محمد مهدی واعظی نژاد

بهار ۹۶

معرفی دوره‌های آموزشی

امنیت سایبری

به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید؛ از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.

تلفن تماس: ۰۹۳۶۰۸۹۵۸۴۸

فهرست مطالب

۱- مقدمه ۴

۲- دوره‌های آموزشی امنیت اطلاعات ۵

۲-۱- امنیت اطلاعات ۵

۲-۲- امنیت سایبری سیستم‌های کنترل صنعتی ۷

۲-۳- ممیز امنیت سایبری ۱۰

۲-۴- ارزیابی و مدیریت مخاطرات سایبری ۱۱

۲-۵- مدیریت حوادث سایبری ۱۳

۲-۶- طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) ۱۷

۲-۷- سرممیزی سیستم مدیریت امنیت اطلاعات (ISMS) ۱۹

۲-۸- مدیریت راهبردی امنیت اطلاعات ۲۰

۲-۹- دفاع فعال سایبری ۲۴

۲-۱۰- راهبردهای امن‌سازی زیرساخت‌های حیاتی ۲۷

۲-۱۱- مدل بلوغ امنیت اطلاعات ۳۴

۲-۱۲- امنیت کاربر رایانه (CSCU) ۳۵

۲-۱۳- تهدیدها و آسیب‌های فضای مجازی ۳۶

۲-۱۴- مدیریت امنیت اطلاعات در گزینش و استخدام کارکنان ۳۷

۳- اطلاعات تماس ۳۹

۱- مقدمه

امروزه امنیت اطلاعات یکی از چالش‌های اصلی در عصر فناوری اطلاعات محسوب می‌شود و حفاظت از اطلاعات در مقابل دسترسی غیرمجاز، تغییرات، خرابکاری و افشا امری ضروری و اجتناب ناپذیر به شمار می‌آید. فراهم‌آوری صحت و تمامیت اطلاعات به گونه‌ای که در زمان مناسب، اطلاعات در دسترس افراد مجازی قرار گیرد که نیازمند آن هستند، عاملی است که منجر به اثربخشی کسب و کارها می‌شود.

در سال‌های اخیر، با افزایش تهدیدات و حملات سایبری به سازمان‌ها و روند رو به گسترش آن، امنیت دارایی‌های اطلاعاتی برای تمام سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش برای آموزش همه کارکنان جهت حفاظت از اطلاعات سازمانی می‌باشد. از اینرو، برگزاری دوره‌های آموزشی امنیت اطلاعات در دو سطح مدیریت و کارکنان، در سازمان‌ها یک ضرورت به شمار می‌رود.

در این سند، به معرفی خدمات آموزشی اینجانب در حوزه امنیت اطلاعات پرداخته می‌شود. لازم به ذکر است دو دوره «مدیریت امنیت اطلاعات» و «شبکه و امنیت اطلاعات در سازمان‌ها»، از مجموعه دوره‌های آموزشی کارکنان دولت که توسط سازمان مدیریت و برنامه ریزی کشور مصوب شده است نیز توسط اینجانب تدریس می‌شود.

خدایا چنان کن سرانجام کار، تو خشنود باشی و ما رستگار

محمد مهدی واعظی نژاد

بهار ۱۳۹۶

۲- دوره‌های آموزشی امنیت اطلاعات

۲-۱- امنیت اطلاعات

امروزه با گسترش روز افزون فناوری اطلاعات در سازمان‌ها و بهره‌گیری از ابعاد گسترده آن در امر خدمات‌رسانی 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 و یا ایجاد وقفه در خدمات می‌باشد.

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 گرفته و می‌توانند از دارایی‌های سازمانی به نحو شایسته‌ای حفاظت کنند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. تعاریف و اصطلاح‌های امنیت اطلاعات
۲. آشنایی با تروجان‌ها، درهای پشتی، روت‌کیت‌ها، ویروس‌ها و کرم‌ها و همچنین نحوه پاکسازی و مقابله با آنها
۳. بررسی تکنیک‌های شکستن پسوردها و روش‌های جلوگیری از آنها
۴. معرفی ابزارهای آزمون نفوذپذیری و ارزیابی آسیب پذیری نرم افزارها و برنامه‌های مبتنی بر وب سازمان
۵. بررسی حملات مهندسی اجتماعی و روش‌های نوین تخلیه اطلاعاتی
۶. امنیت در حملات تزریق کد و چگونگی مقابله با آنها (SQL Injection & XSS)
۷. آشنایی با حملات سازمانی و روش‌های مقابله با آنها
۸. امنیت شبکه‌های بی‌سیم

۹. ایمن‌سازی سیستم عامل‌های ویندوز و لینوکس

۱۰. آشنایی با تنظیمات امنیتی اکتیو دایرکتوری و کارگزار کنترل کننده دامنه (DC)

۱۱. تحلیل حملات انکار سرویس (DoS) و نحوه مقابله با آنها

۱۲. امنیت فیزیکی و محیط پیرامونی

۱۳. نحوه تنظیم خط‌مشی‌ها، روش‌های اجرایی و کنترل‌های امنیتی مناسب، مطابق با الزامات خاص کسب و کار

۱۴. معرفی هانی‌پات‌ها، بررسی نحوه عملکرد آنها و چگونگی پیکربندی آنها در معماری شبکه سازمان

۱۵. امنیت فیزیکی و منطقی مرکز داده سازمان

۱۶. آشنایی با دیواره‌های آتش و پیکربندی امنیتی آنها

۱۷. آشنایی با نحوه تنظیم گزارش‌های وقایع، خطاها و مستندات امنیتی در سازمان

۱۸. امنیت شبکه و پایش امنیتی آن

۱۹. آشنایی با سیستم مدیریت امنیت اطلاعات (ISMS) و الزامات امنیتی آن

۲۰. مدیریت کلمه عبور حساب‌های کاربری و الزام‌های کنترل دسترسی

۲۱. مدیریت آسیب پذیری‌ها و مخاطرات امنیتی در سازمان

۲۲. مدیریت امنیت اطلاعات کارکنان

۲۳. آشنایی با نحوه کرک کردن پسورد انواع سیستم عامل‌های ویندوز و بررسی روش‌های جلوگیری از آنها

۲۴. آشنایی با نحوه کرک کردن رمز عبور بایوس سیستم و چگونگی جلوگیری از آنها

۲۵. امنیت مبتنی بر مرورگر و وبگردی امن

۲۶. امنیت تجهیزات داخلی و بیرونی سازمان و نگهداری ایمن تجهیزات

۲۷. امنیت کابل‌کشی و خطوط ارتباطی شبکه سازمان

۲۸. آشنایی با روش‌های امن امحای اطلاعات

۲۹. آشنایی با نحوه جلوگیری از نشت اطلاعات سازمانی.

۲-۲- امنیت سایبری سیستم‌های کنترل صنعتی

سیستم‌های کنترل صنعتی، سیستم‌هایی مبتنی بر رایانه هستند که برای کنترل فرایندهای صنعتی و عملکردهای فیزیکی استفاده می‌شوند. استفاده گسترده از این سیستم‌ها در زیرساخت‌ها و سامانه‌های حیاتی کشور، موجب شکل‌گیری نوع جدیدی از حملات سایبری به شبکه‌های بزرگ صنعتی کشورمان شده است که از نمونه‌های مشهور و شناخته شده آن در سال‌های اخیر می‌توان به استاکس‌نت اشاره کرد.

در این دوره آموزشی، ضمن بررسی چالش‌ها و مشکلات امنیتی سیستم‌های کنترل صنعتی، ارایه راهکارهای اجرایی برای کاهش مخاطرات امنیتی این سیستم‌ها، روش‌های امن‌سازی آنها بر اساس استانداردهای بین‌المللی، آشنایی با بهترین تجربه‌های جهانی در حوزه حفاظت از سیستم‌های کنترل صنعتی و همچنین بررسی الزامات ملی ایران در این خصوص، از دیگر موارد مطرح در این دوره است.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. آشنایی با سامانه‌های حیاتی و غیرحیاتی
۲. مشکلات و چالش‌های امنیتی سیستم‌های کنترل صنعتی
   - مفاهیم امنیتی سیستم‌های کنترل صنعتی
   - ضرورت توجه به امنیت سیستم‌های کنترل صنعتی
   - رخدادهای امنیتی سیستم‌های کنترل صنعتی
   - انواع بدافزارهای سیستم‌های کنترل صنعتی
   - آشنایی با آسیب‌پذیری‌های موجود در سیستم‌های کنترل صنعتی
   - آشنایی با آسیب‌پذیری‌های حیاتی در طراحی محصولات سیستم‌های کنترل صنعتی
     - آسیب‌پذیری آئورورا (Aurora)
     - آسیب‌پذیری بوریاس (Boreas)
   - نحوه شناسایی سیستم‌های کنترل صنعتی آسیب‌پذیر از طریق اینترنت
   - آشنایی با انواع تهدیدات و مخاطرات امنیتی در سیستم‌های کنترل صنعتی
   - بررسی انواع حملات سازمانی در شبکه‌های صنعتی

- بررسی مشکلات امنیتی در معماری، سیستم کنترلی، تجهیزات و بستر ارتباطی شبکه‌های صنعتی
- بررسی چالش‌های امنیتی سیستم‌های کنترل صنعتی
- معرفی روش‌های جلوگیری از تهدیدات امنیتی سیستم‌های کنترل صنعتی
- بررسی رویکرد واکنشی به امنیت سایبری در سیستم‌های کنترل صنعتی

۳. تاریخچه حملات سایبری به سیستم‌های کنترل صنعتی

۴. استانداردهای امنیتی سیستم‌های کنترل صنعتی

- ISO
- CPNI
- NIST
- NERC
- DHS
- DOE
- ISA

۵. امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی در سایر کشورها (مطالعه موردی)

۶. بررسی امنیت در سیستم‌های کنترل صنعتی و سامانه‌های فناوری اطلاعات

- بررسی وصله‌های امنیتی در سیستم‌های کنترل صنعتی و سامانه‌های فناوری اطلاعات
- بررسی پیچیدگی‌های سیستم‌های کنترل صنعتی نسبت به سامانه‌های فناوری اطلاعات

۷. امنیت سیستم‌های کنترل صنعتی

- فاکتورهای بروز آسیب‌پذیری در سیستم‌های کنترل صنعتی
- مسایل امنیتی مربوط به ارتباط شبکه‌های کنترل فرایند سیستم‌های صنعتی با شبکه داخلی سازمان
- مسایل امنیتی مربوط به طراحی، استقرار و بهره‌برداری از سیستم‌های کنترل صنعتی
- مسایل امنیتی مربوط به پروتکل‌های اختصاصی سیستم‌های کنترل صنعتی
- مسایل امنیتی مربوط به دسترسی‌های غیرمجاز به نرم افزارهای کنترل کننده سیستم‌های کنترل صنعتی
- مسایل امنیتی مربوط به کارمندان ناراضی داخل سازمان

- مسایل امنیتی مربوط به رسانه‌های ارتباطی سیستم‌های کنترل صنعتی (سیستم تلفن سوئیچ عمومی، ارتباطات بی‌سیم و اینترنت)

۸. الزامات مراکز بالادستی کشور در خصوص امن‌سازی سیستم‌های کنترل صنعتی

۹. بررسی متدولوژی‌های مدیریت مخاطرات سایبری سیستم‌های کنترل صنعتی

۱۰. روش‌های اجرایی فراهم‌آوری امنیت در سیستم‌های کنترل صنعتی

- نحوه تدوین خط‌مشی‌ها، روش‌های اجرایی و دستورالعمل‌های امنیتی
- بررسی نقش مدیریت مخاطره در امن‌سازی سیستم‌های کنترل صنعتی
- چگونگی وضع کنترل‌های امنیتی در سیستم‌های کنترل صنعتی
- چگونگی ایمن‌سازی برنامه‌های سیستم کنترل صنعتی
- چگونگی امن‌سازی تجهیزات ارتباطی سیستم‌های کنترل صنعتی
- چگونگی امن‌سازی محیط‌های ذخیره، پردازش و بازیابی اطلاعات سیستم‌های کنترل صنعتی
- چگونگی طراحی ضمانت‌نامه‌های اجرایی مناسب در سیستم‌های کنترل صنعتی
- چگونگی به کارگیری سیستم‌های اخطاردهی و گزارش نقض‌ها و نقص‌ها در سیستم‌های کنترل صنعتی
- روش‌های احراز هویت در سیستم‌های کنترل صنعتی
- آشنایی با سیستم‌ها و تجهیزات امنیتی سیستم‌های کنترل صنعتی
- چگونگی سنجش اثربخشی کنترل‌های امنیتی سیستم‌های کنترل صنعتی
- آموزش و آگاهی‌رسانی امنیتی در شبکه‌های صنعتی
- نحوه امن‌سازی دسترسی‌های از راه دور به سیستم‌های کنترل صنعتی
- امنیت فیزیکی و محیطی سیستم‌های کنترل صنعتی
- نحوه تشکیل گروه‌های واکنش به رخدادها و حوادث امنیتی در شبکه‌های صنعتی
- چگونگی تدوین طرح‌های تداوم کسب و کار (BCP) و بازیابی از وضعیت خرابی (DRP) در سیستم‌های کنترل صنعتی

- آشنایی با معماری‌های امنیتی مرجع در امن‌سازی سیستم‌های کنترل صنعتی
- نحوه برطرف‌سازی آسیب‌پذیری‌های امنیتی محصولات سیستم‌های کنترل صنعتی
- آشنایی با نحوه تهیه و تدوین چک‌لیست‌های امنیتی سیستم‌های کنترل صنعتی
- بررسی استراتژی‌های دفاع در عمق در امن‌سازی سیستم‌های کنترل صنعتی

۱۱. انجمن‌ها و مؤسسات پژوهشی در حوزه امن‌سازی سیستم‌های کنترل صنعتی.

۲-۳- ممیز امنیت سایبری

امروزه امنیت اطلاعات، یکی از چالش‌های اصلی در عصر فناوری اطلاعات محسوب می‌شود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تخریب، تغییر، تحریف، انکار و افشا یک ضرورت انکارناپذیر برای تمامی سازمان‌ها به شمار می‌رود. شدت این حملات گاهی به حدی است که حتی سازمان‌هایی با بهترین زیرساخت‌های امنیتی هم نمی‌توانند تضمین کنند که هیچ گاه اقدامات بدخواهانه بر روی شبکه آنها اتفاق نخواهد افتاد. از سوی دیگر، با رشد تصاعدی جرایم سایبری و افزایش حملات درون سازمانی در ماه‌های اخیر، امنیت اطلاعات به عنوان عنصری حیاتی در بقای کسب و کار سازمان‌ها تبدیل شده است. از اینرو، اتخاذ راهبردهایی به منظور حسابرسی و ممیزی امنیتی تمام سطوح سازمانی جهت شناسایی نقاط آسیب پذیر و برطرف‌سازی آنها قبل از وقوع هر تهدیدی، از اهمیت بسیار ویژه‌ای برخوردار است. بنابراین لازم است در مراحل مختلف، ممیزی‌های دوره‌ای و موردی از وضعیت امنیت سایبری سازمان به عمل آید.

در این دوره آموزشی، مخاطبان آموزش‌های لازم را در خصوص ممیزی امنیت سایبری سازمان‌ها و شرکت‌های مطبوع خویش یا سایر سازمان‌ها، منطبق با رویه‌ها و استانداردهای مربوطه و همچنین قوانین بالادستی کشورمان فرا می‌گیرند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. معرفی کلی فرایند ممیزی امنیت سایبری
۲. بررسی استانداردها و بهروش‌های ممیزی امنیت سایبری
۳. آشنایی با مراحل اجرایی ممیزی امنیت سایبری
۴. اصول مهم در تشکیل تیم‌های ممیزی و وظایف هر یک از اعضای آن
۵. نحوه تهیه چک‌لیست‌های ممیزی امنیت سایبری (در حوزه‌های مختلف مورد بررسی، شامل شبکه محلی و گسترده (LAN & WAN)، ارتباطات، عملیات، فیزیکی، افراد و مرکز داده)

۶. چگونگی تهیه برنامه ممیزی امنیت سایبری (Cyber Security Audit Plan)

۷. اصول و تکنیک‌های مصاحبه، مشاهده و بررسی شواهد و مستندات در ممیزی امنیت سایبری

۸. نحوه بررسی مستندات و اسناد در ممیزی‌های امنیتی

۹. آشنایی با نکات کلیدی در اثربخشی فرایند ممیزی

۱۰. معرفی روش‌های بهره‌گیری از رویکردهای روانشناختی در ممیزی‌های امنیت سایبری

۱۱. آشنایی با تکنیک گزارش‌نویسی فرایند ممیزی امنیت سایبری

۱۲. آشنایی با فرایند گزارش‌دهی عدم انطباق‌ها

۱۳. نمونه فرم‌ها و چک‌لیست‌های ممیزی امنیت سایبری.

۲-۴- ارزیابی و مدیریت مخاطرات سایبری

امروزه با گسترش شدید و قریب الوقوع تهدیدات پیشرفته امنیتی بر ضد سازمان‌ها، ارزیابی و مدیریت مخاطرات امنیت اطلاعات یکی از دغدغه‌های اصلی در عصر فناوری اطلاعات محسوب می‌شود. با رشد یکباره این تهدیدات، امروز بیش از هر زمان دیگری، بقا و دوام سازمان‌ها به حفاظت مناسب از دارایی‌ها و برطرف‌سازی آسیب‌پذیری‌ها بستگی دارد. از اینرو، امنیت دارایی‌های اطلاعاتی و حفظ سرمایه‌های سازمانی، برای تمام سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است.

در این دوره آموزشی، با نگاهی متفاوت به ارزیابی و مدیریت مخاطرات امنیت اطلاعات و با تمرکز اصلی بر فعالیت‌های عملی، فراگیران در یک تجربه مشترک که آمیخته با فعالیت‌های گروهی است ضمن بررسی سناریوهای مختلف و پیچیده مربوط به مخاطرات، با روش‌های شناسایی، طبقه‌بندی و ارزش‌گذاری دارایی‌ها آشنا شده و اصول ارزیابی و مدیریت مخاطرات سایبری را بر اساس استانداردها و بهترین تجربه‌های جهانی فرا می‌گیرند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. آشنایی با مفاهیم اصلی امنیت اطلاعات

۲. بررسی متدولوژی مدیریت دارایی‌ها

- نحوه شناسایی دارایی‌ها
- چگونگی شناسایی وضعیت دارایی‌های اطلاعاتی

- نحوه شناسایی فرایندها و حوزه‌های کسب و کار
- نحوه شناسایی سرویس‌های ارایه شده در هر یک از حوزه‌های کسب و کار
- نحوه طبقه‌بندی دارایی‌های شناسایی شده
- چگونگی تعیین مسئول (مالک) برای هر دارایی
- سازوکارهای تعیین سطح دسترسی افراد به دارایی‌ها بر اساس ماتریس‌های کنترل دسترسی

۳. بررسی متدلوژی ارزیابی مخاطرات امنیتی

- معرفی استانداردهای مطرح در حوزه ارزیابی مخاطرات امنیت اطلاعات
- نحوه انتخاب و تعیین متدلوژی مناسب ارزیابی مخاطرات امنیت اطلاعات
- تبیین شیوه ارزش‌دهی به دارایی‌ها
- تبیین شیوه ارزش‌گذاری دارایی‌های با روابط متقابل
- توصیف ارزش‌دهی به هر یک از دارایی‌ها بر مبنای پارامترهای محرمانگی، صحت و دسترس پذیری
- معرفی آسیب‌پذیری‌ها و نحوه بررسی و اولویت‌بندی آنها
- تبیین شیوه آنالیز ضربه (Impact Analysis) و پیامدهای تهدیدات
- تبیین شیوه دستیابی به احتمال وقوع تهدیدات
- تبیین شیوه ارزیابی و تعیین مخاطره
- تبیین اولویت‌بندی مخاطره و استراتژی‌های مدیریت مخاطرات
- بررسی عوامل مهم در ارزش‌گذاری دارایی‌ها
- نحوه محاسبه ارزش کل دارایی‌ها

۴. شناسایی و بررسی آسیب‌پذیری‌های دارایی‌ها

۵. شناسایی و بررسی تهدیدات دارایی‌ها

- بررسی انواع تهدیدهای متعارف (مصادیق محیطی و انسانی)
- نحوه تعیین لیست تهدیدات ذاتی

- نحوه تعیین لیست تهدیدات واقعی
- نحوه تهیه جدول تهدیدات به تفکیک دارایی‌ها
- نحوه تهیه جدول تهدیدات به تفکیک رخدادها
- تعیین احتمال وقوع تهدیدها بر اساس متدولوژی ارزیابی مخاطره
- بررسی عوامل مورد توجه در تعیین احتمال وقوع تهدیدات

۶. شناسایی و تحلیل پیامد وقوع تهدیدها

۷. محاسبه و تعیین میزان مخاطره هر تهدید، برای هر یک از دارایی‌ها

۸. راهبردهای مدیریت مخاطرات

- آشنایی با گزینه‌های مناسب جهت برخورد با مخاطرات شناسایی شده
- چگونگی تعیین استراتژی مناسب جهت مدیریت مخاطرات
- بررسی انواع گزینه‌های برخورد با مخاطرات
- عوامل مؤثر در انتخاب گزینه‌های برخورد با مخاطرات
- نقش هزینه‌های پیشگیری از مخاطره، در تعیین استراتژی مناسب

۹. تعیین معیار و سطح قابل قبول مخاطرات

۱۰. تعیین شیوه مناسب برخورد با مخاطرات باقی مانده

۱۱. معرفی بهترین تجربه‌های جهانی در حوزه مدیریت مخاطرات سایبری

۱۲. اتخاذ کنترل‌های امنیتی

۱۳. معرفی نرم افزارها و ابزارهای مدیریت مخاطرات.

۲-۵- مدیریت حوادث سایبری

با پیشرفت و گسترش روز افزون فناوری اطلاعات و ارتباطات در دنیای امروز، بحث حفاظت از داده‌ها اهمیت ویژه‌ای یافته است. هر چه راه‌های دسترسی و روش‌های ارتباطی افزایش می‌یابد مسأله حفاظت از امنیت اطلاعات نیز مهم‌تر و پیچیده‌تر می‌شود. وجود حفره‌ها و نقص‌های امنیتی در سیستم‌های فناوری اطلاعات، همواره مورد توجه افراد سودجو بوده است به طوری

که در مقاطعی از زمان، سرعت افزایش تعداد حملات صورت گرفته، از سرعت پیشرفت و گسترش سیستم‌ها بسیار بیشتر است. بنابراین با نگاهی به آمار منتشر شده و وضعیت فعلی پیشرفت فناوری اطلاعات، وجود مراکزی مستقل برای تأمین امنیت فضای تبادل اطلاعات در سازمان‌ها امری حیاتی و ضروری به نظر می‌رسد.

امروزه بیشتر سازمان‌ها دریافته‌اند که یک راهکار امنیتی واحد برای تأمین امنیت سیستم‌ها وجود ندارد بلکه باید از استراتژی امنیتی چند لایه بهره گرفت. یکی از لایه‌هایی که بیشتر سازمان‌ها در استراتژی امنیتی خود در نظر می‌گیرند ایجاد یک مرکز مدیریت رخدادهای امنیتی و تشکیل تیم پاسخگویی به رخدادهای امنیتی رایانه است که در سازمان‌های ایرانی با نام «گوهر» شناخته می‌شود. هدف از ایجاد مرکز مدیریت رخدادهای امنیتی و تشکیل این تیم، فراهم‌آوری قابلیت ارزیابی، پاسخگویی و آموختن از رخدادهای امنیت اطلاعات است. این مرکز با مدیریت صحیح رخدادهای امنیتی در سازمان می‌تواند کمک شایانی را به سازمان‌ها در کاهش صدمات مالی و مهمتر از همه، وجهه و شهرت آن سازمان کند.

در این دوره آموزشی، مخاطبان ضمن آشنایی با چارچوب‌ها و اصول ایجاد تیم‌های امداد رایانه‌ای در سازمان‌های ایرانی، با روش‌های اجرایی طراحی، تشکیل و راه‌اندازی این تیم‌ها به صورت کامل آشنا شده و می‌توانند تیم‌های امداد رایانه‌ای را در سازمان‌های خویش پیاده‌سازی کنند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. تشکیل و راه‌اندازی مرکز گوهر

- معرفی مرکز گروه واکنش هماهنگ رخداد (گوهر)
- اسناد بالادستی الزام‌آور کشور در خصوص تشکیل مرکز گوهر در سازمان‌ها
- اهداف راه‌اندازی مرکز گوهر
- مزایای راه‌اندازی مرکز گوهر
- مأموریت‌ها و وظایف مرکز گوهر
- سطوح پیاده‌سازی مرکز گوهر
- مراحل تکامل مراکز گوهر

۲. گام‌های راه‌اندازی و تشکیل مرکز گوهر در سازمان

- جایگاه مرکز گوهر در چارت سازمان و ارتباط آن با سایر واحدها

- ساختار مرکز گوهر و تیم‌های آن
- نقش‌ها و مسئولیت‌های افراد
- تعیین مکان فیزیکی مرکز گوهر

۳. تعاملات مرکز گوهر

- نحوه تعامل مرکز گوهر با مرکز عملیات امنیت (SoC)
- نحوه تعامل مرکز گوهر با سایر گوهرها
- نحوه تعامل مرکز گوهر با مراکز ماهر و آپا
- نحوه تعامل مرکز گوهر با ذی‌نفعان سازمان (همکاران، مشتریان، بیمه‌گذاران، اشخاص سوم و غیره)
- نحوه تعامل مرکز گوهر با سازمان‌های بالادستی، نهادهای امنیتی و قانون‌گذار

۴. سرویس‌های امنیتی مرکز گوهر

- خدمات پیشگیرانه
- خدمات واکنشی
- خدمات مدیریت کیفی امنیت

۵. فراهم‌آوری امنیت مرکز گوهر

- امنیت شبکه
- امنیت فیزیکی
- امنیت منابع انسانی

۶. ابزارها و نرم افزارهای مورد استفاده در مرکز گوهر

۷. مدیریت رویدادها و حوادث امنیتی در گوهر

- چرخه مدیریت رخدادها و حوادث امنیتی در گوهر
- چگونگی گردش کار بین تیم‌های گوهر
- نحوه رصد و تشخیص نفوذ به سازمان

- نحوه شناسایی رخدادهای امنیتی در سازمان
- نحوه شناسایی آسیب پذیری‌ها
- نحوه جمع‌آوری گزارشات و هشدارها از تجهیزات شبکه و سامانه‌های امنیتی

۸. ارزیابی و تصمیم‌گیری درباره رویدادها و حوادث امنیتی در گوهر

- نحوه تعیین متدولوژی رسیدگی به حوادث امنیتی
- نحوه تدوین طرح ارزیابی و تصمیم اولیه
- نحوه تدوین طرح ارزیابی و تأیید رویدادهای امنیتی
- نحوه تدوین طرح رده‌بندی رویدادهای امنیتی

۹. پاسخگویی به رویدادها و حوادث امنیتی در گوهر

- نحوه تدوین طرح پاسخگویی به حوادث امنیتی
- نحوه تعیین اقدامات لازم در خصوص پاسخگویی فوری به حوادث امنیتی
- نحوه تعیین اقدامات لازم در خصوص پاسخگویی ثانویه به حوادث امنیتی
- نحوه تعیین اقدامات لازم در خصوص پاسخگویی‌ها با موقعیت‌های ویژه
- نحوه تعیین طرح محدودسازی اثرات نامطلوب حوادث امنیتی
- چگونگی طراحی زیرساخت‌های سازمانی مطلوب و مورد نیاز برای پاسخگویی به رویدادهای امنیتی
- نحوه تدوین طرح استمرار کسب و کار
- نحوه تعیین متدولوژی مناسب جهت روز آمد کردن اطلاعات رویدادهای امنیتی
- نحوه تعیین کنترل‌های امنیتی در رابطه با رویدادهای امنیتی
- نحوه تعیین متدولوژی ارزیابی کنترل‌های امنیتی به کار گرفته شده
- نحوه تعیین روش تحلیل امور قانونی امنیت اطلاعات

۱۰. نحوه اعلام هشدار در مورد رخدادهای امنیتی

۱۱. نحوه تهیه فرم‌های مورد نیاز مرکز گوهر

۱۲. فرایندهای ترمیم و بازیابی از حوادث در گوهر

۱۳. چگونگی اشتراک‌گذاری اطلاعات و پایگاه دانش حوادث

۱۴. گزارش‌دهی رویدادها و حوادث امنیتی در گوهر

- نحوه گزارش‌دهی رخدادهای امنیتی به گوهر
- نحوه گزارش‌دهی رخدادهای امنیتی از گوهر به سایر نهادها

۱۵. یادگیری از رویدادها و حوادث امنیتی در گوهر

- نحوه تدوین برنامه‌های آموزشی و آگاهی‌رسانی
- نحوه تدوین متدولوژی مستندسازی رویدادهای امنیتی
- نحوه تدوین روش بازنگری‌های مدیریتی امنیت اطلاعات
- نحوه تدوین طرح‌واره بهبود در کاربرد نظارت امنیت اطلاعات

۱۶. ویژگی‌ها و ساختار پرتال سازمانی مرکز گوهر

۱۷. روش‌های ارزیابی و ممیزی عملکرد مرکز گوهر

۱۸. معرفی بهترین الگوها و استانداردهای جهانی در خصوص راه‌اندازی و تشکیل مرکز گوهر.

۲-۶- طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS)

امروزه با گسترش تهدیدها و حوادث امنیتی در سطح سازمان‌ها، امنیت دارایی‌های اطلاعاتی برای تمام سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است. استاندارد ISO/IEC 27001:2013 زمینه مناسبی را برای طراحی و استقرار سیستم مدیریت امنیت اطلاعات و ارزیابی آن در سازمان‌ها و بهره‌گیری از منافع این رویکرد، فراهم کرده است.

در این دوره آموزشی، مخاطبان آموزش‌های لازم را در خصوص ایجاد، پیاده‌سازی، استقرار و ممیزی داخلی سیستم مدیریت امنیت اطلاعات (ISMS)، مبتنی بر نیازها و الزامات مختص کسب و کار خود و منطبق با رویه‌ها و استانداردهای ISO/IEC 27001:2013 و ISO/IEC 27002:2013 که البته مطابق با الزامات ملی کشورمان، بومی‌سازی شده‌اند فرا می‌گیرند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. تعاریف، اصطلاح‌ها و واژگان امنیت اطلاعات و سیستم مدیریت

۲. آشنایی با سیستم مدیریت امنیت اطلاعات و استانداردهای خانواده ISMS

۳. معرفی اصول، مفاهیم و الزامات سیستم مدیریت امنیت اطلاعات

۴. چرخه بهبود مستمر امنیت اطلاعات

۵. چگونگی تعیین دامنه (Scope) سیستم مدیریت امنیت اطلاعات

۶. چگونگی تعیین نقش‌ها و مسئولیت‌ها

۷. نحوه شناسایی نیازمندهای امنیت اطلاعات

۸. اصول مستندسازی در ISMS و چگونگی تهیه مستندات الزامی

۹. انتخاب و پیاده‌سازی کنترل‌ها و اهداف کنترلی استاندارد ISO/IEC 27001:2013

۱۰. نحوه تدوین و طراحی خط‌مشی‌ها، روش‌های اجرایی و طرح‌های امنیت اطلاعات

۱۱. شناسایی و ارزیابی مخاطرات امنیت اطلاعات

۱۲. چگونگی برنامه‌ریزی، تهیه، اجرا و گزارش‌دهی وقایع امنیت اطلاعات

۱۳. روش‌های مدیریت مخاطرات امنیت اطلاعات

۱۴. مدیریت حوادث امنیتی در طرح تداوم کسب و کار

۱۵. تهیه برنامه‌های آموزشی و آگاهی‌رسانی امنیتی

۱۶. فرایند ممیزی داخلی و اصول انتخاب ممیزان

۱۷. نحوه اجرای طرح ممیزی داخلی امنیت اطلاعات

۱۸. چگونگی تهیه چک‌لیست‌های ممیزی

۱۹. اقدامات اصلاحی و پیشگیرانه و رفع عدم انطباق‌ها

۲۰. نحوه ممیزی شخص سوم و فرایند ثبت و صدور گواهینامه ISO/IEC 27001:2013

۲۱. نمونه پروژه‌ها و فایل‌های مربوط به پیاده‌سازی سیستم مدیریت امنیت اطلاعات.

۲-۷- سرممیزی سیستم مدیریت امنیت اطلاعات (ISMS)

امروزه امنیت اطلاعات، یکی از چالش‌های اصلی در عصر فناوری اطلاعات محسوب می‌شود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تخریب، تغییر، تحریف و انکار، یک ضرورت انکارناپذیر به شمار می‌رود. از اینرو، استاندارد ISO/IEC 27001:2013 زمینه مناسبی را برای بهره‌گیری از این رویکرد در سازمان‌ها فراهم نموده است. پس از پیاده‌سازی و استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در سازمان، لازم است که انطباق آن با کنترل‌ها و الزامات این استاندارد بین‌المللی بررسی شود.

در این دوره آموزشی، مخاطبان آموزش‌های لازم را در خصوص ممیزی شخص سوم سیستم مدیریت امنیت اطلاعات، منطبق با رویه‌ها و استانداردهای مربوطه و همچنین قوانین بالادستی کشورمان فرا می‌گیرند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. معرفی کلی سیستم مدیریت امنیت اطلاعات
۲. سازوکارهای مدیریت مخاطرات امنیتی در سیستم‌های مدیریتی امنیت اطلاعات
۳. معرفی مراحل اجرایی سیستم مدیریت امنیت اطلاعات
۴. بررسی استانداردهای ممیزی سیستم مدیریت امنیت اطلاعات
۵. آشنایی با مراحل اجرایی ممیزی
۶. نحوه تهیه چک‌لیست‌های ممیزی
۷. چگونگی تهیه برنامه ممیزی (Audit Plan)
۸. فرایندهای مربوط به مرور مستندات سیستم مدیریت امنیت اطلاعات و ممیزی مرحله اول
۹. اصول مهم در اثربخشی فرایندی ممیزی
۱۰. اصول تشکیل تیم‌های ممیزی و وظایف هر یک از اعضای آن
۱۱. چگونگی بررسی الزامات استاندارد
۱۲. فرایند گزارش‌دهی عدم انطباق‌ها
۱۳. بهره‌گیری از رویکردهای روانشناختی در ممیزی مرحله دوم
۱۴. اصول و تکنیک‌های مصاحبه، مشاهده و بررسی مستندات سیستم مدیریت امنیت اطلاعات

۱۵. اصول گزارش‌نویسی فرایند ممیزی

۱۶. بررسی الزامات مرکز مدیریت راهبردی افتا در خصوص ممیزی سیستم مدیریت امنیت اطلاعات

۱۷. فرایند صدور گواهینامه سیستم مدیریت امنیت اطلاعات

۱۸. نمونه فرم‌ها و چک‌لیست‌های ممیزی سیستم مدیریت امنیت اطلاعات.

۲-۸- مدیریت راهبردی امنیت اطلاعات

گسترش روز افزون تهدیدات و افزایش حملات سایبری به سازمان‌ها در سال‌های اخیر، بیانگر آن است که شیوه‌های دفاع فعلی در برابر این تهدیدات دیگر جوابگو نیست و سازمان‌ها نیازمند بکارگیری تدابیر اصولی‌تری در این حوزه هستند. امروزه یکی از مهمترین راهکارها در خصوص مدیریت امنیت اطلاعات و پاسخگویی مناسب به تهدیدات سایبری، استفاده از الگوهای راهبردی امنیت اطلاعات است.

در این دوره آموزشی، مخاطبان ضمن آشنایی با الزامات، نیازمندی‌ها، استانداردها و بهروش‌های راهبردی امنیت اطلاعات در سازمان می‌توانند امنیت اطلاعات را در سازمان‌های خویش، مدیریت و راهبری کنند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. آشنایی با اصول و مفاهیم راهبردی امنیت اطلاعات

- اصطلاح‌ها و تعاریف مهم امنیت اطلاعات
- مثلث سه گانه امنیت اطلاعات و نحوه ارتباط اجزای آن با یکدیگر
- مثلث عملکرد، راحتی استفاده و امنیت و اصول رعایت آن در سازمان‌ها
- اصول امنیت اطلاعات
- چرخه تداوم امنیت در سازمان
- مفاهیم امنیت راهبردی و راهبری امنیت
- دارایی و دارایی‌های اطلاعاتی در راهبری امنیت
- روش‌های شناسایی دارایی‌ها
- بهروش‌ها و بهترین درس آموزه‌های امنیت اطلاعات

۲. آشنایی با الزامات و نیازمندی‌های امنیت اطلاعات

- الزامات کلیدی امنیت اطلاعات
- اصول مدیریت امنیت اطلاعات
- نیازمندی‌های امنیت اطلاعات بهینه
- آسیب‌پذیری‌ها و تهدیدات امنیتی
- چالش‌های فراهم‌آوری امنیت اطلاعات در سازمان‌ها

۳. آشنایی با فرایندهای ارزیابی و مدیریت مخاطرات امنیت اطلاعات

- متدولوژی‌های مدیریت دارایی‌ها
- شیوه‌های ارزش‌دهی به دارایی‌ها
- شیوه ارزش‌گذاری دارایی‌های با روابط متقابل
- متدولوژی‌های ارزیابی مخاطرات امنیت اطلاعات
- استانداردهای مطرح در حوزه ارزیابی مخاطرات امنیت اطلاعات
- آسیب‌پذیری‌ها و نحوه بررسی و اولویت‌بندی آنها
- سازوکارهای تبیین آنالیز ضربه (Impact Analysis) و پیامدهای تهدیدات
- شیوه‌های دستیابی به احتمال وقوع تهدیدات
- روش‌های ارزیابی و تعیین مخاطره برای هر دارایی
- روش‌های اولویت‌بندی مخاطرات
- روش‌های شناسایی و بررسی آسیب‌پذیری‌های دارایی‌ها
- روش‌های شناسایی و بررسی تهدیدات دارایی‌ها
- استراتژی‌های مطرح در مدیریت مخاطرات
- روش تعیین معیار و سطح قابل قبول مخاطرات
- روش‌های اتخاذ کنترل‌های امنیتی

- بهترین تجربه‌های جهانی در حوزه مدیریت مخاطرات

۴. بررسی جایگاه افراد، فرایندها و فناوری‌ها در راهبرد امنیت اطلاعات سازمان

۵. چگونگی تعریف نقش‌ها و مسئولیت‌های راهبردی امنیت اطلاعات در سازمان

- نقش‌ها و مسئولیت‌های راهبردی امنیت اطلاعات
- چگونگی تعریف این نقش‌ها و مسئولیت‌ها

۶. اصول راهبری و مدیریت امنیت اطلاعات در سازمان‌های ایرانی

- اصول راهبردی امنیت اطلاعات در حوزه راهبری فناوری اطلاعات و امنیت
- جایگاه مدیریت امنیت راهبردی در سازمان
- نقش امنیت راهبردی در فراهم‌آوری دفاع فعال در سازمان
- حوزه‌های مورد توجه در امنیت راهبردی
- رویکردهای امنیت راهبردی
- مزایای امنیت راهبردی
- مشکلات و چالش‌های امنیت راهبردی

۷. راهکارهای مدیریت راهبردی امنیت اطلاعات در سازمان

- مدیریت عملیات
- مدیریت ظرفیت
- مدیریت تغییرات
- مدیریت ارتباطات
- مدیریت دسترسی
- مدیریت دارایی‌ها
- مدیریت منابع انسانی
- مدیریت امنیت اطلاعات

- مدیریت خدمات شخص سوم

۸. نکات قابل توجه در راهبردهای مدیریتی امنیت فیزیکی و محیطی سیستم‌های اطلاعاتی

۹. معرفی استانداردها و بهروش‌های موجود در حوزه مدیریت راهبردی امنیت اطلاعات

۱۰. راهبردهای طراحی و پیاده‌سازی کنترل‌های امنیتی در سازمان

- راهبردهای کنشی امنیت اطلاعات
- راهبردهای واکنشی امنیت اطلاعات
- راهبردهای مبتنی بر بلوغ امنیت اطلاعات سازمانی
- راهبردهای مبتنی بر استانداردهای امنیتی
- راهبردهای معرفی شده در چارچوب‌های امنیتی
- راهبردهای مبتنی بر بهترین شیوه‌های اجرایی

۱۱. چگونگی تطبیق و بررسی انطباق کنترل‌های امنیتی پیاده‌سازی شده در سازمان با استانداردهای امنیت اطلاعات

۱۲. اصول مستندسازی در امنیت اطلاعات راهبردی

- مستندات الزامی امنیت اطلاعات
- استانداردهای مستندسازی امنیت اطلاعات
- نکات قابل توجه در مستندسازی امنیتی
- روش‌های نسخه‌گذاری مستندات امنیتی
- اصول به روز رسانی مستندات امنیتی

۱۳. اصول تدوین برنامه پاسخ‌دهی به حوادث امنیت اطلاعات

- انواع روش‌های پاسخ‌دهی به حوادث امنیتی
- نحوه تدوین طرح پاسخ‌دهی به حوادث امنیتی
- نحوه تعیین اقدامات لازم در خصوص پاسخگویی فوری به حوادث امنیتی
- نحوه تعیین اقدامات لازم در خصوص پاسخگویی ثانویه به حوادث امنیتی

- نحوه تعیین اقدامات لازم در خصوص پاسخگویی‌ها با موقعیت‌های ویژه
- نحوه تعیین طرح محدودسازی اثرات نامطلوب حوادث امنیتی
- چگونگی طراحی زیرساخت‌های سازمانی مطلوب و مورد نیاز برای پاسخگویی به رویدادهای امنیتی
- نحوه تعیین متدولوژی مناسب جهت روز آمد کردن اطلاعات رویدادهای امنیتی
- نحوه تعیین روش تحلیل امور قانونی امنیت اطلاعات

۱۴. اصول تدوین برنامه‌های تداوم کسب و کار و بازیابی از فاجعه

- استانداردهای و بهترین شیوه‌های اجرایی تداوم کسب و کار و بازیابی از فاجعه
- اصول مهم در تدوین برنامه‌های کسب و کار و بازیابی از فاجعه در سازمان
- چگونگی تدوین برنامه‌های مدیریت تداوم کسب و کار و بازیابی از فاجعه در سازمان
- معرفی روش‌های اندازه‌گیری کارایی برنامه‌های تداوم کسب و کار و بازیابی از فاجعه

۱۵. اصول تدوین خط‌مشی‌ها، دستورالعمل‌ها و روش‌های اجرایی امنیت اطلاعات در سازمان

- چگونگی تدوین خط‌مشی‌ها، دستورالعمل‌ها و روش‌های اجرایی امنیت اطلاعات
- بررسی تفاوت هر یک از این اسناد با یکدیگر
- چگونگی سنجش اثربخشی این اسناد
- نحوه بازنگری این اسناد
- معرفی منابع و وب‌گاه‌های اسناد از قبل تدوین شده
- اصول طراحی و اجرای برنامه‌های آموزشی و آگاهی‌رسانی امنیتی.

۲-۹- دفاع فعال سایبری

امروزه با گسترش تهدیدات و مخاطرات امنیتی، حتی سازمان‌هایی با بهترین زیرساخت‌های امنیتی هم نمی‌توانند تضمین نمایند که اقدامات یا عملیات بدخواهانه بر روی شبکه آنها رخ نخواهد داد. هنگامی که حوادث امنیتی به وقوع می‌پیوندند، برای یک سازمان، حیاتی است که راهکار مؤثری برای دفاع و همچنین پاسخگویی به آن حملات داشته باشد. سرعت تشخیص، تحلیل

و پاسخگویی سازمان به حوادث امنیتی علاوه بر این که می‌تواند خسارت ناشی از حادثه را محدود سازد، هزینه بازیابی از آن حادثه را نیز به شدت کاهش می‌دهد.

در این دوره آموزشی، مخاطبان ضمن آشنایی با حملات پیشرفته سایبری، مهارت‌های مورد نیاز را جهت طراحی، پیاده‌سازی و مدیریت اجزای کلیدی امنیت شبکه‌های سازمانی، فرا گرفته و می‌توانند از سازمان‌ها در برابر مخاطرات و تهدیدهای امنیتی پیشرفته محافظت کنند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. آشنایی با مفاهیم کلیدی امنیت اطلاعات
۲. آشنایی با حملات سایبری و روش‌های نفوذ به سازمان‌ها
۳. آشنایی با اصول دفاع سایبری
۴. روش‌های ارزیابی فناوری‌های دفاع سایبری
۵. چگونگی تدوین، توسعه و پیاده‌سازی خط‌مشی‌های امنیتی
    - نحوه رعایت تعادل میان مخاطرات و نیازمندی‌های سازمان
    - نحوه شناسایی اهداف تضمین امنیتی
    - نحوه انتخاب فناوری‌های امنیتی
۶. راهکارهای انتخاب فناوری‌های امنیتی مناسب برای سازمان
۷. روش‌های نصب و پیکربندی فناوری‌های امنیتی
    - دیواره آتش (Firewall)
        - چگونگی پیکربندی دیواره آتش برای پشتیبانی از خدمات بیرونی
            - پشتیبانی از خدمات عمومی (HTTP & SMTP)
            - پالایش و مسدودسازی محتوای خطرناک
            - پالایش ترافیک‌های رمزنگاری شده
            - مدیریت سرویس‌های پیچیده (VOIP, Audio & Video)
        - سازوکار ارایه خدمات ایمن بیرونی

- پیاده‌سازی سرویس دهنده‌های عمومی قابل دسترس
- ایجاد یک معماری امن برای مناطق نه چندان حفاظت شده (DMZ)

o روش‌های مجوزدهی دسترسی به خدمات داخلی

- سفارشی‌سازی سرویس نام دامنه (DNS) برای معماری‌های دیواره آتش
- پیکربندی سرویس ترجمه آدرس شبکه (NAT)
- ایجاد لیست‌های کنترل دسترسی برای برنامه‌های کاربردی و کاربران

- سیستم‌های تشخیص و جلوگیری از نفوذ (IPS & IDS)

o بکارگیری سیستم‌های تشخیص و جلوگیری از نفوذ

- مکان‌یابی سیستم‌های تشخیص و جلوگیری از نفوذ در معماری شبکه سازمان
- قراردهی حسگرهای عملیاتی در حالت پنهان

o کشف نفوذ در سازمان

- طراحی سیستم‌های تشخیص و جلوگیری از نفوذ سلسله مراتبی چند لایه‌ای در شبکه سازمان
- مدیریت یکپارچه سیستم‌های تشخیص و جلوگیری از نفوذ توزیع شده

o هشدارهای امنیتی

- کاهش خطاهای مثبت و منفی
- اعتباربخشی رویدادها و تشخیص حملات

o فرایندهای پاسخ فعال به رویدادها و حوادث

- ضدبدافزار
- ضدویروس

۸. پیکربندی کاربران راه دور شبکه‌های خصوصی مجازی (VPN)

- ایجاد تونل‌های VPN

o پشتیبانی از کاربران راه دور با پروتکل تونل زنی لایه ۲ (L2TP)

- اتصال سایت‌های راه دور با پروتکل تونل زنی لایه ۳ (IPSec)

- توسعه راه حل‌های کاربری
  - ارزیابی کاربران راه دور VPN
  - پیاده‌سازی سازوکارهای هویت‌سنجی کاربران راه دور VPN
- الگوریتم‌های احراز هویت تونل‌های VPN
- الگوریتم‌های رمزنگاری و درهم‌سازی تونل‌های VPN
- ارزیابی امنیتی پروتکل‌های تونل زنی
- روش‌های حفاظت از تونل‌های VPN
- فناوری‌ها و تجهیزات سخت افزاری VPN

۹. مدیریت گواهینامه‌های دیجیتال از طریق PKI

۱۰. اصول یکپارچه‌سازی اجزای دفاعی سازمان

۱۱. روش‌های کاهش تأثیر حملات سایبری

۱۲. بررسی معماری‌های امنیتی شبکه

۱۳. روش‌های دفاع عمقی

۱۴. روش‌های اجرایی مقاوم‌سازی سیستم‌های عملیاتی سازمان.

۲-۱۰- راهبردهای امن‌سازی زیرساخت‌های حیاتی

همزمان با گسترش روز افزون فناوری‌های نوین در زیرساخت‌های حیاتی و منابع کلیدی کشورمان، مباحث مربوط به امنیت آنها نیز در عین وجود کارایی، از اهمیت بسیار بالایی برخوردار است چرا که هرگونه آسیب جدی به این زیرساخت‌های حساس می‌تواند لطمات جبران‌ناپذیری را برای آن سازمان‌ها و همچنین شمار زیادی از شهروندان دربرداشته باشد.

در این دوره آموزشی، مخاطبان ضمن آشنایی کامل با زیرساخت‌های حیاتی و تجهیزات امنیتی مورد استفاده در آنها با راهکارهای امن‌سازی و تأمین امنیت در زیرساخت‌های حیاتی، مطابق با استانداردهای بین‌المللی و بهترین تجربه‌های جهانی آشنا

شده و می‌توانند طرح‌های جامع امنیتی را که دربرگیرنده نیازهای اصلی زیرساخت‌های حیاتی در کشورمان است، در این مراکز کلیدی، اجرا و پیاده‌سازی کنند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. سازمان‌های حیاتی و غیرحیاتی
   - آیا می‌توان میان سازمان‌های حیاتی و غیرحیاتی، تمایز قایل شد؟
   - تعاریف زیرساخت حیاتی
   - مهمترین جنبه‌های امنیتی سازمان‌های حیاتی
   - رویکرد شبکه‌ای به زیرساخت‌های حیاتی
   - متدولوژی های شناسایی و طبقه‌بندی زیرساخت‌های حیاتی
۲. آشنایی با سازمان‌های حیاتی و منابع کلیدی
   - طبقه‌بندی ۱۸ گانه زیرساخت‌های حیاتی
   - حوزه‌های موجود در هر گروه از زیرساخت‌های حیاتی
   - سازمان‌ها و نهادهای مسئول حفاظت از هر گروه از زیرساخت‌های حیاتی
۳. زیرساخت‌های مهم فناوری اطلاعات در سازمان‌های حیاتی
   - دلایل اهمیت ویژه به فناوری اطلاعات در زیرساخت‌های حیاتی
   - نقش فناوری اطلاعات در تولیدات و خدمات زیرساخت‌های حیاتی
   - لزوم توجه به امنیت فناوری اطلاعات در زیرساخت‌های حیاتی
   - زیربخش‌های مهم فناوری اطلاعات در زیرساخت‌های حیاتی
۴. آشنایی با مفاهیم امنیت اطلاعات
   - اجزای اصلی امنیت اطلاعات
   - عناصر و مؤلفه‌های کلیدی امنیت اطلاعات
۵. اصطلاح‌ها و واژگان امنیت اطلاعات

۶. چرا امنیت اطلاعات در سازمان‌های حیاتی مهم است؟

- جایگاه حفاظت از اطلاعات در بقای سازمان‌های حیاتی
- تهدیدها و مخاطرات متوجه زیرساخت‌های حیاتی
- روش‌های پاسخگویی به رخدادهای امنیتی در زیرساخت‌های حیاتی
- بردار تکامل حملات به سازمان‌های حیاتی در طول زمان
- سازوکارهای نفوذ به سازمان‌های حیاتی
- انواع بدافزارهای مشاهده شده در سازمان‌های حیاتی

۷. ضرورت توجه به امنیت اطلاعات در سازمان‌های حیاتی

- نحوه گزارش رخدادهای امنیتی در زیرساخت‌های حیاتی
- چگونگی تشخیص تهدیدات در زیرساخت‌های حیاتی
- زمان‌های لازم برای تشخیص تهدیدات در زیرساخت‌های حیاتی
- نقش دارایی‌های لیست نشده در بروز تهدیدات در زیرساخت‌های حیاتی
- نواحی خطر متوجه زیرساخت‌های حیاتی
- عوامل تأثیرگذار بر امنیت در زیرساخت‌های حیاتی

۸. ارتباط زیرساخت‌های حیاتی با فضای سایبر

۹. تاریخچه حملات سایبری به سازمان‌های حیاتی

۱۰. نمونه‌هایی از حمله سایبری به سازمان‌های حیاتی

۱۱. آشنایی با انواع حملات در سازمان‌های حیاتی

- مفاهیم و تعاریف حمله سایبری
- اکسپلویت‌ها و سوءاستفاده از آسیب‌پذیری‌های سیستم
- حملات قابل انجام در زیرساخت‌های حیاتی

۱۲. بررسی انواع حملات سازمانی در سازمان‌های حیاتی

- حملات داخلی و حملات بیرونی به زیرساخت‌های حیاتی
- اهداف و تأثیر حملات داخلی و بیرونی به زیرساخت‌های حیاتی
- دیگر حملات شایع به زیرساخت‌های حیاتی
- روش‌های جلوگیری و مقابله با حملات به زیرساخت‌های حیاتی

۱۳. آشنایی با انواع آسیب‌پذیری و نفوذ به سازمان‌های حیاتی

- مفاهیم آسیب‌پذیری
- عناصر تشکیل دهنده آسیب‌پذیری در سامانه‌های حیاتی
- چهار روش اصلی برای نفوذ به سیستم‌های زیرساخت‌های حیاتی
- متدولوژی نفوذ به شبکه سامانه‌های حیاتی
- روش‌های جلوگیری از نفوذ به شبکه سامانه‌های حیاتی

۱۴. آشنایی با انواع آسیب‌پذیری و تهدیدات امنیتی سازمان‌ها

۱۵. دلایل توجه به امنیت سازمان‌های حیاتی

- نقش حساس سازمان‌های حیاتی در خدمات رسانی
- تهدیدات و حملات نوظهور در سازمان‌های حیاتی
- تأثیرات اقتصادی، فرهنگی و سیاسی
- پیامدهای ناشی از انتشار آسیب‌پذیری در زیرساخت‌های حیاتی
- ارزیابی عملکرد سازمان‌های حیاتی در شرایط بحرانی

۱۶. جنبه‌های امنیتی سازمان‌های حیاتی

- دسترسی غیرمجاز به نرم افزارهای کنترل کننده سیستم‌های کنترل صنعتی
- تأثیر کارمندان ناراضی، در بروز تهدیدات داخلی
- مسایل مرتبط با امنیت ملی در حفاظت از زیرساخت‌های حیاتی

۱۷. مهمترین اولویت‌های نیازهای امنیتی سازمان‌های حیاتی

- ارتباطات اضطراری در زیرساخت‌های حیاتی
- ارزیابی خطر در زیرساخت‌های حیاتی
- آموزش اولین پاسخ دهندگان در زیرساخت‌های حیاتی
- امنیت سایبر در زیرساخت‌های حیاتی
- امنیت بیومتریک و هویت‌سنجی در زیرساخت‌های حیاتی

۱۸. مهمترین مخاطرات امنیتی سازمان‌های حیاتی و روش‌های جلوگیری از آنها

۱۹. مخاطرات امنیتی کارمندان سازمان‌های حیاتی از دیدگاه SANS

۲۰. ضرورت توجه به آموزش کارکنان برای گزارش حوادث امنیتی

۲۱. چرا سازمان‌های حیاتی در برابر مخاطرات امنیت اطلاعات، آسیب‌پذیرند؟

۲۲. وظایف سازمان‌های حیاتی در مواجهه با مخاطرات امنیتی

- نحوه شناسایی مخاطرات و جمع‌آوری شواهد وقوع رخدادهای امنیتی
- اصول حاکم بر تدوین طرح تداوم خدمات سازمان‌های حیاتی
- برنامه‌های بازیابی از وضعیت خرابی در زیرساخت‌های حیاتی
- دارایی‌های حیاتی و دارایی‌های سایبری در زیرساخت‌های حیاتی

۲۳. پنج قدم مهم در مدیریت مخاطرات، بر اساس ISO/IEC 27005

۲۴. چالش‌های امنیتی فراروی سازمان‌های حیاتی

- آسیب‌پذیری‌های موجود در تجهیزات مورد استفاده سازمان‌های حیاتی
- مشکلات امنیتی معماری شبکه و سیستم‌های سازمان‌های حیاتی
- مشکلات امنیتی استفاده از بسترهای فناوری اطلاعات
- گزارشات مربوط به حملات و آسیب‌پذیری‌ها به زیرساخت‌های حیاتی
- تناسب بین کنترل‌های امنیتی و رخدادهای امنیت سایبری در زیرساخت‌های حیاتی
- پیاده‌سازی اقدامات جبرانی برای تهدیدهای جدید

- نقش زمان در پاسخ‌دهی به تهدیدات
- وظایف سازمان‌های یاری‌رسان در هنگام بروز تهدیدات امنیتی به زیرساخت‌های حیاتی

۲۵. مهمترین مشکلات امنیتی سازمان‌های حیاتی

۲۶. امنیت سازمان‌های حیاتی در آمریکا

- وظایف رئیس جمورهای پیشین در امنیت زیرساخت‌های حیاتی ملی
- جایگاه کنگره ملی در امنیت زیرساخت‌های حیاتی
- نقش امنیت سایبر در امنیت ملی آمریکا
- اقدامات اوباما در حوزه امن‌سازی زیرساخت‌های حیاتی آمریکا
- نیروهای نظامی سایبری آمریکا جهت حفاظت از زیرساخت‌های حیاتی
- فعالیت‌های تهاجمی ارتش سایبری آمریکا به زیرساخت‌های حیاتی سایر کشورها

۲۷. بررسی قانون حفاظت از زیرساخت‌های حیاتی در آمریکا

- بررسی قانون بهبود امنیت سایبری زیرساخت‌های حیاتی
- نکات کلیدی در قانون حفاظت از زیرساخت‌های حیاتی آمریکا
- نحوه تعامل سازمان‌های دولتی و خصوصی برای اجرای این قانون
- سیاست‌های ایالات متحده آمریکا در حفاظت از زیرساخت‌های حیاتی
- استراتژی‌های امن‌سازی زیرساخت‌های حیاتی در این قانون
- مشکلات فنی و عملیاتی اجرای این قانون
- جایگاه متدولوژی، در مدیریت تهدیدات سایبری به آمریکا

۲۸. چارچوب امنیت رایانه آمریکا در زیرساخت‌های حیاتی

۲۹. آشنایی با سیستم‌های مدیریت امنیت در زیرساخت‌های حیاتی

۳۰. استانداردهای امنیت سازمان‌های حیاتی

- ISO
- NIST

- IETF

۳۱. طرح‌ها و متدولوژی‌های کاهش مخاطره در زیرساخت‌های حیاتی

- انواع مخاطرات امنیت اطلاعات مطرح در متدولوژی‌های مدیریت مخاطره زیرساخت‌های حیاتی
- روش‌های مدیریت مخاطره در زیرساخت‌های حیاتی
- انواع رویدادها و رخدادهای امنیتی در زیرساخت‌های حیاتی
- سناریوهای امنیتی مطرح در تعیین سطح مخاطرات دارایی‌های موجود در زیرساخت‌های حیاتی
- اصول مهم امنیت اطلاعات در تعیین سطح مخاطرات در زیرساخت‌های حیاتی
- سناریوهای ارزیابی مخاطرات در متدولوژی‌های مدیریت مخاطره در زیرساخت‌های حیاتی
- روش‌های برخورد با مخاطرات در متدولوژی‌های مدیریت مخاطره در زیرساخت‌های حیاتی
- فرایندهای اصلی مدیریت مخاطرات در متدولوژی‌های مدیریت مخاطره در زیرساخت‌های حیاتی
- روش‌های پاسخ به مخاطرات در زیرساخت‌های حیاتی
- متدولوژی مدیریت مخاطرات در زیرساخت‌های حیاتی
- چارچوب‌های مطرح در حوزه مدیریت مخاطرات در زیرساخت‌های حیاتی

۳۲. فرایندهای بهبود امنیت در زیرساخت‌های حیاتی

۳۳. استراتژی‌ها و راهکارهای جامع امن‌سازی سازمان‌های حیاتی

- استراتژی‌ها و راهکارهای جامع NIST
- استراتژی‌های ملی چند کشور مورد مطالعه
- استراتژی‌ها و راهکارهای ایران در خصوص امن‌سازی زیرساخت‌های حیاتی
- بهترین تجربه‌های موجود در این حوزه

۳۴. راهبردهای امن‌سازی زیرساخت‌های حیاتی، در اسناد بالادستی کشور

۳۵. روش‌های اجرایی فراهم‌آوری امنیت در سازمان‌های حیاتی

۳۶. چگونگی پیاده‌سازی روش‌های اجرایی امنیتی در زیرساخت‌های حیاتی

۳۷. کنترل‌های حیاتی برای دفاع اثربخش سایبری در سازمان‌های حیاتی

۳۸. معماری‌های امنیتی و دفاع در عمق در زیرساخت‌های حیاتی

۳۹. استراتژی‌های امنیتی توافق‌نامه‌های شخص سوم در زیرساخت‌های حیاتی

۴۰. مستندسازی امنیتی در حوزه زیرساخت‌های حیاتی

- انواع سندهای امنیتی
- اصول کلی در مستندسازی امنیتی
- الزامات یک سند امنیتی
- سیستم کدگذاری سندهای امنیتی
- استانداردهای موجود در حوزه مستندسازی امنیتی

۴۱. امنیت سایبری در سازمان‌های حیاتی؛ جنگ و دفاع سایبری

۴۲. چند نکته مهم در امنیت اطلاعات سازمان‌های حیاتی

۴۳. امن‌سازی سیستم‌های کنترل صنعتی مورد استفاده در زیرساخت‌های حیاتی

۴۴. قوانین حقوقی در رابطه با امنیت زیرساخت‌های حیاتی در ایران

۴۵. انجمن‌ها و مؤسسات پژوهشی در حوزه امن‌سازی سازمان‌های حیاتی

۴۶. بررسی اسناد و راهنماهای امنیتی NIST

۴۷. آشنایی با فعالیت‌های DHS در حوزه مدل‌سازی امنیت میهن

۴۸. بهترین تجارب جهانی در رابطه با امن‌سازی سازمان‌های حیاتی ملی

۴۹. آشنایی با توانمندی‌های نظامی جمهوری اسلامی ایران در حوزه دفاع از سازمان‌های حیاتی

۵۰. مخفف واژگان و اصطلاحات مورد استفاده در زیرساخت‌های حیاتی.

۲-۱۱- مدل بلوغ امنیت اطلاعات

مدل بلوغ امنیت، ابزاری برای سنجش سطح بلوغ امنیت یک سازمان است. بدون استفاده از مدل بلوغ، تصمیم‌گیری درباره وضعیت فعلی امنیت سازمان و برنامه‌ریزی جهت ارتقای آن بسیار دشوار است. در واقع، مدل بلوغ امنیت نشان می‌دهد که

فعالیت‌های امنیتی سازمان، تا چه حد به بهبود وضعیت امنیت در آن سازمان کمک کرده است و نقاط ضعف امنیتی در چه بخش‌هایی وجود دارند.

در این دوره آموزشی، شرکت کنندگان با متدولوژی‌ها و معیارهای اندازه‌گیری بلوغ امنیت اطلاعات در سازمان آشنا می‌شوند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. مفهوم بلوغ مدیریت امنیت اطلاعات
۲. آشنایی با فرایندها و معیارهای امنیت اطلاعات
۳. سطوح بلوغ امنیت اطلاعات
۴. شناسایی شاخص‌های سنجش میزان بلوغ امنیت اطلاعات
۵. به کارگیری معیارهای سنجش میزان بلوغ فرایندهای امنیت اطلاعات و اهداف امنیتی
۶. مدل فرایندی بلوغ مدیریت امنیت اطلاعات
۷. روش‌های مدیریت مخاطرات امنیتی
۸. مدیریت استراتژیک امنیت اطلاعات
۹. مدیریت تاکتیکی امنیت اطلاعات
۱۰. مدیریت عملیاتی امنیت اطلاعات
۱۱. نقش مدیریت استراتژیک تاکتیکی و عملیاتی در ارتقای بلوغ امنیت اطلاعات.

۲-۱۲- امنیت کاربر رایانه (CSCU)

هر کاربر رایانه باید روش حفاظت از دارایی‌های اطلاعاتی خود و نحوه اتصال ایمن به سیستم‌های دیگر را در شبکه بداند. دوره آموزشی CSCU، دانش امنیت اطلاعات و شبکه یک کاربر رایانه را در استفاده از منابع رایانه‌ای در داخل شبکه سازمان و یا حین اتصال به اینترنت ارتقا می‌دهد. اخذ گواهینامه این دوره، بیانگر آن است که دارنده این مدرک، شایستگی و دانش استفاده از مهارت‌های شبکه‌های رایانه‌ای را دارا بوده و مفاهیم ضروری امنیت اطلاعات را می‌داند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. مقدمه‌ای بر اساس امنیت اطلاعات
۲. نحوه امن‌سازی سیستم عامل
۳. حفاظت از سیستم‌ها توسط ضدویروس‌ها
۴. رمزنگاری اطلاعات
۵. تهیه نسخه پشتیبان و بازیابی اطلاعات
۶. امنیت در اینترنت
۷. امن‌سازی ارتباطات در شبکه
۸. امن‌سازی تبادلات آنلاین
۹. امن کردن ارتباطات پست الکترونیک
۱۰. تهدیدهای مهندسی اجتماعی و راهکارهای مقابله با آن
۱۱. امنیت در شبکه‌های اجتماعی
۱۲. امنیت اطلاعات و انطباق‌های قانونی
۱۳. امن‌سازی تلفن‌های همراه.

۲-۱۳- تهدیدها و آسیب‌های فضای مجازی

همزمان با گسترش فناوری اطلاعات و ابزارهای دیجیتال در زندگی روزمره شهروندان، پیشگیری از آسیب‌ها و تهدیدات ناشی از این فناوری‌های هوشمند، به دغدغه بسیاری از مردم تبدیل شده است. از سوی دیگر، با رشد سریع شبکه‌های اجتماعی در طول چند سال گذشته، موج جدیدی از مخاطرات امنیتی، با هدف تغییر الگوی زندگی شهروندان شکل گرفته است که نیازمند آموزش تمام اقشار جامعه و همچنین توجه جدی به این مسأله است.

در این دوره آموزشی، مخاطبان ضمن آشنایی کامل با آسیب‌ها و تهدیدات شبکه‌های اجتماعی و فضای مجازی می‌توانند با استفاده از راهکارها و رهنمودهای ارایه شده در خصوص امنیت در این شبکه‌های مجازی، از بروز مشکلات ناخواسته برای خود و خانواده‌شان جلوگیری کنند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. شبکه‌های اجتماعی مجازی و بررسی تطبیقی کارکرد آنها از منظر محتوایی
۲. آسیب‌ها و تهدیدات اجتماعی، امنیتی، اقتصادی و سیاسی شبکه‌های اجتماعی
۳. آسیب‌ها و تهدیدات فردی ناشی از نقض حقوق کاربران در فضای مجازی
۴. شبکه‌های اجتماعی و آسیب‌های فردی و اجتماعی
۵. جرایم رایانه‌ای و حقوقی در شبکه‌های اجتماعی مجازی
۶. انواع مجرمان و اهداف جرایم رایانه‌ای در شبکه‌های اجتماعی
۷. اخلاق فناورانه در شبکه‌های اجتماعی مجازی
۸. امنیت کاربران در فضای مجازی
۹. چالش‌ها و تهدیدات نوظهور در شبکه‌های اجتماعی
۱۰. انتشار اطلاعات در شبکه‌های اجتماعی و پیامدهای فرهنگی و سیاسی آن
۱۱. نقش شبکه‌های اجتماعی در شکل‌گیری باندهای جاسوسی، جرم و فساد.

۲-۱۴- مدیریت امنیت اطلاعات در گزینش و استخدام کارکنان

رعایت اصول امنیتی در گزینش و استخدام کارکنان، برای افرادی که در فرایندهای اشتغال به کار کارمندان نقش دارند از اهمیت ویژه‌ای برخوردار است. شرکت کنندگان، در پایان این دوره علاوه بر آشنایی کامل با کنترل‌ها و الزام‌های امنیتی در مراحل گزینش، حین خدمت، تغییر شغل یا خاتمه استخدام کارکنان می‌توانند امنیتی پایدار را برای مجموعه سازمانی خویش، از طریق اعمال کنترل‌های امنیتی خاص کارکنان به دست آورند.

سرفصل‌ها و محتوای این دوره عبارت است از:

۱. آشنایی با امنیت اطلاعات و الزام‌های امنیتی
۲. نحوه شناسایی نیازمندی‌های امنیت اطلاعات سازمان
۳. چگونگی برآورد مخاطرات امنیت اطلاعات مرتبط با کارکنان
۴. آشنایی با امنیت منابع انسانی، پیش از اشتغال و در مرحله گزینش
۵. آشنایی با ضوابط و شرایط استخدام کارکنان

۶. آشنایی با نحوه تنظیم تفاهم‌نامه‌های عدم افشای اطلاعات

۷. انتخاب و پیاده‌سازی کنترل‌های امنیتی خاص کارمندان

۸. چگونگی فراهم‌آوری امنیت اطلاعات در حین خدمت کارمندان

۹. آشنایی با نحوه تدوین فرایندهای انضباطی

۱۰. چگونگی تأمین امنیت اطلاعات پس از خاتمه استخدام یا تغییر شغل کارکنان.

۳- اطلاعات تماس

وب سایت: www.Mvaezi.ir

تلفن همراه: ۰۹۳۶۰۸۹۵۸۴۸

ایمیل: info@mvaezi.ir