

Especialista em Segurança de Rede



Disciplina: Informática e Sociedade


Professor: Frederico Sauer

Alunos: Felipe Gomes de Oliveira,
Isabela de Faria Mota Melgaço,
Jefferson Alexandro R. dos Santos

De acordo com um levantamento feito por pesquisadores americanos, uma empresa pode levar quase três semanas para se recuperar totalmente de um ataque virtual, o que pode acarretar cerca de 400 mil reais em prejuízos.

Da necessidade de controle sobre as informações surgiu o conceito de Segurança de Redes. O tema provou ser tão essencial que o mercado de trabalho se viu diante do aparecimento de uma nova ocupação: o **analista de sistemas e segurança da informação**.






Em poucas palavras, este profissional é responsável pela manutenção dos sistemas de uma empresa, sendo seu dever criar políticas de segurança e pesquisa das melhores ferramentas para assegurar os dados armazenados.

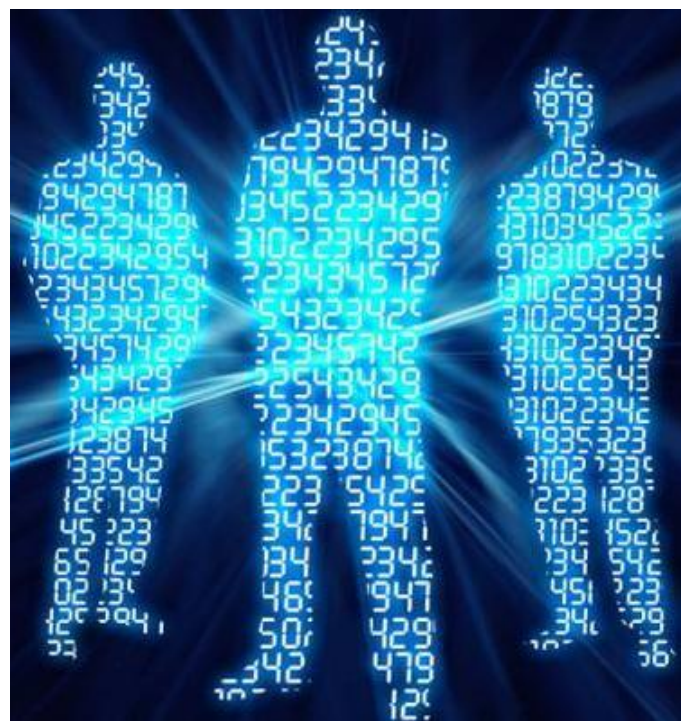
A atuação do analista de segurança não se restringe apenas à criação de dificuldades para os crackers ("*hackers*" que têm como objetivo quebrar sistemas de segurança e praticar crimes cibernéticos), ele também pode fazer parte de um grupo de inteligência, que mapeia as maiores ameaças virtuais em cada país, os grupos de piratas virtuais mais atuantes e os pontos fracos de cada cliente.

Com o volume de dados cada vez maior dentro das corporações e nos órgãos públicos, o especialista em segurança da informação tem ganhado destaque no mercado de trabalho. E não é para menos, se considerarmos o volume de informações que circulam pelos meios digitais atualmente.



Em pesquisa feita pela IDC(Provedora de inteligência de mercado e consultoria e serviço de marketing para mercado de ti), uma das empresas mais atuantes na área de segurança de redes e informações, mais de 40% das empresas consultadas não têm noção de controle de informações e sequer sabe como dar os primeiros passos no que diz respeito à proteção de seus dados. Além disso, apenas 15% das companhias afirmam ter certeza sobre o que querem proteger. Este índice traduz o amplo campo de oportunidades, que surgem conforme as companhias tomam conhecimento da importância de proteger suas informações.

A rotina do profissional de segurança da informação é variável conforme o foco da sua especialização. Entretanto, o ideal é que ele tenha o domínio das quatro principais áreas de atuação do profissional— **gestão, análise de segurança, análise de teste e computação forense** . Isso porque, é comum que o profissional assuma todas essas funções, dependendo do porte e segmento da empresa que trabalha.



Gestão de sistemas, hardwares e softwares

Quem atua nessa área deve estar apto a desenvolver uma série de políticas de segurança para evitar vulnerabilidades nas etapas operacionais. Esse profissional comanda ações para tratar a informação em diversos níveis de confidencialidade.

Analista de segurança

Os profissionais que cumprem esta função ocupam um papel basicamente técnico dentro da empresa. A equipe, ou profissional isolado – em casos de empresas de pequeno porte – funciona como um front de batalha, ou seja, sua atuação cobre a construção e implementação de tecnologias efetivas para cumprimento das políticas de segurança definidas. É necessário ter amplo conhecimento em ferramentas de combate a malware e melhoria da segurança de rede.


Analista de teste

É uma área mais restrita onde o analista irá avaliar a segurança dos sistemas da empresa, realizando testes de intrusão a nível processual e tecnológico, podendo também examinar os controles físicos da companhia.

Analista de computação forense

Quem se especializa nesta área deve estar preparado para dominar toda a parte tecnológica acima citada, e ainda, exercer o papel de investigador, podendo atuar nos âmbitos jurídicos, criminal ou corporativo.


O objetivo é analisar o incidente para detectar questões como: nível de gravidade, invasão de informações sensíveis e comprometimento da base da empresa, de modo a orientar as medidas adequadas para minimizar os riscos do ataque para a corporação.



O analista de computação forense, então, pode seguir por dois caminhos:


No primeiro, utilizará seus conhecimentos em computação forense para buscar informações preciosas no sustento e complemento da argumentação jurídica. Ou seja, nesse cenário o profissional forense vai “à caça” de provas virtuais capazes de comprovar um crime ou atividade ilegal, isto quando ele atua como um "assistente técnico ou perito" requisitado por um advogado ou mesmo juiz.

Já no segundo “caminho”, o profissional de segurança utilizará suas competências técnicas e intelectuais para procurar e analisar toda e qualquer informação sobre o incidente na base de dados sensíveis da empresa, rastreando cada erro e ação que levou ao problema. A grande sacada será descobrir as principais falhas, promovendo melhorias nas barreiras de segurança, para que o incidente não se repita. Embora isto não elimine a possibilidade de em um incidente no âmbito corporativo, pode-se iniciar uma ação jurídica posterior.



Um profissional com pleno domínio das competências exigidas na computação forense estará apto para atuar tanto no âmbito corporativo, como no jurídico.

E para isso, o especialista em segurança da informação precisa conhecer as normas que regem as boas práticas de Segurança da Informação e que direta ou indiretamente tratam da temática de resposta a incidente e computação forense como ISO 27002 e PCI. Deve-se ainda, compreender o funcionamento das principais ferramentas que auxiliam no momento da perícia ou investigação digital tais como: ENCASE, FTK, Sistemas Linux customizados (SANS SIFT, REMNIX, SANTOKU), dentre outros.



Para compreender detalhadamente as principais fases de intervenção do especialista em computação forense tomemos a seguinte situação:

Um banco tem o seu servidor invadido por um grupo de Scriptkids ou crackers e ocorre a quebra do sigilo de dados pessoais e de cartões de créditos dos seus correntistas. Tal fato demanda o trabalho de um perito em tempo ágil, para aplicar medidas de contenção do incidente e fornecer um laudo completo, reunindo todas as provas íntegras do ocorrido.

1. Preservação

O primeiro objetivo é assegurar a inalterabilidade dos dados afetados. Aqui, o profissional utiliza-se de técnicas conhecidas como espelhamento e imagem de discos para duplicar o conteúdo e não correr o risco de perder sua consistência original.

2. Extração

Na sequência, a recuperação das informações que foram perdidas durante a ação maliciosa é executada. O foco do profissional é extrair o máximo possível de dados apagados por meio de técnicas especiais, tais como a indexação de disco.


3. Análise

Com as informações recuperadas, o perito partirá para coleta e análise de evidências digitais que possam contribuir para a solução definitiva do caso. Nessa fase, é comum o surgimento de desafios envolvendo senhas e criptografias específicas.

4. Laudo

A última etapa consiste em formalizar, de forma minuciosa, todas as evidências digitais e suas respectivas análises. O profissional irá elaborar um laudo pericial onde atesta a integridade das informações levantadas.

As quatro fases citadas compõem a ação básica do “post-mortem”, conceito em latim utilizado para definir a análise completa de uma rede, sistema, software ou hardware que sofreu invasão.



Para ser um profissional bem-sucedido, você precisa investir da maneira certa em sua formação.

- **Faça um curso presencial**

É comum pessoas acharem que podem se inserir na área de TI apenas fazendo cursos online e praticando o método “tentativa e erro”. A web é, de fato, uma fonte riquíssima de conteúdo, porém um curso presencial oferece uma formação de base completa, assegurada de instrutores com experiência e certificações, e permite que você pratique os conteúdos com todo o suporte e assistência necessário.

Além disso, muitas empresas ainda fazem questão de contratar profissionais que comprovem terem feito um bom curso, mesmo que sejam excelentes especialistas.

- **Tire certificações**

Certificações em conhecimentos específicos são essenciais em qualquer área de TI e são obtidas por meio de testes.

São com as certificações que se tem credenciais que ressaltam que o especialista passou por teste significativos. Muitas empresas esperam que esse profissional também administre servidores e, portanto, é interessante que possua as certificações.



No caso do especialista em redes, as mais importantes certificações são:

As certificações Cisco (CCENT,CCNA,CCNP,CCIE)

- A CCENT(Cisco Certified Entry Networking Technician) é o primeiro passo para a certificação CCNA e vai ajudá-lo a se destacar da multidão em cargos de nível de entrada .
- A certificação CCNA Security estabelece as bases para papéis de trabalho , tais como Especialista em Segurança de Rede,Administrador de Segurança e Engenheiro de Suporte de Segurança de Rede . É o primeiro passo para indivíduos que desejam obter sua certificação CCNP Segurança.
- A certificação CCNP Security(Certified Network Professional Security) é alinhado especificamente para o cargo de Engenheiro Cisco Network Security responsável pela segurança em roteadores, switches , dispositivos de rede e equipamentos, bem como a escolha , a implantação , suporte e resolução de problemas Firewalls ,VPNs e soluções de IDS / IPS para seus ambientes de rede .
- A certificação a CCIE Security é o desafio da certificação definitiva para levá-lo para uma carreira na gestão e criação de end-to -end de redes seguras .



GISF – GLOBAL INFORMATION ASSURANCE CERTIFICATION INFORMATION SECURITY FUNDAMENTALS

A certificação em Fundamentos de Segurança da Informação (GISF) garante que os profissionais certificados possuam o nível adequado de conhecimento e habilidades para a gestão de riscos e técnicas de defesa em profundidade.

Competências e habilidades adquiridas: Visão geral dos fundamentos de segurança de rede, DNS, roteamento IP, criptografia.

GSEC – GLOBAL INFORMATION ASSURANCE CERTIFICATION SECURITY ESSENTIALS

Os profissionais de segurança que possuem a certificação GSEC demonstram estarem qualificados para executar atividades operacionais no que diz respeito às tarefas de segurança.

Competências e habilidades adquiridas: avaliação de riscos e auditoria, firewalls, detecção de intrusão, políticas de segurança, gerenciamento de senhas.

CEH – CERTIFIED ETHICAL HACKER

Executores de testes de penetração, analistas de segurança de rede e administradores de sistemas são algumas das posições que exigem esta certificação.

Competências e habilidades adquiridas: Tecnologias e técnicas de invasão a partir de uma perspectiva ofensiva, testes de penetração, vulnerabilidades típicas de rede, conhecimento de exploits mais comuns.

GCIA – GLOBAL INFORMATION ASSURANCE CERTIFIED INTRUSION ANALYST

Detecção de intrusão, TCP / IP, análise de tráfego de rede e sistemas de detecção de intrusão são uma amostra das habilidades e conhecimentos adquiridos durante a obtenção do GCIA.

Competências e habilidades adquiridas: detecção de intrusão, TCP / IP, análise de tráfego de rede, sistemas de detecção de intrusão.



CISSP – CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

Esta certificação, que foi formalmente aprovada pelo Departamento de Defesa E.U., foi mencionada em 385 postagens de emprego em ClearanceJobs.com.

Competências e habilidades adquiridas: Gestão de riscos, planejamento e organização da políticas de segurança de rede, aspectos legais, planejamento de atividades de resposta e recuperação.

CISM – CERTIFIED INFORMATION SECURITY MANAGER

A certificação CISM é para profissionais de tecnologia que gerenciam, projetam, supervisionam e/ou avaliam a segurança da informação em suas empresas.

Competências e habilidades adquiridas: Gestão de riscos, gerenciamento de incidentes, desenvolvimento de um programa completo de segurança da informação, criação de políticas



- **Participe de fóruns na web**

- **Mantenha-se atualizado**

Salário médio de Segurança da Informação

Estagiário de Segurança da Informação – R\$ 1.090,94

Assistente de Segurança da Informação – R\$ 1.291,98

Consultor de Segurança da Informação – R\$ 6.752,88

Coordenador, Supervisor ou Chefe de Segurança da Informação – R\$ 7.615,81

Fonte: <http://www.simonsen.br/>





Cargos	Júnior	Pleno	Sênior
Analista de segurança da informação	4.934,72	5.600,00	7.266,93
Gerente de segurança	11.060,00	12.192,00	14.333,00

Fonte: <http://info.abril.com.br/carreira/salarios/>



Bibliografias:

<http://3way.com.br/dicas/5-dicas-para-se-tornar-um-especialista-em-redes>

<http://tecnologia.bandtec.com.br/voce-sabe-o-que-faz-um-profissional-da-seguranca-da-informacao>

<http://www.impacta.com.br/blog/2015/03/17/redes-e-seguranca-da-informacao-por-que-se-especializar/>

<https://learningnetwork.cisco.com/community/certifications>

<http://www.diegomacedo.com.br/6-certificacoes-que-garantirao-seu-emprego-na-area-de-seguranca-da-informacao/>