به نام خدا

پدافند غیر عامل باید همچون شعله ای بلند شود.

مقام معظم رهبری

ملاحظات پدافند غیرعامل در پست الکترونیکی

فهرست:

مقدمه

مجموعه اقدامات غیرمسلحانه که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان ها و تأسیسات، تجهیزات و شریان های کشور در مقابل عملیات خصمانه و مخرب دشمن می گردد، پدافند غیرعامل نامیده می شود. از این منظر، هر عامل خارجی که بطور رسمی تحت کنترل مدیریت حوزه نمی باشد، اما بهره برداری از آن موجب افزایش توانمندی و موفقیت، و عدم توجه بموقع به آن سبب از دست رفتن موقعیت های مناسب و افزایش هزینه ها می شود، «فرصت» و هر عامل موثری که رسماً تحت کنترل مدیریتی حوزه نبوده؛ لیکن پرهیز از آن موجب مصون ماندن توانمندی ها و موفقیت ها، و عدم توجه بموقع به آن موجب بروز خسارات و لطمات می گردد «تهدید» تلقی می گردد.

امروز فناوری اطلاعات و ارتباطات شریان اصلی اطلاعات و کنترل بشمار می آید و از همین رو می بایست از طریق شناخت نقاط قوت، ضعف و فرصت های ملی مان در این حوزه، از فرصت ها در جهت نیل به افزایش توانمندی ها استفاده کنیم و مانع تبدیل آن ها به تهدید شویم. اگر امنیت شبکه برقرار نگردد، مزیت های فراوان آن نیز حاصل نخواهد شد و همگان در معرض دستکاری و سوءاستفاده‌های مادی و معنوی قرار می گیرند، از سوی دیگر

حملات سایبر توسط گروه های سازماندهی شده بین‌المللی، سبب اختلال در امنیت ملی و تهدیدی جدی محسوب می‌شود. در کشور ما از آنجاکه بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکت های خارجی تهیه می‌شود، این موضوع بصورت مسئله‌ای استراتژیک درمی آید که نپرداختن به آن باعث بروز خساراتی بعضاً جبران‌ناپذیر خواهد شد. بنابراین می بایست به فناوری های نوین امنیتی شبکه مجهز بوده و از امکانات آن بصورت امن، ایمن و پایدار استفاده نماییم؛ از آنجاکه انتقال فناوری به صورت خرید محصولات نرم‌افزاری یا سخت افزاری قابل دستیابی نمی باشد، می‌بایست محققین کشور این مهم را بدست گیرند و بمنظور بومی نمودن این فناوری ها فعالیت نمایند.

پست الکترونیکی به مثابه یک فرصت، از مهمترین، فراگیرترین و کاربردی ترین سرویس های تحت شبکه می باشد. در این کتابچه سعی بر آن است تا با بررسی و شناساندن آن گامی در جهت کاهش تهدیدات ناشی برای کشور و منابع اطلاعاتی برداشته شود.

فصل ۱ – تاریخچه

تاریخ پست الکترونیکی را می توان به قدمت شبکه آرپانت[۱] یا اینترنت امروزی دانست. ایده پست الکترونیکی از فعالیت های بسیار ساده پرورش و توسعه پیدا نموده است. اولین سامانه پست الکترونیکی چیزی شبیه به پیاده سازی یک سامانه مدیریت شاخه فایل قابل دسترسی از طریق شبکه بود؛ این سامانه پیام را از شاخه کاربر فرستنده در یک رایانه بزرگ[۲] به جایی روی همان سامانه که توسط کاربران مقصد پس از ورود قابل مشاهده باشد، انتقال می داد. پس از ایجاد توانایی برقراری ارتباط و صحبت در رایانه های متصل به شبکه، موضوع ابعاد تازه تری پیدا نمود: در یک شبکه رایانه ای نیز دقیقاً همانند پست معمولی مفهومی برای اشاره منطقی به کلیت یک نامه (پاکت) و روشی برای نشان دادن و تمایز آدرس رایانه ها از یکدیگر مورد نیاز بود.

«ری تاملینسون[۳]» در سال ۱۹۷۲ سمبل @ از صفحه کلید را برای تفکیک پیام های ارسالی از یک رایانه به رایانه دیگر برگزید و طرح

---

[۱] Advanced Research Projects Agency Network توسط دپارتمان دفاعی امریکا در زمان جنگ سرد و بمنظور ایجاد راه های جدید برای حملات توسعه پیدا نمود. رایانه های مورد استفاده در این شبکه بعدها به پایه های اصلی شبکه اینترنت تبدیل شدند.

[۲] Main frame

[۳] Ray Tomlinson

آدرس دهی رایانه ها و کاربران را ارائه نمود.

نام رایانه کارگزار پست الکترونیکی @ نام کاربر

سرویس پست الکترونیکی با ایجاد یک تغییر ریشه ای در هدف آرپانت، نقش ناجی را برای آن ایفا نمود. محصولات بسیاری بسرعت به سبب این سرویس توسعه یافتند. با ظهور بسته های تجاری در سال ۱۹۷۶، ظرف مدت دو سال ۷۵٪ ترافیک آرپانت را نامه های الکترونیکی تشکیل می دادند.

پست الکترونیکی مسیر تحولات شبکه را از آرپانت بسمت اینترنت تغییر داد. این سرویس نیاز عده زیادی از مردم بمنظور برقراری ارتباط سریع و ارزان را برطرف می نمود .

نخستین استاندارد مهم تبادلات در پست الکترونیکی SMTP[۱] نامیده شد. این پروتکل، بسیار ساده بوده و هنوز هم استفاده می شود. SMTP هیچ تلاشی بمنظور شناسایی ارسال کننده نامه الکترونیکی انجام نمی دهد و به همین دلیل جعل آدرس های ایمیل از گذشته تا به حال بسیار ساده بوده است. این مشکل اساسی بعدها سبب بهره برداری ویروس ها، کرم ها، کلاهبرداران و تولید کنندگان

[۱] Simple Mail Transport Protocol

هرزنامه ها گردید. POP[۱] نیز از دیگر استانداردها در پست‌الکترونیکی است که نقش مهمی در توسعه نحوه ارتباط کاربران سامانه های پست الکترونیکی با یکدیگر داشته است.

در مسیر توسعه پست الکترونیکی ابزار و امکانات جدیدی همچون فهرست پستی، گروه خبری و کنفرانس الکترونیکی ایجاد شده اند. هم اکنون در تار جهان گستر[۲]، شرکت هایی همچون Yahoo، Google[۳] و Microsoft[۴]، سرویس پست الکترونیکی را همراه با رابط های کاربری زیبا، پرقدرت و بصورت رایگان به تمام نقاط جهان ارائه می دهند. در کشور ما نیز هرچند آمار دقیقی از تعداد کاربران این نوع شرکت ها موجودنیست، اما به جرأت می توان هر ایرانی را صاحب حداقل یکی از این حساب های کاربری دانست و متأسفانه بدون آگاهی کافی در نحوه استفاده و بدون توجه به میزان امنیت سرویس ارائه شده و سرویس دهندگان آن، اغلب اطلاعات به سوی میزبان های خارجی ارسال می گردد. هم اکنون برخی سازمان ها و ارگان ها در داخل کشور اقدام به ارائه خدمات

---

[۱] Post Office Protocol

[۲] World Wide Web (WWW)

[۳] ارائه کننده سرویس Gmail

[۴] ارائه کننده سرویس Hotmail

پست الکترونیکی بصورت محدود نموده اند که می توان به پورتال iran.ir اشاره نمود.

فصل ۲ – آشنایی با پست الکترونیکی

پست الکترونیک یا آنچه ما امروز تحت عنوان ایمیل از آن صحبت می کنیم، سال‌هاست که به یکی از پرکاربردترین ابزارهای ارتباطی بمنظور ارسال پیام تبدیل شده است. سهولت، سرعت و قابلیت های ویژه استفاده از پست الکترونیکی، این روش ارتباطی را بی بدیل نموده است.

پست الکترونیکی سرویسی تحت شبکه می باشد که باعث انتقال پیام های الکترونیکی از یک کاربر به کاربران دیگر می‌گردد. این نامه ها در مخزنی در شبکه ذخیره و با روش های مختلف تحویل مقصد می گردند.

پست الکترونیکی در شرایط عادی هیچ گونه امنیتی ندارد، مهاجم در این میان می تواند محتوای نامه الکترونیکی شما را بخواند!

سرویس ایمیل یا پست الکترونیکی یکی از مهمترین و پرکاربردترین خدمات تحت شبکه محسوب می شود و توسط آن قابلیت ارسال و دریافت هرنوع پیام اعم از متن، تصویر، صوت و ... به شکل الکترونیکی امکانپذیر است. این سرویس با دیگر خدمات ارتباطی تحت شبکه از قبیل FTP[۱] یا Telnet[۲] که دارای خدمت‌گیرنده/خدمت دهنده دوطرفه بین کاربر و منبع شبکه بوده و یک ارتباط دوسویه برقرار می‌سازند تفاوت بنیادی دارد؛ چراکه اساس این سرویس بر «ذخیره و ارسال» استوار است.

پست الکترونیکی شباهت های بسیاری به پست معمولی دارد. این سامانه در شبکه‌های مختلف و اینترنت، بین رایانه‌ها ارتباط غیر همزمان بوجود می آورد، به عبارت دیگر فرستنده هر وقت بخواهد پیام خود را ارسال و گیرنده هرزمان بتواند آن را دریافت می کند و لازم نیست فرستنده و گیرنده پیام، ارتباط همزمان داشته باشند.

---

[۱] File Transfer Protocol روشی محبوب جهت انتقال فایل ها روی شبکه می باشد. در این روش رایانه های مبدأ و مقصد می بایست ارتباط برخط داشته باشند.

[۲] روشی برای شبیه سازی محیط یک رایانه از راه دور می باشد. به این ترتیب امکان ورود کاربر از طریق شبکه به رایانه دیگری که با شبکه ارتباط برخط داردو تحت کنترل گرفتن فراهم می‌شود.

گرچه امروزه امکان اضافه کردن پیوست[۱]های مختلف به پیام های الکترونیکی وجود دارد اما ایمیل اساساً چیزی جز یک متن ساده نیست و همچنان این نوشته‌ها هستند که محتوا را تشکیل می‌دهند.

سامانه پست الکترونیک بطور کلی از دو بخش مشتری و کارگزار تشکیل می گردد. در ادامه شرح مختصر این دو قسمت بیان شده است.

❖ **مشتری پست الکترونیکی(Email client)**

مشتری پست الکترونیکی ابزاری برای خواندن، نوشتن و ارسال پست الکترونیکی است و به عبارت ساده تر یک رابط کاربری برای سامانه پست الکترونیک می باشد. این ابزار، برنامه ای مرکب از یک ویرایشگر متن ساده، دفترچه آدرس، قفسه بایگانی و ماژول های ارتباطی است.

وظیفه اصلی یک مشتری پست الکترونیکی برقراری ارتباط با کارگزار و ارسال پیام می‌باشد. امکان ارسال پیام بصورت رمز شده، امضای دیجیتال و تصدیق آن از دیگر امکاناتی است که بمنظور ارائه سرویس امن می بایست در مشتری تعبیه شده باشد.

---

[۱] Attachment

با استفاده از تکنیک های خاص هرکسی می تواند پیام هایی را ارسال کند که به نظر می رسد از طرف شما ارسال شده است!

- نرم افزارهای سرویس گیرنده:

این نرم افزارها روی سامانه کاربر نصب و با اتصال به کارگزار پست، امکان ارتباط را فراهم می سازند. Outlook Express شاید از آشناترین و در عین حال نامطمئن ترین نرم افزارهای مشتری ایمیل باشد.

درصورت استفاده از این نرم افزارها، با توجه به نقش اساسی آن ها در تبادلات شخصی و استفاده آن ها از منابع سیستمی می بایست از نرم افزاری امن، پایدار و قابل اعتماد استفاده نمود.

- سامانه های وب مبنا[۱]:

در این روش یک درگاه تحت وب بعنوان رابط کاربر و کارگزار مورد استفاده قرارمی گیرد.با توجه به ارائه پرقدرت این سرویس از سوی سایت های بزرگ ارائه دهنده خدمات رایگان پست الکترونیکی همچون Yahoo و

---

[۱] Web-base

Google و سهولت استفاده از آن ها، سامانه های وب مبنا محبوبیت و عمومیت فراوانی یافته است. در این روش سعی می شود تا همان محیط نرم افزاری نوع اول همراه با ویژگی های کامل مدیریتی از طریق درگاه وب به کاربر عرضه شود.

در استفاده از این روش ارتباط امن، ایمن و پایدار[1] رایانه کاربر و درگاه و اطمینان از امن و پایدار بودن درگاه و ارائه دهنده سرویس اهمیت فراوانی پیدا می کند.

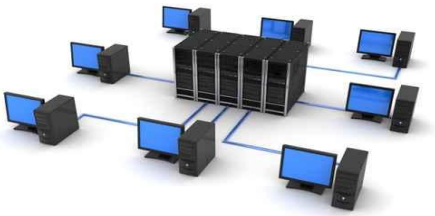
گیرندگان پیام الکترونیکی می توانند پیام دریافت شده را در سطح سازمان شما و یا حتی در سطح شبکه جهانی پخش کنند!

❖ **کارگزار پست الکترونیکی**

هر کارگزار پست الکترونیکی بمنظور ارسال و دریافت پیام، دارای ارتباطی دوسویه با مشتری های پست الکترونیکی و دیگر کارگزارهای پست الکترونیکی است و نقش اصلی را در سامانه پست الکترونیکی ایفا می نماید.

هر کارگزار پست الکترونیکی معمولاً شامل یک فضای حافظه، یک مجموعه قوانین تعریف شده برای کاربران، لیستی از کاربران و ماژول های ارتباطی می باشد.

از پر اهمیت ترین بخش های یک سامانه پست الکترونیکی، تیم پشتیبانی آن می باشد. این تیم همواره رفتار کاربران و وضعیت سرویس های کارگزار پست را رصد کرده و ضامن سرویس دهی مناسب سامانه می‌باشد. تیم پشتیبانی وظیفه بروز نگهداشتن کارگزار، جلوگیری از وقفه در سرویس دهی و مقابله با حملات محتمل را برعهده دارد. در عصر حاضر هیچ کارگزار پست الکترونیکی بدون بهره مندی از تیم پشتیبانی پرقدرت، قادر به ارائه سرویس مطلوب نخواهد بود.



❖ **مزایا و ویژگی ها:**

بطورکلی پست الکترونیکی به عنوان یکی از ابزارهای مهم ارتباطی دارای مزایا و ویژگی‌هایی است که اهم آنها عبارت‌اند از:

- امکان ارتباط همزمان چند کاربر
- امکان ارسال همزمان پیام برای چند کاربر
- امکان عضویت در گروههای مباحثه، گروههای خبری و فهرست های پستی
- عدم نیاز به ارتباط مستقیم و رو در رو
- امکان ذخیره و در صورت لزوم تغییر پیام ها
- سرعت بالای ارسال و دریافت پیام ها
- پایین بودن هزینه
- حذف محدودیت‌های زمانی و جغرافیایی
- سهولت و سرعت

فصل ۳ – معماری و پروتکل های ارتباطی

کارگزارها و مشتری های پست الکترونیکی به منظور ارسال و دریافت پیام از پروتکل‌های SMTP ، POP۳ یا IMAP[۱] و استاندارد MIME[۲] استفاده می کنند.

بطورکلی SMTP، وظیفه انتقال نامه از سامانه مشتری به کارگزار پست الکترونیکی مقصد را برعهده دارد؛ نامه فرستاده شده توسط پروتکل های IMAP یا POP۳ تحویل کاربر نهایی خواهد شد. دلیل عدم استفاده از SMTP بمنظور دریافت نامه ایجاد امکان ارسال و دریافت غیر هم زمان می باشد.

استاندارد MIME نیز پس از ۸۲۲ RFC[۳] و به دلیل ضعف در ارسال فایل های ضمیمه ارائه و مورد استفاده قرار گرفت. استاندارد MIME کاملاً با ۸۲۲ RFC سازگار می باشد.

❖ **ارسال نامه:**

بمنظور ارسال یک پیام الکترونیکی مشابه آنچه در پست معمولی رخ می دهد،

---

[۱] Internet Message Access Protocol

[۲] Multi-purpose Internet Mail Extension

[۳] Request For Coment

برنامه مشتری بایستی با یک دفتر پستی ارتباط برقرار کند. این دفتر پست، کارگزار SMTP یا همان «قرارداد ساده انتقال نامه» می باشد. اگر برنامه مذکور، وبمیل[۱] باشد، کاربر ابتدا از طریق پروتکل های وب با کارگزار وبمیل ارتباط برقرار و کارگزار وبمیل با اتصال به کارگزار SMTP پیام را ارسال می نماید.

کارگزار SMTP ابتدا برای بررسی آدرس مقصد نامه به کارگزار DNS[۲] متصل می‌شود. اگر آدرس دامنه گیرنده مشابه دامنه فرستنده باشد، پیام را به کارگزار POP۳ یا IMAP که وظیفه ارائه پیام به کاربر را دارند تحویل می‌دهد؛ در غیر اینصورت باید با کارگزار SMTP دامنه دیگر ارتباط برقرار کرده و نامه را به آن تحویل دهد. نحوه کار به این صورت است که پس از برقراری اتصال، ماشین فرستنده منتظر ماشین گیرنده می ماند. گیرنده متنی را

---

[۱] در Web mailها برای ورود به حساب کاربری، از شبکه اینترنت استفاده می شود.

[۲] Domain Name Server قسمتی از اینترنت است که دربرگیرنده بانک اطلاعاتی از نام دامنه‌ها و آدرس IP آنهاست. DNS نام دامنه را به آدرسIP تبدیل می کند.

که حاوی هویت خود و مشخص کننده آمادگی برای دریافت پست الکترونیکی می باشد ارسال و اگر آماده دریافت پیام نباشد، اتصال را پس از ارسال متن قطع می نماید. در غیر اینصورت مشتری، مبدأ و مقصد پیام را اعلام و سپس پیام را ارسال می کند. اگر در این میان کارگزار ارسال نامه با مشکلی مواجه شود، پیام فرستاده شده به لیست انتظار اضافه و بطور مرتب برای کارگزار مقصد فرستاده می شود، درصورتیکه بعد از مدت معینی پیام مربوطه به مقصد نرسد، SMTP کاربر را مطلع و پیام را از لیست انتظار خارج می کند.

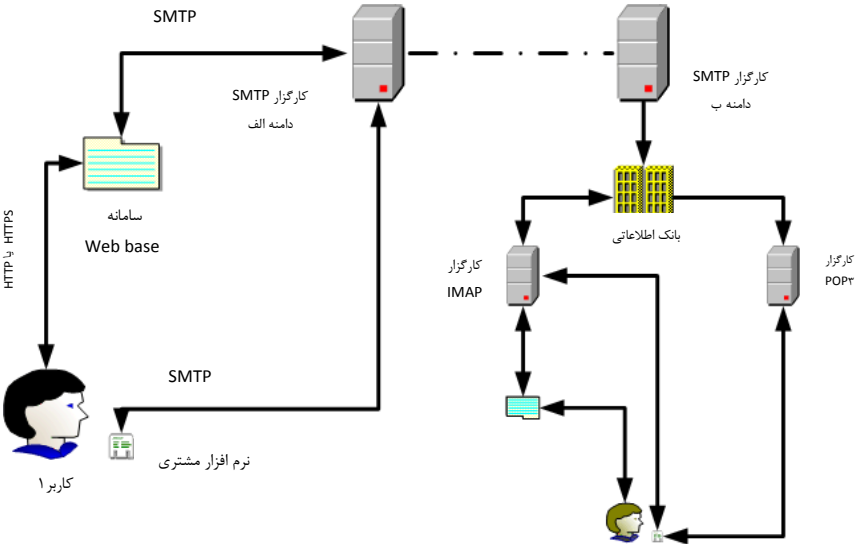
❖ **دریافت پیام:**

از آنجا که سامانه مشتری نمی تواند همواره به شبکه متصل و آماده دریافت پیام باشد؛ استفاده از SMTP برای رساندن پیام مورد نظر به کاربر نهایی امکانپذیر نمی باشد. از اینرو بمنظور دریافت پیام از پروتکل های POP۳ و IMAP استفاده می گردد.

- POP۳ یا قرار داد دفتر پستی؛ حاوی دستورالعمل هایی برای برقراری اتصال، قطع اتصال، دریافت و حذف پیام می باشد. کارگزار POP۳ با هر بار اتصال، تمام پیام ها را به صورت یک فایل به رایانه کاربر فرستاده و اطلاعات کاربر

را از روی کارگزار پاک می‌کند. به این ترتیب پیام ها از طریق سامانه کاربر قابل مشاهده خواهند بود .

- IMAP یا قرارداد دستیابی پستی محاوره ای؛ با استفاده از سامانه مرکزی ذخیره داده کلیه پیام ها را در کارگزار نگه داشته و در صورت ورود کاربر، به وی امکان دسترسی، حذف و ویرایش می دهد. بنابراین IMAP برخلاف POP۳، نامه ها را به سامانه شخصی کاربر انتقال نمی دهد. در نتیجه کاربر می تواند از رایانه های مختلف به کارگزار متصل شده و پس از انجام عملیات احراز هویت، پیام ها را مشاهده نماید.



ارسال نامه «کاربر۱ از دامنه الف» به «کاربر ۲ از دامنه ب»

❖ **استاندارد MIME:**

نخستین ساختار نامه های الکترونیکی براساس RFC ۸۲۲ شکل گرفت. این استاندارد که ساختار یک نامه الکترونیکی کاملاً متنی را تعریف می نمود، سال ها بعنوان استاندارد قالب نامه های الکترونیکی مورد استفاده قرار می گرفت. با وجود کامل و جامع بودن استاندارد فوق الذکر، بدلیل محدودیت های آن شامل عدم حمایت از حروف غیرلاتین و ارسال داده غیر متنی کنار گذاشته شد.

ایده اصلی استاندارد MIME، ابداع روشی بود که بتوان فایل‌های غیرمتنی را بگونه‌ای در بدنه نامه قرار داد تا توسط سرویس‌دهنده‌های قدیمی نیز قابل ارسال و دریافت باشد. استاندارد MIME ضمن پشتیبانی از RFC ۸۲۲، نواقص آن را برطرف و الگویی را برای سازماندهی اطلاعات با ماهیت متفاوت (شامل داده‌های چندرسانه‌ای) در قالب یک ساختمان داده واحد و کاملاً متنی ارائه داده است.

هم‌اکنون بمنظور ارسال فایل همراه نامه الکترونیکی، اطلاعات فایل‌ها به صورت باینری درآورده شده و بصورت متنی ارسال می گردد این‌عمل‌در مقصد بصورت عکس رخ‌می‌دهد.

فصل ۴ – تهدیدات و مخاطرات ناشی از پست الکترونیکی

به نظر می رسد امروزه طراحی حملات به پست های الکترونیکی ساده تر، کاراتر و پردامنه تر از دیگر حملات اینترنتی می باشد. مهاجم می تواند قبل از رسیدن پیام به مقصد مانع ردوبدل شدن آن شود، آن را شنود کند و یا تغییر دهد. پست الکترونیکی راه ساده ای جهت پراکندن محتویات مضر نظیر بدافزارها پیش روی مهاجمان قرار داده است.

پست الکترونیکی همواره می تواند راه مناسبی جهت بدست آوردن اطلاعات، نفوذ و بدست گیری کنترل رایانه یا کارگزار هدف باشد. با وجود اهمیت این موضوع، سازمان ها اغلب در ارائه آگاهی به کارکنانشان درخصوص این نوع مخاطرات کوتاهی می کنند. متأسفانه گاهی کارمندان و مدیران بدون آگاهی از میزان امنیت سرویس مورد استفاده، از پست الکترونیکی بمنظور ارسال اطلاعات محرمانه یا به اشتراک گذاری داده های حساس داخل سازمانی استفاده می کنند. یک کاربر سرویس پست الکترونیکی باید بداند تشخیص مکان جغرافیائی ارسال کننده نامه الکترونیکی از طریق آدرس IP وی براحتی امکان پذیر است و یا احتمال نفوذ به حساب کاربری

فردی که از رایانه های نا مطمئن برای ورود به صندوق شخصی خود استفاده می کند، بسیار محتمل است.

جالب است بدانید طی خبری که از سوی Computer Sweden اعلام گردید در یک حمله اینترنتی به سفارتخانه ها و مراکز دولتی کشورهای سراسر دنیا تعداد بسیاری آدرس ایمیل همراه با نام کاربری و کلمات عبور آن بر روی اینترنت قرار گرفت. در این خبر آدرس پست الکترونیکی مراکز دولتی کشورهای ایران، هند، قزاقستان، ازبکستان، انگلستان و روسیه به چشم می خورد و سفارت روسیه در استکهلم این خبر و درستی اطلاعات به سرقت رفته را تأیید و اعلام نموده تمامی اطلاعات ورودی تغییر یافته اند. این خبر خود نشانگر عدم دقت کافی کاربران در حفاظت از آدرس های پستی و غیر قابل اعتماد بودن استفاده از این سرویس در این شرایط جهت ارسال اطلاعات دارای طبقه بندی می باشد.

نسخه پشتیبان بانک اطلاعاتی پست الکترونیکی برای چندین سال، آرشیو می شود.

از سوی دیگر، ازآنجاکه تبادلات اطلاعاتی فراوانی در کشور از طریق پست الکترونیکی انجام می گیرد، جدا از نگرانی های فوق الذکر این وابستگی روز افزون در صورت قطع سرویس در شرایط خاص بین المللی، خود می تواند تهدید بزرگی بشمار رود. بنابراین تفحص و اندیشیدن تمهیدات لازم در این زمینه بمنظور استفاده از سرویس پست الکترونیک بصورت امن، ایمن و پایدار ضرورت بسیاری دارد.

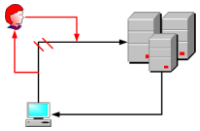
بطورکلی در استفاده از سرویس پست الکترونیکی باید دقت نمود که چه مطالبی ارسال می‌شود و چه نتایجی بدنبال خواهدداشت، چراکه با توجه به پروتکل های ارتباطی پست الکترونیکی که در فصل قبل مورد بررسی قرار گرفت، این سرویس فاقد امنیت ذاتی می باشد.

توجه داشته باشید با استفاده از سرویس هایی نظیر پست الکترونیکی، همواره ردپای شما روی شبکه قابل شناسایی است. لیست برخی سایت های جستجو کننده کاربران شبکه در انتهای فصل ذکر شده است.

تهدیدات و مخاطرات متصور مرتبط با سرویس پست الکترونیکی را می توان بگونه ذیل دسته بندی نمود:

❖ **جاسوسی، جعل و افشای اطلاعات:**

امنیت از مهم ترین موضوعات در ارسال پیام می باشد. پیام می بایست بنحوی ارسال گردد که به سرقت نرود و متن آن برای افراد غیر مجاز قابل فهم نباشد. امروزه پست الکترونیکی یکی از بسترهای انتقال پیام با ویژگی های منحصر بفرد بحساب می آید. از این منظر داده‌های ارسالی ازطریق‌پست‌الکترونیکی را خطرات عمده ذیل تهدید می نماید:



- جعل و شنود[۱]:

نکته حائز اهمیت در ارسال و دریافت پیام از طریق پست الکترونیکی، عدم رمزنگاری و دیگر امکانات مقابله با شنود یا

[۱] شخص ثالثی می‌تواند به اطلاعاتی که بطور خصوصی بین دو فرد دیگر در حال رد و بدل شدن می‌باشد، دست یابد.

جعل پیام در پروتکل های ارتباطی آن می باشد؛ یعنی در صورت عدم دقت و توجه کافی کلیه ارتباطات و حتی تبادلات مربوط به نام کاربری و کلمه عبور به صورت یک متن ساده تبادل می شود. به این ترتیب می توان از محتوای ارتباطات آگاه و آن‌ها را دستکاری نمود[1]. تکنیک های نوین رمز نگاری راه حل مناسبی برای رفع این تهدید می باشد که در حال حاضر بمنظور عملیات ورود به حساب کاربری عموماً مورد استفاده قرار می گیرد. یکی از نیاز های امروز بررسی و تقویت الگوریتم های رمزنگاری جهانی و نهایتاً بومی نمودن دانش آن درکشور می باشد.

- کپی های حفاظت نشده :

درحالیکه پیام ها به صورت یک متن ساده وآشکار در تمامی کارگزارهای SMTP ذخیره می‌شوند، کپی پشتیبانی که از اطلاعات کارگزارها گرفته می شود ممکن است چندین سال نگهداری شده و توسط هر کاربر ناشناس که به آن ها دسترسی پیدا می کند، خوانده شود.

---

[1] رفتار پروتکل HTTP که در وبمیل ها وظیفه برقراری ارتباط کاربر و درگاه را برعهده دارد نیز به همین صورت است. به همین دلیل توصیه می شود تنها زمانی اطلاعات مهم ارسال شود که از پروتکل HTTPS (HTTP امن) جهت انتقال اطلاعات استفاده شده باشد.

- عدم تصدیق هویت[۱]:

هیچ تضمینی برای اثبات هویت ارسال کننده پیام در سامانه پست الکترونیکی به ذات تعبیه نشده است. «پیام ممکن است جعلی باشد»، این بدین معنی است که اگر شخصی پیامی برای شماارسال نمود، می تواند ارسال پیام را انکار کند و یا ممکن است شما پیامی را از فردی دریافت کنید که پیامی برایتان ارسال ننموده است. تکنیک های امضای دیجیتال بعنوان راهی درجهت پوشش این نقص مورد استفاده قرار می گیرد.

❖ **اختلال در فعالیت کاربر نهایی:**

تهدیدات این دسته شامل ویروس ها (به معنای عام بدافزار) و اسپم ها می باشد. آن ها بسته به نوع و با توجه به گستره پست الکترونیکی می توانند در خدمت دیگر انواع تهدید بوده و یا با انتشار سریع، مستقلاً در کار شبکه بستر یا کاربران متصل، اختلال و وقفه جدی ایجاد نمایند.

- ویروس ها:

انتشار ویروس را می توان از رایج ترین کارکرد های امروزی پست الکترونیکی به حساب آورد!

---

[۱] شخص گیرنده یا فرستنده ایمیل می‌تواند خود را شخص دیگری وانمود نماید.

Melissa و LoveLetter جزء اولین ویروس هایی بودند که از ضمیمه های ایمیل برای انتشار استفاده می کردند. این نوع ویروس ها به محض اجرا شدن معمولاً خودشان را به آدرس های پستی که از قربانی و صفحات وب پیدا می کنند، ارسال می نمایند. بعضی ویروس ها، از پسوند چندتایی بمنظور فریب کاربر در تشخیص نوع فایل ضمیمه استفاده می کنند. گاهی ویروس های اینترنتی با استفاده از شکاف های امنیتی نرم‌افزارهای مورد استفاده کاربر، خود را بسرعت در شبکه منتشر می کنند. کرم Nimda نمونه ای از این بدافزارها بود که با فریب بسیاری از ابزارهای امنیت پست الکترونیکی و نفوذ به کارگزارها و شبکه های بزرگ و سرایت به کاربران خانگی، اینترنت را فراگرفت؛ Nimda روی رایانه هایی که از نسخه آسیب پذیری از IE[1] یا نرم افزار Outlook Express جهت ارسال و دریافت پیام استفاده می کردند، بطور خودکار اجرا می شد و از آن ها جهت انتشار خود استفاده می نمود. گاهی حتی کلیک روی موضوع ایمیل نیز امکان نفوذ را فراهم می‌آورد. این روش به مهاجم

[1] Internet Explorer

فرصت می دهد تا بدون جلب توجه، یک بدافزار کوچک جاسوسی[۱] یا مخرب را روی رایانه قربانی نصب نماید.

با توجه به نکات فوق و بمنظور مقابله با چنین مخاطراتی، وجود یک ضدبدافزار و فایروال قابل اعتماد و بروز رسانی منظم و پیکربندی مناسب آن روی سامانه کاربر و کارگزار، استفاده از نرم افزارهای قابل اعتماد و بروز، و دقت هنگام استفاده از این سامانه بسیار ضروری می باشد.

- اسپم[۲]:

اسپم ها اثری بیش از مزاحمت برای کاربران اینترنت دارد و بطور جدی بازدهی شبکه و کارگزاران پست الکترونیکی را تحت تاثیر قرار می‌دهد. فرستندگان اسپم ها از هزینه بسیار پایین ایمیل استفاده کرده و صدها هزار یا حتی میلیون‌ها ایمیل را در یک زمان ارسال می‌کنند. حمله‌های اسپمی پهنای باند زیادی را

---

[۱] نرم‌افزارهای جاسوسی، محتوای فعالیت کاربر را برای هکر ارسال می‌کند. نرم‌افزارهای جاسوسی وسایر انواع بدافزارها از طریق ارسال ایمیل، دانلود بعضی نرم‌افزارهای رایگان و یا مشاهده برخی از سایت ها می‌تواند کامپیوتر قربانی را آلوده کند.

[۲] Spam شامل مجموعه ای از نامه های الکترونیک می شوند که با موضوعات مختلف همچون تبلیغاتی، تجاری، غیراخلاقی(هرزنامه)، سیاسی، معنوی و یا با مقاصد کلاهبردارانه بصورت ناخواسته توسط کاربر دریافت می شود.

می‌گیرد، صندوق‌های پستی را پر می‌کند و در بهترین حالت تنها زمان کاربران پست الکترونیکی را تلف می‌کنند.

ضد اسپم[۱]، نرم‌افزاری است که به کارگزار و کاربر سرویس پست الکترونیکی کمک می‌کند تا از عبور اسپم جلوگیری کند.

❖ **تحریم و اختلال در ارائه سرویس:**

هنگام استفاده از سامانه های پست الکترونیکی با میزبانی خارجی (همچون Yahoo و Gmail) تهدیدات ذیل، متصور می باشد:

۱.عبور ترافیک دارای طبقه بندی و حجم وسیعی از تبادلات عادی، بعنوان یک منبع غنی دانشی از خارج کشور.

۲.عدم کنترل دسترسی داده های ارسالی و انتقال همه مشکلات محتمل میزبانی به سمت داخل.

نبایستی فرض شود که پیام‌های حذف شده قابل بازیابی نیستند. در سیستم پستی ابزار مشابه کاغذ خرد کن وجود ندارد!

[۱] Anti Spam

۳.عدم دسترس پذیری کاربران و امکان دسترسی بیگانگان به اطلاعات؛ باید توجه داشت هر زمان امکان تحریم از سوی چنین سرویس دهندگانی وجود دارد. بامطالعه دو مورد یاهو و گوگل مشخص می شود امکان قطع سرویس در هر زمان و امکان استفاده از پیام های ثبت شده برای پیگیری‌های قانونی در شرایط عضویت لحاظ شده است.

از سوی دیگر این تهدید، ضرورت تقویت توان داخل جهت ارائه پست الکترونیکی بصورت بومی و بدون وجود مشکلات میزبانی و ارائه سرویس در ترافیک های بالا و شرایط متفاوت و خاص کشور بصورت امن، ایمن و پایدار در جهت عدم وابستگی گوشزد می نماید.

برخی سایت های جستجوی اطلاعات کاربران در شبکه اینترنت:

۱. http://www.cvgadget.com
۲. http://www.intelius.com
۳. http://www.switchboard.com
٤. http://www.bigfoot.com
٥. http://www.peekyou.com
٦. http://whozat.com
۷. http://www.usernamecheck.com
۸. http://www.isearch.com
۹. http://www.spokeo.com
۱۰. http://www.۱۲۳people.com

فصل ۵ – ملاحظات پدافند غیرعامل

متأسفانه امروز و در تکاپو و رقابت های آماری توسعه کاربری فناوری اطلاعات و ارتباطات، اصول و مبانی امنیت کمتر در الویت قرار می گیرد. دغدغه اصلی پدافند غیرعامل کشور در حوزه فناوری اطلاعات و ارتباطات کشور توسعه امن زیرساخت‌های کشور و ارتقای ضرایب امنیت، ایمنی و پایداری می باشد.

❖ **ملاحظات پدافند غیرعامل در کاربری پست الکترونیک**

- محققین، مسئولین و کاربران می بایست به طور مستمر تحقیق و مطالعه نموده وخود را بروز نگه دارند.
- قبل از استفاده از هر نرم افزار مشتری یا درگاه سرویس دهنده، می بایست شناخت کافی از آن حاصل شود.
- کاربران جهت اتصال به حساب کاربری می‌بایست از نرم‌افزارها مشتری یا درگاه های اینترنتی امن، پایدار و قابل اعتماد و حتی المقدور بومی استفاده نمایند.
- از رؤیت پیام های ناشناس و مشکوک در پست الکترونیکی می بایست اجتناب شود.
- وجود ضدبدافزار، ضد اسپم و فایروال قابل اعتماد، بروزرسانی منظم و پیکربندی مناسب آن روی سامانه کاربر

و کارگزار و دقت هنگام استفاده از پست الکترونیکی جهت مقابله با مخاطرات محتمل ضروری است.

- پیام های ارسالی می بایست بصورت رمز شده و دارای امضای دیجیتال باشد.
- از درج نام کاربری و کلمه عبور در سایت های متفرقه و یا صفحات مشکوک می بایست خودداری شود؛ بدون شناخت ارسال کننده پیام، نباید روی هیچ دعوتنامه ای کلیک و یا به آن پاسخ داد.
- هیچگاه نمی بایست از کلمه عبور مشابه برای پست الکترونیکی و سایت های متفرقه استفاده نمود.
- هر کاربر هنگام پایان استفاده از پست الکترونیکی حتماً می بایست از حساب کاربری خارج شود. (Log out یا Sign out).
- پیام های الکترونیکی که نگهداری آن ها ضرورت ندارد، می بایست به طور مرتب از صندوق ارسال و دریافت کاربر پاک گردد.

❖ **ملاحظات راهبردی**

- کار گسترده و داشتن برنامه فرهنگی برای ارتقاء آگاهی کاربران در خصوص مخاطرات، تهدیدات امنیتی و روش مقابله با آن ها در حوزه پست الکترونیکی ضروری است.
- می بایست به امر ایجاد اینترانت[۱] ملّی مستقل از بستر اینترنت و تقویت آن اهتمام گردد.
- دانش رمزنگاری و الگوریتم های رمز بومی می بایست تقویت گردد.
- ظرفیت ملی سرویس پست الکترونیکی بومی امن، ایمن و پایدار می بایست در داخل کشور و روی میزبان های داخلی تأمین گردد. این اقدام عدم وابستگی کشور در این حوزه را بدنبال خواهد داشت.

[۱] Intranet ها شبکه هایی هستند که بصورت داخلی و مستقل از اینترنت فعالیت می کنند.