امنیت فضای مجازی و دفاع الکترونیکی

جلسه یازدهم

فصل دوم : امنیت فضای مجازی

۹۴/۱۱/۰۸

فصل دوم: «امنیت فضای مجازی»

۲,۱. تعریف امنیت فضای مجازی

۲,۲. تهدیدهای امنیتی فضای مجازی

تعریف امنیت فضای مجازی:

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

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

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

۲- دسترسی

- دسترسی نامجاز به شبکه ممکن است با یک اتصال یک سخت‌افزار نامجاز به شبکه داخلی ساختمان یا با هک کردن یک سخت‌افزار مجاز و متصل به شبکه مستقیماً یا از راه دور صورت گیرد.

- گاهی یک کاربر که دسترسی محدودی دارد با یک اقدام، دسترسی خود را به سطح بالاتری افزایش می‌دهد طوری که می‌تواند اطلاعات و خدماتی که مجاز به دریافت یا ارسال آن نبوده دریافت یا ارسال کند.

۲- دسترسی

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

مثال ۱- شخصی که مجاز به رؤیت اطلاعات نبوده اطلاعات را رؤیت می‌کند یا مطلع می‌شود که چه کسانی خدمت را دریافت کرده‌اند

مثال ۲- بیماری که به تشخیص پزشکان نباید از بیماری خود اطلاع داشته باشد، از طریق دسترسی نامجاز به اطلاعات از آن اطلاع یابد.

مثال ۳- با دسترسی نامجاز به یک نرم‌افزار بفهمد که نرم‌افزار حاوی چه نکاتی است ولو اطلاعات یا نرم‌افزار را به سرقت نبرد، و در آن اخلال یا تخریبی صورت ندهد.

۲- دسترسی

گاهی اوقات با کاری مثل استراق سمع اطلاعات صوتی و یا تصویری اشخاص به سرقت می رود.

- اگر اطلاعات صوتی تصویری را صرفاً بشنوند یا ببینند نوعی دسترسی غیر مجاز به اطلاعات صوتی تصویری صورت گرفته
- اگر آن اطلاعات را ضبط کنند و برای اغراض دیگری در جایی نگهداری کنند سرقت اطلاعات شکل گرفته و داخل در فرض سرقت است.

ممکن است هر دو فرض در یک مورد با هم رخ دهد در آن حال هم دسترسی غیر مجاز و هم سرقت صورت گرفته است. به هر حال صدق مفهوم سرقت یا دسترسی امری عرفی و تابع آنست.

۲- دسترسی

- دسترسی نامجاز ممکن است به کاربری خاص باشد.
- مثلاً اگر خسرو مایل نیست در تماس با افراد ناشناس باشد و آدرس یا تلفنش یا گروه خانوادگیش در شبکه اجتماعی، و امور شبیه به آن که به هویت خسرو مربوط است، در اختیار همگان یا افراد نامطلوب قرار گیرد.
- صرف افشای اطلاعات تلفن خسرو مصداقی از دسترسی نامجاز به خسرو نیست بلکه اگر فرد نامطلوب با او تماس بگیرد یا به گروه خانوادگیش متصل گردد، دسترسی نامجاز به کاربر محقق شده است.

- اخلال و تخریب

اخلال = خرابکاری در یک محصول به نحوی که کاری غیر از آنچه در صورت سلامت انجام می‌داد انجام دهد.

تخریب = خرابکاری در یک محصول طوری که فقط کاری که در صورت سلامت انجام می‌داد انجام ندهد.

هر دو نوعی تغییر هستند؛ تخریب تنها جلوگیری از کارکرد درست است ولی در اخلال باید کار نادرست دیگری نیز به دستگاه سپرده شود.

- تخریب و اخلال

تخریب و اخلال می‌تواند در سخت‌افزار رخ دهد. مثل آن که در دستگاه رایانه یک قطعه جاسازی کنند تا در شرائط مد نظر عملکرد دستگاه را کُند یا متوقف سازد یا حتی دستگاه را منفجر کند.

گاهی خرابکاری طوری است که ممکن است در صورت اقدامی خاص از سوی مجرمان به مشتری آسیبی وارد کند، در این حال مجرمان تلاش می‌کنند از تولید کنندگان اخاذی کنند تا جلوی این صدمات گرفته شود. بسته به این که کار خرابکاران به چه نیتی صورت گیرد موضوعات مختلفی برای بررسی فقهی اخلال و تخریب پیش خواهد آمد.

تخریب و اخلال در نرم‌افزار

تخریب نرم‌افزار به این است که کارکرد نرم‌افزار متوقف شود.

مثال ۱- مثلاً نرم‌افزار را طوری تغییر دهد که اطلاعات را ثبت نکند.

اخلال در نرم‌افزار هم متصور است .

مثال ۱- مثلاً دستوراتی در نرم‌افزار وارد کند اطلاعات ثبت شده را به طور منظم یا نامنظم تغییر دهد.

مثال ۲- مهندسی نرم‌افزار طوری باشد که مثلاً در زمان خاصی دستوری خاص را به اجرا درآورد که صدماتی به سامانه‌ها وارد آید مثلاً تاریخ دستگاه را عوض کند طوری که نرم‌افزار در زمان مورد تقاضا کارکردی نامطلوب داشته باشد.

- اخلال و تخریب

اخلال و تخریب در شبکه نیز متصور است.

تخریب در شبکه : اگر با دستکاری نرم‌افزاری یا سخت‌افزاری در شبکه، اطلاعات ارسالی در شبکه به مقصد نرسد
مثال ۱- فردی وارد ساختمان شود و سیم ارتباطی با سرور را در شبکه ساختمان قطع کند.

اخلال در شبکه: اگر اطلاعات و خدمات به جای این که به مقصد برسد به محل دیگری در شبکه منتقل شود
مثال ۱- کسی وارد ساختمان شرکتی شود و با اتصال رایانه همراه خود به شبکه، اطلاعات یا خدمات را به عنوان یک کاربر داخلی دریافت یا ارسال کند.

- اخلال و تخریب

اخلال یا تخریب در اطلاعات و خدمات نیز مشابه موارد فوق است.

در برخی از آن مثالها علاوه بر موارد فوق، اخلال یا تخریب در اطلاعات یا خدمات نیز رخ خواهد داد.

تخریب در اطلاعات و خدمات

مثال ۱- گاهی تخریب در اطلاعات و خدمات با ارسال ویروس به سامانه رخ می‌دهد طوری که اطلاعات مخدوش می‌شود و دیگر قابل بازیابی نیست یا خدمات متوقف می‌شود و سامانه پاسخگوی خدمات نیست.

- اخلال و تخریب

اخلال در اطلاعات و خدمات

مثال ۱- گاهی خدمات دولتی که به صورت الکترونیکی درآمده مورد حمله دشمنان کشور قرار می‌گیرد به این صورت که دشمنان آن قدر درخواستهای کاذب به سامانه ارسال می‌کنند که درخواست‌های واقعی با قرار گرفتن در صفی طولانی مجال تحقق نخواهند یافت و سامانه عملاً در دسترس کاربران واقعی قرار نخواهد گرفت. به این نوع اخلال در خدمات، حملات رد خدمات (DOS) گویند.

مثال ۲- گاهی این حملات چنان توزیع یافته از محل‌های بسیار متعدد و مختلفی صورت می‌گیرد که عملاً هر نوع شناسایی و مسدودسازی حمله کننده برای محافظان الکترونیکی (firewall) ناممکن می‌شود. به این نوع اخلال حملات رد خدمات توزیع‌یافته (DDOS) گویند.

والحمد لله رب العالمين