اندیشه
پردازان
طلیعه نو

DLP(Data Leakage Prevent)

سامانه جلوگیری از نشت اطلاعات و ویروس

دارای تاییدیه فنی از شورای عالی انفورماتیک کشور و ثبت مالکیت در مرکز توسعه فناوری رسانه های دیجیتال

سامانه جامع رســـان

نسل جدید شبکه ها بدون نیاز به آنتی ویروس

دارای تائیدیه فنی از شورای عالی انفورماتیك كشور

و

ثبت در مرکز توسعه فناوری اطلاعات و رسانه های دیجیتال

« سامانه جلوگیری از نشت اطلاعات »

Data Leak Prevention

اطلاعات گرانبهاترین سرمایه سازمان را تشکیل می دهد

اگر در یک شبکه ی کامپیوتری اینترنت و تمام پورت های انتقال فایل مانند USB و انواع درایو های دیسک های نوری بسته شوند می توان ادعا کرد که دو مشکل امنیتی بزرگ که همواره سیستم ها را تهدید می کند بطور کامل از بین می رود .

اولا با بستن راه های ارتباطی سیستم می توان گفت که هیچ کامپیوتری دچار ویروس و نهایتا تخریبها و مشکلات آتی بعد از آن حتی بدون داشتن آنتی ویروس هم نخواهد شد.

ثانیا دیگر نگران ورود و یا خروج اطلاعات درای طبقه بندی از کامپیوترها نخواهیم بود.

اما با وجود این دو دستاورد عالی در بخش امنیت و پایداری سیستم ها و شبکه ,استفاده از این راهکار ها بدلیل اینکه در انتقال اطلاعات تاثیر کاملا منفی دارند سال هاست که مطرود مانده و ما برای مقابله با ویروس ها و سرقت اطلاعات همواره بصورت منفعلانه با این مشکلات برخورد می کنیم.

باز کردن و بستن پورتهای کامپیوترها برای افراد خاص و یا بایند کردن سریال فلش با سیستم های خاص و استفاده از آنتی ویروس برای آلوده نشدن به ویروس ها از راهکارهای رایج و سنتی است که از آن استفاده می شود و البته همانطور که میدانید و می بینید باز هم با این دو چالش امنیتی دست به گریبان هستیم.

سامانه جامع رسان برای اولین بار با ارائه یک روش منحصر به فرد علاوه بر حذف تهدیدهای فوق ، چابکی سازمان را در استفاده از رسانه های ذخیره ساز مانند انواع کول دیسک ها و لوح های فشرده را از بین نمی برد .

ابتدا به بررسی راهکار های سنتی پرداخته و پس از با بیان نقاط ضعف آنها راهکار نوین سامانه جامع رسان توضیح داده می شود.

سیستم های جلو گیری از نشت اطلاعات (DLP) سنتی

سیستم های جلوگیری از نشت اطلاعات سنتی ابتدا ازطریق نرم افزاری که بر روی رایانه کاربران نصب می شود پورتهای ورود و خروج اطلاعات مانند USB را غیر فعال کرده سپس از طریق کنترل مرکزی که توسط نرم افزار سرور سامانه صورت می گیرد اقدام به باز یا بسته کردن پورت ها بر اساس نام کاربران یا رایانه ها می نمایند.

اشکالاتی که این نرم افزار های سنتی جلوگیری از نشت اطلاعات را به چالش میکشد موارد زیر می باشد:

- از آنجا که کنترل پورت ها در این سیستم ها بصورت نرم افزاری می باشد یقینا روش هایی که بتوان بکمک آنها پورت های یک رایانه را باز کرد وجود دارد، از بوت شدن با USB گرفته تا روش های نرم افزاری متنوعی که هر روزه توسط هکرها در حال ساخت و توسعه می باشند.
- بعلت اینکه نرم افزار سرور این سامانه باید دسترسی کامل به سیستم های شبکه داشته باشد ، نیاز به شبکه های مبتنی بر دامین دارد
- عدم امکان لاگ گیری از محتوای وارد یا خارج شده به کامپیوترها
- مهم ترین تهدیدی که در روش های سنتی وجود دارد ابتلاء کامپیوتر به انواع ویروس ها از طریق ابزار های ذخیره ساز مانند فلش ها می باشد.

- نشت اطلاعات در سه بخش تعریف می شود و آنچه این سیستم ها بر آن متمرکز هستند نشت اطلاعات از رایانه کاربران می باشد در صورتی که نشت اطلاعات در حین انتقال و در محل ذخیره سازی در سرور را مورد توجه قرار نمی دهند.

در مورد ویروس ها نکته قابل توجه دیگری وجود دارد و آن اینکه روشی که تمام ویروس ها بعد از آلوده کردن یک سیستم برای انتشار خود در شبکه از آن بهره می گیرند استفاده از پروتکل فایل شیرینگ (file sharing)ویندوز می باشد.

این بدان معناست که اگر در شبکه , یک سیستم دچار ویروس شود تمام شبکه و حتی سرور ها (مانند باج افزار های جدیدی که به سرور های بانک اطلاعاتی حمله میکنند) در معرض تهدید ویروس ها واقع می شوند.

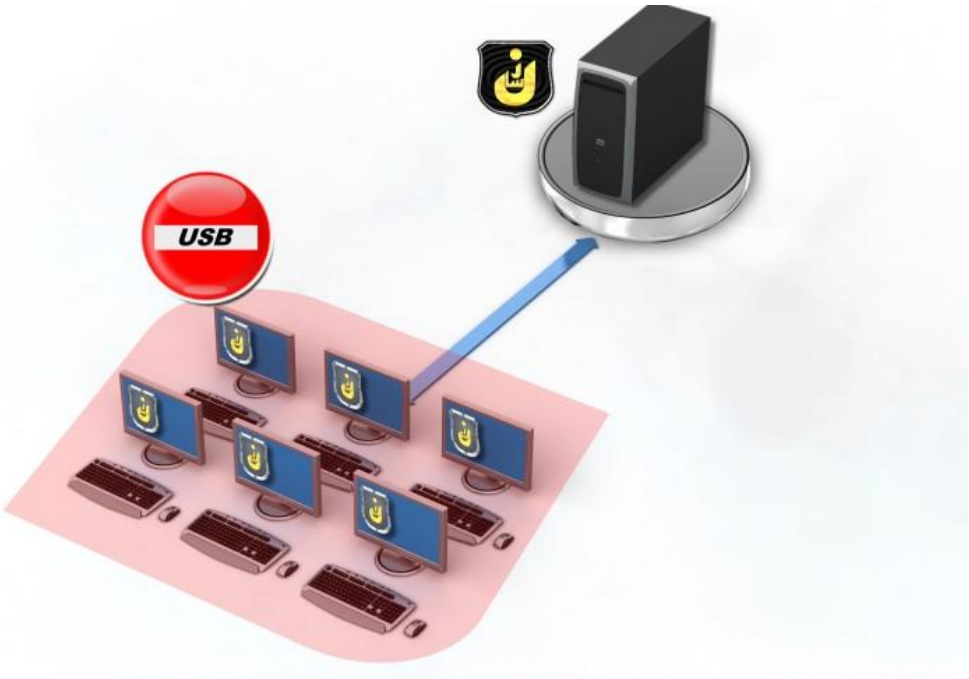
از آنجا که برای انتقال فایل در سیستم های ویندوزی از پروتکل File Share استفاده می شود امکان غیر فعال کردن آن میسر نمی باشد , و همانند بستن پورتهای کامپیوتر ها که در ابتدا اشاره شد بدلیل ایجاد مانع در روند انتقال اطلاعات غیر قابل اجرا گشته است , در اینجا نیز با وجود پی بردن به اینکه تنها راه انتشار ویروس ها در شبکه File Sharing است , بعلت نبودن جایگزین برای آن مجبور به استفاده از آن بوده و همواره خطر انتشار ویروس های نا شناخته ما را تهدید می کند.

سامانه جلوگیری از نشت اطلاعات در سامانه جامع رسان

با توجه به نکات ارائه شده فوق و همچنین رابطه پورت USB با ویروس ها و همچنین موضوع سرقت اطلاعات ابتدا می بایست بطور کامل از دست این پورت و همچنین سایر پورت های انتقال فایل رها شد، توجه داشته باشید که این کار را می توان بصورت فیزیکی (پلمب کردن یا حذف کردن) یا سخت افزاری (غیر فعال کردن از بایوس) و یا حتی بصورت نرم افزاری انجام داد و البته آنچه در انتخاب یکی از روش های ذکر شده تعیین کننده می باشد درجه اهمیت اطلاعات سازمان است.

نکته دیگر اینکه اینکار باید در سطح تمام شبکه و بدون حتی یک استثناء انجام شود.

سپس می بایست یک سرور را بر روی شبکه به سامانه جامع رسان اختصاص داده و نسخه سرور رسان را بروی آن نصب کرد.

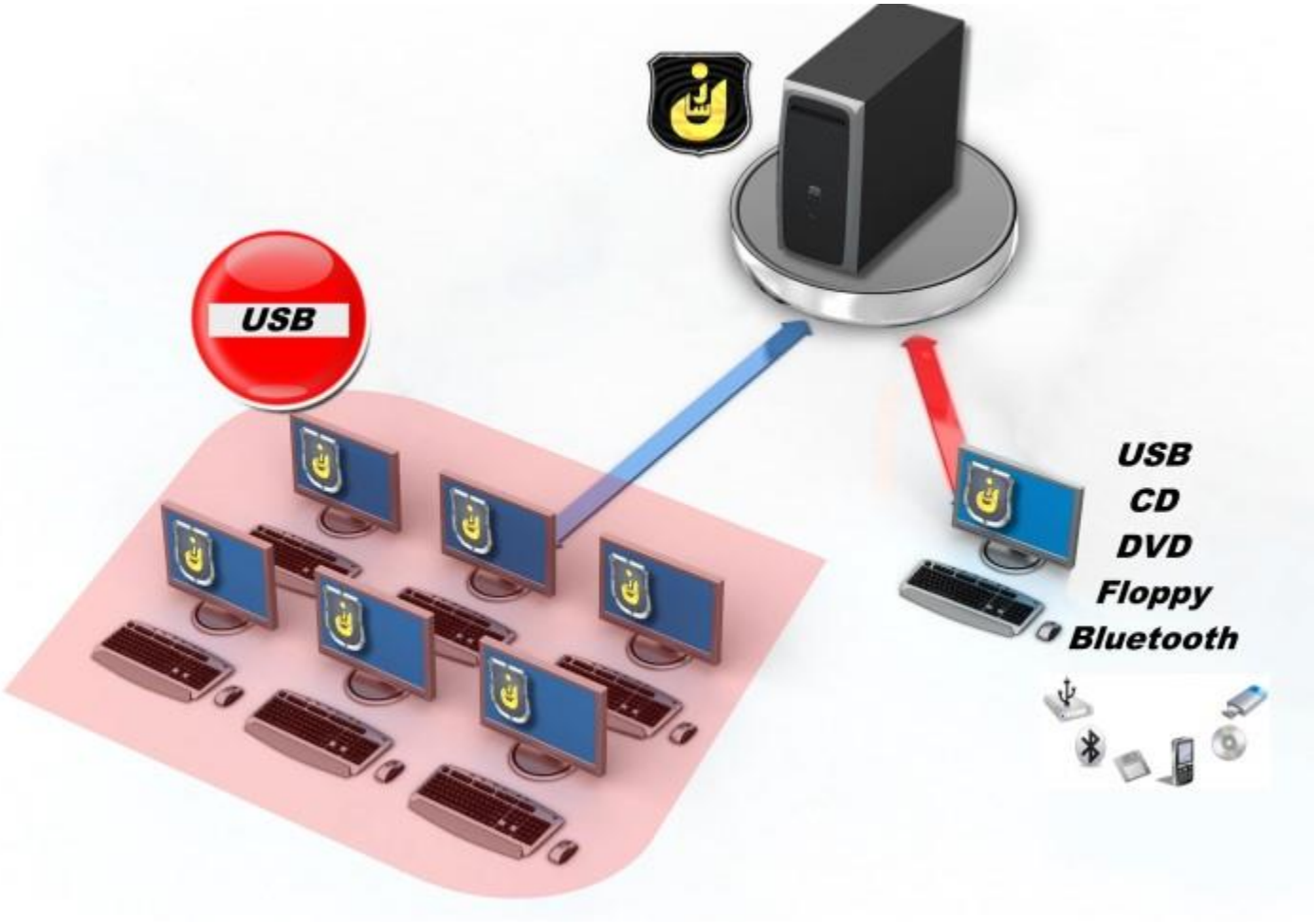


تا اینجا سامانه جامع رسان بعنوان یک فایل سرور کاملا بومی و امن با امکانات فوق العاده در تعریف سطوح دسترسی که پیچیده ترین سناریو های فایل سرور را براحتی اجرا می کند ، قابل بهره برداری می باشد.

در همین حال ، سامانه جامع رسان می تواند بعنوان یک سامانه پیام رسان جایگزین مناسبی برای انواع میل سرور های رایج باشد ،که با پروتکل بومی و اختصاصی خود از تمام تهدید های میل سرور ها در امان می باشد .

اکنون می بایست در شبکه سیستم هایی را در نظر بگیرید که از طریق یک مسیر مجزا به سرور متصل شوند ، این سیستم ها که از این به بعد به آنها سیستم های خود پرداز فایل می گوییم دارای تمام تجهیزات انتقال فایل می باشند و البته از نظر سخت افزاری هم حداقل تجهیزات را نیاز دارند چرا که این سیستم ها جز انتقال فایل هیچ کار دیگری انجام نمی دهند.

این سیستم ها نیاز به هارد نداشته و با یک سی دی LIVE ویندوز فعال می شوند



برای ورود اطلاعات به یکی از سیستم های شبکه ابتدا کاربر می بایست از طریق یکی از سیستم های خود پرداز فایل ، نرم افزار رسان را اجرا کرده و بعد از احراز هویت به فایل سرور رسان متصل شود.

بصورت پیش فرض هر کاربر پوشه ای بنام "*ورود و خروج سازمان* "در حساب کاربری خود دارد ، در سامانه جامع رسان برای اینکه هر کاربری بتواند اطلاعاتی را از رایانه خود خارج کند دیگر حق استفاده از هیچ درگاه انتقال فایل سخت افزاری مانند انواع فلش ها و یادی وی دی و یا سی دی و

غیره را ندارد زیرا که تمامی این تجهیزات می بایست از روی رایانه کاربران حذف و یا غیر فعال شوند ، اکنون کاربر درصورت داشتن مجوز ورود اطلاعات که می بایست قبلا از مدیر سامانه اخذ کرده باشد میتواند فایل مورد نظر خود را به پوشه "*ورود و خروج از سازمان* "ارسال کند ، به این ترتیب بجای استفاده مستقیم از یک رسانه ذخیره ساز در واقع از سرور رسان برای جابجایی اطلاعات استفاده می شود.

سپس کاربر از طریق رایانه خود ،نرم افزار رسان را اجرا کرده و از حساب کاربری خود فایل مورد نظر را برداشت می کند.

برای خروج اطلاعات نیز ابتدا کاربر پس از ورود به سامانه از طریق رایانه خود و البته در صورت دارا بودن مجوز خروج اطلاعات که مدیر سامانه آنرا تعیین می کند می تواند اطلاعات خود را به پوشه "*ورود و خروج از سازمان* "منتقل کند، سپس کاربر از طریق یکی از سیستم های خود پرداز ،اقدام به برداشت اطلاعات از آن می کند .

همانطور که بیان شد در واقع هر تراکنش دیتا بین کاربر و خود پرداز ها از طریق سامانه جامع رسان صورت می گیرد که این خود باعث می شود بر تمام این تراکنش ها کنترل داشت، یعنی تعیین حق ورود و خروج اطلاعات و همچنین تمام تراکنش ها نیز در سرور لاگ گیری شده و در اختیار مدیر سامانه می باشد ، بصورتیکه مدیر سامانه جامع رسان می تواند ببیند که چه کاربری در چه روز و ساعتی چه اطلاعاتی را به شبکه وارد یا از آن خارج کرده است.

در معماری فوق ، خود پرداز ها خط مقدم دفاع در برابر ویروس ها می باشند ، از آنجا که سیستم های خود پرداز هیچ کاری جز انتقال فایل انجام نمی دهند می توان این سیستم ها را تنها با سی دی LIVE ویندوز را ه اندازی کرد در این صورت این سیستم ها هیچ گاه با هیچ نوع ویروسی حتی بدون آنتی ویروس آلوده نمی شوند و از آنجا که شبکه سیستم های خود پرداز ، اولا از شبکه

اصلی سازمان جدا می باشد و ثانیا این سیستم ها در دامین شبکه سازمان تعریف نشده اند، امکان آلوده شدن سیستم های شبکه نیز وجود ندارد .

از آنجا که در بخش شبکه خود پردازها و سرور سامانه جامع رسان ، از هیچ سرویس انتقال فایلی استفاده نمی شود و البته سرور سامانه رسان نیز در دامین شبکه سازمان تعریف نشده است ، آن هم در معرض آلودگی و یا انتشار ویروس نمی باشد و در این صورت نه تنها سیستم های خود پرداز حتی بدون آنتی ویروس آلوده نمی شوند بلکه شبکه نیز از آلودگی ویروس ها در امان خواهد بود .

اما شاید این سئوال پیش بیاید که بالاخره شاید ویروسی بتواند از یک خود پرداز به سرور راه پیدا کرده و البته از آنجا هم به کل شبکه سرایت کند، چه تضمینی برای عدم بوقوع آمدن این اتفاق وجود دارد .

در جواب باید بگوییم که این اتفاق هیچ گاه و با هیچ تکنولوژی ممکن نخواهد بود ، البته شاید تعجب کنید، اما برای درک بهتر این مسئله یک مثال بسیار ملموس برای شما می آوریم.

به تعداد کامپیوترهایی که در شبکه جهانی اینترنت هستند فکر کنید و تصور کنید که چه تعداد از این سیستم ها آلوده به ویروس های مختلف هستند ، به طور حتم به عدد بسیار بزرگی خواهید رسید، خوب حالا شما به این سئوال پاسخ دهید آیا این تعداد از سیستم های آلوده می توانند حتی یک سرور وب را که بطور طبیعی تمام کاربران اینترنت به تمام وب سرور های دنیا از طریق شبکه اینترنت متصل هستند آلوده کنند ، قطعا پاسخ شما به این پرسش منفی است ، چرا که اگر چنین چیزی امکان داشت باید هر روز سرور های اینترنتی در حال از کار افتادن باشند، اما چطور می شود که در یک شبکه وقتی یک سیستم آلوده می شود به سرعت تمام سیستم ها و حتی سرور ها

نیز آلوده می شوند ولی این اتفاق در شبکه جهانی اینترنت نمی افتد.پاسخ در نحوه برقراری ارتباط بین رایانه کاربر و سرور نهفته است.

همانطور که بیان گردید ارتباط در اینترنت بوسیله DataSocket ایجاد می شود که هیچ بستر بالقوه ای برای توزیع ویروس نمی باشد.

اما در شبکه های محلی سرویس فایل شیرینگ ویندوز وظیفه برقراری ارتباط را بعهده دارد و در واقع همین سرویس فایل شیرینگ ویندوز است که حتی با وجود لاگین نکردن کاربر هم تمام سیستم های شبکه را بصورت یکپارچه بهم متصل میکند و کار را برای انتشار ویروس ها در سطح شبکه آسان میکند.

همانطور که بیان شد بعلت استفاده گسترده از فایل شیرینگ ویندوز در شبکه های محلی ویروس ها بهترین و راحت ترین ابزار را برای توزیع خود در میان سیستم های شبکه دارند.

اکنون مشخص می شود اگر در یک شبکه محلی بجای استفاده از فایل شیرینگ ویندوز از یک سامانه انتقال فایل مبتنی بر Socket استفاده شود , هیچگاه بستری برای انتشار ویروس نخواهیم داشت.

آنچه که سامانه جامع رسان موفق به پیاده سازی آن گشته اولین فایل سرور بومی مبتنی بر Socket می باشد که علاوه بر حل مشکل انتشار ویروس ها, بعلت بومی بودن از امنیت و پایداری بسیار بالای بر خوردار می باشد.