Por **Eduardo Person Pardini, CICP, CCoAudExp** (artigo escrito com ajuda da inteligência humana)

O poeta grego Homero, na Ilíada, conta que Troia resistiu por dez anos ao cerco grego. Suas muralhas eram consideradas intransponíveis. A cidade não caiu porque alguém derrubou os muros, e sim porque os próprios troianos abriram os portões e puxaram o cavalo de madeira para dentro.

Três mil anos depois, a dinâmica nas organizações continua exatamente a mesma.

Nas minhas andanças, vejo empresas investindo pesado em firewalls, criptografia, antivírus de última geração e ferramentas de monitoramento. O cavalo de Troia moderno, no entanto, não é de madeira. É um e-mail urgente do “diretor financeiro” pedindo uma transferência. É um link de “atualização cadastral” do banco. E, cada vez mais, é um vídeo com a voz e o rosto de um executivo gerados por inteligência artificial.

Na tríade clássica de segurança, a tecnologia faz o trabalho de fundação. Na prevenção, exige-se autenticação em múltiplos fatores e rigor no princípio do menor privilégio. Na detecção, ferramentas acusam acessos indevidos em tempo real. Na contingência, backups atualizados e planos de resposta a incidentes garantem a sobrevivência dos dados.

Tudo isso é o equivalente a "trancar o cofre". Mas não adianta trancar o cofre e deixar a chave pendurada na porta.

A engenharia social funciona porque explora a pressa, o medo e o respeito à hierarquia. Assim como escrevi no artigo sobre compliance, a cibersegurança precisa sair do campo do TER para o campo do SER.

Quando separamos o fator humano da tecnologia, fica evidente que o comportamento é o fiel da balança em cada uma das etapas críticas da segurança:

Treinamentos anuais maçantes não funcionam. A verdadeira prevenção humana exige a criação de uma cultura de conscientização contínua. O objetivo é desenvolver no colaborador um ceticismo saudável e automático. Ele precisa ser treinado para desconfiar do "urgente", do "confidencial" e das quebras repentinas de processo, blindando sua mente contra os gatilhos psicológicos que os atacantes usam para forçar o erro.

A tecnologia alerta sobre anomalias no sistema, mas só o ser humano percebe sutilezas de contexto. Um funcionário bem treinado é o sensor mais sofisticado de uma organização. Ele nota quando o tom do e-mail do chefe está estranho, quando um fornecedor subitamente muda o jargão de cobrança ou quando um pedido foge à normalidade da empresa. O ser humano detecta o que os filtros lógicos deixam passar.

Durante um ataque de ransonware ou vazamento de dados, o pânico é o maior inimigo. Trabalhar o fator humano na contingência significa garantir que as pessoas saibam operar no caos. Isso envolve simulações de crise corporativa para que todos saibam exatamente como se comunicar, quem acionar e como tomar decisões racionais, evitando que o desespero piore o impacto do incidente.

Assim como os nudges que comentei no artigo sobre compliance, o design do ambiente pode tornar o comportamento seguro o caminho mais natural. Um aviso automático de “este e-mail veio de fora da organização”. Uma regra inegociável de confirmar, por telefone e com um número já cadastrado, qualquer pedido de alteração de dados bancários de fornecedores. Uma pausa obrigatória antes de aprovar transferências acima de determinado valor.

Neste cenário, a Auditoria Interna não pode se limitar a verificar se o antivírus está instalado ou se

os acessos foram revogados. Atuando como Trusted Advisor, a auditoria precisa avaliar a prontidão cultural e comportamental da organização.

Isso se traduz em três atuações práticas:

Auditar a Segurança Psicológica: O funcionário que clicou no link malicioso precisa se sentir seguro para avisar imediatamente. Se a cultura é de punição, ele esconderá o erro, dando ao atacante horas preciosas para se espalhar. A auditoria deve questionar a liderança: nossa cultura encoraja o relato rápido ou promove o constrangimento?

Validar a "Fricção Positiva": O design dos processos deve tornar o comportamento seguro o caminho mais natural. A auditoria deve verificar se existem regras inegociáveis, como a pausa obrigatória para aprovação de transferências ou a exigência de confirmação por voz para mudanças de dados bancários. São pequenas fricções que salvam patrimônios.

Avaliar a Realidade da Contingência: Um plano de contingência não testado é apenas uma intenção. A auditoria deve avaliar se as pessoas realmente participam dos testes de resposta a incidentes e se estão psicologicamente preparadas para operar os controles quando a pressão aparecer.

A tecnologia protege os sistemas. As pessoas protegem a organização. Troia não precisava de muralhas mais altas. Precisava de alguém que perguntasse o que havia dentro do cavalo antes de abrir os portões.

E na sua organização, quando foi a última vez que a auditoria avaliou o plano de resposta a incidentes, e não apenas a existência do antivírus?

Seja feliz!

(12.11.2026)