1.Security awareness

Imagine que você trabalha em uma empresa e quer saber quantos funcionários clicariam em um link de phishing dentro de um e-mail corporativo. Para descobrir isso, é possível realizar uma campanha de phishing interna. Isso pode ser feito por meio de um sistema de phishing próprio ou utilizando serviços terceirizados que fornecem essa funcionalidade. Essas campanhas automatizadas registram aberturas, cliques e interações com os e-mails fraudulentos em um painel de controle centralizado.

Se um usuário clicar no link de phishing, ele recebe um e-mail automático informando sobre o erro e pode ser direcionado para um treinamento adicional. Esse treinamento pode ser feito online ou presencialmente nas instalações da empresa. O objetivo é educar os funcionários para reconhecer sinais de phishing, como erros ortográficos e gramaticais, domínios suspeitos e anexos incomuns. Além disso, é fundamental que os funcionários nunca cliquem em links ou executem anexos de e-mails não verificados.

A empresa também deve garantir que seus filtros de e-mail estejam funcionando corretamente para bloquear tentativas de phishing antes que cheguem às caixas de entrada dos funcionários. Caso um e-mail suspeito seja recebido, deve haver um processo claro para que os funcionários possam reportá-lo à equipe de segurança de TI.

Além do phishing, a equipe de segurança deve monitorar comportamentos anômalos dentro da rede corporativa. Isso pode incluir modificações inesperadas em arquivos do sistema operacional, login de usuários a partir de locais incomuns ou um aumento repentino na transferência de dados. Algumas ações podem ser não intencionais, como digitar o domínio errado de um site ou perder um dispositivo USB, mas ainda assim precisam ser monitoradas.

Para garantir a segurança, é essencial um processo automatizado de monitoramento, alertas e relatórios. Isso inclui o rastreamento da taxa de cliques em links maliciosos, o uso de gerenciadores de senhas e a adoção de autenticação multifator. Quando um funcionário comete um erro de segurança pela primeira vez, ele deve receber treinamento para evitar que aconteça novamente. Se o comportamento se repetir, medidas adicionais podem ser tomadas, como ajustes nas configurações de segurança desse usuário.

A equipe de conscientização de segurança desempenha um papel crucial, criando materiais educativos, treinamentos e campanhas para manter os funcionários informados sobre ameaças cibernéticas. Essa equipe pode adaptar treinamentos específicos para diferentes funções dentro da empresa e acompanhar métricas detalhadas para avaliar a eficácia das estratégias de segurança. O objetivo é garantir

que a segurança da organização seja constantemente aprimorada com base em dados e evidências.

Esses esforços podem ser vistos no ambiente de trabalho por meio de treinamentos presenciais, cartazes informativos e campanhas internas de segurança. Como todas essas ações geram métricas detalhadas, os gestores podem correlacionar os treinamentos com melhorias na segurança da empresa.