronPort desde o início da instalação, mas é o melhor produto para segurança de email do mercado e posteriormente pode passar a integrar a sua abordagem de sistemas. Em resumo, a Cisco desenvolveu uma visão e uma estratégia para a plataforma de segurança de rede que se assemelha a uma jornada para seus clientes.

A Cisco promete que a postura de segurança da sua empresa melhora ao longo dessa jornada. Por exemplo, para proporcionar uma prevenção contra perda de dados (DLP), os clientes podem otimizar a solução de segurança de email IronPort com os recursos CSA (Cisco Security Agent), além da criptografia para armazenamento de mídia, e integrar essas melhores soluções do mercado em um único sistema para proporcionar uma solução eficaz contra a perda de dados. Essa é uma abordagem de sistemas criada com base nos melhores produtos disponíveis no mercado. Ela aumenta o valor das melhores soluções do mercado, que são excelentes para mitigar ameaças existentes e emergentes de curto prazo para proporcionar uma proteção contra ameaças difundidas como a perda de dados.

Não espere que os órgãos de padronização definam o padrão para as interfaces ou arquiteturas de segurança. A indústria não possui essa função organizadora. Os executivos administrativos e de TI devem recorrer aos grandes fornecedores de sistemas de TI como a Cisco, EMC, IBM, HP, Microsoft et al para obter uma visão, uma plataforma e parcerias para combater essas ameaças inteligentes. Todos esses grandes fornecedores de sistemas de TI estão se dando conta de que a segurança é um processo comum que engloba toda a indústria de Tecnologia da Informação e precisa fazer parte de uma abordagem de sistemas global. Essa é uma boa notícia porque, para se proteger contra as explorações do Network Security 2.0, é preciso adotar uma abordagem de sistema integrado. Não pense na abordagem de sistema como uma resposta automatizada às ameaças que fecha portas, endereços IP, subredes ou muda as ACLs. Imagine-a como um sistema autônomo para entender que a nova proposta é uma proteção contra ameaças que englobe todo o sistema.

Segurança de rede autônoma

A visão da indústria é pensar em termos de um efeito autônomo que aumente ao longo do tempo à medida que mais dos quatro componentes são conectados em uma abordagem de sistemas. Quando os quatro componentes passam a trabalhar juntos sob a gestão do sistema, o efeito autônomo aumenta. Da mesma forma que quanto o sistema nervoso humano responde automaticamente a sensores, o cérebro não precisa pensar antes de executar uma ação. Por exemplo, se uma pessoa coloca a mão sobre um forno quente, o sistema nervoso responde automaticamente informando à mão para sair do forno quente. Não é preciso pensar. Também não é preciso pensar para o seu sistema imunológico combater um vírus ou uma infecção ou para os pulmões respirarem ou o coração bater. Esses sistemas são autônomos. É assim que as redes começarão a se comportar quando os melhores produtos de segurança do mercado estiverem conectados na abordagem de sistemas.

Como começar a construir uma abordagem de sistema para a segurança de rede

O melhor da abordagem de sistemas é que ela aproveita uma infra-estrutura de proteção já existente e não exige que você aposente prematuramente os seus atuais investimentos em segurança. A Cisco é líder nesta abordagem com os investimentos nos seus produtos MARS (Sistema de Monitoração, Análise e Resposta) e CSA. Os clientes que possuem esses produtos podem começar a sua implantação sem sequer precisar adquirir novos produtos. Outros grandes fornecedores de produtos de segurança e TI como IBM, Microsoft, HP e CA responderão com suas próprias ofertas e ecossistemas. O que diferenciará essas soluções dependerá dos pontos fortes de cada empresa em particular. A solução da Microsoft será baseada em desktop e servidor enquanto a IBM e a HP podem ser voltadas para Data Center; a CA seria baseada em aplicativos. A Cisco é a única empresa com uma solução baseada na rede e com todos os ativos da TI conectados através da rede. Essa é uma posição sólida para proteger contra as ameaças.

Os executivos administrativos e de TI precisam decidir que fornecedor de gestão de sistemas escolher. O MARS da Cisco foi mencionado acima, mas há também o Q1 Labs QRader, que é um sistema de gestão e correlação de eventos de segurança que pode evoluir para um sistema de Gestão de Sistemas. A Nortel e a Juniper formaram uma parceira com a Q1, e a Enterasys produz seu próprio sistema para o Dragon Security Command Console. Apesar de disporem de um conjunto de recursos para fornecer política, reputação e identidade, as soluções da Nortel, Juniper e Enterasys não são tão abrangentes e não possuem visão, plataforma e ecossistema para realisticamente fornecer uma abordagem de sistema para a segurança de rede.