SI – Segurança da Informação

PROF. ANDERSON VANIN

Problemas de segurança da informação

Em segurança de informação, a palavra Ativo refere-se a tudo que representa valor para a organização. Caso esse ativo seja violado, poderá trazer impactos negativos para o prosseguimento das atividades da organização.

Podemos citar como ativos as pessoas, os programas, os equipamentos, enfim, tudo que na sua ausência gera transtornos, implicando no bom funcionamento dos negócios.

Problemas de segurança da informação

Quando falamos em problemas de segurança, há inúmeros fatores que acarretam a perda e/ou violação dos dados de uma empresa, como por exemplo, a má operação do sistema ou mesmo quando a segurança está sofrendo ameaça, risco, vulnerabilidade, falhas e desastres. A seguir abordaremos cada um desses fatores.

Ameaças

Quando um ativo da informação sofre um ataque potencial, podemos entender como ameaça. Este ataque poderá ser efetuado por agentes externos (empresas, pessoas que não são funcionários da organização) ou internos (pessoas pertencentes à organização), se prevalecendo das vulnerabilidades apresentadas no sistema empresa.

Ameaças

As vulnerabilidades são mais nítidas em sistemas de informação online e nos sistemas que utilizam os recursos das telecomunicações, por interligarem seus sistemas em vários locais, as chamadas intranets ou mesmo as extranets. Nesses casos, a exposição é muito grande, pois as ameaças aumentam substancialmente, uma vez que o sistema da empresa está na rede Internet. Muitas pessoas tentarão acessar informações mesmo sem autorização, se houver falhas de segurança.

Ameaças

Esses sistemas que utilizam esses novos padrões de rede ampliam consideravelmente as vulnerabilidades, uma vez que a comunicação pode ser feita também pelas redes de dados sem fio, que por sua vez são difíceis de serem protegidas em virtude dos vários pontos de acesso, possibilitando ainda mais a quebra da confidencialidade das informações.

As redes empresariais precisam de muitos recursos tanto físicos como lógicos para proteger seus ativos das ameaças e fraquezas.

Existem diversos tipos de ameaças, Sêmola (2003) classifica-as em categorias, a saber:

Ameaças

Naturais: decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição.

Involuntárias: são inconscientes, podendo ser causadas por acidentes, erros, falta de energia etc.

Voluntárias: são propositais, causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de malwares, incendiários etc.

Riscos

- Ao acessar a Internet, sua máquina já está exposta na rede, você poderá ter seus dados pessoais expostos, e caso sejam acessados por alguém mal intencionado, isso poderá lhe proporcionar grandes transtornos.
- Um exemplo que tivemos aqui no Brasil foi o ataque ao site do governo federal, os sites presidencia.gov.br e o brasil.gov.br, deixando-os indisponíveis em função da grande quantidade de acessos, esses acessos poderiam estar sendo feitos pelo seu computador também, os chamados ataques de spam.

Riscos

- Para as empresas todo ativo apresenta algum risco para a organização, podendo gerar um impacto grande ou pequeno aos negócios. Para isso, é necessário fazer um levantamento dos ativos e classificá-los quanto aos riscos, de forma que a facilitar a implementação de uma política de segurança mais eficiente.

Vulnerabilidades

Podemos entender por vulnerabilidades as falhas que um sistema possui, podendo provocar a indisponibilidade das informações, ou até mesmo a quebra do sigilo e alteração sem autorização, podendo ser decorrente de uma série de fatores, como falta de treinamento, falta de manutenção, falha nos controles de acesso, ausência de proteção de uma determinada área ameaçada. Por exemplo, a criação de contas no sistema sem especificar as restrições e permissões.

Vulnerabilidades

Podemos classificar as vulnerabilidades em três categorias:

- **Tecnológicas**: compreendem as redes de computadores, os computadores, ameaças por vírus, hacker, enfim, todas as atividades que envolvem tecnologia.
- **Físicas**: representadas pelo ambiente em que se encontram os computadores e periféricos. Exemplo: ausência de gerador de energia, normas para senhas, entre outros.
- **Humanas**: esta categoria envolve o fator humano, considerada a mais difícil de avaliar, por envolver características psicológicas, emocionais, socioculturais, que variam de pessoa para pessoa. Exemplos: falta de treinamento, qualificação, ambiente organizacional inapropriado para desenvolvimento das atividades etc.

Falhas

É quando um sistema permite a quebra de alguns dos princípios da segurança da informação. Essas falhas podem ser humanas ou não, intencionais ou não. Mas a maioria dos problemas de segurança da informação está basicamente relacionada às falhas oriundas das fases de implantação e desenvolvimento de uma política de segurança.

Falhas

Nesse sentido, podemos citar algumas falhas bastante comuns que ocorrem em virtude dessas dificuldades, sendo elas: inexistência de uma política de segurança formalizada, gerenciamento dos acessos efetuados no sistema, backups atualizados, treinamentos e informativos aos usuários sobre como explorar com segurança os recursos tecnológicos e, não menos importante, a definição de uma gerência de Tecnologia da Informação – TI para implementar as regras e fazê-las vivas na empresa.

Atividades

1. O que você entende por ativo de uma empresa? Explique.

2. Os incidentes em uma empresa ocorrem quando uma e/ou várias ameaças exploram os pontos fracos da mesma, seja intencionalmente ou não. Cite quais os princípios da segurança da informação foram violados.

3. Quando um ativo da informação sofre um ataque potencial podemos entender como ameaça. Esse ataque poderá ser efetuado por agentes externos ou internos diante das vulnerabilidades apresentadas no sistema da empresa. Como as ameaças podem ocorrer?

Atividades

4. Cite alguns riscos aos quais as pessoas estão sujeitas ao utilizar a Internet.

5. Leia as afirmações e assinale a alternativa correta.

a) Quando os princípios da segurança da informação são violados e há interrupção dos processos normais de negócio, denomina-se Incidente.

b) Ativo é conhecido como tudo que tem valor para a organização e, uma vez violados, não trarão impactos relevantes para a empresa.

c) As falhas podem ser apenas humanas e causadas de forma intencional.

d) Quando as atividades são interrompidas na empresa em decorrência de um furacão, essa interrupção é entendida como risco.

6. Explique a importância de um Plano de Recuperação de Desastre para as empresas.