SEGURANÇA DA INFORMAÇÃO



SEGUNDA PARTE

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

VULNERABILIDADE

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Vulnerabilidade

Podem ser consideradas **Vulnerabilidades** as falhas, fraquezas e brechas inerentes de um elemento que constitui o sistema ou do sistema como um todo. *Pontos fracos* esses que podem ser explorados por algum *indivíduo mal intencionado*.

Vulnerabilidade

Os ativos de informação, que suportam os processos de negócio, possuem vulnerabilidades. É importante destacar que essas vulnerabilidades estão presentes nos próprios ativos, ou seja, que são inerentes a eles, e não de origem externa.

Vulnerabilidade

- Tecnologias:

Computadores são vulneráveis por serem construídos para troca e armazenamento de dados, seja por meio de disquetes, CD/DVD, portas USB ou porta de acesso à rede local e à Internet. Isto pode ser explorado por vírus, worms, cavalos de troia, negação de serviço, entre outras pragas virtuais.

Vulnerabilidade

- Tecnologias:

Cabos de rede, fibras óticas e redes wireless, por sua própria construção, possibilitam a interferência no sinal ou o acesso aos dados que neles trafegam.

Vulnerabilidade

- Tecnologias:

Aparelhos celulares podem ser facilmente roubados e/ou dados da agenda, mensagens e outras informações podem ser retiradas deles.

Vulnerabilidade

- Tecnologias:

Sistemas de informação permitem a entrada e consulta de informações valiosas e podem ser indevidamente acessados.

Vulnerabilidade

- Pessoas:

As pessoas, por natureza, tendem a divulgar informações de trabalho para outras pessoas em quem confiem, sejam da própria organização, de uma organização concorrente ou mesmo pessoas do círculo de amigos e/ou familiares.

Pessoas possuem sentimentos diversos, que podem ser explorados por técnicas de engenharia social.

Vulnerabilidade

- Processos:

Muitas vezes as organizações não constroem normas e regras explícitas para as relações dos colaboradores com as informações da organização.

Vulnerabilidade

- Processos:

As contratações, acompanhamentos e demissões de pessoal são desprovidos de procedimentos específicos que preservem a segurança da informação.

Vulnerabilidade

- Ambientes:

Os ambientes são suscetíveis a incêndios, enchentes, terremotos e outras catástrofes. Outra vulnerabilidade é o acesso, que eventualmente pode ser realizado por pessoa não autorizada.

É preciso dar a devida atenção as manutenções preventivas de hardware (limpeza), poluentes diversos podem danificar os equipamentos e meios de armazenagem.

Vulnerabilidade

Essas vulnerabilidades são inerentes aos ativos e não podem ser simplesmente eliminados, pelo menos não sem prejudicar o objetivo principal do ativo.

Vulnerabilidade

A questão fundamental é: mesmo que proteções tenham sido criadas para os ativos, suas vulnerabilidades continuam ali. Essas vulnerabilidades poderão ser exploradas ou não, ou seja, é possível que um ativo possua uma vulnerabilidade que nunca será efetivamente explorada.

Vulnerabilidade

Vídeo: Quais as vulnerabilidades em segurança mais comuns em um ambiente?

Duração: 02min e 06seg

Produção: BHS

Local: YouTube

Link:

https://www.youtube.com/watch?v=EDvqArdm67s

AMEAÇA

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Ameaça

Pode ser considerada uma **Ameaça** qualquer agente externo ao ativo da informação, que se aproveitando de suas vulnerabilidades, poderá quebrar a confidencialidade, integridade ou disponibilidade.

Ameaça

Alguns exemplos de ameaça são fraudadores, espiões, sabotadores, vândalos, sobrecargas no sistema elétrico (que podem causar incêndio), tempestades (que podem causar inundação), vírus, spywares, worms, entre outros.

Ameaça

Infelizmente, é fácil perceber que, pouco se pode fazer para diminuir ou acabar com as ameaças, ou porque são imprevisíveis ou porque estão realmente fora do nosso controle.

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

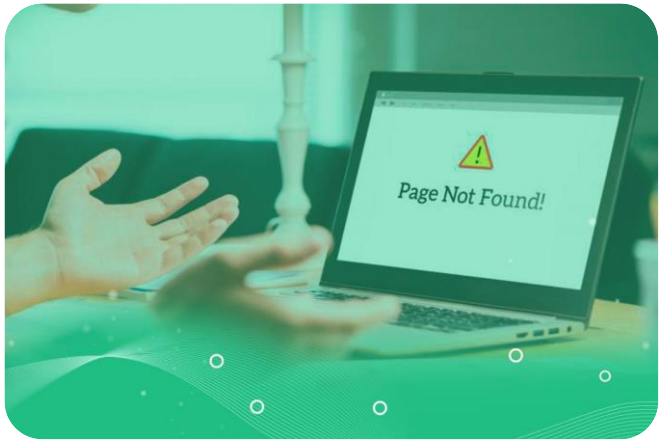
UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Incidente

Incidente de Segurança da Informação é a ocorrência de um evento que possa causar interrupções ou prejuízos aos processos do negócio, em consequência da violação de um dos princípios da *Segurança da Informação*.

Incidente

Se um vírus explora a vulnerabilidade de um servidor de serviços Web, deixando-o inoperante ou indisponível, isto gera um prejuízo ou um impacto para a organização. O mesmo se dá no caso de uma empresa concorrente (ameaça) conseguir convencer um colaborador (ativo) a passar informações confidenciais.



PROBABILIDADE

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Probabilidade

Probabilidade é a chance de um determinada falha de segurança ocorrer. **Probabilidade da Ocorrência:** Os dois fatores que contribuem para a probabilidade são Grau de Ameaça e Grau de Vulnerabilidade.

Probabilidade

Eventualmente pode haver vulnerabilidades em *ativos de informação*, mas sem aparentes *potenciais ameaças* que as explorem, ou casos em que a probabilidade de determinada ameaça *explorar uma vulnerabilidade* é muito pequena, próxima de zero.

Probabilidade

Existem as vulnerabilidades de *alto grau*, como uma rede local de computadores ligada à Internet, e as vulnerabilidades de *baixo grau*, como um armário sem tranca para guardar o backup na sala dos computadores servidores (datacenter).

IMPACTO

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Impacto

O impacto de um incidente refere-se aos potenciais prejuízos causados ao negócio por esse incidente. Esses prejuízos podem significar perdas financeiras, desgaste da imagem na organização perante o mercado ou perda de recursos e colaboradores, entre outros.

Impacto

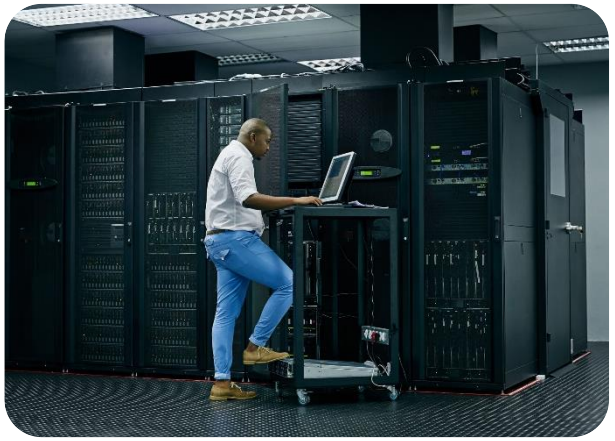
O impacto de um mesmo incidente pode ser diferente para organizações diferentes, dependendo de suas estratégias de negócio, dos processos afetados pelo incidente e da capacidade de resposta ao incidente que cada organização possua.

Impacto

Se o site na Internet de uma empresa vier a ficar fora do ar, que dano isto causará ao negócio? Depende da empresa. *Ela faz negócios através desse site?* Quanto o site representa para a imagem da empresa? Se for uma fábrica de calçados que não fecha negócios pela Internet, o impacto sobre o negócio será *relativamente pequeno*, mas se for um banco que disponibiliza suas operações de movimentação de contas através da Internet *o impacto será enorme*.

Impacto

Os ativos possuem valores diferentes, já que a informação que eles suportam ou utilizam tem relevâncias diferentes para o negócio da organização. Quanto maior for a relevância do ativo, tanto maior será o impacto de um eventual incidente. É preciso definir o grau do impacto ou do dano para cada eventual incidente de segurança da informação que possa ocorrer.



CONTROLE

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Controle

Controle é o *mecanismo* utilizado para diminuir a *Vulnerabilidade* de um *Ativo de Informação*. Seja esse ativo uma tecnologia, um processo, uma pessoa ou um ambiente.

Controle

As ameaças são agentes externos, que normalmente estão fora do nosso raio de ação, ao passo que as vulnerabilidades existem nos ativos, que geralmente estão dentro do nosso raio de ação.

Controle

Os esforços devem ser feitos para diminuir as vulnerabilidades e não as ameaças. De fato, a maior parte das medidas de segurança da informação resume-se a isso: *diminuir as vulnerabilidades dos ativos de informação.*

COMO GARANTIR A SEGURANÇA DA INFORMAÇÃO

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Garantias à Segurança da Informação

Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir essa segurança. Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados.

Garantias à Segurança da Informação

Muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema.

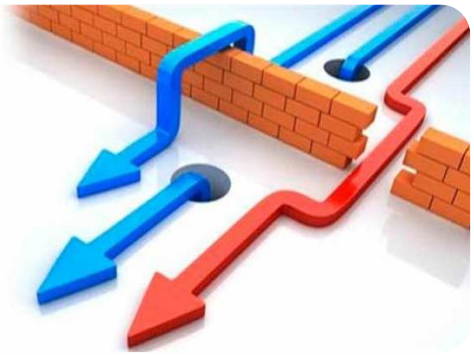
Garantias à Segurança da Informação

É importante saber entender os conceitos, tais como os de processos de negócio, retorno sobre investimento, fluxo de caixa, entre outros. Esses são componentes importantes para a segurança da informação, já que as ações nessa área objetivam preservar os investimentos da organização.

Parece que o pessoal executivo fala uma língua diferente daquela usada pelo pessoal da área técnica e dificilmente esses dois grupos chegam a um acordo sem antes gerar muito desgaste para ambos.

Garantias à Segurança da Informação

- Um **Plano de Continuidade de Negócios** (*BCP - Business Continuity Plan*) dá prioridades às funções de que uma organização precisa para se manter.
- Um **Plano de Recuperação de Desastre** (*DRP - Disaster Recovery Plan*) define como uma empresa retoma suas atividades após um grande desastre, como um incêndio ou um furacão.



ONDE INVESTIR

UNIFAI
Ciência da Computação
Prof. José Ricardo P. de Moraes

Investimentos

Quando se consegue algum investimento (sempre limitado), para investir em segurança, o que fazer? São muitas as possibilidades e não é raro encontrar os responsáveis pela segurança da informação imobilizados diante da indecisão.

Há muitos casos em que, mesmo após a implementação de algum recurso, os incidentes continuem ocorrendo. Em outros, a implementação acontece com algum sucesso inicial, mas com o passar do tempo, vão se perdendo e deixando de ser funcionais.

Investimentos

O melhor caminho é investir em mecanismos que diminuam as vulnerabilidades dos ativos de informação e, ainda, que esses mecanismos não deixem de funcionar adequadamente com o passar tempo.

A questão pode ser desafiadora, mas não insolúvel. E a solução precisa ser algo mais do que a implantação isolada de algumas tecnologias ou mesmo procedimentos.

Investimentos

Comprar os mais caros produtos de segurança da informação não garante bons resultados e, às vezes, pode até prejudicar seriamente os processos de negócio da organização. Um médico de verdade analisa o paciente, faz exames e só então estabelece um plano de ação completo para atacar a doença, com remédios que atuam de forma sinérgica objetivando a cura.

Investimentos

Um gerente de segurança da informação de verdade também trabalha com fatos, com resultados de análise e exames da organização em questão. A partir desses resultados, ele estabelece um conjunto de ações coordenadas no sentido de garantir a segurança da informação.

Um conjunto de ações, um conjunto de mecanismos integrados entre si, um sistema de segurança da informação, também conhecido como sistema de gestão de segurança da informação (SGSI).

Priorizando Investimentos em Segurança da Informação

Vídeo: Priorização de Investimentos e Ações em Segurança da Informação

Duração: 02min e 48seg

Produção: IGTI

Local: YouTube

Link:

https://www.youtube.com/watch?v=WqBqAmKJylQ