OUCH! فوریه 2022

ماهنامه آگاهی از امنیت اطلاعات برای شما

حرفه ی امنیت سایبری برای همه

مفدمه

تقریبا همه روزه در مورد امنیت سایبری در اخبار میخوانیم و میبینیم که سازمانها و دولت ها همچنان در سراسر جهان توسط باج افزارها، کلاهبرداری ها و حملات سایبری مورد حمله قرار میگیرند. تقاضاهای بسیاری برای کمک به دفاع در برابر تهدیدات رو به رشد، برای افرادی که در زمینه امنیت سایبری آموزش دیده اند وجود دارد. در حقیقت، مطالعات اخیر تخمین زده است که تقریبا 3 میلیون فرصت شغلی جدید در زمینه امنیت سایبری در سراسر جهان وجود دارد.

آیا در نظر دارید شغل شما به عنوان یک حرفه ای در زمینه امنیت سایبری باشد؟ امنیت سایبری با توجه به پویایی و شاخه های متعددی که دارد به شما این امکان را میدهد تا در حوزه های تخصصی مختلف حق انتخاب داشته باشید. این موقعیتهای شغلی شامل زمینه هایی مانند جرم شناسی(forensics)، آگاهی و آموزش، امنیت نقطه پایانی(endpoint Security)، زیرساختهای حیاتی، پاسخ به حوادث (incident Response)،کد نویسی ایمن(secure coding) و سیاستهای امنیتی (Policy) است. اشتغال درامنیت سایبری به شما این را امکان می دهد تا درهرنقطه ای از جهان مشغول به کار شده و ازمزایای مختلف آن بهره مند شوید.

آیا به مدرک در علوم و رشته مربوط به کامپیوتر نیاز است؟

قطعا خیر. بسیاری از بهترین متخصصان امنیتی سوابق غیر فنی دارند. نکته اصلی اشتیاق به یادگیری است.زمانی که متوجه شدید که فناوریها چگونه کارمیکنند(و چگونه آسیب می بینند)، بهتر میتوانید آنها را ایمن کنید. امنیت سایبری بسیار هیجان انگیز است چون میتوانید آموزش را از منزل خود شروع کنید.

چگونه شروع کنم؟

شروع به بررسی و کاوش در حوزه های مختلف کرده تا علایق خود را کشف کنید. شما اغلب میتوانید تنها با رایانه ها یا دستگاههایی که در منزل دارید شروع کنید.

- کد نویسی: **اصول برنامه نویسی را بیاموزید. پایتون(Python، HTML)، یا جاوا اسکریپت، همگی زبانهای خوبی برای شروع کار هستند. در خصوص برنامه نویسی ابتدایی میتوانید آموزش توسط سایت های آموزشی آنلاین و یا خواندن کتاب در این مورد را مد نظر قرار دهید.**
- سیستم ها: **اصول مدیریت یک سیستم عامل مانند لینوکس یا ویندوز را بیاموزید. اگر واقعا میخواهید که حرفه ای شوید، تجربیات خود را در استفاده از خط فرمان(Command Line) و یا اسکریپ نویسی افزایش دهید.**
- برنامه ها: **نحوه پیکربندی، اجرا و نگهداری برنامه های کاربردی مانند وب سرورها را بیاموزید**
- شبکه سازی: **بیاموزید که تجهیزات و کامپیوترها در شبکه چگونه با یکدیگر ارتباط برقرار میکنند و تجزیه و تحلیل ترافیک شبکه چگونه است. این مورد میتواند بسیار سرگرم کننده باشد زیرا خانه شما به احتمال زیاد در حال حاضر یک محیط شبکه ای با انواع و اقسام تجهیزات متصل به هم است.**
- فضای ابری فناوری ها: **نحوه عملکرد سرویس های ابری و روشهای مختلف استفاده از آنها را بیاموزید.**

آزمایشگاه شخصی خود را در منزل راه اندازی کنید. شما میتوانید از منابع آنلاین ابری مانند AWS آمازون یا Azure مایکروسافت استفاده کنید. یا میتوانید سیستمهای مجازی متعددی روی یک رایانه فیزیکی با استفاده از سرویسهای مجازی سازی بسازید. اگر میخواهید مستقیما با سخت افزار کار کنید، کامپیوترهای ساده و ارزان قیمتی مانند Raspberry Pi یا Arduino خریداری کنید. زمانیکه سیستم خود را راه اندازی و آماده به کار نمودید، شروع به کار با آنها نموده و هر آنچه که میتوانید در مورد پیکربندی و بهینه سازی آنها بیاموزید، یا شروع به برنامه نویسی وکدنویسی روی این سیستمها نمائید. راه درست یا راه غلط برای شروع کار وجود ندارد، فقط مسیر علایق خود را دنبال کنید.

راه عالی دیگری برای شروع کار، ملاقات و همکاری با دیگران در زمینه امنیت سایبری است. شرکت در یک کنفرانس امنیت سایبری محلی یا یک انجمن مجازی(Virtual con) مانند Bsides یا SANS New2Cyber را در نظر داشته باشید. سخت ترین قسمت کار پیدا کردن اولین رویداد یا گردهمایی است. پس از حضور، با سایر شرکت کنندگان ارتباط برقرار کرده و شبکه حرفه ای خود را گسترش دهید.

گزینه های دیگر برای یادگیری امنیت سایبری شامل ویدیوهای YouTube، گوش دادن به پادکست ها، بازدید از انجمن های آنلاین، اشتراک در وبلاگ های متخصصان امنیتی، یا شرکت در رویدادهای آنلاین Capture the Flag (CTF) است. در نهایت، اجازه ندهید تحصیلات یا پیشینه شما مانع پیشرفت شما شوند. اشتیاق به یادگیری و کمک به دیگران، و همچنین توانایی "خارج از چارچوب فکر کردن یا داشتن خلاقیت" از ویژگی های کلیدی هستند. زمانی که شروع به توسعه مهارت های فنی خود کنید و با دیگران ملاقات کنید، فرصت ها خود به خود به وجود خواهند آمد.

سردبیر مهمان

Lodrina Cherne (hexplates@) مدافع اصلی امنیت در Cybereason است که نوآوری و توسعه بهترین شیوه‌های مربوط به استانداردها و سیاست‌های امنیت سایبری را هدایت می‌کند. او همچنین یک مدرس معتبر در موسسه SANS است که در آنجا به متخصصان امنیت اطلاعات کمک می کند تا درک اساسی خود را از جرم شناسی دیجیتال و پاسخ به حوادث (DFIR) ارتقا دهند.

منابع

کنفرانسهای امنیتی Bsides: http://www.securitybsides.com/
زنان در امنیت سایبری: https://www.wicys.org/
لیست پخش یوتیوب New2Cyber: https://youtube.com/playlist?list=PLtgaAEEmVe6BQkZiJC5nIk9xx74QTGtsZ
آکادمی های سایبری SANS: https://www.sans.org/scholarship-academies/
SANS Cyber Aces: https://www.cyberaces.org
پادکستهای امنیت سایبری: https://www.sans.org/blog/cybersecurity-podcast-roundup/

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو