CST0207-Arte de Enganar: Parte 2 - Defesa e Protecção contra a Engenharia Social

Data do Post	@August 5, 2022 9:00 AM
Status	Not started
Palavras-chave	Engenharia Social
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☐

Nor artigo anterior vimos de modo geral o *modus operandis* dos engenheiros sociais. Agora, pode ver nesse artigo algumas estratégias e técnicas para se proteger desses ataques.

Leia o artigo na íntegra.

Siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
#cybersecurity #technology #linux #ataquescibernéticos #hacking #socialengineering

Introdução

Políticas de segurança garante consistência na implementação dos controles adequados para redução dos ataques de engenharia social.

Essas políticas envolvem treinamentos de segurança para todas as pessoas envolvidas com tecnologia e todas as pessoas com acesso electrónico ou físico aos activos de TI da empresa.

Como evitar ataques de engenharia social

As organizações precisam de promover a consciencialização sobre as tácticas de engenharia social e educar adequadamente os funcionários sobre medidas de prevenção, como as seguintes:

- Nunca fornecer informações confidenciais ou credenciais via e-mail, sessões de chat, em pessoa ou por telefone a partes desconhecidas.
- Resistir ao desejo de clicar em e-mails atraentes e hiperligações de websites.
- Ficar atento aos downloads não iniciados ou automáticos.
- Estabelecer políticas e educar os funcionários sobre essas políticas.
- Quando se trata de segurança, dê aos funcionários uma sensação de propriedade.
- Não ceder à pressão de indivíduos desconhecidos.

Para poder evitar os ataques, é necessário considerar as recomendações abaixo.

Protecção dos dispositivos

No processo de defesa contra engenharia social é importante assegurar dispositivos para que um ataque de engenharia social, mesmo que bem-sucedido, seja limitado no que pode alcançar. Os princípios básicos são os mesmos, quer se trate de um ‘smartphone’, uma rede doméstica básica ou um sistema empresarial importante.

- **Anti-malware e antivírus actualizados: isso** permite evitar que o malware que vem por e-mails de phishing seja instalado automaticamente.
- **Software e firmware regularmente actualizados**: os desenvolvedores diariamente criam actualizações para melhorar os sistemas e principalmente patches de segurança, para garantir a melhor experiência para os usuários.
- **Não usar o seu telefone com root ou computador em modo administrador**: Mesmo se um ataque de engenharia social conseguir a sua senha de usuário para a sua conta de "usuário", ele não permitirá que eles reconfigurem o seu sistema ou instalem software nele.
- **Usar autenticação de dois factores:** para que ter sua senha não seja suficiente para acessar a conta. Isso pode envolver reconhecimento de voz, uso de um dispositivo de segurança, impressão digital ou códigos de confirmação por SMS.

Presença digital

Quer empresas como as pessoas têm a necessidade de ter uma presença digital. Ambos podem arriscar partilhar demasiadas informações pessoais on-line, por exemplo, através das redes sociais, pode ajudar os criminosos.

Existem pessoas com a tendência de postar rotinas e muitos aspectos sobre a vida pessoal e até mesmo profissional. Essas informações podem ser pontas soltas para que os criminosos criem os perfis das vítimas e, consequentemente, desferir um ataque de engenharia social.

Por outro lado, muitos ataques de engenharia social tentam ganhar credibilidade, referindo-se a eventos recentes que as pessoas compartilham em redes sociais.

É recomendável que as redes sociais sejam confirmadas de modo que as informações sejam visíveis para "apenas amigos" e é necessário ter cuidado com o que é compartilhado nas redes sociais.

Outros aspectos da sua vida que deve-se considerar são as pessoas que possuem perfis em sites de empregos. Nesse caso, as informações como, endereço, número de telefone e data de nascimento podem ser úteis para quem planeia um ataque de engenharia social.

A engenharia social é muito perigosa, porque leva situações perfeitamente normais e as manipula para fins maliciosos. No entanto, ao estar plenamente consciente de como funciona, e adoptar as precauções básicas, será muito menos provável que você se torne uma vítima da engenharia social.

Como as empresas podem proteger-se contra Engenharia Social

Para proteger uma organização de acções relacionadas a engenharia social algumas medidas preventivas devem ser adoptadas:

- Implementação de uma Política de Segurança da Informação, e sua ampla divulgação;
- Consciencialização dos funcionários em geral no que se refere às ameaças associadas à Engenharia Social;
- Implementação de mecanismos de segurança física;
- Monitoramento constante dos sistemas de controle de acesso a áreas, centrais telefónicas, entre outros;
- Identificação visual e documental dos visitantes e prazo de expiração para crachá de identificação;
- Acompanhamento de visitantes às instalações da organização por funcionário da organização, sem excepções;
- Não fornecimento de informações de cunho pessoal ou sigiloso sem a devida autorização da pessoa competente para tal;
- Remoção de evidências visuais de informações sigilosas (senhas de acesso, números de telefone restritos), em qualquer ambiente;
- Cuidados especiais com os descartes de lixos;
- Implementação de regras de descarte de informações armazenadas em quaisquer meios (papel, mídias magnéticas).

Analisar as fontes

Deve-se analisar a proveniência das informações; não confie cegamente nela. Uma pen drive USB que aparece na sua mesa e não conhece a origem? Um telefonema do nada diz que herdou 1 milhão de dólares? Tudo isto soa suspeito e deve ser tratado como tal.

Para verificar fontes não é difícil. Por exemplo: com um e-mail, analise o cabeçalho do e-mail e verifique com os e-mails válidos do mesmo remetente. Veja para onde os links direccionam - hiperlinks falsos são fáceis de detectar simplesmente colocando o cursor por cima deles (não clique no link!) Verifique a ortografia: os bancos têm equipes inteiras de pessoas qualificadas dedicadas a produzir comunicações com os clientes, por isso um e-mail com erros graves é provavelmente falso.

Solicitação de identificação

Não é comum em Angola, mas em muitos países, um dos ataques de engenharia social mais fácil é contornar a segurança para entrar num edifício, carregando uma caixa grande ou com as mãos cheias de arquivos. Isso é uma grande ideia, pois uma pessoa sempre o ajudará a manter uma porta aberta visto que está com as mãos ocupadas. Mesmo nesses casos, as empresas devem sempre instruir seus funcionários responsáveis por permitir o acesso de funcionários, a solicitar sempre a sua identificação.

Mesmo quando somos abordados, é importante verificar quem faz pessoas perguntas muito pessoais. É importante optar por uma resposta básica a esses pedidos de informação.

Conclusão

Ataques de engenharia social são difíceis de serem defendidos, pois, eles são criados para actuar nos comportamentos das pessoas como curiosidade, respeito pela autoridade ou pela vontade de ajudar outras pessoas.

Portanto, deve-se evitar divulgar sem nenhuma necessidade sua função e local de trabalho. E quando conversamos é importante tomar muito cuidado com o que responder quando questionados sobre a organização que prestam serviço ou sobre outros funcionários da instituição.

O sigilo de uma organização depende do esforço e do profissionalismo dos seus funcionários.