بسمه تعالی

در طول دو دهه اخیر، پست الکترونیکی یکی از ابزارهایی است که رسانه های ارتباطی را رهبری می کند، و حتی جانشین تلفن و نامه فرستادن های سنتی شده است. متاسفانه در طول همین مدت زمانی، پست الکترونیکی خود را در برابر تهدیدات بیرونی بسیار آسیب پذیر نشان داده است، از جمله افراد و سازمان هایی که بدنبال آسیب زدن به برخی فن آوری ها هستند یا در تلاش برای درآمد از طریق روش های غیرقانونی هستند. در نتیجه، امنیت برای کاربران پست الکترونیکی از اهمیت فراوانی برخوردار گشته است.

تهدیدات پست الکترونیکی

اگر چه امنیت پست الکترونیک اغلب به عنوان یک موضوع واحد در نظر گرفته می شود، اما در واقع این موضوع یکی از انبوه تهدیداتی است که کار آن فرد ازکار انداختن کامپیوتر، کلاهبرداری، تضعیف اثربخشی و قابلیت اطمینان پست الکترونیکی است.تهدیدات پست الکترونیکی می تواند به دسته های مختلفی تقسیم گردد:

•**ویروس ها، کرم ها و تروجان ها :** دریافت پست الکترونیکی حامل ضمیمه، کد مخرب می تواند داده های سیستم میزبان را از بین ببرد، کامپیوتر را تحت کنترل یا اصطلاحاً (Slave) کامپیوتر دیگری در آورد، کامپیوتر دریافت کننده را بوت کند یا باعث ضرر مالی شدیدی به وی شود.

•**فیشینگ :** حملات فیشینگ جهت سرقت اطلاعات شخصی یا داده های مالی افراد توسط سارقان سایبری صورت می گیرد. این گونه حملات با تکیه بر جعلی بودنشان، به طور مستقیم به آدرس دریافت کننده ارسال می گردند، تا آن ها را به سایت های جعلی که برای فریب آنها جهت دریافت اطلاعات مالی محرمانه شان(همچون شماره کارت اعتباری، نام های کاربری، کلمه عبور و سایر اطلاعات محرمانه شخصی) طراحی کرده اند وصل نمایند. عاملان فیشینگ معمولا تحت عناوین ساختگی و بصورت مخفیانه فعالیت می کنند تا بتوانند از این طریق از بانک ها، تجار و شرکت های صادر کننده کارت های اعتباری سرقت نمایند.

•**هرزنامه :** اگرچه به مانند پست الکترونیکی های حامل ضمیه های ویروسی تهدید آشکاری محسوب نمی گردند، اما این پست الکترونیکی های ناخواسته می توانند به سرعت صندوق پستی شما را پر کنند، و گاها یافتن پست الکترونیکی های شخصی و کاری شما را بسیار سخت یا غیر ممکن می سازد. مشکل هرزنامه ها برخی اوقات کاربر را مجبور می کند بجای اینکه به مقابله با این مشکل بپردازد حساب کاربری اش را رها کند. هرزنامه معمولا توسط عاملان فیشینگ و ویروس ها ارسال می گردد. روزانه بیش از ده ها میلیارد هرزنامه به پست الکترونیکی کاربران ارسال می گردد.

تدابیر حفاظت از پست الکترونیکی

حراست از پست الکترونیکی کاربران و سیستم هایشان در مقابل مهاجمان و هکر ها نیاز به چند ابزار امنیتی دارد که عبارتند از :

•**سرویس گیرنده امنیتی : (Client Security)**عملا تمامی سرویس گیرندگان اصلی پست الکترونیکی اکنون تنظیمات امنیتی را ارائه می کنند، به تازگی ابزارهای ضد-هرزنامه، فیلترینگ فیشینگ ها و سایر ویژگی هایی که برای به دام انداختن و جداسازی پیام های پر مخاطره قبل از اینکه اثرات مخربی بر روی سیستم بگذارند، طراحی شده اند. کاربران بایستی در مورد این ویژگی ها بررسی های لازم را صورت دهند و از آنها بعنوان اولین سد دفاعی استفاده کنند.

•**دیواره ی آتشین : (Firewall)**دیواره آتشین می تواند امنیت پست الکترونیکی را از طریق فیلتر کردن فایل ضمیمه حاوی تروجان و نیز دیگر پست الکترونیکی های ناخواسته که تنظیمات از پیش تعیین شده آن ها را برآورده نمی کند، تقویت کند.

•**رمزگذاری : (Encryption)**نرم افزارهای رمزگذاری کامل نیستند، اما حتی بهترین محصولات با سریعترین پردازنده ها و بیشترین فضای ذخیره سازی از آن ها استفاده می کنند. البته گاها کاربران رمز خود را فراموش و یا گم می کنند. رمزگذاری می تواند توسط دیواره ی آتشین یا سایر نرم افزار های امنیتی مدیریت شود.

•**ابزارهای آنتی ویروس :** محصولات و خدمات آنتی ویروس ها عمدتا کارشان را برای شناسایی و حذف ویروس ها، تروجان ها و کرم ها به خوبی انجام می دهند.

•**فیلتر هرزنامه :** یک فیلتر هرزنامه ی خوب می تواند به خوبی تفاوت پست الکترونیکی های عادی را از هرزنامه ها تشخیص دهد، و صندوق پستی شما را از مقدار بسیار زیادی از هرزنامه ها پاک کند.

•**آموزش :** آموزش یکی از اولین اصول حراست از پست الکترونیکی است. کاربرانی که از تهدیدات پست الکترونیکیی آگاهی دارند، کمتر از دیگران در معرض حملات ویروسی، لینک های فیشینگ و سایر فعالیت های توام با ریسک قرار می گیرند.

منبع itsecurity