چهار شنبه 30 تیر 1389 - 08:57

با ايميل‌هاي جعلي چه كنيم؟

جعل هويت در ايميل ممكن است به اشكال مختلفي اتفاق بيفتد اما نتيجه يكساني حاصل مي‌شود...

جعل هويت در ايميل ممكن است به اشكال مختلفي اتفاق بيفتد اما نتيجه يكساني حاصل مي‌شود؛ كاربر اي‌ميلي دريافت مي‌كند كه ظاهرا از طرف يك نفر فرستاده شده، در حالي كه در حقيقت شخص ديگري آن را ارسال كرده است و اين كار معمولا با هدف تحريك كاربر براي افشاي اطلاعات مهم و حساس انجام مي‌شود.
مثال‌هايي از ايميل‌هاي جعلي كه ممكن است روي امنيت سايت شما تاثير بگذارد عبارتند از: ايميل‌هايي كه ادعا مي‌كنند از سوي مدير سيستم هستند و از كاربر مي‌خواهند كه كلمه عبور خود را به كلمه خاصي تغيير دهند و تهديد مي‌كنند كه اگر اين كار انجام نشود، حساب كاربري او مسدود خواهد شد.
ايميل‌هايي كه ادعا مي‌كنند از طرف فرد موثق و مهمي هستند و از كاربر مي‌خواهند كه يك كپي از كلمه عبور يا اطلاعات مهم ديگر خود را براي وي ارسال كند.

راه‌هاي مقابله با هرزنامه و بمباران ايميلي

بدون شك شما نيز تاكنون تعداد زيادي از ايميل‌هاي ناخواسته را دريافت كرده‌ايد. بعضي از اين ايميل‌ها ادعا مي‌كنند كه شما را به سرعت ثروتمند مي‌كنند. برخي قول محصولات يا خدمات جديد را مي‌دهند. بعضي نيز فضايي از صندوق پستي شما را اشغال مي‌كنند و از شما مي‌خواهند كه ايميل را به سايرين نيز ارسال كنيد يا وب سايت مشخصي را ببينيد. در جامعه اينترنتي ايميل‌هاي بعضا تجاري ناخواسته، هرزنامه ناميده مي‌شوند.
هرزنامه‌ها اثري بيش از مزاحمت براي استفاده‌كنندگان اينترنت دارند و به طوري جدي بازدهي شبكه و سرويس دهندگان ايميل را تحت تاثير قرار مي‌دهد. زيرا فرستندگان هرزنامه از هزينه بسيار پايين ايميل استفاده مي‌كنند و صدها هزار يا حتي ميليون‌ها ايميل را در يك زمان ارسال مي‌كنند.
ايميل‌هاي مذكور معمولا داراي داده‌هاي بي‌معني با حجم زياد بوده و به منظور مصرف منابع سيستم و شبكه ارسال مي‌شوند. اين گونه حملات به بمباران ايميلي شهرت داشته و پهناي باند زيادي را اشغال مي‌كنند. بمباران ايميلي احتمال انكار سرويس سرور هدف را به شدت افزايش مي‌دهد.
حمله‌هاي هرزنامه‌اي نيز يك نوع از حمله‌هاي بمباران ايميلي بوده و پهناي باند زيادي را ميگيرند، صندوق‌هاي پستي را پر مي‌كنند و زمان خوانندگان ايميل را تلف مي‌كنند.
گاهي اوقات مي‌توان هرزنامه‌ها را از عناوين عجيب، غير منطقي و مضحكشان تشخيص داد. حملات هرزنامه‌اي در صورت پاسخ دادن به هرزنامه‌ها بدتر و شديدتر مي‌شوند زيرا تمام آدرس‌هاي مبدا، پاسخ را دريافت خواهند كرد گاهي اوقات حملات هرزنامه‌اي غيرتعمدي و در اثر ارسال يك پيغام به ليست‌هاي ايميل و بدون اطلاع از ارسال پيغام براي هزاران كاربر، رخ مي‌دهند. برخي از آنها هم بر اثر تنظيمات اشتباه در پاسخگويي اتوماتيك به ايميل‌ها رخ مي‌دهند.
حملات بمباران ايميلي / هرزنامه‌نويسي مي‌تواند با حملات جعل هويت در ايميل تركيب شده و تشخيص فرستنده واقعي ايميل را بسيار سخت كند.

مقابله با هرزنامه‌ها

تشخيص در صورتي كه سيستم شما ناگهان بسيار كنده شده و ارسال / دريافت ايميل‌ها به سختي صورت مي‌گيرد، ممكن است به اين دليل باشد كه سرور ايميل شما مشغول رسيدگي به پردازش تعداد زيادي ايميل است. در اين صورت با استفاده از ابزارهاي كنترل ترافيك شبكه مي‌توانيد پي به حمله‌هاي هرزنامه ببريد.

پيشگيري

متاسفانه در حال حاضر هيچ راه مطمئني براي پيشگيري و ممانعت كامل از حملات هرزنامه‌اي وجود ندارد، زيرا دسترسي به ليست‌هاي عظيم آدرس ايميل يا منابع اطلاعاتي كه داراي حجم زيادي از آدرس‌هاي ايميل هستند كار سختي نيست و از طرفي نيز هر شخصي كه داراي يك آدرس ايميل معتبر است مي‌تواند از طريق ليست‌هاي ايميل، هرزنامه ارسال كند.
يكي ديگر از مشكلات پيشگيري از بمباران ايميلي / هرزنامه، عدم امكان پيش‌بيني مبدا حمله بعدي است. اما بسته به اين كه مدير شبكه باشيد يا كاربرد عادي، براي كاهش اين گونه حملات تدابير متفاوتي وجود دارد.

مديران

ابزارهايي را كه براي تشخيص و پاسخگويي به بمباران ايميلي/ هرزنامه‌نويسي تهيه ديده و براي كاهش اثر اين گونه حملات مورد

استفاده قرار دهيد. ابزارهاي مذكور بايد توانايي ثبت گزارش (logging) را افزايش داده و همچنين هشدارهاي مناسب را در زمان كوتاهي درباره تعداد زياد ايميل‌هاي ارسالي/ دريافتي از يك كاربر خاص و يا يك وب سايت خاص ارائه دهند.
به محض تشخيص فعاليت‌هاي مشكوك، از ابزارهاي ديگري براي متوقف كردن ارسال/ دريافت پيغام از كاربران يا وب سايت‌هاي خاطي استفاده كنيد.
اگر سايت شما از تعداد كمي سرور ايميل استفاده مي‌كند، فايروال را به گونه‌اي پيكربندي كنيد كه مطمئن شويد ورودي‌هاي SMTP فقط به سرويس‌هاي ايميل اصلي شما اتصال پيدا مي‌كنند و بقيه سيستم‌ها درگير نمي‌شوند. درست است كه اين اقدام از حملات پيشگيري نمي‌كند ولي تعداد ماشين‌هاي در دسترس را براي نفوذگران در حملات مبتني بر SMTP كاهش مي‌دهد. از طرفي اگر مايل باشيد ابزارهاي ديگري را براي كنترل ورودي‌هاي SMTP به كارگيرد. تعداد دستگاه‌هايي كه نيازمند تنظيمات هستند كاهش پيدا مي‌كند.
سيستم‌هاي رسيدگي به ايميل خود را طوري تنظيم كنيد كه ايميل‌ها را فقط براي سيستم‌هاي فايلي ارسال كنند كه سهميه‌بندي فضا را براي هر كاربر فعال كرده‌اند. اين اقدام خسارات حمله را فقط به حساب‌هاي كاربري كه هدف قرار گرفته‌اند كاهش مي‌دهد و كل سيستم تحت تاثير قرار نمي‌گيرد. به كاربران خود، گزارش‌دهي را در صورت مشاهده بمباران ايميلي /هرزنامه آموزش دهيد يا مشكل را با ارسال مجدد هرزنامه يا پاسخ دادن به آن گسترده‌تر نكنيد.

كاربران خانگي

اولين اقدام براي جلوگيري از هرزنامه داشتن يك ايميل ديگر براي استفاده به عنوان ايميل كم ارزش است كه مي‌توانيد به اين منظور به ليست استفاده‌كنندگان سرويس‌دهندگان ايميل مجاني مانند HOTMAIL، YAHOO يا GMAIL بپيونديد.
از اين ايميل براي مواقعي كه نياز به وارد كردن آدرس ايميل خود در سايت‌ها داريد، مثلا براي دانلود كردن نرم‌افزارها استفاده كنيد. گاهي وارد كردن ايميلتان، باعث پيوستن شما به ليست‌هاي ايميلي مي‌شود كه خودتان نمي‌خواهيد. با وارد كردن ايميل كم ارزش خود، مطمئن خواهيد بود كه هرزنامه به ايميل اصلي شما وارد نخواهد شد.
تمام تلاش خود را براي جلوگيري از ارسال آدرس ايميل اصلي خود به فروم‌ها و كروم‌هاي خبري بكار گيريد. فرستندگان هرزنامه برنامه‌هاي كوچكي به اسم زبان‌هاي اينترنتي را براي جست‌وجو در اين مكان‌ها مي‌فرستد كه به‌دنبال @ يا نشانه‌هاي ديگري كه آدرس ايميل را مشخص كنند، بگردند (اين علامت به آنها مي‌گويد كه عبارت يافت شده يك آدرس ايميل است).
چنانچه مي‌خواهيد آدرس خود را روي اين فروم‌ها و گروه‌ها بفرستيد، دو انتخاب داريد: اول اين كه از ايميل دوم خود استفاده كنيد؛ و دوم اين‌كه، اگر شما به نيت پاسخ گرفتن از افراد ديگر آدرس خود را مي‌فرستيد، ممكن است بخواهيد از ايميل اصلي خود استفاده كنيد بنابراين به جاي نوشتن آدرس ايميل خود به صورت عادي، آن را مانند اين مثال ارسال كنيد:
Info AT certcc COOT ir اين كار به توجه بيش‌تري از طرف كاربران ديگر براي ارسال ايميل به شما نياز دارد، اما شما را از كشف توسط ربات‌هاي اينترنتي مصون مي‌دارد.
انتخاب آخر مشخصا براي گروه‌هاي خبري مناسب است ممكن است به شمار اجازه داده شود كه نحوه نمايش آدرس ايميل خود را هنگام ارسال پيام تغيير دهيد.
ممكن است بتوانيد حروف اضافه به انتهاي آدرس خود اضافه كنيد و آن را به چيزي تبديل كنيد كه از ديد ربات‌هاي اينترنتي متعلق به شما نباشد. مثلا Info.comPUTER @ certcc برخي از ربات‌هاي اينترنتي نمي‌دانند كه با اين آدرس‌ها چه كنند!
اما فردي كه اين آدرس را روي گروه خبري مي‌بيند، خواهد فهميد كه چه كند. البته بيش‌تر كاربران يك جمله با مضمون براي ارسال ايميل PUTER را از آدرس حذف كنيد، اضافه مي‌كنند تا از سردرگمي احتمالي جلوگيري كنند. البته اين اقدامات فقط احتمال ارسال هرزنامه را براي شما كاهش مي‌دهند.

استفاده از فيلترينگ

نرم‌افزارهاي خاصي براي فيلترينگ برروي سرور ايميل وجود دارد كه اكثر هرزنامه‌هايي را كه ممكن است دريافت كنيد فيلتر مي‌كند. اين نرم‌افزارها ايميل را قبل از اين كه شما آن را در صندوق پستي خود ببينيد دريافت مي‌كند و پيغام‌هايي را كه به عنوان هرزنامه تشخيص دهد پاك مي‌كند.
برخي از اين نرم‌افزارها كه براي سرويس‌دهنده ايميل نصب مي‌شود، چند ويژگي ديگر نيز دارد كه مي‌تواند جلوي هرزنامه‌هاي آتي را هم بگيرد. برنامه يك پيام به فرستندگان هرزنامه مي‌فرستد و به آنها مي‌گويد كه ايميل شما وجود ندارد تا ديگر از آن فرستنده به آدرس ايميل شما هرزنامه فرستاده نشود. شما همچنين مي‌توانيد پيام‌ها را قبل از دانلود كردن پاك كنيد كه روش جلوگيري از ورود يك ويروس به داخل رايانه شما خواهد بود.

مسدود كردن فرستندگان

چنانچه متوجه شويد كه هرزنامه‌هايي به‌طور منظم از يك آدرس مشخص دريافت مي‌كنيد، روشي براي مسدود كردن پيام‌هايي كه از طرف آن آدرس مي‌آيد، وجود دارد.
در Outlook Express يك پيغام را كه از طرف فرستنده‌اي كه مي‌خواهيد مسدود كنيد، انتخاب كنيد. از منوي MESSAGE گزينه BLOCK SENDER را انتخاب كنيد.

نرم‌افزار Outlook به شما خواهد گفت که این فرستنده مسدود شده است و از شما خواهد پرسید که آیا مي‌خواهید تمام پیغام‌هایي را که از این فرستنده در رایانه شما وجود دارد، پاك کنید یا خیر. یا مثلا در YAHOO مي‌توانید در قسمت OPTIONS...، با انتخاب BLOCK ADDRESS فرستنده خاصي را مسدود کنید.
با وجود تمام تدابیري که ذکر شد، همچنان از هرزنامه‌ها در امان نخواهید بود، بهترین وسیله براي مقابله با بقیه هرزنامه‌ها استفاده از کلید DELET است. چنانچه در مورد یك پیغام مطمئن نیستید، مخصوصا اگر نگران ویروس‌ها هستید فقط آن را پاك کنید.
مشکل را با ارسال مجدد هرزنامه یا پاسخ دادن به آن گسترده‌تر نکنید. پاسخگویي به یك هرزنامه به فرستندگان آن اطمینان مي‌دهد که این نشاني معتبر و در حال استفاده است و لذا هرزنامه‌هاي بیش‌تري را براي شما ارسال خواهند کرد.

ایسنا