COMO CONSTRUIR UMA CARREIRA EM SEGURANÇA DA INFORMAÇÃO?

SAIBA QUAIS SÃO AS OPORTUNIDADES, AS POSIÇÕES EMERGENTES, QUANTO GANHA UM PROFISSIONAL DA ÁREA E QUAIS COMPETÊNCIAS UM TALENTO DEVE REUNIR PARA SER BEM-SUCEDIDO NO MERCADO.

TÉCNICAS DE INVASÃO

ÍNDICE

INTRODUÇÃO

O avanço do digital fez a demanda por profissionais de segurança de informação (SI) saltar exponencialmente nos últimos tempos. E, nesse cenário, diversas consultorias do mercado classificaram a carreira na área como uma das mais promissoras para os próximos anos. Contudo, o contexto que se desenha é preocupante. As ameaças virtuais aumentam e a escassez de talentos em SI tira o sono das empresas.

Estudo realizado pelo (ISC)², instituto internacional sem fins lucrativos, focado em educação e certificações profissionais em segurança da informação e cibersegurança, intitulado Global Information Security Workforce Study (GISWS) 2017, constatou que dois terços das companhias não têm o número suficiente de profissionais de segurança cibernética para enfrentar os desafios com os quais se deparam atualmente.

Para chegar a essa conclusão, a entidade ouviu 19.641 profissionais de segurança em 170 países. O estudo revela, ainda, que o gap de profissionais nessa área deve atingir 1,8 milhão em 2022, aumento de 20% em relação à projeção feita em 2015. Na América Latina, 51% das empresas vão contratar mais profissionais nessa área e a escassez deve chegar a 185 mil profissionais até 2022.

A saída para essa encruzilhada? Investir na capacitação de profissionais. Aliás, é muito mais do que um investimento em um plano de carreira, é vital para o futuro e para a segurança

das informações, que é o ativo de maior valor de uma companhia. Se as organizações desejarem continuar desfrutando de todas as maravilhas da era digital, precisam arcar com o ônus da insegurança e vencê-la estando mais atentos, mais informados e alinhados às restrições corporativas e pessoais.

É por isso que neste E-book, produzido pela equipe do Técnicas de Invasão, você vai encontrar um guia completo para construir uma carreira em segurança da informação. Mostraremos as oportunidades na área, setores emergentes, guia salarial e o que fazer para se destacar nesse mercado em ebulição e cheio de oportunidades.

CAPÍTULO 1

CENÁRIO ATUAL DA SEGURANÇA DA INFORMAÇÃO

Todos os dias, manchetes em sites e jornais em todo o mundo indicam empresas e pessoas vítimas de ataques virtuais. O fato é que o cibercrime se tornou uma indústria, com estratégia, orçamento e equipes, que, segundo estimativas da fabricante de segurança digital russa Kaspersky, por meio de seu laboratório Kaspersky Lab, gera uma perda de US$ 450 bilhões por ano às companhias globalmente, o mesmo valor de 13 naves aeroespaciais. Uma estimativa da Cyberventures, consultoria internacional na área de segurança na internet, indica que crimes cibernéticos custarão ao mundo US$ 6 trilhões até 2021.

Malwares, phishing, trorjans, ransomware e outras técnicas rondam os usuários, que, quase sempre desavisados, clicam em links maliciosos e acabam sendo vítimas dos cibercriminosos, ou crackers.

Nos Estados Unidos, onde uma lei exige que companhias notifiquem o mercado sobre invasões aos seus sistemas, 72% das empresas com mais de 250 empregados sofreram ao menos um ataque cibernético em 2016, e 60% das empresas com menos de 250 empregados também foram alvos.

Globalmente, de 1986 a 2006, a Kaspersky registrou um total de 1 milhão de ameaças. Agora, são 2,2 milhões, ou 310 mil por dia. Com 647 milhões de habitantes, 20 países e quase 60% da região conectada à internet, a América Latina também está definitivamente na mira dos cibercriminosos. Nos oito primeiros meses do ano, a Kaspersky Lab bloqueou 677 milhões de ameaças na região, número 59% superior ao computado no mesmo período do ano passado. Trocando em miúdos, são 117 ataques por hora, ou 33 ataques por segundo.

Os dados têm explicação, aponta Fabio Assolini, analista sênior da equipe global de Investigação e Análise da Kaspersky Lab, uma vez que a população da América Latina segue crescendo e a conexão de internet fica mais barata, incentivando o uso da web. “Dos ataques, 85% são feitos por meio da web e 15% por e-mail”, contabiliza o executivo.
O estudo revela que os usuários no Brasil, no México e na Colômbia registraram o maior número de ataques de malware até agosto de 2017. Se considerado o per capita, no Brasil, os ataques na rede afetaram 30% dos usuários, seguido por Honduras (23,5%), Panamá (22,6%), Guatemala (21,6%) e Chile (20,6%).

O Brasil também lidera os países latino-americanos em hospedagem de sites mal-intencionados: 84% dos hosts localizados na América Latina utilizados em ataques a usuários em todo o mundo estão no País.

Na categoria ataques baseados na web, o Trojan.Clicker.HTML.Iframe.dg está em primeiro lugar. Ele foi desenvolvido para direcionar a vítima a uma página com conteúdo malicioso. Na lista dos dez maiores ataques baseados na web, em comum a maioria tem JS no nome, que se refere à

Java Script.
O Java Script é essencial para navegar pela internet. Antes, tecnologias como Flash e Java eram as mais comuns, mas elas estão morrendo e navegadores mais modernos bloqueiam esses plugins automaticamente. Agora, cibercriminosos preferem usar um Java malicioso enquanto a pessoa navega pela internet.
A segunda categoria, a de mensagens de e-mail, tem em sua maioria a extensão Trojan.PDF. Ele chega até as vítimas por meio de uma mensagem com um arquivo PDF anexado com conteúdo malicioso. Dentro, há um arquivo pequeno em Zip, que ao ser descompactado libera a ameaça. Ele instala um trojan bancário ou até mesmo um ransmware, o malware sequestrador.

Entre as ameaças off-line, é comum a infecção via um dispositivo USB, ou CD. Ele não depende da internet para infectar pessoas e é muito comum em softwares piratas, revela o analista do Kaspersky Lab. Nessa categoria, 50% da infecção acontece via pirataria, 40% por malware e 10% outros. O Brasil, mais uma vez, está na liderança desse problema, com 61%, seguido por Honduras e Peru.

As ameaças virtuais hoje estão cada vez mais indo parar no bolso das pessoas. Com nove a cada dez usuários de internet por meio de smartphones na América Latina, cibercriminosos identificaram uma janela enorme de oportunidades para obter dinheiro com o advento da mobilidade.

Somente na América Latina, segundo dados da Kaspersky Lab, foram mais de 931 mil detecções em dispositivos móveis, afetando cerca de 120 mil usuários únicos. O Brasil, como é de se esperar e até pela quantidade de smartphones, é o primeiro

da lista, com 31%. Em seguida, estão México e Colômbia.
De acordo com a Kaspersky, são três os principais riscos que os usuários de smartphones correm no mundo on-line: phishing, malware e privacidade. Uma técnica emergente é a do SMiShing, phishing, que se passa por um SMS. Nele, o cibercriminoso envia um link para que o usuário confirme informações.

Outro exemplo é o Trojan-Banker.AndroidOS.Marcher, que chega ao dispositivo depois de o usuário baixar um app supostamente oficial de bancos, por exemplo. Antes da tela real, os cibercriminosos pedem que a pessoa insira informações sensíveis da conta. Basta isso para que o hacker tenha acesso a dados valiosos.

Levantamento do Kaspersky Lab constatou que nos oito primeiros meses de 2017 foram 931 mil ataques contra dispositivos móveis na América Latina. São seis ataques por usuário.

Os malwares chegam de diversas formas. Uma delas é o Adware, que exibe propaganda invasiva no dispositivo infectado, malware ou tentativas de inserir links da web maliciosos para usuários Android ou iOS. No Brasil, 85% dos smartphones são Android. Assim, a maioria das ameaças mira o sistema operacional do Google.

O Kaspersky Lab reportou ainda um total de 5.028 ataques diferentes de códigos maliciosos e programas indesejados destinados a usuários do MacOS. Em primeiro lugar está a ameaça AdWare.OSX.Geonei.s, que geralmente se espalha via web como um aplicativo de atualização falsa para o Adobe Flash Player. O Trojan-Clicker.HTML.Iframe.dg, em segunda colocação, é a número 1 para sistemas operacionais Windows. A ameaça existe em páginas da web e, portanto, é

multiplataforma.

No mercado corporativo, o aumento das ameaças e dos alvos vem acompanhado no de um agravante. O investimento em segurança da informação em todo o mundo é de cerca de 5% a 6% do orçamento de TI, sendo que no Brasil cai para 2% a 3%. Grande parte do valor (90%) é direcionado para a prevenção.

Contudo, a segurança da informação, para que seja efetiva, engloba quatro pilares: prevenção, detecção, resposta e previsão de ameaças. Além, naturalmente, do investimento em educação dos colaboradores, o elo mais fraco da cadeia de segurança. Sabe-se que nenhum sistema ou empresa está 100% seguro. Por outro lado, é possível reduzir os riscos, evitando problemas gigantescos financeiro ou de imagem. Assim, além de espaço para mais investimento em segurança da informação por parte das empresas, deve-se fomentar um olhar holístico sobre o tema.

BÊ-Á-BÁ DOS CRIMES VIRTUAIS

Conheça algumas das técnicas usadas
por cibercriminosos contra pessoas
físicas e empresas

MALWARE

Um malware é considerado um tipo de software maligno que acessa secretamente um dispositivo sem o conhecimento do usuário. Os tipos de malware incluem spyware, adware, phishing, vírus, trojans, worms, rootkits, ramsoware e sequestradores de navegador. Ao lançar um malware por meio de um e-mail ou pela web, um cibercriminoso acessa o dispositivo do usuário.

PHISHING

Milhares de ameaças virtuais são espalhadas pela internet todos os dias. Boa parte desse montante pode ser classificada como phishing. Essa prática, como o nome sugere, corresponde à "pescaria" em português e tem o objetivo de "pescar" informações e dados pessoais importantes por meio de mensagens falsas enviadas por e-mails.
O objetivo é roubar informações como senhas, CPFs ou números de contas bancárias. Com o avanço da mobilidade, muitos criminosos virtuais passaram a usar SMS e correntes no WhatsApp e outros serviços de comunicação para aplicar o golpe.

BÊ-Á-BÁ DOS CRIMES VIRTUAIS

TROJAN

Um Trojan, ou Cavalo de Troia, é um tipo de vírus espalhado geralmente a partir de um anexo de e-mail infectado ou um download que esconde games gratuitos, aplicativos, filmes ou cartões de visita.

RANSOMWARE

O ransomware, conhecido como malware sequestrador, restringe o acesso ao sistema do usuário ao seu computador e pede que um resgate seja pago para que os dados sejam devolvidos. Os ataques de ransomware mais perigosos conhecidos até o momento são: WannaCry, Petya, Cerber, Cryptolocker e Locky.

O ransomware atinge pessoas por meio de um anexo de e-mail ou a partir do navegador de um usuário, que é atacado ao visitar um site infectado com esse tipo de malware.

Em 12 de maio de 2017, o WannaCry atacou empresas famosas, grandes companhias aéreas, bancos, hospitais e pequenos negócios. Em apenas quatro dias, ele provocou prejuízos que excederam bilhões de dólares, segundo as consultorias de segurança na internet. De acordo com levantamento da Kaspersky, só na América Latina, durante os quatro dias de atividade do WannaCry em maio, os crackers conseguiram arrecadar ilegalmente, com o pagamento de resgates, US$ 62 mil, só falando de usuários comuns.

BÊ-Á-BÁ DOS CRIMES VIRTUAIS

ROOTKIT

Um rootkit é um programa designado a fornecer a crackers acesso administrativo ao computador sem que o usuário tenha conhecimento. Tootkits podem ser instalados de várias maneiras, incluindo via anúncio de produtos de segurança e extensões de aplicativos de terceiros, que parecem seguros. Rootkits não podem se espalhar sozinhos, mas em vez disso, se tornam um componente de várias ameaças.

DDoS

Os ataques de DDoS tentam derrubar sites ou redes inteiras sobrecarregando-as com tráfego proveniente de milhares de computadores infectados, os PCs robôs, que fazem parte de redes conhecidas como botnets.

Os sites de bancos, notícias e até de governos são os principais alvos de ataques de DDoS, cujo objetivo é torná-los indisponíveis para os usuários. Além disso, tanto o alvo quanto os computadores usados na botnet são vítimas. Assim, os usuários comuns se tornam danos colaterais do ataque, sofrendo lentidão ou travamento dos seus PCs, enquanto trabalham involuntariamente para o cracker.

BÊ-Á-BÁ DOS CRIMES VIRTUAIS

BOTNET

Botnet, também conhecido como exército de zumbis, é uma rede composta por um grande número de computadores que foram infectados por malwares para atender aos comandos do cracker que a criou. Com o controle de centenas ou mesmo milhares de computadores, as botnets são geralmente usadas para enviar spam ou vírus, roubar dados pessoais ou executar ataques de DDoS. Elas são consideradas uma das maiores ameaças on-line da atualidade.

ZERO DAY

Zero Day, ou Dia Zero, se refere a um problema de segurança em um software. Há dois tipos de dia zero. Uma vulnerabilidade de dia zero é uma falha na segurança de um software e pode estar presente em um navegador ou um aplicativo. Ou um ataque digital que faz uso das vulnerabilidades de dia zero para instalar softwares maliciosos em um aparelho.

CRACKERS

Os crackers são pessoas que utilizam seus conhecimentos na área de tecnologia para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. Em alguns casos, o termo “Pirata Virtual” é usado como sinônimo para cracker.

Na outra ponta, ao contrário do cracker, o hacker possui

BÊ-Á-BÁ DOS CRIMES VIRTUAIS

conhecimentos profundos de informática e faz uso deles de forma positiva. Os hackers, que não são criminosos, dedicam boa parte do tempo para conhecer e modificar softwares, hardwares e redes de computadores.

DEEP WEB

Composta por conteúdos que não podem ser encontrados por mecanismos de busca, como o Google, a Deep Web esconde cibercriminosos dispostos a vender e a comprar informações roubadas de usuários da internet. Lá é, ainda, o local onde se compartilham novas técnicas criminosas para invasão.

FONTE: AVAST

CAPÍTULO 2

CAPACITAÇÃO, UMA FORMA DE SE DESTACAR NO MERCADO

Já é sabido que as ameaças virtuais aumentam. Contudo, há um gigantesco desafio nesse contexto: a escassez de talentos na área, algo que tira o sono das empresas. Estudo realizado pelo (ISC)², instituto internacional sem fins lucrativos, focado em educação e certificações profissionais em segurança da informação e cibersegurança, intitulado Global Information Security Workforce Study (GISWS) 2017, constatou que dois terços das companhias não têm o número suficiente de profissionais de segurança cibernética para enfrentar os desafios com os quais se deparam atualmente.

Para chegar a essa conclusão, a entidade ouviu 19.641 profissionais de segurança cibernética em 170 países. O estudo revela, ainda, que o gap de profissionais nessa área deve atingir 1,8 milhão em 2022, aumento de 20% em relação a projeção feita em 2015. Na América Latina, 51% das empresas vão contratar mais profissionais nessa área e a escassez deve chegar a 185 mil profissionais até 2022.

O levantamento, realizado com quase mil profissionais de segurança da informação da América Latina, revela que empresas reduziram os investimentos em treinamentos para seus funcionários. Um movimento na contramão do que os

analistas pregam: a capacitação dos profissionais é mais do que um investimento em um plano de carreira, é fator-chave de diferenciação no mercado.

Para piorar o quadro, outro estudo da (ISC)², realizado com mais de 3,3 mil profissionais de TI em todo o mundo, apontou que organizações não maximizam plenamente a oportunidade de empoderar os profissionais que atuam com segurança da informação.

David Shearer, CEO do (ISC)², alerta para o fato de que empresas precisam investir na capacitação dos times. "Para muitas organizações a forma mais rápida de fortalecer sua ciberdefesa é a educação continuada em segurança e o empoderamento das suas equipes de TI", comenta.

Dos respondentes da pesquisa, 43% declararam que suas organizações não oferecem recursos adequados para o treinamento em segurança. Apenas 35% concordaram que as suas sugestões em relação à segurança são postas em prática. Enquanto isso, 63% declararam que existe um número muito limitado de profissionais de segurança em suas organizações e 51% indicaram que os sistemas hoje são menos capazes de proteger contra um ciberataque do que no ano anterior.
Um passaporte para quem quer trilhar uma carreira em segurança da informação é ter uma experiência de sucesso em alguma área da Tecnologia da Informação. Sean Tierney, chefe da equipe de inteligência cibernética da Infoblox, disse recentemente ao site da Forbes: "Para ter uma carreira bem-sucedida em segurança é preciso ser ótimo em alguma outra coisa primeiro. Por exemplo, torne-se um mestre dos fundamentos das redes de dados, seja um especialista na administração de vários sistemas operacionais, ou busque

proficiência em algumas linguagens de script (Python, Bash etc)".

Rod Rasmussen, vice-presidente de CyberSecurity da Infoblox, apresentou à Forbes recomendações para quem já está em TI. "Estude segurança de rede, por exemplo. Você poderá se tornar muito rapidamente 'o guru da segurança' em sua empresa e, a partir daí, a transição se torna mais fácil."

DE OLHO NAS CERTIFICAÇÕES

Outra frente para se destacar no mercado é apostar na capacitação. Algumas certificações em segurança da informação ajudam o talento a criar as bases necessárias para seguir a trilha da constante atualização na área. Uma delas é a Certified Information Systems Security Professional (CISSP). A CISSP engloba desenvolvimento de políticas de segurança, procedimentos de desenvolvimento de software seguro, vulnerabilidades da rede, tipos de ataque e contra-medidas correspondentes, conceitos de criptografia e seus usos, planos de recuperação de desastres e procedimentos, análise de risco, leis e regulamentos essenciais, noções básicas de perícia e procedimentos de investigação computacional do crime. Contudo, não se trata de uma certificação barata, nem tampouco rápida de se obter, sendo necessários quatro meses de estudos.

A ISO 27002 também é fundamental para a carreira, sendo considerada praticamente pré-requisito para os talentos da

área. Antes conhecida como ISO 1779, a ISO 27002 é uma norma internacional que contém controles para a segurança da Informação, publicada pela International Organization for Standardization (ISO), organização internacionalmente responsável pelo desenvolvimento e publicação de normas.
Seu objetivo é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Composta por 11 seções, essa norma é praticamente um guia de como implementar a estratégia de segurança de uma companhia,
passando por itens como política de segurança da informação, gestão de ativos, segurança física e segurança em recursos humanos. Saiba mais sobre essa certificação no box.
Outra interessante é a Certified Information Systems Auditor (CISA), certificação de segurança oferecida pela Information Systems Audit and Control Association (ISACA). Como o nome diz, a certificação é focada no controle, auditoria e monitoramento de segurança dos ambientes de TI. Ela é requisito para quem quer trabalhar com auditoria de sistemas de informação. Para obter o CISA, é preciso ter, no mínimo, cinco anos de experiência em infosec e tirar mais de 450 pontos no exame, em um total de 800.
Fala-se muito no mercado, ainda, sobre a Security+. Ela serve como benchmark para várias práticas de segurança e quem conta com esse diferencial no currículo estará bem cotado em qualquer mercado do mundo.

A certificação é oferecida pela Computing Technology Industry Association (CompTIA) e entrega ao profissional certificado um conhecimento geral da segurança, cobrindo o essencial da segurança de rede, gestão de riscos, criptografia,

gerenciamento de identidades, segurança de sistemas e de sistemas organizacionais. Muitos profissionais fazem do Security+ um primeiro passo para o CISSP e para a criação de uma carreira de sucesso em segurança da informação.
Há ainda a Certified Ethical Hacker (CEHv9), umas das principais certificações internacionais voltada a profissionais da área de segurança da informação, com ênfase em profissionais que demandem conhecimentos em auditorias e teste de invasão. Veja no box outras certificações que podem ser obtidas para atuar na área.

Thiago Bordini, profissional de segurança da informação, aponta que o talento precisa ir além das certificações. “Acredito que as habilidades devem se sobressair, como paixão e ética.” Para ele, há muitas oportunidades na área, mas ainda é preciso vencer o desafio da falta de talentos. Para o executivo, esse problema tem motivo. “Vejo jovens pouco interessados ou com conhecimento superficial, pautado na internet, sobre a área e isso acaba os afastando”, acredita.

ISO 27002: O QUE É, COMO ESTUDAR E OBTER A CERTIFICAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Entenda, ainda, o que muda na carreira do profissional da área após conquistar a credencial

Profissionais que atuam no campo da segurança da informação precisam se atualizar constantemente e a certificação é o caminho ideal para adquirir conhecimento e reunir as competências necessárias exigidas pelo mercado. Nesse contexto, a ISO 27002 é fundamental para a carreira, sendo considerada praticamente pré-requisito para os talentos da área.

PORQUE ELA É IMPORTANTE?

Por ser como um guia para o profissional de segurança da informação, ela aponta caminhos e medidas para implementar e melhorar a prática de segurança de uma empresa. Ela indica que o profissional está apto para traçar uma estratégia de proteção, considerando todas as frentes da empresa. Todo talento no início da carreira deve obter essa certificação. Com ela, você aprende habilidades práticas que ajudarão a melhorar a consciência da segurança e o sentido de propriedade de sua organização.

COMO TIRAR A CERTIFICAÇÃO?

Para obter a certificação, o profissional precisa demonstrar conhecimentos sobre os conceitos básicos de segurança, como formas da informação, requisitos básicos da informação, conceitos de riscos ligados à segurança da informação, a medidas de redução do risco e aos tipos de ameaças.

A prova é composta por 40 perguntas, sendo ser preciso que o candidato acerte 65% (26 questões) para ser aprovado e receber o certificado.

O candidato terá de escolher três níveis de certificação: Foundation, que é considerado o mais básico; o Advanced, para profissionais que têm experiência prática; e o Expert, para os mais avançados em segurança da informação, como gestores de segurança da informação, chefes de escritórios de segurança ou arquitetos de segurança da informação para a área de negócio.

ONDE ESTUDAR E FAZER A PROVA?

O Técnicas de Invasão, conta com um curso preparatório para a certificação, que é totalmente gratuito. Na grade do programa, você aprende sobre conceitos básicos da segurança da informação e como proteger a empresa adequadamente, sempre levando em conta políticas, tecnologia e, especialmente, pessoas.
O Técnicas de Invasão estabeleceu, ainda, parceira com o EXIN para que os alunos possam tirar o certificado da ISO 27002. O EXIN tem como objetivo fornecer certificação independente e acreditação para gerenciamento da informação, tendo presença em todo o mundo.
A preparação para o exame, com a ajuda dp Técnicas de

Invasão, é simples. Um dos alunos da Técnicas de Invasão, por exemplo, conseguiu passar na prova com um planejamento para o exame de oito dias.

9 CERTIFICAÇÕES QUE NÃO PODEM FICAR DE FORA DO CURRÍCULO

1. Information Systems Security Engineering Professional (ISSEP/CISSP)

Desenvolvido em conjunto com a Agência de Segurança dos EUA (NSA), a Information Systems Security Engineering Professional (ISSEP) abrange a integração de metodologias e melhores práticas de segurança em todos os sistemas de informação, incluindo projetos, aplicações e práticas de negócios.

2. EC-Council Licensed Penetration Tester

A certificação LPT demonstra a capacidade de um profissional de auditoria em segurança de rede para realizar testes de invasão e recomendar ações corretivas para quaisquer deficiências encontradas.

3. GIAC Certified Penetration Tester

A certificação GPEN é para profissionais de segurança que avaliam redes e sistemas alvo para encontrar vulnerabilidades.

4. GIAC Security Essentials

A GSEC é direcionada para profissionais que querem demonstrar que estão qualificados para aplicações de tarefas de segurança relacionadas a uma ampla gama de sistemas de TI.

5. Cybersecurity Forensic Analyst

O CSPA prova que os detentores de seu certificado podem conduzir uma análise global dos sistemas de informação, interpretar apropriadamente a evidência e entregar resultados das investigações para os acionistas da empresa de forma eficaz e eficiente. A certificação também demonstra que os profissionais podem realizar essas análises dentro de um prazo limitado.

6. EC-Council Certified Secure Programmer

A maioria das vulnerabilidades de software acontece devido a erros de programação, fazendo emergir agora o que se chama de segurança by design. A ECSP tem provado que eles podem desenvolver código de alta qualidade que faz uso das melhores práticas de programação para proteger contra vulnerabilidades.

7. Check Point Certified Security Expert

A CCSE ensina profissionais de segurança como construir, modificar, implementar e solucionar problemas de verificação de segurança em sistemas no sistema operacional Gaia.

8. Certified Secure Software Lifecycle Professional (CSSLP)

O CSSLP valida a capacidade do profissional para desenvolver protocolos de aplicação e segurança de software em suas organizações e reduzir vulnerabilidades.

9. Security Security Certified Practiceser (SSCP)

Muitos profissionais de segurança começam suas carreiras obtendo a certificação do Security Security Certified Practiceser (SSCP). O SSCP reconhece os candidatos que entendem conceitos de segurança fundamentais, sabem como usar ferramentas de segurança básicas e podem monitorar sistemas e manter medidas para prevenir incidentes de segurança.

CAPÍTULO 3

OPORTUNIDADES DE CARREIRA EM CIBERSEGURANÇA E ÁREAS EMERGENTES

Segundo o site tom's IT Pro, as certificações em segurança da informação são porta de entrada para atuar em algumas áreas. Profissionais com o Security Security Certified Practiceser (SSCP) normalmente atuam como administradores de rede, administradores de sistemas, especialistas em segurança ou consultores de segurança.

Aqueles com um Certified Information Systems Security Professional (CISSP) são mais comumente contratados como analistas de segurança e engenheiros de sistemas de segurança. No entanto, o CISSP é uma ampla certificação com requisitos de alta experiência, para que se possa atuar como gerente de segurança, consultor, diretor de TI e chief information security officer (CISO), auditor e arquiteto de rede.

O U.S. Bureau of Labor Statistics (Secretaria de Estatísticas Trabalhistas dos Estados Unidos) estima que haverá

crescimento de 37% em posições relacionadas à segurança da informação entre 2012 e 2022. O salto tem motivo. Tecnologias emergentes vão demandar, de forma contínua, mais atenção às práticas de proteção corporativas.

Segundo consultores desse mercado, o especialista em segurança do futuro precisará garantir que a proteção esteja embutida em todas as camadas da companhia. Mais do que isso: ela terá de ser garantida no desenvolvimento das soluções, formando o conceito de segurança by design.

Thiago Bordini, profissional de segurança da informação, destaca que há, atualmente, um grande campo de atuação em segurança da informação, com diversas vertentes emergentes para se trabalhar, muito em função dos avanços tecnológicos, da evolução das técnicas de cibercrime e do investimento crescente no tema por parte das empresas. Ele cita alguns exemplos: inteligência cibernética, forense computacional, cibersegurança, segurança para internet das coisas (IoT) e cloud.

O pulo do gato é ir atrás. Isso aconteceu com ele. “Meu interesse surgiu cedo, quando passei a ter contato com o tema ainda na faculdade. Desde então, procurei encontrar uma área em segurança da informação, em que eu me encaixava melhor. Então, cheguei à inteligência cibernética, meu foco de atuação há mais de seis anos”, relata.

Cibersegurança: diretamente do campo de batalha

Analistas do mercado indicam que a segurança cibernética será "a segurança" da indústria do futuro. Com IoT cada vez mais sob os holofotes, a maioria das atividades será realizada por meio da internet, o que levará ao salto de ameaças à privacidade e à segurança da informação.

Existem várias perspectivas na indústria que vão desde segurança móvel, infraestrutura de segurança Wi-Fi, desenvolvimento de estrutura de segurança IoT, segurança do site, serviços VPN, criptografia de arquivos, segurança bancária on-line e segurança cibernética miliar.

Contudo, sem dúvida alguma, a de maior destaque é a cibersegurança. Segundo estudo recente da Delloite, o mercado de cibersegurança recrutará mais de 1,5 milhão de talentos até 2019. Outro levantamento da Cybersecurity Nexus (CXS) da Isaca nos Estados Unidos aponta que 59% das companhias recebem pelo menos cinco candidatos para cada vaga em cibersergurança. O número de pessoas interessadas na área ainda é baixo, mas tenderá a crescer nos próximos anos, com profissionais atentos especialmente aos salários atraentes da área.

O QUE LER?

Além de artigos na web, blogs, revistas, sites de notícias e fóruns para troca de conhecimento, o talento de tecnologia da informação deve consumir certo tempo lendo livros sobre o tema. Abaixo algumas dicas:

"A Arte de Enganar", de Kevin D. Mitnick, que retrata métodos de ataques nas maiores organizações dos Estados Unidos. É um livro macro que abrange a importância de investir na conscientização dos funcionários, e demonstra que o elo mais fraco sempre será o ser humano.

"Direito Digital 5a edição", da Patrícia Peck, advogada especializada em direito digital, que explora os conceitos envolvidos em segurança da informação e no direito digital.

"Cyber War: The Next Threat to National Security and What to Do About It Paperback", sem tradução para o português, foi escrito por Richard A. Clarke, autor do best seller Times Against All Enemies, ex-assessor presidencial e especialista em antiterrorismo. Na obra, ele emite um alerta oportuno e arrepiante sobre a vulnerabilidade da América à ciberguerra.

CAPÍTULO 4

QUEM SÃO, O QUE FAZEM E QUANTO GANHAM TALENTOS DE SEGURANÇA DA INFORMAÇÃO

Dados de junho de 2017 da (ISC)², instituto focado em educação e certificações profissionais em Segurança da Informação e Cibersegurança, apontam que, globalmente, 70% dos chief security officer (CISOs) aumentarão sua força de trabalho neste ano: 30% desejam expandir em 20% ou mais.

As áreas de saúde, varejo e manufatura particularmente são as que mais devem aumentar as contratações, com quase 40% em cada setor dizendo que planeja ampliar sua força de trabalho em 15% ou mais.

A posição mais procurada globalmente é para gerenciamento de operações e segurança. Sessenta e dois por cento dos CISOs indicam que há poucos profissionais para esse cargo, seguido por gerente de incidentes, ameaças e forense, com 58%. Na verdade, esta última posição é a que apresenta a maior demanda na América Latina (63%) e no Oriente Médio e África (65%). Apesar dos esforços dos gestores para aumentar a contratação, a demanda historicamente tem ultrapassado a oferta de mão de obra capacitada.

Para ser um profissional de segurança da informação, não basta apenas investir em capacidades técnicas e certificações. Pesquisa recente realizada pelo (ISC)² apontou que os gerentes encarregados de contratações classificam capacidade de comunicação (62%) e capacidade analítica (52%) como competências mais desejadas nos novos candidatos, enquanto

que os profissionais de TI citam computação e segurança na nuvem (64%), e avaliação e gestão de risco (40%) como as principais competências necessárias. Segundo a empresa de recrutamento e seleção de talentos, Robert Half, segurança da informação é a segunda área em TI mais difícil de encontrar talentos, logo atrás de desenvolvimento de software.

Para as companhias que recrutam talentos na área, ter um perfil inovador e curioso é fundamental, já que sempre há novidades e atualizações nesse mercado. Além disso, conhecimento do inglês se mostra importante, já que grande parte da literatura está no idioma.

Thiago Bordini, profissional da área, acrescenta outros itens à lista. “Os desafios estão na atualização constante, associados à velocidade que surgem novas ameaças, estratégias de defesa e tecnologias. Isso tudo provoca uma estafa de conhecimento se não focarmos no que é prioridade.” Há ainda a necessidade de ser colaborativo, para que se busque alinhamento com outras áreas, ter foco na resolução de problemas e raciocínio dedutivo.

O que fazem os talentos de segurança da informação ?

Há diferentes funções em segurança da informação. O site norte-americano PayScale, que compila salários e benefícios de profissionais de diversas áreas, listou cinco importantes profissionais da área e suas atividades.

1. Administrador de segurança de rede

Funções:

1. Administra e mantém firewalls.

2. Implementa atualizações de segurança de rede, patches e medidas preventivas.

4. Gerencia e atualiza sistemas de prevenção de malware.

2. Administrador de segurança de sistemas

Funções:

1. Monitora a segurança dos sistemas e responde a incidentes de segurança.

2. Cria, modifica e exclui contas de usuário conforme necessário.

3. Monitora a segurança dos sistemas e responde a incidentes de segurança.

3. Coordenador de segurança de rede

Funções:

1. Analisa o desempenho da rede e identifica as áreas de preocupação.

2. Desenvolve e implementa planos de ação para corrigir áreas problemáticas.

3. Planeja, testa e executa atualizações quando necessário.

4. Analista de segurança de dados

Funções:

1. Realiza auditorias de segurança e avaliações de risco.

2. Investiga tentativa de violações e fraquezas de segurança.

3. Cria, implementa e atualiza políticas de segurança.

5. Gerente de segurança de sistemas de informação

Funções:

1. Dirige, orienta e treina profissionais da segurança da informação.

2. Gerencia auditorias de segurança e avaliações de ameaças.

3. Revisa, implementa e atualiza políticas de segurança para toda a empresa.

E os salários?

Segundo o Guia Salarial 2017 da Robert Half, no Brasil, um analista de segurança recebe entre R$ 3,1 mil a R$ 12 mil, dependendo da senioridade. Em patamares mais altos, está o gerente de segurança, com salários entre R$ 15,1 mil e R$ 22 mil, dependendo do porte da organização.Algumas certificações podem turbinar essas cifras em até 9%. No caso da CISSP, o adicional é de 6%, por exemplo, segundo a Robert Half.

Já o site Love Mondays, alimentado por profissionais de diversas áreas que indicam seus ganhos de forma anônima, o salário médio para Especialista em Segurança da Informação é de R$ 8.057/mensal. A variação é de R$ 3.523 a R$ 15.408. Esta estimativa salarial tem base em dez salários postados por funcionários no Love Mondays para esse cargo.

SEGURANÇA (C)

CARGO	2016	2017	%
Gerente de Segurança da Informação	R$ 15.000 - R$ 22.000	R$ 15.100 - R$ 22.000	0.3%
Analista de Segurança	R$ 3.000 - R$ 12.000	R$ 3.100 - R$ 12.000	0.7%
Analista de Continuidade de Negócio	R$ 7.000 - R$ 12.000	R$ 7.140 - R$ 12.240	2.0%
Auditor de TI	R$ 4.000 - R$ 20.000	R$ 4.200 - R$ 21.000	5.0%

Fonte: Guia Salaria Roberto Half 2017

(C) Aos salários pode ser acrescentado o percentual abaixo, de acordo com as habilidades específicas:

Certified Information System Security Professional (CISSP)	+6%	Cisco network Administration	+9%
Check Point Firewall Administration	+7%	Linux/Unix Administration	+8%

Fonte: Guia Salaria Roberto Half 2017

Nos Estados Unidos, o salário de um administrador de segurança de redes, por exemplo, varia de US$ 107,740 a US$ 155,250 anualmente, segundo dados da Robert Half em seu Guia Salarial 2017.

Especificamente em cibersegurança, nos Estados Unidos, a média é de US$ 116, ou aproximadamente US$ 55,77 por hora. O valor é quase três vezes a renda média nacional para trabalhadores salariais e de tempo integral, de acordo com o Bureau of Labor Statistics dos Estados Unidos.

Não só pelos salários, mas pelas oportunidades de aprendizado diário de segurança da informação, que está longe de ser monótono, o setor se tornou atraente para talentos.
Você vai ficar de fora?

Sobre Bruno Fraga

Bruno Fraga, professor e idealizador do projeto Técnicas de Invasão, que ensina pessoas sobre segurança da informação e proteção de dados, projeto que em sua última edição alcançou mais de 3 milhões de pessoas na internet. Fraga é brasileiro, mas divide-se entre Irlanda e Coreia do Sul.

Inscreva-se no Mini-Treinamento em Técnicas de Invasão

QUANDO SERÁ?

DE 5 A 12 DE MARÇO
100% ONLINE E GRATUITO

Acesse e garanta a sua vaga!

www.tecnicasdeinvasao.com