Seis dicas simples para frustrar os hactivistas
Carolyn Duffy Marsan

Mais da metade - 58% - de todos os casos de violação de dados em 2011 foram resultado de ataques politicamente motivados. É preciso muio pouco para proteger sua empresa.

Mais dados foram roubado de redes corporativas no ano passado pelos hactivistas do que por criminosos, segundo relatório recente da Verizon (2011 Investigative Response (IR) Caseload Review), que analisou 855 casos de quebras de segurança cibernética em todo o mundo, envolvendo 174 milhões de registros comprometidos.

Mais da metade - 58% - de todos os casos de violação de dados em 2011 foram resultado de ataques politicamente motivados e não por ganhos financeiros.

Segundo a Verizon, a maioria das violações poderia ter sido evitada se os gerentes de rede seguissem as melhores práticas em segurança da informação.

Aqui estão seis dicas que a Verizon considera que podem ajudar os CIOs a evitarem ataques feitos por hactivistas:

1. Proteja seus servidores

A Verizon descobriu que 94% de todos os dados comprometidos no ano passado estavam em servidores atacados, em vez de dispositivos finais como laptops ou smartphones. Assim, enquanto os CIOs estão preocupados com o gerenciamento de dispositivos móveis e as políticas de BYOT, deveriam estar prestando mais atenção à segurança física e cibernética dos servidores que contêm informações de identificação pessoal ou de propriedade intelectual.

2. Livre-se de dados desnecessários

As corporações tendem a coletar dados muito sensíveis, e quase sempre não conseguem eliminá-los quando não precisam mais deles. Todas as organizações precisam ter políticas rígidas para manter o mínimo de dados necessários para atender às exigências regulamentares. Precisam saber quais dados devem ser mantidos, e onde estão localizados, para que possam mantê-los seguros.

3. Olhe para seus registros

Muitas empresas têm software de segurança que geram logs de acesso à rede, e de outras atividades, mas não têm ferramentas automatizadas para analisar os logs e encontrar vulnerabilidades ou falhas.

Os CIOs precisam alocar recusos humanos para monitorar e explorar os logs de eventos e identifcarem evidências de ataques à rede ou aos servidores.

Atividades incomuns na rede podem ser sinal de presença de um malware que coleta, monitora e registra as ações dos usuários, logins e senhas. O monitoramento também pode identificar ataques de injeção de SQL, que visam os sites web apoiando-se em bases de dados relacionais. Uma das formas mais comuns de hackear sistemas é a inserção de códigos SQL em formulários web para atingir os bancos de dados escritos nessa linguagem.

4. Use autenticação de dois fatores

Ter um sistema de autenticação de dois fatores para controle de acesso - como senhas e um cartão de acesso - reduz o risco de hackers invadirem servidores com nomes de usuário e senhas roubados.

Também é importante ter políticas estritas de senhas, como o uso de senhas complexas, a obrigatoriedade de mudança da senha regularmente e a adoção de mecanismos para limitar as

tentativas de login. Outra sugestão é o uso de listas negras de IP para restringir o acesso aos servidores.

5. Cuidado com o PCAnywhere

Ferramentas que permitem o acesso remoto a sistemas pesoais, como o PCAnywhere, são comumente usados por hackers para criar backdoors desbloqueadas em sistemas corporativos.

Gerentes de rede podem usar listas negras de IP para bloquear que os sistemas tenham acesso a estas ferramentas, bem comofiltros que evitem que informações confidenciais fluam para fora de uma rede corporativa. O uso de sistemas de prevenção de perdas de dados e de detecção de intrusão também podem ajudar.

6. Treine seus funcionários

Muitas vezes os hackers empregam truques que tiram proveito de “vulnerabilidades humanas” apelando para emoções ou incitando a curiosidade para levar as pessoas a clicarem em links maliciosos, baixarem programas ou darem informações confidenciais como senha da rede corporativa, do e-mail, etc. As empresas precisam investir na formação contínua para manter funcionários constantemente conscientes das ameaças desses ataques de engenharia social.

Fonte: CIO, 22 mar. 2012. [Portal]. Disponível em: <http://cio.uol.com.br>. Acesso em: 23 mar. 2012.