امنیت فضای مجازی و دفاع الکترونیکی

جلسه دهم

فصل دوم : امنیت فضای مجازی

۹۴/۱۱/۰۱

فصل دوم: «امنیت فضای مجازی»

۲.۱. تعریف امنیت فضای مجازی

۲.۲. تهدیدهای امنیتی فضای مجازی

تعریف اصطلاحی امنیت:

حفاظت و مقاوم‌سازی هر دارایی ارزشمند و آسیب‌پذیردر برابر تهدیدها

تعریف امنیت فضای مجازی: (امنیت رایانه / امنیت فناوری اطلاعات):

«حفاظت و مقاوم‌سازی دارایی‌های فضای مجازی در برابر تهدیدهای فضای مجازی»

دارایی‌های فضای مجازی:

۱- سخت‌افزارها

۲- نرم‌افزارها

۳-شبکه

۴- اطلاعات

۵- خدمات

۶- کاربران

۲.۲. تهدیدهای امنیتی فضای مجازی

مهمترین تهدیدهایی که ممکن است مربوطه به یک یا چند مورد از این شش حوزه باشند، عبارتند از:

۱- سرقت

۲- دسترسی

۳- جعل

۴- تغییر

۵- تخریب

۶- اخلال

	سرقت	دسترسی	جعل	تغییر	تخریب	اخلال
سخت افزار						
نرم افزار						
شبکه						
اطلاعات						
خدمات						
کاربران						

تهدیدهای امنیتی فضای مجازی

۱- سرقت

اولین تهدید که گاهی از سوی متخصصان امنیتی فضای مجازی به عنوان مهمترین تهدید امنیت فضای مجازی محسوب می‌گردد، سرقت فیزیکی سخت‌افزارهاست.

- سخت‌افزار و اطلاعات هر دو باهم سرقت رفته‌اند و بدترین شکل تهدید همین است.

همچنین است اگر امور سخت‌افزاری شبکه مثل سوئیچ‌ها یا مسیریابها به سرقت رود که آنها هم نوعی سخت‌افزار هستند.

- دارایی بودن سخت‌افزارها امری واضح و برای سنت فقهی آشناست و در کتاب الغصب از آن بحث می‌شود.

۱- سرقت

اگر کسی نرم‌افزاری را که دارای قفل یا مجوز بهره‌برداری است کپی کند یا قفلش را بشکند و از آن استفاده کند دست به سرقت نرم‌افزار زده است.

اما سرقت اطلاعات و نیز سرقت نرم‌افزار مانند سرقت محتوای کتاب، و مثل رونوشت‌گیری از یک کتاب یا افست یک کتاب چاپ شده است بحث از آن نیازمند مباحثی پویا در باب مالکیت فکری است.
از آنجا که بحث مالکیت فکری یکی از موضوعات اصلی فقه فضای مجازی است این قسمت از بحث را به آنجا موکول می‌کنیم.

از آنجا که سرقت خدمات بدون دسترسی به مواضع خدماتی ممکن نیست این بحث نیز داخل در بحث دسترسی می‌گنجد.
استراق سمع را می‌توان نوعی سرقت اطلاعات صوتی یا نوعی دسترسی غیر مجاز محسوب کرد. از این لحاظ بحث از آن داخل در بحث از سرقت اطلاعات یا دسترسی غیر مجاز به اطلاعات است.

تهدیدهای امنیتی فضای مجازی

۱- سرقت

سرقت در بخش کاربران به معنای

- سرقت هویت حقیقی
- سرقت هویت مجازی

- سرقت هویت حقیقی

مثال ۱: فردی با سرقت کارت هوشمند ملی فردی دیگر و تغییراتی در آن، هویت او را بدزد طوری که از این به بعد او را به جای فرد اصیل بشناسند.

مثال ۲- اگر کسی در بانک اطلاعات هویت ملی، هویت حقیقی فردی مثل خسرو را بدزد و به خود اسناد دهد مثلاً عکس خود را به جای عکس خسرو قرار دهد طوری که او را خسرو بدانند،

مثال ۳- همچنین اگر کسی نام کاربری و رمز عبور خسرو برای ورود به سامانه بانک را بدزدد و از طرف او پولهایی را در حسابهایی جابه‌جا کند

مثال ۴- اگر کسی در شبکه‌های اجتماعی خود را به جای یک فرد مشهور جا بزند و به جای او مطالبی را منتشر کند هویت حقیقی او را در فضای مجازی به سرقت برده است.

۱- سرقت

- هویت مجازی کاربران:

مثال ۱- فرض کنید شیرین در فضای مجازی خود را به عنوان خسرو معرفی کرده و با نام کاربری و رمز عبور خاصی در گفتگوهای اینترنتی شرکت می‌کرده است. حال اگر این نام کاربری و رمز عبور به وسیله فردی چون بابک دزدیده شود، هویت مجازی شیرین به سرقت رفته است.

۲- دسترسی

دسترسی غیر مجاز به سخت‌افزار به این معناست که فردی به صورت نامجاز به سخت‌افزارها دسترسی یابد مثلاً در اتاق کنترل مرکز داده وارد شود یا فردی به صورت غیر مجاز پشت رایانه دیگری بنشیند و تصرفی در آن سخت‌افزار انجام دهد. این کار گاهی با ورود غیر مجاز به یک منطقه فیزیکی صورت می‌گیرد و گاهی ورود مجاز است ولی استفاده از سخت‌افزار نامجاز است. مثل همکارانی که در یک اتاق کار می‌کنند ولی به هر کدام یک سخت‌افزار مستقل اختصاص یافته باشد.

حتی گاهی اخلال یا تخریبی صورت نمی‌گیرد و اطلاعات و خدماتی نیز جابجا نمی‌شود ولی فقط دسترسی نامجاز صورت می‌گیرد.

۲- دسترسی

دسترسی غیر مجاز به نرم‌افزار به این صورت محقق می‌شود که فردی که مجاز به بهره‌برداری از نرم‌افزار نیست از آن استفاده کند.

دسترسی غیر مجاز می‌تواند از طریق نصب یک درب مخفی (backdoor)درون نرم‌افزارها یا سخت‌افزارها یا شبکه‌ها صورت گیرد. از این طریق ابتدا دسترسی غیر مجاز به نرم‌افزار یا سخت‌افزار یا شبکه شکل می‌گیرد و در نهایت دسترسی غیر مجاز به اطلاعات و خدمات مربوط به یک کاربر به عمد یا خطا به کاربر دیگری منتقل می‌گردد.

والحمد لله رب العالمين