Professor
Edson Pedro FERLIN

Infraestrutura de TI

Segurança da Informação

Prof. Edson Pedro Ferlin

Professor
Edson Pedro FERLIN

Infraestrutura de TI

Segurança Física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, algo que possa danificar a parte física da segurança, acesso indevido de estranhos (**controle de acesso**), forma inadequada de tratamento e manuseio do veículo.

Segurança Lógica (Cybersegurança)

Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backup* desatualizados, violação de senhas, furtos de identidades, etc.
Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação.

Vulnerabilidades

Ameaças

As ameaças são todas as situações que colocam em causa a Segurança da Informação.

Uma ameaça pode ser qualquer ação, acontecimento ou entidade que age sobre um ativo ou pessoa, por meio de uma vulnerabilidade e consequentemente gera um determinado impacto.

Ataques

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.

Tipos de Ameaças

Naturais	são decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc
Involuntárias	são inconscientes, podendo ser causadas por acidentes, erros, falta de energia, etc
Voluntárias	são propositais, causadas por agentes humanos como *hacker, cracker*, invasores, espiões, ladrões, criadores e disseminadores de *malwares*, incendiários, etc

Classificação das Ameaças

Físicas	são decorrentes de fenômenos da naturais
Tecnológicas	são ataques propositados causados por agentes humanos como hackers, invasores, criadores e disseminadores de vírus, mas também por defeitos técnicos, falhas de *hardware* e *software*
Humanas	são consideradas as mais perigosas, podendo ser casos de roubos e fraudes causados por ladrões e espiões

Vulnerabilidade

Refere-se à incapacidade de suportar os efeitos de um ambiente hostil.

É uma fraqueza que permite que um atacante reduza a garantia da **informação** de um sistema.

Ações

É a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças [ISO 27002].

As vulnerabilidades devem ser gerenciadas (identificadas e corrigidas).

Classificação das Vulnerabilidades

- **Tecnológicas**
- **Físicas**
- **Naturais**
- **Humanas**

Tecnológicas

Compreendem as redes de computadores, os computadores, ameaças por vírus, *hacker, cracker*, ou seja, 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

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.

Naturais

São situações decorrentes de fenômenos da natureza.

Exemplo: incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.

Infraestrutura Tecnológica

A vulnerabilidade da infraestrutura tecnológica de *hardware* e *software* é outro fator agravante, pois esses sistemas podem ser danificados e os equipamentos também são muito visados por ladrões por serem portáteis e atraírem a atenção de *crackers*, espiões ou empregados dispostos a trocar os seus privilégios em troca de dinheiro ou vantagens oferecidas por um concorrente.

Sistemas Web

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.

Catálogo de Vulnerabilidades

Conforme ISO 27005 tem-se:

a. vulnerabilidades de hardware;
b. vulnerabilidades de software;
c. vulnerabilidades de rede;
d. vulnerabilidades de pessoal;
e. vulnerabilidades de instalações e
f. vulnerabilidades da estrutura organizacional

Professor Edson Pedro FERLIN

Infraestrutura de TI

Áreas e Aspectos

a. organização;
b. processos e procedimentos;
c. rotinas gerenciais;
d. pessoal;
e. ambiente físico;
f. configurações de sistemas de informação;
g. hardware, software e equipamentos de comunicação;
h. dependências de parceiros externos.

Professor Edson Pedro FERLIN

Infraestrutura de TI

Segurança da Informação

Na publicação (**A Segurança da Informação é uma realidade nas empresas?**)
(link: http://professorferlin.blogspot.com/2016/04/a-seguranca-da-informacao-e-uma.html)
temos uma reflexão sobre os aspectos relativos à segurança da informação nas empresas.

Segurança da Informação

É a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios [ISO 27002].

SEGURANÇA DE DADOS

Segurança de dados é a prática de proteger dados armazenados contra acesso, uso, modificação, destruição ou exclusão não autorizados.

É um nível de segurança da TI que se preocupa em proteger armazenamentos de dados, repositórios de conhecimento e documentos.

Malware (aplicativos maliciosos)

É o termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.

Cavalo de Tróia

É um programa, normalmente, recebido como um "presente" (jogo, protetor de tela e etc), que além de executar funções para as quais foi aparentemente projetado, também, executa outras funções maliciosas e sem o conhecimento do usuário.

Backdoor

É uma rotina/programa que facilita o acesso ao um sistema computacional comprometido, utilizando serviços criados ou modificados para este fim.

Adware

É um tipo de *software* especificamente projetado para apresentar propagandas, seja por meio de um *browser*, seja por meio de algum outro programa instalado.

Spyware

É o termo utilizado para se referir a uma grande categoria de *software* que tem por objetivo monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Keylogger

É um programa que duplica o que é digitado pelo usuário. Um arquivo é gerado e enviado para o invasor ou para um servidos de arquivos.

Screenlogger

É um programa que coleta as informações na forma de imagem a região clicada pelo usuário.

Vírus

É um programa ou parte de um programa que se propaga infectando, isto é, inserindo cópias de sí mesmo e se tornando parte de outros programas e arquivos.

O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Worm

É um programa independente com capacidade de se auto-propagar pelas redes, enviando cópias de sí mesmo de computador para computador, explorando vulnerabilidade de programas e sistema ou falhas na configuração de *software* instalado.

O *worm* não é um vírus, pois não embute cópias de sí mesmo em outros programas ou arquivos e não necessita ser executado para se propagar.

Spam

É o termo usado para se refeir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.

Hoax (Boato)

É *e-mail* que possui conteúdo alarmante ou falsos e que, geralmente, tem como remetente ou apontam como autora da mensagem alguma instituição, empresa ou órgão governamental.

Phishing

É o termo criado para descrever qualquer ação maliciosa que tenha como objetivo obter dados pessoas e financeiros do usuário.

As técnicas *phishing* dão-se por meio do envio de mensagens não solicita, se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas falsificadas, projetadas para furtar dados.

Pharming

É a técnica que utiliza o sequestro ou a "contaminação" do DNS (*Domian Name System*) para levar os usuários a um *site* falso, alterando o DNS do *site* de destino.

Os *sites* falsificados coletam números de cartões de crédito, nomes de contas, senhas e números de documentos.

Isso é feito por meio da exibição de um *Pop-up* para roubar informação antes de levar o usuário ao *site* real.

Engenharia Social

É a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo.

É uma técnica utilizada pelo atacante para obeter informações pessoas de um usuário.

Principais Riscos às Coorporações

Roubo de Dados

É preciso monitorar constantemente o tráfego de informações dentro da empresa para evitar que quaisquer dados possam ser subtraídos e garantir que ninguém de fora teve acesso.

Sequestro de Dados

Os ***ramsomware*** são vírus que não têm como objetivo destruir qualquer dado, mas sim sequestrar as informações e só liberá-las mediante um pagamento — geralmente em *Bitcoins*, por não ser rastreável.

A melhor forma de evitar esse tipo de situação é realizar *backups* constantes de todos os dados da empresa. Assim, caso a infraestrutura seja sequestrada, basta restaurar a cópia e não pagar nenhum tipo de resgate aos criminosos.

Espionagem Industrial

Permitir que os projetos autorais de seu cliente acabem vazando compromete totalmente a capacidade de se manter competitivo e faz com que ele perca receita.

Para evitar que esse tipo de situação venha a acontecer é preciso criar políticas rígidas de acesso, restringindo a visualização de determinados dados apenas a pessoas autorizadas.

Software desatualizado

Um risco existente em praticamente todas as empresas é a utilização de *software* desatualizado e legados, sendo uma das principais portas de acesso para que *hackers* consigam ter acesso aos dados de um negócio.

Essa situação expõe a empresa por meio de sistemas que mantêm erros de código e problemas de segurança não resolvidos.

Colaboradores

Um dos maiores riscos dentro de uma empresa é o próprio colaborador.

A falta de instrução sobre segurança da informação e de uma política bem definida pode ser muito prejudicial para o negócio.

Dispositivos Móveis (*Smartphone*)

Os *smartphones* tornaram o acesso aos mais variados serviços na ponta do dedo em um *click*, contudo a disseminação da utilização dessa tecnologia traz uma série de cuidados e de responsabilidades para os usuários.

Eles são suscetíveis às ameaças cibernéticas da mesma forma que os computadores, e com um agravante que eles podem ser roubados/extraviados, deixando à *mercê* de pessoas estranhas.

Política de Segurança da Informação

"Uma Política de Segurança da Informação é um documento que deve descrever as práticas que a organização espera que sejam seguidas por todos os empregados para proteger seus ativos de informação"

Scott Barman
Information Security and Systems Architecture Analyst

Importância PSI

- Comunicar os objetivos e as diretrizes da segurança da informação;
- Garantir a implementação apropriada de controles de segurança;
- Demonstrar o compromisso e apoio da alta administração;
- Evitar problemas legais (indenizações, multas);
- Alcançar um nível de segurança consistente evitando esforços segmentados.

Diretriz

É um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos.

As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações.

Objetivo – ISO 27002

Uma política de segurança da informação tem como objetivo prover uma orientação e apoio da alta administração para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

LGPD – Lei Geral de Proteção de Dados

A LGPD regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil.

Válida para esferas privadas e públicas, a norma define os personagens do cenário digital, assim como suas responsabilidades e direitos.

Além disso, também dispõe sobre obrigatoriedades e penalidades

LGPD – Lei Geral de Proteção de Dados

Aprovada em julho de 2018 no Senado Federal, a LGPD foi sancionada em 14 de agosto pelo presidente Michel Temer.

Oficialmente nomeada Lei Nº 13.709, ela altera a Lei nº 12.965 – Marco Civil da Internet, que era de abril de 2014.

O principal objetivo da Lei Geral de Proteção de Dados é garantir mais segurança para empresas e consumidores por meio de uma gestão transparente de informações.

Contato

eferlin@live.com

(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.webnode.com.br

(YOUTUBE) ProfEdsonPedroFerlin