نفوذ چیست؟

یک نفوذ به مجموعه ای از فعالیتهایی گفته می شود که می تواند موارد ذیل را از یک منبع به خطر اندازد:

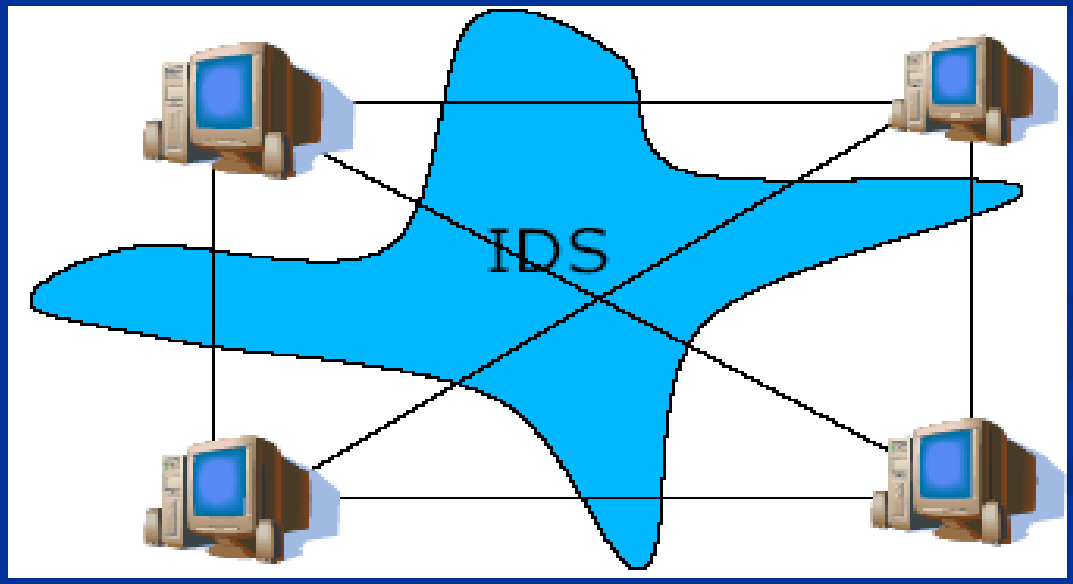
- یکپارچگی
- قابلیت اعتماد
- قابلیت استفاده و در دسترس بودن

نفوذگر کیست؟

- کارمند داخلی و خودی : در واقع شخصی که با در دست داشتن مجوز دسترسی ار اختیار خود سوء استفاده می نماید
- Hacker : شخصی که با استفاده از لینکهای ارتباطی از قبیل اینترنت به شبکه داخلی سازمان نفوذ می کند.
- نرم افزارهای بداندیش: نرم افزارهایی از قبیل *'MalWare'* ، *'Trojan Horse'* و *ویروسها* که با اجرا شدن این نرم افزارها بر روی سیستم گونه ای از حمله و نفوذ علیه سیستم تلقی می گردد.

سیستم تشخیص نفوذ چیست؟

سیستم تشخیص نفوذ یا همان IDS در واقع سیستمی می باشد که قابلیت شناسایی حملات را بر روی سیستم های کامپیوتری دارا می باشد.



فعالیت های اساسی IDS

- ✓ استراق سمع کردن یا Monitoring :
جمع آوری اطلاعات از شبکه
- ✓ تحلیل نمودن یا Analyzing :
تصمیم گیری هر آنچه اتفاق میافتد.
گزارش دهی با Reporting :
تولید نتیجه و یا در غیر اینصورت
فعالیت بر روی نتایج مرحله
Analyzing

شبکه اختصاصي مجازي (VPN)

یک VPN ، شبکه ای اختصاصی بوده که از اینترنت برای ارتباط با سایت های از راه دور و ارتباط کاربران با یکدیگر استفاده می نماید. این نوع شبکه ها بجای استفاده از خطوط واقعی نظیر خطوط Leased ، از یک ارتباط مجازی به کمک اینترنت برای ایجاد شبکه اختصاصی استفاده می کنند .

نکات مرتبط با کلمات عبور

اغلب کاربران کامپیوتر، به طور معمول از رمزهای عبور ساده و آسان استفاده می کنند. اما دقت داشته باشید که این سهل انگاری در انتخاب رمز عبور، عواقب خطرناکی به دنبال خواهد داشت. رمزهای عبور آسان و معمولی در ظرف چند ثانیه لو خواهند رفت و اطلاعات شخصی شما در سیستم مورد نظر به راحتی در معرض دید هکرها قرار خواهند گرفت. د ر ادامه تهدیدهای ممکن در این رابطه بررسی خواهند شد :

تهدیدهای مرتبط با کلمات عبور

- **Passive Online Attacks :**

در این روش هکرها از نرم افزار یا سخت افزارهای جاسوسی یا Snifferها استفاده می‌کنند. به این ترتیب که این نرم افزار یا سخت افزار با قرار گرفتن بر روی شبکه، اطلاعات در حال انتقال بر روی سیم ها را Sniff کرده و برای هکر ارسال می‌کنند.

تهديدهای مرتبط با کلمات عبور

- **Active Online Attacks :**

اين روش در واقع حدس زدن رمز کاربران است که روش تجربي و با توجه به فرهنگ و ذهنيات فرد است. به طور معمول کاربران از مبتدي تا حرفه اي سعي مي‌کنند رمزي را براي خود در نظر بگيرند که به راحتي بتوانند آن را در خاطر نگهدارند. که همگي قابل حدس زدن مي‌باشند را به عنوان رمز خود در نظر مي‌گيرند. کاربران زرنگتر از ترکيب آنها استفاده مي‌کنند که يافتن و حدس زدن آن کمي مشکل‌تر خواهد بود. هکرها نيز با توجه به اين اصل که کارايي بسياري نيز براي آنها دارد، ابتدا اطلاعات پرسنلي افراد را يافته و با آنها به حدس‌زني رمز مي‌پردازند.

تهدیدهای مرتبط با کلمات عبور

- **Offline Attacks:**

در این روش از ابزاری برای یافتن رمز استفاده می‌شود. این ابزارها معمولا بر دو نوع هستند:

الف - Dictionary Attack : ابزارهای این روش، با کمک گرفتن از ذهن هکر، به یافتن رمز در کلمات لغتنامه می‌پردازند.

ب - Brute Force : در این روش نرم افزار ابتدا تعداد حروف رمز را با کمک هکر یا بدون کمک یافته و با استفاده از حروف و کلمات پیشنهادی هکر، به صورت منظم و یک به یک با جایگذاری آنها، سعی در یافتن رمز می‌کند در این روش بدیهی است که انتخاب رمز مناسب و قوی می‌تواند به شکست این نرم افزار بیانجامد.

تهديدهای مرتبط با کلمات عبور

- **Electronic Attacks :**

در اين روش از راه‌هاي غير معمول و غيركامپيوتري براي يافتن رمز ديگران استفاده مي‌شود. برخي از اين روش‌ها عبارتند از:

الف- نگاه كردن به كي‌بورد هنگام تايپ كاربر

ب- از پشت سر فرد نگاه كردن

ج- كاغذ فسفري: با دادن يك كاغذ مخصوص فسفري به كاربر بدون اينكه او متوجه شود، دستانش به فسفر آغشته شده، سپس بر روي كي‌بورد اثر كلماتي كه تايپ مي‌كند، برجا خواهد ماند.

د- مهندسي اجتماعي: هكرها اعتقاد بسياري به اين مهندسي دارند. در اين روش با استفاده از فرهنگ، ذهنيات، كمبودهاي روحي و ... افراد مختلف، اطلاعات مهمي را به دست مي‌آورند.

تهديدهای مرتبط با کلمات عبور

- Key Loggers :

اين نوع نرم افزارها با قرارگيري بر روي يك سيستم، كليه استفاده هاي كاربر از ماوس و كيبورد را ضبط كرده و براي هكر ايميل ميكند. در اين روش حتما ميبايست نرم افزار بر روي كامپيوتر شما نصب شود پس دقت كنيد هيچ نرم افزاري را بدون شناسايي و نوع عملكرد بر روي كامپيوتر خود نصب نكنيد.

تهدیدهای مرتبط با کلمات عبور

- **Fishing :**

در اين روش، صفحه‌اي مشابه يكي از سايت‌هاي معتبر جهان ساخته و براي شما ارسال مي‌شود يا اينكه شما را تشويق به ثبت نام براي شركت كردن در يك قرعه‌كشي بزرگ مي‌كند و شما نيز بدون توجه، تمام اطلاعات خود را وارد مي‌كنيد. توجه داشته باشيد حتي اگر اين كار را انجام مي‌دهيد، از رمز ايميل يا رمزهاي مهم خود در اين صفحات استفاده نكنيد و به صفحاتي كه از شما اطلاعات مي‌خواهند به راحتي پاسخ ندهيد.

راهکارهای امنیتی مرتبط با کلمات عبور

۱ . به هیچ وجه از اسامی استفاده نکنید فرقی نمی کند که اسم فامیلتان باشد، یا باشگاه فوتبال مورد علاقه تان. بسیاری از برنامه های هکر، رمزهای عبور را با کمک فرهنگ لغت هک می کنند. فقط چند ساعت طول خواهد کشید که با کمک لغات یک فرهنگ لغت، دستیابی به رمز عبور امکان پذیر شود.

۲. برای رمز عبور خود حداقل از ۸ حرف استفاده کنید:

برای رمز عبوری که از ۴ حرف تشکیل شده است، حدود ۴۵۰۰۰ حالت وجود دارد. اما برای رمز عبوری که از ۸ حرف و علامتهای ویژه تشکیل شده است، یک میلیارد حالت مختلف وجود دارد!

راهکارهای امنیتی مرتبط با کلمات عبور

۳. برای رمز عبور، از حروفی که در کنار هم قرار گرفته اند استفاده نکنید! رمزهای عبوری مانند qwert یا asdf کار هکرها را برای دستیابی به رمز عبور بسیار آسان می کند، این مطلب در ترکیب اعداد نیز به همین صورت است؛ مثل " ۱۲۳۴۵۶۷۸ ".

۴. برای رمز عبور خود، ترکیبی از حروف بزرگ و کوچک یا اعداد و علامتهای ویژه را انتخاب کنید. استفاده از علامتهای ویژه به تنهایی کافی نیست. پنج درصد همه کاربرها بر این امر اتفاق نظر دارند که رمز عبوری حداقل یکي از کاراکترهاي خاص (@-$=% و ...) را دارا باشند. در این صورت نرم افزارهاي Brute Force از یافتن رمز عاجز می شوند.

راهکارهای امنیتی مرتبط با کلمات عبور

۵. رمز عبور خود را تا حد امکان جایی ننویسید حتی اگر کاغذی که رمز عبور خود را بر روی آن نوشته اید، در جای امنی مانند کیف تان باشد، از این کار اجتناب کنید. عنوان کاغذی که رمز عبور خود را بر روی آن نوشته اید، به هیچ عنوان زیر صفحه کلید یا به مانیتور خود نچسبانید!

۶. رمز عبور خود را همواره تغییر دهید. هر قدر، مدت زمان استفاده از رمز عبورتان بیشتر باشد، خطر هک شدن شما بیشتر خواهد بود. اداره فناوری اطلاعات آلمان فدرال، توصیه می کند که هر ۹۰ روز یکبار رمز عبور خود را تغییر دهید.

راهکارهای امنیتی مرتبط با کلمات عبور

۷. رمز عبور خود را در کامپیوتر ذخیره نکنید!
کامپیوتر قادر است رمز عبور شما را ذخیره کند تا شما مجبور نباشید هر بار آن را وارد کنید.

۸. رمز عبور خود را به شخص دیگری ندهید!
اگر از شما تلفنی یا با ایمیل، رمز عبورتان را خواستند، آن را بازگو نکنید! هکرها معمولاً خود را به عنوان همکاران شرکتهای بزرگ معرفی می کنند.

هفت روش حرفه ای برای ایجاد رمز عبور

۱.برای ایجاد کلمه عبور، از حروف بزرگ و کوچک و به صورت یک در میان استفاده کنید. مثال:
cOmPuTeR

۲.حروف اول کلمات یک جمله را به عنوان رمز عبور خود انتخاب کنید.
مثلاًدر جمله: " If sentence is longer password would be safer "
که رمز عبور آن به این صورت تبدیل می شود: "
Isilpwbs "

۳.عدد یا تاریخی را برای خود در نظر بگیرید و آن را با دکمه Shiftتایپ کنید.
مثلاً : تاریخ: ۱۳,۰۶,۲۰۰۲ با دکمه Shiftبه این کلمه تبدیل می شود: !#>)^<@))@

هفت روش حرفه ای برای ایجاد رمز عبور

۴. لغتی را در نظر بگیرید و سپس حروف سمت راست آن را که بر روی صفحه کلید قرار دارد، بنویسید:
مثال: Hardware تبدیل می شود به: Jstfestr
5. لغت یا ترکیبی را برای خود در نظر بگیرید مانند "۲۴ Oktober" و بعد آن را بهم بریزید به این صورت که حروف اول آن را با حرف آخر، حرف دوم را با حرف ماقبل آخر و به همین ترتیب بقیه را بنویسید: ۲۴ r4eObkot
6. لغات یک جمله را به اختصار بنویسید این اختصارات را خود شما تعیین می کنید و از قاعده خاصی پیروی نمی کنند. مثلاً عبارت White meat with cabbage تبدیل می شود به: "whtmtwtcabge"
7. در رمز عبور از علائم ویژه استفاده کنید. مثال: "c/Om%u\t$E~

نکات امنیتی مرتبط با مرورگرها

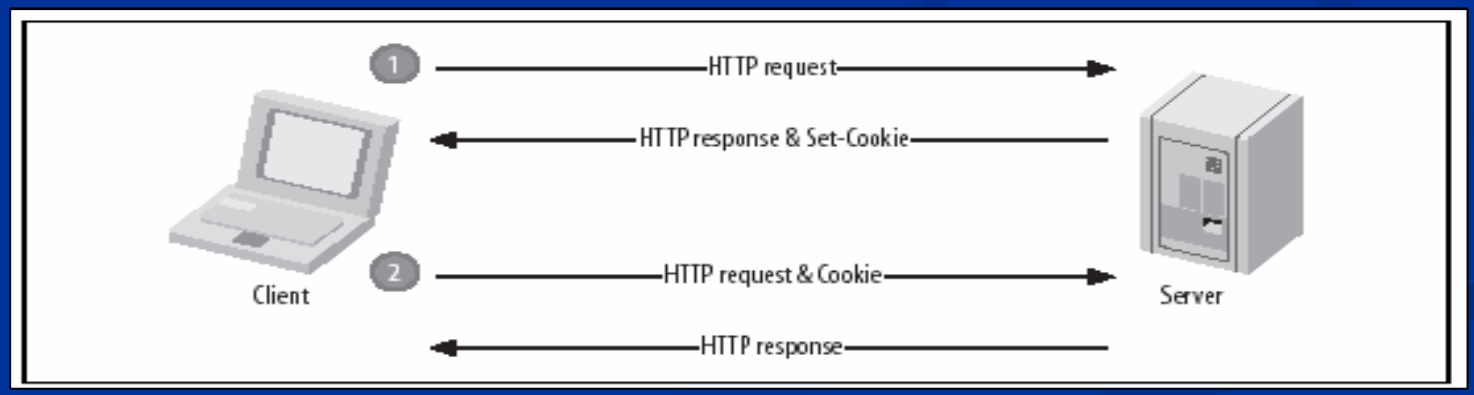
مرورگرهای وب ، اولین نقطه ارتباطی کاربران با اینترنت بوده و همین موضوع توجه جدی به آنان را مضاعف می نماید. بدیهی است وجود نقاط آسیب پذیر و یا عدم پیکربندی مناسب آنان، کاربران اینترنت را در معرض تهدیدات و حملات گسترده ای قرار خواهد داد .

با توجه به توسعه ي روزافزون وب و نياز به تعاملي شدن هر چه بيشتر سايت هاي وب، استفاده از امكانات نشست ها و كوكيها در زبان PHP بيشتر مي شود. از آنجايي كه استفاده ناحتاطانه از اين امكانات و ويژگيها مي تواند نقاط نفوذ بسيار مهمي را براي نفوذگران و مهاجمان سايت ها فراهم نمايد. پروتكل HTTP پروتكلي فاقد حالت است، بدين معنا كه در حركت كاربر بين صفحات مختلف يك سايت وب و يا بين درخواست هاي متوالي، اطلاعات كاربر حفظ نمي شود و يا به عبارتي HTTP آن ها را به ياد نمي آورد.

نکات امنیتی مرتبط با مرورگرها

کوکي ها در حقيقت يکي از توسعه هاي پروتکل HTTP به شمار می روند. در استفاده از آن ها نياز به دو سرآيند HTTP است :

۱- سرآيند پاسخ Set-Cookie ۲- سرآيند درخواست Cookie



نکات امنیتی مرتبط با مرورگرها

با پیکربندی مناسب مرورگرها ، می توان یک سطح مناسب امنیتی را ایجاد نمود. گرچه ممکن است به موازات افزایش سطح ایمنی ، امکان استفاده از برخی قابلیت های یک سایت بخصوص وجود نداشته باشد ، ولی شما در مقابل برخی از حملات محافظت شده و پیشگیری اولیه را انجام داده اید . برنامه های مرورگر ، اولین نقطه ارتباطی شما با اینترنت می باشند و ممکن است چندین برنامه دیگر نیز به منظور ارائه خدمات و سرویس ها در ارتباط با آنان باشند و همین موضوع پیکربندی امنیتی مرورگرها را مضاعف می نماید.

نکات امنیتی مرتبط با مرورگرها

تعداد زیادی از برنامه های وب با بکارگیری برخی از قابلیت های مرورگرها ، خدمات و سرویس های خاصی را در اختیار کاربران قرار می دهند .
رویکرد فوق علیرغم وجود برخی نکات مثبت، می تواند کاربران را مستعد انواع حملات نماید .
مطمئن ترین سیاست امنیتی ، غیرفعال نمودن اکثر ویژگی های ارائه شده همراه مرورگرها می باشد .
در صورتی که پس از غیرفعال نمودن برخی از ویژگی های مرورگرها در زمان استفاده از یک سایت تائید شده و مطمئن ، مشکلات خاصی ایجاد گردد ، می توان موقتا" آنان را فعال و پس از اتمام کار و استفاده از سایت مورد نظر ، مجددا" آنان را غیرفعال نمود .

نکات امنیتی مرتبط با مرورگرها

- علیرغم ارائه پتانسیل های مثبت توسط تکنولوژی هائی نظیر اکتیو ایکس و یا اسکریپت های فعال ، مهاجمان با استفاده از آنان قادر به نادیده گرفتن و یا دور زدن تنظیمات امنیتی سیستم می باشند .
- نقاط آسیب پذیر Spyware/Adware که تمامی مرورگر ها و سیستم هائی را که از منابع موجود بر روی وب استفاده می نمایند ، تحت تاثیر قرار می دهد .
- تلفیق مرورگر IE با سیستم عامل باعث شده است که مشکلات IE به سیستم عامل ویندوز نیز سرایت نموده و بر نحوه عملکرد آن تاثیر منفی داشته باشد .

نکات امنیتی مرتبط با مرورگرها

مهاجمان با استفاده از نقاط آسیب پذیر مرورگرها قادر به انجام عملیات متفاوتی می باشند :

- افشای کوکی ها
- افشای فایل ها و داده های محلی
- اجرای برنامه های محلی
- دریافت و اجرای هرگونه کد دلخواه
- در اختیار گرفتن کنترل کامل سیستم آسیب پذیر و انجام هر گونه عملیات دلخواه

نکات امنیتی مرتبط با مرورگرها

تنظیمات امنیتی در مرورگرها

این مسئله به نوع مرورگر وب بستگی داشته و هر یک از آنان امکانات خاصی را در اختیار استفاده کنندگان قرار می دهند . مثلا" در مرورگر Internet Explorer، می توان پس از انتخاب منوی Toolsگزینه Internet Optionsرا انتخاب و در ادامه با کلیک بر روی Security tabو نهایتا" دکمه Custome Level، سطح امنیتی مورد نظر را انتخاب نمود . در مرورگر Mozila، پس از انتخاب منوی Edit می توان گزینه Preferencesرا انتخاب و با کلیک بر روی Privacy & Security، سطح امنیتی مورد نظر را تعریف نمود .

نکات امنیتی مرتبط با مرورگرها

مرورگرهای وب از اصطلاحات متفاوتی در ارتباط با پیکربندی امنیتی استفاده می نمایند :

Zones ✓

مرورگرهای وب، گزینه های مختلفی را به منظور استقرار وب سایت ها در سگمنت ها و یا نواحی متفاوت ارائه می نمایند . هر ناحیه می تواند دارای تنظیمات امنیتی مختص به خود باشد . مثلا" مرورگر Internet Explorer دارای نواحی زیر است :

نکات امنیتی مرتبط با مرورگرها

- **Internet :**

ناحیه فوق یک سگمنت عمومی و برای وب سایت های عمومی است .در زمان استفاده از اینترنت ، تنظیمات تعریف شده برای این ناحیه به صورت اتوماتیک در ارتباط با سایت هائی که مشاهده می گردد ، اعمال خواهد شد . به منظور تامین بهترین سطح حفاظتی و امنیتی مرورگر ، می بایست این ناحیه دارای بالاترین سطح امنیتی و یا حداقل سطح mediumباشد .

نکات امنیتی مرتبط با مرورگرها

- **Local Intranet :**

در صورتی که سازمان شما دارای یک اینترانت است ، می توان از این ناحیه استفاده نمود . ناحیه فوق شامل تنظیمات امنیتی به منظور استفاده از صفحات داخلی است . با توجه به این که محتویات وب توسط یک سرویس دهنده وب داخلی مدیریت می گردد ، می توان محدویت های به مراتب کمتری را در ارتباط با اینگونه از صفحات اعمال نمود .

نکات امنیتی مرتبط با مرورگرها

- **Trusted Sites :**

در صورتی که برخی از سایت ها با رعایت مسائل امنیتی پیاده سازی شده باشند و تهدیدی از جانب آنان متوجه شما نمی باشد ، می توان آنان را در ناحیه فوق قرار داد . مثلا" می توان سایت هائی را که با استفاده از تکنولوژی SSL پیاده سازی شده اند را در این ناحیه قرار داد ، چراکه همواره امکان شناسائی هویت سایت مورد نظر وجود خواهد داشت . سطح امنیتی این ناحیه ، می بایست بگونه ای تعریف شود که اگر سایت های مستقر در این ناحیه مورد تهاجم قرار گرفتند ، تهدیدی متوجه شما نباشد (پیشگیری از اختصاص یک سطح امنیتی پائین) .

نکات امنیتی مرتبط با مرورگرها

- **Restricted Sites :**

در صورتی که وب سایت های خاصی وجود دارد که نسبت به غیرایمن بودن آنان اطمینان حاصل شده است ، می توان آنان را در این ناحیه قرار داد و برای آن بالاترین سطح امنیتی را تعریف نمود . با توجه به این که تنظیمات امنیتی برای حفاظت شما در مقابل اینگونه سایت ها به اندازه کافی مناسب نمی باشند ، بهترین گزینه عدم استفاده از سایت های غیرایمن است .

نکات امنیتی مرتبط با مرورگرها

✓ جاوا اسکریپت

برخی وب سایت ها از زبان های اسکریپت نویسی نظیر جاوا اسکریپت به منظور ارائه قابلیت های خاصی استفاده می نمایند . از اسکریپت های فوق ممکن است به منظور انجام حملات متفاوتی استفاده گردد .

✓ کنترل های اکتیوایکس و جاوا

از برنامه های فوق به منظور اجرای محتویات فعال و ارائه برخی قابلیت ها در وب سایت ها استفاده می گردد . از این نوع برنامه ها همانند کدهای جاوا اسکریپت، ممکن است به منظور انجام حملات متفاوتی استفاده گردد.

نکات امنیتی مرتبط با مرورگرها

Plug-ins ✓

در برخی موارد مرورگرها به منظور ارائه خدمات ، نیازمند نصب نرم افزارهای اضافه ای با نام Plug-insمی باشند . از این نوع برنامه ها همانند کدهای جاوا اسکریپت ، کنترل های اکتیوایکس و جاوا ، ممکن است به منظور انجام حملات متفاوتی استفاده گردد. بنابراین لازم است در زمان نصب اینگونه نرم افزارها از صحت عملکرد و ایمن بودن آنان اطمینان حاصل گردد . در صورتی که برنامه های فوق می بایست از طریق اینترنت دریافت و نصب گردند ، بررسی هویت سایت ارائه دهنده ، امری ضروری است .

فقدان امنيت در پست الكترونيكي

به طور كلي پست الكترونيكي نا امن است. در اين مرحله، بسيارمهم است كه نا امني در مسير تحويل پيام آشكار شده و بررسي شود:

- Webmail : اگر اتصال به سرويس دهنده Webmail نا امن باشد در اين صورت همه اطلاعات شامل كلمه عبور و نام كاربري به صورت رمز نشده بين سرويس دهنده Webmail و كامپيوتر كاربر ارسال مي شود.
- SMTP : SMTP پيام ها را رمز نمي كند (مگر اين كه از سرويس دهندگان درخواست شود تا ازTTS پشتيبانی كنند.) ارتباطات بين سرويس دهندگان SMTP به صورت متن آشكار۲ است كه ممكن است پيام ها را براي هر استراق سمع كننده اي قابل رويت سازد.

فقدان امنيت در پست الكترونيكي

- IMAP-POP: در صورتی که POP و IMAP درخواست کلمه عبور و نام کاربري براي ورود کند؛ اين اعتبار نامه ها رمز شده نيستند. بنابراين، اعتبارنامه ها و پيام ها ممکن است توسط استراق سمع کنندگان در جريان ارسال اطلاعات بين کامپيوترکاربر و کامپيوتر فراهم کننده سرويس پست الکترونيکي شنود شوند.
- نسخه هاي پشتيبان: پيام ها در سرويس دهند گان SMTP به صورت متن آشکار و رمز نشده ذخيره مي شوند. بر روي اين سرويس دهند گان، نسخه هاي پشتيبان در هر زماني ممکن است ساخته شوند و با اين مکانيزم هر داده اي توسط مدير قابل خواندن است. پيام هاي الکترونيکي که ارسال مي شوند ممکن است به صورت ناخواسته يا نامحدود ذخيره شده و يا توسط
افراد ناشناس خوانده شوند.

تهديدات امنيتي در ارتباطات پست الكترونيكي

در اينجا بسياري از مشكلات امنيتي معمول در رابطه با ارتباطات و پست الكترونيكي اشاره ميشود:

- استراق سمع
- سرقت هويت
- نقض حريم خصوصی
- تغيير و تبديل در پيام ها
- ارسال پيام هاي جعلي
- تكرار پيام ها
- نسخه هاي پشتيبان محافظت نشده
- انكار

امن سازي پست الكترونيكي توسط SSL و TLS

ساده ترين راهي كه براي امن سازي پست الكترونيكي وجود دارد اين است كه از يك سرويس دهنده پست الكترونيكي استفاده شود كه از SSL براي سرويس دهندگان SMTP و IMAP، POP، Webmail پشتيباني مي كند.

TLS نيز يك نوع از SSL است كه مي تواند در طي يك نشست پست الكترونيكي راه اندازي شود. بر خلاف TLS ، SSL بايد قبل از ارسال پست الكترونيكي راه اندازي شود.

SSL تركيبي از مكانيز مهاي رمزگذاري متقارن و نامتقارن است.

نکات امنیتی مربوط با پست الکترونیکی

در نهایت چند توصیه را نیز همواره در ایمیل می بایست رعایت نمود:

- هیچگاه ایمیل کسی را که نمی-شناسید اصلا باز نکنید. مخصوصا ایمیل-هایی را که جذاب به نظر می-رسند. چون ممکن است دچار حملات XSS شوید.
- هیچگاه هیچ برنامه-ای را که از ایمیل یا چت دریافت کرده-اید نصب یا اجرا نکنید. چون ممکن است Trojan روی سیستم شما نصب شده و تمام اطلاعات شما را بدزدد.
- فایل-های عکس و صوتی و تصویری و متنی (مانند pdf و doc) را تنها در صورتی که مطمئن هستید فرد آشنا و مطمئنی آن را برای شما فرستاده است باز و استفاده کنید. چون ممکن است توسط این فایل-ها Trojan روی سیستم شما نصب شود.

نکات امنیتی مربوط با پست الکترونیکی

امنیت ایمیل این روزها یک نیاز حیاتی محسوب شده و چیزی بیش از فیلترینگ ضداسپم یا ضدویروس را شامل می شود. کلاهبرداری های Phishing، کاربران سازمانی را تهدید به سرقت رمزهای عبور آنها می کند تا بتوانند به شبکه های سازمانی دسترسی یابند؛ سایر حملات، سرور میل را مستقیماً هدف قرار می دهند و تلاش خود را بر دستیابی به نام های کاربری یا آدرس های ایمیل معتبر یا دسترسی به سرور میل متمرکز می نمایند. این امکان وجود دارد که سازمان ها از جانب اشخاص حقیقی که ایمیل های مهاجم را از سوی کاربران شرکت دریافت می کنند یا حتی از جانب کارمندان خودشان که محتویات مهاجم را از سایر کارمندان یا منابع خارجی دریافت می کنند، تحت پیگرد قرار گیرند.

نکات امنیتی مربوط با پست الکترونیکی

شرکت ها همچنین با تهدید سرقت اسرار سازمانی یا دارایی های فکری- معنوی از طریق ایمیل مواجه می باشند. ابزارهای امنیت ایمیل از قبیل، IronPort C-Series، Mirapoint Message Server M-Series نه تنها می توانند با کوتاه کردن دست اسپم ها موجب صرفه جویی در وقت کاربران شوند، بلکه می توانند همه مسایل امنیتی دیگر را نیز مدنظر قرار دهند. این ابزارها در نسخه های متعدد قابل دستیابی هستند و برای سازمان های متوسط تا بزرگ با ۵۰۰ تا ۵۰۰۰ کاربر طراحی شده اند.