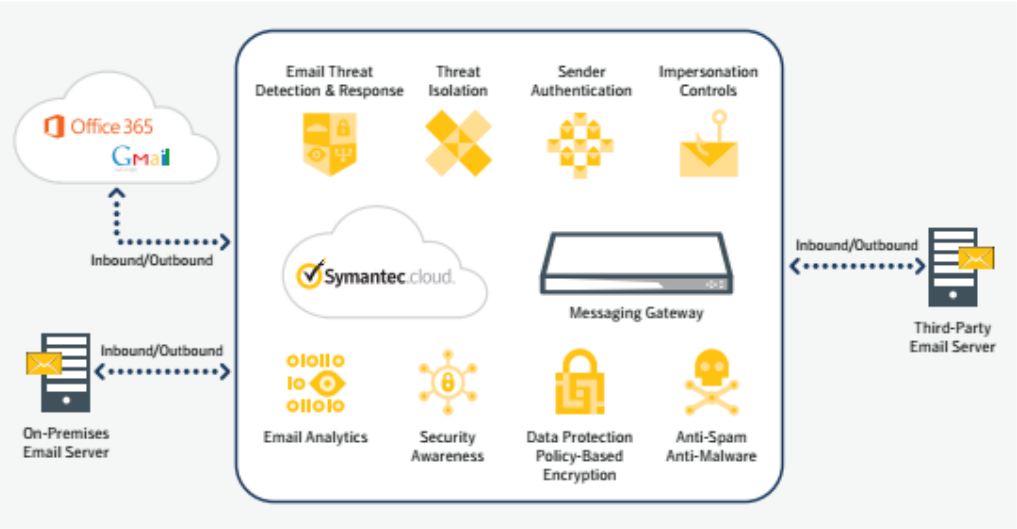
امنیت پست الکترونیک در سازمان ها

دفاع چند لایه در برابر تهدیدات محیط پست الکترونیک

HAUMOUN
IT PIONEERS
پیشگامان فناوری اطلاعات هامون

Symantec

امنیت پست الکترونیک در سرویس ابری یا ابزارهای درون سازمانی



مواجهه با چالش های تضمین امنیت در فضای پست الکترونیک

امنیت پست الکترونیک جامع و هوشمند، چه سیستم پست الکترونیک شما درون سازمانی باشد، چه مبتنی بر فضای ابری یا هر دو، با درکی شفاف و واقعی از آنچه قصد مبارزه با آن را دارید شروع می شود. پست الکترونیک هنوز محبوب ترین راه برای مجرمان سایبری برای اجرا و توزیع تهدیدها است. بر اساس گزارش تهدید امنیت اینترنتی Symantec (ISTR) ۲۰۱۸، در سال ۲۰۱۷ از هر ۴۱۲ پست الکترونیک یک پست الکترونیک حاوی حمله بدافزار بوده است، هر ماه ۷،۷۱۰ سازمان هدف رخنه به پست الکترونیک های سازمانی (BEC) قرار گرفته و اسپیرفیشینگ پرکاربردترین ابزار انتشار ویروس است که توسط ۷۱ درصد گروه های حملات هدفمند استفاده می شود.

با افزایش حجم این حملات، سطح پیچیدگی آنها نیز افزایش می یابد. شناسایی و توقف تهدیدهای پیشرفته و روز صفر سخت تر از بدافزارهای سنتی است، درحالیکه ثابت شده ابزارهای ضد بدافزار مبتنی بر امضا عمدتا دربرابر آنها کارایی ندارند. اکنون مهاجمان به اسپیر فیشینگ هدفمند علاقه نشان می دهند، مخصوصا به شکل کلاهبرداری های نفوذ به پست الکترونیک های سازمانی. این حملات هدفمند خطرناک و گیج کننده از روش های پیچیده ای مثل جعل دامنه و مغشوش کردن لینک های مخرب که در پیام های پست الکترونیک جاسازی شده استفاده می کنند. زیان حاصل از این حملات اکنون ۱۲،۵ میلیارد دلار بوده و در طی ۱۷ ماه، ۱۳۶ درصد رشد کرده است.

اهداف با ارزش مثل مدیران اجرایی یا تیم های مالی بیشتر در معرض خطر هستند، زیرا آنها معمولا به داده ها و سیستم های حساس دسترسی دارند. همچنین، کاربران ناآگاه از تهدیدهای پست الکترونیک در مقابل حملات پیشرفته آسیب پذیرند، مسئله ای که خطرات امنیتی را برای سازمان افزایش می دهد.

استفاده سریع از مایکروسافت آفیس ۳۶۵ و Google G Suite نحوه تحویل سرویس های پیام رسانی دپارتمان های IT به سازمان های خود را تغییر می دهد. این سرویس های پست الکترونیک مبتنی بر فضای ابری در مقایسه با پست الکترونیک درون سازمانی سنتی، با کاهش سربار عملیاتی، هزینه ها را به طور قابل توجهی کاهش می دهند. و ارائه دهنده هر دو سرویس اشاره می کنند که پست الکترونیک آنها به همراه قابلیت ضد بدافزار و محافظت در برابر هرزنامه عرضه می شود. اما این قابلیت های درونی چقدر می تواند کامل و موثر باشد؟ چه مسائل امنیتی را باید هنگام آمادگی سازمان خود برای مهاجرت به پست الکترونیک مبتنی بر فضای ابری درنظر داشته باشید؟

سازمان ها برای رسیدن به یک راه حل امنیت پست الکترونیک کامل و یکپارچه از بین چندین محصول تکی که هرکدام تنها بخشی از مشکل امنیت پست الکترونیک را حل می کنند مشکلات زیادی دارند. از آن بدتر، اغلب راه حل های امنیت پست الکترونیک با بقیه زیرساخت های امنیتی شما (مثل Endpoint Protection، امنیت شبکه، SIEM ها و SOC ها) ادغام نمی شوند، که این مسئله بار یکپارچه سازی پیچیده را به دوش تیم های امنیت IT می گذارد. همه این مسائل در کنار کمبود پرسنل آموزش دیده امنیت IT باعث می شود سازمان ها پیچیدگی عملیات و شکاف در معماری امنیتی خود داشته باشند و از این رو در مقابل حملات چندبرداری پیچیده آسیب پذیر باشند.

درآخر، سازمان ها برای پیشگیری از افشای داده های حساس هنگام به اشتراک گذاری اطلاعات توسط کاربران از طریق پست الکترونیک سخت تلاش می کنند. این داده ها باید امن و خصوصی نگهداری شوند تا نیازهای امنیتی، حقوقی و انطباق با استانداردهای امنیت اطلاعات برآورده شود. افشای آنها می تواند به آسیب دیدن برند و اعتبار شرکت، جریمه های قانونی و در نهایت، زیان های مالی و حتی ورشکستگی مالی منجر شود.

➢ استفاده از کامل ترین راهکار امنیت پست الکترونیک

شرکت Symantec کامل ترین پرتفوی امنیت پست الکترونیک درون سازمانی و ابری را در این صنعت ارائه می دهد. این راهکار از چند لایه فن آوری های امنیتی تشکیل شده است و از توانمندی بزرگترین شبکه اطلاعاتی تهدیدهای سایبری غیرنظامی دنیا، یعنی Symantec Global Intelligence Network (GIN) استفاده می کند که تصویر واضحی از تهدیدها سایبری را در سراسر دنیا ارائه می دهد. GIN از طریق دور سنجی بدست آمده از ۱۷۵ میلیون کاربر، ۸۰ میلیون کاربر پروکسی وب و ۵۷ میلیون سنسور تشخیص حمله در ۱۵۷ کشور به تضمین نتایج بهتر در تامین امنیت کمک می کند. امنیت پست الکترونیک Symantec بخشی از پلتفرم دفاع سایبری یکپارچه ما است که امنیت وب، Endpoint و پست الکترونیک، تحلیل تهدیدها، هماهنگ سازی و اتوماسیون امنیت و غیره را پوشش داده و با هم ترکیب می کند.

➢ امنیت پست الکترونیک Symantec: قابلیت ها

پرتفوی امنیت پست الکترونیک Symantec شما را قادر می سازد تا:

- **از تهدیدهای رو به رشد و روز صفر پیشگیری کنید**

- مسدودسازی هرزنامه ها، بدافزارها و تهدیدهای پست الکترونیکی پیشرفته مثل اسپیر فیشینگ، باج افزارها و BES با تعدیل فن آوری های شناسایی چندلایه نظیر یادگیری ماشین، تحلیل رفتار، کنترل های جعل هویت کاربر و دامنه و اعتبار فرستنده، فایل و IP. چند موتور پایش پست الکترونیک ناخواسته مثل هرزنامه، خبرنامه ها و پست الکترونیک های بازاریابی را متوقف می کند.
- پیشگیری از پیچیده ترین و دائمی ترین تهدیدهای پست الکترونیکی با تکنیک جعبه شنی آگاه از ماشین و برون ریزی کدهای مخرب که با توانمندی ماشین یادگیری پیشرفته، تحلیل ترافیک شبکه و تحلیل رفتار انجام می شود.
- مسدودسازی حملات پیشرفته فیشینگ که لینک را بعد از تحویل پست الکترونیک برای حمله تجهیز می کند. Link Protection لینک ها را در زمان واقعی، هم قبل از تحویل پست الکترونیک و هم در زمان کلیک روی پست الکترونیک، آزمایش و ارزیابی می کند. Link Protection لینک

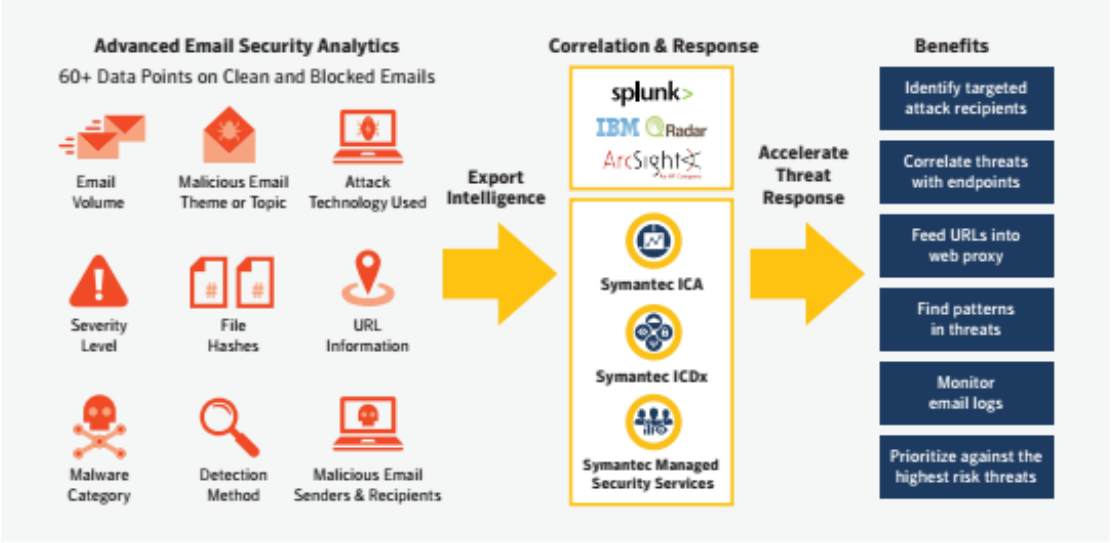
ها را تا مقصـــد نهایی آنها دنبال می کند، حتی وقتی مهاجمان تلاش می کنند با تکنیک های پیشـرفته، شـناسـایی را دور بزنند. همچنین، چون مجرمان سـایبری اغلب کدها را در حملات جدید مجددا استفاده می کنند، ما از شناسایی گونه های پیشرفته فیشینگ برای پیدا کردن و مسدودسازی لینک های اسپیرفیشینگی که شبیه حملات فیشینگ شناخته شده هستند استفاده می کنیم.

- **URL های پست الکترونیک را برای تامین حداکثری امنیت ایزوله کنید**

- دفاع از کاربران دربرابر ا سپیرفیشینگ و حملات پیشرفته با اولین فن آوری ایزوله سازی تهدیدهای پســـت الکترونیک ، اجرا یا پرداخت (Render) از راه دور لینک های مشـــکوک وب در یک محیط اجرایی امن ضمن اسکن دانلودها از این سایت ها قبل از تحویل آنها به دستگاه کاربر.
- پیشگیری از سرقت داده های محرمانه با قراردادن وب سایت های مشکوک در وضعیت فقط خواندنی که کاربران را از ارسال داده های حساس مثل گذرواژه های شرکت منع می کند.

- **سریعا به تهدیدهای امنیتی واکنش نشان دهید**

- عمیق ترین دید به حملات پست الکترونیکی پیشرفته و هدفمند با گزارش مفصل درباره هر پست الکترونیک تمیز و مخرب ورودی که اسکن شده است: بیش از ۶۰ نقطه داده مثل URL، هش های فایل، داده های فرستنده/گیرنده و اطلاعات حمله هدفمند.
- شـتاب بخشـیدن به واکنش به حملات هدفمند و پیشـرفته با اطلاعات غنی از تهدیدها که از طریق ادغام API با SEIMهای طرف ثالث یا پایش توســط Symantec Managed Security Services به Security Operation Center شما منتقل شده است.
- همبســتگی پســت الکترونیک، Endpoint، وب و دیگر نقاط کنترل امنیت در راســتای رفتار کاربر برای درک کامل بیشترین خطراتی که شما برای عملیاتی سازی واکنش درست با آنها مواجهید.



- **کاربران را برای جلوگیری از تهدیدها با آگاهی بخشی امنیت سایبری و آموزش آماده کنید**

  - ارزیابی آمادگی کارمندان برای شناسایی حملات فیشینگ با ارزیابی های امنیتی که تقلیدکننده تهدیدهای جهان واقعی است؛ ارزیابی ها را می توان برای تحقق نیازهای سازمان شما و تطابق با زمینه تهدید درحال تکامل سفارشی سازی کرد.
  - ردیابی پیشرفت آگاهی کارمندان درباره امنیت در طول زمان با ارزیابی های به روز رسانی شده و گزارش مفصل.
  - ایجاد پرتفوی ریسک کاربران با ترکیب نتایج ارزیابی با تحلیل های امنیت پست الکترونیک

- **از داده های حساس در پست الکترونیک محافظت کنید**

  - حفظ داده های حساس و بررسی نیازهای حقوقی و تطبیقی با کنترل های داخلی پیشگیری از مفقودی؛ تقویت تطبیق قانونی و پیشگیری از نشت داده ها با انتخاب از میان فهرست موسطی از قالب های از پیش ساخته شده و قابل سفارشی سازی.
  - تضمین امنیت و حریم خصوصی پست الکترونیک های محرمانه باکنترل های رمزگذاری مبتنی بر سیاست که به طور خودکار پست الکترونیک های خروجی خاص را رمزگذاری می کند.

- **در اکوسیستم امنیت IT و سیمانتیک ادغام شوید**

- پلاتفرم امنیت پست الکترونیک Symantec بخش لاینفک پلتفرم دفاع سایبری یکپارچه Symantec است که محافظت چندکانالی کامل شامل تحلیل تهدیدها، مسدودسازی، ترمیم و غیره را در وب، Endpoint، پست الکترونیک و اپلیکیشن های ابری ارائه می دهد؛ این راه حل که مورد پشتیبانی شبکه اطلاعاتی Symantec GIN است به طور متراکم تغذیه شده و با استفاده از برترین فناوری های Symantec تولید شده است.
- ادغام یکپارچه با Symantec Data Loss Prevention باعث تقویت پلاتفرم پست الکترونیک برای سیاست های حفظ داده می شود.
- کتابخانه گسترده API امکان یکپارچه سازی با SIEM شخص ثالث و ابزارهای صدور شماره (ticketing)، تقویت فرآیندهای عملیات امنیتی برای بیشترین کارایی و واکنش هماهنگ را امکان پذیر می سازد.

➢ محصولات امنیت پست الکترونیک شرکت Symantec

- **محصول Symantec Messaging Gateway**

به خاطر قوانین سختگیرانه صنعت، نظارت بر داده ها و الزامات شرکت برای حفظ کنترل کامل بر زیرساخت پست الکترونیک، پیام رسانی درون سازمانی به این زودی ها از بین نمی رود. برای بسیاری از سازمان ها، راه حل های امنیتی برای پست الکترونیک درون سازمانی همانند پست الکترونیک های تحویل شده در فضای ابری حائز اهمیت هستند.

Symantec Messaging Gateway امنیت پیام رسانی درون سازمانی ورودی و خروجی را فراهم می کند که شامل محافظت قدرتمند دربرابر آخرین تهدیدهای پیام رسانی و قابلیت های حفظ داده داخلی برای ایمن و محرمانه نگاه داشتن پست الکترونیک های شما می شود. این محصول بیش از ۹۹ درصد اسپم ها را

به دام انداخته، کمتر از ۱ در ۱ میلیون خطای مثبت را ثبت کرده و به طور موثر به تهدیدهای پیام رسانی جدید با به روزرسانی های ضداسپم و ضدبدافزار اتوماتیک در زمان واقعی پاسخ می دهد.

Messaging Gateway با Symantec Content Analysis برای محافظت پیشرفته دربرابر فایل های مخرب، با Symnatec DLP جهت محافظت در برابر نشت اطلاعات و با Symantec Web Isolation برای سطوح بالاتر محافظت از لینک ادغام می شود.

- **محصول Mail Security for Microsoft Exchange**

این محصول به شما کمک میکند تا محدود حفاظت از ایمیل رو به Mailbox کاربران گسترش دهید و حتی بعد از دریافت ایمیل ها نیز بر روی آن ها کنترل داشته باشید.

Mail Security for Microsoft Exchange میتواند فایل های آلوده Zero Day که ممکن است در زمان دریافت شناسایی نشوند را در Mail Box کابران شناسایی کند و همچنین آیمیل های ناخواسته که ممکن است در لایه Messaging Gateway شناسایی نشده باشند حذف نماید.

امکان جستجوی ایمیل های قرنطینه شده و امکان محافظت در هنگام ارسال و دریافت ایمیل های درون سازمانی از دیگر قابلیت های این محصول می باشد.