به نام خدا

وزارت ارتباطات و فناوری اطلاعات

اداره کل ارتباطات و فناوری اطلاعات استان اصفهان

جرائم سایبری

تیرماه ۹۲

مقدمه

امروزه زیرساخت فناوری اطلاعات به بخش جدایی ناپذیر زیرساخت‌های حیاتی کشور تبدیل شده است. آسیب پذیری‌های ذاتی موجود در فضای سایبری، ریسک سامانه‌های مبتنی بر فناوری اطلاعات که برای اقتصاد کشور حیاتی می‌باشند را افزایش می‌دهد. بنابراین آشنایی با انواع جرائم سایبری و هدف‌های آنها به منظور مصون سازی بستر موجود از این تهدیدات ضروری است. هدف این مقاله آشنایی بیشتر با جرائم سایبری است.

جرائم سایبری

جرائم سایبری به هر گونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و کنترل داده‌ها و نرم افزارهای رایانه‌ای و ایجاد یا وارد کردن انواع ویروس‌های رایانه‌ای و امثال آن اتلاق می‌شود.

اهداف جرائم سایبری

در فضای سایبری بسیاری از جرائم براساس هداف و انگیزه‌های مختلفی صورت می‌پذیرد که برخی از آنها شامل موارد زیر است:

- انگیزه‌های رقابتی ناسالم، انتقام جوئی و ضربه زدن به رقیب
- اهداف سیاسی
- اهداف تروریستی
- اهداف دولتی
- کسب درآمد نامشروع
- تفریح یا اندازه گیری ضریب توانائی فردی یا کنجکاوی
- آزار رسانی و کسب شهرت از طریق مردم آزاری
- جاسوسی و کسب اطلاع از وضعیت نظامی و سیاسی یک کشور یا منطقه
- رقابت ناسالم در عرصه تجارت و اقتصاد

انواع جرائم سایبری

۱- انکار خدمات[۱]: حملات انکار سرویس، حملاتی هستند که هدف اصلی آنها ممانعت از دسترسی قربانیان به منابع کامپیوتری، شبکه‌ای و یا اطلاعات است. در این نوع حملات نفوذگر تلاش می‌کند به یکی از روش‌های علمی یا عملی، مانع از سرویس دهی یک سرویس دهنده در شبکه شود. در واقع نفوذگر با ایجاد ترافیک بی مورد و بی استفاده، حجم زیادی از منابع سرویس دهنده و پهنای باند شبکه را مصرف یا به نوعی درگیر رسیدگی به این تقاضاهای بی مورد می‌کند و این تقاضاها تا جایی که دستگاه سرویس دهنده را از کار بیندازد، ادامه پیدا می‌کند.

۲- انکار گسترده خدمات[۲]: در این حملات به جای شروع حمله از یک منبع، همزمان از تعداد زیادی سامانه توزیع شده اقدام به حمله می‌شود. غالباً این کار با استفاده از کرم‌ها و تکثیر آنها در رایانه‌های متعدد برای حمله به هدف صورت می‌گیرد.

[۱] DoS (denial of service)
[۲] DDoS (distributed denial of service attack)

۳- بمب منطقی: نوعی خرابکاری که در آن برنامه نویس کدی وارد برنامه می‌کند که در صورت بروز اتفاقی خاص برنامه خود به خود یک فعالیت تخریبی را صورت می‌دهد.

۴- اسنیفر: برنامه‌ای است که داده‌های مسیریابی شده را شنود نموده و با بررسی هر بسته در جریان داده‌ها به دنبال اطلاعات خاصی مانند کلمه‌های عبور می‌گردد.

۵- اسب تراوا: برنامه‌ای است که کدی خطرناک را مخفی می‌کند. معمولاً اسب تراوا دارای ظاهری مشابه برنامه‌های مفیدی است که کاربر تمایل به اجرای آنها دارد.

۶- ویروس: برنامه‌ای است که فایل‌های رایانه‌ای که معمولا برنامه‌های اجرایی هستند را با وارد کردن نسخه‌ای از خود در آن فایل ها آلوده می‌سازد. با بارگذاری فایل‌های آلوده در حافظه، این نسخه‌ها اجرا و به ویروس امکان آلوده کردن سایر فایل‌ها را می‌دهد. ویروس ها بر خلاف کرم‌ها برای انتشار نیازمند دخالت انسانی است.

۷- کرم: برنامه‌ای رایانه‌ای مستقل که با نسخه برداری از خود از یک سامانه به سامانه دیگر در شبکه تکثیر می‌شود. کرم ها بر خلاف ویروس‌های رایانه‌ای نیازی به دخالت انسان برای انتشار ندارند.

۸- جاسوس افزار: بدافزار نصب شده بدون اطلاع کاربر برای ردیابی و یا ارسال داده‌ها به طرف سوم غیر مجاز به صورت پنهانی.

۹- شماره‌گیری مکرر: برنامه ساده‌ای که شماره تلفن‌های متوالی را شماره‌گیری می‌کند تا مودمی را پیدا کند.

۱۰- جنگ شبکه‌های بی سیم: روشی برای امکان ورود به شبکه‌های رایانه‌ای بی سیم با استفاده از یک لپ تاپ، آنتن و کارت شبکه بی سیم که شامل گشت زنی در موقعیت‌های خاص برای دسترسی غیر مجاز است.

۱۱- ارسال هرزنامه: ارسال نامه‌های پست الکترونیک تجاری ناخواسته که می‌تواند حاوی ساز و کار تحویل نرم افزارهای مخرب و سایر تهدیدات سایبری باشد.

۱۲- سرقت کلمه‌های عبور و اطلاعات مالی: با استفاده از هرزنامه افراد را فریب می‌دهد تا اطلاعات حساس خود را افشا نمایند.

۱۳- ساخت وب سایت جعلی: ایجاد یک وب سایت فریب برای تقلید از یک سایت واقعی و مشروع و معمولاً در مورد پست الکترونیک این عمل هنگامی رخ می‌دهد که نشانی فرستنده و دیگر بخش‌های مشخصات نامه الکترونیک تغییر داده می‌شود به طوری که گیرنده تصور می‌کند نامه از مبدا معتبری ارسال شده است.

۱۴- فریب: روشی که دزدان کلمه عبور برای فریب کاربران و متقاعد کردن آنها از ارتباط با وب سایت معتبر بکار می‌برند.

۱۵- بات نت: شبکه‌ای از سامانه‌های کنترل از راه دور که برای هماهنگی حملات، توزیع بدافزار و هرزنامه و پیام‌های سرقت اطلاعات بکار برده می‌شود. بات ها معمولا به صورت مخفیانه در سامانه هدف نصب می‌شوند و امکان کنترل از راه دور رایانه مورد هدف را به کاربر غیر مجاز می‌دهند تا اهداف خرابکارانه خود را محقق کنند.