محتوای دوره آموزشی

شبکه و امنیت اطلاعات در سازمان‌ها

مدت دوره: ۸ ساعت

عناوین این بخش:

- آشنایی با فضای سایبری
- آشنایی با جرایم رایانه‌ای و پلیس فتا
- امنیت، حفاظت و نگهداری از اطلاعات
- آشنایی با انواع تهدیدات سایبری

فصل اول

آشنایی با فضای سایبری

- ❑ **در این فصل، با مفاهیم زیر آشنا خواهیم شد:**
  - ✓ **مفهوم فضای سایبری**
  - ✓ **ویژگی های فضای سایبر**
  - ✓ **مقایسه فضای سایبر و فضای واقعی**
  - ✓ **آسیب‌های ناشی از فضای سایبر**

پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های ارتباطی در هر کشور، مستلزم توجه تمامی کاربران، صرف نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات بوده و باید به این مقوله در سطح کلان، نگاه شود.

وجود تهدیدات امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمام کاربران، صرف نظر از موقعیت شغلی آنان، نسبت به جایگاه و اهمیت اطلاعات، همچنین عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی و مواردی از این قبیل، مسائلی را به دنبال خواهد داشت که ضرر آن، متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد.

در این بخش از کتاب قصد داریم مفاهیمی را از دنیای امنیت اطلاعات (*Information Security*) بیاموزیم.

فضای سایبری چیست؟

فضای سایبر را به دو صورت تعریف کرده‌اند:

- محیط الکترونیکی مشتمل بر ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی

- محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی، با ابزارهای خاص بصورت زنده و مستقیم، انجام می‌گیرد.

مجازی بودن این فضا به معنای غیر واقعی بودن آن نیست. در این فضا همان ویژگی‌های تعاملات انسانی در دنیای خارج وجود دارد. فضای سایبر، یک محیط است که در آن، ارتباطاتی انجام می‌شود. در بعضی جاها، فضای سایبر را به مجموعه‌ای از ارتباطات محدود می‌کنند در حالی که ارتباطات، در یک محیط انجام می‌شود. همچنین، در تعریف فضای سایبر گفتیم که ارتباطات به صورت زنده و مستقیم انجام می‌شود. ممکن است این ارتباطات به صورت آنلاین (از طریق اینترنت) نباشد، اما ویژگی بارز آن این است که به صورت زنده، واقعی و مستقیم انجام می‌شود و به همین دلیل، تاثیرات متقابل روابطی که در فضای سایبری انجام می‌شود، بسیار بالاست.

ویژگی‌های فضای سایبر

۱- جهانی بودن

می‌توان اولین ویژگی فضای سایبر را جهانی بودن آن در نظر گرفت. هر فردی از هر نقطه جهان، می‌تواند از طریق فضای منحصر بفرد سایبر، به آسانی به جدیدترین اطلاعات دسترسی داشته باشد. مرزهای جغرافیایی تا کنون نتوانسته‌اند از گسترش روزافزون فضای سایبر، جلوگیری کنند. در نتیجه، هر نوع فیلتر و مرزبندی در فضای سایبر، بسیار دشوار خواهد بود.

۲- آزادی اطلاعات و ارتباطات

دومین ویژگی فضای سایبر را می‌توان آزادی اطلاعاتی حاکم بر این فضا دانست. در واقع، معنای واقعی آزادی اطلاعات در فضای سایبر محقق شده است. در نتیجه هر نوع اطلاعاتی از جمله فرهنگی، سیاسی، اقتصادی و غیره، بدون محدودیت‌های موجود در رسانه‌های دیگر، در فضای سایبر قابل دسترسی است.

۳- دستیابی آسان به آخرین اطلاعات

از دیگر ویژگی‌های فضای سایبر، آزادی ارتباطی است. مسلماً آزادی ارتباطی به شکلی که در فضای سایبر، امکان‌پذیر شده است، در هیچ یک از رسانه‌های ارتباطی دیگر، عملی و ممکن نخواهد بود.

۴- جذابیت و تنوع

کاربرد فیلم، عکس، متن و یا هر نوع از قطعات هنری دیگر، توانسته است برتری فضای سایبری را در زمینه تنوع و جذابیت، در رقابت با رسانه‌های ارتباطی دیگر، امکان‌پذیر نماید.

۵- تعاملی بودن

تعامل رسانه‌ای در فضای سایبر به گونه‌ایست که کاربران می‌توانند با ارسال پیام با یکدیگر ارتباط برقرار کنند. در یک ارتباط تعاملی، نقش گیرنده یا فرستنده معنای خود را از دست داده و چرخه ارتباط، از سوی تمام مشارکت کنندگان در ارتباط، تداوم پیدا می‌کند. سیستم نظرگذاری موجود در وبلاگها می‌تواند نمونه‌ای از یک ارتباط تعاملی باشد.

۶- واقعی بودن

فضای سایبر، یک واقعیت است و مجازی (*Virtual*) نیست. فضای سایبر، واقعیتیست که ماهیت آن به لحاظ شکلی با جهان پیرامون ما متفاوت است. به عنوان مثال، گفتگوی دو نفر هنگام چت (گپ‌زنی)، به همان میزانی واقعیست که گفتگو بین دو نفر در کلاس درس واقعی. بنابراین، اصل گفتگو در بین هر دو روش ارتباطی، مشترک است و جریان دارد و تفاوت، تنها در روش برقراری ارتباط است.

۷- دیجیتالی بودن

به لحاظ لغوی، دیجیتال به مفهوم بازنمایی اطلاعات بعنوان عدد است. دیجیتالی بودن یعنی منطق ریاضی داشتن، صفر و یکی بودن اطلاعات. ویژگی دیجیتالی بودن فضای سایبر، باعث از بین رفتن فاصله‌های مکانی و زمانی است. مثلاً مکالمه صوتی یا تصویری با دوستی که در خارج از کشور ساکن است، یا استفاده از مقالات و کتاب‌های دانشمندان بزرگ دنیا که هیچوقت آن‌ها را از نزدیک ملاقات نکرده‌ایم، از فرصت‌هایی است که ویژگی دیجیتالی بودن فضای سایبری در اختیار ما قرار می‌دهد.

۸- حافظه طولانی مدت فضای سایبر

در فضای سایبر، تمام اموری که از طریق داده‌ها به سیستم وارد می‌شوند، نگهداری می‌شود. لذا دسترسی به داده‌های مرتبط با گذشته‌های دور، امکان‌پذیر خواهد بود.

اگر حافظه سایبر را در برابر حافظه فیزیکی قرار دهیم، به راحتی می‌توانیم تفاوت آن‌ها را دریابیم. انسان ذاتاً فراموشکار است و به همین دلیل در حافظه فیزیکی، امکان فراموشی وجود دارد. اما در حافظه فضای سایبر، هیچ چیز فراموش نمی‌شود، حافظه، متعلق به فرد خاصی نیست تا فراموش شود. مثلاً هر

فردی با مراجعه به آرشیوهای موجود در وب‌سایت‌ها و وبلاگ‌ها، به اطلاعات موجود در آن‌ها دسترسی پیدا کند.

۹- فرامتنی یا *Hypertext* بودن

قبل از صحبت در مورد فرامتنی بودن فضای سایبر، باید مفهوم فرامتن یا *Hypertext* را بدانیم. یک فرامتن (*Hypertext*)، متنی است که با سایر متون خارج از فضای متن، ارتباط برقرار می‌کند. در واقع، به ارتباط یک متن با فضای خارج از خودش، *Hypertext* بودن متن گفته می‌شود. *Hypertext* بودن فضای سایبر، امکان دسترسی به اشکال مختلف متن را از طریق متن فراهم می‌کند.

مقایسه فضای سایبری و فضای واقعی

می‌توان مقایسه‌های زیر را بین فضای واقعی و فضای سایبری انجام داد:

- در فضای واقعی، بعد جغرافیایی، معنا دارد ولی فضای سایبری فاقد بعد است.
- در فضاهای واقعی، نوعی نظام‌مند بودن وجود دارد، در حالی که فضای سایبری فاقد هر گونه نظام خاصی است.
- فضای واقعی، محدود است در حالی که فضای سایبری، در فضا و مکان محدود نمی‌شود.
- فضای واقعی، طبیعی است، در حالی که فضای سایبری، غیر طبیعی است.
- فضای واقعی، قابل تکثیر نیست (دو دنیا در کنار هم نمی‌توان داشت) ولی فضای سایبری، قابل تکثیر است.
- هم فضای واقعی و هم فضای سایبری، قابل دسترسی است. در فصل بعد راجع به دردسترس بودن صحبت می‌کنیم که یکی از المان‌های امنیتی اطلاعات است.
- در فضای واقعی، خواننده می‌تواند با خواندن یک متن، تصوری راجع به نویسنده پیدا می‌کند، اما در فضای سایبری، هویت هر اطلاعاتی که وجود دارد، همان چیزی نیست که تصور می‌شود.
- در فضای واقعی، اجسام، غیر قابل شبیه‌سازی هستند. اما در فضای سایبری می‌توان تمام اشکال را شبیه‌سازی کرد.

آسیب‌های ناشی از فضای سایبر

یکی از پیامدهای پیدایش کامپیوترها و اینترنت، مخاطراتی است که در جای جای قلمروی گسترده این فن‌آوری در کمین است. در صورتی که این پیامدها مورد بی‌توجهی جامعه و دولت قرار بگیرد، مخاطرات آن می‌تواند بسیار بزرگ و پر رنگ شده و لطمات جبران‌ناپذیری را به بدنه جامعه وارد آورد.

آسیب‌های روانی ناشی از کاربری نادرست و خلاف قانون، می‌تواند موجب اختلال در رفتار شهروندان شده و جامعه را در رسیدن به فواید این فن‌آوری، ناکام کند.

این اختلالات، باعث فرسودگی و ناتوانی شهروندان شده و می‌تواند فعالیت روزمره آنان را دچار اختلال کند. آسیب‌های فرهنگی و اجتماعی فضای سایبر، اعضای جامعه را از لحاظ رفتار فردی با خانواده و رفتار اجتماعی با شهروندان جامعه، متزلزل خواهد کرد. با وجود چنین مخاطراتی، قاعدتاً هنجارها و ارزشهای جامعه از بین رفته و احساس امنیت و آرامش در جامعه، کمرنگ خواهد شد.

در این مبحث، راه‌کارهای فرار از آسیب‌ها و پیشگیری از آسیب‌های ناشی از فضای سایبری را مورد بررسی قرار خواهیم داد. آسیب‌های ناشی از فضای سایبر به دو دسته تقسیم می‌شود:

- آسیب‌های فرهنگی فضای سایبر
- آسیب‌های روانی فضای سایبر

آسیب‌های فرهنگی فضای سایبر

۱- کم‌رنگ شدن ارزش‌های مترقی در جامعه

می‌دانیم که هر جامعه‌ای دارای ارزشهایی است که ناشی از فرهنگ همان جامعه است. برخی از ارزشهای مترقی در جوامع اسلامی، به موجب تأثیر گرفتن از فرهنگ غربی، در حال کمرنگ شدن است. ارزش‌هایی مثل حیا و عفت، ارجحیت شخصیت افراد به جنسیت آن‌ها و غیره، در حال کم‌رنگ شدن هستند و قبح برخی اعمال خلاف، از بین رفته و این اعمال، جایگزین اعمالی می‌شوند که در جامعه ارزش تلقی می‌شوند.

۲- تضعیف فرهنگ‌های کم‌حضور

یکی از ویژگی‌های فضای سایبر این است که به شدت تحت تأثیر عرضه‌های گسترده قرار می‌گیرد. این فضا می‌تواند گذرگاه فرهنگ‌های گوناگونی باشد که قصد عرضه خود به شکل‌های گوناگون را دارند. تنها فرهنگی می‌تواند پیشتاز باشد که حضور گسترده‌تری در فضای سایبر داشته باشد. از این جهت، فرهنگ قالب، فرهنگی جز فرهنگ قدرتمند و منحط غربی نیست. این فرهنگ با بهره‌مندی از امکانات وسیع کشورهای غربی توانسته است خود را به عنوان فرهنگ قالب، به جوامع دیگر، تحمیل کند.

به طور متوسط می‌توان گفت که توسعه وب، که یکی از مهمترین ابزارهای عرضه فرهنگ است، هر سه ماه یک بار، دو برابر می‌شود که این رشد روزافزون، به نفع فرهنگ غربی خواهد بود. چرا که در فضای سایبری، پررنگ‌ترین حضور، از آن فرهنگ غربی است.

طبق آمار، آمریکا و کانادا ۶۳ درصد از کامپیوترهای متصل به اینترنت در جهان را به خود اختصاص داده‌اند. اروپا ۴/۲۲ درصد و استرالیا و ژاپن و نیوزیلند، ۶/۴ درصد و بقیه کشورهای آسیایی و آفریقایی، فقط حدود ۵/۹ درصد از این آمار را به خود اختصاص می‌دهند. آمار استفاده از اینترنت، امروز افزایش پیدا کرده و سلطه فرهنگ غرب در جای جای فضای سایبر، سایه انداخته است.

زبان انگلیسی در فضای سایبر، گسترده‌ترین پوشش را به خود اختصاص می‌دهد. کاربران با حضور در فضای سایبر، ضمن درگیر شدن با زبان انگلیسی حاکم بر این فضا، رفته رفته از زبان بومی و ملی خود دور می‌شوند. به عنوان مثال، در چت‌های اینترنتی فارسی زبانان، افراد تمایل به استفاده از الفبای انگلیسی به جای الفبای فارسی دارند. مسلماً گسترش این کاربرد، موجب تضعیف الفبای زبان فارسی خواهد شد.

۳- تضعیف اعتقادات و شبهات فکری

دستیابی آسان به اطلاعات، یکی از ویژگی‌های فضای سایبر، ذکر شد. اما دسترسی آسان به اطلاعات، معایبی نیز دربردارد. ازجمله این که طراحی و نشر شبهات در فضای سایبر، به راحتی قابل انجام بوده و باعث از هم پاشیدگی کاربران سست عقیده و کم اعتقاد خواهد شد. فضای سایبری را می‌توان یک چاقوی دو لبه در نظر گرفت که باید به نفع خود از آن سود جست. اما تنوع و گسترش فرهنگ غربی، به حدی است که در شرایط فعلی، کوشش‌های فرهنگ‌های بومی بسیار کم اثر است و به راحتی می‌توانند با ایجاد شبهات فکری، به اعتقادات افراد لطمه وارد کنند.

۴- رواج سطحی نگری فکری

آزادی بیان و طرح اندیشه‌های متضاد در فضای سایبری از اهداف اولیه ایجاد این فضا بوده است. اما در صورتی که یک اندیشه و تفکر، بدون هیچ بنیاد و اساس معتبری مطرح شده و گسترش پیدا کرده کند، ثمره آن، این خواهد بود که اندیشه‌های بسیاری روی هم انباشته خواهد شد که توان بررسی و نقد و تحلیل این اندیشه‌های متفاوت و متضاد، از عهده مخاطبان این فضا خارج خواهد شد. بنابراین، روحیه حق پذیری کاربران، به ویژه جوانان و افراد کم تجربه به سطحی نگری و مسامحه کاری در پذیرش اندیشه‌های نوظهور، تبدیل خواهد شد.

۵- ایجاد سردرگمی

وقتی می‌خواهیم کودکی را آموزش دهیم، ابتدا مفاهیم ابتدایی و سپس مطالب پیچیده‌تر را به او آموزش می‌دهیم. طرح مفاهیم متنوع و تفکرات متضاد و متناقض برای کودک، میوه‌ای جز تحیر و تعجب کودک نخواهد داشت و او قادر به درک دنیایی از اندیشه‌های متفاوت و متضاد نخواهد بود. اگرچه فضای سایبر، مولد آزادی بیان است، ولی این آزادی بیان باعث انباشتن اندیشه‌های خوب و بد و

در نتیجه، سخت‌تر شدن گزینش اطلاعات صحیح شده و نامحدود بودن حجم اطلاعات و طبقه‌بندی نشده بودن اطلاعات خوب و بد، منجر به سردرگمی افرادی خواهد شد که در تحلیل تفکرات موجود در فضای سایبر، دچار ضعف هستند.

۶- به خطر افتادن حقوق مادی و معنوی مؤلفین

با توجه به گسترش روزافزون سرقت اطلاعات و نرم افزارهای مختلف، نگرانی مؤلفان در خصوص حقوق مادی و معنویشان بیشتر خواهد شد. زیرا با توجه به قدرتمند شدن ابزارهایی مثل قفل‌شکن‌ها و نبود نظارت لازم در فضای سایبر، مؤلفانی که می‌خواهند از اثر خود بهره‌مند شوند، از ارائه آثارشان به صورت الکترونیکی، خودداری خواهند کرد.

۷- گسترش محصولات فرهنگی غربی

عمده محصولات فرهنگی، مثل فیلم، عکس، متن، بازی‌های کامپیوتری، بازی‌های اینترنتی و غیره از سوی کشورهای غربی و شرقی تولید و در فضای سایبر، پخش می‌شوند. در نتیجه، یکی از خطرات ناشی از فضای سایبر، متوجه کشورهایی است که دارای فرهنگ متضاد با فرهنگ‌های حاکم بر فضای سایبر است. جامعه ما که ارزش‌های آن متضاد با فرهنگ غربی است، می‌تواند هدف تهاجم فرهنگی غرب واقع شود.

آسیب‌های روانی فضای سایبر

۱- افسردگی و گوشه‌گیری

کاربران اینترنت، معمولاً ترجیح می‌دهند در محیطی آرام و خلوت از اینترنت استفاده کنند تا هم بهتر بتوانند از اطلاعات خود بهره‌مند شوند و هم در مدت زمان کمتری از این اطلاعات بهره‌مند شوند تا هزینه‌های کمتری را متحمل شوند. اما این نوع خلوت و گوشه‌گیری، در طولانی مدت می‌تواند مشکلاتی مثل افسردگی را به دنبال داشته باشد.

بسیاری از روان‌شناسان این نگرانی را داشته‌اند که آسان بودن ارتباطات اینترنتی، افراد را مجبور می‌کند که زمان بیشتری را به تنهایی به صورت آنلاین با افراد غریبه صحبت کنند. این ارتباطات سطحی، به غیمت از دست دادن گفتگوها و ارتباطات دوستانه رو در رو با فامیل و دوستان منجر شده و در درازمدت به گوشه‌گیری اجتماعی فرد منجر خواهد شد.

۲- بازداری زدایی

همه می‌دانیم که کاربران فضای سایبر، گمنام و نامرعی هستند و این نامرعی بودن روابط اینترنتی، منجر به پیدایش آسیب‌های روانی اخلاقی و روانی در افراد خواهد شد. اشخاص می‌توانند به صورت ناشناس، هر مطلبی را مطرح کرده و بدون ترس از شناخته شدن و لو رفتن، نقاب‌های مختلفی را روی

صورت خود قرار دهند. این ویژگی باعث کاهش پیدا کردن خویشتن‌داری و بازدارندگی بین کاربران شده به طوری که هر کسی، بدون دلهره از نتایج عملکرد خود بتواند کارهای ناهنجاری را در فضای سایبری انجام دهد.

۳- بحران هویت و اخلال در شکل‌گیری شخصیت

فضای سایبر، یک فضای فرهنگی و اجتماعی است که فرد می‌تواند خود را در نقش‌ها، موقعیت‌ها و سبک‌های زندگی مختلف نمایش دهد. این ویژگی، زمینه‌ساز آسیب‌پذیری شخصیت کاربران فضای سایبر خواهد شد و در نتیجه، کاربر به سمت چند شخصیتی شدن پیش خواهد رفت. در فضای سایبر، فرد می‌تواند هویت واقعی خود را پنهان کرده و در هر فضایی و هر مجلسی، هویت جعلی و غیر واقعی خود را بروز دهد.

اینکه هویت اصلی شخص در همه محل‌ها مطرح نمی‌شود، منجر به شکل‌گیری شخصیت‌های چندگانه در فرد می‌شود. به عنوان مثال، در چت روم‌ها یک فرد می‌تواند خود را فرد متفاوتی نمایش دهد. می‌تواند سن، محل سکونت و تحصیلات غیر واقعی را به دیگران بروز دهد و این باعث می‌شود شخصیت‌های مختلفی در شخص، شکل بگیرد و این در باور شخص، تثبیت شده و این شرایط، آسیب‌های جدی را برای فرد و جامعه به همراه دارد.

۴- اعتیاد مجازی

اعتیاد مجازی، یعنی استفاده بیش از حد از اینترنت، به طوری که بدون استفاده از اینترنت، احساس کمبود در فرد ایجاد شود. به عنوان عواملی که باعث ایجاد اعتیاد به اینترنت و فضای سایبر در افراد می‌شود می‌توان به نبود روابط صمیمی و پایدار با دیگران، نداشتن اعتماد به نفس، شکست خوردن و عدم موفقیت در عرصه‌های زندگی و غیره اشاره نمود.

طبق پژوهش‌های یانگ در زمینه اعتیاد مجازی، یکی از دلایل مهم اعتیاد مجازی در افرادی که روابط عمومی کمتری دارند، به دست آوردن حمایت‌های اجتماعی است.

این مورد، در کشورهایی که استفاده از اینترنت، آسان و ارزان است، بسیار چالش زا بوده و بسیاری از نهادهای دولتی را برای حل این مشکل، درگیر کرده است. در کشوری مثل آمریکا، تعداد معتادان به اینترنت، از معتادان دیگر بیشتر است به طوری که بعضی از آنان، روزانه ۱۸ ساعت از وقت خود را در اینترنت سپری کرده‌اند. قاعدتاً اعتیاد مجازی، نتایج و پیامدهای زیان‌بخشی را برای فرد در پی داشته و آسیب‌های روانی، خانوادگی و اجتماعی بسیاری را برای آنان در پی داشته است.

فصل دوم

آشنایی با جرایم رایانه‌ای و پلیس فتا

- ❑ **در این فصل، با مفاهیم زیر آشنا خواهیم شد:**
  - ✓ **مفهوم جرایم رایانه‌ای**
  - ✓ **پلیس فتا (پلیس فضای تبادل اطلاعات)**
  - ✓ **ضرورت تشکیل پلیس فتا**
  - ✓ **اهداف و وظایف پلیس فتا**

جرایم رایانه‌ای

قبل از پرداختن به پلیس فتا به مفهوم و تعریف جرایم رایانه‌ای می‌پردازیم. در واقع جرایم رایانه‌ای، همزمان با توسعه و کاربردپذیری رایانه‌ها و سیستم‌های رایانه‌ای به وجود آمده‌اند. از اواخر دهه ۶۰ میلادی تا امروز، می‌توانیم جرایم رایانه‌ای را به ۳ نسل طبقه‌بندی کنیم.

نسل اول جرایم رایانه‌ای به سال‌های دهه ۷۰ و اوایل دهه ۸۰ میلادی باز می‌گردد. در آن زمان، به دلیل شایع نبودن استفاده از اینترنت، عمده جرایم رایانه‌ای به کاربرد خود رایانه‌ها مربوط می‌شود. به همین دلیل، به نسل اول، نسل جرایم رایانه‌ای هم گفته می‌شود.

نسل دوم جرایم رایانه‌ای به اوایل دهه ۸۰ تا اوایل دهه ۹۰ میلادی بازمی‌گردد. در این نسل، داده‌ها بیشتر مورد تمرکز جرایم قرار گرفتند نه کامپیوترها. در واقع، صرف‌نظر از این‌که داده‌ها در رایانه‌ها قرار داشته باشند یا در واسطها و یا ابزارهای انتقال یا شبکه‌ها، وجود خود داده مورد توجه قرار می‌گرفت. در این نسل، تأکیدی بر خود کامپیوترها نبود و به همین دلیل، به این نسل، نسل جرایم علیه داده‌ها نیز می‌گویند.

اما نسل سوم جرایم رایانه‌ای که همزمان با فراگیرشدن اینترنت، به وجود آمد، در اوایل سال‌های دهه ۹۰ میلادی آغاز شد. در واقع جرایم در این نسل با گسترش کاربرد شبکه و اینترنت، به وجود آمدند و به این نسل، نسل جرایم سایبری نیز گفته می‌شود و تا به امروز، با این قبیل جرایم، رو به رو هستیم.

اقدامات انجام شده برای مبارزه با جرایم رایانه‌ای در دنیا

گسترش جرایم رایانه‌ای دردنیا مخصوصاً در کشورهایی که بیشترین استفاده‌کنندگان از کامپیوتر و اینترنت را دارند، باعث شده است که دولت‌های مختلف، به فکر مکانیزم‌ها و سازوکارهای قانونی و حقوقی برای رسیدگی و مبارزه با این‌گونه جرایم بیافتند. برای این منظور، کنوانسیون‌های بین‌المللی نیز برای سهولت در روند شناسایی جرم و مجرم، هم‌کاری در پی‌جویی و تعقیب قضایی و پلیسی مجرمان، تبادل دانش و اطلاعات پلیسی در شناخت و کشف علمی جرایم سایبری تشکیل شدند. از مهم‌ترین این کنوانسیون‌ها می‌توانیم به کنوانسیون بوداپست در سال ۲۰۰۱ اشاره کنیم. از کشورهای فعال در زمینه پیجویی و مبارزه با جرایم رایانه‌ای، می‌توانیم به کشورهایی مثل ایالات متحده آمریکا، روسیه، چین، کره جنوبی، انگلستان، هند، فرانسه و آلمان اشاره کنیم. این کشورها، در واقع برای پیجویی و مبارزه با جرایم رایانه‌ای پیشرو بودند و راه‌کارهایی را در این زمینه ارائه داده‌اند.

ضرورت تشکیل پلیس فتا

توسعه روزافزون زیرساخت‌های فن‌آوری اطلاعات و ارتباطات در کشورمان و همچنین، افزایش کاربران و استفاده‌کنندگان از اینترنت و سایر فن‌آوری‌های اطلاعاتی و ارتباطی و مخابراتی نظیر خطوط تلفن ثابت و همراه، شبکه‌های دیتای کشوری و محلی و ارتباطات ماهواره‌ای، از جمله دلایلی هستند که لزوم ایجاد و توسعه مکانیزم و ساز و کاری برای برقراری امنیت در فضای تولید و تبادل اطلاعات در کشورمان را توجیح می‌کنند. همچنین، امروزه می‌بینیم که توسعه خدمات الکترونیک در کشور، مثل دولت الکترونیک، بانک‌داری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سایر خدماتی که امروزه با آن درگیر هستیم، لزوم ایجاد یک پلیس تخصصی در مجموعه نیروی انتظامی را برای تامین امنیت در فضای سایبری و مبارزه با جرایم رخ داده در این فضا را بر همگان، آشکار می‌کند.

از طرف دیگر، رشد جرایم در حوزه فضای تبادل اطلاعات کشور، مثل کلاه‌برداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت داده‌ها، تجاوز به حریم خصوصی افراد و گروه‌ها، هک شدن و نفوذ در سامانه‌های رایانه‌ای و اینترنتی و جرایم اخلاقی و برخی از جرایم سازمان یافته اقتصادی، اجتماعی و فرهنگی، ایجاب می‌کنند که یک پلیس تخصصی که توان پی‌جویی و رسیدگی به جرایم رایانه‌ای را در سطح بالای فن‌آوری داشته باشد، به وجود آمده و فعالیت کند.

از طرف دیگر، با توجه به تصویب قانون جرایم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای اجرای این قوانین، مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، پلیس فتا در بهمن ماه ۱۳۸۹ به دستور فرماندهی محترم نیروی انتظامی جمهوری اسلامی ایران تشکیل شد.

اهداف و وظایف پلیس فتا

موارد زیر، جزء اهداف و وظایف پلیس فتاست:

- تامین امنیت فضای تولید و تبادل اطلاعات کشور
- حفظ و صیانت از هویت دینی، ملی و ارزشهای انسانی جامعه
- حفظ حریم خصوصی افراد و آزادی‌های مشروع
- صیانت از منافع، اسرار و اقتدار ملی در فضای تولید و تبادل اطلاعات
- حفظ زیرساخت‌های حیاتی کشور در مقابل حملات الکترونیکی
- اعتماد و آسودگی خاطر شهروندان جامعه، برای انجام امور قانونی، از جمله فعالیت‌های اقتصادی و فرهنگی
- ایجاد امنیت و کاهش مخاطرات در فعالیت‌های علمی، اقتصادی و اجتماعی در جامعه اطلاعاتی کشور
- مراقبت و پایش از فضای تولید و تبادل اطلاعات برای پیش‌گیری از تبدیل شدن این فضا به بستری برای انجام هماهنگی‌ها برای فعالیت‌های غیر قانونی.

فصل سوم

امنیت، حفاظت و نگهداری از اطلاعات

- ❑ **در این فصل، با مفاهیم زیر آشنا خواهیم شد:**
  - ✓ **تعاریف و مفاهیم پایه در امنیت اطلاعات (الفبای امنیت)**
  - ✓ **مفاهیم رمزنگاری داده‌ها و راه‌کارهای حفظ محرمانگی داده‌ها**
  - ✓ **امضای دیجیتال**
  - ✓ **راه‌کارهای حفظ جامعیت اطلاعات**

تعاریف و مفاهیم پایه امنیت اطلاعات

واژه امنیت یا *Security*، به معنای دوری از هرگونه ریسک ایمنی است. به عبارت دیگر، هر چیزی که به ما ایمنی و اعتماد بدهد، به عنوان امنیت تلقی می‌شود. در حوزه امنیت اطلاعات، سه جنبه اساسی وجود دارد که توجه به این سه جنبه، در تمام حوزه‌ها مدنظر است. در کتاب‌ها این سه جنبه را تحت عنوان مثلث سه‌گانه امنیت اطلاعات نیز، معرفی کرده‌اند:

- محرمانگی (*Confidentiality*)
- جامعیت (*Integrity*)
- دسترسی پذیری (*Availability*)

این سه جنبه، به مثلث *CIA* در حوزه امنیت اطلاعات، معروف است. می‌خواهیم با این سه جنبه آشنا شده و به هر یک از جنبه‌ها به طور جداگانه بپردازیم.

محرمانگی (*Confidentiality*)

محرمانگی اطلاعات، یعنی فقط افراد خاصی (افراد مجاز) به اطلاعات دسترسی داشته باشند. به عبارت دیگر، افراد غیر مجاز به داده‌های افراد مجاز، دسترسی نداشته باشند. چرا که در این صورت، محرمانگی داده‌ها از بین رفته و داده‌ها فاش خواهند شد.

جامعیت (*Integrity*)

جامعیت، را از دو جنبه بررسی می‌کنند: جامعیت داده و جامعیت مبدأ. جامعیت داده، یعنی آن‌چه که گیرنده دریافت کرده، باید همان چیزی باشد که فرستنده، فرستاده است. یعنی فردی یا عنصری در وسط راه، داده را دستکاری نکرده باشد.

جامعیت فرستنده یا جامعیت مبدأ، یعنی آن‌چه گیرنده دریافت کرده است، باید همان چیزی باشد که فرستنده، ارسال کرده است. در این شرایط، هیچ‌کس نمی‌تواند خود را به جای فرستنده پیام، جابزند. در جامعیت مبدأ، جعل هویت را کنترل می‌کنیم.

دسترسی پذیری (*Availability*)

سومین جنبه امنیت اطلاعات یا دسترسی پذیری (*Availability*)، به این معناست که منابعی که یک کاربر، مجاز به دسترسی به آن‌هاست، باید به طور مدام در اختیار و دردسترس او باشد.

نکته مهمی که در مورد جنبه‌های سه‌گانه امنیت باید به آن اشاره کرد این است که نقض یک یا چند مورد از جنبه‌های سه‌گانه، به معنای نقض امنیت خواهد بود.

اصطلاحات حوزه امنیت

۱- دارایی (*Asset*)

دارایی به عناصری از یک سیستم گفته می‌شود که ارزش حفاظت دارد. اگر سیستم ما سیستم اطلاعاتی است، دارایی‌های یک سیستم اطلاعاتی، داده‌هایی هستند که ارزش حفاظت کردن دارند. دارایی در حالت کلی، فقط اطلاعات نیست و به هر چیزی که ارزش حفاظت کردن را دارد، دارایی گفته می‌شود. در یک سیستم یا یک سازمان، فقط نباید از داده مراقبت کنیم، ممکن است به لحاظ فنی، محافظت‌های لازم از داده‌ها صورت گرفته باشد، اما یک کارمند ساده‌لوح، داده‌ها را به راحتی در اختیار دیگران قرار دهد.

۲- تصدیق اصالت (*Authentication*)

تصدیق اصالت، یعنی اطمینان حاصل کنیم که کاربر، همان فردیست که ادعا می‌کند. یکی از مکانیزم‌های پیاده‌سازی تصدیق اصالت، استفاده از نام کاربری و کلمه عبور است.

۳- مجازشناسی (*Authorization*)

مجازشناسی، دسترسی کاربران مختلف به اجزای سیستم را تعریف می‌کند. در تصدیق اصالت، با استفاده از یک مکانیزم نام کاربری و کلمه عبور، می‌توان مطمئن شد که افراد مجاز، وارد سیستم

می‌شوند، اما مجازشناسی مشخص می‌کند که افراد وارد شده، هر کدام مجاز به استفاده از کدام المان‌های سیستم هستند.

مثال:

در یک سازمان، برای کنترل ورود و خروج کارمندان، سیستم کارت‌زنی، فرایند تصدیق اصالت (*Authentication*) را انجام می‌دهد. اما بعد از ورود کارمندان، هر یک از کارمندان، مجاز به ورود و خروج به همه اطاق‌های سازمان نیست و این مجوزها برای تردد و دسترسی کارمندان به اجزای سازمان، توسط خود سازمان، تعریف می‌شود. این فرایند، مجازشناسی (*Authorization*) نامیده می‌شود.

٤- حریم خصوصی (*Privacy*)

حریم خصوصی، به معنای مقاومت در مقابل اشفای اطلاعاتی است که از مشاهده فعالیت‌های یک سازمان یا سیستم، قابل استنتاج است. محرمانگی (*Confidentiality*) با حریم خصوصی (*Privacy*)، تفاوت دارد. به عنوان مثال، اطلاعات زندگی شخصی افراد، اطلاعات محرمانه‌ای نیست. مثلاً کد ملی یک کارمند، جزو اطلاعات محرمانه سازمان حساب نمی‌شود ولی جزو حریم خصوصی کارمند است. یا این که اطلاعات حساب بانکی همکار شما، اطلاعات محرمانه‌ای نیست ولی جزو حریم خصوصی همکار شماست.

٥- خط‌مشی امنیتی (*Security Policy*)

بیان رسمی قواعد و باید و نبایدهایی که باعث امن نگه داشته شدن دارایی‌های یک سیستم یا سازمان می‌شود. هر سیستم برای خود مجموعه‌ای از بایدها و نبایدها را دارد. مجموعه این بایدها و نبایدها به حفظ امنیت سازمان یا سیستم، کمک می‌کند. خط مشی‌های امنیتی به سه دسته تقسیم می‌شوند:

- خط‌مشی‌های پیشگیرانه (*Primitive Policies*)
- خط‌مشی‌های تشخیصی (*Detective Policies*)
- خط‌مشی‌های بازیابی (*Recovery Policies*)

مجموعه خط‌مشی‌های فوق، امنیت سیستم را برقرار می‌کنند.

خط‌مشی‌های پیشگیرانه، بایدها و نبایدهایی هستند که باعث پیشگیری از به خطر افتادن امنیت اطلاعات می‌شوند. گفته می‌شود که امنیت، نسبی است و در هیچ‌جا نمی‌توان تضمین کرد که امنیت، صد در صد است. خط مشی‌های پیشگیرانه، کمک می‌کنند که اتفاق بدی نیافتد؛ ولی با توجه به نسبی بودن امنیت، نمی‌توان تمام بایدها و نبایدهای ممکن جهان را وضع کرد تا اتفاق بدی نیافتد. هرچقدر تمهیدات لازم برای پیشگیری از وقوع اتفاقات ناگوار را پیش‌بینی کرده باشیم، باز هم ممکن است،

امنیت اطلاعات ما در سیستم، با خطراتی مواجه شود. بنابراین باید برخی خط‌مشی‌های تشخیصی را در یک سیستم وضع نمود که این خط مشی‌ها کمک می‌کنند که در صورت نقض امنیت یک سیستم، تشخیص داده و به شکلی به ما اطلاع دهند (مثلاً آلارم دهد).

از آن‌جا که قدرت تشخیص را هم نمی‌توان به صورت صد در صد تضمین نمود، خط‌مشی‌های گروه سوم، که به آن‌ها خط‌مشی‌های بازیابی گفته می‌شود، در سیستم به کار می‌آیند. این خط مشی‌ها، بایدها و نبایدهایی هستند که می‌گویند، اگر امنیت یک سیستم، نقض شد، چه طور آن را به وضعیت، قبل، برگردانیم.

مثال۱

اگر سیستم اتومبیل را به عنوان سیستم، در نظر بگیریم، برای جلوگیری از تصادفات و اتفاقات ناگواری مثل سرقت، لازم است، بایدها و نبایدهایی در این اتومبیل درنظرگفته شود.

نصب قفل فرمان می‌تواند از نوع خط‌مشی‌های پیشگیرانه (*Primitive*) برای جلوگیری از سرقت اتومبیل به شمار برود و نصب دزدگیر و آژیر از نوع خط مشی‌های تشخیصی (*Detective*) است. اما به هر حال، ممکن است علی‌رقم وجود تمهیدات پیشگیرانه، اتومبیل در شرایطی دچار سرقت شود. در این صورت، چه باید کرد؟ بیمه کردن اتومبیل، از نوع خط‌مشی‌های امنیتی بازیابی (*Recovery*) است.

مثال۲

به عنوان مثال دیگر، وقتی شما می‌گویید باید فرایند *Authentication* (تصدیق اصالت) را در یک سازمان به کارگرفته شود تا هویت اشخاص، کنترل شود، یک خط‌مشی امنیتی پیشگیرانه به کار بسته شده است.

در این سیستم، خط مشی تشخیصی می‌تواند به کار بستن سیستم ثبت وقایع باشد تا بعد از ورود اشخاص به سیستم (نقض فرایندهای پیشگیرانه)، بتوان فعالیت‌های او را زیر نظر داشت.

در چنین سیستمی، تهیه نسخه پشتیبان (*Backup*)، می‌تواند یک خط مشی بازیابی باشد. به این ترتیب، در صورت نقض خط‌مشی‌های پیشگیرانه و تشخیصی، می‌توان اطلاعات از دست رفته یا تغییر یافته را بازیابی نمود.

۶- راهکار امنیتی (*Security Mechanism*)

مکانیزم‌های امنیتی، راهکارهایی هستند برای تشخیص، جلوگیری و یا ترمیم آسیب‌های ناشی از حملات امنیتی. به عبارت دیگر، می‌توان گفت، راهکارهای امنیتی، پیاده‌سازی بایدها و نبایدهایی هستند که برای حفظ امنیت در یک سیستم، وضع شده‌اند. مثلاً برای ورود به یک نرم افزار، قانونی وضع شده است که به موجب آن باید هویت فرد، شناسایی شود. این یک باید یا راهکار امنیتی است.

۷- آسیب‌پذیری (*Vulnerability*)

به هرگونه نقطه ضعف در توصیف، طراحی، پیاده‌سازی، پیکربندی یا اجرای یک سیستم، به طوری که امکان سوءاستفاده از آن برای نقض خط‌مشی‌های یک سیستم، آسیب‌پذیری گفته می‌شود.

۸- مخاطره یا تهدید (*Threat*)

به احتمال سوء استفاده کردن از یک یا چند آسیب‌پذیری، مخاطره یا تهدید گفته می‌شود. باید دقت کنیم که در این تعریف، سوء استفاده، محقق نشده است و فقط احتمال سوء استفاده مد نظر است.

۹- حمله امنیتی (*Security Attack*)

محقق شدن یک تهدید از طریق یک یا چند آسیب‌پذیری بری روی یک دارایی (*Asset*)، حمله گفته می‌شود. در واقع، حمله، وضعیت بالفعل تهدید است.

حمله کنندگان در یک سیستم، چه کسانی هستند؟

هر فرد یا عنصری در یک سیستم که اعمال یا فعالیت‌های او اثرات سوء روی سیستم دارد را حمله کننده می‌نامیم. حمله کنندگان یا مهاجمانی کامپیوتری، کاربران یا نرم‌افزارهایی هستند که اعمال خلافی را در کامپیوترها انجام می‌دهند. حمله می‌تواند انفرادی یا گروهی باشد و حمله‌کننده می‌تواند اهداف مختلفی را دنبال کرده و روش‌های مختلفی را برای حمله خود به کار گیرد.

در نسل‌های مختلف جرایم رایانه‌ای، اهداف مختلفی برای حمله به سیستم‌های کامپیوتری، وجود داشته است. مثلاً ممکن است حمله‌کننده بخواهد به خاطر رسیدن به شهرت و اثبات مهارت خود به دیگران، این کار را انجام دهد. دسترسی به حساب بانکی یک نفر نیز یک انگیزه مالی است که فرد را به حمله، ترقیب نموده است. بنابراین، بنابر سناریوهای مختلف، حمله کننده می‌تواند اهداف و روش‌های مختلفی را برای اجرای حمله خود به کارگیرد.

حمله‌کنندگان در سیستم‌های کامپیوتری به دو دسته تقسیم می‌شوند:

- **حمله کننده داخلی**
- **حمله کننده خارجی**

حمله‌کننده داخلی، عضو معتبری از یک سیستم یا سازمان است که فعالیت‌های مخربی را علیه اهداف سازمان خود انجام می‌دهد. طبق آمار، بیش از شصت درصد از حملات کامپیوتری در یک سیستم یا سازمان را حمله‌کنندگان داخلی انجام می‌دهند.

در نقطه مقابل، حمله‌کننده خارجی را داریم که عضوی خارج از سیستم یا سازمان است که داخل سازمان، مجاز شمرده نمی‌شود ولی فعالیت‌های مخربی را داخل آن سازمان انجام خواهد داد.
در واقع، حمله‌کنندگان داخلی، خطرناک‌تر از حمله‌کنندگان خارجی هستند؛ چون حمله کننده داخلی، زیر و بم سازمان را می‌شناسد و به نقاط ضعف آن آگاه است، ولی حمله کننده خارجی تا زمانی که وقت زیادی را صرف شناسایی محیط سیستم یا سازمان نکند، نمی‌تواند حمله خود را عملی کند.

انواع حمله (*Attack*)

حملات کامپیوتری به دو دسته تقسیم می‌شوند:

- **حملات غیر فعال (*Passive Attack*)**
- **حملات فعال (*Active Attack*)**

حمله غیر فعال، ترافیکی را در شبکه ایجاد نمی‌کند (هیچ داده‌ای را اضافه یا کم نمی‌کند)، بلکه قصد دارد اطلاعاتی را از سیستم یا سازمان، استخراج کند تا بتواند از آن اطلاعات، نتایجی را استنتاج کند. به عنوان مثال، وقتی یک شخص ثالث، به گفتگوی دو نفر گوش می‌کند، هیچ مکالمه‌ای بین او و دو نفر دیگر صورت نمی‌گیرد ولی این شخص با کسب اطلاعات، می‌تواند اهداف خود را عملی کند. به چنین حمله‌ای، حمله غیرفعال می‌گوییم.
در مقابل حملات غیرفعال، حملات فعال را داریم. در حملات فعال، فرد حمله کننده، سعی می‌کند منابع سیستم را تغییر بدهد یا بر عملکرد منابع سیستم، تأثیر بگذارد. در این نوع حمله، حمله کننده باعث تولید اطلاعات جدیدی خواهد شد. در این نوع حمله، حمله‌کننده سعی می‌کند اطلاعات را دستکاری کند. مثل جعل هویت، قطع ارتباط، تغییر اطلاعات و غیره، جزو حملات فعال محسوب می‌شوند.
در هر یک از حملات امنیتی، یکی از جنبه‌های امنیت، نقض می‌شود. مثلاً در حمله غیر فعال شنود، محرمانگی (*Confidentiality*) از جنبه‌های سه گانه *CIA*، نقض شده است. در حمله جعل هویت، جنبه جامعیت *(Integrity)* نقض شده است. در حمله قطع ارتباط (*DOS*)، فرد سرویس گیرنده از سرویس دهنده قطع خواهد شد. بنابراین، در این نوع حملات، جنبه دسترسی پذیری (*Availability*) نقض شده است.

مثال۱:

فرض کنید، کاربر *A*، فایلی را برای کاربر *B* ارسال می‌کند. این فایل، حاوی اطلاعات مهمی است که نباید فاش شود. کاربر *C* که مجوز خواندن آن فایل را ندارد، می‌تواند یک نسخه از آن را در بستر شبکه

به دست بیاورد. به این ترتیب، یک نسخه از فایل محرمانه را کاربر C در اختیار دارد. در این صورت، چیزی از سیستم کم یا زیاد نمی‌شود. بنابراین، این نوع حمله، یک حمله غیر فعال است.

مثال۲:

فرض کنید کاربر مدیر به نام D، قصد دارد پیامی را برای کاربر E ارسال کند. محتوای پیام، به کاربر E دستور می‌دهد که فایلی را در شبکه داخلی شرکت به روز کند تا تعدادی از کارمندان جدید بتوانند به شبکه دسترسی پیدا کنند. حال اگر کاربر دیگری، این پیام را دزدیده و محتوای آن را تغییر دهد. مثلاً نام چند نفر را حذف یا نام چند نفر کارمند جعلی دیگر را به لیست کاربران ذکر شده در پیام اضافه کند و بعد پیام را به دست کارمند E برساند، کارمند E با فرض این که پیام از مدیر، رسیده است، برای کاربران ذکر شده در پیام، کاربری می‌سازد. در این سناریو، با یک حمله فعال مواجهیم چرا که در آن، اطلاعاتی از سیستم کم یا اطلاعاتی به سیستم اضافه شده است.

تهیه نسخه پشتیبان (*Backup*)

یکی از راه‌کارهای پاسخگویی به حوادث و رخدادهای رایانه‌ای نظیر خرابی یا عملکرد نادرست سخت‌افزار یا نرم‌افزار، اشتباه کاربران، حملات عمدی یا غیر عمدی رایانه‌ای و یا هر حادثه‌ای که منجر به تخریب داده‌ها می‌شود این است که یک نسخه پشتیبان قابل اعتماد از داده‌ها و دارایی‌های خود داشته باشیم.

در واقع، تهیه نسخه پشتیبان، یکی از خط‌مشی‌هایی است که برای بازیابی اطلاعات به کار رفته و منجر به حفظ دارایی‌های یک سیستم یا سازمان می‌شود. در یک سازمان، لازم است که از کلیه دارایی‌های الکترونیکی آن سازمان، شامل بانک‌های اطلاعاتی (*Database*ها)، نرم‌افزارهای کاربردی (*Applications*)، فایل‌های پیکربندی (*Configuration Files*)، سیستم‌های عامل (*Operating Systems*)، فایل‌های داده (*Data Files*)، ابزارهای سیستمی و کلیه دارایی‌های اطلاعاتی، یک نسخه پشتیبان قابل اعتماد، تهیه شود و این نسخه پشتیبان قابل اعتماد، در محل امنی نگهداری شده و به طور مستمر، به روزرسانی شود.

توصیه می‌شود که نسخه پشتیبانی که از نرم‌افزارهای سیستم خود تهیه می‌کنیم، در محلی به غیر از محل استقرار فیزیکی سیستم نگهداری شود تا در صورت بروز حوادث و بلایای طبیعی، احتمال خرابی همزمان سیستم اصلی و سیستم پشتیبان، به صفر نزدیک شود.

با تهیه کردن یک نسخه پشتیبان قابل اعتماد از دارایی‌ها به عنوان یک خط مشی بازیابی، می‌توانیم تا حدودی امنیت اطلاعات را در سیستم، به حالت امن اولیه بازگردانیم.

انواع روش‌های تصدیق اصالت

در سیستم‌های اطلاعاتی کامپیوتری، می‌توان چهار روش را برای تصدیق اصالت، در نظر بگیریم:

۱- **تصدیق اصالت از طریق دانش کاربر (روش *What you know*)**

در این روش، شخص شناسایی کننده، اطلاعاتی را در مورد هویت شخص ادعا کننده دارد که آن اطلاعات را فقط فرد ادعا کننده می‌داند که با استفاده از این اطلاعات، می‌توان هویت شخص ادعا کننده را تصدیق نمود.

مثلاً برای تصدیق اصالت اطلاعات کاربر، می‌توان از روش کلمه عبور (*Password*) استفاده نمود. در این حالت، فقط کسی که کلمه عبور را می‌داند و می‌تواند مجاز بودن خود را ثابت کند، می‌تواند وارد سیستم شود.

۲- **تصدیق اصالت از طریق دارایی‌ها (روش *What you have*)**

در این روش، شخص ادعا کننده، از طریق داشتن شیئی که با خود همراه دارد، مجاز شناخته می‌شود. به عنوان مثال، هنگام ورود یک کارمند به سازمان، این کارمند با کشیدن کارت روی دستگاه کارت‌زنی، می‌تواند اصالت خود را به اثبات برساند. یا وقتی کارت بانکی خود را وارد دستگاه کارت‌خوان یک فروشگاه می‌کنید، اصالت خود را برای سیستم بانک صادر کننده کارت خود به اثبات می‌رسانید.

۳- **تصدیق اصالت از طریق خاصیت‌ها (روش *What you are*)**

در این روش تصدیق اصالت، یک سری خصوصیات انسانی یا فردی در شخص ادعا کننده وجود دارد که با ارزیابی مستقیم این خصوصیات، مجاز بودن فرد، تشخیص داده می‌شود. اثر انگشت، شبکیه چشم و چهره نگاری از نمونه‌های خصوصیات فردی است که برای تشخیص اصالت، از آن استفاده می‌شود.

۴- **تصدیق اصالت از طریق محل استقرار کاربران (روش *Where you are*)**

در این روش، محلی که کاربر در آن‌جا استقرار دارد، عامل تشخیص اصالت درنظر گرفته می‌شود. با ارزیابی این محل، اصالت فرد، تشخیص داده می‌شود. به عنوان مثال، وقتی به اطاق همکارتان تلفن می‌زنید، می‌توانید در مورد اصالت فردی که قصد صحبت با او را دارید، اطمینان حاصل کنید.

فصل چهارم

آشنایی با انواع تهدیدات سایبری

- ❑ **در این فصل، با مفاهیم زیر، آشنا خواهیم شد:**
  - ✓ **انواع تهدیدات امنیتی**
  - ✓ **بدافزارها (*Malware*)**
  - ✓ **شبکه‌های اجتماعی اینترنت و تهدیدات آن**
  - ✓ **تهدیدات شبکه‌های کامپیوتری بیسیم**

انواع حملات امنیتی

حمله قطع ارتباط

فرض کنید در یک ساختار ارتباطی، یک فرستنده، داده‌ای را بدون این که هیچ یک از خطرات امنیتی آن را تهدید کند، برای یک گیرنده ارسال می‌کند. اولین تهدیدی که در فضای ارتباطی شبکه، داده ارسال شده را می‌تواند به خطر بیاندازد، حمله قطع ارتباط یا *Denied Of Service* (*DOS*) نام دارد. در این حمله، فرد حمله کننده کاری می‌کند که داده‌های ارسال شده از فرستنده در اختیار گیرنده قرار نگیرد یا با کاهش سرعت و کیفیت در اختیار گیرنده قرار بگیرد. پس در حمله قطع ارتباط، منظور، قطع کامل کانال ارتباطی نیست، بلکه کند شدن نرخ دریافت اطلاعات توسط گیرنده نیز می‌تواند حمله ممانعت از سرویس یا قطع ارتباط محسوب شود.

در فصل‌های گذشته دیدیم که در بسترهای ارتباطی، به دنبال این هستیم که سه جنبه *CIA* یا همان (محرمانگی، جامعیت و دسترسی پذیری حذف شود). قاعدتاً در تهدیدات امنیتی، زمانی یکی یا چند یک از جنبه‌های سه گانه نقض شود، اصطلاحاً یک تهدید رخ داده است. در حمله ممانعت از سرویس یا قطع ارتباط، به نوعی مفهوم دسترسی پذیری (*Availability*) نقض خواهد شد.

در فصل قبل، حملات امنیتی را به دو دسته فعال (*Active*) و غیر فعال (*Passive*) تقسیم کردیم. حمله قطع ارتباط، یک نوع حمله فعال محسوب می‌شود که در آن، حمله کننده، ترافیک رد و بدل شده بین

فرستنده و گیرنده را دستکاری می‌کند. فرق نمی‌کند که کاملاً ترافیک را قطع کند یا فقط نرخ ارسال داده‌ها را کند کند.

حمله استراق سمع

حمله دیگری که در فضای شبکه با آن مواجه هستیم، حمله استراق سمع یا شنود کردن است. وقتی فرستنده قصد دارد طبق جریان عادی اطلاعات، داده‌هایی را برای گیرنده ارسال کند، اگر فرد حمله کننده یک نسخه از داده‌های ارسال شده را نگه دارد و روی آن‌ها استنتاج انجام دهد و از محتوای اطلاعات، مطلع شود، حمله استراق سمع یا شنود رخ داده است. در واقع، محرمانگی اطلاعات (*Confidentiality*) در اثر این حمله، خدشه‌دار خواهد شد. در این نوع حمله، حمله‌کننده ترافیک شبکه را تغییر نمی‌دهد و فقط یک نسخه از آن را نگه می‌دارد. به همین دلیل، شنود، از نوع حملات غیر فعال محسوب می‌شود.

حمله تغییر

وقتی فرستنده داده‌ای را برای گیرنده ارسال می‌کند و تصور می‌کند که گیرنده، همان داده‌ای را که ارسال کرده است، عیناً دریافت کرده است. غافل از این که، یک حمله کننده در مسیر ارتباطی قرار گرفته و بعد از دریافت داده‌های ارسال شده از فرستنده، بعد از تغییر داده‌ها، داده‌های تغییر یافته را برای گیرنده ارسال کند. در این سناریو، گیرنده پیام، داده‌های ارسالی توسط فرستنده را دریافت نکرده است و کاملاً چیز متفاوتی را دریافت کرده است. در این نوع حمله، جامعیت داده (*Data Integrity*) از وجوه سه‌گانه *CIA*، نقض شده است. چون، چیزی که گیرنده دریافت کرده است، آن چیزی نیست که فرستنده ارسال کرده است.

حمله جعل هویت

در این سناریو، فرستنده هیچ داده‌ای را برای گیرنده ارسال نمی‌کند، ولی یک حمله کننده با جازدن خود به عنوان فرستنده واقعی، داده‌هایی را برای گیرنده ارسال می‌کند. در واقع، حمله کننده، هویت فرستنده پیام را جعل می‌کند. در این حمله، جامعیت داده (*Data Integrity*) نقض شده است و این حمله، یک نوع حمله فعال محسوب می‌شود.

حمله *Fishing* یا سرقت آنلاین اطلاعات

به تلاش برای به دست آوردن اطلاعاتی مثل نام کاربری، رمز عبور، اطلاعات حساب بانکی و غیره از طریق جعل یک وب‌سایت یا آدرس *E-mail*، اصطلاحاً حمله *Fishing* یا سرقت آنلاین گفته می‌شود. این حمله در عمل، با کمک یک کپی دقیق اما جعلی از رابط گرافیکی یک وب‌سایت معتبر، مثلاً

وب‌سایت یک بانک انجام می‌شود. در این صفحات، از کاربر درخواست می‌شود که اطلاعاتی مثل حساب بانکی یا هر اطلاعات حساس و مهم دیگری را وارد کند. به عنوان مثال، شماره کارت بانکی و رمز عبور کارت، در آن صفحه جعلی وارد شود، فرد حمله کننده به راحتی می‌تواند با استفاده از این اطلاعات، از طریق کارت بانکی فرد، خرید کرده و امنیت او را به خطر بیاندازد. به این حمله، حمله *Fishing* یا سرقت آنلاین اطلاعات گفته می‌شود.

مهندسی اجتماعی (*Social Engineering*)

در مهندسی اجتماعی، از تمایل طبیعی وفطری انسان‌ها به اعتماد کردن، به شکل زیرکانه‌ای سوء استفاده می‌شود. مهاجم با استفاده از مجموعه‌ای از تکنیک‌های موذیانه، افراد را متقاعد می‌کند که اطلاعاتی را فاش کنند یا کارهایی را انجام دهند که باب میل مهاجم است. در این روش، مهاجم به جای استفاده از روش‌های معمول برای نفوذ به سیستم‌های یک سازمان و پایگاه داده‌های مربوطه، سعی می‌کند از مسیر افرادی که به این اطلاعات دسترسی دارند و با استفاده از تکنیک‌های فریب آن‌ها، اطلاعاتی را در جهت دستیابی به خواسته‌های خودش، از آن سازمان، جمع‌آوری کرده و حملاتی را ترتیب دهد.

فرایندها و عملیاتی که برای حمله مهندسی اجتماعی مورد استفاده قرار می‌گیرند، چرخه‌ای را به وجود می‌آورند که به آن چرخه مهندسی اجتماعی گفته می‌شود. این چرخه، شامل چهار مرحله است:

در مرحله اول، حمله‌کننده سعی می‌کند اطلاعات عمومی جامعی را در مورد سازمان مورد حمله، جمع‌آوری کند.

در مرحله دوم، و برای این کار، سعی می‌کند با افراد سازمان، طرح دوستی ریخته و با آن‌ها ارتباط برقرار کند. بعد از این که افراد مجاز در یک سازمان، به این فرد حمله کننده اعتماد نسبی پیدا کردند، زمان مرحله سوم فرا می‌رسد.

در مرحله سوم، حمله کننده سعی می‌کند از این ارتباط، سوء استفاده کرده و با کمک این افراد، اطلاعات محرمانه‌ای را در مورد سازمان به دست آورد.

در مرحله چهارم، حمله، عملی می‌شود و بسته به سناریویی که حمله کننده دنبال می‌کند، از اطلاعات کسب شده به شکل‌های مختلف، استفاده می‌کند.

راه‌کارهای پیشگیری از حملات مهندسی اجتماعی

توصیه‌های پیشگیرانه برای مصون ماندن در برابر حملات مهندسی اجتماعی، از این قرار است:

- اولین نکته این است که به تلفن‌ها، ایمیل‌ها و ملاقات‌های ناخواسته‌ای که در آن‌ها اطلاعات شخصی کارمندان سازمان از ما درخواست می‌شود، با دید شک و سوء ظن نگاه کنید.

- اطلاعات شخصی و اطلاعات سازمانی خود را بدون دلیل در اختیار افراد قرار ندهید.
- اطلاعات شخصی و مالی خود را هرگز در اختیار درخواست‌کننده‌های ناشناس، چه از طریق ایمیل، چه از طریق شبکه‌های اجتماعی یا هر روش ارتباطی دیگری قرار ندهید.
- اطلاعات حساس و مهم شخصی خود و سازمان خود را بر روی فضای اینترنت، قرار ندهید. توصیه می‌شود که برای ارسال اطلاعات درون سازمانی، از یک کانال ارتباطی داخلی استفاده شود و این اطلاعات، از طریق اینترنت، مبادله نشود.
- آدرس *URL* وب‌سایت‌ها را با دقت وارد کنید و از وب‌سایت‌های جعلی دور باشید.
- زمانی که نامه یا درخواستی را دریافت کردید، در صورت امکان، به صورت تلفنی، از هویت فرستنده نامه یا درخواست، اطمینان حاصل کنید.
- توصیه می‌شود نرم‌افزارهای آنتی‌ویروس، *Firewall* و فیلترینگ نامه‌های ناخواسته را برای برقراری سطح مناسبی از امنیت، بر روی سیستم‌های کامپیوتری خود نصب کنید تا سیستم کامپیوتر خود را از حملات ویروسی محفوظ دارید.

بدافزارها و نرم‌افزارهای مخرب

بدافزار یا *Malware* (*Malicious Software*)، نرم‌افزار کامپیوتری مخربیست که با هدف آزار و اذیت کاربران و ایجاد خسارت، طراحی و ساخته شده‌اند. به منظور آشنایی بیشتر با خراب‌کاری‌هایی که با استفاده از نرم‌افزارهای مخرب یا بدافزارها انجام می‌شوند، باید با انواع آن‌ها آشنا شویم:

ویروس

ویروس، نوعی بدافزار است که اغلب، بدون اطلاع کاربر، اجرا شده و تلاش می‌کند خود را در کد اجرایی دیگری، کپی کند. بعد از کپی شدن ویروس در یک کد اجرایی، اصطلاحاً گفته می‌شود که کد اجرایی، ویروسی شده است.

اگر نرم‌افزاری به ویروس، آلوده شود، در اثر اجرای نرم‌افزار آلوده به ویروس، نرم‌افزارهای دیگری به همان ویروس، آلوده خواهند شد.

کرم اینترنتی یا *Internet Worm*

کرم‌ها، برنامه‌هایی هستند که توانایی بازتولید خود را داشته و می‌توانند با استفاده از شبکه، کپی‌های متعدد ساخته شده را به کامپیوترهای دیگر شبکه ارسال کرده و به همین روش، همه کامپیوترهای موجود در شبکه را ویروسی کنند. مهم‌ترین ویژگی مشترک کرم‌ها و ویروس‌ها این است که کرم‌ها هم

می‌توانند خودهمانندساز باشند. البته تولید مثل کرم‌ها و ویروس‌ها از دو جهت با هم تفاوت دارد. اول این که کرم‌ها، مستقل و متکی به خود هستند و برای تکثیر، نیازی به کدهای اجرایی دیگر ندارند. دوم این که کرم‌ها توانایی انتقال و توزیع از طریق شبکه را دارند، اما ویروس‌ها برای انتقال از کامپیوتری به کامپیوتری دیگر باید خود را به برنامه‌های اجرایی دیگر چسبانده و از این طریق، خود را از کامپیوتری به کامپیوتر دیگر منتقل کنند.

اسب تروا (*Trojan Horse*)

یک تروجان، برنامه‌ایست که کاربران را در حالی که از اثرات مخرب آن‌ها بی‌اطلاع هستند، ترغیب به اجرای خود می‌کند. اجرای یک تروجان، اثرات مخربی در کامپیوتر مقصد، ایجاد خواهد کرد.

در پشتی (*Back Door*)

به هر کد یا قطعه برنامه‌ای که منجر به دور زدن فرایند امنیتی یک سیستم شود و از این طریق، موجبات دسترسی یک نفوذگر به منابع یک سیستم را ایجاد کند، درب پشتی می‌گوییم. به عبارت دیگر، درب پشتی، به راهی گفته می‌شود که بتوان از آن طریق، به قسمت یا قسمت‌های مشخصی از یک سامانه، مانند کامپیوترها، فایروال‌ها و غیره دسترسی پیدا نمود. در واقع، درب پشتی، مانند درب حیاط خلوت است که توجهات و کنترل‌های کمتری روی آن وجود دارد و یک نفوذگر، به راحتی می‌تواند با حداقل درگیری با نکات امنیتی، خود را وارد سیستم کرده و تحرکات خرابکارانه خود را با سهولت بیشتری انجام دهد.

جاسوس‌افزار

جاسوس‌افزارها مستقیماً دارای اثر مخرب روی نرم‌افزارها و سخت‌افزارهای یک کامپیوتر نیستند و هدف آن‌ها، جمع‌آوری اطلاعات کامپیوترهای موردنظر هستند. درواقع، جاسوس‌افزارها به مانند یک جاسوس در کامپیوتر ما عمل کرده و اطلاعات ما را برای شخص ثالثی ارسال می‌کنند.

بمب منطقی (*Logic Bomb*)

قطعه کدی است که در یک سیستم نرم‌افزاری قرار گرفته و هنگام رخ دادن شرایط خاص، عملیات مخربی را انجام می‌دهد. در واقع، بمب منطقی، مانند یک بمب ساعتی است که در هنگام حصول شرایط خاصی در یک کامپیوتر، منفجر شده و امنیت اطلاعات را به خطر بیاندازد.

به عنوان نمونه یکی از شرایطی که می‌تواند یک بمب منطقی را فعال کند، می‌توان وجود یا عدم وجود یک فایل باشد. یعنی اگر فایلی در محلی از کامپیوتر هدف وجود داشته باشد یا وجود نداشته باشد،

بمب منطقی، اجرا می‌شود. به عنوان نمونه‌ای دیگر از شرایطی که می‌تواند یک بمب را فعال یا تریگر (شلیک) کند، وارد شدن یک کاربر خاص به حساب کاربری خود باشد.

اثرات بدافزارها روی سیستم‌های کامپیوتری

بدافزارها به اشکال گوناگون می‌توانند آثار مخرب خود را برجای بگذارند. نمونه‌ای از این اثرات، می‌تواند اشغال منابع سیستم و کندی عملکرد آن باشد. اثرات دیگری از جمله موارد زیر، می‌تواند در نتیجه عملکرد یک بدافزار در سیستم یک کامپیوتر حاصل شود:

- ایجاد پیام‌های خطای پی در پی
- راه‌اندازی مجدد (*Restart* شدن) به صورت پی‌در پی و بدون دلیل
- ارسال پیام‌های ناخواسته (*Spam*) از کامپیوتر ما برای دوستان ما در حالی که ما هیچ اطلاعی از آن پیام‌ها نداریم
- ساخته شدن آیکن‌های ناخواسته در کامپیوتر

به طور کلی، کارهایی که بدافزارها انجام می‌دهند، امنیت ما را به خطر می‌اندازد و در نمونه‌های مطرح شده مشاهده می‌شود که کندی عملکرد سیستم، از میان جنبه‌های سه‌گانه *CIA*، جنبه دسترسی‌پذیری (*Availability*) کاربر را به خطر می‌اندازد.

روش‌های مقابله با بدافزار

نمونه‌هایی از روش‌های مقابله با بدافزار، عبارتند از:

- نصب و به روزرسانی آنتی‌ویروس‌ها
- استفاده از مرورگرهای امن
- مدیریت کردن کامپیوتر
- اسکن نرم‌افزارهای جدید
- به روز نگه داشتن دانش نرم‌افزاری و سخت‌افزاری
- تهیه نسخه‌های پشتیبان (*Backup*) از داده‌ها و اطلاعات
- خرید نرم‌افزارها از منابع معتبر

آنتی‌ویروس

آنتی‌ویروس به مجموعه‌ای از برنامه‌ها گفته می‌شود که برای مقابله با ویروس‌ها و بدافزارها از آن‌ها استفاده می‌شود. مهم‌ترین قسمت هر برنامه آنتی‌ویروس، موتور اسکن (*Scanning Engine*) آن‌هاست.

عملکرد موتور اسکن آنتی‌ویروس‌های مختلف، با هم متفاوت است ولی وظیفه اصلی همه موتورهای اسکن، شناسایی فایل‌های آلوده به بدافزار است. آنتی‌ویروس‌ها دارای یک بانک اطلاعاتی هستند که امضاهای ویروس در آن‌ها وجود دارد. امضای ویروس، یک رشته بایتی است که با استفاده از آن می‌توان یک ویروس را به صورت یک کد یکتا و منحصر به فرد، مورد شناسایی قرار داد.

در واقع، آنتی‌ویروس‌ها یک بانک اطلاعاتی دارند که در آن، مجموعه‌ای از امضای ویروس قرار گرفته و زمانی که فرایند اسکن را از آنتی‌ویروس درخواست می‌کنید، به محض مواجه شدن با کدی که معادل امضای یکی از ویروس‌هاست، آن را به عنوان ویروس، شناسایی کرده و آن را یک فایل مخرب خواهند دانست.

به طور خلاصه، می‌توان گفت که آنتی‌ویروس، ضمن نگهداری امضاهای ویروس در یک بانک اطلاعاتی، در فرایند اسکن فایل‌ها، در صورت مواجه شدن با کد امضای ویروس، آلارم داده و آن را به عنوان ویروس، به کاربر معرفی می‌کند. در صورت یافتن فایل آلوده به ویروس، در اکثر مواقع، برنامه‌های آنتی‌ویروس می‌توانند آن را برطرف کنند. اما در برخی موارد، حذف فایل‌های آلوده به ویروس، امکان‌پذیر نیست. در این گونه مواقع، فرایندی تحت عنوان قرنطینه کردن تعبیه شده است که نرم‌افزار آنتی‌ویروس، فایل آلوده به ویروس را از فایل‌های دیگر، قرنطینه کرده و از آلوده شدن فایل‌های دیگر، جلوگیری می‌کند.

شبکه‌های اجتماعی اینترنتی و تهدیدات مربوطه

شبکه اجتماعی، یک ساختار اجتماعی مجازیست که در آن، افراد به واسطه نقاط مشترکی مثل تبادل ایده و تجارت، علاقه‌مندی‌های مشترک، روابط خویشاوندی، پیوندهای وب و مجامع دانشگاهی و مجامعی از این دست، به یکدیگر، مرتبط شده‌اند. با توجه به حجم وسیع استفاده از شبکه‌های اجتماعی اینترنتی، ضروریست که تهدیدات امنیتی این شبکه‌ها را بررسی کنیم.

در این درس، به سه مقوله زیر خواهیم پرداخت:

- اهداف شبکه‌های اجتماعی
- مزایای شبکه‌های اجتماعی
- تهدیدات امنیتی شبکه‌های اجتماعی

اهداف شبکه‌های اجتماعی

شبکه‌های اجتماعی، می‌توانند اهداف زیر را دنبال کنند:

- سازمان‌دهی انواع گروه‌های اجتماعی مجازی

- توسعه مشارکت‌های اجتماعی
- به‌اشتراک گذاشتن علاقه‌مندی‌ها
- ایجاد محتوا توسط اعضا
- تبلیغات هدفمند اینترنتی

سازمان‌دهی انواع گروه‌های اجتماعی مجازی

هدف اول شبکه‌های اجتماعی را می‌توان سازمان‌دهی انواع گروه‌های اجتماعی مجازی بدانیم. همان‌طور که فلسفه شبکه‌های اجتماعی واقعی، بر محور مشترکات اعتقادی، فرهنگی، سیاسیست، بسیاری از شبکه‌های اجتماعی در اینترنت نیز، با تکیه بر این اشتراکات، شکل می‌گیرند. طبیعی است که اعضای یک شبکه اجتماعی مجازی در نهایت، به دنبال تحصیل یک هدف مشترک هستند که قالباً یک هدف اعتقادی، اجتماعی و سیاسی است.

توسعه مشارکت‌های اجتماعی

اعضای یک شبکه اجتماعی، به طور مستقیم و غیر مستقیم به شرکت در فعالیت‌های اجتماعی واقعی، تحریک و تشویق می‌شوند. تاثیرگذاری قابل توجه شبکه‌های اجتماعی بر میزان و کیفیت مشارکت‌های اجتماعی در جوامع مختلف، به حدی بوده است که اخیراً تعداد قابل توجهی از شبکه‌های اجتماعی دقیقاً با هدف توسعه مشارکت اجتماعی مردم در زمینه‌های خاص شکل گرفته‌اند.

به اشتراک گذاشتن علاقه‌مندی‌ها

موضوع به اشتراک گذاشتن علاقه‌مندی‌ها در شبکه‌های اجتماعی، چنان اهمیتی دارد که می‌توان گفت، بدون آن، شبکه‌های اجتماعی، معنا و مفهوم نخواهند داشت. هدف از به اشتراک گذاشتن علاقه‌مندی‌ها، مطرح کردن دغدغه‌های شخصی و اطلاع از دل‌مشغولی‌های کاربران دیگر است. به موجب این ویژگی شبکه‌های اجتماعی، کاربران می‌توانند به آسانی به نرم‌افزارهایی که سایر کاربران به اشتراک گذاشته‌اند، دسترسی داشته باشند.

ایجاد محتوا توسط اعضای شبکه اجتماعی

برخلاف سایر رسانه‌های ارتباطی دیگر که مخاطبان در تولید و انتخاب محتوای دلخواه خود دخالتی ندارند، کاربران شبکه‌های اجتماعی، تولید کننده، تاثیر گذار و دارای حق انتخاب و بهره‌مند از تنوع بیشتر خواهند بود.

به همین دلیل، پایگاه‌های شبکه‌های اجتماعی با پیشرفت فن‌آوری و توسعه جوامع، بیش از هر رسانه دیگری می‌توانند بر سایر رسانه‌ها (مثل تلویزیون که از دو قوه شنیداری و دیداری بهره می‌برد)، برتری پیدا کنند.

تبلیغات هدفمند اینترنتی

شبکه‌های اجتماعی اینترنتی، یکی از منابع مهم کسب درآمد از راه تبلیغات به شمار می‌آیند. اعضای یک شبکه اجتماعی در صفحات مربوط به خود، در مورد علاقه‌مندی‌های خود صحبت می‌کنند و این ویژگی به شرکت‌های تبلیغاتی این فرصت را می‌دهد که با توجه به علاقه‌مندی کاربران شبکه‌های اجتماعی برای آنان آگهی ارسال کنند.

علاوه بر این، بسیاری از شرکت‌های تجاری با ایجاد حساب کاربری و صفحات شخصی در شبکه‌های اجتماعی معروف، می‌توانند با سایر کاربران و مشتریان خود و همچنین شرکت‌های دیگر، ارتباط برقرار کرده و امور کسب و کار خود را پیش ببرند.

مزایای شبکه‌های اجتماعی اینترنتی

شبکه‌های اجتماعی اینترنتی مزایای زیر را دارا هستند:

- انتشار سریع و آزادانه اخبار و اطلاعات
- افزایش سرعت در فرایند آموزش و ایجاد ارتباط شبانه‌روزی بین استاد و شاگرد
- امکان بیان ایده‌ها به صورت آزادانه و آشنایی با ایده‌ها، افکار و سلایق دیگران
- کاربرد تبلیغاتی و محتوایی

انتشار سریع و آزادانه اخبار و اطلاعات

اخبار شبکه‌های اجتماعی معمولاً بدون سانسور، منتشر می‌شوند و این می‌تواند یک مزیت برای شبکه‌های اجتماعی، محسوب شود؛ هرچند امکان تکثیر اطلاعات مخدوش و نادرست نیز در این شبکه‌ها بیش از نسل قبلی رسانه‌ها وجود دارد. البته امکان تحلیل و مقایسه اطلاعات برای مخاطبان وجود دارد و نباید بنا را بر اعتماد بر آن‌چه در این شبکه‌ها منتشر می‌شود، گذاشت.

تحلیل اخبار متناقضی که در این نوع شبکه‌ها منتشر می‌شود، قدرت نقد و نگاه عمیق‌تر به مسائل اجتماعی را فراهم می‌کند و این نوع شبکه‌ها به مخاطب خود فرصت می‌دهند که به جای تبعیت کورکورانه، به خرد نقادانه روی بیاورند.

افزایش سرعت در فرایند آموزش و ایجاد ارتباط شبانه‌روزی بین استاد و شاگرد

بدون شک، شبکه‌های اینترنتی اجتماعی، نقش بسیار موثری در توسعه آموزش‌های تخصصی و عمومی دارند. هرچند که به دلیل عدم امکان نظارت علمی، بسیاری از محتواهای اینترنتی هنوز به مرتبه قابل قبولی از اعتبار علمی نرسیده‌اند، ولی در عین حال، شبکه‌های اجتماعی، یکی از عرصه‌هایی هستند که

کاربران بیشمار آن‌ها به صورت خودجوش نسبت به آموزش و انتقال دانسته‌های تخصصی و عمومی خودشان به دیگران، اقدام می‌کنند.

امکان بیان ایده‌ها به صورت آزادانه و آشنایی با ایده‌ها، افکار و سلایق دیگران

شبکه‌های اجتماعی، ارسال بازخورد از سوی مخاطب و همگامی و همکاری کاربران با یکدیگر را تسهیل کرده و آن‌ها را به مشارکت در مباحث، تشویق می‌کنند. این شبکه‌ها، مرز و خط‌کشی بین رسانه و مخاطب را از بین برده‌اند. اغلب شبکه‌های اجتماعی، برای مشارکت اعضا و دریافت بازخورد آن‌ها باز هستند.

این شبکه‌ها، رای دادن، کامنت گذاشتن و به اشتراک گذاری اطلاعات را تشویق کرده و به ندرت، مانعی برای تولید و دسترسی به محتوا در این نوع شبکه‌ها وجود دارد. رسانه‌های سنتی، عمل انتشار را انجام می‌دادند و محتوا را برای مخاطب ارسال می‌کردند ولی در شبکه‌های اجتماعی، امکان محاوره دوطرفه وجود دارد و جریان اطلاعاتی از حالت یک سویه به دو سویه تغییر کرده است.

کاربرد تبلیغاتی و محتوایی

حضور افراد در شبکه‌های اجتماعی، امکان مشارکت‌ها و کنش‌های اجتماعی را در آن شبکه‌ها افزایش می‌دهد، لذا هرچه پیوند افراد و اعضا در شبکه‌ها بیشتر و انبوه‌تر باشد، همراهی و تعاملات و نزدیکی دیدگاه‌ها و حرکت همسو و مشترک، محتمل‌تر خواهد شد. از این رو، استفاده از چنین فضایی برای معرفی و تبلیغ و همچنین هم‌راستایی مخاطبان در جهت اهداف رسانه‌ای خود، نقش بسیاری دارد.

تهدیدات شبکه‌های اجتماعی اینترنتی

تهدیدات شبکه‌های اجتماعی اینترنتی عبارتند از:

- شکل‌گیری و ترویج سریع شایعات و اخبار کذب
- تبلیغات ضد دینی و القای شبهات
- نقض حریم خصوصی افراد
- گوشه‌گیری و دور ماندن از محیط‌های واقعی اجتماع
- تاثیرات منفی رفتاری
- امکانات فن‌آورانه برای جاسوسی‌های مدرن

شکل‌گیری و ترویج سریع شایعات و اخبار کذب

به دلیل عدم امکان شناسایی هویت واقعی افراد در شبکه‌های اجتماعی و نیز عدم امکان کنترل محتوای تولید شده توسط کاربران، یکی از مهم‌ترین پیامدهای منفی این شبکه‌ها، شکل‌گیری و ترویج

سریع شایعات و اخبار کذبی خواهد بود که توسط بعضی از اعضای این شبکه و با اهداف خاص و قالباً سیاسی منتشر خواهد شد.

تبلیغات ضد دینی و القای شبهات

در شبکه‌های اجتماعی اینترنتی نیز، مانند سایر رسانه‌ها، افراد و گروه‌های مقرض، با اهداف از پیش تعیین شده و با استفاده از شیوه‌های مخصوص، اقدام به تبلیغات ضد دینی و حمله به اعتقادات مذهبی می‌نمایند. بعضی اوقات، پس از تحقیق و ریشه یابی درمی‌یابیم که هدف اصلی گردانندگان بعضی از این تبلیغات، دین‌زدایی و حمله به مقدسات بوده است.

نقض حریم خصوصی

معمولاً شبکه‌های اجتماعی، ابزارها و امکاناتی را در اختیار کاربران قرار می‌دهند تا آن‌ها بتوانند تصاویر و اطلاعات شخصی خود را در این شبکه‌ها قرار دهند. در اغلب شبکه‌های اجتماعی، برای حفظ حریم خصوصی افراد، راه‌کارهایی تعبیه شده است. به عنوان مثال، شبکه‌های اجتماعی، با تعبیه گزینه‌های خاصی، دسترسی به تصاویر و اطلاعات را با توجه به درخواست کاربر، محدود می‌کنند و اجازه دسترسی به پروفایل کاربر را به هر کسی نمی‌دهند. ولی این راه‌کارها کافی نیستند. مشکلاتی از قبیل ساخت پروفایل‌های تقلبی در شبکه‌های اجتماعی و عدم امکان کنترل آن‌ها به دلیل حجم بالای این هرزنامه‌ها، باعث شده که افرادی با پروفایل‌های تقلبی به شبکه‌های اجتماعی وارد شده و با ورود به حریم خصوصی افراد مورد نظر، تصاویر و اطلاعات آن‌ها را سرقت کرده و شروع به انتشار آن‌ها نمایند. به این ترتیب، حریم خصوصی افراد، نقض می‌شود.

گوشه‌گیری و دور ماندن از اجتماعات واقعی

جامعه مجازی هیچ‌گاه جایگزین جامعه واقعی نخواهد شد، بلکه به عنوان تسهیل‌کننده تجارب اجتماعی عمل خواهد کرد. تسهیلات ارتباطی مثل اینترنت، این امکان را به ما می‌دهد که در سطح جهانی و از راه دور، با شیوه‌ای جدید به اجتماعاتی که منافع مشترک داریم، بپیوندیم. درنتیجه، با پیوستن به این اجتماعات از راه دور، قادر خواهیم بود تا در دنیای واقعی نیز روابط اجتماعی بهتری با همسایگان، همکاران و یا سایر شهروندان جامعه واقعی، برقرار کنیم.

تاثیرات منفی رفتاری

هر شبکه اجتماعی، فرهنگ ارتباطی خاص خود را دارد. یعنی منش‌ها و گفتار مخصوص و منحصر به فردی را برای خود انتخاب کرده است. البته شبکه‌های اجتماعی دیگری هم وجود دارند که در آن‌ها فرهنگ ارتباطی تقلیدی را برای خود انتخاب کرده‌اند. فرد با عضویت با هر یک از شبکه‌های اجتماعی، درگیر نوع خاصی از فرهنگ ارتباطی می‌شود که شامل برخورد، تکیه کلام، اصطلاحات مخصوص، رفتار، تیپ شخصیتی و غیره است.

بدون تردید، میزان تاثیرپذیری فرد از آن محیط، صفر مطلق نخواهد بود و هر شبکه اجتماعی، هویت مطلوب خود را ترویج خواهد کرد. مثلاً در سایت‌هایی مثل فیسبوک و توییتر، کاربر درکنار این که عضو جامعه بزرگ پایگاه مورد نظر است، در گروه و شبکه‌های اجتماعی کوچکتری عضو خواهد شد که هر یک، وابستگی‌های خاص خود و به تبع آن، فرهنگ ارتباطی خاص خود را دارند. پس فرد در تاثیر پذیری از فرهنگ ارتباطی این گروه‌ها، بر خود لازم می‌داند که هویت ارتباطی، یعنی سبک و هویت کنش‌های کلی ارتباطی خود را تغییر دهد. به طور کلی، همه اجزای یک شبکه اجتماعی که فرد با آن در تعامل است، در ضمیر ناخودآگاه فرد، تاثیر می‌گذارد.

امکانات فن‌آورانه برای جاسوسی‌های مدرن

سازمان‌ها و افراد می‌توانند با تجاوز به حریم خصوصی افراد در این شبکه‌ها، اطلاعاتی را که در حالت عادی، مجاز به دسترسی به آن‌ها نیستند، در اختیار بگیرند.

تهدیدات شبکه‌های کامپیوتری بی‌سیم

شبکه‌های بی‌سیم شخصی یا *Bluetooth*، شبکه‌های بی‌سیم شهری که به وایمکس مشهورند و شبکه‌های محلی بی‌سیم، سه طبقه رایج از شبکه‌های بی‌سیم هستند که به طور وسیع مورد استفاده قرار می‌گیرند. با توجه به رشد روزافزون کاربرد شبکه‌های بی‌سیم، شناسایی و مقابله با تهدیدات این حوزه، اهمیت ویژه‌ای پیدا می‌کند.

به دلیل انتشار آزادانه امواج بی‌سیم در محیط و سهولت دسترسی به شبکه، شبکه‌های محلی بی‌سیم معمولاً نسبت به شبکه‌های کابلی با تهدیدات بیشتری مواجه هستند. تهدیدات امنیتی اصلی شبکه‌های کابلی و بی‌سیم، یکسان هستند. اما علاوه بر این تهدیدات، تهدیدات خاصی برای شبکه‌های بی‌سیم وجود دارد که به دلیل عدم محدودیت دسترسی به شبکه‌های بی‌سیم توسط افراد و انتشار اطلاعات در فضای باز باید در نظر گرفته شوند.

تهدیدات امنیتی رایج مبتنی بر شبکه‌های کابلی و بی‌سیم را قبلاً بررسی کرده‌ایم. مثلاً تهدید جلوگیری یا ممانعت از سرویس، تهدیدی است که در آن مهاجم، استفاده عادی از منابع شبکه را برای کاربران آن مختل می‌کند. یا مثلاً در حمله جعل هویت، مهاجم با جعل هویت یکی از کاربران مجاز، حق دسترسی‌های غیر مجاز را به دست می‌آورد.

مقایسه راه‌کارهای برقراری امنیت در شبکه‌های کابلی و بی‌سیم

- در این بحث می‌خواهیم راه‌کارهای برقراری امنیت در شبکه‌های کابلی و بی‌سیم را با هم مقایسه کنیم. در شبکه‌های بی‌سیم، به دلیل این‌که بستر بی‌سیم از امواج منتشر در فضا

استفاده می‌کند، دسترسی به ارتباطات شبکه به راحتی توسط مهاجمان، امکان‌پذیر خواهد بود.

- چون افراد در شبکه‌های بی‌سیم، امکان جابه‌جایی مکانی دارند و موقعیت هر فرد به طور ثابت مشخص نیست، تغییر بسته‌های ارتباطی، به گونه‌ای که مجاز به نظر برسند، در شبکه‌های بی‌سیم به راحتی قابل انجام است.
- در شبکه‌های کابلی، مهاجم نیازمند دسترسی فیزیکی به شبکه و انجام حمله از راه دور است، در حالی که در شبکه‌های بی‌سیم، کافیست مهاجم در محدوده امواج بی‌سیم شبکه قرار بگیرد.
- شبکه‌های بی‌سیم، اغلب به طور منطقی به شبکه‌های کابلی، مرتبط هستند. لذا در شبکه‌های کابلی نیز باید تهدیدات مرتبط با شبکه‌های بی‌سیم نیز مد نظر قرار گرفته شود.

سه جنبه محرمانگی، جامعیت و دسترسی‌پذیری در شبکه‌های بی‌سیم

در حوزه امنیت شبکه، مطرح کردیم که اگر یکی از سه جنبه محرمانگی، جامعیت و دسترسی پذیری (*CIA*) نقض شود، امنیت نقض شده است. می‌خواهیم نحوه نقض جنبه‌های سه‌گانه *CIA* را بررسی کنیم.

نقض محرمانگی ***(Confidentiality)***

در شبکه‌های بی‌سیم، مهاجم با استفاده از تکنیک‌هایی سعی در نقض محرمانگی خواهد کرد. به دلیل ماهیت رادیویی و انتشار همگانی شبکه‌های بی‌سیم، تضمین محرمانگی اطلاعات در شبکه‌های بی‌سیم، به طور چشم‌گیری مشکل‌تر از شبکه‌های کابلی است. شبکه‌های بی‌سیم، امواج را در هوای آزاد منتشر می‌کنند و این، دسترسی به شبکه را بسیار آسان‌تر می‌کند. روی هم رفته، همه این عوامل، اهمیت حفظ محرمانگی در سطح مطلوب برای شبکه‌های بی‌سیم را افزایش می‌دهد.

شنود ترافیک عبوری در شبکه‌های محلی بی‌سیم می‌تواند خطر چشم‌گیری برای سازمان‌ها محسوب شود. یک مهاجم می‌تواند با اسکن سیگنال‌های بی‌سیم، داده‌های عبوری را ضبط کند. اطلاعاتی مثل شناسه‌های شبکه، کلمه‌های عبور و داده‌های مربوط به پیکربندی شبکه، نمونه‌ای از داده‌های حساسی هستند که امکان ضبط و شنود آن‌ها وجود دارد. مهاجمان مجهز به آنتن‌های گیرنده تقویت کننده، می‌توانند اطلاعات را در منطقه‌ای خارج از بورد محرمانگی شبکه، ضبط کنند. این ویژگی، اهمیت محرمانگی در تضمین امنیت را افزایش می‌دهد.

نقض جامعیت

مسائل مربوط به صحت و جامعیت داده‌ها در شبکه‌های بی‌سیم، مشابه شبکه‌های کابلی است. با توجه به این که در اغلب موارد، سازمان‌ها ارتباطات کابلی و بی‌سیم را بدون مکانیزم‌های رمزگذاری مناسب، پیاده‌سازی می‌کنند، دستیابی به صحت اطلاعات می‌تواند کار مشکلی باشد. به عنوان مثال، مهاجم با دستکاری یا پاک‌کردن محتوای یک ایمیل از طریق سیستم بی‌سیم به مخاطره بیاندازد. اگر ایمیل‌های مهم به طور گسترده در میان کاربران سازمان پخش شود، این امر می‌تواند یک تهدید جدی برای سازمان محسوب شود.

نقض دسترسی‌پذیری

خشه‌دار شدن دسترسی‌پذیری شبکه‌های محلی بی‌سیم، اغلب در نتیجه وقوع انواع حملات جلوگیری از سرویس (*Denied of service*)، مانند ارسال سیل‌آسا و ارسال پارازیت صورت می‌گیرد. علاوه بر این، کاربران هم می‌توانند با استفاده انحصاری از پهنای باند بی‌سیم، ناآگاهانه باعث نقض دسترسی‌پذیری شبکه‌های بی‌سیم شوند. دانلود فایل‌های حجیم توسط یک کاربر می‌تواند دسترسی سایر کاربران شبکه بی‌سیم را به طور موثری محدود کند.

ممانعت از سرویس توسط ارسال پارازیت

گفتیم که مختوش شدن جنبه دسترسی‌پذیری در شبکه‌های بی‌سیم، با دو نوع حمله ارسال سیل‌آسا و ارسال پارازیت، امکان پذیر است. پارازیت هنگامی اتفاق می‌افتد که سیگنال رادیویی منتشر شده از یک دستگاه بی‌سیم بر سایر دستگاه‌ها پیروز شده و ارتباطات بی‌سیم را مختل کند. پارازیت ممکن است توسط یک مهاجم مخرب یا به طور غیر عمد و به دلیل انتشار سیگنال از سوی دستگاه‌های مجازی که در طیف فرکانسی غیر استاندارد و ثبت نشده قرار دارند، صورت بگیرد. دستگاه‌هایی مثل تلفن‌ها و اجاق‌های مایکروویو، از این دسته هستند.

ممانعت از سرویس توسط ارسال سیل‌آسا

حملات ارسال سیل‌آسا توسط نرم‌افزارهایی انجام می‌شوند که برای ارسال حجم انبوهی از بسته‌های اطلاعاتی به سوی نقطه دسترسی (*Access Point*) خاصی یا سایر دستگاه‌های بی‌سیم، طراحی شده‌اند. در این شرایط، دستگاه بی‌سیم گیرنده، زیر انبوهی از بسته‌های ارسالی غرق شده و از انجام فعالیت معمول خود باز ماند. ارسال سیل‌آسا می‌تواند باعث کاهش کارایی شبکه‌های بی‌سیم به پایین‌تر از سطوح قابل قبول و یا حتی از کار افتادن این شبکه‌ها شود.