Medanet

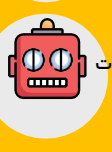
۱۰ کنترل امنیتی
برای امنیت سایبری موثر

نگه داشتن موجودی نرم افزار مجاز و غیر مجاز

باید مطمئن شوید که می توانید تمامی نرم افزارهای موجود در شبکه سازمان را به نحوی نگهداری کنید که امکان شناسایی و حذف نرم افزار ممنوعه میسر شود و همچنین از خطر استفاده از نرم افزار ناشناخته مطلع شوید..

سال ۲۰۱۶ بدافزار میرای Mirai اعلان موجودیت کرد!

سال ۲۰۱۷ بدافزار rickerbot و CloudPet

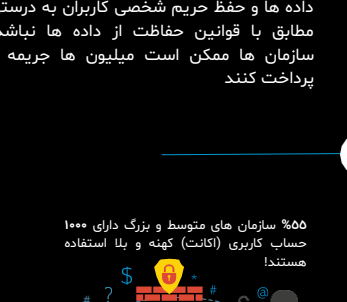


و در سال ۲۰۱۹ باید منتظر حملات وسیع تری باشیم!

نگه داشتن موجودی سخت افزار مجاز و غیر مجاز

نگهداری و محافظت از سخت افزارهای شبکه از راه دور - یعنی اینکه به سادگی تشخیص دهید که آیا دستگاه متصل شده به شبکه، لپ تاپ است یا تلفن همراه- این موضوع را هرگز نباید را نادیده گرفت، زیرا هر دستگاهی فرصتی برای نفوذ در شبکه بوجود می آورد. مدیریت رمزگذاری و مدیریت متمرکز می تواند در این زمینه کمک حال شما باشد.

به یاد داشته باشید:
روزانه ۲۳۰ هزار بدافزار شناسایی می شود.



پیکربندی ایمن سخت افزار و نرم افزار

دقت کنید تنظیمات سفارشی سخت افزارها و نرم افزارها می تواند به کاهش هر دو حملات سخت افزاری و نرم افزاری کمک کند.

هر ۳۹ ثانیه یک حمله سایبری رخ می دهد و از هر ۳ نفر ۱ نفر در آمریکا قربانی حملات سایبری شده است.

به طور مداوم شبکه را برای بهبود آسیب پذیری، ارزیابی کنید

آسیب ها همه جا هست مطمئن شوید که نرم افزارها و سیستم عامل ها را همواره به روز نگاه میدارید و پاچ های آپدیت آنها را نصب می کنید.

تا سال ۲۰۲۰، ۹۹ درصد از سوء استفاده کنندگان به مدت حداقل یک سال به عنوان متخصص امنیت و فناوری اطلاعات شناخته خواهند شد.

میانگین هزینه از بین رفتن اطلاعات ناشی از حملات سایبری تا سال ۲۰۲۰ بیش از ۱۵۰ میلیون دلار خواهد شد.

از سال ۲۰۱۳ هر روز:
۳,۸۰۹,۴۴۸ پرونده از طریق نقض امنیتی به سرقت رفته
۱۵۸,۷۲۷ در هر ساعت
۲,۶۴۵ در هر دقیقه
و ۴۴ در هر ثانیه

همواره کنترل استفاده از دسترسی ها و مجوزات اداری را بطور دقیق در دست داشته باشید.

با GDPR و DPB (قوانین حفاظت از داده ها) که در حال حاضر امسال در حال اجرا است، امنیت جامع اطلاعات، تنها حسن نیت کسب و کار خوب نیست، بلکه یک امر اجباری است.

حفاظت از مرورگرها

نرم افزارهای مخرب جدید نظیر بدافزارهای ارز دیجیتال به طور فزاینده ای مرورگرها را آلوده می کنند تا از آنها بعنوان استخراج کننده ارز دیجیتال یا ماینتر استفاده کند.

64% از سازمان ها حملات مبتنی بر وب را تجربه کردند

62% از سازمان ها حملات مهندسی اجتماعی و فیشینگ را تجربه کردند

93% ایمیل های دریافتی ناشناس باج افزار است.

باج افزاری بنام Eternalblue برای پورت شبکه هست که بیش از ۳۰۰،۰۰۰ کامپیوتر در سراسر جهان را آلوده کرد.

کنترل پورت های شبکه

با نظارت دقیق بر روی وضعیت پورت های شبکه، امنیت اتصال از طریق پروت سکیوریتی، مانیتورینگ پورت های باز و نظارت بر ترافیک پورت ها کمک بسیار مفیدی به شما می کند.

امنیت داده ها

مقدار زیادی اطلاعات وجود دارد که هر روز به یک سازمان وارد می شود، اما فقط برخی از این اطلاعات استفاده می شود در حالی که بقیه به عنوان اطلاعات دائمی بدون هیچ سیاست امنیتی، فقط حفظ می شوند! اگر محافظت از داده ها و حفظ حریم شخصی کاربران به درستی مطابق با قوانین حفاظت از داده ها نباشد، سازمان ها ممکن است میلیون ها جریمه را پرداخت کنند

طبق قانون حفاظت از اطلاعات اروپا از این پس نشت هرگونه اطلاعات شخصی افراد تا ۲/۵ برابر جریمه در پی خواهد داشت.

در سال ۲۰۱۹، مجرمان سایبری نرم افزارهای امنیتی بیشتری را هدف قرار می دهند و از آن استفاده می کنند
.

۵۵% سازمان های متوسط و بزرگ دارای ۱۰۰۰ حساب کاربری (اکانت) کهنه و بلا استفاده هستند!

حساب های کاربری کاربران در اکتیودایرکتوری را جدی بگیرید!

اغلب، در سازمان های متوسط و بزرگ اکانت های کاربران منقضی شده از اکتیودایرکتوری حذف نمی شوند و یا هیچ پالیسی برای مجبور کردن کاربران به تغییر پسوردها وجود ندارد! همین موضوع یک شکاف امنیتی عمیق در سازمان بوجود می آورد، که قطعاً میلیون ها تومان هزینه سوء استفاده بر دوش سازمان خواهد گذاشت!
.

۶۵% سازمان های متوسط و بزرگ دارای ۵۰۰ حساب کاربری (اکانت) هستند که پسورد آنها هرگز منقضی نمی شود!

حفاظت از برنامه ها

با افزایش شمار زیادی از کدهای مخرب قابل اجرا از راه دور یا بهره گیری از آسیب پذیری های صفر روز، امنیت نرم افزارها به ویژه نرم افزارهای سازمانی به یکی از مهمترین دغدغه های سازمان ها تبدیل شده است. آیا شبکه کسب و کار سازمان شما ایمن است؟

این ده کنترل امنیتی را با استفاده از نرم افزاردسکتاپ سنترال به دست آوردید و حفظ کنید.

ManageEngine
Desktop Central

Medanet

www.DesktopCentral.ir