
" ...
...يميل رعا...

مقدمه

ایمیل دائمی و در همه جا وجود دارد. میلیاردها پیام هر ماه ارسال و تعداد بی‌شمار دیگری هر هفته و هر روز توسط کاربران دریافت می‌شوند. هرکدام از این پیام‌ها می‌تواند حامل یک حمله، محتوی باج افزار یا روشی برای نابودی کسب‌وکار شرکت شما باشند.

چکیده

متأسفانه، ایمیل آسیب‌پذیر است. راه های بی شماری برای حمله هکرها وجود دارد که به معنای واقعی هر لحظه بدتر می‌شود. از راه‌های محافظت از شبکه در مقابل تهاجمات، رجوع به اصول اولیه و اطمینان یافتن از انجام تمام مراحل مرسوم برای تقویت امنیت ایمیل است. همچنین تکنیک‌های حمله جدید دیگری نیز وجود دارند که باید اقدامات حفاظتی در مقابل آن‌ها انجام شود. در این مطلب مسئله مطرح و سپس ۱۰ راه‌حل برای مشکل آسیب‌پذیری ایمیل بیان می‌شود.

چرا ایمیل این‌قدر آسیب‌پذیر است؟

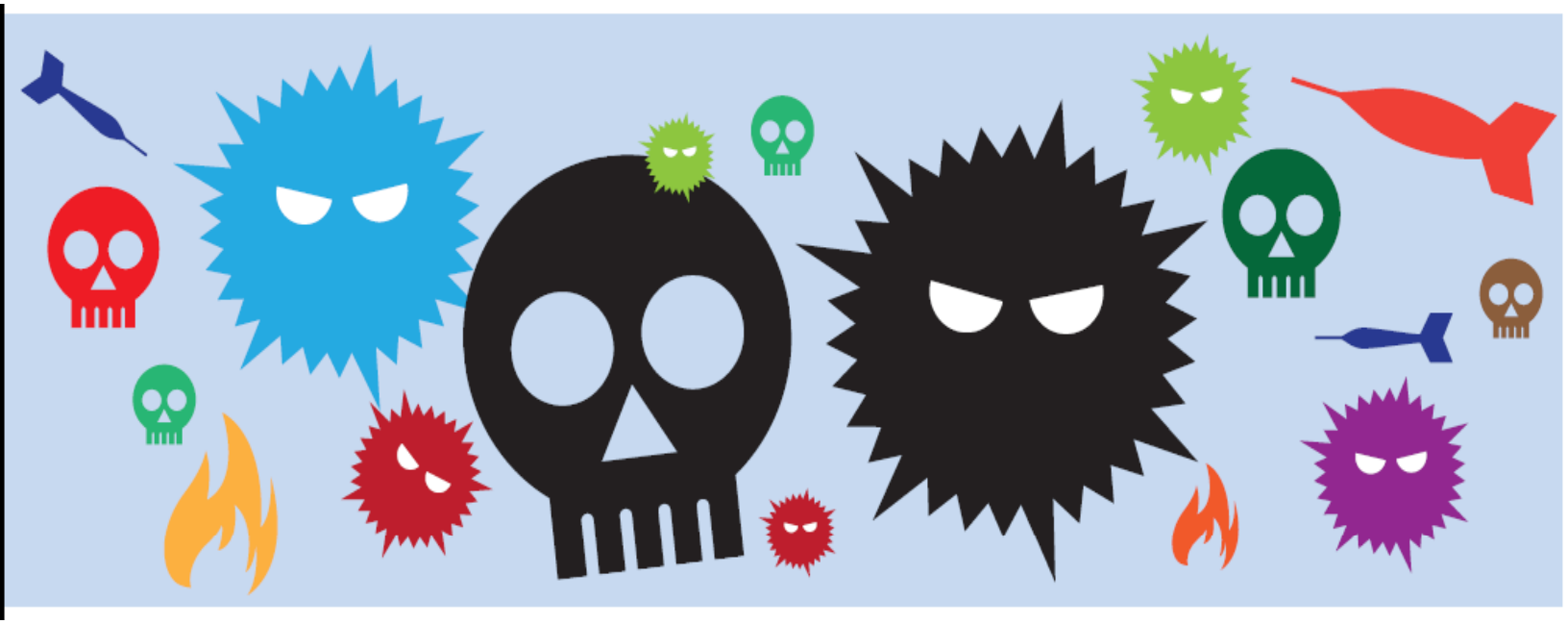
ایمیل می‌تواند روشی ساده برای دسترسی به شبکه توسط مهاجمان باشد. زمانی که آن‌ها به ایمیل نفوذ می‌کنند می‌توانند علاوه بر دسترسی سطح بالا به شبکه، اقدام به حمله گسترده ای کنند. آن‌ها می‌توانند تمام محتوای اطلاعات کاربر مورد هدف را مشاهده و در همان حال هویت وی را جعل کنند.

ایمیل بیش از حد آسیب‌پذیر است. کاربران معمولاً رمزهای عبور ساده و ضعیفی انتخاب می‌کنند و طعمه آسانی برای مهندسی اجتماعی هستند.

کنترل لیست مخاطبان کاربر سرگرمی ربات است. تاکنون چند مرتبه ایمیل‌های جعلی از طرف دوستان و یا همکاران به علت هک شدن لیست مخاطبان آن‌ها دریافت کرده‌اید؟

چه آسیب‌هایی هکرها می‌توانند از طریق ایمیل انجام دهند؟

در سال ۱۹۹۹ حمله‌ای توسط ویروسی خطرناک به نام ملیسا انجام شد. ملیسا از طریق ایمیل، بار محاسباتی سیستم را اضافه کرده و آن را از کار می‌انداخت. ملیسا با ارسال پیامی با این مضمون که سند درخواستی برای شما ارسال شده است لطفاً آن را به کسی نشان ندهید کاربر را به کلیک و دریافت سند مربوطه ترغیب می‌کرد. این حمله لقب عفونت عظیم را به خود اختصاص داد.



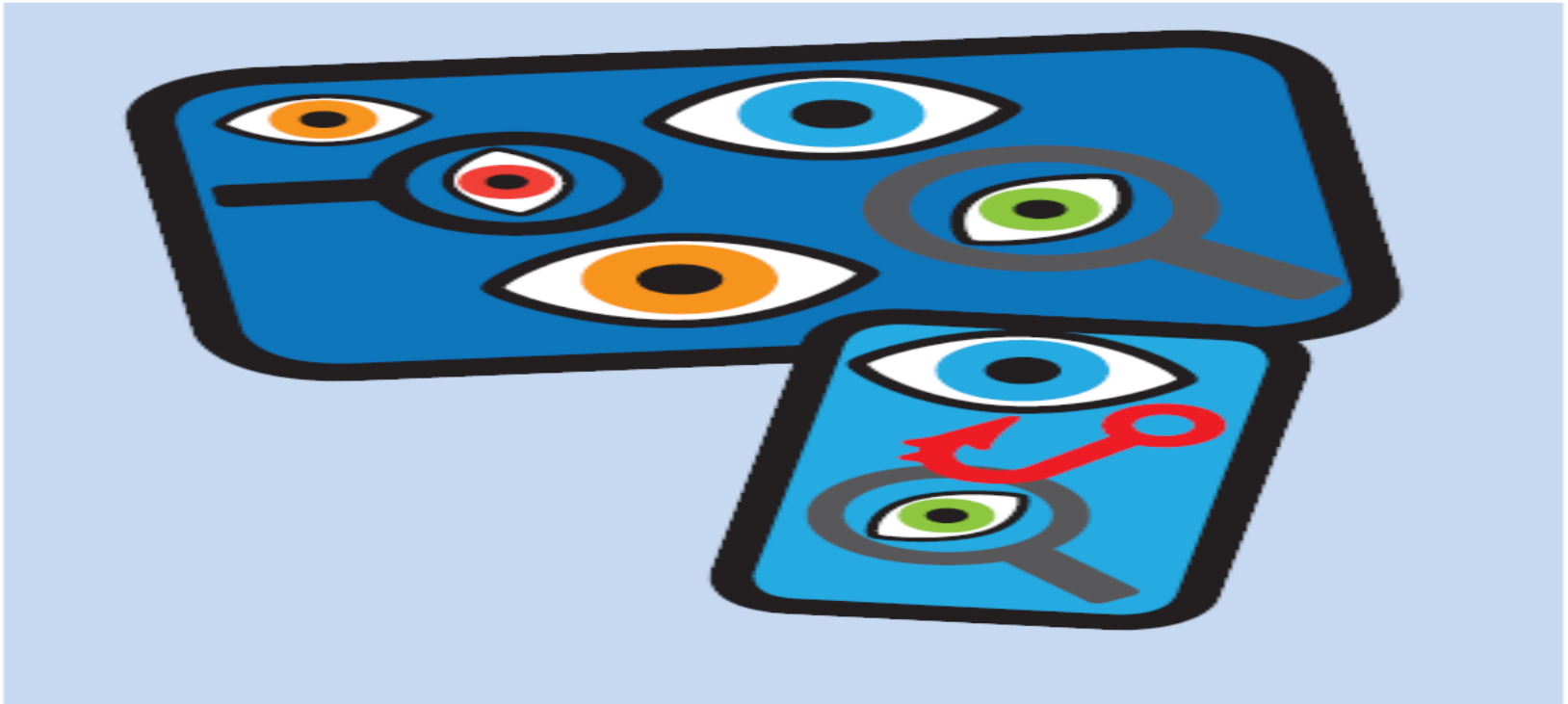
گسترش و شدیدتر کردن حملات:

هکرها به اهدافی که در همه‌جا قابل دسترسی هستند بیشتر علاقمندند. به همین دلیل محصولات مایکروسافت بزرگ‌ترین هدف مورد علاقه هکرها هستند. ایمیل کاربران به طور منظم با فیشینگ، لینک‌های مخرب و حملات لیست مخاطبان روبرو است.

ظهور ایمیل آن را به یک مسئله بزرگ تبدیل کرد. امروزه کاربران، ایمیل‌های شرکتی نیز دارند ولی ممکن است چندین ایمیل اینترنتی نیز داشته باشند که این موضوع خطر حمله را افزایش می‌دهد. موارد استفاده زیاد از ایمیل آن را آسیب‌پذیر می‌سازد. برای بیشتر ما، ایمیل برنامه‌ای است که هنوز بیشترین وقت ما را به خود اختصاص می‌دهد. با این حجم زیاد از ایمیل‌های درست و قانونی، اجتناب از هرزنامه سخت است؛ بنابراین هنگامیکه ایمیل‌های مخرب، خود را در غالب ایمیل‌های قانونی پنهان می‌کنند حتی کاربران حرفه ای نیز می‌توانند قربانی این دسیسه شوند.

ایمیل کانال ایده آلی برای انتشار کرم‌هاست، شکلی از بدافزار که عمدتاً از طریق ایمیل، پخش و تکثیر می‌یابد، به خاطر وجود هکرهای آماتور (بچه اسکریپتی- به فردی گفته می‌شود که بدون

داشتن مهارت و دانش کافی در زمینه‌ی هک کردن و برنامه‌نویسی، با استفاده از اسکریپت‌ها و برنامه‌های آماده شده توسط سایرین به سیستم‌های رایانه‌ای، شبکه‌ها، وب‌سایت‌ها و ... حمله می‌کند.) این کرم‌ها هرگز از بین نمی روند. Win32/Brontk سال‌ها وجود دارد. این کرم کلاسیک از طریق ایمیل تکثیر می‌شود. این کرم‌ها از طریق پیوست ایمیل‌های به ظاهر معمولی منتشر می شوند و آدرس‌ها را با دزدیدن کتاب‌های آدرس کاربران پیدا می‌کنند. بدتر از همه کرم‌هایی مانند این، می‌توانند نرم‌افزار آنتی‌ویروس را خاموش کرده و حتی آدرس ایمیل‌های ربوده شده را برای شروع حملات انکار سرویس DOS به کار ببرند. حمله هوشمندانه جدید دیگر به کلاهبرداری نیجریه ای معروف شد. در این نوع کلاهبرداری مجرمین با ارسال ایمیل‌های فریبنده سعی در اغفال کاربران داشتند. مثلاً خانمی اهل کنیا با ارسال ایمیل هایی به مخاطبان اعلام می کرد که همسرش بعد از عمل قلبی فوت کرده و مبلغی بالغ بر ۱۰ میلیون به ارث گذاشته است و وی هم دچار بیماری سرطان کشنده است و به دنبال مکانی امن برای نگهداری این پول‌هاست. تایید این قبیل دعوت‌نامه‌ها شما را دچار حملات جدی می‌کند. این درخواست‌ها باید بلافاصله حذف شوند. هرگز نباید به هرزنامه پاسخ داد و نباید این قبیل دعوت‌ها را پذیرفت.



معمولاً کارکنان در محل کار از چندین حساب ایمیل استفاده می‌کنند که این خود عامل افزایش تهدید است. بهتر است کاربر در هنگام فعالیت در شبکه شرکت تنها از ایمیل شرکت استفاده کند زیرا این شبکه با ابزارهای دفاع در عمق تجهیز شده است. حساب‌های محافظت نشده منبع اصلی نشت اطلاعات، کرم‌ها و دیگر بدافزارها هستند.

"هرزنامه همچنان یک مشکل است، شاید بیشتر از هر وقت دیگر."

ما غالباً در معرض پیام‌های توهین‌آمیز هستیم، صندوق‌های پستی روزانه با پیام‌های بدرد نخور پر می‌شوند. هرزنامه حاوی بدافزار یا فیشینگ است و به عنوان کانالی مهم برای حملات هک بکار می رود. هرزنامه از همیشه بیشتر خطرناک است، افراد نادرست فقط در تلاش برای فروش محصولات جعلی به شما نیستند، آن‌ها همچنین خواهان دسترسی به اطلاعات ، لیست مخاطبان و حمله به شبکه کامپیوتری شما هستند.

تهدید ThingBot جدید:

امروزه حملات به صورت خودکار درآمده‌اند مانند کرم‌ها. بیشتر دستگاه‌های کوچک و حتی لوازم، دستگاه‌های IP هستند که با همدیگر و با شبکه ما ارتباط برقرار می‌کنند. این به عنوان اینترنت اشیا (IoT) و ماشین به ماشین (M2M) شناخته شده است. مشکل اینست که تعداد دستگاه‌هایی که می‌توانند مورد حمله قرار گیرند به شدت در حال افزایش است. این حملات جدید ThingBot نامیده می‌شوند، آن‌ها این دستگاه‌های نوظهور را برای شروع حملات بات نت بکار می‌برند. شبکه شرکت، برنامه‌های کاربردی و داده‌ها عوامل حیاتی کسب و کار شما هستند.

۱۰ روش برای محافظت از ایمیل

۱- رمزهای عبور مناسب

نخستین و غالباً تنها لایه دفاعی ایمیل رمز عبور است. رمز عبور باید پیچیده باشد. متأسفانه بیشتر رمزهای عبور ضعیف هستند، حتی تعداد زیادی از حساب‌های اشتراکی که توسط افراد حرفه ای ایجاد شده‌اند نیز دارای رمزهای عبور ساده و غیرمعقولی هستند. روش خوب دیگر داشتن رمزهای عبور گوناگون برای ایمیل‌های مختلف و دیگر حساب‌های کاربری است، بنابراین در صورت نفوذ به یکی از حساب‌های کاربری، در امنیت حساب‌های دیگر خللی ایجاد نمی‌شود. اگر تصمیم دارید که فقط با رمز عبور ادمین وارد شوید باید سطح بالایی از پیچیدگی را در انتخاب رمز عبور رعایت کرده و رمز عبور را در فواصل زمانی مرتب تغییر دهید.

ایمیل صرفاً برای ارسال و دریافت پیام بکار نمی‌رود. ایمیل دارای یکپارچگی و لینک‌هایی به فیس بوک و دیگر رسانه‌های اجتماعی است، در سرویس‌هایی از قبیل LinkedIn، Amazon **یا** eBay اطلاعات زیادی در مورد کاربر وجود دارد. اگر هکر موفق به نفوذ به ایمیل شود نخستین کاری که انجام می دهد بررسی نحوه ارتباط این قبیل سرویس ها با رمز عبور است. در صورت نفوذ اطلاعات زیادی در مورد شما بدست آورده، می‌توانند سرقت هویت کرده یا از این اطلاعات برای حملات شخصی دروغین و انجام شرارت‌های دیگر استفاده کند. این حملات به راحتی می‌توانند از طرف شخصی که شما می شناسید انجام شود.

کاربران به کلمات عبور پیچیده (ترکیبی از حروف و اعداد) که به طور منظم تغییر یابند نیاز دارند. آن‌ها به روشی امن برای ذخیره رمز عبور نیاز دارند. نگهداری آن‌ها در یک فایل رمزنگاری شده بهترین روش است.

"رمز عبور را هرگز روی یک کاغذ یادداشت بر روی کامپیوتر نچسبانید یا آن را در کشوی میز قرار ندهید"

۲- نشت اطلاعات را با فیلتر کردن محتوا متوقف کنید.

نشت اطلاعات مشکل بزرگ و رو به رشدی است. آنچه واقعاً نیاز است ۱. سیاستی است که بیان می‌کند اطلاعات مهم تحت هیچ شرایطی نباید بدون تصدیق مدیریتی صریح ارسال شود ۲. ابزاری برای بررسی کلید واژه که ارسال داده‌های نامناسب به بیرون را نشان دهد ۳. اسکن کلید واژه برای ایمیل‌ها و پیوست‌ها (پیوست ها اغلب حاوی ویروس هستند که با ابزارهای اسکن محتوا از بین می‌روند. اسکن باید برای جستجوی عمیق در پیام‌ها مانند اسکن سطر موضوع، بدنه پیام، هدرها و محتوا قابل تنظیم باشد.) ٤- ابزارهای محتوا که انواع مختلف از تکنیک های تطبیق الگو را بکار گیرد.

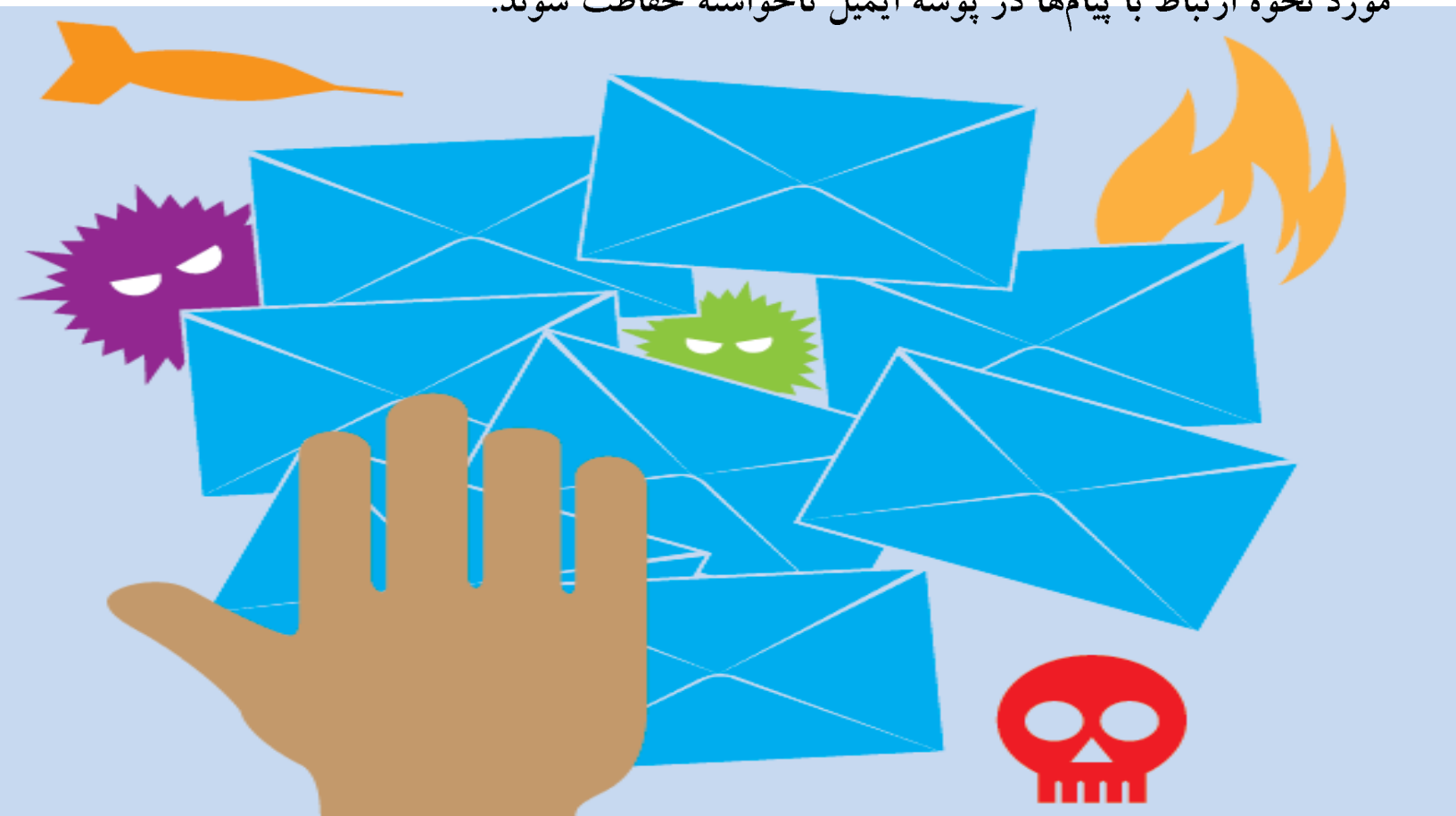
نشت اطلاعات به صورت تصادفی یا عمدی توسط کاربر و تعمداً توسط هکر انجام می‌شود. در بسیاری از این موارد محرمانگی اطلاعات به خطر می‌افتد، رقبا می‌توانند مالکیت فکری یا مالی شما را بدست آورند و هکر می‌تواند اطلاعات شخصی مشتری را بدست آورد. گاهی اوقات کاربران نهایی سهواً اطلاعات محرمانه را ایمیل می‌کنند. گاهی اوقات آن‌ها از لیست توزیع سوءاستفاده کرده و اطلاعات خصوصی را به چندین نفر یا شاید به صدها نفر از گیرندگان ارسال می‌کنند. اکثر نفوذها از طریق کارمندان داخلی است به این علت که کارمندان داخلی اطلاعات شرکت را داشته و به شبکه دسترسی دارند، آن‌ها می‌توانند بیشتر از یک هکر آسیب ایجاد کنند.

این شامل جمع‌آوری و توزیع اطلاعات کارت اعتباری، فروش اطلاعات شخصی پزشکی یا فروش برنامه‌های محرمانه و نتایج می‌شود.

۳- هرزنامه را قبل از اینکه واقعاً آزار دهنده شود متوقف کنید.

هرزنامه فقط یک مزاحم نیست بلکه خطری واقعی برای کسب‌وکار است. فروشگاه‌ها باید از ضد هرزنامه مناسب استفاده کنند. آن‌ها روزانه تعداد زیادی هرزنامه دریافت می‌کنند، بررسی و حذف آن‌ها باعث اتلاف وقت کارمندان می‌شود.

هزینه‌های هرزنامه شامل هزینه پهنای باند برای انتقال پیام‌های بی‌ارزش یا ذخیره‌سازی آنلاین برای نگهداری آن‌ها است. راه‌کارهایی برای جلوگیری از این مزاحمت‌ها وجود دارد که برخی تکنیکی و برخی دیگر مبتنی بر سیاست یا از طریق آموزش انجام می‌شود. سیاست تکنیکی محدود کردن آدرس‌های ایمیل است. کاربران باید حداکثر استفاده از فیلترینگ هرزنامه را داشته باشند و در مورد نحوه ارتباط با پیام‌ها در پوشه ایمیل ناخواسته حفاظت شوند.

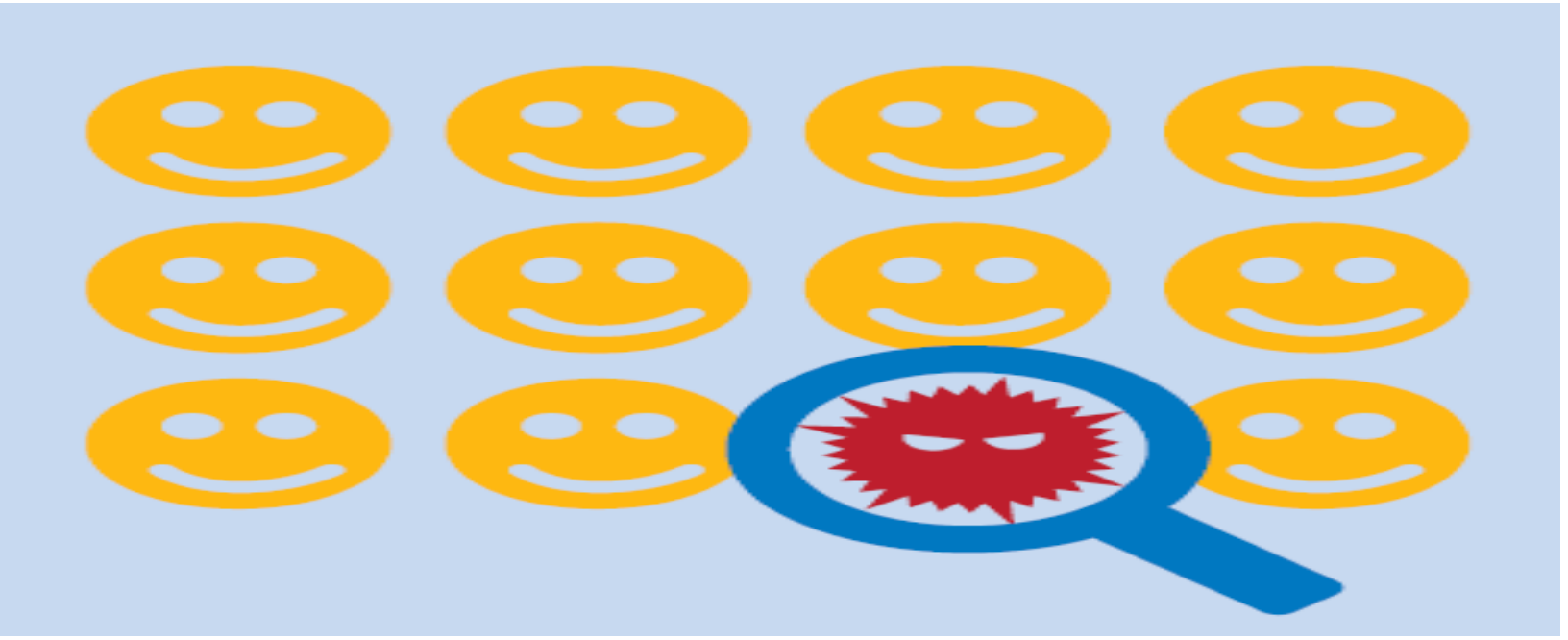


نباید هرگز هرزنامه را باز یا به آن پاسخ دهید، با باز کردن آن دچار حملات فیشینگ یا بدافزار شده و با پاسخ دادن به آن به سادگی اعتبار آدرس ایمیل را تأیید می‌کنید و در نتیجه در معرض حملات نفوذ قرار می گیرید.

٤- کنترل محتوا از طریق فیلترینگ و نظارت:

فناوری اطلاعات و مدیران بالایی داده‌هایی مانند گزارش‌های مالی، داده‌های مشتری، محصولات منتشر نشده و استراتژی‌ها را با ارزش‌ترین منابع خود می‌دانند. این داده‌ها اگر دزدیده شوند مسائل زیادی به خطر می‌افتد.

خطر دیگر محتوای نامناسب است.



بسیاری معتقدند که تنها تهدید امنیتی واقعی از طرف هکرهای بیرونی است اما تهدید داخلی می‌تواند بسیار خطرناک تر باشد. با استفاده از ایمیل، کاربران نهائی در اکثر مواقع حتی خود نمی‌دانند که مسبب مشکلات شده‌اند.

برخی از مشکلات مانند گسترش بدافزار یا افشای داده‌های شرکتی به‌وسیله سقوط ناخواسته قربانی در فیشینگ به وجود می‌آیند. کنترل و مانیتورینگ محتوای ایمیل نجات دهنده است. روش‌های بی‌شماری برای پیاده سازی این آسیب‌ها وجود دارد، نشت اطلاعات، شکایات جنایی در صورتیکه ایمیل برای نقض قوانین و مقررات به کار رفته باشد. اغلب دادگاه‌ها سازمان‌ها را مسئول رخداد اتفاقاتی که در سیستم از طریق ایمیل روی می‌دهد، می‌دانند. مانیتورینگ محتوای ایمیل می‌تواند به حل بیشتر این مشکلات، حفاظت از شرکت از طریق مسدود کردن پیام‌های نامناسب کمک کند.

ابزارهای امنیت محتوای ایمیل در توقف نشت اطلاعات مؤثر هستند، همچنین اتلاف وقت با کارهای بیهوده مانند قمار آنلاین را پایان می‌دهند.

۵- بدافزار را از بین ببرید.

مانند هرزنامه، برای حفاظت درست به چندین ضد بد افزار نیاز است. فیلترینگ محتوا روش دیگری برای مبارزه با حملات روز صفر است. فیلترینگ خوب انواع ضمیمه‌هایی که احتمالاً حامل ویروس هستند را شناسائی و مسدود می‌کند.

٦- حفره‌های امنیتی را مسدود کنید.

بیشتر حملات ایمیل با هدف جاسوسی است. این حملات توسط مجرمان یا سازمان‌های مربوط به دولت راه اندازی می‌شوند. برخی حملات در چین ساخته شده که اغلب در غالب ایمیل فیشینگ هستند، با یک‌بار کلیک برای بارگیری بدافزار روی کامپیوتر کاربر نصب می‌شود.

۷- متابعت از قاعده (انطباق)

همه این مسائل برای شرکت‌هایی که توسط مقررات انطباق حفاظت می‌شوند جدی است. ایمیل و محتویات آن باید امن باشند. انطباق فقط راهنما نیست بلکه فرمان است.

۸- آموزش و بهترین شیوه‌ها:

فناوری اطلاعات برای راه‌اندازی تکنولوژی حل مشکلات فنی بکار می‌رود، چنانکه آن‌ها فایروال‌ها، ضد بدافزار و دیگر دستگاه‌ها را پیاده‌سازی می‌کنند. متأسفانه این روش‌های دفاعی همیشه به اندازه کافی عمیق نیستند. یک مسئله رفتار کاربر است. همه این روش‌های دفاعی در جهان نمی‌تواند در برابر یک کارمند فریب خورده، دفاعی انجام دهند. آموزش به طور خاص به مسائل مربوط به مسدود کردن فیشینگ می‌پردازد.

لینک امنیتی ضعیف، کاربران نهایی هستند. کارکنان اثبات کرده‌اند که عامل ضعیفی در امنیت اینترنت شرکت‌ها هستند. در بیشتر موارد، درگیر شدن آن‌ها در مسائل غیرعمدی است. آن‌ها ندانسته به سادگی اجازه دسترسی به شبکه شرکت را می‌دهند برای اینکه نمی‌دانند چه کارهایی را نباید انجام دهند.

بعضی کلاهبرداری ها به دلیل اینکه کاربران کافی که آموزش‌های لازم را برای مقابله با آن گذرانده باشند کم است هرگز از بین نمی‌روند. کارمندان آموزش دیده به عنوان فایروال انسانی عمل می‌کنند.

تهدید ناشی از بدافزارها نیز نباید دست کم گرفته شود.

جدول نکات و ترفندهای آموزشی:

- ✓ هرگز روی لینکی در ایمیل که صد در صد به آن اطمینان ندارید کلیک نکنید.
- ✓ هرگز به هرزنامه‌ها پاسخ ندهید.
- ✓ هرگز فایل پیوست را باز نکنید مگر اینکه شما آن را خواسته یا دقیقاً می‌دانید که محتوای آن چیست.
- ✓ هرگز به ایمیلی که منتظر آن نیستید پاسخ ندهید حتی اگر این‌طور به نظر بیاید که از طرف بانکتان است.
- ✓ بکارگیری ابزارهای امنیتی ضد هرزنامه: اطمینان حاصل کنید که تنظیمات و سیاست‌ها، نیازهای امنیتی شما را برآورده می‌کند.
- ✓ اگر فکر می‌کنید که روی لینک نادرستی کلیک کرده اید یا کاری برای شروع یک حمله را انجام داده اید بلافاصله اسکن را شروع کنید یا دستگاه را سریع خاموش کرده و از متخصص فناوری اطلاعات قبل ازگسترش مشکل کمک بگیرید.
- ✓ ضد بدافزار خود را به طور مرتب اجرا کنید. آن را به روز نگهدارید و اگر مشکوک هستید که سیستم مشکلی دارد بلافاصله یک اسکن کامل انجام دهید.

جدول نکات و ترفندهای آموزشی:

- ✓ مراقب Wi-Fi عمومی باشید.
- ✓ یک ایمیل جداگانه و غیر سازمانی را برای استفاده شخصی در نظر بگیرید. اما با این ایمیل هم مانند ایمیل شرکت رفتار کنید و آن را زمانی که در شبکه شرکت هستید استفاده نکنید.
- ✓ مراقب باشید که آدرس خود را در فرم‌ها، وبلاگ ها و وب سایت ها پر نکنید. چرا که هکرها می‌توانند به این سایت‌ها نفوذ کرده و آدرس ایمیل شما را به لیست هرزنامه خود اضافه کنند. اگر فکر می کنید که باید حتماً آدرس ایمیل وارد کنید، آدرس ایمیل شخصی را به جای آدرس شرکتی وارد کنید.
- ✓ برنامه های کاربردی را به روز نگهدارید و وصله های امنیتی را دریافت و نصب کنید.
- ✓ از نرم افزارهای قانونی استفاده کنید.
- ✓ قبل از اینکه فایل پیوست را باز کنید مطمئن شوید که قانونی و درست است.
- ✓ پیام‌های غیرعادی را باز نکنید حتی اگر از طرف دوستان، خانواده و یا همکاران باشد.
- ✓ فیشینگ و دیگر حملات را به شرکت‌های امنیتی گزارش کنید.
- ✓ اگر دعوت غیرمنتظره ای دریافت کردید آن را حذف و در صورت شناخت فرستنده با وی تماس گرفته تا از صحت آن مطلع شوید.

۹- مبارزه با فیشینگ:

افراد خاطی در ارسال فیشینگ مصر هستند که این دلیل موفقیت فیشینگ است. آموزش شناسایی فیشینگ نیمی از معادله پیشگیری است. نیم دیگر ابزارهای قوی است که می توانند پیام‌های فیشینگ را کشف و مسدود کنند.

گرامر بد و املای نادرست مسائلی است که در فهمیدن فیشینگ به ما کمک می‌کند،این موارد به ویژه در پیام‌های فیشینگ ارسالی از چین و شرق اروپا قابل مشاهده است.

۱۰- پیاده‌سازی دفاع در عمق:

آموزش کاربران برای شناسانی ایمیل‌های مخرب و حملات مهندسی اجتماعی حیاتی است ولی مهم‌تر، داشتن دفاع فنی مناسب است. این به معنای حفاظت در برابر تمام اشکال نفوذ و نشت اطلاعات است. بدان معنی است که:

- ضد ویروس/ ضد بد افزار
- حفاظت از هرزنامه
- فیلترینگ محتوا

بهتر است همه این ابزارها یکپارچه شوند.

منبع:

[1] https://www.gfi.com

لیدا رسول اهری- کارشناس آموزش و پژوهش اداره پدافند غیر عامل استانداری