معرفی دوره آموزشی

عنوان دوره:

فارسی: **امنیت اطلاعات**

انگلیسی: **Information Security**

درباره دوره:

امروزه با گسترش روز افزون فناوری اطلاعات در سازمان‌ها و بهره‌گیری از ابعاد گسترده آن در امر خدمات رسانی و حتی تولید محصولات، عنصر ارزشمندی به نام اطلاعات در پیکره سازمان‌ها پدید آمده که مهمترین دارایی آن سازمان نیز به شمار می‌رود. استفاده از فناوری اطلاعات و بهره‌مندی از سیستم‌های ذخیره و پردازش اطلاعات، به عنوان ابزاری قدرتمند باعث متمایز شدن سازمان‌ها از یکدیگر شده و آنهایی که از این فرصت‌های بی‌بدیل فناورانه توانسته‌اند در زمان مناسب خویش، به بهترین نحو ممکن بهره‌برداری کنند گوی سبقت را از سایر رقبا ربوده و موجب سودآوری کسب و کار خود شده‌اند. بنابراین در دنیای رقابتی امروز، اطلاعات به عنوان عنصری حیاتی که بقای سازمان‌ها به شدت به آن وابسته است نیازمند راهکارهای حفاظتی مناسب جهت جلوگیری از تخریب، دستکاری، حذف یا ایجاد وقفه در خدمات است.

در دوره آموزشی امنیت اطلاعات، با نگاهی ویژه به امنیت اطلاعات و تمرکز بر حفظ و نگهداشت اطلاعات، مخاطبان آموزش‌های لازم را در این خصوص فرا می‌گیرند.

اهداف دوره:

۱. آشنایی با اصول و مفاهیم امنیت اطلاعات
۲. آشنایی با راهبردهای جامع امنیتی
۳. آشنایی با تهدیدها و حملات امنیتی
۴. آشنایی با راهکارهای امن‌سازی سیستم عامل و سرویس‌های سازمانی
۵. آشنایی با اصول تدوین خط‌مشی‌ها، دستورالعمل‌ها و روش‌های اجرایی امنیت اطلاعات

مخاطبان دوره:

- ✓ مدیران، راهبران و کارشناسان فناوری اطلاعات
- ✓ کارمندان سازمان‌ها و شرکت‌های خصوصی و دولتی
- ✓ سایر علاقمندان به مباحث امنیت اطلاعات

مدت زمان دوره:

۱۶ ساعت (۲ روز)

محتویات دوره:

- تعاریف و اصطلاح‌های امنیت اطلاعات
- آشنایی با تروجان‌ها، درهای پشتی، روت‌کیت‌ها، ویروس‌ها و کرم‌ها و همچنین نحوه پاکسازی و مقابله با آنها
- بررسی تکنیک‌های شکستن پسوردها و روش‌های جلوگیری از آنها
- معرفی ابزارهای آزمون نفوذپذیری و ارزیابی آسیب پذیری نرم افزارها و برنامه‌های مبتنی بر وب سازمان
- بررسی حملات مهندسی اجتماعی و روش‌های نوین تخلیه اطلاعاتی
- امنیت در حملات تزریق کد و چگونگی مقابله با آنها (SQL Injection & XSS)
- آشنایی با حملات سازمانی و روش‌های مقابله با آنها
- امنیت شبکه‌های بی‌سیم
- ایمن‌سازی سیستم عامل‌های ویندوز و لینوکس
- آشنایی با تنظیمات امنیتی اکتیو دایرکتوری و کارگزار کنترل کننده دامنه
- تحلیل حملات انکار سرویس و نحوه مقابله با آنها
- امنیت فیزیکی و محیط پیرامونی

- نحوه تنظیم خط‌مشی‌ها، روش‌های اجرایی و کنترل‌های امنیتی مناسب، مطابق با الزامات خاص کسب و کار
- معرفی هانی‌پات‌ها، بررسی نحوه عملکرد آنها و چگونگی پیکربندی آنها در معماری شبکه سازمان
- امنیت فیزیکی و منطقی مرکز داده سازمان
- آشنایی با دیواره‌های آتش و پیکربندی امنیتی آنها
- آشنایی با نحوه تنظیم گزارش‌های وقایع، خطاها و مستندات امنیتی در سازمان
- امنیت شبکه و پایش امنیتی آن
- آشنایی با سیستم مدیریت امنیت اطلاعات و الزامات امنیتی آن
- مدیریت کلمه عبور حساب‌های کاربری و الزام‌های کنترل دسترسی
- مدیریت آسیب پذیری‌ها و مخاطرات امنیتی در سازمان
- مدیریت امنیت اطلاعات کارکنان
- آشنایی با نحوه کرک کردن پسورد انواع سیستم عامل‌های ویندوز و بررسی روش‌های جلوگیری از آنها
- آشنایی با نحوه کرک کردن رمز عبور بایوس سیستم و چگونگی جلوگیری از آن
- امنیت مبتنی بر مرورگر و وبگردی امن
- امنیت تجهیزات داخلی و بیرونی سازمان و نگهداری ایمن تجهیزات
- امنیت کابل‌کشی و خطوط ارتباطی شبکه سازمان
- آشنایی با روش‌های امن امحای اطلاعات
- آشنایی با نحوه جلوگیری از نشت اطلاعات سازمانی

ویژگی‌های دوره:

- ✓ امکان صدور گواهینامه معتبر حضور در دوره آموزشی
- ✓ برخورداری از ۱۰٪ تخفیف در صورت ثبت نام گروهی