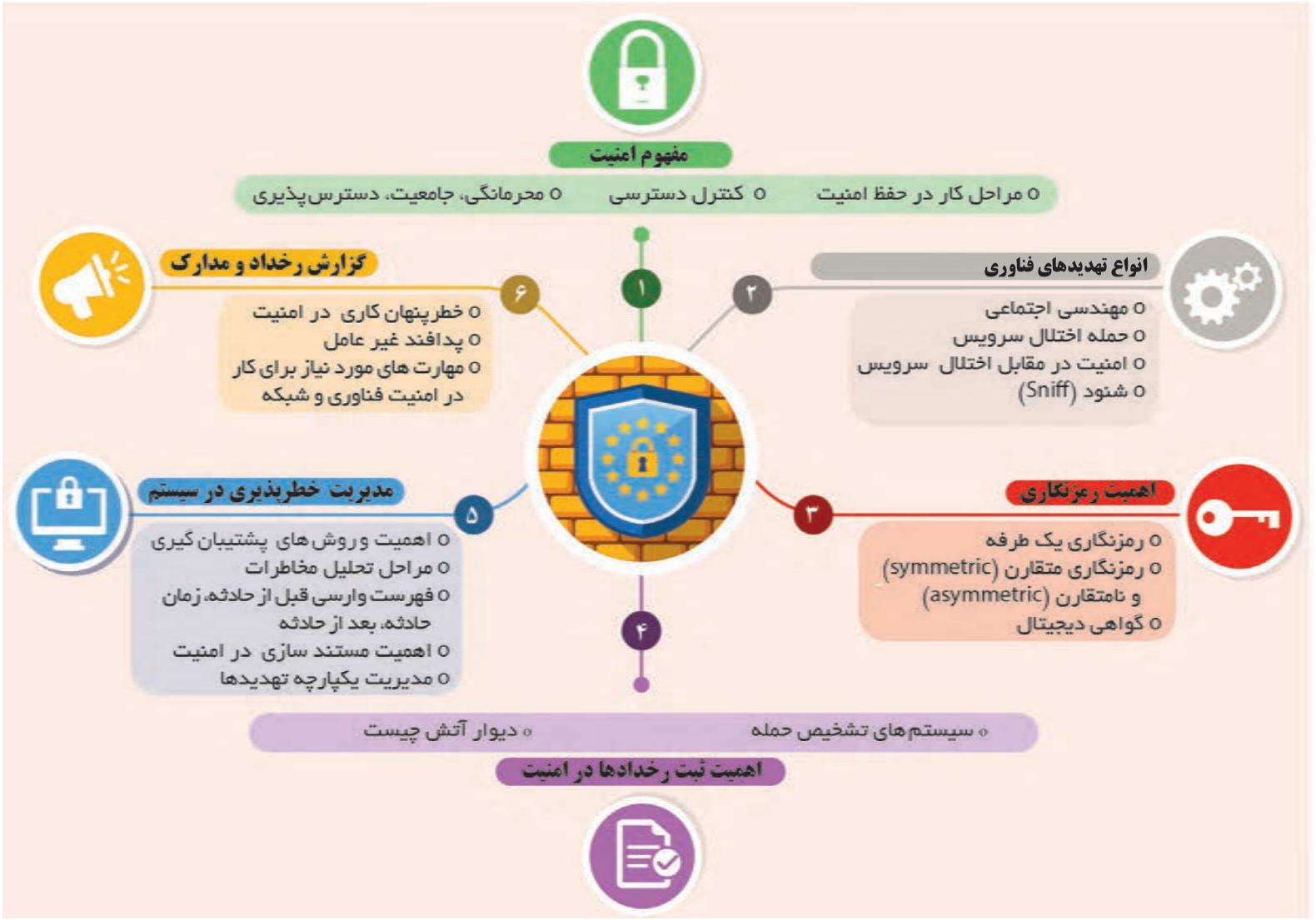
پودمان دوم

تحلیل امنیت در فاوا

در دنیای فناوری اطلاعات و ارتباطات، داده‌ها و منابع اطلاعاتی سرمایه‌های باارزشی هستند که حفظ امنیت آنها بسیار مهم است. منابع اطلاعاتی همواره در معرض انواع تهدیدهای امنیتی و حملات هستند. بنابراین شناسایی انواع تهدیدهای امنیتی در دنیای فناوری اطلاعات و ارتباطات و نحوهٔ پیشگیری از آنها برای حفظ پایداری ارتباط در شبکه ضروری است. در این پودمان با شیوهٔ تشخیص حملات فعال و غیرفعال در شبکه، کاربرد رمزنگاری یک‌طرفه و دوطرفه، تحلیل کنترل دسترسی کاربران به شبکه، نحوهٔ پیاده‌سازی گواهی دیجیتال، ثبت و مستندسازی رخدادهای امنیتی، دیوار آتش، انواع پشتیبان‌گیری، مدیریت خطرپذیری در سیستم‌های اطلاعاتی و پدافند غیرعامل آشنا می‌شوید.

شایستگی‌هایی که در این پودمان کسب می‌کنید:

- تحلیل ناامنی و راهکارهای مقابله با آن
- تحلیل حمله و امن‌سازی


مفهوم امنیت
o مراحل کار در حفظ امنیت
o کنترل دسترسی
o محرمانگی، جامعیت، دسترس‌پذیری
۱
۲
انواع تهدیدهای فناوری
o مهندسی اجتماعی
o حمله اختلال سرویس
o امنیت در مقابل اختلال سرویس
o شنود (Sniff)
۳
اهمیت رمزنگاری
o رمزنگاری یک طرفه
o رمزنگاری متقارن (symmetric) و نامتقارن (asymmetric)
o گواهی دیجیتال
۴
o سیستم‌های تشخیص حمله
o دیوار آتش چیست
اهمیت ثبت رخدادها در امنیت
۵
مدیریت خطرپذیری در سیستم
o اهمیت و روش‌های پشتیبان گیری
o مراحل تحلیل مخاطرات
o فهرست وارسی قبل از حادثه، زمان حادثه، بعد از حادثه
o اهمیت مستند سازی در امنیت
o مدیریت یکپارچه تهدیدها
۶
گزارش رخداد و مدارک
o خطرپنهان کاری در امنیت
o پدافند غیر عامل
o مهارت های مورد نیاز برای کار در امنیت فناوری و شبکه

امنیت

بشر به‌طور فطری نیاز به آرامش دارد و از هرآنچه که ترس او را برمی‌انگیزد دوری می‌کند. در اطراف انسان‌ها عواملی وجود دارند که جان و مال آنها را به خطر انداخته، با ایجاد ناامنی، آرامش را از آنها می‌گیرند. در شرایط ناامنی هر لحظه ممکن است این عوامل دست به کار شده، با تهدید و حمله به دارایی‌ها سبب خسارت شوند. انسان همیشه در این شرایط سعی کرده است تا با کنترل و کاهش این عوامل ناامنی از به خطر افتادن آرامش خود جلوگیری کند و امنیت را به وجود آورد. با تغییر و تحول در عوامل ناامن‌کنندهٔ موجود، ممکن است عوامل جدیدی ایجاد شود به همین علت حفظ امنیت نیاز به مراقبت مداوم و همیشگی دارد.

کنجکاوی

دیروز در راه بازگشت از مدرسه دو موتورسوار با تهدید، رایانه قابل حمل یکی از هنرجویان را به زور گرفتند.
- آیا شنیدن این خبر آرامش شما را تحت تأثیر قرار داده است؟
- عامل ناامنی در این اتفاق چیست؟
- پیشنهاد شما برای کنترل یا حذف عامل ناامنی و جلوگیری از اتفاق مشابه برای دیگر هنرجویان چیست؟
- باخبر شدید که رایانه قابل حمل هنرجو، بیمه سرقت داشته است و شرکت بیمه یک دستگاه جدید به او داده است. آیا تمام خسارت آن هنرجو جبران شده است؟ در این سرقت هنرجو چه چیزهایی را از دست داده است که جبران‌نشدنی است؟ ۳ مورد را یادداشت کنید.

در دنیای فناوری اطلاعات و ارتباطات دو نوع دارایی وجود دارد:

۱ داده‌ها و اطلاعات

۲ منابع: هر بخش فیزیکی یا مجازی که داده‌ها و اطلاعات به شمار نیاید.

فعالیت کلاسی

پول نقد، رایانهٔ قابل حمل، عکس‌ها و پرونده‌های موجود در رایانهٔ قابل حمل شما، از کدام نوع دارایی است؟ اگر برای رایانه قابل حمل شما اتفاقی رخ دهد، بیمه کدام یک از دارایی‌های شما را می‌تواند جبران کند؟ داده‌ها یا منابع؟

هر عامل ناامنی ممکن است دارایی‌های ما را تهدید کند و هنگامی‌که این تهدید عملی شود حمله به دارایی‌های ما رخ داده است.

عامل ناامنی ← تهدید ← حمله

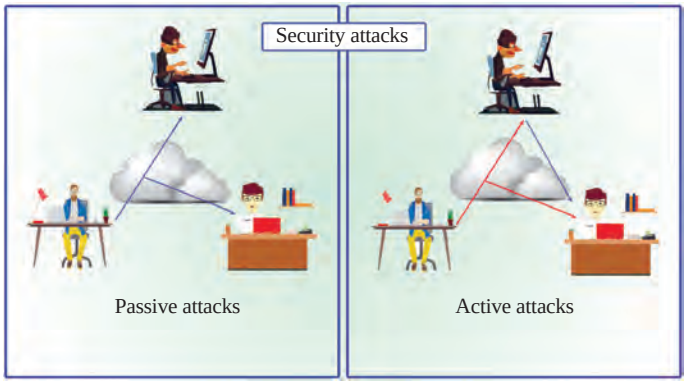
فعالیت کلاسی

ممکن است افرادی با روش‌های مختلف به رایانهٔ قابل حمل یا تلفن همراه دیگران نفوذ کرده، پرونده‌ها و اطلاعات شخصی آنها را مشاهده کنند، بدون اینکه کسی متوجه این اتفاق شود. آیا این کار یک حمله به شمار می‌آید؟

در دنیای فناوری اطلاعات و ارتباطات دو نوع حمله وجود دارد:

۱ فعال: در حملهٔ فعال، تغییر در دارایی و یا خسارت واردشده به وضوح حس می‌شود و قابل مشاهده است.

۲ غیرفعال: در حملهٔ غیرفعال، به داده‌ها دسترسی غیرمجاز صورت گرفته است؛ اما در دارایی‌ها تغییر ظاهری یا خسارتی ایجاد نشده است، حتی ممکن است اثری از حمله دیده نشود.



کنجکاوی

از میان سرقت رایانهٔ قابل حمل و مشاهدهٔ پرونده‌ها با نفوذ به رایانه قابل حمل، کدام مورد حمله فعال و کدام مورد حملهٔ غیرفعال به‌شمار می‌آید؟

محرمانگی (Confidentiality)، جامعیت (Integrity) و دسترس‌پذیری (Availability) به عنوان سه هدف مهم از اهداف مورد نظر در امنیت محسوب می‌شوند(شکل ۱).

شکل۱- مثلث امنیت

محرمانگی عبارت است از اینکه اطلاعات حساس در دست افراد غیرمجاز قرار نگیرد. این کار با کنترل دسترسی افراد انجام می‌شود و فقط به افراد مجاز اجازه دسترسی به اطلاعات داده می‌شود. برای مثال استفاده از گذرواژه برای ورود به تلفن همراه، به منظور افزایش سطح محرمانگی اطلاعات شخصی است.

دسترس‌پذیری به این معنا است که افراد بتوانند به اطلاعات یا دارایی‌های خود در شرایط و مکان‌های مختلف دسترسی داشته باشند. برای مثال فرض کنید شما مقداری پول در یک حساب بانکی دارید. اگر برداشت از حساب بانکی فقط از شعبهٔ خاص، در مکانی خاص و به‌وسیلهٔ شخص شما ممکن باشد، ظاهراً امنیت بالا است؛ اما دسترس‌پذیری به پولتان برای شما کم است. اکنون فرض کنید در مسافرت هستید و به پول نیاز دارید، با اینکه پول دارید و جای پول شما هم امن است، اما چون در لحظهٔ نیاز به این پول دسترسی ندارید، آرامش شما در آن لحظه از بین می‌رود و امنیت کم می‌شود.

جامعیت یا یکپارچگی به قابل استناد بودن اطلاعات گفته می‌شود. فرض کنید برای خرید از یک فروشگاه از کارت بانکی استفاده کرده‌اید. بعد از انجام مراحل و تعیین مبلغ، کلید تأیید را فشار می‌دهید. دستگاه کمی منتظر مانده، سپس پیامی ظاهر می‌شود که تراکنش ناموفق بوده است. هم‌زمان پیامکی دریافت می‌کنید که پول از حساب شما کسر شده است. در این حالت که در اطلاعات خدشه ایجاد شده است یا اعتبار ندارد، گفته می‌شود جامعیت اطلاعات دچار مشکل شده است.

کنجکاوی

فرض کنید پیام تراکنش ناموفق با کاهش مبلغ از حساب برای شما رخ داده است، بانک برای حفظ جامعیت اطلاعات بانکی چه روشی را پیش‌بینی کرده است؟ آیا این پیش‌بینی بانک باعث افزایش امنیت شما شده است؟

مراحل کار در حفظ امنیت

فعالیت‌های ما در برابر حملات به سه بخش پیش از حمله، زمان حمله و پس از حمله تقسیم می‌شود. در فعالیت‌های پیش از حمله سعی می‌شود تا امکان تهدید و حمله کاهش داده شده یا حذف شود. این مرحله مهم‌ترین و اصلی‌ترین بخش امنیت سیستم‌ها به‌شمار می‌آید که اگر این بخش انجام نشود دو بخش بعدی هیچ سودی نخواهد داشت.

بیشترین تلاش ما در زمان حمله باید بر تشخیص حمله و توقف آن باشد. توقف حمله از طریق شناسایی سریع، تشخیص شیوهٔ حمله و از بین بردن نقاط ضعف موجود انجام می‌شود.

فعالیت‌های پس از حمله شامل بررسی شیوهٔ حمله، تعیین خسارت، بازیابی سیستم، تهیه گزارش و پیشنهادهای لازم برای تکرار نشدن حمله است. اطلاعات و نتایج این بخش برای رفع ناامنی موجود ضروری است. پس از این بخش می‌توان دوباره به مرحله پیش از حمله وارد شد.

حفظ امنیت یک فرآیند همیشگی و پیوسته از فعالیت‌های پیش، همزمان و پس از حمله است(شکل ۲).

شکل ۲-چرخه فعالیت‌ها برای حفظ امنیت

کنترل دسترسی

یکی از فعالیت‌های پیش از حمله، کنترل دسترسی است. کنترل دسترسی به این معناست که بتوان مشخص کرد چه کسی به چه مواردی دسترسی داشته باشد. کنترل دسترسی در رسیدن به هدف محرمانگی بسیار حائز اهمیت است. کنترل دسترسی شامل سه بخش احرازهویت (Authentication)، اعتبارسنجی (Authorization) و حسابرسی (Accounting) است.

مثال: فرض کنید برای یک بازی آنلاین، نام کاربری و گذرواژه خریده‌اید. هنگامی که می‌خواهید به تارنمای بازی وارد شوید، این نام کاربری و گذرواژه را وارد می‌کنید. این کار را احرازهویت می‌نامند که در واقع کنترل ورود و خروج است. پس از ورود به تارنما، با توجه به نوع کاربری که دریافت کرده‌اید برخی بازی‌ها را می‌توانید

انجام دهید و به برخی دیگر اجازه دسترسی ندارید. این که پس از ورود چه مجوزهایی دارید، اعتبارسنجی است. با توجه به هزینه پرداختی، نام کاربری و گذرواژه‌ای که به شما داده شده است، تارنمای بازی به شما اجازه بازی به مدت ۳۰ روز را می‌دهد. به این محاسبهٔ تعداد بازی‌ها و میزان حضور شما در تارنمای بازی، حسابداری می‌گویند.

فعالیت کلاسی

دانا برای رایانهٔ رومیزی که برای استفادهٔ همهٔ اعضای خانواده است، تعدادی نام کاربری و گذرواژه تنظیم کرده است. در هرکدام از گزینه‌های زیر مشخص کنید کدام جنبه از کنترل دسترسی انجام شده است.
- برای ورود هر کدام از اعضای خانواده به ویندوز یک نام کاربری و گذرواژه تعریف شده است.
- بعضی از این نام کاربری‌ها اجازهٔ نصب و برخی فقط اجازهٔ اجرای برنامه‌ها را دارند.
- نام کاربری و گذرواژهٔ برادر کوچک‌تر فقط اجازهٔ ورود به مدت ۲ ساعت در ساعات اولیهٔ عصر را دارد.

فعالیت منزل

- برای کنترل دسترسی و احراز هویت روش‌های مختلفی وجود دارد. ساده‌ترین روش نام کاربری و گذرواژه است. در فهرست زیر تعدادی از این روش‌ها معرفی شده‌اند. در مورد میزان امنیت هر کدام از این روش‌ها، مکان‌ها و وسایلی که از این روش‌ها استفاده می‌کنند در اینترنت جست‌وجو کنید و نتایج آن را به کلاس ارائه دهید:
اثر انگشت، اسکن عنبیه چشم، دستگاه گذرواژه‌ساز یا توکن، کارت هوشمند، اسکن چهرهٔ افراد و RFID
- امروزه تقریبا همهٔ بانک‌ها تارنما دارند که مشتری در آن می‌تواند امور بانکی مانند انتقال وجه را انجام دهد. از میان بانک‌های ایران، یکی را به دلخواه انتخاب کنید و در مورد شیوهٔ احراز هویت مشتری در ورود به تارنمای اینترنتی و انتقال وجه تحقیق کرده، نتایج را به کلاس ارائه کنید.

اهمیت قطعات اطلاعاتی در امنیت فناوری

شما مسئول رایانهٔ یک شرکت هستید. این شرکت برنامهٔ حسابداری و کنترل حضور و غیاب دارد.
رخداد اول: برنامه نشان می‌دهد که در روزهای کاری، حسابدار وارد برنامه حسابداری شده است. آیا این یک اتفاق غیرعادی است؟
رخداد دوم: در برخی از زمان‌ها برنامهٔ حضور و غیاب نشان می‌دهد که حسابدار وارد شرکت نشده است. آیا این رخداد غیرعادی است؟

کنجکاوی

رخداد اول و دوم در یک زمان رخ داده‌اند! برنامه نشان می‌دهد که حسابدار در شرکت حضور ندارد؛ اما وارد برنامه حسابداری شده است! آیا این اتفاق یک وضعیت خوب است یا بد؟ حدس شما چیست؟ آیا باز همه چیز به نظر عادی می‌رسد؟

امنیت فناوری مانند یک تصویر بزرگ درنظر گرفته می‌شود. اگر هر قطعه اطلاعات مانند یک نقطه از این تصویر فرض شود، معنای خاصی نمی‌دهد و در ظاهر تک تک این قطعه‌ها بی‌معنا و کم اهمیت هستند؛ اما وقتی این نقطه‌ها کنار هم قرار می‌گیرند، معنا پیدا می‌کنند و به یک تصویر مهم تبدیل می‌شوند. اگر بتوان قطعه‌های مناسب را جمع‌آوری کرد، ممکن است از یک نقطه ضعف یا خطر مهم آگاه شد.

انواع تهدیدهای فناوری اطلاعات و ارتباطات

اکنون سؤال این است که ناامنی در دنیای فناوری اطلاعات و ارتباطات به چه دلیل رخ می‌دهد؟ در واقع غفلت یا اشتباه در یکی از مراحل کار باعث ناامنی می‌شود. این اشتباه ممکن است در مراحل تولید یک نرم‌افزار، ساخت سخت‌افزار، فرستادن اطلاعات یا حتی با پاسخ به یک تماس تلفنی بدون بررسی هویت فرد تماس‌گیرنده رخ دهد.

مهندسی اجتماعی

شرکتی برای مشتریان خود حساب اینترنتی با امکان واریز پول به حساب باز کرده است. امروز یکی از مشتریان با پشتیبانی تماس گرفت و اعلام کرد گذرواژهٔ خود را فراموش کرده است و امکان دسترسی به حساب خود را ندارد. از آنجایی که این مشتری گردش مالی زیادی دارد، برای شرکت جلب رضایت او از اهمیت زیادی برخوردار است.

اکنون شما به عنوان کارشناس امنیت چه تصمیمی می‌گیرید و چه کاری انجام می‌دهید؟

اتفاق ماه گذشته: در ماه قبل یک مشتری ادعا کرده بود گذرواژه خود را فراموش کرده است؛ بنابراین گذرواژهٔ جدیدی برای او تنظیم شد. روز بعد مشتری تماس گرفت که چرا نمی‌تواند وارد حساب خود شود! گذرواژه مجدد تغییر کرد و بعد از ورود به حساب خود ادعا کرد حسابش خالی است! با او در مورد تغییرگذرواژهٔ روز قبل صحبت شد و او اظهار بی‌اطلاعی کرد!

در دنیای فناوری ممکن است افرادی با دروغ بخواهند دیگران را فریب دهند. آنها معمولا با اطلاعات کمی که قبلا به دست آورده‌اند سعی می‌کنند با افراد ارتباط برقرار کرده، بر اساس علایق آنها رفتار و اعتمادشان را جلب کنند تا به هدف خود برسند. این سارقان بر اساس روابط اجتماعی از فرصت‌های ارتباطی با افراد سوءاستفاده کرده، به نوعی ذهن طرف مقابل را مهندسی می‌کنند. این فرآیند به مهندسی اجتماعی معروف است. بعضی اوقات مهندسی اجتماعی برای کسب اطلاعات بیشتر در مرحله بعدی صورت می‌گیرد. برای مثال یک رایانامه به شما اعلام می‌کند در یک مسابقه برنده شده‌اید و برای دریافت جایزه، باید فرم اطلاعات شخصی خود را پر کنید. شما این کار را بدون خطر می‌دانید! پس فرم را بدون بررسی بیشتر پر می‌کنید، غافل از اینکه فردا یک نفر با داشتن اطلاعات شخصی شما با شرکت تماس می‌گیرد و با دادن آن اطلاعات، درخواست تغییر گذرواژهٔ شما را می‌دهد!

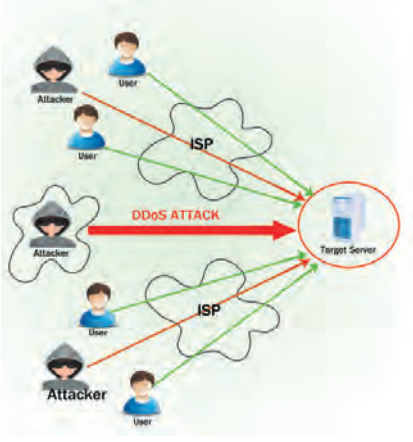
بهترین راه برای مقابله با مهندسی اجتماعی این است که برای انجام کارها مراحل مشخصی تعریف شود و همه موظف به رعایت آن باشند تا خطر سوءاستفاده از بین برود.

کنجکاوی

در پایان وقت اداری، ناگهان یک حافظهٔ فلش کنار میز خود مشاهده می‌کنید! روی برچسب آن، عبارت «فیلم‌های جدید» نوشته شده است و به نظر می‌رسد پر از فیلم است. کنجکاو شده‌اید که بدانید داخل حافظه فلش چیست؟ رایانهٔ شرکت روشن است،کار هم تمام شده است و شاید فرصت مناسبی باشد تا حافظهٔ فلش را بررسی کنید! برای یافتن صاحب آن هم شاید لازم باشد محتویاتش را مشاهده کنید. در این موقعیت چه می‌کنید؟ آیا فلش را بررسی می‌کنید؟

یکی از روش‌های نفوذ به سیستم‌ها، ایجاد یک برنامهٔ مخرب روی یک حافظه فلش یا لوح فشرده است. معمولاً کاربران با روش مهندسی اجتماعی فریب داده می‌شوند و این برنامه‌ها را اجرا می‌کنند و با اجرای این برنامه‌های مخرب، رایانه کاربر در اختیار مهاجم قرار می‌گیرد. البته مشکل اصلی مهاجم این است که چطور کاربر را تحریک کند تا حافظهٔ فلش یا لوح فشرده را باز کند. آیا پیشنهادی دارید؟

حمله اختلال سرویس(DoS)



هر خدمتی مراحلی از شروع تا پایان دارد که به آن خدمت، سرویس و به انجام آن خدمت، سرویس‌دهی می‌گویند. هزینه و زمان لازم برای انجام سرویس با توجه به شرایط مختلف متفاوت است. کاهش سرعت دریافت خدمت به هر دلیلی را اختلال سرویس می‌گویند. بدترین حالت اختلال سرویس، نقص یا توقف کامل یک خدمت است. دلیل اختلال سرویس ممکن است عمدی یا غیرعمدی باشد. این دلیل می‌تواند ناشی از یک اتفاق ساده مانند قطع برق، رخداد طبیعی یا یک تصمیم اشتباه باشد. اما در هر صورت وقتی که سرویس‌دهی درست انجام نشده باشد، اختلال سرویس رخ داده است.

برای مثال فرض کنید تارنمایی بخواهد برای ۶۰۰ نفر کارنامه اعلام کند. توان تجهیزات تارنما نمایش ۱۰ کارنامه در دقیقه است. تارنما به‌صورتی طراحی شده است که ابتدا صفحهٔ ورود مشخصات نمایش داده می‌شود و پس از فشردن کلید جست‌وجو، پردازش لازم انجام شده، کارنامه مشاهده می‌شود. اگر افراد با نظم و به نوبت برای مشاهدهٔ کارنامه اقدام کنند، زمان کار تجهیزات برای اعلام همهٔ نتایج در حدود ۶۰ دقیقه معادل یک ساعت خواهد بود؛ اما اگر تمام افراد بخواهند در همان شروع اعلام نتیجه همزمان وارد تارنما شوند ازدحام رخ می‌دهد، حتی ممکن است تا چند ساعت صفحهٔ اول تارنما هم باز نشود و در عمل برای مدتی اختلال سرویس رخ دهد. این اختلال سرویس غیرعمدی است و با افزایش توان تجهیزات یا زمان‌بندی افراد برای مراجعه به تارنما قابل پیشگیری است.

اما کارها همیشه به همین خوبی پیش نمی‌رود. فرض کنید فردی یک برنامهٔ مخرب نوشته است که با ارسال درخواست‌های مکرر به تارنمای ذکر شده در مثال بالا، صفحهٔ اول آن را چند هزار بار در دقیقه فراخوانی می‌کند. به ظاهر کار خطرناکی صورت نگرفته و آسیبی به دستگاه‌ها و تارنما وارد نشده است؛ اما تارنمای موردنظر به طور مداوم درحال نمایش صفحهٔ اول و پاسخگویی به درخواست برنامهٔ مخرب است که باعث می‌شود هیچ یک از کاربران دیگر موفق به مشاهدهٔ صفحهٔ اول تارنما یا دریافت کارنامهٔ خود نشوند. این یک مثال از حملهٔ اختلال سرویس (Denial of Service) است.

مدیر شبکه با تشخیص حملهٔ اختلال سرویس، برای اینکه حملهٔ صورت گرفته از بین برود و کارها به حالت عادی بازگردد، می‌تواند دسترسی آن فرد و برنامه مخرب را قطع کند.

اکنون فرض کنید این فرد برنامه‌ای را که نوشته است، مانند یک ویروس در تمام رایانه‌های یک شهر پخش کند و این رایانه‌ها به طور همزمان به تارنمای موردنظر درخواست ارسال کنند، در این مورد با حملهٔ اختلال سرویس توزیع شده (DDoS(Distributed Denial of Service)) روبه‌رو هستیم که متاسفانه این نوع حمله به راحتی قابل رفع نیست.

کنجکاوی

بیشتر دانشگاه‌ها انتخاب درس در هر نیم‌سال تحصیلی را به صورت اینترنتی انجام می‌دهند. معمولاً دانشگاه‌ها، افراد را بر اساس حروف الفبا یا سال ورود به دانشگاه، در روزهای متفاوتی ملزم به انجام این کار می‌کنند. دلیل این زمان‌بندی چیست؟

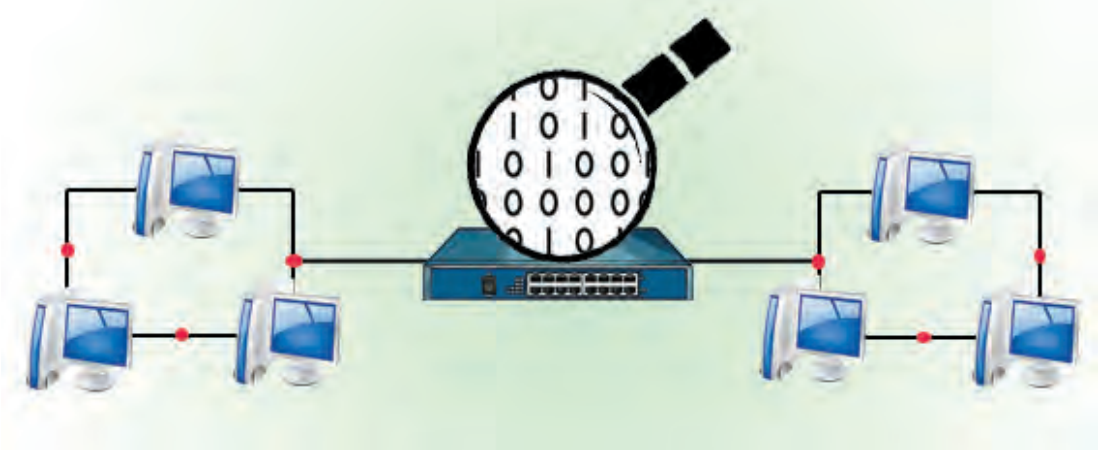
امنیت در مقابل اختلال سرویس

فرض کنید برای دیدن بازی فوتبال به ورزشگاه رفته‌اید. برای ورود نیاز به ارائه بلیت است. این موضوع باعث کاهش سرعت ورود به ورزشگاه و ایجاد صف شده است. در این بازی علاوه بر دریافت بلیت قرار است برای جلوگیری از ورود اشیا ممنوعه، افراد بازرسی شوند. آیا بهتر نیست برای جلوگیری از تجمع و ایجاد صف، بررسی بلیت ورود به ورزشگاه یا وسایل ممنوعه هنگام ورود انجام نشود؟

روان‌ترین و سریع‌ترین روش انجام کارها این است که هیچگونه امنیتی بررسی نشود. اما هرگاه لازم باشد امنیت حفظ شود، باید کنترل‌هایی صورت بگیرد که این کنترل‌ها، هزینه اضافی یا اختلال در انجام کار خواهند داشت. این هزینه‌ها و اختلالات، خود نوعی اختلال سرویس به‌شمار می‌آیند. به همین دلیل باید مراقب بود که امنیت تا جایی اضافه شود که باعث توقف یا اختلال در کار اصلی نشود. نقطه تعادل میان سطح امنیت و اختلال سرویس برای هر کار بر اساس اهداف، حساسیت و اهمیت آن کار متفاوت است و تشخیص این نقطه تعادل از وظایف مهم یک کارشناس امنیت است.

شنود (Sniff)

هنگامی که دو نفر با تلفنی صحبت می‌کنند، اگر شخص سومی بتواند به هر روشی حتی داشتن یک تلفن دیگر روی خط، صدای آنها را بشنود در واقع شنود انجام داده است. در دنیای شبکه شنود به شکل دیگری هم رخ می‌دهد. برای مثال هنگامی که برای ورود به یک تارنما، نام کاربری و گذرواژه وارد می‌شود، در واقع نام کاربری و گذرواژهٔ ارسالی به صورت بسته‌های اطلاعاتی به تارنمای مورد نظر فرستاده می‌شود. ممکن است فرد دیگری روی شبکه دستگاهی نصب کرده باشد که از هر بستهٔ اطلاعاتی که از شبکه عبور می‌کند یک نسخه تهیه کند. اکنون این فرد نام کاربری و گذرواژه شما را می‌داند!



یادداشت

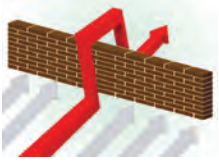
به برداشت غیرمجاز اطلاعات در یک ارتباط، بدون اطلاع فرستنده و گیرنده، شنود گفته می‌شود.

کنجکاوی

در جنگ تحمیلی فرمانده‌های ایران برای هماهنگی با مرکز فرماندهی با دستگاه بی‌سیم تماس داشتند. دشمن هم برای اینکه بتواند از فرمان‌های پایگاه اصلی مطلع شود، سعی می‌کرد با دستگاه بی‌سیم مشابه به مکالمه‌ها گوش کند. برای اینکه این اتفاق رخ ندهد، افرادی که با بی‌سیم‌ها کار می‌کردند آموزش‌های ویژه‌ای می‌دیدند. آیا می‌توانید یکی از این آموزش‌ها را حدس بزنید؟

شنود در دنیای فناوری اطلاعات و ارتباطات غیرقابل اجتناب است. برای مثال وقتی با تلفن همراه هوشمند یا رایانه قابل حمل به صورت بی‌سیم به اینترنت متصل هستید، چه بخواهید و چه نخواهید امواج دستگاه بی‌سیم در فضای اطراف شما پخش می‌شود و افرادی که در نزدیکی خانهٔ شما هستند می‌توانند این امواج را دریافت کنند. در مثالی دیگر وقتی شما نام کاربری و گذرواژه را در یک تارنمای اینترنتی وارد می‌کنید، در مسیر بین شما و تارنمای مورد نظر، بسته‌های اطلاعاتی از دستگاهی به نام مسیریاب (Router) عبور می‌کنند، این دستگاه به راحتی امکان ذخیره و شنود این بسته‌ها را دارد و هیچ تضمین صد درصدی وجود ندارد که بسته‌ها در دنیای اینترنت از مسیریاب‌های دشمن شما عبور نکنند.

خطرهای امنیتی بر اساس ملاک‌های مختلف قابل دسته‌بندی است؛ اما به صورت کلی با توجه به منبع اصلی اشتباه، موارد زیر را می‌توان نام برد:

ریشه و پایهٔ تهدید	شرح و خلاصه
مهندسی اجتماعی 	در میان این دسته‌بندی شاید بتوان گفت خطرناک‌ترین و غیرقابل کنترل‌ترین نوع، همان تهدیدهای مهندسی اجتماعی است. زیرا عامل اصلی در آن، اشتباه نیروی انسانی است که غیرقابل پیش‌بینی است و گستردگی تهدید نیز غیرقابل اجتناب است. به همین دلیل خبر انواع حملات مهندسی اجتماعی هر روزه در رسانه‌ها دیده می‌شود.
بدافزاری 	بدافزار یک برنامه برای خرابکاری است. بدافزارها بر اساس شیوه کار، روش ورود به رایانه، نوع تکثیر و نوع خسارت به انواع مختلفی تقسیم می‌شوند. یکی از مثال‌های معروف بدافزارها اسب تروا (Trojan) است. این برنامه در ظاهر به صورت یک برنامه مفید و کار راه‌انداز به کاربر داده می‌شود ولی در عمل ممکن است رایانه قربانی را تحت کنترل بگیرد یا اطلاعات حساسش را سرقت کند.
شبکه 	به قراردادهایی که برای هماهنگی کار شبکه‌ها طراحی شده است، پروتکل گفته می‌شود. تهدیدهای بر پایه شبکه در واقع تهدیدهایی هستند که ریشه در پروتکل‌های شبکه‌ها دارند. به عنوان نمونه می‌توان به حمله اختلال سرویس روی پروتکل عیب‌یابی شبکه (ICMP) اشاره کرد. پروتکل‌های عیب‌یابی برای بررسی و رفع اشکالات شبکه ساخته شده‌اند؛ اما اگر تعداد زیادی پیام عیب‌یابی به یک تارنما فرستاده شود، آن تارنما متوقف می‌شود و کاربران نمی‌توانند با آن کار کنند و اختلال سرویس رخ خواهد داد.

ریشه و پایه تهدید	شرح و خلاصه
ساختار نرم‌افزارها 	این نوع تهدیدها به شیوه کارکرد نرم‌افزارها بستگی دارند. به عنوان نمونه شما برنامه‌ای را برای کنترل رایانه از راه دور نصب می‌کنید. این یک امکان مفید است؛ اما اگر این نرم‌افزار، ایراد یا ضعف امنیتی داشته باشد ممکن است حمله‌کننده بتواند رایانه شما را از راه دور کنترل کند.
ساختار سخت‌افزار (فیزیکی) 	برخی سخت‌افزارها نقاط ضعف دارند. برای مثال هنگامی که یک کلید را در یک صفحه کلید معمولی فشار می‌دهید، با فشاردادن کلید، یک ضربه مغناطیسی ایجاد می‌شود که شبیه به صدای ضربه‌ای است که روی طبل زده می‌شود و به صورت امواجی در فضا منتشر می‌شود. این امواج فقط با دستگاه‌های قوی و در فاصله‌ای خاص قابل دریافت هستند که از طریق آنها می‌توان مشخص کرد کدام کلید فشرده شده است. فرض کنید کاربر در حال ورود گذرواژه بوده است. به همین دلیل برای مکان‌ها و رایانه‌های حساس نباید از هر صفحه کلید معمولی استفاده کرد.

پژوهش

نام اسب تروا از یک داستان قدیمی یونانی گرفته شده است. در مورد این نام تحقیق کنید.

فعالیت منزل

در مورد شیوهٔ کار و خسارت انواع تهدیدهای بدافزاری زیر در اینترنت جست‌وجو کنید و نتایج را در قالب گزارش به هنرآموز خود تحویل دهید.

Virus , Worm, SpyWare , Trojan , Rootkit ,Ransomware

اهمیت رمزنگاری

فعالیت گروهی

من هنرجوی پایه دوازدهم هستم. این روزها خبر برگزاری مسابقات رباتیک در هنرستان ما پیچیده است. مسابقه به صورت گروه‌های ۵ نفره برگزار می‌شود. همه دوست دارند که عضو گروه باشند. هنرآموز، ماهر را که یکی از هنرجویان فعال و پرتلاش کلاس است به عنوان کاپیتان انتخاب کرد و از او خواست نام خود و سه نفر دیگر را به عنوان اعضای اصلی گروه رباتیک و یک نفر هم به عنوان رابط بین هنرآموز و گروه، به ایشان معرفی کند. امروز ماهر سه نفر را برای اعضای گروه خود انتخاب کرد و برای انتخاب رابط، پای تخته رفت و این واژه‌ها را نوشت:

nbifs bsnbo ebob pnje

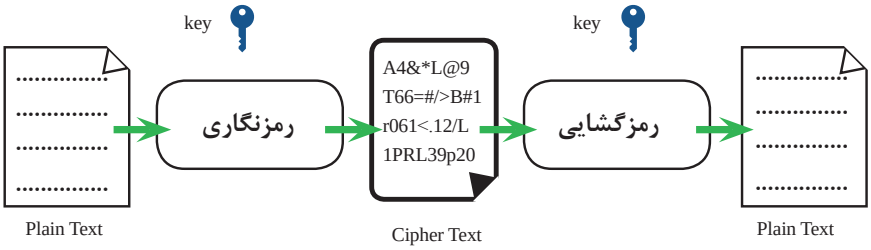
ماهر گفت این واژه‌ها، اسم افراد گروه است که به صورت رمز نوشته شده است. او گفت دانا، آرمان و خودش اعضای گروه هستند و اسم‌ها را روی تخته نوشت.

maher arman dana .....

ماهر نفر بعدی را اعلام نکرد، او گفت هر کس بتواند نام نفر بعد را تشخیص دهد به عنوان رابط انتخاب می‌شود. قرار است مسابقات در شهر دیگری برگزار شود و من خیلی دوست دارم همراه گروه باشم. می‌توانید به من کمک کنید تا نام نفر بعدی را کشف کنم؟

معمایی که مطرح شد یک مثال ساده از رمزنگاری است. از آنجایی که امکان حذف شنود وجود ندارد باید اطلاعات ارسالی رمزنگاری شود تا دیگران که آن را مشاهده می‌کنند، نتوانند مفهوم آن را متوجه شوند و فقط واژه‌ها و حروف به هم‌ریخته‌ای ببینند.

در هر ارتباطی حداقل سه بخش وجود دارد: فرستنده اصلی پیام، مسیر(Channel) ارتباطی، گیرندهٔ اصلی پیام. فرستنده یک پیام ساده (PlainText) را با انجام مراحلی، رمزنگاری (Encryption) می‌کند. اکنون فرستنده این متن رمزشده یا اصطلاحا کدشده (CipherText) را روی کانال ارتباطی می‌فرستد. گیرنده متن کدشده را دریافت می‌کند. در همین زمان دشمن روی کانال ارتباطی در حال شنود است و متن کدشده را دریافت می‌کند! اما متن دریافتی برای دشمن مفهومی ندارد چون کلید معما را ندارد! ولی گیرنده اصلی کلید را دارد و با انجام مراحل رمزگشایی (Decryption) روی متن کدشده، دوباره متن ساده را از آن به‌دست می‌آورد (شکل ۳). در واقع همه گیرنده‌ها چه گیرنده اصلی و چه دشمن پیام را دریافت می‌کنند؛ اما فقط افرادی می‌توانند مفهوم آن را درک کنند که کلید رمزنگاری را دارند.



شکل ۳- رمزنگاری پیام

اصل مهم امنیت فناوری اطلاعات و ارتباطات : همیشه فرض کنید کانال ارتباطی در حال شنود است! بنابراین قبل از فرستادن اطلاعات باید رمزنگاری را فعال کنید تا اطلاعات به صورت رمزشده فرستاده شوند. به این کار امن کردن کانال ارتباطی می‌گویند و همیشه قبل از فرستادن باید کانال ارتباطی را امن کرد.

کنجکاوی

برای خرید یک قفل به مغازه‌ای مراجعه کرده‌اید. فروشنده به شما یک ردیف قفل نشان داده است تا یکی را انتخاب کنید. اما همهٔ قفل‌ها مشابه یکدیگر هستند! پس چه تضمینی وجود دارد که قفل خریداری شده به‌وسیلهٔ فرد دیگری باز نشود؟ آیا مشابه بودن قفل‌ها سبب خطر باز شدن آنها به‌وسیلهٔ دیگران می‌شود؟

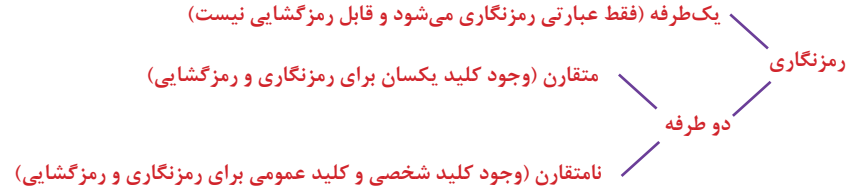
فعالیت گروهی

در ماجرای قبل با کمک شما توانستم نام نفر چهارم را تشخیص دهم. اکنون من عضو گروه رباتیک شدم. ماهر یک پیام رمزنگاری شده برای من فرستاده است. به من کمک کنید تا متوجه شوم ماهر چه پیامی به من داده است:

gbseb tpci cjzb tbmpo ufoojt ubnsjo ebsjl

در معمایی که حل کردید روش رمزنگاری "جابه‌جایی حرف" است و کلید آن ۱ است. یعنی هر حرفی به اندازهٔ ۱ حرف بعدی تعویض شده، فرستاده می‌شود. گیرنده هم آن را دریافت می‌کند و با همان روش یعنی جابه‌جایی حرف و با داشتن کلید یعنی یک حرف جابه‌جایی، متن اصلی را به‌دست می‌آورد. پس واژهٔ maher به nbifs تبدیل می‌شود. البته ممکن است شما کلید ۲ را انتخاب کنید در این صورت واژهٔ maher با جابجایی با ۲ حرف به ocjgt تبدیل می‌شود.

این روش یکی از قدیمی‌ترین و البته ساده‌ترین روش‌های رمزنگاری است که در تاریخ بشر ثبت شده است. امروزه با سرعت و توانایی رایانه‌ها، کلید رمز این روش به راحتی کشف می‌شود و باید روش‌های پیشرفته‌تری را به کار برد. علم ریاضی در این موضوع به کمک فناوری آمده و روش‌های بسیار جالبی را اختراع کرده است. تمام سازندگان وسایل ارتباطی، روش‌ها را می‌دانند و از آن استفاده می‌کنند. فرستنده و گیرنده روش رمزنگاری را می‌دانند و حتی دشمن هم روش رمزنگاری را می‌داند! تنها چیزی که محرمانه است کلید رمزنگاری است. هر چه کلید رمزنگاری پیچیده‌تر و بزرگ‌تر باشد، شکستن رمز سخت‌تر می‌شود. پس بسیار مهم است که کلید رمزنگاری فاش نشود. انواع رمزنگاری در شکل زیر آمده است.



شکل۴- انواع رمزنگاری

رمزنگاری یک طرفه و کاربرد آن

رمزنگاری‌هایی که تاکنون گفته شد دوطرفه و بازگشت‌پذیر بوده است. یعنی متن معمولی به متن کدشده رمزنگاری می‌شود و متن کدشده نیز دوباره می‌تواند با کلید رمزگشایی، به متن معمولی برگردانده شود؛ اما در رمزنگاری یک طرفه، متن معمولی به صورتی رمز می‌شود که دیگر نتوان از آن متن اصلی را به‌دست آورد. رمز نگاری یک طرفه غیر قابل بازگشت است.

فیلم

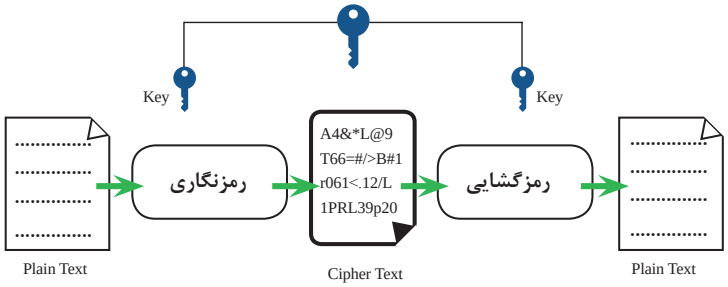
پویانمایی «رمزنگاری یک‌طرفه»

کنجکاوی

چرا تارنماهای مختلف پیشنهاد می‌کنند برای گذرواژه حتما از ترکیب حروف بزرگ و کوچک، ارقام و چند علامت استفاده کنید و طول گذرواژه هم کمتر از ۱۰ نویسه نباشد؟

رمزنگاری متقارن (Symmetric) و نامتقارن (Asymmetric)

برای رمزنگاری و رمزگشایی دو طرفه، کلید لازم است. اگر کلید فرستنده و گیرندهٔ اصلی یکسان باشد به آن رمزنگاری متقارن گفته می‌شود (شکل۵).

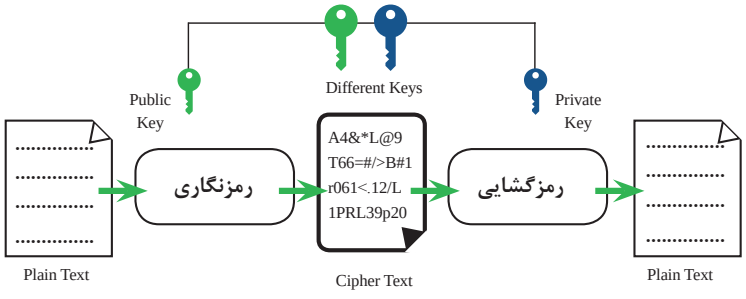


شکل۵- رمزنگاری متقارن

دانا و بینا می‌خواهند برای ارسال پیام، کانال ارتباطی را امن کنند. برای این کار می‌خواهند از روش رمزنگاری متقارن استفاده کنند. دانا چگونه باید کلید اصلی را به بینا برساند؟ یک مشکل جدی، رساندن کلید به طرف دیگر است! دقت کنید که اگر قرار باشد فرستنده، کلید را روی کانالی که هنوز رمزنگاری نشده است برای گیرنده ارسال کند، دشمن هم کلید را می‌بیند! پس ادامهٔ کار دیگر چه فایده‌ای دارد!. برای ارسال محرمانهٔ کلید نیاز به کانال امن دارید و برای داشتن کانال امن ابتدا باید کلید رمزنگاری یکسان در فرستنده و گیرنده داشته باشید! (داستان مرغ و تخم مرغ!)

این موضوع به ظاهر ساده، یکی از بزرگترین مشکلات دنیای رمزنگاری بوده است و حتی در جنگ جهانی دوم هم باعث تغییر سرنوشت چند جنگ مهم شده است زیرا باید به روشی کلید به گیرنده‌ها می‌رسید و مدیریت فرستادن کلیدها سخت بود و روش فرستادن به راحتی فاش می‌شد.

تنها راه‌حل ممکن، استفاده از دو کلید متفاوت است! یک کلید نزد فرستنده بماند و یک کلید به طرف مقابل فرستاده شود. به کلیدی که نزد فرستنده است کلید خصوصی (Private Key) و به کلیدی که برای طرف مقابل فرستاده می‌شود کلید عمومی (Public Key) می‌گویند. قانون کار این است که اگر پیام با کلید عمومی رمزنگاری شود فقط با کلید خصوصی قابل رمزگشایی و باز شدن است. این نوع رمزنگاری که در آن کلید رمزنگاری با کلید رمزگشایی متفاوت است را رمزنگاری نامتقارن می‌گویند(شکل۶).



شکل۶- رمزنگاری نامتقارن

تنها مسئلهٔ باقی مانده این است که چطور می‌شود کلید خصوصی و عمومی را ساخت که با یکی متن رمزگذاری و با دیگری رمزگشایی شود؟ تعدادی ریاضی‌دان شیوهٔ انجام این کار را در سال‌های ۱۹۷۰ تا ۱۹۷۳ با استفاده از محاسبات ریاضی پیدا کردند.

فیلم

پویانمایی «رمزنگاری دوطرفه»

شیوه‌های رمزنگاری خطر شنود را تا حدود زیادی کاهش داده است، اما آیا هکرها هیچ راه‌حلی برای فریب ما ندارند؟

شکل ۷ را ببینید و حدس بزنید چگونه یک هکر توانسته است با این همه رمزنگاری، پیام‌های ارسالی را کشف کند! راهنمایی: کاربر ۱ واقعا تصور می‌کند که مستقیماً با کاربر ۲ در ارتباط است!

شکل ۷- شنود پیام‌ها به‌وسیله هکر

گواهی دیجیتال

با روش‌های رمزنگاری می‌توان از طریق یک کانال ناامن کلید اصلی رمزنگاری را بدون نگرانی از لو رفتنش فرستاد. اما باز هم یک مشکل وجود دارد. ممکن است سیستمی میان ما و سیستم اصلی قرار گرفته باشد که خود را به جای سیستم اصلی جا بزند و حتی یک کانال امن برقرار کند! این سیستم همهٔ اطلاعات ما را با این حیله مشاهده خواهد کرد! در واقع این نوع از فریبکاری فقط به یک روش قابل کشف است، آن هم وجود نفر سومی است که بتواند هویت مکانی را که به آن متصل شده‌ایم، تأیید کند. به همین دلیل در دنیای فناوری، گواهی (Certificate) دیجیتال ایجاد شده است.

گواهی دیجیتال یک سند الکترونیکی است که به‌وسیلهٔ مرجع صدور گواهی دیجیتال که هویت آن برای ما تأیید شده است صادر می‌شود و در اختیار ما قرار می‌گیرد. سیستم ما قبل از فرستادن اطلاعات به مقصد ابتدا گواهی دیجیتال مقصد را با آن مقایسه می‌کند.

برای داشتن گواهی دیجیتال دو روش معمول است:

۱ **گواهی دیجیتال بین‌المللی:** معمولا دارای هزینهٔ زیاد است؛ اما به‌وسیلهٔ تمام سیستم‌های فناوری اطلاعات بین‌المللی قابل استفاده است.

۲ **گواهی دیجیتال داخلی شرکت‌ها یا سازمان‌ها:** هزینه بسیار کمتر است ولی فقط برای محدودهٔ داخلی معتبر است و نیاز به تنظیم سیستم‌های داخلی شرکت یا سازمان مربوط دارد.

پژوهش

با استفاده از منابع اینترنتی و کتابخانه‌ای تحقیق کنید رمزنگاری در جنگ تحمیلی چگونه بوده است. برای این موضوع می‌توانید از مدیریت هنرستان خواهش کنید تا شما را با برگزارکنندگان اردوهای راهیان نور یا افرادی که در جبهه حضور داشته‌اند، مرتبط کنند.

اهمیت ثبت رخدادها در امنیت

داستان سر نخ یک سرقت: در کارخانهٔ ساخت تجهیزات پزشکی گزارش یک سرقت در یک روز تعطیل داده شد. کارآگاه علوی مأمور بررسی موضوع بود. در زمان سرقت فقط یک نگهبان ناشنوای معلول در اتاقکی کوچک مشرف به در ورودی کارخانه حضور داشت. این نگهبان که کسی حتی از حضورش مطلع نبود، تنها وظیفه ثبت مدل و پلاک خودروهای ورودی و خروجی را داشت و اصلاً متوجه اتفاق خاصی نشده

بود، نگهبان اصلی هم ادعا می‌کرد فقط حدود یک ساعت تا رستوران نزدیک کارخانه رفته و برگشته است و از هیچ چیز خبر ندارد. متأسفانه حدود یک کامیون تجهیزات از انبار کارخانه سرقت شده بود. کارآگاه علوی توانست محل اموال سرقتی را کشف کند! به نظر شما سر نخ کارآگاه چه بود؟

بسیاری از برنامه‌ها وقوع اتفاق‌ها و رخدادها را در پرونده‌هایی ثبت می‌کنند. اطلاعاتی مانند زمان و تاریخ اجرا، نام برنامه و جزئیات دیگر به انتهای این پرونده‌ها اضافه می‌شوند و حتی برخی مواقع برنامهٔ کوچک و مستقلی از برنامه‌های اصلی بدون اطلاع آنها این وقایع را ثبت می‌کند. این پرونده‌ها را پروندهٔ ثبت رخداد یا به صورت خلاصه log می‌گویند. در مواقعی که خطا یا مشکلی در سیستم رخ می‌دهد، بررسی رخدادهای ذخیره شده در این پرونده‌ها می‌تواند روشن‌کنندهٔ داستان و حتی سرنخی برای پیدا کردن مشکل و دلیل بروز آن باشند.

فعالیت منزل

با استفاده از اینترنت تحقیق کنید جعبهٔ سیاه هواپیما چیست و چه کاربردی دارد؟

کنجکاوی

علیرضا یک مغازه‌دار باهوش است که یک دوست متخصص فناوری دارد. او از دوستش خواهش کرده است وسیله‌ای طراحی کرده و به گاوصندوق مغازه وصل کند تا در صورتی که درگاوصندوق باز شد پیامکی به تلفن همراه او فرستاده شود. آیا این شیوه می‌تواند نوعی سیستم ثبت رخداد باشد؟

سیستم‌های تشخیص نفوذ

در زمان حمله، عکس‌العمل سریع می‌تواند باعث کاهش قابل‌توجه خسارت شود. اما عکس‌العمل سریع‌تر وقتی ممکن است که بتوانیم وقوع حمله را هر چه زودتر تشخیص دهیم. به سیستم‌های خودکاری که مدیر سیستم را از وقوع یک حمله آگاه می‌کنند، سیستم‌های تشخیص نفوذ (IDS) می‌گویند. سیستم تشخیص نفوذ با مقایسه شرایط عادی و غیرعادی، کاربرش را از احتمال وقوع یک حمله آگاه می‌کند. یکی از روش‌های تشخیص حمله بررسی دائم و خودکار پرونده‌های ثبت رخداد است. اگر بتوان این پرونده‌ها را به صورت لحظه‌ای بررسی و با شرایط عادی مقایسه کرد، ممکن است بتوان از وقوع یک حمله اطلاع پیدا کرد.

علیرضا نیمه‌شب یک پیامک از بازشدن در گاوصندوق دریافت کرده است! این نشانهٔ چیست؟

یک قدم به جلو: به پیشنهاد دوست علیرضا برنامه طوری تنظیم شد که علاوه بر فرستادن پیامک بعد از باز شدن در، اگر در گاو صندوق در خارج از ساعات کاری باز شود، یا بیش از ۲ دقیقه باز بماند، در مغازه به صورت خودکار با یک قفل الکترونیکی بسته شود و تا زمانی که گذرواژهٔ خاصی را وارد نکنند در مغازه باز نشود!

سیستم‌های پیشرفته‌تر می‌توانند بعد از تشخیص حمله، عکس‌العمل مناسبی انجام دهند. سیستمی که بتواند حمله را تشخیص دهد و با عکس‌العمل مناسب جلوی حمله یا ادامهٔ آن را بگیرد، سیستم جلوگیری از نفوذ (IPS) نام دارد.

کنجکاوی

نیمه‌شب پلیس به مغازهٔ علیرضا رفت و سارقان را در هنگام ارتکاب جرم دستگیر کرد. نکتهٔ جالب این بود که سارقان با آنکه متوجه آمدن پلیس شدند، موفق به فرار نشدند! چگونه سرقت مغازه تشخیص داده شد؟ چگونه از سرقت دارایی‌ها و ایجاد خسارت به علیرضا جلوگیری شد و پلیس توانست سارقان را دستگیر کند؟
تاکنون چند بار در طول ساعات کاری در مغازه به صورت خودکار روی خود علیرضا قفل شده است. علت چه بوده است؟

فعالیت منزل

بررسی کنید IDS و IPS مخفف چه واژگانی است؟

دیوار آتش

در زمان‌های دور یکی از مشکلات ساحل‌نشین‌ها حملهٔ غارتگران از دریا به ساحل بود. ساحل‌نشین‌ها برای در امان ماندن از حملهٔ دشمنان از سمت دریا، یک راه‌حل هوشمندانه داشتند. آنها در فاصلهٔ مشخصی از ساحل مشعل‌ها و مواد سوختنی را روی آب شناور می‌کردند و در زمان حملهٔ دشمن آتش می‌زدند! در آن زمان کشتی‌ها چوبی بود و دشمن نمی‌توانست با کشتی‌های چوبی به ساحل نزدیک شود چون کشتی خود آنها آتش می‌گرفت. با این کار گویی دیواری از آتش جلوی ورود دشمن را می‌گرفت. البته در حالت عادی این دیوار برای خروج ماهی‌گیران از ساحل به سمت دریا روشن نمی‌شد و همه چیز عادی بود. فقط وقتی فردی ناشناس می‌خواست از بیرون (دریا) به سمت داخل (ساحل) وارد شود، دیوار آتش فعال شده، جلوی ورود او را می‌گرفت.

کنجکاوی

آیا هنگام خروج از خانه، به کلیدی برای باز کردن درِ خانه از داخل نیاز دارید؟ آیا درِ خانهٔ شما از بیرون نیز به‌راحتی بدون کلید باز می‌شود؟ آیا درِ خانه می‌تواند نوعی دیوار آتش به‌شمار آید؟

روی رایانهٔ شما، روی مودم اینترنت یا هر جای شبکه ممکن است نرم‌افزار کوچکی وجود داشته باشد که اجازهٔ برقراری اتصال از داخل به بیرون را بدهد؛ اما اجازهٔ اتصال از بیرون به داخل را مسدود کند یا فقط با شرایط خاصی اجازهٔ ورود بدهد. به این سرویس، دیوار آتش (FireWall) گفته می‌شود. فایروال‌های امروزی امکانات بیشتری دارند و علاوه بر ورود حتی خروج را بر اساس شرایط مختلف بررسی می‌کنند.

مدیریت خطرپذیری در سیستم

سلام، من مهدی هستم. با کمک شما عضو گروه مسابقات رباتیک شدم و با کار جمعی و تلاش زیاد، گروه ما توانست به عنوان نماینده منطقه برای مسابقات استانی انتخاب شود. ما یاد گرفتیم که برای کارهای بزرگ و جدی باید یک سیاست کاری داشته باشیم تا کارها را منظم کند. همه باید با تقسیم وظایف، کارهای خود را با نظم انجام دهند، در غیر این‌صورت با تلاش نامنظم یک یا دو نفر ممکن است نتیجهٔ مناسبی گرفته نشود. دانا کاپیتان گروه به خاطر انتقال پدرش به یک استان دیگر از مدرسه رفت و از ما جدا شد و من به عنوان کاپیتان گروه انتخاب شدم. هنرآموز، یک روش جالب و درخور توجه به من آموخت و قرار شد فهرست وارسی برای پیش از کار، هنگام انجام کار، و پس از انجام کار تهیه کنم و دیگر دوستان فقط ملزم به رعایت و انجام مراحل داخل فهرست وارسی شوند. با این روش، امنیت کار حفظ می‌شود و امکان اشتباه افراد هم با درج علامت در فهرست وارسی و رعایت همهٔ موارد کاهش می‌یابد. نکته مهم‌تر این است که دیگر آموزش‌های طولانی مدت هم لازم نیست و افراد فرصت دارند به کارهای شخصی خود برسند.

فعالیت کلاسی

- فهرست زیر حداقل وسایل لازم برای سفر به مرکز استان و شرکت در مسابقات است. آن را تکمیل کنید تا افراد گروه چیزی را فراموش نکنند: رایانه قابل حمل، ابزار و وسایل کار ربات، تلفن همراه...
- مزیت‌های استفاده از فهرست وارسی در ایجاد نظم و امنیت را در داستان بالا پیدا کرده، بنویسید.

عوامل ناامنی به نوعی خطر احتمالی به‌شمار می‌آیند. کنترل یا حذف خطرها از اهداف اصلی امنیت فناوری است. به شیوهٔ کنترل یا رفتار در برابر خطرهای احتمالی، مدیریت خطرپذیری گفته می‌شود. در این زمینه، اولین قدم بررسی و تحلیل مخاطرات است. در واقع تفاوت و کیفیت روش کار کارشناسان امنیت به سبب تفاوت تحلیل خطر به‌وسیلهٔ آنها است. کارشناسان امنیت ۶ مرحله برای تحلیل مخاطرات معرفی می‌کنند که باید به ترتیب انجام شود:

۱ تشخیص ارزش یا دارایی
۲ بررسی آسیب‌پذیری ارزش‌ها یا دارایی‌های مشخص شده (خطر احتمالی)
۳ شناسایی عامل فعال‌ساز خطر یا استفاده‌کننده از نقطه ضعف برای ایجاد خطر
۴ بررسی اندازهٔ احتمال عملی شدن تهدید و خطر
۵ تعیین شدت تأثیر و خسارت ناشی از بروز خطر
۶ تدوین عکس‌العمل و رفتار مناسب در برابر خطر

دقت کنید که هر مرحله پیش‌نیاز مرحلهٔ بعد است و باید مراحل به ترتیب انجام شود. معمولاً برای شدت یا احتمال، مقادیر عددی مانند درجه یا درصد و یا کیفیتی مانند کم، متوسط یا زیاد بیان می‌شود. مرحلهٔ آخر یعنی تدوین عکس‌العمل معمولاً شامل یک یا چند رفتار است که در ۵ حالت کلی دسته‌بندی می‌شود. مدیران

سیستم‌ها معمولاً علاقه دارند پررنگ‌ترین حالت را اعلام کنند؛ ولی تقریبا در همهٔ عکس‌العمل‌ها درصدی از ۵ حالت وجود دارد:

- **اجتناب:** کارها یا روش‌هایی مانند دقت و نظارت بیشتر از وسایل در برابر احتمال سرقت که باعث می‌شود احتمال بروز خطر کمتر شود.
- **کاهش تأثیر:** روش‌هایی که در صورت بروز خطر، شدت تأثیر آن را کم‌تر کند. برای مثال پشتیبان‌گیری از اطلاعات می‌تواند اثر خطر آتش‌سوزی برای اطلاعات شرکت را تا حد زیادی کاهش دهد.
- **پذیرش:** مواقعی که جلوگیری از بروز خطر غیرممکن است و بخشی از خسارت با تمام تلاش‌ها غیرقابل اجتناب است و باید به روشی با آن کنار آمد. مانند تسویه و اتمام همکاری با تعدادی از کارکنان برای جلوگیری از ورشکستگی شرکت.
- **انتقال:** انتقال مسئولیت یا جبران خسارت به بخش یا فرد دیگر مانند بیمهٔ آتش‌سوزی یا بیمهٔ سرقت خودرو
- **بازدارندگی:** معمولا با ایجاد رویه‌ها یا ساختارهای فیزیکی یا قانونی، احتمال یا انگیزهٔ فعال شدن عاملان خطرساز را از بین می‌برند. به عنوان نمونه وجود نگهبان یا دوربین مداربسته و موانع سخت و محکم در مقابل سرقت، انگیزه سارق را برای ارتکاب سرقت از بین می‌برد.

فعالیت گروهی

جدول تحلیل خطرپذیری زیر را برای مهدی تکمیل کنید.

ردیف	عنوان دارایی	خطر برای دارایی	عامل فعال‌کننده خطر	احتمال رخ دادن (درصد / سطح)	شدت تأثیر در کار (عدد / کیفیت)	روش مقابله و عکس‌العمل در برابر خطر
۱	رایانهٔ قابل حمل	مفقود شدن، سرقت، فراموش کردن	سارق، حواس پرتی	کم	بالا	دقت و مراقبت بیشتر برای جلوگیری از سرقت
۲	اطلاعات نرم‌افزاری	ویروس، سوختنِ دیسک سخت	حافظهٔ فلشِ آلوده، نوسان برقی	متوسط	بالا	پشتیبان‌گیری از اطلاعات حساس و به‌روز رسانی ویروس‌یاب
۳	آرامش رفاهی افراد گروه	مسمومیت غذایی - بیماری	مواد غذایی آلوده - عدم رعایت بهداشت	زیاد	متوسط	بررسی تاریخ مصرف مواد غذایی و همراه داشتن وسایل بهداشتی
۴	سلامت جسمی افراد گروه	تصادف	صدمات ناشی از خطرات مسافرت جاده‌ای	کم	بالا	بیمه افراد گروه و بررسی بیمه سلامت راننده و معاینه فنی وسیله نقلیه

ردیف	عنوان دارایی	خطر برای دارایی	عامل فعال‌کننده خطر	احتمال رخ دادن (درصد / سطح)	شدت تأثیر در کار(عدد / کیفیت)	روش مقابله و عکس‌العمل در برابر خطر
۵	سرحالی و شادابی اعضای گروه	خواب‌آلودگی	چت در شب پیش از مسابقه تا دیر وقت	بالا	بالا	قانون خاموشی در ساعت ۱۰ شب به بعد
۶						
۷						
۸						

پشتیبان‌گیری

داستان یک اتفاق: حسن در یک شرکت برنامه‌نویسی کار می‌کند. او یک رایانه داشت که تمام پروژه‌های خود را روی آن ذخیره کرده بود و برای جلوگیری از حمله‌های اینترنتی و یا ویروسی شدن، تمام پیش‌بینی‌های لازم را کرده بود. دیشب باد شدیدی وزید. حسن باخبر شد که ساختمان شرکت به دلیل طوفان و اتصال برق دچار آتش‌سوزی شده، تمام تجهیزات شرکت در آتش سوخته است! اکنون با سوختن آن رایانه، اطلاعات، پروژه‌ها و به نوعی سرمایهٔ وی از بین رفته است.

آیا احتمال آتش‌سوزی، سیل یا دیگرحوادث طبیعی می‌تواند یک عامل ناامنی به‌شمار آید؟ آیا می‌توان جلوی حوادث طبیعی را گرفت؟

در برخی موارد پیش‌بینی نشده مانند حوادث طبیعی، ممکن است امکان توقف یا جلوگیری از رخ دادن آن حادثه وجود نداشته باشد. به همین دلیل بهتر است یک نسخهٔ پشتیبان (Backup) از دارایی‌های اطلاعاتی خود تهیه و آن را در جای امن و مناسبی حفظ و نگهداری کرد. به این کار پشتیبان‌گیری می‌گویند. در صورت بروز حادثه و از بین رفتن اصل اطلاعات، می‌توان از نسخهٔ پشتیبان اطلاعات استفاده کرد و اطلاعات را برگرداند. این کار را بازیابی (Restore) می‌نامند.

کنجکاوی

هر چیزی که دارایی‌های اطلاعاتی ما را تهدید کند، عامل ناامنی است و در صورت خسارت در واقع نوعی حمله به ما صورت گرفته است. آیا پشتیبان‌گیری می‌تواند نوعی پیشگیری از حمله یا جلوگیری از خسارت حمله به‌شمار آید؟

انواع روش‌های پشتیبان‌گیری

پروانه مسئول فناوری یک شرکت تبلیغاتی است. به طور متوسط روزی یک گیگابایت به حجم پرونده‌ها و پوشه‌های پروژه‌های مختلف شرکت افزوده می‌شود. پروانه می‌خواهد برای افزایش امنیت، پشتیبان‌گیری را انجام دهد. او می‌تواند به سه روش این کار را انجام دهد:

۱ کامل: هر روز از همهٔ اطلاعات یک بار به صورت کامل پشتیبان بگیرد.

۲ افزایشی: هر روز فقط از تغییرات همان روز پشتیبان بگیرد.

۳ تفاوتی دوره‌ای: در یک دوره زمانی مشخص (هرهفته یا ماه) یک پشتیبان کامل بگیرد و در طول دوره هر روز، از تغییرات از ابتدای همان دوره پشتیبان بگیرد. این روش به نوعی ترکیبی از دو روش قبلی است.

پروانه می‌خواهد بداند کدام روش برای شرایط او بهتر است. برای مقایسه سه عامل: زمان لازم برای گرفتن پشتیبان، حجم پرونده‌های پشتیبان گرفته شده و زمان لازم برای برگرداندن پشتیبان برایش مهم است.

فعالیت گروهی

با دوستان خود در این مورد به بررسی و بحث بپردازید و نتایج را برای کمک به تصمیم‌گیری بهتر پروانه در جدول یادداشت کنید.

روش پشتیبان‌گیری	مزیت‌ها	عیب‌ها
کامل		
افزایشی		
تفاوتی دوره‌ای		

فعالیت منزل

سیستم‌های اعلام سرقت در منازل مسکونی به نوعی سیستم‌های تشخیص حمله به‌شمار می‌آیند. امکانات چند مدل از این سیستم‌های اعلام سرقت را در اینترنت و بازار بررسی کنید و گزارش فعالیت خود را در کلاس ارائه دهید.

فهرست وارسی پیش از حادثه، در زمان حادثه، پس از حادثه

یک کارشناس خبره امنیت دائما باید چرخهٔ ارزیابی، تحلیل و عکس‌العمل به مخاطرات را تکرار کند تا همیشه بتواند در برابر خطرات کمترین آسیب‌پذیری را داشته باشد و به‌روز بماند. اما این سطح از تلاش، تحقیق و کار را نمی‌توان به همه افراد شرکت یا سازمان آموزش داد یا از آنها درخواست کرد که آن را انجام دهند. به همین دلیل معمولاً دستورالعمل‌هایی به‌صورت فهرست وارسی، نمون‌برگ یا راهنمای مراحل انجام کارها برای پیش از اتفاق، زمان اتفاق و پس از اتفاق به‌وسیلهٔ کارشناسان امنیت تهیه شده، افراد موظف به انجام آن می‌شوند. این فهرست‌های وارسی از نتایج حاصل از جدول تحلیل خطرپذیری قابل استخراج هستند.

فعالیت کلاسی

- آیا می‌توان گفت قوانین راهنمایی و رانندگی مثل بستن کمربند برای سرنشین‌های خودرو، نوعی فهرست وارسی تهیه شده به‌وسیلهٔ کارشناسان راهنمایی و رانندگی برای کاهش خطرات در رانندگی است؟ دلیل خود را بنویسید.
- بیمهٔ تصادف رانندگی از کدام دسته از عکس‌العمل‌ها در برابر خطر است؟

اهمیت مستندسازی در امنیت

ما کم سابقه ولی با تجربه‌ایم...

هنرآموز، یک پرونده از مسابقات سال‌های گذشته به من تحویل داد و گفت در یک الی دو روز آینده همهٔ پرونده را مطالعه کنید. این پرونده شامل چند کتاب قطور، عکس، یادداشت، لوح فشرده، خاطرات و مواردی دیگر از مسابقات سال‌های قبل به اضافهٔ نقشه‌ها و طرح‌های ربات بود. ابتدا گفتم موردی برای استفاده در آن نیست ولی اکنون که عکس‌ها و فیلم‌های آن را مشاهده و کتاب‌ها را مطالعه کردم خیلی خوشحال هستم. گویی امروز چند بار در مسابقات مختلف شرکت کردم. جالب است که حتی تجربه و دلیل شکست در چند مسابقه و نقاط قوت و ضعف گروه‌های دیگر که امسال نیز در مسابقه شرکت کرده‌اند، نوشته شده است. چقدر خوب است که گروه‌های قبلی این موارد را ثبت و دسته‌بندی کردند. هنرآموز گفت این کار مستندسازی است و من باید این کار را انجام دهم.

یادداشت

به ثبت و نگه‌داری وقایع و پردازش‌ها در قالب اسناد دسته‌بندی شده، مستندسازی می‌گویند.

مستندسازی می‌تواند شامل تصویر، فیلم یا موارد دیگر هم باشد؛ ولی معمولا نوشته‌ها یا یادداشت‌ها به صورت کتبی یا دیجیتال بیشترین کاربرد را دارند. هرگونه فعالیت یا تغییر در کارها باید مستندسازی شود و برخی اوقات یک اقدام مستند نشده و طبیعتا فراموش شده ممکن است باعث به خطر افتادن کل کار شود.

گزارش رخداد و مدارک

داستان یک اتفاق ساده: ابراهیم مسئول کنترل ورود و خروج یک شرکت طلاسازی است. کارمندان شرکت برای رفت و آمد و استفاده از پارکینگ مخصوص، باید کارت داشته باشند. ابراهیم خودش مسئول ثبت و تحویل کارت‌ها است. امروز صبح ابراهیم متوجه شد کارتش را گم کرده است. او با خودش فکر می‌کند که کارت او چیز مهم و حساسی نیست و به نظر می‌رسد اگر حرفی نزند اتفاق خاصی نمی‌افتد و برای خودش هم یک کارت دیگر برمی‌دارد. از طرفی اگر خبر گم شدن کارتش پخش شود آبروی خودش به عنوان مسئول همین کار می‌رود!

اکنون ابراهیم گم شدن کارتش را به بخش فناوری اطلاع بدهد؟

یکی از مهمترین فعالیت‌های پس از هر اتفاق نوشتن گزارش آن برای مدیر یا مسئول مرتبط در شرکت یا اداره

است. البته کارشناسان با تجربه امنیت فناوری، معمولاً نمون‌برگ‌هایی را تهیه می‌کنند که افراد غیرفنی نیز با پاسخ به گزینه‌ها و پرکردن آن، اطلاعات مهم یک اتفاق را ارائه کنند. این نمون‌برگ‌ها و گزارش‌ها معمولا دارای ۶ بخش زیر هستند:

۱ مشخصات گزارش‌دهنده: معمولاً شامل اطلاعات فردی، آدرس تماس با نویسنده یا تکمیل‌کننده گزارش است.

۲ طبقه‌بندی و فوریت: گزارش‌ها ممکن است حساسیت بالایی داشته باشند و هر چه سریع‌تر باید به‌وسیله مدیر مربوطه بررسی شوند. بعضی اوقات هم ممکن است گزارش یا پیوست‌ها دارای گذرواژه یا اطلاعات مهمی باشند که نباید برای همه پخش شود. در این موارد باید عنوان یا درجهٔ اهمیت یا سطح محرمانگی گزارش حتماً ذکر شود تا مدیر مربوطه بهتر و سریع‌تر بتواند تصمیم بگیرد. معمولاً شرکت‌ها یا سازمان‌ها برای محرمانگی و فوریت، سطح‌هایی مانند محرمانه، سری، فوری، عادی و... را تعریف می‌کنند.

۳ شرح خلاصه اتفاق: در این قسمت باید علائم ظاهری یا موارد مشاهده شده، فارغ از نظر شخصی یا قضاوت نوشته شود. جزئیات زیاد و ریز فنی بهتر است به صورت پیوست گزارش قرار داده شود و از ذکر آن در این قسمت خودداری شود. معمولاً در این شرح باید به صورت خلاصه، سریع و با کمترین کلمات، اتفاق رخ داده را اعلام کرد و دریافت‌کنندهٔ گزارش در صورت نیاز برای جزئیات به پیوست مراجعه کند.

۴ اعلام سطح خسارت: برآورد تقریبی خسارت احتمالی در این بخش اعلام می‌شود. این برآورد برای تصمیم‌های بعدی و سرعت رسیدگی اهمیت دارد.

۵ اعلان راهکار و پیشنهاد برای توقف یا کاهش خسارت

۶ مدارک پیوست: معمولا یک نسخه از پرونده‌های ثبت رخداد، پروندهٔ آلوده به بدافزار، یک نسخه از سیستم مورد حمله یا هر مورد ضروری دیگری، برای بررسی دقیق‌تر به همراه گزارش ارائه می‌شود.

فعالیت کلاسی

ابراهیم به محض اطلاع از مفقود شدن کارت خود می‌خواهد به بخش فناوری این اتفاق را گزارش دهد تا بخش فناوری، کارت قبلی را در فهرست گم‌شده‌ها ثبت کند. گزارش این اتفاق را برای ابراهیم تهیه کنید. مشخصات ابراهیم را به‌صورت فرضی بنویسید.

خطر پنهان کاری در امنیت

هنگامی که یک اتفاق مشکوک کوچک و به‌ظاهر کم‌اهمیت رخ می‌دهد، کارشناس یا کارمند مربوطه ممکن است احساس کند لازم نیست این اتفاق کوچک و کم‌اهمیت را اعلام کند. اما در مواقعی گزارش همان اتفاق ساده و ظاهراً کم ارزش، ممکن است باعث کشف یا جلوگیری از یک خطر بزرگ شود. مخفی‌کاری و پنهان‌کاری از اشتباه‌های بسیار خطرناک کارمندان یک شرکت در امنیت به‌شمار می‌آید و کارمندان در رابطه با محدوده کاری نباید مخفی‌کاری انجام دهند. یکی از دلایل پنهان‌کاری، احساس کم‌اهمیت بودن یک موضوع است. به همین دلیل کارشناس امنیت باید روال منظم و خاصی را ایجاد کند تا کارمندان اتفاق‌های رخ داده را بدون توجه به سطح اهمیت آن به مدیر یا مسئول مربوطه گزارش دهند.

یادداشت

خطر جدی: هر فردی که احساس کند خود یا سیستم تحت مدیریتش دارای ارزش یا اهمیت خاصی نیست، یک فرصت خوب برای نفوذگران به‌شمار می‌آید و ممکن است نفوذگران از طریق سیستم آن فرد که بدون امکانات امنیتی است، دست به حمله اصلی بزنند. این افراد معمولاً اهمیتی به رخدادهای اطراف خود نداده، ناخواسته نوعی پنهان‌کاری را انجام می‌دهند که ممکن است باعث خسارت‌های سنگینی شود.

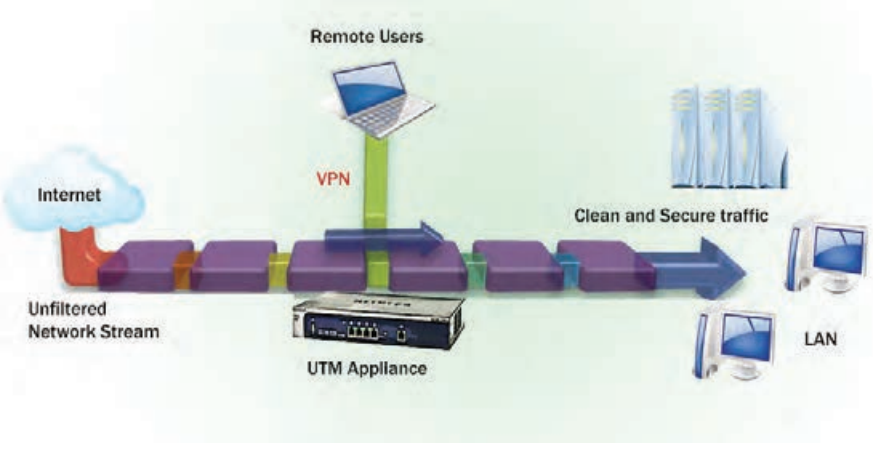
خبر کشف یک سرقت بزرگ از شرکت ساخت طلا و جواهرات: پلیس اعلام کرد یک باند بزرگ سرقت طلا و جواهرات را در همان ابتدای اقدام به سرقت دستگیر کرده است. سارقان قصد داشتند با استفاده از کارت شناسایی یکی از کارکنان که به روشی ماهرانه سرقت کرده بودند، از در اصلی وارد شرکت شوند و سرقت کنند. اما با هوشیاری بخش امنیت فناوری که به ماشین سارقان مشکوک شده بودند، موضوع کشف و در همان دقایق اولیه حمله سارقان ناکام ماند.

کنجکاوی

آیا مفقود شدن کارت ورود و خروج ابراهیم اتفاقی بوده است؟ آیا بین کارت گم شده و مشکوک شدن بخش حراست شرکت به خودروی سارقان در بدو ورود به پارکینگ ارتباطی است؟ حدس خود را بنویسید.

مدیریت یکپارچه تهدیدها (UTM)

هماهنگی و سیاست‌گذاری متمرکز در حفظ امنیت یکی از روش‌های مدیریتی است. به همین دلیل معمولاً امکانات سخت‌افزاری و نرم‌افزاری ساخته شده در قالب استانداردهای مشخصی می‌توانند به یکدیگر متصل شده، یک سیستم یکپارچه را تشکیل دهند که به سیستم مدیریت یکپارچه تهدیدها (Unified Threat Management) معروف است. شرکت‌های مختلف سعی کرده‌اند سیستمی تولید کنند که بتواند تمام این امکانات را به صورت یکپارچه و متمرکز به‌کار بگیرد. حتی بعضی از تولیدکنندگان، تمام امکانات امنیتی مورد نظر را در قالب یک دستگاه تولید کرده‌اند. سیستم‌های مدیریت یکپارچه تهدید معمولاً دارای دیوار آتش، سیستم تشخیص و توقف حمله، تحلیل‌گر محتویات، آنتی‌ویروس و موارد مشابه هستند و مزیت آنها مدیریت متمرکز برای افزایش امنیت است. در مقابل، عیب این سیستم‌ها این است که اگر به هر دلیل، سیستم اصلی دچار مشکل شود بلافاصله تمام بخش‌های دیگر و کل کار متوقف می‌شود.



فعالیت کلاسی

نقطه تجمع، نقطه‌ای است که در مواردی مانند آتش‌سوزی یا اتفاقات مشابه، دیگر کارکنان یا اعضای آن مجموعه باید هر چه سریع‌تر در آن نقطه جمع شوند تا بتوانند مدیریت پس از حادثه را بهتر انجام دهند. این نقطه معمولاً در فضای امن روباز، دور از احتمال تخریب یا ریزش و دور از مواد آتش‌زا یا مضر است.

- بررسی کنید نقطه تجمع مدرسه شما کجا تعیین شده است. آیا تابلو و علامتی در آن نقطه نصب شده است؟

- به عنوان اقدام پیش از حادثه، یک راهنما با کروکی نقطه تجمع مدرسه و مسیرهای امن برای رسیدن به آن را با معرفی مختصر مکان آماده کنید و به هنرآموز تحویل دهید.

پدافند غیرعامل

برای هر کشوری در دنیا، حفظ امنیت و تمامیت ارضی، جانی و مالی مردم بسیار بااهمیت است. مدل امنیت کشورها در واقع مدل بزرگی است که از تعداد زیادی زیربخش تشکیل شده است. بخش‌هایی مثل امنیت غذایی، بهداشت، آموزش، فرهنگ و موارد مشابه دیگر که از جهت حفظ امنیت دارای ابعاد بسیار متنوعی است. بعضی مواقع حوادث یا اتفاق‌هایی رخ می‌دهد که نتایج و اثرات آن مانند خسارت یک حمله نظامی است. به همین دلیل امنیت یک کشور علاوه بر نیروی نظامی به تمام بخش‌های دیگر نیز وابسته است.

مثال: فرض کنید برق تمام شهر برای یک روز قطع شود، در آن صورت سردخانه‌ها، مغازه‌ها، رایانه‌ها و هزاران بخش دیگر از کار می‌افتند. در چنین شرایطی خسارت و ناامنی ایجاد شده از این اتفاق تا حدی ممکن است شبیه به خسارت یک حمله نظامی باشد! پس فعالیت‌ها و اقدامات لازم برای اینکه در چنین شرایطی بتوان برق شهر را از روش‌های دیگر دوباره وصل کرد، به نوعی دفاع در برابر چیزی شبیه به یک حمله است، اگر چه اصلاً موضوع نظامی نیست!

در این مثال، ممکن است به روش غیرنظامی خسارتی به کشور ما وارد شود که به اندازهٔ خسارت نظامی باشد! در واقع بحث از دفاع بدون سلاح است. به این اقدام‌ها پدافند غیرعامل می‌گویند. به عبارت دقیق‌تر و کامل‌تر پدافند غیر عامل عبارت است از:

مجموعه اقدامات غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدام‌های دشمن می‌شود.

تقریباً تمام صنایع، نیروگاه‌ها و بخش‌های مهم به‌وسیلهٔ شبکه‌های رایانه‌ای اداره می‌شوند؛ بنابراین امنیت فناوری در این امور بسیار مهم است و تمام اقدامات کارشناسان امنیت فناوری به نوعی در زیرمجموعهٔ پدافند غیرعامل قرار می‌گیرد.

مهارت‌های مورد نیاز برای امنیت فناوری و شبکه

انجام هر کاری مهارت خاص خود را نیاز دارد. برای شغل‌های مرتبط با امنیت فناوری و شبکه نیز حداقل مهارت‌هایی مورد نیاز است که در ادامه به صورت

مختصر معرفی می‌کنیم:

۱ **توانایی کار با سیستم‌عامل لینوکس:** همه برنامه‌های اجرایی روی سیستم‌عامل اجرا می‌شوند. شناخت، آگاهی و یا حتی دستکاری برنامه‌ها و خود سیستم‌عامل برای یک کارشناس امنیت فناوری بسیار ضروری است. به همین دلیل آشنایی با دنیای متن‌باز (Open Source) و به‌خصوص مهارت در استفاده از سیستم‌عامل لینوکس که کد برنامه‌نویسی آن برای همه در دسترس است، از ضرورت‌های کاری کارشناس امنیت فناوری است.

۲ **مهارت در یک زبان برنامه‌نویسی بر پایهٔ زبان C:** سیستم‌عامل‌ها و اکثر برنامه‌ها با زبان‌هایی نوشته شده‌اند که بسیار شبیه به زبان C هستند. مانند سی‌شارپ، جاوا، پایتون، PHP و بسیاری دیگر. دانستن حداقل یکی از این زبان‌ها برای کارشناس امنیت فناوری ضروری است.

۳ **آشنایی با یک پایگاه داده:** در دنیای امروز اطلاعات، ثروت واقعی است و محل تجمیع و ذخیره داده‌ها یا پایگاه داده بسیار با ارزش است. دانستن شیوهٔ کار و استفاده از حداقل یک پایگاه دادهٔ ترجیحاً متن باز بسیار ضروری است.

علاوه بر موارد گفته شده یک کارشناس امنیت شبکه همیشه باید در حال مطالعه و تحقیق باشد. معمولاً برای آموزش ابزارهای اختصاصی و تست امنیت، دوره‌هایی در دانشگاه‌ها یا مراکز علمی برگزار می‌شود و مدارک معتبر نیز برای درج در رزومهٔ کاری به فراگیر داده می‌شود. آموزش‌ها در دو دسته کلی هستند:

- **دوره‌های رسمی دانشگاهی:** دانشگاه‌های معتبر در موضوع امنیت فناوری اطلاعات و شبکه، دارای رشته‌های تحصیلی رسمی هستند. ورود به این رشته‌ها معمولاً با آزمون‌های ورودی و با داشتن مدارک تحصیلی ممکن است.
- **دوره‌های آزاد:** دوره‌های آزاد غیررسمی در همهٔ دانشگاه‌های معتبر یا مجتمع‌های آموزشی وجود دارد که برای ورود، نیاز به مدرک یا آزمون خاصی ندارند و شرکت در آنها برای عموم علاقه‌مند به امنیت آزاد است.

فعالیت کلاسی

- فرض کنید صبح وارد اتاق کاری خود شده و متوجه شدید که دیسک‌سخت رایانه شما سوخته است. یک گزارش از این واقعه برای مدیر شرکت بنویسید.
- با جست‌وجو در اینترنت و تارنماهای مرتبط با پدافند غیرعامل، یک اقدام پدافند غیرعامل را که در یکی از سازمان‌ها، ادارات یا شرکت‌های ایرانی انجام شده است یافته، خلاصه‌ای از آن را به هنرآموز تحویل دهید.

پژوهش

در رابطه با محتوای دوره‌های آموزشی زیر و شیوه کسب مدارک آن تحقیق کنید.

Security+

CEH - Certified Ethical Hacker

CISSP - Certified Information Systems Security Professional

جدول ارزشیابی پایانی

ارزشیابی پیشرفت تحصیلی مبتنی بر شایستگی درس دانش فنی تخصصی					
عنوان پودمان	تکالیف عملکردی (واحدهای یادگیری)	استاندارد عملکرد	نتایج مورد انتظار	شاخص تحقق	نمره
تحلیل امنیت در فاوا	۱-تحلیل ناامنی و راهکارهای مقابله با آن ۲-تحلیل حمله و امن سازی	تحلیل عوامل ناامنی و حمله و ارائه راهکارهای مقابله با آنها برای کاهش تهدیدهای مبتنی بر فناوری	بالاتر ازحد انتظار	- تعیین نقاط آسیب‌پذیر در یک کاربرد خاص و ارائه راهکارهای مناسب جهت اجتناب از حملات - ارائه یک طرح رمزنگاری برای ذخیره و تبادل اطلاعات در طراحی یک تارنمای فرضی - ارائه فهرست اطلاعات ضروری در یک سیستم ثبت رخداد فرضی جهت یک کاربرد خاص - انتخاب بهترین گزینه میان چند سخت‌افزار مدیریت یکپارچه تهدیدها - ارائه راهکار برای افزایش توان پدافند غیرعامل در یک کاربرد خاص درحوزه فاوا	۳
			درحد انتظار	- تعیین اجزا مثلث امنیت برای یک کاربرد خاص - تعیین و دسته‌بندی دارایی‌های یک حوزه کاری و پیشنهاد سطح دسترسی به دارایی‌ها - انتخاب رمزنگاری موردنیاز (یک طرفه یا دو طرفه) در یک کاربرد خاص - تعیین نوع بدافزار امنیتی و طرح یک سیستم تشخیص یا جلوگیری از حمله برای یک کاربرد خاص - ارائه راهکار بهینه پشتیبان‌گیری برای یک کاربرد خاص - تهیه گزارش نقض امنیت رخ داده - ارائه یک نمونه از پدافند غیرعامل	۲
			پایین‌تر از حدانتظار	- تعیین عوامل ناامنی برای یک سیستم مشخص - دسته‌بندی انواع رمزنگاری - معرفی فایل ثبت رخداد و دیوار آتش	۱
نمره مستمر از ۵					
نمره واحد یادگیری از ۳					
نمره واحد یادگیری از ۲۰					