Capítulo 5

Gestão de vulnerabilidades

Neste capítulo falaremos sobre a importância da segurança dos softwares de caráter preventivo. A gestão de vulnerabilidade trata deste assunto com a relevância que ele merece.

Quando concluímos um determinado desenvolvimento, fica evidente que a preocupação com a gestão de vulnerabilidade tem um papel importante no processo, pois os gastos dispendiosos no processo de correção das vulnerabilidades encontradas são muito maiores que aqueles empregados na prevenção dessas falhas (A. SILVA, 2008). Embora muitas organizações desprezem este processo de gestão de vulnerabilidade, as que estão preocupadas com este assunto estão à frente das demais por este simples mas eficaz processo.

Assim, ao longo deste capítulo abordaremos importantes questões relacionadas à gestão de vulnerabilidades, seus fundamentos, execução e elaboração de relatórios.

1 Fundamentos de gestão de vulnerabilidades

A vulnerabilidade de um sistema caracteriza-se por uma ou mais fragilidades de um ativo da organização que pode ser explorado por uma ou mais ameaças.

Para Baars et al. (2018), essa vulnerabilidade é apresentada como:

- Um serviço executado em um servidor.
- Aplicações ou sistemas operacionais não corrigidos.
- Acesso discado irrestrito, via modem.
- Uma porta aberta em um firewall.
- Segurança física fraca que permite que qualquer pessoa entre em uma sala de servidores.
- Um fraco gerenciamento de senha em servidores e estações de trabalho.

Ainda de acordo com os autores, é possível também elencar diversos benefícios da implementação do processo da gestão de vulnerabilidades, como:

- Conhecimento do ambiente.
- Apoio no processo de inventário de software e hardware (responsabilidade por ativos).
- Transparência.

- Informações claras sobre cada ativo e o que é necessário implementar.
- Auxílio para tomada de decisão.
- Priorização de ações.

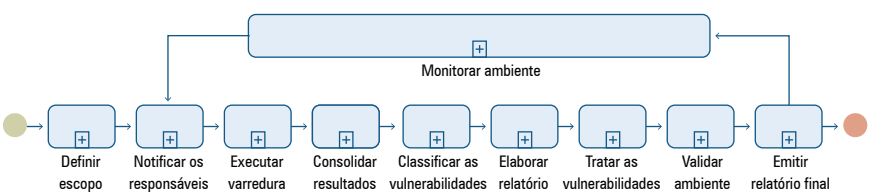
Saber identificar as falhas e planejar ações que minimizem essas vulnerabilidades proporciona a empresas e usuários segurança em meio a suscetibilidades que podem acometer os sistemas e prejudicar o andamento da instituição e dos serviços prestados.

2 Planejamento para realizar a gestão de vulnerabilidade

A gestão de vulnerabilidades nada mais é que a forma que a empresa se defende das ameaças digitais e lida com elas. É importante destacar que, além de saber se proteger dessas ameaças, que estão cada vez mais presentes e frequentes, as empresas precisam de um sistema que trabalhe a prevenção de possíveis falhas em sua segurança, evitando assim danos maiores (MOREIRA, 2001).

A figura 1 destaca os aspectos operacionais que devem ser considerados em um processo de gestão da vulnerabilidade:

Figura 1 – Macroprocesso de gestão da vulnerabilidade



Fonte: adaptado de RNP; CAIS, 2019.

Conforme demonstrado na figura, cada processo tem uma função diferente e é essencial para que a gestão seja bem-sucedida. Cada passo definido auxilia no método de análise e determinação de ações realizadas por cada equipe dentro do processo.

Portanto, o macroprocesso apresentado objetiva identificar, analisar, classificar e tratar as vulnerabilidades que podem acometer os serviços, sendo um processo contínuo dentro da área de TI.

3 Mapeamento de risco

Uma atividade importante na gestão das vulnerabilidades é o mapeamento de riscos, que representa todos os possíveis fatores de qualquer origem que ameaçam a segurança da empresa. Isso poderá evitar que a empresa tenha danos ou prejuízos maiores em todas as suas áreas, podendo gerenciá-los e identificar possíveis melhorias.

De acordo com uma pesquisa realizada por Andrade et al. (2013), os pontos mais significativos que devem ser considerados são: contexto dos riscos; identificação das ameaças e vulnerabilidades que estão acometendo a empresa; análise dos riscos (prioridades); mitigação de riscos; criação de projetos de resposta; e contingência e monitoramento das medidas implantadas.

Ainda de acordo com Andrade et al. (2013), ao estabelecer o contexto dos riscos, a empresa estipula e identifica as vulnerabilidades que existem e quais seriam seus impactos dentro da instituição e quais fatores a impediriam de chegar a determinado objetivo do projeto criado. É preciso listar e analisar as causas e os possíveis problemas que podem ocorrer e o nível de impacto que cada um acarretaria para a empresa.

A análise e a mitigação dos riscos nada mais é que a ação que será tomada frente à ameaça encontrada. Existem formas de lidar com elas, tais como: aceitar, mitigar, transferir, evitar.

Por fim, tem-se o monitoramento dos riscos, o qual avalia se as medidas determinadas para tratamento de cada um deles são adequadas e efetivas dentro daquele contexto.

4 Detecção de vulnerabilidades

Detectar as fraquezas ou chamados "buracos" de um sistema de segurança de uma empresa é uma tarefa importante do profissional de TI, pois isso evitará futuras ameaças. Ela se faz necessária para que haja tempo hábil para lidar com o problema e resolvê-lo de forma efetiva, sem danos mais graves para a organização (STONEBURNER, 2002).

A origem das vulnerabilidades pode ser diversa, como falha humana, erros de programação e configuração. Para constatação dessas vulnerabilidades, é preciso que haja identificação de todos os ativos de TI, utilização de um scan de vulnerabilidades, realização de teste de invasão, produção de uma lista com as principais vulnerabilidades e corrigi-las, além de uma constante varredura no sistema, que possibilita controle na segurança dos dados.

É importante ressaltar que os benefícios para empresas que procuram o tratamento consiste na correção da vulnerabilidade, aplicação de controles para minimizar a probabilidade de exploração ou o impacto, ou na aceitação do risco (BASTOS, 2018). Sendo assim, o trabalho preventivo de detecção de possíveis ameaças é necessário constantemente para a segurança da empresa e seus usuários.

5 Análise e prioridade das vulnerabilidades

É imprescindível que as organizações analisem as vulnerabilidades de suas informações a fim de promover a segurança contra os riscos não só da área de TI mas também de toda a empresa.

Após a identificação das ameaças, os responsáveis devem identificar as falhas de sistema que podem prejudicar de forma grave o andamento dos negócios. De acordo com a ABNT (2008), os riscos podem ser definidos em uma escala entre "muito baixo" e "muito alto", dependendo de sua gravidade. Analisar ameaças continuamente é fundamental, pois uma suscetibilidade pode aparecer a qualquer momento, dependendo do plano de prevenção adotado por cada organização.

Essa análise deve ser realizada com frequência pelo profissional de TI, para identificar as fragilidades atuais e a execução das correções necessárias. Conforme já citado em capítulos anteriores, as prioridades para tratamento dessas questões variam de acordo com as consequências que podem resultar à empresa, especialmente se houver necessidade de parar suas atividades.

Os resultados que podem ser alcançados com a análise de vulnerabilidades são: redução da incidência de problemas (diversos níveis, como senhas fracas, sistemas desatualizados e contas inativas); monitoramento contínuo (alertas a possíveis problemas), proteção contra ataques cibernéticos e aumento de conformidade com a LGPD, o que garante confiabilidade nos serviços prestados e na instituição em si (OLIVEIRA et al., 2021).

6 Relatórios de vulnerabilidades

O profissional de TI deve promover relatórios de vulnerabilidades encontradas, classificando-as como de maior ou menor grau. Essa ação é importante para definir as correções mais urgentes a serem realizadas.

Os relatórios são fundamentais para organizar as evidências levantadas, bem como ajudar a equipe de gestão de TI a realizar os investimentos necessários para a proteção da segurança. Os relatórios devem conter informações pertinentes sobre os testes realizados referentes a um incidente, após realizados os testes de vulnerabilidade.

De acordo com Gonçalves (2008), o relatório deve conter dados fundamentais que mostrem à empresa e responsáveis a melhor maneira de lidar com ameaças e protegê-la de possíveis vulnerabilidades, além de indicar os níveis de gravidade que aquele problema acarretará para a instituição. Esses dados constituem informações como: quais são as ameaças, nível do dano, objetivo, criticidade e sensibilidade de sistemas e dados.

Ainda para o autor, é preciso conhecer o objetivo, a criticidade e a sensibilidade dos sistemas de dados. Para isso, existem relatórios como, por exemplo, a avaliação de ativos críticos já existentes na empresa ou o relatório de análise de impacto no negócio (sigla em inglês: BIA).

Os relatórios não têm como objetivo apontar os erros, mas sim evidenciar de forma analítica os riscos intrínsecos do negócio, evitando prejuízos e perdas. Eles ajudam a equipe a investir no que for necessário, dão suporte na resolução de problemas, analisam o trabalho da equipe e sua capacidade frente a ameaças, apresentam dados reais de testes realizados e atestam informações relevantes sobre os testes realizados pelos responsáveis no sistema da empresa. Essas características se apresentam no relatório conhecido como BIA,[1] no qual identificam-se as formas de danos, custos, influências negativas e tempo de recuperação, no caso de alguma falha.

7 Tratamento das vulnerabilidades

Conforme já citado, existem métodos eficientes para tratamento das vulnerabilidades. Neste tópico, citamos o Stride (Microsoft), que evidencia e categoriza os tipos de vulnerabilidade; além disso, nele cada letra corresponde a uma ameaça, ou seja, os riscos que podem acometer a organização, visando os objetivos do possível invasor. De acordo com Silva (2018):

1 O relatório BIA será abordado no próximo capítulo.

- Spoofing (S) – são evidenciadas as ameaças em que o invasor acessa o sistema com identidades falsas (roubadas).
- Tampering with data (T) – está ligada à adulteração de dados, sem que haja autorização.
- Repudiation (R) – ocorre quando usuários, legítimos ou não, negam a realização de alguma ação.
- Information disclosure (I) – quando ocorre exposição não autorizada de dados.
- Denial of service (D) – métodos para tornar o sistema inoperante.
- Elevation of privilege (E) – é evidenciado quando um usuário que possui direitos limitados é capaz de realizar ações que exigem maiores permissões.

Cada uma das categorias acima citadas propõe medidas para resolução de problemas ligados à segurança da informação. Portanto, o tratamento de dados é uma relação entre falhas, fraquezas e aplicação de medidas de minimização dos impactos da empresa.

8 Métricas aplicadas às vulnerabilidades

De acordo com Miani (2009), métricas podem ser definidas como um grupo de medidas que geram uma abordagem quantitativa sobre um determinado problema. O objetivo primário de uma métrica é transformar dados brutos em informações passíveis de análise.

Portanto, para o autor, as métricas abordam os seguintes aspectos, qualitativos ou quantitativos:

1. Defesa: compreensão dos riscos que se encontram fora do ambiente da empresa (eficiência de antivírus, anti-spam, firewalls e sistemas de detecção de intrusão).

2. Cobertura: explicita o quanto a empresa conseguiu alcançar no quesito políticas de segurança (o quanto seus sistemas estão cobertos de forma segura).

3. Disponibilidade e confiabilidade: aumentar sua capacidade de detectar um problema e resolvê-lo da melhor e mais rápida forma, minimizando os problemas de segurança e continuando a operar.

4. Riscos em aplicações: contabilização do número de defeitos, complexidade e riscos em ações desenvolvidas pela empresa.

Além das métricas citadas acima pelo autor, podemos mencionar:

I. Tempo de permanência: determina o tempo que a ameaça circula no ambiente virtual.

II. Número médio de vulnerabilidades: média das vulnerabilidades que acometeram a empresa e prejudicaram sua infraestrutura.

III. Velocidade na correção de problemas: pois quanto maior a velocidade na correção, menores serão as consequências e os custos.

A aplicação das métricas podem minimizar as consequências de ameaças, prevenir vulnerabilidades e economizar custos da empresa. Seu objetivo é diagnosticar a eficiência dos programas de segurança implementados na instituição.

9 Treinamento de equipes

Como os ataques cibernéticos estão cada vez mais constantes, é importante ter uma equipe bem treinada, alinhada à política de segurança da organização. Pode-se fazer necessária a contratação de empresas especializadas para promover esses treinamentos.

A capacitação dos funcionários permite que sejam aprimoradas as habilidades para lidar com todos os tipos de ameaças, inclusive "novidades" que surgem no ambiente virtual.

As certificações de TI, por exemplo, treinam os colaboradores em áreas específicas que serão muito importantes caso haja alguma vulnerabilidade.

Os treinamentos podem acontecer de forma interna (a empresa utiliza seus próprios recursos para treinar seus funcionários) ou de forma externa, na qual uma empresa terceirizada e especializada é contratada para formar os trabalhadores.

Considerações finais

Conforme explorado no capítulo, a gestão de vulnerabilidades é muito importante para os processos de segurança das organizações. Uma equipe que está bem informada sobre as fragilidades dos sistemas tem como prever e agir em casos de ataques das mais diversas origens.

Entender e analisar os riscos, saber classificá-los quanto a suas prioridades para tratamento também é um ponto importante para o planejamento da empresa frente às ameaças que são acometidas.

Treinar a equipe para entender as gravidades e saber estabelecer o que será mais urgente dentro da funcionalidade da empresa auxilia no planejamento da resolução dos problemas. Entender quais são as ameaças que a empresa poderá passar ao longo de sua rotina fará com que a instituição se previna quanto a esses ataques.

Por fim, vimos que mapear os riscos e analisar as prioridades trará bons resultados e ajudará no tratamento das vulnerabilidades. É importante ressaltar que os relatórios auxiliam nas análises e nos próximos passos da instituição frente aos possíveis ataques.

Referências

ANDRADE, Simone Alves de et al. Proposta de um quadro conceitual para mapeamento de riscos em projetos de implantação de sistemas de informação: uma experiência na área de ERP. In: CONGRESSO BRASILEIRO DE ENGENHARIA DE PRODUÇÃO, 3., Ponta Grossa, PR, Brasil, 4-6 dez. 2013. **Anais**... Ponta Grossa: Aprepro, 2013. Disponível em: http://anteriores.aprepro.org.br/conbrepro/2013/down.php?id=322&q=1. Acesso em: 14 out. 2021.

A. SILVA, Claudete. **Gestão da segurança da informação**: um olhar a partir da ciência da informação. Campinas: São Paulo, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005:2008**: tecnologia de Informação: Técnicas de segurança: Gestão de riscos de Segurança da Informação. Rio de Janeiro, 2008.

BAARS, H. et al. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

BASTOS, Rodrigo. **Gestão de vulnerabilidades**: técnicas processos e ferramentas. [S.l.:] Fórum CSIRT, 2018.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANÇA DA RNP (CAIS). **Guia para Implementação do Processo Gestão de Vulnerabilidades Técnicas**. 2019. Disponível em: https://www.cais.rnp.br/docs/guia-gest-vulns-v2.pdf. Acessado em: 29 maio 2021.

GONÇALVES, Admilson. **Metodologia de gerenciamento de riscos em sistemas de tecnologia da informação e comunicação** – abordagem prática para conscientização e implantação nas organizações. Dissertação (Mestrado) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008.

MIANI, Rodrigo Sanches. **Utilização de métricas na elaboração de metodologias para o cálculo e aplicação de indicadores de segurança**. 2009. Tese (Doutorado) –Faculdade de Engenharia Elétrica e de Computação (FEEC), Universidade Estadual de Campinas, Campinas, 2009.

MOREIRA, Nilton Stringasci. **Segurança mínima**. Rio de Janeiro. Axcel Books, 2001.

OLIVEIRA, D. M. et al. **Guia do framework de segurança**: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2021.

SILVA, V. **Uma metodologia para modelagem de ameaças em ambientes baseados na internet das coisas**. Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Recife, 2018.

STONEBURNER, G. et al. **Risk Management Guide for Information Technology Systems**. National Institute of Standars and Techonology, July 2002. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01. Acesso em: 17 ago. 2021.