

As Dez Maiores Ameaças de Segurança nas Empresas de Pequeno e Médio Porte

O artigo seguinte é extraído de "Top 10 Threats to SME Data Security", documento escrito por Scott Pinzon, CISSP, da equipe WatchGuard @ LiveSecurity. Este resumo contém a lista das dez principais ameaças e um resumo de cada uma. Para maiores informações sobre a forma como foram selecionadas as ameaças, quais tipos de rede que estamos a tratando e, pelo menos, mais duas contramedidas para cada ameaça, baixe uma cópia gratuita de todo o documento em <http://www.watchguard.com/infocenter/whitepapers.asp>.

É difícil encontrar relatórios precisos sobre o que realmente ameaça a segurança das redes atualmente, para a grande maioria das empresas.

Desde 1999 a equipe WatchGuard LiveSecurity tem monitorado, diariamente, emergentes ameaças de segurança de rede, com um foco especial nas questões que afetam as pequenas e médias empresas (PME). Quando percebemos uma ameaça que pode afetar as empresas negativamente, alertamos imediatamente nossos assinantes por avisos via e-mail.

Sabedores de que nossos assinantes têm restrição no quesito tempo em função do excesso de trabalho usualmente existente nas áreas de TI, nossos comunicados alertam apenas quando sabemos que não é apenas um ataque possível, mas potencialmente provável.

Esta ênfase no contexto empresarial e praticidade tornam o nosso serviço quase exclusivo.

Esta abordagem é constantemente aperfeiçoada, seja pela entrada de dezenas de milhares de novos assinantes, bem como por visitas aos clientes locais e grupos específicos de reflexão e estudos.

O resultado: o documento contém a lista dos 10 principais vetores de dados mais comuns na nossa experiência como analistas de segurança para as PME. Sugerimos também as práticas, técnicas e defesas para combater cada vetor.

Ameaça # 10: Ataques Internos

A *Verizon's Intrusion Response Team* investigou 500 intrusões em 4 anos e pode atribuir 18% das brechas/violações aos corruptos internos. Destes 18%, cerca de metade surgiu da própria equipe de TI.

Aplicar o princípio do duplo controle.

Aplicar duplo controle significa que, para cada chave de recurso, você tem um *back up de segurança*. Por exemplo, você pode optar por ter um técnico principal responsável pela configuração da sua Web e servidores SMTP. Mas, pelo menos, credenciais de login para os servidores devem ser conhecidas ou estar à disposição de outra pessoa.

Ameaça # 9: Falta de contingência

As empresas que se orgulham de ser "ágeis" e "responsáveis" muitas vezes atingem essa velocidade, abandonando a padronização, processos maduros de planejamento e contingência. Muitas PME têm verificado que uma simples falha em função de bases de dados ruins ou falta de compromisso com segurança da informação se tornam desastrosos quando não existe Plano de Continuidade de Negócios, Plano de Recuperação de Desastre, Política de Resposta a Invasões e Backup Atualizado dos Sistemas (que possa ser realmente restaurado armazenado em outro site).

Solução para a falta de planejamento

Certamente se você tiver dinheiro para isso, contrate um especialista para ajudá-lo a desenvolver metodologias adequadas de segurança da informação. Se você não tem recursos para tanto, O SANS

Security Policy Project oferece modelos gratuitos e outros recursos que podem ajudá-lo a escrever as suas próprias políticas. Para mais informações, visite <http://www.sans.org/resources/policies/>

Ameaça # 8: Configuração Inadequada

Empresas inexperientes às vezes instalam roteadores, switches, redes e outros appliances de rede sem envolver qualquer técnico que compreenda e garanta a melhor aplicabilidade de cada equipamento. Neste cenário, uma rede amadora só tem utilidade para o envio e recebimento de dados, não garantindo qualquer proteção à informação.

Soluções para uma má configuração

Realize um escaneamento automatizado. Se você não pode se dar ao luxo de contratar consultores especializados, provavelmente você pode pagar, uma única vez, por uma varredura automática em sua rede. Há muitos e muitos produtos de Gerenciamento de Vulnerabilidades no mercado, em todos os níveis de preços. O uso regular dos mesmos deve ser parte da sua rotina de manutenção de sua rede.

Ameaça # 7: Despreocupação com as redes de hotéis e quiosques

Redes de Hotéis são usualmente vulneráveis com relação a vírus, worms, spywares e malwares, e muitas vezes são administradas com precárias práticas de segurança. Quiosques públicos são 'ótimos ambientes' para um hacker deixar um keylogger, o que bastaria para que ele possa ver e monitorar o que se passa no âmbito daquela rede. Notebooks que não têm softwares de firewall, antivírus e anti-spyware atualizados podem ficar comprometidos. Defesas tradicionais podem se tornar inúteis quando o usuário literalmente carrega o laptop em torno do gateway firewall, e se conecta a partir de zonas confiáveis de segurança.

Soluções nas redes de hotéis

Definir e executar políticas que proíbam funcionários de desligar os recursos de defesa implantados no seu equipamento (laptops). De acordo com uma pesquisa encomendada pelo Fiberlink, 1 em cada 4 usuários habituais de laptops autorizam alterar ou desativar as configurações de segurança em seus laptops. Os usuários nunca devem desligar as defesas a menos que recebam autorização para tanto. Muitos antivírus populares podem ser configurados de modo que não possam ser desligadas as configurações de segurança, até mesmo por usuários com privilégios de administrador local.

Ameaça # 6: Utilização imprudente de Wi-Fi nos Hot Spots

Wireless Hot Spots contém os mesmos riscos que as redes de hotéis - e mais alguns. Hackers invasores normalmente disponibilizam pontos de acesso wireless que são disponibilizados e acessados como se fossem um "Free Public WiFi". Isto feito, aguardam por uma conexão de usuários de laptops wireless. Com um pacote sniffer ativado, o invasor passa a ter a habilidade de ver tudo do outro computador, inclusive logins. Este ataque é particularmente nefasto, porque o atacante rouba os dados, não deixando absolutamente nenhum vestígio de invasão no laptop *hackeado*.

Soluções na utilização de Wi-Fi

Instrua os usuários a sempre escolher conexões criptografadas e acesse-las através de uma Rede Virtual Privada (VPN). Este procedimento permite a criptografia de todo o fluxo de dados.

Ameaça # 5: Dados perdidos armazenados em dispositivos portáteis

Todos os anos, muito dados sensíveis e importantes são comprometidos quando usuários acidentalmente deixam seus *smartphones* em um táxi, seu *pen drives* em um quarto de hotel, ou seu laptop em um evento qualquer. Quando dados são armazenados em dispositivos portáteis e móveis é mais prudente e eficiente se os administradores pensarem antecipadamente sobre.... "o que vão fazer quando o equipamento for perdido" ao invés de "o que vão fazer se o equipamento for perdido".

Soluções para dados perdidos armazenados em dispositivos portáteis

Gerenciar dispositivos móveis de forma centralizada. Considere investir em servidores e softwares que, de forma centralizada, gerenciem esses dispositivos móveis. Como exemplo, *RIM's BlackBerry Enterprise Servers* pode ajudá-lo a assegurar transmissões encriptadas. Desta forma, se o usuário notificar que o seu aparelho *Blackberry* foi extraviado, você pode limpar (deletar)

remotamente os dados do Blackberry perdido. Estes cuidados e procedimentos são o melhor caminho para se minimizar o impacto negativo da perda de dispositivos e seus respectivos dados e informações.

Ameaça # 4: Comprometendo servidores Web

O mais comum hoje em dia é identificar botnets atacando sites da Web; e a maioria dos sites é desenvolvida em linguagens não efetivas e ineficientes em relação às falhas fatais. Invasores têm comprometido centenas de milhares de servidores em um único ataque injetado de SQL automatizado. Sites confiáveis são criados e em seguida servem de abrigo para o malware, assim, involuntariamente espalhando o bot pela rede.

Soluções para o comprometimento do servidor Web

Monitore sua Web. Se (por exemplo) um formulário da Web tem um campo para um visitante fornecer o número do telefone, a página web deve descartar excesso de caracteres. Se a aplicação web não sabe o que fazer com os dados ou um comando, deve rejeitá-la, não processá-lo. Procure a solução que você possa pagar (seja um expert ou uma ferramenta automatizada), com ênfase em descobrir se o seu código tem validação.

Ameaça # 3: Uso indevido da Internet pelos funcionários

Um estudo da Universidade de Washington em 2006 descobriu que os sites que espalham o maior número de spy wares foram (em ordem):

- Fã Sites (como os que fornecem notícias atualizadas de Paris Hilton e Britney Spears);
- Sites de jogos on-line (onde você pode jogar contra um estranho)
- Sites Pornô (surpreendentemente em terceiro lugar)

Sites de Relacionamento como MySpace, Orkut e Facebook têm se tornado o maior abrigo para spams, trojans e spyware. Usuários que navegam por estes sites estão convidando, para o mundo empresarial, bots, spyware, keyloggers, spambots, ou seja, toda a gangue dos malwares.

Soluções para a navegação imprópria na Internet

Implementar filtragem de conteúdo web. Uso de filtros de conteúdo, como a da WatchGuard WebBlocker. Soluções de filtro de Web mantêm bases de dados (atualizadas diariamente) de URLs bloqueadas por categorias. Quanto maior o número de categorias, maior o número de nuances. Tais ferramentas irão lhe ajudar a reforçar sua Política Satisfatória de Uso da Tecnologia.

Ameaça # 2: E-mails maliciosos HTML

O ataque mais comum a e-mail agora chega como um e-mail HTML, que liga o usuário a um site com armadilhas maliciosas. Um clique errado pode desencadear download de um arquivo executável. Os perigos são os mesmos da Ameaça # 3, mas o atacante utiliza um e-mail atrativo para receber a vítima em seu site malicioso.

Soluções E-mails maliciosos HTML

Implementar ponto único de tráfego web proxy. Você pode configurar sua rede local para que todos as solicitações e respostas HTTP sejam redirecionadas para um servidor web proxy, o que proporciona um único ponto do tráfego da Web em que todos os dados serão controlados apropriadamente. O web proxy não vai detectar um e-mail entrante malicioso, mas, se um usuário em sua rede clica em um link no qual o e-mail HTML irá gerar uma solicitação http, o proxy web pode detectá-lo. Se o usuário da solicitação HTTP nunca chegar ao site do atacante, o usuário não se torna vítima.

Ameaça # 1: Exploração automatizada de uma vulnerabilidade conhecida

Verizon's 2008 Data Breach Investigations Report tem compilada evidências de mais 500 violações de dados ocorridas ao longo de 4 anos. O *Verizon's RISK Team* concluiu que 73% das violações ocorreram a partir de fontes externas.

Empresas SMB negligentes se tornam vítimas se não instalam as atualizações do Windows durante o mês de sua publicação. Porém, sua rede contém muito mais do que produtos da Microsoft. Sua rotina de atualizações precisa se estender sistematicamente a todas as aplicações e Sistemas Operacionais componentes da sua rede.

Solução de Exploração Automatizada

Invista no gerenciamento de patches. Softwares de gerenciamento de patches irão ajudá-lo a *scanear* sua rede, identificando patches faltantes e/ou atualizações de software necessárias, atualizando-os automaticamente a partir de um controle central, aumentando em muito sua chance de ter toda a rede atualizada e segura.

Construa um teste de rede barato. Mesmo empresas bem conceituadas no quesito segurança de rede podem falhar. Por isso, recomendamos instalar os patches e atualizações em um ambiente de teste, antes de instalá-lo diretamente em sua rede. Se você não tiver um ambiente de teste, sugerimos que, na próxima vez que você substituir os computadores e servidores, guarde-os e dedique-os a seus próximos testes de rede.

Conclusão

As medidas que sugerimos acima podem ser um grande passo no intuito de proteger sua rede. Mas é apenas uma pequena amostra das medidas que um administrador de TI poderia implementar para aumentar a segurança da sua rede. Para obter conselhos práticos e para fortalecer a sua rede contra problemas comuns, baixe uma cópia gratuita do completo **As Dez Maiores Ameaças de Segurança nas Empresas de Pequeno e Médio Porte** (e o que fazer com elas) da WatchGuard.

Os equipamentos de segurança de rede da WatchGuard® disponibilizam Gerenciamento Estendido de Ameaças (XTM) que tratam nove das dez ameaças listadas aqui (Infelizmente, os nossos aparelhos não podem impedir os usuários de perder os seus dispositivos portáteis). Podemos ajudá-lo a proteger a sua rede wireless, verificar a integridade de clientes solicitando o acesso à sua rede, filtrar spam, proxy web services, minimizar ameaças internas, criar VPNs, e muito mais.

Para obter informações sobre a WatchGuard® e nossas soluções de segurança e de proteção contra ameaças em sua rede visite-nos em www.watchguard.com ou fale com um de nossos canais autorizados.