1.User training

É uma boa prática fornecer treinamento de segurança para os usuários antes que eles se conectem à rede da empresa pela primeira vez. Esse treinamento geralmente é especializado, pois diferentes departamentos podem ter requisitos distintos. Por exemplo, o setor de contabilidade pode precisar de diretrizes diferentes do setor de expedição e recebimento. Além disso, é importante considerar terceiros, como contratados, parceiros e fornecedores, que também podem precisar de treinamento adequado.

Manter um registro de quem já foi treinado e quem ainda não recebeu o treinamento ajuda a garantir que todos tenham um conhecimento básico de segurança da informação. Além disso, é essencial documentar todas as políticas de segurança e torná-las acessíveis, seja online no intranet corporativo ou no manual do funcionário.

Os usuários também devem estar atentos a ameaças de segurança em suas atividades diárias. Eles devem ser treinados para identificar e-mails de phishing, verificando erros ortográficos, URLs suspeitas e anexos incomuns. Além disso, é preciso estar atento a ataques físicos, como a recepção de dispositivos USB desconhecidos, que podem estar contaminados com malware.

Embora os funcionários possam ser uma forte linha de defesa contra ameaças, eles também podem representar riscos internos. Identificar ameaças internas é um grande desafio e exige múltiplas camadas de segurança. Algumas estratégias incluem a exigência de aprovações duplas para alterações críticas no sistema, monitoramento ativo de arquivos e a implementação de barreiras que dificultem contornar os sistemas de segurança.

A gestão de senhas também é um fator essencial para a segurança. Políticas de senhas fortes podem ser aplicadas administrativamente, como no ambiente Windows, onde é possível impor requisitos de complexidade por meio de diretivas de grupo. Além disso, os funcionários devem ser orientados a evitar o uso de mídias removíveis não verificadas, pois dispositivos USB podem ser vetores de malware. Também é importante alertá-los sobre o risco de usar cabos desconhecidos para carregar dispositivos móveis em locais públicos.

Os ataques baseados em engenharia social são uma ameaça significativa, e os usuários devem estar cientes das técnicas mais comuns utilizadas pelos invasores. Eles precisam ser treinados para reconhecer e reportar tentativas de engenharia social à equipe de segurança de TI. O ideal é que os funcionários desenvolvam um nível básico de segurança operacional, adotando uma mentalidade de defesa sob a perspectiva do atacante.

Muitos funcionários lidam com grandes volumes de dados, e é essencial que saibam diferenciar informações sensíveis e garantir sua proteção. O trabalho

remoto adiciona desafios adicionais, como o risco de compartilhamento de dispositivos com familiares ou amigos. Para mitigar esses riscos, podem ser implementadas soluções de segurança em endpoints e políticas rigorosas para acesso via VPN.

Essas práticas ajudam a fortalecer a postura de segurança da empresa e a reduzir vulnerabilidades tanto dentro quanto fora do ambiente corporativo.