آشنایی با شغل مهندس امنیت شبکه

چگونه یک مهندس امنیت شبکه شویم؟

امنیت یکی از جذاب‌ترین حوزه‌های فناوری‌اطلاعات است که افراد زیادی دوست دارند در این حوزه مشغول به کار شوند. با این حال، ورود به این حوزه کار ساده‌ای نیست، زیرا یک کارشناس امنیتی برای آن‌که بتواند کار خود را به بهترین شکل انجام دهد، مجبور است دانش زیادی در ارتباط با مباحث مختلف همچون برنامه‌نویسی، شبکه، سیستم‌عامل و... داشته باشد. مشکل دیگری که افراد با آن روبرو هستند به تنوع مشاغل حوزه امنیت باز می‌گردد که هر یک اشاره به تخصص خاصی دارند.

به‌طور معمول، شرکت‌ها از یک کارشناس امنیت شبکه انتظار دارند در ارتباط با دیوارهای آتش، شبکه‌های خصوصی مجازی، تجزیه و تحلیل خط‌مشی‌ها و پیکربندی، فیلترینگ شبکه، فناوری‌های مقابله با هرزنامه‌ها، تشخیص نفوذ، کنترل و نظارت بر شبکه، رصد بسته‌ها، مدیریت گزارش‌ها و ترکیبی از مهارت‌های نرم اطلاعات کافی داشته باشند. سایت Simply Hired می‌گوید: «چشم‌انداز فرصت‌های شغلی برای متخصصان امنیت شبکه روشن است. مهندسان امنیت شبکه باید جنبه‌های امنیتی زیرساخت‌ها و تجهیزات شبکه را بررسی کرده و اطمینان حاصل کنند سامانه‌های تحت شبکه در صورت بروز نقض‌های امنیتی و تهدیدات سایبری مقاوم هستند و در صورت بروز مشکل یا خراب شدن سامانه‌ها در اثر حملات هکری، بلایای طبیعی یا سایر تهدیدات در کوتاه‌ترین زمان شبکه به وضعیت عادی خود باز خواهد گشت یا این امکان وجود دارد تا بخشی که آلوده به بدافزارها است را از شبکه اصلی جدا کرد تا امکان هدایت و تخصیص منابع به ترافیک عادی شبکه فراهم شود.»

افرادی که قصد دارند به عنوان مهندس امنیت شبکه در سازمانی مشغول به کار شوند، مجبور هستند دانش میان‌رشته‌ای در حوزه‌های فناوری‌اطلاعات، امنیت اطلاعات، شبکه‌سازی و مهندسی داشته باشند. فارغ‌التحصیل رشته‌های علوم کامپیوتر و فناوری‌اطلاعات باید پس از اخذ مدرک دانشگاهی به فکر دریافت مدارک بین‌المللی نیز باشند. تقریبا هیچ شرکت و سازمانی فارغ‌التحصیلان رشته‌های علوم کامپیوتر را بدون داشتن مدارک تخصصی امنیت استخدام نمی‌کند، زیرا دروس دانشگاهی مباحث تخصصی و به‌روز حوزه امنیت را آموزش نمی‌دهند و مهم‌تر آن‌که افراد در طول مدت تحصیل تنها با مباحث تئوری و کاملا ساده حوزه امنیت آشنا می‌شوند. به‌طور معمول، فرآیند آموزش با دوره سکوریتی پلاس و پس از آن CEH آغاز می‌شود، اما دقت کنید مدارک فوق برای احراز شغلی همچون مهندس امنیت شبکه کافی نیست. در ادامه باید به فکر دریافت گواهینامه مدرک متخصص تائیدشده امنیت سیستم‌های اطلاعاتی (CISSP) سرنام Certified Information Systems Security Professional یا دستیار تایید شده شبکه سیسکو (CCNA) سرنام Cisco Certified Network Associate باشید. قبل از آن‌که به فکر حضور در دوره‌های CISSP یا CCNA باشید در ارتباط با شرح وظایف و حقوقی که یک کارشناس امنیت شبکه دریافت می‌کند تحقیقی انجام دهید. یک کارشناس امنیت شبکه قبل و بعد از استخدام در یک سازمان مجبور است سطح مهارت و دانش خود در ارتباط با مهارت‌های سخت و نرم را بهبود بخشد. مهارت سخت (hard skill) به مباحث فنی و تخصصی حوزه کاری اشاره دارد. به‌طور مثال، آشنایی با نحوه پشتیبانی از سامانه‌های کلاینتی و دسکتاپ، آشنایی با

یک یا چند زبان برنامه‌نویسی (عمدتا پایتون به منظور اسکریپت‌نویسی) و مدیریت کامپیوترها در کنار مباحث تخصصی و فنی امنیت شبکه اشاره دارد. در مقابل مهارت‌های نرم‌افزار (soft skills) به مهارت‌هایی در زمینه برقراری ارتباط با همکاران و مدیران، حل مسائل و تصمیم‌گیری‌ها اشاره دارند که بیشتر روی جنبه‌های فکری و خلاقیتی متمرکز هستند.

به‌طور مثال، در برخی موارد با مشکلات امنیتی خاصی روبرو می‌شوید که برای حل آن‌ها باید یک راه‌حل خلاقانه ارائه کنید. مهندسان امنیت شبکه برای غلبه بر تهدیدات سایبری ناشناخته و جدید مجبور هستند سطح دانش تئوری و فنی خود در ارتباط با مباحث امنیتی شبکه‌ها را دائما به‌روز کنند. این موضوع شامل بررسی فناوری‌ها و ابزارهای جدیدی می‌شود که به دنیای امنیت و شبکه وارد می‌شوند. به عبارت دقیق‌تر، یک مهندس امنیت شبکه مجبور است برای پیشبرد هرچه بهتر وظایف خود با راه‌حل‌های نوین دنیای شبکه‌ها آشنا باشد تا بتواند خط‌مشی‌های امنیتی را در شبکه‌های ارتباطی یک سازمان پیاده‌سازی کند.
بهترین روش برای به‌روز نگه داشتن سطح دانش، مطالعه نشریات امنیتی است که ابزارها و بدافزارهای جدید و راه‌حل‌های امنیت سازمانی را نقد و بررسی می‌کنند. مهندسان امنیت شبکه برای آن‌که بتوانند بر چالش‌های روزانه غلبه کنند باید از یکسری مهارت‌های خاص در محیط کار استفاده کنند. از مهم‌ترین وظایف یک مهندس امنیت شبکه به موارد زیر می‌توان اشاره کرد:

- **نیازهای امنیتی شبکه را ارزیابی کنید**

مهندسان امنیت شبکه به عنوان بخشی از وظایف خود باید روزانه مواردی همچون وضعیت دیوارآتش و تنظیمات مرتبط، عملکرد ضدهرزنامه، وضعیت ضدویروس‌ها، وضعیت فیلترینگ محتوای وب، آماده‌سازی نسخه‌های پشتیبان از داده‌های حساس، بررسی خط‌مشی تغییر گذرواژه در یک بازه زمانی مشخص، وضعیت ضدبدافزار و ضد فیشینگ را بررسی کنند. در برخی از سازمان‌ها این وظایف به شکل هفتگی انجام می‌دهد، در حالی که در سازمان‌های بزرگ این وظایف به شکل روزانه انجام می‌شوند. مهندسان امنیت شبکه پس از ارزیابی دقیق شبکه سازمانی در مرحله بعد باید راه‌حل‌هایی که خطر تهدیدات سایبری را کاهش می‌دهند را در قالب یک سند راهبردی آماده و به دپارتمان‌های امنیت و شبکه ارائه دهند تا در صورت لزوم زیرساخت‌های شبکه بازبینی شده و اگر نیاز است شبکه‌ها بازطراحی شوند. آگاهی در مورد گیت‌وی‌های امنیتی وب، امنیت محیطی، کنترل دسترسی به شبکه، امنیت نقطه پایانی و سامانه‌های تشخیص و پیشگیری از نفوذ اهمیت ویژه‌ای دارند. به دلیل این‌که فناوری‌های نوینی همچون MPLS، SD-WAN، HAIPE/IP و QOS به تدریج در تمامی شرکت‌ها به شکل گسترده استفاده خواهند شد، لازم است درباره عملکرد این فناوری‌ها اطلاعات کافی داشته باشید.

- **مشارکت در تدوین خط‌مشی‌های جامع امنیت شبکه**

به‌طور مثال، گذرواژه‌هایی که کاربران از آن‌ها استفاده می‌کنند باید در چه بازه زمانی تغییر پیدا کند، از چه فناوری‌هایی باید استفاده شود، در زمان بروز حمله چه اقداماتی انجام شود، استراتژی سازمان در ارتباط با انعطاف‌پذیری سایبری چیست، خط‌مشی‌های امنیتی چگونه باید پیاده‌سازی شوند و چه افرادی مجاز هستند به اسناد محرمانه و مالی دسترسی داشته باشند.

- **تمرکز روی استراتژی بازیابی پس از حمله هکری**

مهندسان امنیت شبکه در تهیه برنامه‌های بازیابی پس از فاجعه نقش کلیدی دارند، به همین دلیل در تدوین یک برنامه راهبردی کارآمد با مدیران ارشد سازمان در تعامل هستند و نقشه راه بازیابی پس از حمله را آماده کرده و با مدیران واحدهای مختلف به‌اشتراک قرار می‌دهند. این تعامل باعث می‌شود سازمان در زمان بروز یک حمله سایبری برآوردی از خسارت‌ها داشته باشد. به عبارت دقیق‌تر، سازمان‌های بزرگ می‌دانند هیچ شبکه‌ای ایمن نیست و پس از یک حمله هکری ضررهای مالی متوجه سازمان می‌شود، بر همین اساس سعی می‌کنند یک تخمین اولیه در این زمینه به دست آورند. مهندسان امنیت شبکه باید به‌طور مرتب آزمایش‌های بازیابی پس از حادثه را انجام دهند، نتایج این آزمون‌ها را در اختیار مدیران مربوطه قرار دهند و هرگونه تغییر برای رفع نواقص را اعمال کنند. مهندسان امنیت شبکه باید ارزیابی‌های تجاری سالانه‌ای در ارتباط با چالش‌های امنیتی انجام دهند و گزارشی ساخت‌یافته و مفصل در اختیار مدیرعامل و اعضا هئیت مدیره قرار دهند تا این افراد بدانند به دلیل حملات هکری در یک سال چقدر ضرر کرده‌اند.

• آزمایش فنی (با رویکرد امنیتی) تجهیزات پیش از استقرار

مهندسان امنیت شبکه باید بدانند چگونه قبل از عملیاتی کردن تجهیزاتی همچون سرورها، نرم‌افزارها، سوئیچ‌ها، روترها و سایر تجهیزات به لحاظ امنیتی هر یک از این ابزارها را آزمایش کنند. به‌طور مثال، ممکن است سازمان سوییچ‌ها یا روترهایی خریداری کند که 3 سال قبل از خرید تولید شده‌اند و آسیب‌پذیری‌هایی در آن‌ها شناسایی شده و وصله‌هایی برای آن‌ها ارائه شده است. این وظیفه مهندس امنیت شبکه است که این مسئله را بررسی کرده و با استفاده از راهکارها و ابزارهایی که در اختیار دارد این مشکلات را شناسایی کند. آزمون‌های فوق باعث می‌شوند شبکه‌ای پایدار در اختیار سازمان و کارمندان قرار گیرد.

• بررسی گزارش‌های تولید شده توسط سامانه‌های امنیتی

مهندس امنیت شبکه باید روزانه گزارش‌های امنیتی تولید شده توسط دیوارهای آتش، سامانه‌های تشخیص و پیشگیری از نفوذ را بررسی کند و هرگونه مورد مشکوکی همچون الگوهای دسترسی نامتعارف به حساب‌های کاربری و سامانه‌ها یا هرگونه ناهنجاری در شبکه را به عنوان یک خطر جدی در نظر بگیرند. برخی از کارشناسان امنیتی پیشنهاد می‌کنند این فرآیند بازرسی هفته‌ای یکبار انجام شود، اما شرکت‌هایی همچون سیسکو بر این باور هستند که سازمان‌ها بر مبنای اطلاعات حساسی که دارند باید این فرآیند را روزانه انجام دهند.

• رفع مشکلات در محل و خارج از سازمان

مهندسان امنیت شبکه باید بتوانند بی‌نظمی‌های شبکه را هم در محل کار و هم از راه دور بررسی، عیب‌یابی و رفع کنند و در ارائه خدمات نهایی به کاربران نهایی، توسعه‌دهندگان برنامه‌ها و پرسنل عملیاتی تخصص و دانش کافی داشته باشند. در برخی از سازمان‌ها این افراد وظایفی تقریبا مشترک با مهندسان شبکه دارند و باید مشکلات عادی شبکه‌ها را برطرف کرده، مدیریتی بر شبکه‌ها اعمال کرده و مشکلات تجاری کلاینت‌ها را برطرف کنند. در ارتباط با مورد آخر مشکلات کلاینت‌ها عمدتا در عدم دسترسی به حساب کاربری، ناآشنایی با مکانیزم فعال‌سازی احراز هویت دو عاملی و مواردی از این دست خلاصه می‌شود.

بازار کار و وضعیت شغلی یک مهندس امنیت شبکه

مهندسان امنیت شبکه در بیشتر موارد با چالش‌های جدی در مقابله با تهدیدات سایبری روبرو هستند، با این‌حال، بازار کار این شغل خوب است و هیچ نشانه‌ای از افول به چشم نمی‌خورد. وب‌سایت SANS پژوهشی در ارتباط با مشاغل حوزه امنیت انجام داده که نشان می‌دهد از میان 20 شغل پر تقاضا و جذاب حوزه امنیت اطلاعات، مهندس امنیت شبکه شماره 7 را به خود اختصاص داده است. وب‌سایت SANA از اصطلاح شوخ‌طبعانه‌ای برای توصیف شغل مهندس امنیت شبکه استفاده کرده و می‌گوید: «مهندسی امنیت شبکه جایگاهی بین مکان 6 (تحلیل‌گر بدافزار) و مکان 7 (تحلیل‌گر امنیت) دارد و میان دو موقعیت شغلی ساندویچ شده است! در صدر این فهرست، شغل بازرسی جرایم امنیت اطلاعات (ISCI) و کارشناس اسناد و شواهد جنایی قرار دارد. البته نگران نباشید، زیرا هیچ متخصص حوزه امنیت بیکار نمی‌ماند و بازار کار متخصصان امنیت نیز هیچگاه با رکورد روبرو نمی‌شود.» سایت Indeed می‌گوید: «میانگین حقوق مهندس امنیت شبکه 91000 هزار دلار در سال است.» گاتهام گودوانی بنیان‌گذار و مدیر اجرایی شرکت Sunny vale در گفت‌وگویی که با سایت Simply Hired انجام داده به نکته جالبی اشاره کرده و اعلام می‌دارد: «چشم‌انداز مشاغل حوزه امنیت شبکه مثبت است. آمارها نشان می‌دهند هر ساله مشاغل حوزه امنیت رشد چشم‌گیری دارند.» در زمان نگارش این مقاله نزدیک به 16000 فرصت شغلی با کلمه کلیدی امنیت شبکه در سایت SimplyHired.com برچسب‌گذاری شده است. گاتهام گودوانی در بخش دیگری از صحبت‌های اضافه می‌کند: «از سپتامبر 2010 تا به امروز جست‌جوی کلیدواژه امنیت شبکه 52٪ و امنیت اطلاعات 14٪ افزایش رشد داشته‌اند، در حالی که جست‌وجوی کلیدواژه فناوری‌اطلاعات 2٪ کاهش رشد داشته است. این آمارها نشان می‌دهند که تعداد مشاغل امنیتی در حوزه شبکه در مقایسه با سایر حوزه‌های فناوری‌اطلاعات رشد چشم‌گیری داشته‌اند. جالب آن‌که موفقیت شغلی با نوع مهارت‌هایی که مهندسان امنیت شبکه دارند رابطه مستقیم دارد.
متخصصانی که تجربه کافی در زمینه شبکه‌های کامپیوتری و دیوارهای آتش دارند به نسبت متخصصانی که تنها یک آشنایی اولیه با مفاهیم فوق دارند موفق‌تر هستند. آشنایی با عملکردهای رایج شبکه و پروتکل‌های کاربردی همچون HTTP، IPSec، TCP / IP، TLS / SSL، شبکه‌های مبتنی بر ویندوز، FTP و DNS حائز اهمیت است. یک مهندس امنیت شبکه باید بداند که چگونه در زیرساخت‌های ارتباطی یک سازمان شبکه‌های خصوصی مجازی را پیاده‌سازی کند، شناخت دقیقی درباره نحوه استقرار سامانه‌های IDS و IPS داشته باشد و بداند برای کاهش تهدیدات DDoS باید از

چه الگوهایی استفاده کند. مهارت‌های مربوط به مدیریت پروژه، عیب‌یابی و مدیریت سیستم‌عامل لینوکس نیز مهم هستند.»

چگونه به یک مهندس امنیت شبکه حرفه‌ای تبدیل شویم؟

برخی از مدیران منابع انسانی انتظار دارند مهندسان امنیت شبکه در رزومه کاری خود فهرستی بلندبالا از گواهی‌نامه‌ها را درج کرده باشند. جیم مک لئود کارشناس برجسته حوزه امنیت گوید: « گواهینامه‌ها ممکن است در مصاحبه اولیه راهگشا باشند، اما مهارت‌های نرم همچون برقراری ارتباط خوب شانس شما در احراز شغل موردنظر را تثبیت می‌کنند. اولین باری که برای شغل مهندس امنیت شبکه درخواستی را برای سازمانی ارسال کردم، پس از چند روز کارمندان منابع انسانی به من گفتند پاراگرافی که در توصیف خود در لینکدین نوشته بودم، همان چیزی بود که آن‌ها را متقاعد کرد با من تماس بگیرند. گواهینامه‌ها بخشی از روند استخدام هستند و نشان می‌دهند شما دانش لازم برای احراز شغل موردنظر را دارید، اما یک رزومه روان، ساده و روشن نشان می‌دهد که آیا این شخص می‌تواند از پس از انجام شغلی که قرار است به او محول شود برآید یا خیر.» مشکلی که امروزه بیشتر متخصصان دارند، عدم رعایت اصول نگارشی است. در بیشتر موارد رزومه‌ها و مطالبی که تحت عنوان مقاله از افراد منتشر می‌شود، بیش از حد مشکل گرامری دارند. همین مسئله باعث می‌شود کارمندان منابع انسانی با نگاه کردن به رزومه‌ای مملو از غلط‌های نگارشی از تماس با فردی که رزومه را ارسال کرده صرف‌نظر کنند. نکته مهم دیگری که بیشتر افراد نسبت به آن بی تفاوت هستند، دوره‌ای به‌نام کارآموزی است. کارآموزی به افراد کمک می‌کند پیش از ورود به محیط حرفه‌ای نحوه تعامل با افراد را یاد بگیرند، با تکنیک‌های کنترل خشم آشنا می‌شوند و یاد بگیرند چگونه در یک محیط کاری رفتار حرفه‌ای داشته باشند.

مک لئود می‌گوید: «پیشنهاد می‌کنم قبل از آن‌که به شکل مستقیم به سراغ شغل کارشناس امنیت شبکه بروید، ابتدا در شرکتی که حیطه کاری آن پیرامون شبکه است کار کنید. این‌کار به شما کمک می‌کند تجربه فنی در ارتباط با شبکه‌ها به دست آورید، اطلاعات مفیدی در ارتباط با آی‌پی و سرآیندهای پروتکل TCP به‌دست آورید، با عملکرد پروتکل‌های مختلف آشنا شده و آن‌ها را تجزیه و تحلیل کنید و نحوه کار با دیوارهای آتش نرم‌افزاری و سخت‌افزاری را یاد بگیرید.

رزومه‌ای که چنین تجربیاتی در آن درج شده باشد به سازمان‌ها نشان می‌دهد که پیش‌زمینه امنیتی لازم برای احراز شغل موردنظر را دارید. به‌طور مثال، ممکن است سازمانی اعلام کند که مسئولیت پیاده‌سازی شبکه خصوصی مجازی، پیاده‌سازی سامانه ضد اسپم و آدرس‌های اینترنتی بر عهده شما است. در هر سه مورد اگر دانش کافی در ارتباط با شبکه‌های کامپیوتری نداشته باشید کار چندان خاصی نمی‌توانید انجام دهید. متاسفانه اگر بدون پیش‌زمینه کافی اقدام به نصب چنین سامانه‌هایی کنید یک شکاف امنیتی در زیرساخت‌های یک سازمان به وجود می‌آورید و در زمان بروز یک حمله سایبری اولین فردی خواهید بود که بازخواست می‌شود. در بیشتر موارد کارمندان یک سازمان به درستی نمی‌دانند عملکرد تجهیزات چگونه است و این شما هستید که باید درباره آسیب‌پذیری‌ها و رخنه‌های احتمالی آموزش‌های لازم را به افراد بدهید.»

منبع:

resources.infosecinstitute

تاریخ انتشار:
16 فروردین 1399

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16751/%DA%86%DA%AF%D9%88%D9%86%D9%87-%DB%8C%DA%A9-%D9%85%D9%87%D9%86%D8%AF%D8%B3-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87-%D8%B4%D9%88%DB%8C%D9%85%D8%9F