Redes sociais: sete brechas que podem colocar sua empresa em risco
Tim Greene

Sites como Facebook e LinkedIn são fonte rica para invasores em busca de dados para golpes de engenharia social, aponta executivo de segurança

As redes sociais são uma rica fonte para hackers, que podem colher dados corporativos valiosos ou se infiltrar em redes empresariais, alertou um diretor de segurança da informação de uma grande empresa de trading.

"Os sites de redes sociais são uma verdadeira praga", pelo menos da perspectiva de segurança corporativa, afirmou Alan Lustiger, diretor de segurança de informação da Gain Capital Holdings, durante a conferência The Security Standard 2010 esta semana, em Nova York (EUA).

Sete brechas

Eis as sete razões apontadas por Lustiger:

1 - A busca em sites sociais por nomes de empresas revela, mesmo que parcialmente, uma lista dos funcionários, o que já facilita bastante o trabalho de quem pretende explorar ataques de engenharia social.

2 - Endereços corporativos de e-mail publicados em sites sociais fornecem informação valiosa. Se o esquema de formação dos e-mails (inicial do primeiro nome e sobrenome, ou primeiro nome mais "sublinhado" e sobrenome) for o mesmo da senha, então a segurança estará comprometida. "Você estará a meio caminho de divulgar seu usuário e senha", diz.

3 - Informações publicadas em sites sociais dão pistas para tentativas de adivinhação de senha – nomes de crianças, comida favorita, equipes esportivas, etc.

4 - Concursos falsos anunciados em sites sociais que exigem todo tipo de dado, e que poderiam ser usados para redefinir senhas: que escola você frequentou, nome de seu primeiro animal de estimação, seu tio favorito, entre outros.

5 - URLs encurtadas usadas frequentemente no Twitter podem levar a qualquer lugar - e a URL não lhe dá pista alguma de qual lugar seria esse.

6 - O garimpo de informação em quadros de avisos pode render notícias de vagas de TI em empresas dentro do alvo do invasor. Este, por sua vez, poderia se qualificar para uma entrevista e, nela, obter informações detalhadas sobre a rede corporativa no decorrer da discussão sobre o trabalho em potencial e sua experiência com tecnologias específicas.

7 - O uso do GPS pelo Google Latitude torna público o local onde a pessoa está no momento, revelando também todos os lugares onde ela não está. Pessoas que buscam um pretexto para entrar num prédio comercial poderiam usar esta informação para passar na empresa e pedir para falar com um empregado que sabidamente não estará lá.

Pé na empresa

Lustiger diz que tudo que os exploradores de engenharia social precisam é conseguir colocar um pé dentro da empresa, mesmo que seja na área da recepção. Basta que um deles entre, pergunte por alguém que não está lá, decida esperar e, então, peça à recepcionista para imprimir uma planilha que deveria ser levada à reunião com a pessoa que não está lá.

As recepcionistas, treinadas para serem solícitas, irão inserir um pen drive USB em seu computador para imprimir o documento. Ao mesmo tempo, na retaguarda, um malware estará plantando um backdoor, roubando dados ou liberando código destrutivo, diz o diretor – tudo sem deixar rastro.

A utilização deste artigo é exclusiva para fins educacionais

Outros truques de engenharia social incluem conseguir qualquer vaga na empresa, dando ao invasor acesso interno às redes e mais tempo do que realmente precisariam para causar estrago. “Levaria minutos e não seria algo difícil de fazer”, diz.

Educar os empregados sobre os riscos é a melhor forma de bloquear vetores de ataque social, diz Lustiger. Relacionar essas medidas a suas vidas pessoais ajuda. “Por que um site web precisa saber sua data de aniversário?”, pergunta, apontando que a informação pode ser utilizada como um fator de identificação para mudar senhas ou roubar identidades. Ele tem uma data de nascimento falsa que utiliza para ajudar a protegê-lo contra roubo de identidade.
As recomendações de segurança física que os empregados deveriam seguir incluem não deixar que pessoas aproveitem a passagem por uma porta aberta depois que alguém a tenha destravado com um cartão, e pedir identificação a qualquer pessoa que não seja reconhecida como funcionário.

Quanto aos sites de redes sociais, as equipes de segurança corporativa deveriam promover a monitoração, mesmo que amostral, dos sites de rede social usados por seus funcionários em busca de informação que, tornada pública, poderia comprometer a segurança de ativos da empresa. “Os empregados estão colocando informação lá fora em seu próprio tempo livre”, diz.

Mesmo as empresas mais diligentes permanecem vulneráveis, afirma. “É virtualmente impossível defender-se contra um invasor de engenharia social realmente dedicado que tenha tempo suficiente”, diz.

Fonte: IDG Now, 17 set. 2010. [Portal]. Disponível em: <http://idgnow.uol.com.br>. Acesso em: 21 set. 2010.

A utilização deste artigo é exclusiva para fins educacionais