GTI - V - NOTURNO
ARTHUR OLIVEIRA, ISADORA SERRANO, JOÃO MOITA MATHEUS FERREIRA

SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO
GESTÃO DE RISCOS

Trabalho realizado como tema do projeto Integrador
do componente curricular de Segurança da Informação,
Ministrado pelo professor: **Kelly Alves**

Goiânia
2018

Implantação e Gestão de Segurança da Informação

Gestão de Riscos / Análise de Risco

Para implantar a gestão de segurança da informação em um ambiente corporativo, faz se necessário verificar os riscos que rondam o ambiente. Para esse fim, o COBIT, presente na governança de tecnologia da informação, implementa a gestão de risco, onde é feito o levantamento dos ativos críticos de risco de várias categorias, especificamente hardware e software.

Nesse documento serão levantados as vulnerabilidades, ameaças, impactos e o nível de risco oferecido a Loja Online. Abaixo serão levantados os principais riscos oferecidos ao hardware, software e a infraestrutura da Loja, assim como seus periféricos.

ANÁLISE DE RISCOS

ANÁLISE DE RISCOS				
Categoria	**Ativos Típicos**	**Vulnerabilidades**	**Ameaças**	**Impactos**
Software	Sistema Operacional	Senhas Frágeis	Invasão e exposição de dados	Edições desautorizadas e acesso por usuários desautorizados
		Firewall desabilitado, Sistema desatualizado	Infecção de vírus	Exclusão de dados
		Antivírus Inativo	Keyloggers, ScreenLogger, malwares	Exposição de dados, Acesso desconhecido, controle desautorizado
Software	Aplicação Web	Erro no código fonte	SQL Injection	exposição de dados sensíveis

		Configuração incorrecta da aplicação Web	Man in the middlle, Ransoware, DoS, DDoS	quebras no controle de acesso
Software	Banco de Dados	Banco de dados sem controle de acesso	Acessos desautorizados	Exposição de Dados; Inserção incorreta de dados
Hardware	Servidor	Antivírus não instalado ou desabilitado	ataque de negação de serviço DoS	Serviços Indisponíveis, Perda de arquivos
		Controle de acesso não implantado	Acesso público aos dados e serviços	Perda de arquivos, exposição de dados, configurações não autorizadas
		Proxy mal configurado ou desabilitado	Vírus, Malwares, Trojans	Serviços Indisponíveis, implantação de Backdoors
		Firewall desabilitado	Vírus, Malwares	Execução de processos involuntários, Infecção por vírus
Hardware	Roteador	Interface de linha de comando desprotegida	Inserção de comandos aleatórios, Invasão por vírus	Rede desconfigurada, Perda e descentralização de dados, Instalação de vulnerabilidades
		Firmware desatualizado	Invasão de Hackers, Instalação de vulnerabilidades	Configuração desautorizada no roteador, Queima de arquivo
Hardware	Switch	Mal configuração do switch	Configuração desautorizada, Ataque Man in the Middle	Serviços Indisponíveis

Infraestrutura	Rede	Porta de serviços aberta	Invasão de Hackers	Serviços Indisponíveis
		Servidor em local vulnerável	Ameaças Naturais (água, roedores, desgaste)	Rompimento dos cabos, queima de circuitos
Hardware	Computador	Antivírus desabilitado	Ameaças maliciosas	Perda de dados
		Firewall desabilitado	Infecção por vírus	Perda de arquivos, exposição de dados
		Erros Humanos	Vírus, trojans e malwares	Manipulações indevidas por terceiro no sistema
Software	Navegador	pop up desbloqueados	malwares	Infecções por vírus
		Armazenamento de senhas e dados de formulário em cache	Exposição de dados,vulnerabilidade de informações, acesso remoto desautorizado, ataque por *phishing*	Perda de dados, exposição de dados
Hardware	Roteador – Wifi	Senha Wi-fi compartilhada	Invasão de Hackers	Exposição de dados

Após as vulnerabilidades dos ativos serem levantados, assim como as ameaças e impactos, é preciso definir o nível do impacto e a probabilidade com que podem ocorrer, sucessivamente pode ser realizado um calculo para a definição dos riscos. Abaixo estão as legendas do índice de impacto, critério de probabilidade e impacto e o nível de risco.

LEGENDAS

Legenda índice de Impacto	
0	Irrelevante
1	Efeito pouco significativo
2	Sistemas não disponíveis por determinado período
3	Perdas Financeiras
4	Efeitos desastrosos, sem comprometimento dos negócios
5	Efeitos desastrosos, comprometendo os negócios

Critério de Probabilidade		
Probabilidade	Descrição	Peso
Alta	Tem ocorrido uma vez a cada duas semanas	3
Média	Tem ocorrido a cada seis semanas	2
Baixa	Ocorreu uma vez no ano	1

Critério de Impactos	
Alto	Vazamento de dados sensíveis
Médio	Na ocorrência seus prejuízos causarão grandes perdas financeiras
Baixo	Perdas de equipamentos de TI

Risco	
Altíssimo	>= 10
Alto	> 5
Médio	>3 <= 5
Baixo	<=2

MATRIZ RISCO X IMPACTO

Uma ameaça pode ter vários impactos, mas somente uma probabilidade, para se obter o nível de risco é preciso utilizar a seguinte formula:

Classificação de risco = Impacto * Probabilidade

Onde as ameaças possuem múltiplos impactos, a classificação de risco pode ser obtida apesar da seguinte formula: Risco = (impacto + impacto) * probabilidade.

Ameaças	Impacto	Probabilidade	Cálculo Risco = Impacto * Probabilidade	Classificação de Risco
Infecção de vírus	2	2	2*2=4	**Média**
Senhas Frágeis	3	2	2*2=5	**Média**
Keyloggers, ScreenLogger, malwares	3,5	1	(3+5) * 1 = 8	**Alto**
SQL Injection	2,3,5	1	(2+3+5)*1 = 10	**Altíssimo**
Man in the middle, DoS, DDoS	2,3,4,5	2	(2+3+4+5) * 2 = 28	**Altíssimo**
Acessos desautorizados	4,5	1	(4+5) * 1 = 9	**Alto**
Ransoware	2,3,4,5	1	(2+3+4+5) *1 = 14	**Altíssimo**
Vírus, Malwares, Trojans	2,4,5	2	(2+4+5) * 2 = 22	**Altíssimo**
Acesso público aos dados e serviços	2,3,4,5	3	(2+3+4+5) * 3 = 42	**Altíssimo**

Inserção de comandos aleatórios, Invasão por vírus	2,5	2	(2+5)*2=14	**Altíssimo**
Invasão de Hackers, Instalação de vulnerabilidades	2,3,4,5,	1	(2+3+4+5) * 1 = 14	**Altíssimo**
Ameaças Naturais (água, roedores, desgaste)	2,3,4,5,	1	(2+3+4+5) * 1 = 14	**Altíssimo**
Ameaças maliciosas	2,3,4,5,	2	(2+3+4+5+) * 2 = 28	**Altíssimo**
Exposição de dados, vulnerabilidade de informações, acesso remoto desautorizado, ataque por *phishing*	2,3,4,5	2	(2+3+4+5+) * 2 = 28	**Altíssimo**

MEDIDAS PARA CONTROLE DOS RISCOS BASEADO NA NORMA ISO/IEC - 27002:

1) Realizar backups incremental ou diferencial semanalmente de todos os arquivos armazenados;
2) Instalação de antivírus confiáveis, que possuam várias funções, filtros, proteção contra spams, analise de rede e trafego, escaneamento completo do sistema, etc.
3) Nunca desabilitar o firewall, caso esse bloquei algum arquivo, opte por criar uma regra de segurança, liberando somente a porta solicitada;
4) Sempre revisar a política de segurança, seja por período a cada nova suspeita de ataque;
5) Registrar todos os dados em um inventário, procurando sempre ter todos os itens documentados;
6) Quanto maior a complexidade e relevância dos arquivos maior deve ser o nível de segurança implantada;

7) Os riscos listados acima são podem possuir uma solução em comum, no entanto para riscos mais específicos, Ransoware, malwares, entre outros, devem ser tomadas medidas mais especificas, tais como:
    - Configuração e implantação de sensores de segurança IDS (Sistema de Detecção de Intrusos) e IPS (Sistema de Prevenção de intrusos). Esses quando utilizados em conjunto detectam e previnem a ameaça antes que essa ocorra;
    - Implantação ou virtualização de um servidor HoneyPot, onde as ameaças são redirecionadas para um falso servidor de serviços e essas são estudadas e eliminadas.
8) Manter dispositivos e ferramentas tais como, servidores, roteadores, switches e computadores em locais seguros e elevados, onde a luz do sol não peque diretamente, o local deve estar sempre seco, temperatura baixa e arejado, o que evita inundações, acumulo de poeira, infiltrações e superaquecimento dos equipamentos;
9) Utilização de sistemas de autenticação e logs de verificação de atividades de usuários, para fins de pericia e auditoria de processos. Essa medida quando aplicada estabelece o principio do não repúdio, onde todos os registros de atividades são armazenados em logs, assim como seus respectivos usuários;
10) Evitar entrar em sites de origem desconhecida ou sites que não possuem certificação HTTPS;
11) Não clicar em todo pop-up, ou mensagem que são enviadas via e-mails ou redes sociais ofertando prêmios ou convites suspeitos;
12) Não acessar redes desconhecidas, evitando assim ataques do tipo *man in the middle* e invasão através de redes falsas;
13) Procurar sempre um profissional de segurança certificado ou de confiança, quando preciso, evitando assim que pessoas mal intencionadas implantem *backdoors* ou outras vulnerabilidades;
14) Estabelecer mecanismos de controles, tais como, troca de senhas vulneráveis, backups semanais, firewall e antivírus sempre habilitados e desconfiar sempre de usuários e sites suspeitos.