هرگاه صحبت از امنیت سیستم های کامپیوتری به میان می آید خود به خود ویروس های رایانه ای خود را مطرح می کنند. ویروس ها کارکردهای متفاوتی دارند. برخی به دنبال تخریب، سرقت و یا حذف اطلاعات می باشند، برخی به دنبال مزاحمت و برخی دیگر به دنبال ضربه زدن به سیستم های حیاتی و حساس کشور و یا از بین بردن اطلاعات می باشند .

کارشناس پیشگیری از جرائم سایبری پلیس فضای تولید و تبادل اطلاعات ناجا با اشاره به این موضوع که امنیت سیستم‌های کامپیوتری فقط مختص به ویروس‌ها و تروجان‌های نیست،گفت: امنیت سیستم‌های کامپیوتری را می توان به دو بخش تقسیم کرد. سیستم‌های خانگی و شخصی، سیستم‌های سازمانی و مرتبط با حوزه کاری.

ایشان در خصوص تهدید شدن امنیت سیستم‌های شخصی و خانگی توسط ویروس‌ها و تروجان‌ها گفت:

ویروس‌ها تکه کدهایی هستند که خود را به سایر برنامه‌ها و نرم افزارها متصل کرده و با ایجاد تغییر در آن برنامه‌ها اهداف مخرب خود را که همان تخریب اطلاعات می‌باشد، عملی می‌کنند. اما تروجان‌ها و کرم‌ها بدافزارهایی هستند که به صورت مستقل عمل می‌کنند و گروهی با مخفی کردن خود در برنامه‌های دیگر، از رایانه‌ای به رایانه‌ی دیگر منتقل می‌شوند و بیشتر به دنبال سرقت اطلاعاتی از قبیل تصاویر و فایل های شخصی قربانیان می‌باشند.

وی ادامه داد:

نصب نسخه اصلی یک آنتی ویروس و نرم افزار ضد جاسوسی و فایروال مناسب می‌تواند تا حدودی تاثیرات مخرب این بدافزارها را خنثی کرد. هرچند نباید به روز رسانی مستمر این نرم افزارها را فراموش کرد. این ابزارها قابلیت شناسایی بسیاری از این بدافزارها را دارند و از نفوذ آنها به کامپیوتر شما جلوگیری می‌کنند.

این کارشناس تهیه نسخه پشتیبان را راهکاری برای باز یابی فایل های تخریب شده دانست و گفت:

در نهایت ممکن است برخلاف مراقبت‌های زیاد باز هم کامپیوتر ما مورد هجوم ویروس‌ها و تروجان‌ها قرار بگیرد بنابراین باید به دنبال راهی برای حفاظت از اطلاعات خود باشیم. آن راه می‌تواند ذخیره‌سازی فایل های مهم و حساس در رسانه‌های قابل حمل مثل کول دیسک‌ها و سی دی و ... باشد.

این مقام آگاه در ادامه به رمز نگاری پوشه ها و فایل‌ها اشاره و تاکید کرد:

هر چند ذخیره سازی بر روی فایل‌های قابل حمل می تواند از دسترسی سود جویان سایبری جلوگیری نماید ولی در مورد سرقت فیزیکی نمی تواند موثر باشد. اگر فایل‌ها و پوشه‌ها به صورت پیشرفته رمزگذاری شوند امکان دستیابی به اطلاعات را حتی برای کاربران حرفه ای سخت می‌کند.

ایشان ادامه داد: از دیگر تهدیداتی که سیستم‌های خانگی را مورد هجوم قرار داده است می توان به نفوذ افراد غیر مجاز به کامپیوترهای خانگی و تغییر فایل ها، استفاده از کامپیوترهای خانگی برای تهاجم علیه دیگران، سرقت اطلاعات حساس نظیر شماره کارت اعتباری و خرید غیر مجاز اشاره کرد.

به گفته ایشان با رعایت برخی نکات می توان احتمال بروز و یا موفقیت این نوع از حملات را در کامپیوترهای خانگی به حداقل رساند.

وی امنیت در سیستم های اداری و کاری را نیز بسیار مهم و حیاتی دانست و افزود:

بخش بزرگی از امنیت اطلاعات مهم و محرمانه در محیط کار بر عهده مسئولین IT مثل شبکه های کامپیوتری، امنیت نرم افزار و بانک اطلاعاتی و... است و حفاظت فیزیکی سیستم های اداری با حراست ادارات می باشد.

کارشناس پلیس فتا راه اندازی شبکه داخلی یا اینترانت را یکی از راه کارهای موثر در بالا بردن میزان امنیت سیستم های کاری دانست و گفت:

اینترانت شبکه‌ای محلی و محدود بوده که برای یک موسسه یا شهر، شرکت یا کلاً یک فضای کوچکتر تعریف می شود که برای ورود به آن باید نام کاربری و رمز عبور داشته باشیم. همین امر می تواند تا حد بسیار زیادی تضمین کننده امنیت این شبکه باشد. هدف اصلی از ارائه این سرویس ایجاد زیرساختی اختصاصی و مستقل از اینترنت جهت تبادل اطلاعات و به اشتراک گذاری است.

ایشان ادامه داد: مدیران IT باید نسبت به محرمانگی(اطمینان از اینکه اطلاعات فقط در دسترس افراد مجاز قرار دارد(، صحت(تامین صحت، دقت و کامل بودن اطلاعات و روشهای پردازش آنها)، دسترس پذیری(اطمینان از اینکه کاربران مجاز در صورت نیاز به اطلاعات و دارائیهای مربوطه به آنها دسترسی دارند) اهتمام داشته باشند.

وی توصیه نمود: در صورت ذخیره سازی اطلاعات حساس و مهم کاری می‌توان از حافظه های جانبی از قبیل هارد های اکسترنال، فلش مموری ها و یا لوح های فشرده استفاده نمود. البته حفاظت فیزیکی این حافظه ها نیز بسیار مهم و حیاتی است که نباید این قبیل اطلاعات دسته بندی شده مهم که بر روی سی دی فلش مموری یا هارد اکسترنال ذخیره شده در دسترس عموم کارکنان باشد.

ایشان با اشاره به لزوم استفاده از سیستم های حفاظتی سخت افزاری و نرم افزاری گفت:

انتصاب و تعیین افرادی به عنوان مسئول کنترل، حفاظت وپشتیبانی نرم افزارها، تهیه نرم افزارهای پشتیبان و حفاظت آنها، تنظیم لیست برنامه های حیاتی و مهم سازمان و ذخیره سازی و نگهداری اطلاعات و برنامه های حساس و مهم از جمله اقدامات پیشگیرانه در جهت بالا بردن امنیت می باشند.

این فرد آگاه با اشاره به اینکه روزانه اخبار جدیدی از نفوذ و حملات صورت گرفته به سیستم های رایانه ای در رسانه ها منتشر می شود، افزود:

اگر کاربران و مسئولین it نکاتی جزئی را در مورد سیستم‌های اداری تحت نظر خود رعایت کنند تا حدود زیادی امنیت سیستم های اداری تامین می گردد. نکاتی از قبیل :

- باز نکردن نامه ها و ایمیل های دریافتی از منابع ناشناس
- خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه
- قطع اتصال به اینترنت در مواقع عدم استفاده
- گرفتن منظم وصله های امنیتیPatches
- حصول اطمینان از آگاهی کاربران از نحوه برخورد با کامپیوترهای آلوده

- بررسی مرتب میزان دریافت و ارسال اطلاعات

ایشان با اشاره به ضروری بودن ارائه آموزش‌های لازم به کاربران و مدیران IT گفت: پلیس فتا همواره رویکرد پیشگیرانه و آموزشی را در صدر وظایف خود قرار داده است و در این زمینه کارگاه‌های آموزشی متعددی برگزار نموده است .مطالب آموزشی، کلیپ های تصویری، اطلاع رسانی‌ها در قالب هشدارهای پلیسی نیز در سایت www.cyberpolice.ir در اختیار عموم قرار گرفته است.

وی در انتها به کاربران اینترنت توصیه کرد:

کامپیوتری که در محل کار خود استفاده می‌کنید را محدود به انجام کارهای محل کارتان کنید؛ زیرا در هنگامی که کاربران به اینترنت متصل می‌شود افراد سودجو در کمین شما هستند و می‌توانند از این ابزار سودمند استفاده ناصحیح کرد و با طراحی نرم افزارهای مخرب و ویروس‌ها به دیگر سیستم‌ها ورود غیر مجاز داشته باشند و به دنبال اهداف مخرب خود باشند.

منبع :

پایگاه اطلاع رسانی پلیس فتا