1.Segurança da informação

A ***Segurança da Informação*** é um campo multidisciplinar que se concentra em proteger os ativos de informação de uma organização contra ameaças e garantir que esses ativos permaneçam confidenciais, íntegros e disponíveis quando necessário. É um conjunto de práticas, políticas, procedimentos e tecnologias projetadas para salvaguardar informações sensíveis e valiosas.

O termo ***hacker*** descrevia indivíduos com qualificações profissionais avançadas de programação. Eles usavam estas qualificações para testar os limites e recursos dos primeiros sistemas. Existem muitos grupos de dados que compõem os diferentes domínios do mundo cibernético. Quando os grupos conseguem coletar e utilizar grandes volumes de dados, eles começam a acumular poder e influência. Os dados podem estar na forma de números, fotos, vídeos, áudios, ou qualquer tipo de coisa que pode ser digitalizada. Grandes empresas e corporações podem ser consideradas como domínios de dados e eles são fortes devido à capacidade de coletar dados de usuários, com a contribuição dos próprios usuários. Nos dias de hoje, o mundo dos criminosos virtuais tornou-se mais perigoso. Os invasores são indivíduos ou grupos que tentam explorar vulnerabilidades para ganho pessoal ou financeiro.

2.Atributos dos atores de ameaças

Existem diferentes tipos de atores de ameaças no contexto da segurança cibernética e compreender esses atores é fundamental para identificar suas motivações, métodos e como se proteger contra possíveis ameaças.

2.1 Script Kiddies

Tem pouca ou nenhuma qualificação profissional, muitas vezes usando ferramentas existentes ou instruções encontradas na Internet para lançar ataques. Características dos script kiddies:

- **Atividades:** Qualquer atividade hacker.
- **Motivação:** Suas motivações podem variar, mas frequentemente estão relacionadas à busca de notoriedade.
- **Habilidades:** São indivíduos com habilidades de hacking limitadas. Eles não têm o conhecimento técnico profundo dos hackers mais experientes e, assim, usam ferramentas e scripts prontos para realizar ataques.
- **Padrão de atuação:** Script kiddies geralmente conduzem ataques simples, como ataques de negação de serviço distribuídos (DDoS) ou tentativas de invasão com base em tutoriais encontrados online.

2.2 White hats

São hackers éticos que usam suas habilidades de programação para fins bons, éticos e legais. Eles podem realizar testes de penetração na rede na identificação das vulnerabilidades da rede. Estas vulnerabilidades são informadas aos desenvolvedores para que sejam corrigidas, antes de serem exploradas. Algumas empresas premiam ou recompensam white hats quando são informadas sobre uma vulnerabilidade. Características dos white hat hackers:

- ➢ **Atividades:** White hat hackers são hackers éticos que usam suas habilidades técnicas para proteger sistemas e redes. Eles trabalham em empresas de segurança cibernética, organizações governamentais ou como consultores, visando melhorar a segurança.
- ➢ **Motivação:** É ética e legal, focada na proteção e melhoria da segurança. Colaboração com organizações para encontrar e corrigir vulnerabilidades.
- ➢ **Habilidades:** Usam técnicas avançadas e conhecimento profundo de sistemas e redes.
- ➢ **Padrão de atuação:** Conduzem testes de penetração autorizados, procurando por vulnerabilidades em sistemas e redes. Seu trabalho contribui para a identificação e correção de falhas de segurança.

2.3 Grey hats

São indivíduos que cometem crimes e fazem coisas discutivelmente antiéticas, mas não para ganho pessoal ou para causar danos. Eles podem divulgar vulnerabilidades à organização afetada depois de terem comprometido sua rede. Características dos gray hat hackers:

- ➢ **Atividades:** Atividades que podem estar na fronteira da legalidade. Realizam atividades que podem ser questionáveis em termos legais, como divulgar vulnerabilidades sem autorização. Suas intenções nem sempre são maliciosas.
- ➢ **Motivação:** Pode ser variável, geralmente um desejo de revelar vulnerabilidades ou desafiar. Muitas vezes operam de forma independente, sem serem diretamente contratados por organizações.
- ➢ **Habilidades:** Também possuem habilidades avançadas.
- ➢ **Padrão de atuação:** Gray hat hackers podem agir de forma independente, identificando vulnerabilidades e, em seguida, comunicando suas descobertas às partes afetadas, às vezes sem permissão. Suas motivações podem variar, mas geralmente buscam desafiar sistemas ou expor vulnerabilidades.

2.4 Black hats

São criminosos antiéticos que violam a segurança do computador e da rede para ganho pessoal ou por motivos mal intencionados, como ataques às redes. Eles exploram as vulnerabilidades para comprometer os sistemas de computadores. Suas principais características são:

- ➢ **Atividades:** Suas atividades incluem invasões, roubos de dados, distribuição de malware e outros crimes cibernéticos.
- ➢ **Motivação:** Financeira, desonestidade e intenção de prejudicar. As suas motivações podem variar desde o roubo de informações pessoais e financeiras até a realização de ataques que interrompem serviços críticos.
- ➢ **Habilidades:** Possui habilidades avançadas na exploração de vulnerabilidades.
- ➢ **Padrão de atuação:** Os black hat hackers geralmente operam na clandestinidade, usando técnicas para ocultar sua identidade. Eles exploram vulnerabilidades em sistemas e redes para obter ganhos financeiros ou causar danos. Motivações incluem lucro, roubo de informações pessoais e empresariais, ou mesmo sabotagem.

2.5 Blue Hat hackers

Os blue hat hackers são frequentemente indivíduos externos que testam sistemas internos com permissão. Eles podem ser contratados por organizações para avaliar a segurança de seus sistemas e redes. Esses hackers têm uma função mais controlada e legal do que os black hat hackers. Características dos blue hat hackers:

- **Atividades:** Frequentemente contratados por organizações para avaliar a segurança de seus sistemas. Normalmente de fora de uma organização e com autorização, eles testam sistemas internos, fornecem relatórios e recomendações de segurança após avaliações.
- **Motivação:** Suas motivações incluem a remuneração por serviços de teste de penetração e a contribuição para a segurança.
- **Habilidades:** Habilidades e técnicas avançadas.
- **Padrão de atuação:** Atuam com permissão e cooperação de organizações. Possuem contrato de colaboração com organizações, realizando avaliações de segurança e fornecendo relatórios com recomendações.

2.6 Hacktivistas

São grey hats que se reúnem e protestam contra diferentes ideias políticas e sociais. Os hacktivistas protestam publicamente contra organizações ou governos, publicando artigos, vídeos, vazando informações confidenciais e realizando ataques DDoS. Os grupos ambientalistas e de defesa dos animais podem ter como alvo uma vasta gama de indústrias.

- **Atividades:** Eles podem tentar obter e divulgar informações confidenciais para o domínio público, realizar ataques de negação de serviço (DoS) ou desfigurar sites.
- **Motivação:** Suas motivações estão enraizadas em convicções políticas ou sociais. Atuam para promover suas causas políticas, sociais ou ideológicas.
- **Habilidades:** Possuem habilidades técnicas avançadas e conhecimento profundo de sistemas e redes.
- **Padrão de atuação:** Hacktivistas podem realizar ataques cibernéticos, como vazamento de informações, interrupção de serviços ou desfigurar sites, como forma de protesto ou divulgação de mensagens.

2.7 Grupo de hackers

Estes incluem hacktivistas, criminosos virtuais, terroristas e os hackers patrocinados pelo Estado. Geralmente são grupos profissionais, focados em controle, poder e riqueza. São altamente sofisticados, organizados e ainda podem proporcionar o crime digital como um serviço. Eles fazem declarações políticas para sensibilizar questões que são importantes para eles, além de publicar informações embaraçosas sobre suas vítimas.

2.8 Patrocinados pelo Estado

Dependendo da perspectiva de uma pessoa, são hackers do bem ou do mal, que roubam segredos do governo, reúnem informações e sabotam redes. Seus alvos são outros governos estrangeiros, grupos terroristas e corporações.

3.A Surface web

É a parte visível da internet que é indexada por mecanismos de busca comuns, como o Google, Bing ou Yahoo. Representa a rede como a maioria das pessoas usa e conhece. Corresponde a todo conteúdo disponível pelos mecanismos de busca e que pode ser facilmente acessado por meio de navegadores convencionais, como o Google Chrome, Mozilla Firefox ou Safari. Aqui, encontramos sites públicos, páginas da web e conteúdo acessível a qualquer pessoa. A maioria das atividades online ocorre na Web Superficial.

3.1 Deep web

A ***Deep Web***, frequentemente mal compreendida e confundida com a Dark Web, representa uma parte substancial, porém menos visível, da internet. Ela engloba todas as partes da rede que não são indexadas pelos mecanismos de busca tradicionais, tornando-as inacessíveis por meio de pesquisas no Google, Bing ou outros mecanismos de busca comuns. Embora a Deep Web não seja acessível diretamente por mecanismos de busca, não é necessariamente obscura ou maliciosa; muitas atividades legítimas ocorrem aqui. Características da deep web são:

- **Conteúdo não indexado:** A principal característica da deep web é que seu conteúdo não é acessível por meio de mecanismos de busca convencionais. Isso inclui sistemas de gerenciamento de banco de dados, intranets corporativas, sistemas de e-mail privado, informações governamentais confidenciais e qualquer outro tipo de conteúdo que não seja destinado ao acesso público.
- **Acesso controlado:** Muitos recursos da deep web são protegidos por senhas, autenticação ou outras medidas de controle de acesso. Isso significa que apenas pessoas autorizadas têm permissão para acessar essas informações, serviços ou sistemas.
- **Atividades legítimas:** É importante destacar que a maior parte da deep web é composta por atividades legítimas e inofensivas. Empresas utilizam intranets para gerenciar informações internas, e sistemas de gerenciamento de banco de dados são usados para armazenar registros confidenciais. As atividades na deep web são essenciais para o funcionamento de muitas organizações.
- **Privacidade e segurança:** A natureza não indexada da deep web fornece um nível de privacidade e segurança, tornando-a um local preferido para atividades que requerem discrição, como troca segura de mensagens, comunicações empresariais confidenciais e acesso seguro a informações de pacientes em hospitais.
- **Papel na cibersegurança:** A deep web desempenha um papel importante na cibersegurança, pois as empresas muitas vezes usam sistemas internos e sistemas de autenticação para proteger informações sensíveis. Também é um espaço onde as organizações podem compartilhar informações confidenciais com terceiros de maneira segura, como relatórios de auditoria, documentos legais e contratos
- **Desafios de segurança:** Embora a deep web seja predominantemente utilizada para fins legítimos, também pode ser alvo de ataques. A segurança dos sistemas e a autenticação desempenham um papel crucial na proteção desses recursos contra o acesso não autorizado.

3.2 Dark web

A ***dark web*** é uma parte específica da Deep Web que é deliberadamente oculta e inacessível através de navegadores padrão. Ela utiliza redes criptografadas e sistemas de anonimato, como o Tor para ocultar a identidade dos usuários e servidores. A dark web é conhecida por hospedar mercados clandestinos, fóruns de hacking, conteúdo ilegal e atividades ilícitas.

A dark web opera em grande parte sob o princípio do anonimato. Os usuários acessam sites e recursos usando redes como o Tor, que roteiam o tráfego através de uma série de servidores criptografados, tornando difícil a rastreabilidade. Isso permite que indivíduos naveguem e participem de atividades sem revelar sua localização ou identidade.

O navegador Tor roteia o tráfego através da rede Tor, permitindo o acesso a sites ***.onion***, que são exclusivos da dark web. Esses sites muitas vezes contêm fóruns, mercados clandestinos, serviços de hospedagem e outros recursos.

A organização da dark web é descentralizada e baseada em comunidades. É composta por várias redes independentes denominadas ***darknets***, compartilhando o espaço da dark web. Dentro dessas ***darknets***, grupos e indivíduos operam sites, fóruns e serviços independentes.

Embora a dark web seja frequentemente associada a atividades ilegais e maliciosas, também tem potencial para uso legítimo. Pode ser usada como uma ferramenta para ativistas, jornalistas e pessoas em países com censura para se comunicarem de forma segura. Além disso, as organizações de segurança cibernética e de aplicação da lei monitoram a Dark Web para identificar ameaças e investigar atividades criminosas.

3.3 Dark net

A ***darknet*** é uma parte da internet que não é acessível por meio dos navegadores padrão e não é indexada pelos mecanismos de busca convencionais. Ela é uma rede obscura, muitas vezes associada a atividades clandestinas e anônimas. A darknet opera por meio de redes privadas e sistemas criptografados, garantindo um alto grau de anonimato para seus usuários.

A darknet consiste de um conjunto de redes privadas como a rede Onion, I2P ou Freenet compostas de sites, fóruns, comunidades e serviços que não estão disponíveis na internet convencional. Para acessá-la, os usuários precisam usar software especializado, como o Tor (The Onion Route da rede Onion), que encaminha as conexões por meio de uma série de servidores, mascarando o endereço IP do usuário. A organização da darknet é descentralizada. Os sites e serviços são frequentemente hospedados em servidores que operam sob domínios exclusivos chamados de "sites .onion.". Os proprietários desses sites variam desde defensores da privacidade e jornalistas até cibercriminosos e grupos de hackers.

4.Não repúdio

Um sujeito não pode negar que fez algo, tal como criar, modificar ou enviar um documento. Impedir que uma pessoa negue ter realizado uma ação específica, como enviar uma

mensagem ou realizar uma transação. Mecanismos de não repúdio, tal como assinaturas digitais, podem ser usados para garantir a autenticidade das ações.

4.1 Autenticidade
Certifica-se de que a origem das informações seja legítima e confiável.

4.2 Controle de Acesso
Gerenciar quem tem permissão para acessar informações ou recursos. O controle de acesso define quais usuários ou sistemas podem acessar quais dados e em que condições.

4.3 Autenticação e Autorização
A autenticação envolve verificar a identidade de um usuário antes de conceder acesso a recursos. A autorização determina o que um usuário autenticado pode fazer após o acesso ser concedido.

4.4 Princípio do Menor Privilégio
Os usuários e sistemas devem ter apenas o acesso necessário para realizar suas tarefas.. Isso minimiza o risco de acesso não autorizado.

4.5 Gestão de Riscos
Avaliar e mitigar os riscos de segurança associados às informações. Isso envolve a identificação de vulnerabilidades, ameaças potenciais e a implementação de medidas para reduzir esses riscos a níveis aceitáveis.

4.6 Ativos de Informação
São todos os dados e recursos que têm valor para uma organização. Isso pode incluir dados confidenciais, sistemas de computador, documentos físicos, hardware e software.

4.7 Ameaças à Segurança da Informação
As ameaças são eventos ou circunstâncias que podem causar danos aos ativos de informação. Isso pode incluir hackers, malwares, desastres naturais, erro humano e outros.

4.8 Ataques Cibernéticos
Ataques cibernéticos são ações deliberadas para comprometer a segurança da informação. Isso inclui malware, phishing, ataques de negação de serviço (DoS) e engenharia social.

4.9 Criptografia
A criptografia é uma técnica que transforma informações em um formato ilegível, a menos que o receptor tenha a chave apropriada para decifrá-las.

A Segurança da Informação passa pelo entendimento da diversidade de profissionais que desempenham papéis fundamentais na proteção das informações e ativos digitais. Os profissionais de TI que trabalham em funções com responsabilidades de segurança devem ser

competentes em uma ampla gama de disciplinas, desde projeto de redes e aplicações até compras e recursos humanos.

- Participar de avaliações de risco e testes de sistemas de segurança e fazer recomendações.
- Especificar, prover, instalar e configurar dispositivos e softwares de segurança.
- Configurar e manter controle de acesso a documentos e perfis de privilégio de usuário.
- Monitorar registros de auditoria, revisar privilégios de usuários e controlar o acesso a documentos.
- Gerenciar resposta a incidentes e relatórios relacionados à segurança.
- Criar e testar os planos de continuidade de negócio e de recuperação de desastres e procedimentos.
- Participar de programas de treinamento e educação em segurança.

5.Papéis e responsabilidades na área de Segurança da Informação

Os principais profissionais no campo de Segurança da Informação, destacando seus papéis e responsabilidades, são:

5.1 CISO (Chief Information Security Officer)

A responsabilidade interna geral pela segurança pode ser executada por um departamento dedicado, administrado por um Diretor de Segurança (CSO) ou um Diretor de Segurança da Informação (CISO). O CISO é o líder sênior de Segurança da Informação. Ele é o principal responsável pela Segurança da Informação em uma organização. Seu papel de liderança é fundamental na definição de estratégias de segurança, na gestão de riscos cibernéticos e na supervisão das equipes de segurança.

Principais responsabilidades de um CISO:

- Desenvolver e implementar políticas de Segurança da Informação
- Supervisionar equipes de Segurança
- Garantir conformidade com regulamentações de segurança
- Avaliar e mitigar riscos de segurança
- Responder aos incidentes de segurança

5.2 DPO (Data Protection Officer)

É um profissional cuja função central é garantir que uma organização esteja em conformidade com regulamentações de privacidade de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, e a Lei Geral de Proteção de Dados (LGPD), no Brasil. O DPO tem o papel de fazer a ponte entre a organização e a autoridade nacional de proteção de dados, garantindo que a organização cumpra regulamentações de privacidade de dados.

Principais responsabilidades de um DPO:

- Monitorar e aconselhar sobre o tratamento de dados pessoais
- Elaborar avaliação de Impacto de Proteção de Dados
- Garantir a conformidade com regulamentações de privacidade
- Revisar contratos e parcerias

- Atuar como ponto de contato para autoridades de proteção de dados
- Responder pela comunicação com os titulares dos dados
- Educar os funcionários sobre políticas de privacidade

5.3 Analista de Segurança da Informação

Esse profissional atua no gerenciamento da infraestrutura de TI. Ele também desempenha um papel fundamental na implementação de medidas de segurança. Seu papel é técnico-analítico, desempenhando funções no monitoramento da infraestrutura de TI, identificando vulnerabilidades e respondendo aos incidentes de segurança.

Principais responsabilidades de um Analista de Segurança da Informação:

- Monitorar sistemas e redes em busca de atividades suspeitas
- Implementar medidas de segurança, como firewalls e antivírus
- Investigar e responder sobre incidentes de segurança
- Avaliar a eficácia das políticas de segurança

5.4 Hacker ético

Os hackers éticos (também conhecidos como pentesters) são contratados para testar a segurança de sistemas e aplicativos de uma organização. O papel dos hackers éticos é atuar como um ator de ataque com consentimento para testar a segurança de sistemas e aplicativos, procurando vulnerabilidades e evitar que criminosos o façam.

Principais responsabilidades de um hacker ético:

- Realizar testes de penetração em sistemas
- Identificar e relatar vulnerabilidades
- Simular ataques para avaliar a resistência das defesas
- Ajudar na melhoria da segurança da organização

5.5 Especialista em segurança em Nuvem

Esses profissionais se concentram em disponibilizar recursos em nuvem com segurança e em conformidade com padrões estabelecidos. Se concentram em garantir que os recursos na nuvem estejam seguros e em conformidade com as melhores práticas. Possui especialização em computação em nuvem.

Principais responsabilidades de um Especialista em Segurança em Nuvem:

- Avaliar e configurar a segurança em ambientes de Nuvem
- Monitorar ameaças na Nuvem
- Implementar políticas de segurança na Nuvem
- Garantir a conformidade com regulamentações em Nuvem

5.6 Analista forense digital

É responsável pela investigação de incidentes de segurança, coleta de evidências eletrônicas em apoio a processos legais e seu principal papel é atuar em investigações forenses, fornecendo suporte a processos legais.

Principais responsabilidades de um analista forense digital:

- Coletar e analisar evidências digitais
- Reconstruir incidentes de segurança
- Preparar relatórios de forense digital para fins legais
- Ajudar na identificação de invasores

5.7 Cientista em dados de segurança

Esses profissionais aplicam técnicas de análise de dados para identificar ameaças e tendências de segurança e seu principal papel é analisar dados identificando comportamentos que possam ameaçar a segurança.

Principais responsabilidades de um cientista de dados em segurança:

- Analisar grandes conjuntos de dados para identificar padrões de ameaças
- Desenvolver modelos preditivos de segurança
- Monitorar o tráfego de rede em busca de atividade suspeita
- Identificar anomalias e ameaças em tempo real

5.8 Analista a resposta a incidentes de segurança

Encarregados de responder a incidentes de segurança, mitigar danos e implementar medidas corretivas e seu principal papel é atuar na linha de frente na ocorrência de incidentes de segurança.

Principais responsabilidades de um Analista a resposta de incidentes de segurança:

- Detectar e analisar incidentes de segurança
- Isolar e conter ameaças
- Recuperar sistemas após um incidente
- Documentar e reportar incidentes às partes interessadas

5.9 Pentesters

Testadores especializados em segurança que avaliam aplicativos em busca de vulnerabilidades e seu principal papel é atuar no aperfeiçoamento da segurança dos aplicativos, buscando vulnerabilidades que devem ser corrigidas.

Principais responsabilidades de um pentester:

- Realizar testes de segurança em aplicativos e sistemas
- Identificar vulnerabilidades, como falhas de injeção SQL ou XSS
- Trabalhar com equipes de desenvolvimento para corrigir falhas de segurança
- Validar a eficácia das correções implementadas