۱۵ شیوه برای محافظت کسب و کار در مقابل حملات سایبری

گذر واژه

سیاست های امنیتی را در شبکه خود اعمال کنید. برای مثال: دسترسی به ذخیره سازی فایل USB را محدود کنید ، خط مشی های رمز عبور پیشرفته را فعال کنید ، زمان استفاده از صفحه نمایش کاربر را محدود کنید و دسترسی کاربر را محدود کنید.

Spam Email

ایمیل خود را ایمن کنید. بیشتر حملات از ایمیل شما سرچشمه می گیرند. ما به شما کمک می کنیم سرویسی را انتخاب کنید که برای کاهش هرزنامه و قرار گرفتن در معرض حملات به کارکنان از طریق ایمیل طراحی شده است.

ارزیابی امنیتی

ایجاد یک خط پایه و بستن آسیب پذیری های موجود بسیار مهم است. آخرین ارزیابی شما چه زمانی بوده است؟

تشخیص و پاسخ پیشرفته نقطه پایانی

از داده های رایانه خود در برابر بدافزارها ، ویروس ها و حملات سایبری با امنیت نقطه پایانی پیشرفته محافظت کنید. جدیدترین فناوری امروزی (که جایگزین آنتی ویروس قدیمی شما می شود) در برابر تهدیدات بدون فایل و مبتنی بر اسکریپت محافظت می کند و حتی می تواند حمله باج افزار را بازگرداند.

آیا میدانستید

1 in 5 مشاغل کوچک امسال دچار نقص سایبری می شوند.

81% همه تخلفات برای مشاغل کوچک و متوسط رخ می دهد.

97% با استفاده از فناوری امروزی می توان از تخلفات جلوگیری کرد.

آگاهی از امنیت

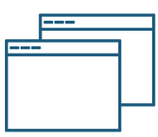
کاربران خود را آموزش دهید - اغلب! در مورد امنیت داده ها ، حملات ایمیل و خط مشی ها و رویه های خود به آنها آموزش دهید. ما یک راه حل آموزشی مبتنی بر وب و سیاست های امنیتی "انجام شده برای شما" ارائه می دهیم.

تحقیقات Dark WEB

دانستن بلادرنگ گذرواژه ها و حساب هایی که در Dark Web ارسال شده اند به شما این امکان را می دهد تا در جلوگیری از نفوذ به داده ها پیشقدم باشید. ما Dark Web را اسکن می کنیم و برای محافظت از کسب و کار شما در برابر اطلاعات سرقت شده که برای فروش ارسال شده است، اقدام می کنیم.

بروز رسانی رایانه

برای امنیت بیشتر محصولات مایکروسافت ، Adobe و جاوا را به روز نگه دارید. ما یک سرویس "به روز رسانی مهم" را بصورت خودکار ارائه می دهیم تا از رایانه های شما در برابر آخرین حملات شناخته شده محافظت کند.



احراز هویت چندگانه

هر زمان که می توانید از احراز هویت چند عاملی استفاده کنید ، از جمله در شبکه ، وب سایت های بانکی و حتی رسانه های اجتماعی. این یک لایه حفاظتی اضافی به شما می دهد تا اطمینان حاصل کنید که حتی اگر رمز عبور شما به سرقت برود ، اطلاعات شما محافظت می شود

امنیت دستگاه موبایل

مجرمان سایبری امروز سعی می کنند داده ها را سرقت کرده یا از طریق تلفن و رایانه کارکنان شما به شبکه شما دسترسی پیدا کنند. آنها روی شما حساب می کنند که از این قطعه پازل غافل می شوید. امنیت دستگاه های تلفن همراه این فاصله را برطرف می کند.

امنیت گیت وی وب

امنیت اینترنت یک مسابقه با زمان است. امنیت مبتنی برشبکه ابری تهدیدات وب و ایمیل را هنگام بروز در اینترنت تشخیص می دهد و آنها را در عرض چند ثانیه قبل از رسیدن به کاربر مسدود می کند.

مدیریت رخدادهای امنیتی

(Security Incident & Event Management)

از موتورهای داده بزرگ جهت بررسی کلیه گزارشات رویداد و امنیت همه دستگاه های تحت پوشش برای محافظت در برابر تهدیدات پیشرفته و برآوردن الزامات انطباق استفاده می کند.

پشتیبان گیری

پشتیبان گیری محلی انجام دهید. پشتیبان گیری از شبکه ابری صورت گیرد. برای هر ماه از سال یک نسخه پشتیبان تهیه کنید. پشتیبان گیری خود را اغلب آزمایش کنید. و اگر مطمئن نیستید پشتیبان گیری شما به درستی کار می کند، در اسرع وقت با ما تماس بگیرید.

رمزنگاری

در صورت امکان، هدف رمزگذاری پرونده ها می باشد، به ویژه در دستگاه های تلفن همراه

Firewall

قابلیت تشخیص و پیشگیری از نفوذ را روشن کنید. فایلهای گزارش را به SIEM مدیریت شده ارسال کنید. اگر تیم فناوری اطلاعات شما نمی داند این موارد چیست، همین امروز با ما تماس بگیرید!

اگر همه چیز با شکست مواجه شد ، از درآمد و کسب و کار خود با بیمه نامه های خسارت سایبری و بازیابی محافظت کنید.