به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

مراکز عملیات امنیت؛ چرایی و چگونگی راه اندازی

Security Operations Centers (SOC); Why and How to Setup

محمد نادری

زمان: شنبه ۱۹ بهمن ماه ۱۳۹۲ ساعت ۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

واکنش در برابر حوادث امنیتی، مولفه‌ای اساسی در برنامه‌ریزی‌های مدیران فناوری اطلاعات است. تهدیدها در حوزه امنیت، نه تنها زیاد و متنوع شده‌اند بلکه اثرات مخرب و زیان باری نیز دارند. فعالیت‌های پیشگیرانه، مبتنی بر نتایج حاصل از تشخیص به موقع، تجمیع و ارزیابی موثر تهدیدات، می‌تواند سبب کاهش تعداد حوادث شود، اما آنچه مسلم است این است که راهی برای جلوگیری از وقوع همه حوادث وجود ندارد. بنابراین قابلیت واکنش در برابر حوادث، از طریق افزایش سرعت در تشخیص آن‌ها، کاهش نقاط آسیب پذیر و بازیابی سریع سرویس‌هایی که دچار حمله می‌گردند، بسیار مهم است.

از این رو ایجاد ساختاری که بتواند به سازمان‌ها در مدیریت سریع، کارا و هوشمندانه تهدیدات و رخدادهای امنیتی یاری رساند از مهمترین رسالت مراکز عملیات امنیت می‌باشد. اما ایجاد مراکز عملیات امنیت، به پیش‌نیازها، الزامات و راهکارهایی نیاز دارد که هدف در این سخنرانی پرداختن علمی به این مسائل است.

شرکت در این جلسه برای تمامی دانشجویان علاقه مند آزاد است.