1.Tipos de ameaças

Ameaças podem ser divididas em: ameaças não humanas e ameaças humanas. Para determinar as ameaças, profissionais de segurança da informação frequentemente irão se referir a listas padrões de ameaça. Essas listas são baseadas nas melhores práticas e em experiências prévias. É necessário determinar quais ameaças são relevantes e quais não são. A segurança, afinal de contas, exige que as organizações gastem dinheiro e não é sensato investir em segurança contra ameaças que não vão realmente acontecer

2.Ameaças humanas

2.1 Intencional

As pessoas podem intencionalmente causar danos a sistemas de informação por várias razões. Normalmente pensamos em intrusos, tais como um hacker que tem algo contra a empresa e deseja invadir e causar danos a ela. Engenharia social busca explorar a falta de consciência sobre segurança dentro de uma organização. Usar as expressões corretas ou nomes de pessoas conhecidas e seus departamentos dá a impressão de que se é um colega. Agir de forma educada e parecer confiável pode dar ao “colega” a oportunidade de obter segredos comerciais e da empresa. Um engenheiro social tira proveito dos pontos fracos das pessoas para concretizar seus objetivos. A maioria das pessoas não sabe o que é engenharia social e não reconhece um engenheiro social.

2.2 Não intencional

As pessoas também podem causar danos de forma não intencional. Por exemplo, pressionando acidentalmente o botão "delete" e confirmando de forma descuidada com OK. Além disso, em pânico, você pode usar um extintor de pó para apagar um pequeno incêndio e, de segurança, são aplicadas de maneira inadequada ou subvertida.

3.Ameaças não humanas

Existem também eventos não humanos que ameaçam uma organização. Estes incluem influências externas, tais como raios, incêndios, inundações e tempestades. Grande parte dos danos causados dependerá da localização do equipamento nas instalações. Podemos subdividir as ameaças humanas e não humanas em interrupções na infraestrutura básica, tais como equipamentos, software ou bases de dados computacionais, e perturbações no ambiente físico, tais como edifícios, arquivos em papel, instalações elétricas, abastecimento de água, aquecimento, ventilação e refrigeração.

4.Tipos de danos

Danos resultantes da ocorrência das ameaças citadas anteriormente podem ser classificados em dois grupos: danos diretos ou indiretos. Um exemplo de dano direto é o furto. O furto tem consequências diretas no negócio. Outro exemplo é o dano causado pela água dos extintores de incêndio. Dano indireto é a perda consequente que pode ocorrer. Um exemplo de dano indireto é ser incapaz de atender a um contrato devido à infraestrutura de TI ter sido destruída pelo fogo ou a perda de boa vontade por uma falha não intencional em cumprir as obrigações contratuais.

5.Tipos de riscos

Podemos lidar com os riscos de diferentes formas. As estratégias mais comuns são: tolerância ao risco (aceitação); redução/mitigação do risco; prevenção do risco.

Tolerância ao risco significa que certos riscos são aceitos. Isso pode acontecer porque os custos das medidas de segurança excedem o possível dano. As medidas que uma organização que tolera riscos toma na área de segurança da informação são geralmente de natureza repressiva.

Redução/mitigação do risco significa que medidas de segurança são tomadas de forma que as ameaças não mais se manifestam ou, se o fizerem, o dano resultante é minimizado. A maioria das medidas tomadas na área de segurança da informação por uma organização que neutraliza os riscos é uma combinação de medidas preventivas, de detecção e repressivas.

Prevenção do risco significa que medidas são tomadas de modo que a ameaça seja neutralizada, de tal forma que não leve mais a um incidente. Considere, por exemplo, as atualizações de software de um sistema operacional. Ao atualizar o SO assim que as atualizações estiverem disponíveis, você está prevenindo o seu sistema contra problemas técnicos conhecidos ou questões de segurança. Muitas das contramedidas nessa estratégia possuem um caráter preventivo. Independentemente da estratégia que uma organização escolhe, a administração tem que tomar uma decisão consciente e arcar com as consequências.