SANS SECURITY AWARENESS

Biuletyn Bezpieczeństwa Komputerowego

Kariera w cyberbezpieczeństwie

Wstęp

Organizacje i rządy na całym świecie nieustannie padają ofiarą ataków internetowych, praktycznie nie ma już dnia bez medialnych doniesień dotyczących cyberbezpieczeństwa. Stąd też ogromne zapotrzebowanie na osoby wyszkolone w zakresie bezpieczeństwa teleinformatycznego, które będą w stanie ochronić nas przed wzrastającym zagrożeniem. Szacuje się, że aktualnie na całym świecie brakuje około trzech milionów specjalistów w dziedzinie cyberbezpieczeństwa. Czy rozważałeś już karierę jako specjalista ds. bezpieczeństwa teleinformatycznego? Jest to szybko rozwijająca się i dynamiczna branża z dużą ilością specjalizacji do wyboru w tym m.in.: informatyka śledcza, bezpieczeństwo stacji roboczych (end point), ochrona infrastruktury krytycznej, reagowanie na incydenty, bezpieczne programowanie oraz prowadzenie szkoleń w zakresie świadomości bezpieczeństwa. Dodatkowo kariera w cyberbezpieczeństwie pozwala na pracę z każdego zakątka świata z niesamowitymi świadczeniami pracowniczymi| i jest pracą mającą głębszy sens.

Czy konieczne jest wykształcenie w zakresie cyberbezpieczeństwa?

Zdecydowanie nie. Niektórzy z najlepszych specjalistów od cyberbezpieczeństwa mają wykształcenie nietechniczne w takich kierunkach jak: filologia czy medycyna. W branży są też nauczyciele historii, mechanicy samochodowi, artyści i gospodynie domowe. Kluczowa do opanowania dziedziny cyberbezpieczeństwa jest ciekawość jak działają rzeczy. Gdy tylko zrozumiesz jak funkcjonuje technologia będziesz w stanie poprawiać jej bezpieczeństwo. To co najbardziej ekscytujące to to, że nauczysz się jak działają różne technologie również dla własnych potrzeb i ułatwień we własnym domu.

Jak zacząć?

Nie wiesz od czego zacząć. Próbuj różnych technologii i sprawdź co cię naprawdę interesuje:

programowanie – naucz się podstaw programowania, najlepiej zacząć od Pythona, HTML lub Javascript. Jeśli nie jesteś pewien od czego zacząć rozważ internetowe kursy lub przeczytaj jedną z podstawowych książek do programowania

systemy – naucz się podstaw administrowania systemami operacyjnymi: Linux, Windows. Jeśli chcesz stać się prawdziwym pasjonatem zacznij od Linuksa. Umiejętność administrowania Linuksa z pozycji konsoli to potężne narzędzie przydatne niezależnie od tego jako ścieżkę ostatecznie obierzesz

aplikacje – naucz się konfigurowania, uruchamiania i utrzymania aplikacji takich jak serwer DNS czy serwer WWW;

sieci komputerowe – poznaj zasady działania sieci komputerowych, przechwytuj i analizuj ruch sieciowy, żeby zrozumieć jak działa komunikacja między różnymi urządzeniami. W sieci domowej to fajna zabawa, zwłaszcza jeśli masz do niej podłączone rozmaite urządzenia.

Świetnym sposobem do nauki jest stworzenie domowego laboratorium testowego. Jest to całkiem proste, dzięki wykorzystaniu wirtualizacji możesz stworzyć wiele wirtualnych urządzeń w jednym komputerze. Możesz też skorzystać z chmury obliczeniowej takiej jak Amazon AWS czy Microsoft Azure. Gdy zainstalujesz już różne systemy rozpocznij interakcję między nimi i staraj się jak najwięcej nauczyć. Inną możliwością jest praca i spotykanie się z osobami ze środowiska cyberbezpieczeństwa. Pomyśl nad udziałem w jednej z konferencji w twoim otoczeniu (z reguły nazwy konferencji oznaczone są przyrostkiem „con"). W każdym większym mieście odbywa się przynajmniej kilka konferencji rocznie. Znaną serią spotkań przeznaczoną dla osób początkujących jest wydarzenie z serii Bsides [w Polsce - BSidesWarsaw w Warszawie - redakcja]. Najtrudniejsze jest znalezienie tego pierwszego wydarzenia bądź spotkania. Uczestnictwo w pierwszym wydarzeniu otwiera niezliczoną ilość nowych możliwości. Kolejnymi sposobem jest czerpanie wiedzy z takich źródeł jak: YouTube, fora internetowe, blogi specjalistów, uczestnictwo w internetowych rywalizacjach typu CTF (Capture The Flag). Ponadto dostępnych jest wiele programów startowych dla kariery takich jak: CyberTalent Immersion Academics, Cyber Aces i programy Cyber Patriot.

Nie pozwól na to aby powstrzymał cię brak formalnego wykształcenia, czy przekonanie o braku doświadczenia zawodowego. To właśnie twoje dotychczasowe doświadczenia z innej branży są unikalną wartością dodaną, której koniecznie potrzebuje obszar bezpieczeństwa teleinformatycznego. Kluczem jest zapał do nauki. Gdy będziesz rozwijać swoje umiejętności i zaczniesz obcować z ludźmi z branży, to możliwości same przyjdą.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor wydania

Heather Mahalik *(@heathermahalik) – dyrektor ds. inżynierii śledczej (Forensic Engineering) w ManTech CARD, a także starszy wykładowca i autorka kursów organizowanych przez SANS Digital Forensics and Incident Response (DFIR). Związana od 17 lat z ukochaną przez nią branżą cyberbezpieczeństwa. Wpisy jej autorstwa dostępne są na:* www.smartforensics.com

Źródła

Bsides:	http://www.securitybsides.com
CyberTalent Immersion Academies:	https://www.sans.org/cybertalent/cybersecurity-career/seekers
Cyber Aces:	https://www.cyberaces.org
Cyber Patriot:	https://www.uscyberpatriot.org/
Code Academy:	www.codeacademy.com