Segurança

A segurança é algo que começa com o seu conhecimento. Para que esta seja o mais forte possível entender como funcionam e se comportam as coisas é de suma importância. Então neste texto vamos falar, de forma resumida, do firewall, um recurso importante e sobre Ransomwares.

Segurança: Planejamento e implementação de um firewall[1]

Firewall é o gateway para a Internet, no qual tem o objetivo de controlar todo o tráfego de dados e comunicação do ambiente interno com o externo (tanto o ponto de vista de entrada e saída, quanto os pacotes que passam por ele). Estamos falando de firewall corporativo que possui funções e recursos, tais como, VPN, controle de navegação, regras de filtragem, controles de acesso externo, logs, proxy http e https, entre outros.

Quando existe a demanda de realizar este tipo de implementação, é fundamental entender o ambiente da empresa e se já existe outro firewall realizando este serviço. Se a empresa já possui um firewall e pretende atualizar por uma versão mais nova, ou adquirir outro com mais recursos e capacidade de gerenciamento, o trabalho de planejamento da implementação se torna, de certa forma, mais fácil de ser realizado pelo fato das regras e configurações do ambiente já estarem prontas. Com isso, pode-se assim analisar o antigo firewall, apresentar para o gestor as configurações atuais e, em cima disto, realizar os ajustes, melhorias e aplicar no novo firewall.

Um simples trabalho de transpor regras nunca é eficiente, pois na administração de firewalls muitas das regras acabam sendo colocadas de forma emergencial e ficam sobressalentes. Algumas regras os administradores nem sabem para que servem e elas permanecem lá ativas, deixando o firewall cada vez menos confiável. Agora é a melhor hora para reorganizar tudo!

Já empresas que não possuem um firewall, nas quais toda a navegação é realizada pelos usuários sem controle algum e não existe conhecimento do tráfego que é realizado entre os ativos de TI e a Internet e vice-versa, o trabalho de planejamento se torna mais efetivo e necessário, já que uma implementação sem este alinhamento inicial com certeza irá impactar toda operação da empresa e gerar descontentamento dos serviços realizados.

DICAS PARA O PLANEJAMENTO

Definir as regras de navegação e perfis de acesso: Algumas empresas podem optar por não realizar nenhum controle ou bloqueio dos websites acessadas pelos funcionários, downloads realizados, softwares de torrent, entre outros. A questão, neste tipo de cultura empresarial, pode refletir negativamente em algumas situações, tais como, funcionários

[1] http://cegconsultoria.com.br

improdutivos, elevado risco de infecção de vírus, trojan, malware, armazenamento de conteúdos indevidos (pornografia, pedofilia, racismo), etc.

A definição das regras de navegação e perfis de acesso, além de garantir um ambiente mais seguro, direciona os funcionários a acessarem e realizarem as atividades pertinentes às suas funções.

Geralmente são definidos alguns perfis de navegação e neles são vinculadas as categorias de acesso permitido e quais categorias serão bloqueadas. Com os grupos definidos e as categorias de navegação vinculadas, é hora de planejar quais setores da organização e/ou quais funcionários serão vinculados em qual perfil de navegação.

É importante este planejamento ser definido com a alta direção e os gestores estarem alinhados neste processo, já que mudanças culturais e até comportamentais irão ocorrer na empresa. Algum descontentamento inicial por parte dos funcionários pode ocorrer, como exemplo: o Facebook sempre foi liberado e no dia seguinte está bloqueado.

Os funcionários irão recorrer aos gestores para solicitar a liberação e, se existir exceção sem critérios, em pouco tempo a exceção irá virar regra. Normalmente estas solicitações chegam de modo genérico, tais como: não estou conseguindo trabalhar, pois não consigo acessar mais nada. Os administradores do firewall devem estar preparados para lidar com este tipo de situação de forma tranquila e sem estresse.

Outro ponto importante a ser mencionado neste tipo de alinhamento e planejamento é que não existe um padrão a ser seguido. Se os gestores definirem que as categorias "entretenimento" e "redes sociais" serão liberadas para todos os perfis, não haverá problema algum, isso depende muito do foco e cultura de cada empresa.

Definir as regras de filtragem: As regras de filtragem do firewall irão definir e controlar todo o tráfego de informações que passa através do gateway, ou seja, se for definida uma regra com a origem "rede interna", destino "Internet", porta "80 e 443" como liberada, esta estará permitindo os computadores, servidores e dispositivos a se conectarem ou acessarem qualquer website ou serviço que utilize uma destas portas, neste caso, a maioria dos web-servers na Internet.

Estas regras precisam ser definidas junto à área de negócios da empresa, já que computadores do financeiro, contabilidade e TI precisam do acesso liberado a todos os sites e sistemas do governo e prefeituras. Quando a empresa não sabe exatamente como definir estas regras, é interessante configurar o firewall somente para monitorar, sem bloquear nada. Desta forma, em algumas semanas é possível analisar, através de logs e relatórios, o tráfego realizado e em cima deste fazer as regras de liberação e bloqueio.

Regras de NAT: *Network Address Translation* (NAT), de forma bem simples, é o meio de comunicação dos IPs privados para se comunicarem com o mundo externo e vice-versa.

No planejamento das regras de NAT é definido, por exemplo, em qual dos links de Internet irá sair a navegação, ou ainda, quando a empresa possui sites, portais ou sistemas publicados na Internet, é através do NAT que se configura uma solicitação de acesso da Internet no IP Público pela porta XX que será direcionado ao servidor XYZ, o qual, normalmente, fica em um DMZ (*Demilitarized Zone*).

VPN: *Virtual Private Network* (VPN) é a forma de comunicação entre dois meios, podendo ser matriz com a filial, parceiros ou funcionários externos. Com a VPN é possível, mesmo estando em outro local fisicamente, acessar as informações que estão dentro dos servidores da empresa. A VPN fecha um túnel criptografado para comunicação do cliente com o servidor. Para a definição destas VPNs, quem irá ter o acesso e como será realizado, deve ser analisada

a viabilidade de realizar este serviço, já que para fechar uma VPN IPsec entre dois sites, o outro lado também precisa ter um firewall.

Ransomwares: O que são e como evitá-los[2]

Vírus que "sequestram" dados dos usuários ameaçam a segurança de empresas em todo o mundo

Recentemente uma grande empresa de soluções de segurança divulgou um estudo que aponta o Brasil como um dos maiores propagadores de vírus do mundo. Somos o décimo país no ranking mundial e o primeiro na América Latina. Muito disso se deve aos hábitos dos usuários de internet no país, que costumam ser descuidados na hora de abrir e compartilhar informações, mesmo que manualmente.

Mais preocupante do que esse cenário, é o fato de que, nós brasileiros, somos a população mais exposta a um tipo de vírus que vem causando muitos transtornos em usuários domésticos e corporativos – os ransomwares.

Trata-se de uma categoria de malware – aplicações maliciosas que acessam sistemas clandestinamente – que, literalmente, sequestram os dados do computador infectado. O vírus criptografa, com códigos fortíssimos, todas as informações do usuário. Em seguida, cyber-criminosos cobram o resgate dos dados, normalmente via bitcoins ou outras operações não rastreáveis.

Apesar do recente crescimento de dificuldades ocasionadas pelos ransomwares – a incidência deste tipo de ataque aumentou 35% em 2016, de acordo com o mesmo estudo anteriormente citado – o problema não é novo. A primeira vez que um caso de sequestro de dados foi sinalizado, foi em 1989.

Porém, foi somente na última década que o termo ganhou atenção especial, graças a um vírus conhecido como Gpcode. De lá para cá, uma infinidade de novos ransomwares foi criada no mundo da tecnologia, como o Simplocker, que afeta dispositivos Android, e o temido Cryptolocker, que ataca o sistema Windows.

O risco que essas ameaças representam, sobretudo às empresas, é imenso. Portanto, os dados e informações de uma empresa devem ser tratados como um ativo valioso. Medidas básicas de proteção como, manter os softwares atualizados, o firewall ativado e evitar clicar em e-mails e programas estranhos, podem ajudar a evitar uma grande dor de cabeça.

No entanto, a melhor prevenção contra os ransomwares ainda é o bom e velho backup. É importante conscientizar os gestores de negócios que a cópia periódica de

[2] http://cegconsultoria.com.br

arquivos importantes em um serviço de nuvem seguro garante que não haverá problemas maiores no caso de uma infecção do sistema físico da empresa.

Se prevenir contra vírus, especialmente ransomwares, pode ser determinante para a saúde de um negócio. A proteção ideal para dados e informações corporativas não requer um alto investimento. Com a oferta existente de serviços e soluções de backup e contando com um suporte de TI de confiança, não há razões para deixar o backup de lado.

Conclusão

Mais uma vez devemos lembrar que por mais que a tecnologia evolua sempre vai depender do homem. Ele é o grande prejudicado e um dos poucos que pode evitar que as coisas erradas aconteçam. Você pode notar que no primeiro caso, firewall, depende de uma boa pesquisa para verificar o mais adequado e configura-lo de forma correta. Alguns destes podem ser instalados na sua própria máquina, firewall individual ou particular, agregando mais dificuldade ao invasor. O segundo depende da promiscuidade digital, não entrando em qualquer site, cuidado com os e-mails e não instalando qualquer coisa. As armadilhas estão aos montes na internet, principalmente oferecendo coisa gratuitas. CUIDADO.