Acesse os informativos anteriores

ADVANCE GROUP
BECAUSE IT MUST BE A SOLUTION

Quanto vale a senha de um colaborador? Para um hacker, talvez milhões.

O Cavalo de Troia humano: o risco real do funcionário aliciado

A ameaça que explora a vulnerabilidade mais complexa e difícil de mitigar: o ser humano. Quando o *hacker* não invade, apenas recruta, o caminho é muito mais rápido e eficaz. Recentemente, **uma fraude milionária** no Brasil **não começou com um código malicioso complexo e usando inteligência artificial, mas com uma simples mensagem em uma rede social.** O que se seguiu foi um lembrete brutal de que **a maior vulnerabilidade de uma empresa, às vezes, tem crachá, nome, sobrenome e acesso legítimo à rede.**

Além do *firewall*: protegendo sua empresa de dentro para fora

- "Desconstruindo" a ameaça: não é o "*insider* típico", o clássico funcionário insatisfeito que age por vingança. O "*insider* aliciado" é uma vítima de engenharia social sofisticada, manipulação financeira ou até mesmo coação.
- Recrutados facilmente em redes sociais, alvos principais são colaboradores em posições chave ou que demonstram insatisfação.
- Abordagem inicial sutil por mensagens (Telegram, WhatsApp etc.), oferecendo dinheiro fácil por "pequenos favores" (ex: fornecer uma senha, plugar um *pendrive* etc.).
- Caso não seja detectada, a ação inicial pode evoluir para uma colaboração contínua, com

remuneração crescente e até mesmo com ameaças veladas.

A defesa começa fora da tecnologia: o fator humano

Certamente cada empresa pode definir as melhores formas de atuação junto aos seus colaboradores, contudo algumas sugestões podem ser úteis:

- **Os treinamentos devem ir além do "não clique aqui"**, para auxiliar o reconhecimento de abordagens de engenharia social, ofertas irrecusáveis, táticas de pressão, responsabilidades cíveis e criminais etc.
- Manutenção de cultura de confiança e apoio, na qual o colaborador se sinta seguro para relatar abordagens suspeitas sem receios, se necessário através de canais confidenciais.
- Capacitar os gestores a identificar sinais de alerta comportamentais (mudança de comportamento, estresse incomum, desengajamento etc.).

Nosso foco é a segurança!

A metodologia da Advance viabiliza a rápida detecção de qualquer comprometimento na cibersegurança e é baseada no princípio do menor privilégio (*Zero Trust*): mesmo que o aliciamento viabilize a invasão, o dano é contido por políticas de segurança que limitam os acessos, e os *backups* 100% seguros garantem a recuperação.

At.,
Nilton Teixeira
https://www.advancegroup.com.br
Microsoft Partner ID 3288934
Segurança nunca é demais!

ADVANCE GROUP
BECAUSE IT MUST BE A SOLUTION

Acesse os informativos anteriores