بسمه تعالی

راه‌کارهای کاهش اثرات مخرب پست‌های الکترونیکی

چکیده

از آن‌جا که امروزه استفاده از پست‌های الکترونیکی[1] در بین کاربران اینترنت بسیار متداول است، به همین دلیل توجه‌ی بدخواهان زیادی را نیز به خود جلب کرده است. در این گزارش راه‌کارهایی برای کاهش خطرهای امنیتی که توسط پست‌های الکترونیکی مخرب[2] ایجاد شده‌اند، مطرح می‌شود. سازمان‌ها باید سعی کنند با توجه به استفاده‌ای که از پست‌های الکترونیکی دارند، از روش‌های موثری برای در امان ماندن از آثار مخرب پست‌های الکترونیکی استفاده کنند.

[1] Email
[2] Malicious

فهرست مطالب

1. مقدمه

امروزه پست‌های الکترونیکی زیادی در بین کاربران اینترنت ردوبدل می‌شود. این پست‌های الکترونیکی می‌توانند حاوی فایل‌های پیوست[1] نیز باشند. از آن‌جا که تعداد پست‌های الکترونیکی زیاد است، توجه بدخواهان اینترنتی را به خود جلب کرده‌اند. در طی تحقیقاتی که توسط متخصصین حوزه‌ی امنیت انجام شده است، تعداد زیادی پست‌های الکترونیکی حاوی فایل‌های پیوست و یا لینک‌های مخرب جاسازی‌شده را شناسایی کرده است که در اغلب موارد هدفمند و برعلیه سازمان‌ها بوده‌اند.

این گزارش توسط سازمان ASD و به منظور فراهم کردن راهکاری برای کاهش خطرهای امنیتی که توسط پست‌های الکترونیکی مخرب ایجاد شده‌اند، گردآوری شده است. در این گزارش تعدادی راهکار برای کاهش چنین خطراتی ارایه شده است. قابل توجه است که هر راهکار ارایه‌شده در این گزارش، لزوما برای تمامی سازمان‌ها مناسب نیست و سازمان‌ها باید با در نظر گرفتن نیازمندی‌های کاری و محیط ریسک خود، راه‌حل کاهشی مناسبی را برای خود انتخاب کنند.

2. فیلتر کردن پیوست‌ها

پیوست‌ها در پست‌های الکترونیکی یکی از ریسک‌های امنیتی قابل توجه‌اند. فیلتر کردن پیوست‌ها، احتمال دریافت محتویات مخرب بر روی سیستم کاربر را تا حد خوبی کاهش می‌دهد. راهکارهای کاهش در مورد پیوست‌های مخرب در ادامه آورده شده‌اند. این راه‌کارها براساس تاثیری که بر روی امنیت دارند، دسته‌بندی می‌شوند.

2-1 اثربخشی امنیتی عالی

1. تبدیل قالب[2] پیوست‌ها

تبدیل قالب پیوست‌ها به قالبی دیگر تاثیر به‌سزایی در حذف محتویات مخرب دارد. برای نمونه یکی از این تبدیلات، تبدیل فایل‌های آفیس مایکروسافت به قالب پی‌دی‌اف است.

2. لیست سفید[3] پیوست‌ها براساس نوع فایل

---

[1] Attachment
[2] Format
[3] White List

در این لیست برای تعیین نوع فایل، به جای در نظر گرفتن پسوند فایل، محتویات فایل بررسی می‌شود. انواعی از فایل که اهداف کسب‌وکار مجاز و مشخصات خطر قابل قبولی برای سازمان دارند، می‌توانند در لیست سفید قرار گیرند. توصیه به لیست سفید بیشتر از لیست سیاه[1] است، زیرا در این لیست همه‌ی انواع قابل قبول که می‌توانند از طریق پست الکترونیکی دریافت شوند، مشخص می‌شوند.

در صورتی که نوع فایل تشخیص داده شده براساس محتویات آن، با پسوند آن مغایرت داشته باشد، این مورد به عنوان یک مورد مشکوک باید مورد توجه قرار گیرد.

3. مسدود کردن[2] پیوست‌های غیرقابل شناسایی و یا رمزگذاری‌شده

پیوست‌های غیرقابل شناسایی و یا رمزگذاری‌شده قابل اعتماد نیستند چون که محتویات پست الکترونیکی نمی‌توانند رمزگشایی و بررسی شوند. هر پیوست رمزنگاری‌شده تا زمانی که بی‌خطر تلقی نشده است، باید مسدود شود.

4. انجام تحلیل پویای خودکار برای پیوست‌ها با اجرای آن‌ها در یک جعبه‌ی شنی[3]

تحلیل پویا، قابلیت شناسایی ویژگی‌های رفتاری را دارد. بنابراین انجام یک تحلیل پویای خودکار در یک جعبه‌ی شنی می‌تواند رفتارهای مشکوک در ترافیک شبکه، فایل‌های جدید یا تغییریافته و یا تغییرات در رجیستری ویندوز را شناسایی کند.

5. حذف پیوست‌هایی با محتویات فعال[4] یا به طور بالقوه خطرناک

محتویات فعال مانند ماکروها در فایل‌های آفیس مایکروسافت و جاوا اسکریپت‌ها باید قبل از تحویل پیوست‌ها به کاربر، از پست‌های الکترونیکی حذف شوند. ابزارهای حذف محتویات فایل باید پیوست‌ها را برای پیدا کردن محتویات فعال نامطلوب براساس کلمات کلیدی یا به صورت اکتشافی[5] بررسی و با بازنویسی آن‌ها اثر نامطلوبشان را خنثی کنند. هر چند که عملیات بررسی و حذف محتویات فعال در پیوست‌ها، پردازشی دشوار است.

6. کنترل یا غیرفعال کردن ماکروها در فایل‌های آفیس مایکروسافت

---

1 Black List
2 Block
3 Sandbox
4 Active
5 Heuristic

استفاده از ماکروها در فایل‌های آفیس مایکروسافت به شدت افزایش یافته است. از این‌رو بهتر است سازمان‌ها برنامه‌های خود را برای غیرفعال کردن همه‌ی ماکروها به صورت پیش‌فرض پیکربندی کنند و فقط ماکروهای قابل اعتماد که معمولا توسط افراد با سطح دسترسی بالا نوشته می‌شوند را بررسی کنند.

2-2 اثربخشی امنیتی خوب

1. بررسی کنترل‌شده فایل‌های آرشیو[1]

یک فایل مخرب می‌تواند در کنار فایل‌های مجاز دیگر تشکیل یک فایل آرشیو داده و برای مقصدی ارسال شود. برای تشخیص این فایل مخرب، گیرنده باید فایل‌های آرشیو را از حالت فشرده خارج کرده و تمامی فایل‌های درون آن را از نظر مخرب و یا مجاز بودن بررسی کند.

بررسی فایل‌های آرشیو باید به صورت کنترل‌شده انجام شود تا بررسی‌کننده دچار پیمایش‌های تو در تو یا حالت منع سرویس نشود. برای نمونه بررسی محتویات پست الکترونیکی که حاوی یک فایل متنی یک گیگابایتی آرشیوشده است و این فایل فقط از فضای خالی[2] تشکیل شده است، منابع پردازشی قابل توجهی را اشغال می‌کند. نمونه‌ی دیگر، فایل‌های آرشیو تو در تو هستند. اگر فایل آرشیوی از 16 فایل آرشیو دیگر تشکیل شده باشد و هم‌چنین هر کدام از فایل‌های آرشیو جدید نیز از 16 فایل آرشیو دیگر تشکیل شده باشند و این کار تا 6 سطح ادامه داشته باشد، بررسی‌کننده‌ی محتویات پست الکترونیکی باید در حدود یک میلیون فایل را بررسی کند. در این مواقع تنظیم کردن زمان منقضی شدن برای پردازنده، حافظه و دیسک باعث می‌شود تا اگر کاری بیشتر از زمان تعیین‌شده ادامه پیدا کرد، آن کار لغو شده و منابع به سیستم بازگردند.

از حالت فشرده درآوردن فایل‌ها از انتهای فایل آرشیو شروع شده و تا زمانی که همه‌ی فایل‌ها ایجاد شوند، ادامه پیدا می‌کند. یک فایل آرشیو مخرب می‌تواند به‌راحتی به انتهای یک فایل عکس مجاز اضافه شود و در سمت گیرنده با اسکن فایل مجاز عکس، دریافت شود. بنابراین نیاز است تمامی پیوست‌ها از حالت فشرده خارج شده و فایل‌های ایجاد شده از آن‌ها با دقت بررسی شود.

---

[1] Archive
[2] Space

3-2 اثربخشی امنیتی متوسط

1. لیست سفید فایل‌های پیوست براساس پسوندشان

بررسی پیوست‌ها بر اساس پسوندشان نسبت به بررسی محتویات فایل برای تشخیص نوع فایل، عملی ضعیف‌تر برای تشخیص بدخواهانه بودن آن‌ها است. زیرا به راحتی می‌توان پسوند فایل‌ها را تغییر داد بدون این‌که اصل فایل‌ها عوض شود. برای نمونه می‌توان فایل readme.exe را به readme.doc تغییر نام داد. در این بخش تمام فایل‌هایی که پسوند مجاز دارند در لیست سفید قرار می‌گیرند.

4-2 اثربخشی امنیتی کم

1. لیست سیاه فایل‌های پیوست براساس نوع‌شان

نگه‌داری یک لیست سفید از محتویات مجاز، چه بر اساس نوع فایل و چه بر اساس پسوند فایل، بهتر از نگه‌داری یک لیست سیاه از پیوست‌ها بر اساس نوع آن‌ها است. هم‌چنین تهیه و نگه‌داری لیست سیاهی از همه‌ی فایل‌های بد، سربار بیشتری نسبت به لیست سفید دارد. به همین دلیل این دسته در بخش اثر بخشی کم قرار گرفته است.

2. اسکن فایل‌های پیوست با نرم‌افزار ضدویروس[1]

پیوست‌ها باید با ضدیروس‌های به‌روزرسانی‌شده و با قابلیت خوب در تشخیص محتویات مخرب اسکن شوند. برای بیشتر شدن شانس تشخیص، بهتر است از ضدویروس‌های مختلف در این زمینه استفاده شود.

3. لیست سیاه فایل‌های پیوست براساس پسوندشان

استفاده از لیست سیاه برای پیوست‌ها بر اساس پسوندشان تاثیر کمتری نسبت به لیست سفید پیوست‌ها براساس پسوند یا نوع فایل‌ها دارد. واضح است که پسوند فایل‌ها به‌راحتی قابل تغییر است.

[1] Anti-Virus

3. فیلتر کردن محتوای پست الکترونیکی

اگرچه تعداد حملات ممکن از طریق بدنه[1]ی پست الکترونیکی نسبت به پیوست‌های آن کمتر است، اما فیلتر کردن بدنه‌ی یک پست الکترونیکی کمک می‌کند که محتوای بدخواه در متن آن شناسایی و برای جلوگیری از آن حمله، راه‌حلی استفاده شود. راه‌کارهای کاهش براساس فیلتر کردن بدنه‌ی پست الکترونیکی در ادامه آورده شده‌اند. این راه‌کارها در دو دسته با سطح امنیتی متفاوت قرار می‌گیرند.

3-1 اثربخشی امنیتی خوب

1. جایگزینی آدرس‌های وب فعال در بدنه‌ی پست الکترونیکی با نسخه‌های غیرفعال

آدرس‌های وب فعال به صورت Hyperlink در بدنه‌ی پست الکترونیکی ظاهر می‌شوند و کاربر با کلیک بر روی آن‌ها به یک سایت برده می‌شود. این آدرس‌ها می‌توانند در ظاهر ایمن نشان داده شوند اما کاربر را به یک آدرس مخرب منتقل کنند (شکل 1).

شکل 1 آدرسی مخرب با ظاهری ایمن

تمامی آدرس‌های وب فعال که در بدنه‌ی پست الکترونیکی قرار دارند باید به صورت غیرفعال درآیند تا کاربر برای رسیدن به سایت موردنظر، آدرس را به صورت دستی در مرورگر خود کپی کند. در این حالت کاربر متوجه‌ی بدخواهانه بودن آدرس می‌شود.

3-2 اثربخشی امنیتی متوسط

1. حذف محتویات فعال در بدنه‌ی پست الکترونیکی

[1] Body

در سازمانی که مرورگر کاربر قابلیت اجرای محتویات فعال را داشته باشد، محتویات فعال بدنه‌ی پست‌های الکترونیکی مانند VB Script و جاوا اسکریپت‌ها، ریسک امنیتی محسوب می‌شوند. بنابراین بدنه‌ی پست‌های الکترونیکی که دارای محتویات فعال هستند یا باید دقیق بررسی شوند و یا اینکه برای کاهش ریسک‌های امنیتی مسدود شوند. بعد از بررسی بدنه‌ی پست الکترونیکی، محتویات فعال می‌توانند بازنویسی شوند تا اثر مخربشان از بین برود.

4. تصدیق فرستنده

بررسی صحت و جامعیت یک پست الکترونیکی می‌تواند یک سازمان را از دریافت برخی از پست‌های الکترونیکی مخرب محافظت کند. استراتژی‌های کاهش در حیطه‌ی تصدیق فرستنده در ادامه در سطوح امنیتی متفاوت بررسی شده‌اند.

4-1 اثربخشی امنیتی خوب

1. پیاده‌سازی DMARC[1] برای ارتقای چارچوب سیاست‌های فرستنده[2] و شناسایی کلیدهای دامنه‌ی پست‌های الکترونیکی[3]

DMARC، پست‌های الکترونیکی را از نظر چارچوب سیاست‌های فرستنده و کلیدهای شناسایی بررسی می‌کند و مشخص می‌کند که پست الکترونیکی دریافت‌شده باید رد[4] شود، به عنوان هرزنامه[5] در نظر گرفته شود و یا هیچ‌کدام. هم‌چنین DMARC گزارش‌هایی را درباره‌ی اقدامات انجام‌داده در مورد کارگزارهایی که از آن‌ها پست الکترونیکی دریافت کرده است، ثبت می‌کند، تا صاحب دامنه بتواند آن‌ها را مشاهده و ردگیری کند.

4-2 اثربخشی امنیتی متوسط

1. مسدود کردن پست‌های الکترونیکی براساس آی‌دی فرستنده

---

[1] Domain-based Message Authentication, Reporting and Conformance
[2] SenderID/Sender Policy Framework (SPF)
[3] Domain Keys Identified Mail (DKIM)
[4] Reject
[5] Spam

با بررسی آی‌دی فرستنده، مشخص می‌شود که آیا پست الکترونیکی دریافت‌شده واقعا از سازمانی که ادعا می‌کند ارسال شده است یا خیر. در صورتی که این بررسی با شکست مواجه شود یا به عبارت دیگر شکست سخت[1] رخ دهد، پست الکترونیکی موردنظر مسدود می‌شود.

2. مسدود کردن پست‌های الکترونیکی براساس شناسایی کلیدهای دامنه‌ی پست‌های الکترونیکی

شناسایی کلیدهای دامنه‌ی پست‌های الکترونیکی، یک روش برای تایید دامنه‌ی فرستنده‌ی یک پست الکترونیکی است که با استفاده از امضاهایی که توسط فرستنده تهیه شده است، انجام می‌شود. پست الکترونیکی که در شناسایی کلیدهای دامنه شکست خورده است باید مسدود و بررسی شود. هم‌چنین باید به سازمان مربوط به آن گزارش داده شود که این پست الکترونیکی ادعا دارد که از طرف شما فرستاده شده است.

3-4 اثربخشی امنیتی کم

1. ترکیب لیست‌های سیاه هرزنامه

فرستنده‌هایی که پست‌های الکترونیکی آن‌ها به عنوان هرزنامه شناسایی شده‌اند و آدرس‌های آن‌ها باید بدون بررسی مسدود شوند.

2. قرنطینه کردن پست‌های الکترونیکی براساس آی‌دی فرستنده

با بررسی آی‌دی فرستنده، مشخص می‌شود که آیا پست الکترونیکی دریافت‌شده واقعا از سازمانی که ادعا می‌کند ارسال شده است یا خیر. گاهی اوقات این بررسی نمی‌تواند نظر قطعی را در مورد پست‌های الکترونیکی دریافت‌شده اعلام کند یا به عبارت دیگر شکست نرم[2] اتفاق افتاده است. در چنین شرایطی پست الکترونیکی به جای مسدود شدن قرنطینه شده و به کاربران اجازه داده می‌شود که در صورتی که پست الکترونیکی را مجاز در نظر گرفته‌اند، آن را بازیابی کنند.

4-4 اثربخشی امنیتی ضعیف

1. برچسب زدن پست‌های الکترونیکی بر اساس آی‌دی فرستنده

با بررسی آی‌دی فرستنده، مشخص می‌شود که آیا پست الکترونیکی دریافت‌شده واقعا از سازمانی که ادعا می‌کند ارسال شده است یا خیر. گاهی اوقات این بررسی نمی‌تواند نظر

---

[1] Hard Failed
[2] Soft Fail

قطعی را در مورد پست‌های الکترونیکی دریافت‌شده اعلام کند یا به عبارت دیگر شکست نرم اتفاق افتاده است. در این شرایط به جای مسدود و یا قرنطینه کردن، پست‌های الکترونیکی قبل از ارسال به کاربران برچسب بالقوه مخرب می‌خورند و این گونه به کاربران اطلاعی از احتمال خطر داده می‌شود و به آن‌ها اجازه می‌دهند که تصمیماتی برای رد و یا پذیرفتن پست‌های الکترونیکی بگیرند.

2. مشخص کردن پست‌های الکترونیکی خارجی

بهتر است که پست‌های الکترونیکی که از سازمان‌های خارجی دریافت می‌شوند، با یک سرآیند اضافه مشخص شوند. این سرآیند به کاربران هشدار می‌دهد که در موقع کار کردن با لینک‌ها و پیوست‌های درون پست الکترونیکی، احتیاط کنند.

5. جمع‌بندی

امروزه استفاده از پست الکترونیکی در بین کاربران اینترنت و سازمان‌ها افزایش یافته است. به طبع آن بدافزارهای این حوزه نیز رشد زیادی داشته‌اند. به این ترتیب آشنایی با راه‌کارهایی جهت افزایش امنیت پست الکترونیکی اهمیت زیادی دارد. در این مقاله برخی از راه‌کارهای پیشنهادی برای در امان ماندن از آثار مخرب پست‌های الکترونیکی بررسی شد.