Segurança Computacional: Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação

Debora C. Faria[1]

RESUMO

Este artigo tem o objetivo de demonstrar de forma prática e aplicável metodologias de gerenciamento de riscos e como seus processos são úteis para que uma organização tenha condições de estimar, tratar e avaliar os riscos que porventura possam afetar seus negócios. Gerenciar a segurança de suas infraestruturas, bem como o valor comercial que geram tem se mostrado o principal desafio dos departamentos de TI. Entretanto, as atuais infraestruturas apresentam altos níveis de integração e compartilham ambientes cada vez mais hostis, que exigem respostas rápidas e precisas diante de incidentes que podem importar risco de danos às empresas. Na maioria das vezes, as organizações não estão preparadas o suficiente para reagir com efetividade às ameaças, em outras palavras, no tempo hábil para evitar que seus negócios sejam prejudicados. Caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação, a Segurança da Informação protege os principais ativos de uma organização visando à continuidade, a minimização dos danos e maximização das oportunidades e investimentos do negócio. A principal fonte que uma organização tem para identificar seus requisitos de segurança é derivada da avaliação de riscos, que é parte do processo geral e contínuo de gerenciamento de riscos, cuja finalidade é reduzir riscos a níveis aceitáveis pela organização.

Palavras-Chave: Segurança da Informação, Vulnerabilidades, Gerenciamento de Risco.

INTRODUÇÃO

A Segurança da Informação protege a informação contra ameaças no intuito de garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio. Pode ser obtida pela utilização de controles de políticas, práticas, procedimento, estruturas organizacionais e infraestruturas de hardware e software. É caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação, e visa preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização.

Existem três fontes principais para que uma organização identifique seus requisitos de segurança. A primeira é o conjunto de princípios, objetivos e necessidades para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações. A segunda é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de

[1] Debora C. Faria, acadêmica do curso de Análise e Desenvolvimento de Sistemas da Fatec SJC – Faculdade de Tecnologia de São José dos Campos.

serviço têm que atender. As duas anteriores são utilizadas como referências para desenvolver a principal fonte de requisitos de segurança, que é derivada da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao negócio.

Evolução dos Ataques Cibernéticos

Identificamos os ataques cibernéticos que mais causaram impacto nas últimas três décadas, que mostram a evolução dos ciberataques e a permanência de técnicas, como a de engenharia social e distribuição de malwares por meio de software pirata. Abaixo alguns exemplos:

I. CIH/Chernobyl (1998): originário de Taiwan, este é considerado um dos vírus mais prejudiciais da história por causa dos milhões de dólares de perdas que causou em todo o mundo, e da rapidez com que se espalhou. Seu modus operandi era letal: uma vez instalado em um computador, ele excluía todas as informações de todo o computador, até mesmo corrompendo bios para que o sistema não pudesse inicializar. Estima-se que afetou mais de 60 milhões de usuários do Windows 95, 98 e ME.

II. Stuxnet (2010): é o primeiro exemplo conhecido de uma arma de guerra cibernética, pois foi projetado para atacar a infraestrutura crítica iraniana. Este worm, que se espalhou através de dispositivos USB removíveis, realizou um ataque direcionado contra empresas com sistemas SCADA, com o objetivo de coletar informações e, em seguida, ordenar que o sistema se autodestruísse. Ele explorava a vulnerabilidade do Windows MS10-046, que afetou atalhos, para se instalar no computador, especificamente no Windows 2003, XP, 2000, NT, ME, 98 e 95. Ele também foi capaz de entrar em dispositivos que não estavam conectados à Internet ou a uma rede local.

III. Mirai (2016): é o mais conhecido botnet por trás de grandes ataques de negação de serviço (DDoS) até o momento. Isso afetou grandes empresas como Twitter, Netflix, Spotify e PayPal. Este malware infectou milhares de dispositivos IoT, permanecendo inativo dentro deles. Os criadores do Mirai o ativaram em 21 de outubro de 2016, usando-o para atacar o provedor de serviços DNS Dyn. Tanto seus serviços quanto seus clientes caíram ou enfrentaram problemas por horas.
Foi criado com a finalidade inicial de derrubar servidores de Minecraft.

IV. Ryuk (2019): o ransomware Ryuk colocou em risco a infraestrutura crítica de grandes empresas nacionais e internacionais no último trimestre de 2019. Entre suas vítimas estão a prefeitura do condado de Jackson, na Geórgia (EUA). Este malware, cujas origens são associadas ao grupo russo Grim Spider, criptografa os arquivos em dispositivos infectados, e só permite que a vítima recupere seus arquivos se pagar um resgate em bitcoins.

Ryuk parece ser derivado de Hermes, um pedaço semelhante de malware que pode ser comprado na dark web e personalizado para atender às necessidades do comprador.

Monitoramento de Segurança da Informação

Um substancial número de eventos suspeitos ocorrem dentro da maioria das redes corporativas todos os dias e passam completamente despercebidos. Só com uma estratégia eficaz de monitoramento de segurança, um plano de resposta a incidentes, validação de segurança e métricas no lugar certo, com ferramentas adequadamente configuradas, que será possível um bom nível de segurança ser alcançado.

A ideia é simples, termos um relacionamento automático aos eventos presentes e vulnerabilidades, para construir inteligência em ferramentas de segurança para que tenhamos alertas de eventos ocorridos, ocorrendo, ou sintomas de futuros ataques.

Para que isso ocorra, é necessário:

- Definir um monitoramento de segurança e logs em geral por meio de uma estratégia de gestão;
- Plano de resposta a incidentes integrado;
- Exercícios de validação e de ataques contra controles de segurança;
- E controle de métricas de segurança objetivando a mensuração e avaliação de melhorias;

O monitoramento de segurança envolve em tempo real, o monitoramento de eventos e atividades acontecendo em todos os sistemas importantes da sua organização em todos os momentos. Para monitorar corretamente uma organização, por meio de eventos técnicos que podem levar a um incidente ou de uma investigação, geralmente é usado um produto como o SIEM - Gerenciamentos de Informações de Segurança e Eventos.

Estas ferramentas são usadas pelos analistas de segurança e gerentes para filtrar toneladas de dados para identificar e focar apenas nos eventos mais relevantes.

Além disso, é necessário ter o entendimento de impactos regulamentares de cada evento e alertas em sua empresa, além de um planejamento e profunda compreensão da quantidade de dados que o sistema será obrigado a lidar. Estes pontos são importantes para monitorar não somente um compliance de invasão, mas de leis e regras.

Os melhores registos podem ser armazenados, compreendidos e correlacionados, melhorando a possibilidade de detectar um incidente à tempo de mitigação. A necessidade de responder a incidentes, identificar comportamentos anômalos ou não autorizados, e a proteção à propriedade intelectual, nos dias de hoje nunca foi tão crítica. Sem um log sólido, uma estratégia de gestão e tratativas corretas, torna-se quase impossível ter os dados necessários para realizar uma investigação forense, e sem ferramentas de monitoramento, identificação de ameaças e responder a ataques contra a confidencialidade, integridade ou disponibilidade, tornam-se muito mais difíceis.

Alguns pontos importantes para uma resposta à incidentes ou investigação

forense ser bem sucedida é fundamental:

- Adquirir e armazenar dados de registros de ativos de redes, softwares, e demais dispositivos e ativos tanto quanto possível, proporcionando pesquisar e restaurar as capacidades destes para análise;
- Monitorar eventos destes ativos em tempo real tanto quanto possível;
- Executar varreduras de vulnerabilidades regulares em seus hosts e dispositivos e correlacionar essas vulnerabilidades para alertas de detecção de intrusão ou outros eventos críticos, identificando assim ataques de alta prioridade, e como eles acontecem minimizando falsos positivos;
- Agregar eventos normalizando dados de dispositivos de rede independentes, e adequar a segurança de dispositivos e servidores de aplicativos em informação utilizável;
- Analisar informações correlacionadas a partir de várias fontes, tais como scanners de vulnerabilidade, IDS, IPS, firewalls, servidores, e assim por diante. De modo a identificar ataques logo que possível;
- Revisão e análise periódica forense em eventos históricos ou em tempo real através de visualização e repetição de eventos;
- Criação de relatórios personalizados para melhor visualização da sua segurança organizacional;
- Efetuar ajustes de performance e desempenho em dispositivos de segurança periodicamente de modo a proporcionar um aumento de velocidade em análises.

Times de Infosec

A ideia por trás dos times de infosec é a compreensão da segurança como uma preocupação constante, do desenvolvimento à implementação e manutenção do software.

Cada time é representado por uma cor do círculo cromático. São eles:

Red Team - O time vermelho é constituído por “hackers autorizados”. O papel dele é encontrar vulnerabilidades na aplicação que podem ser exploradas para fins maliciosos. Para isso, esse time usa técnicas de ataque com autorização da organização e mapeia as vulnerabilidades encontradas para serem corrigidas.

Blue Team - Enquanto o time vermelho deve atacar a aplicação para expor vulnerabilidades, o time azul tem o papel de defender e antecipar esses ataques. Ele é responsável pela segurança de toda a infraestrutura da organização e tem como funções o mapeamento de riscos, controle de danos, resposta a incidentes e segurança operacional.

Yellow Team - Esse é o time dos desenvolvedores. Suas tarefas envolvem o desempenho do backend, as funcionalidades da aplicação e a experiência do usuário.

Purple Team - O time roxo consiste nas interações entre os times vermelho e azul e tem como objetivo maximizar os resultados do time vermelho e melhorar a capacidade de resposta do time azul.

Assim, o time roxo integra os resultados dos testes de segurança à capacidade de defesa da organização.

Orange Team - Fazem parte desse time as interações entre os times vermelho e amarelo. Essas interações são importantes para educar desenvolvedores a programar com segurança. Como as atividades do time vermelho envolvem atacar a aplicação construída pelo time amarelo e expor vulnerabilidades, as interações entre os dois times tendem a ser reativas: os problemas encontrados pelo time vermelho retornam para o amarelo, que busca resolvê-los.

A implementação de um time laranja, no entanto, pressupõe uma atitude mais proativa por parte dos desenvolvedores. Ao aprender com o time vermelho sobre vulnerabilidades que podem ser evitadas a nível de código, menos problemas serão detectados pelos "hackers autorizados" e, consequentemente, menos tempo será gasto pelos dois times.

Green Team - Esse time diz respeito à comunicação entre os times amarelo e azul. O seu objetivo é melhorar as defesas baseadas em código e design da aplicação. Isso acontece através do feedback do time azul em relação a aplicação e do compartilhamento de limitações do software por parte do time amarelo. Essas interações ajudam a identificar vulnerabilidades e montar estratégias de defesa já no início do ciclo de desenvolvimento da aplicação.

White Team - O time branco é responsável por manter os padrões de segurança exigidos por auditores internos e externos (PCI, ISO 27001, entre outros) e pelas políticas e requerimentos do negócio. Esse é um time neutro que organiza os demais, planeja e monitora o seu progresso.

Por que implementar?

Times de segurança da informação são uma forma de organizar procedimentos de segurança e implementá-los no decorrer do ciclo de desenvolvimento de software, ao invés de apenas no final.

Metodologias de Gerenciamento de Riscos

O gerenciamento de riscos é um processo que tem como objetivo possibilitar a segurança efetiva dos sistemas, responsáveis pelo processamento, armazenagem e transmissão de informações; cria uma base sólida para as tomadas de decisão, principalmente no que se relaciona com execução coerente do orçamento e no investimento em tecnologias necessárias para mitigar riscos de impacto para a empresa.

I. Abordagem Reativa e Proativa

Quando ocorre determinado incidente de segurança, muitos profissionais de TI tendem a agir para conter a situação, descobrir as causas e reparar os danos no menor tempo possível. Tal abordagem é dita reativa, depende de um estímulo causado por um incidente para que ações sejam tomadas.

As respostas a incidentes são taticamente eficazes, principalmente se executada com rigor para se descobrir as causas raiz. Como resultado, incidentes de segurança recentes podem auxiliar na prevenção de incidentes futuros.

A abordagem proativa de gerenciamento de riscos de segurança almeja a redução da probabilidade de um incidente com a utilização de planos de controles. Ao contrário da abordagem reativa, a abordagem proativa não espera pelo surgimento de um incidente.

II. Identificação de Vulnerabilidades

Vulnerabilidades são falhas ou fraquezas nos processos de segurança, nos projetos, no desenvolvimento ou nos controles internos de um sistema, os quais, se explorados, podem resultar em eventos não desejados, ou seja, os ataques. Métodos proativos de testes podem ser utilizados para identificar vulnerabilidades:

- Sistemas de varredura e análise de vulnerabilidades;
- Testes e simulações;
- Testes de invasão de sistemas;
- Auditorias em códigos-fonte;
- Listas de verificação e análise crítica de segurança.

CONCLUSÃO

Segurança da Informação é muito mais que ter um software antivírus instalado ou utilizar um firewall que impeça o ataque de agentes indevidos a sua rede. Segurança da Informação está relacionada a proteção de dados, a segurança física, a segurança do ambiente, o alinhamento da Tecnologia da Informação com os objetivos e a missão da empresa, dentre outras funções essenciais para a continuidade dos negócios. Portanto, se faz tão necessária no atual cenário em que estamos, não apenas como uma medida reativa, mas sim com planejamento organizado e medidas proativas.