Análise de Risco

Loja Virtual

Goiânia, Maio de 2018.

ANALISE DE RISCO DA LOJA VIRTUAL

Cliente

Loja Virtual

(Segurança da Informação)

Autores:

Desiron Filho e Jefferson Mendes

Versão: 1.0

OBJETIVO

A análise de riscos de segurança da informação é um método de identificação de riscos e avaliação dos possíveis danos que podem ser causados, a fim de justificar os controles de segurança. A análise de risco da informação possui três objetivos principais: identificar riscos, quantificar o impacto de possíveis ameaças e conseguir um equilíbrio financeiro entre o impacto do risco e o custo da contramedida.

LEVANTAMENTO DOS ATIVOS DA LOJA VIRTUAL

O levantamento dos ativos tem por objetivo listar todos os Hardwares e Softwares que acercam de processos e sistemas utilizados pela Loja Virtual de modo a explorar suas ameaças e impactos em relação às vulnerabilidades que podem ser encontradas no ambiente.

Gestão de Riscos (Loja Virtual)				
Ativos		Vulnerabilidades	Ameaças	Impactos
Hardware	Switch	Ataque DDoS	Perda de Pacotes	Lentidão nas respostas do site
	Nobreak	Ausência de Alimentação	Desligar o Servidor	Loja virtual indisponível.
	Servidor	Inoperância, não refrigeração do Servidor	Falha ou problemas técnicos, Super Aquecimento, Aumento na fila de espera de requisições	Parada inesperada do Servidor, perda de dados, dados corrompidos, Loja virtual Inacessível, Lentidão nas respostas do site
	Roteador	Falha na configuração	Falha na conexão com WAN	Loja virtual inacessível
	Firewall	Acesso não Autorizado Controle de Acesso, Controle de Uso	Acesso a dados internos	Prejuízo financeiro, acesso a informação indevida, perda de informação, perda do banco de dados, perda do serviço
Software	SO	SO desatualizado Metasploit	Invasão	Controle total do servidor
	Banco de Dados	Erro de Comunicação SQL Injection, Não acesso ao Banco de Dados	Acesso não autorizado ao Banco de Dados, perda de comunicação com banco	Comprometimento as funcionalidades da Loja Virtual
	Servidor Web	Falta de definição de uma configuração sólida do serviço	Indisponibilidade do Serviço	Loja virtual indisponível
	Servidor DNS	Envenenamento de DNS	Indisponibilidade do Serviço, roubo de DNS	A não de resolução de endereço da loja, dificuldade de acesso a loja, indisponibilidade de serviço
	Link de Internet	Falha de disponibilidade da operadora	Serviço de rede Indisponível	Loja virtual inacessível
	Serviço Loja Virtual	Captura de dados	Roubo de informações	Acesso a informações sigilosas, insegurança

ANÁLISE DE IMPACTOS

A análise de risco faz a classificação dos riscos de uma empresa levando em conta as necessidades da organização e seus modelos de estratégia. As duas principais classificações envolvem a chance de o risco ocorrer e a gravidade do seu impacto.

Classificação dos Índices das Ameaças

- 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

Riscos	Pesos
Irrelevante	0
Efeito pouco significativo	1
Sistemas não disponíveis por determinado período.	2
Perdas financeiras	3
Efeitos desastrosos, sem comprometimento dos negócios	4
Efeitos desastrosos, comprometendo os negócios	5

Matriz de Relacionamento		
Vulnerabilidades	Ameaças	Probabilidade
Ataque DDoS	2;3	10%
Ausência de Alimentação	2;3;5	15%
Inoperância, não refrigeração do Servidor	2;3;5	7%
Falha na configuração	2;3;4	3%
Acesso não Autorizado Controle de Acesso, Controle de Uso	1;2;3;4;5	20%
SO desatualizado Metasploit	1;5	2%
Erro de Comunicação SQL Injection, Não acesso ao Banco de Dados	1;4;5	4%
Falta de definição de uma configuração sólida do serviço	1;2	1%
Envenenamento de DNS	1;2	30%
Falha de disponibilidade da operadora	1;2	25%
Captura de dados	1;3;4;5	11%

CALCULO E CLASSIFICAÇÃO DE RISCO

Para calcularmos é necessário apresentar o referencial dos métodos utilizados nessa análise, além de atribuirmos de forma detalhada as variáveis utilizadas, as escalas de valores e a fórmula proposta para o cálculo do risco.

Para realizarmos o cálculo de risco trabalhamos com a multiplicação de 2 variáveis (Impacto) x (Probabilidade), como segue abaixo:

$$Risco = Impacto * Probabilidade$$

Classificação	
>2	Altíssimo
>=1,5 e <2	Alto
>=0,7 e <1,5	Médio
>=0,3 e <0,7	Baixo
>0,1 e <0,3	Baixíssimo
<0,1	Nenhuma

Classificação de Risco				
Vulnerabilidades	Peso	Probabilidade	Risco	Classificação
Ataque DDoS	5	19%	0,95	Médio
Ausência de Alimentação	10	15%	1,5	Alto
Inoperância, não refrigeração do Servidor	10	7%	0,7	Médio
Falha na configuração	9	3%	0,27	Baixíssimo
Acesso não Autorizado, Controle de Acesso e Controle de Uso	15	20%	3	Altíssimo
SO desatualizado Metasploit	6	2%	0,12	Baixíssimo
Erro de Comunicação SQL Injection, Não acesso ao Banco de Dados	10	4%	0,4	Baixo
Falta de definição de uma configuração sólida do serviço	3	1%	0,03	Nenhuma
Envenenamento de DNS	3	30%	0,9	Médio
Falha de disponibilidade da operadora	3	25%	0,75	Médio
Captura de dados	13	11%	1,43	Alto

MEDIDAS DE CONTROLE DE RISCOS

Após identificação dos riscos e seus impactos categorizamos os riscos de maior probabilidade e impacto sobre o negócio da ChambaryTek, dentre eles criamos medidas de controle desses riscos.

Ataque de DDoS - Uma das principais ações para o excesso de provisionamento de banda é a utilização de serviços de segurança escalável sob demanda que seja capaz de absorver e filtrar o tráfego DDoS. Esses serviços são projetados para parar ataques sem sobrecarregar as conexões, assim os usuários e clientes não são prejudicados com latência e indisponibilidade de aplicações.

Ausência de Alimentação – Como solução para tal indisponibilidade, optamos por construir uma rede estabilizada com o uso de nobreaks temporária para sustentar todo o sistema do servidor até que o nosso provedor de energia elétrica seja restabelecido. Caso esse prazo se delongue os geradores de energia a combustão assumiram e manterão sistema operante. Asseguramos também revisões preventivas de rotina nesse sistema para a garantia da disponibilidade desse serviço.

Inoperância, não refrigeração do Servidor – Para mantermos a ChambaryTek sempre operante, realizamos manutenções preventivas semanalmente do servidor e de seu ambiente com um checklist mensal e semanal a ser comprido. Nesse checklist estão vários itens que são estabelecidos pelo Gestor de TI, tais como: limpeza do ambiente do servidor, manutenção das condições do ar em baixa umidade e temperatura, testes de estresse entre outros.

Falha na configuração – Esse tipo de risco é pouco provável, pois no momento de implementação da Loja foram investidos em segurança e solidez no código fonte do sistema. Porém, a ChambaryTek conta com uma equipe de desenvolvedores pronta para tratar esse tipo problema e solucionar o quanto antes, devolvendo a disponibilidade do sistema ao cliente.

Acesso não Autorizado, Controle de Acesso e Controle de Uso – Contamos com uma equipe terceirizada que gerencia através de um sistema embarcado de firewall todas as movimentações na rede. Trata essas informações e efetua bloqueis caso seja necessário de IPs internos ou externos, bloqueis de MACs, leitura do tráfego, criptografia das transações entre outras informações.

SO desatualizado Metasploit – Para tratarmos esse risco, mantemos todos os nossos SOs dos servidores e colaboradores em dia com as atualizações do fabricante, evitando assim boa parte dos riscos com invasão através de Metasploit entre outras ferramentas.

Erro de Comunicação, SQL Injection e não acesso ao Banco de Dados – No momento de implementação da Loja, um dos principais pontos direcionas a atenção foi a respeito de SQL Injection, sendo assim estamos completamente assegurados pela equipe desenvolvedora sobre esse método de injeção.

Para garantirmos a comunicação com o banco de dados, utilizamos um server juntamente com o servidor oficial do site, assim conseguimos reduzir a latência na resposta evitando uma série falhas devida a disponibilidade do sistema. Caso esse servidor primário sofra com alguma queima inesperada, optamos por utilizar um espelhamento local do banco, e caso essa medida venha falhar também partiremos para o uso do banco de dados espelhado na nuvem.

Falta de definição de uma configuração sólida do serviço – Esse risco possui uma possibilidade muito baixa de vir ocorrer, mas para prevenir realizamos uma auditoria periódica ao serviço buscando sempre a otimização de parâmetros do serviço, atualizações dos repositórios e manter assim o serviço sempre atualizado.

Envenenamento de DNS – Para nos resguardamos desse risco, utilizamos um certificado SSL como proteção de fraude, das quais o cliente deverá ficar atento sobre essas informações da Loja. Outra medida protetiva é o

suo de um novo sistema antifraude chamado *DNSSEC,* onde na teoria, os servidores passam a ser à prova de envenenamento, já que o criminoso não conseguiria plantar um IP falso no DNS.

Falha de disponibilidade da operadora – Esse é um risco inerente do qual qualquer cliente da provedora estar suscetível a sofrer, contudo como solução caso ela venha ocorrer, optamos pelo uso de um segundo link de internet com uma provedora diferente, caso ocorra a falha o link secundário assumiria.

Captura de dados – Esse é um risco recorrente e mais comum que muitos achem o contrário, e para nos resguardamos utilizamos o certificado SSL, que criptografa os dados transacionados sendo mais um meio de impedir caso consiga capturar os dados.