برای بهبود سطح امنیتی روتر یا سوئیچ، اقدامات مختلفی را انجام می دهیم. این می تواند حذف یک سرویس سیستم موجود یا به روز رسانی برخی از تنظیمات فعلی باشد.

سخت شدن روتر/سوئیچ فرآیند انجام کارهای "درست" برای امنیت شبکه است. هدف افزایش سطح امنیتی زیرساخت ها است. جنبه های زیادی برای ایمن سازی صحیح یک سیستم وجود دارد. با این حال، اصول اولیه برای اکثر سیستم عامل ها مشابه است. بنابراین فرآیند سخت شدن سیستم برای روترها و سوئیچ ها بسیار خاص است.

برخی از مراحل سخت شدن روتر/سوئیچ ما:

بررسی کنید که چارچوب مورد استفاده به روز باشد

همه به روز رسانی ها و وصله های سیستم عامل و خدمات را بررسی کنید

رابط های روتر/سوئیچ استفاده نشده را غیرفعال کنید

همه سرویس های استفاده نشده، پورت های قابل دسترسی را غیرفعال کنید.

پروتکل های مدیریتی را که استفاده نمی کنید غیرفعال کنید

ویژگی هایی را که تکنیک هایی برای هدایت مجدد ترافیک شما هستند غیرفعال کنید

غیرفعال کردن ویژگی هایی که تکنیک هایی برای کاوشگر و اسکن در حملات شناسایی هستند

از امنیت اتصالات ترمینال اطمینان حاصل کنید

سیاست های رمز عبور برای همه سرویس های مورد نیاز احراز هویت کنترل می شود

ARP رایگان و ARP پروکسی را غیرفعال کنید

پخش های IP-directed را غیرفعال کنید

بررسی های امنیتی SNMP

استفاده از HTTP به جای HTTP

زمانی که از DNS استفاده نمی کنید غیرفعال کنید یا به صورت ایمن پیکربندی کنید.

حذف سرویس های غیر ایمن مانند telnet

فعال سازی ورود

بررسی اتصال SIEM

کنترل دسترسی بین VLAN ها

اگر می‌خواهید بدانید که خدمات سخت‌سازی روتر/سوئیچ چگونه می‌تواند برای شرکت شما مفید باشد یا اطلاعات بیشتری در مورد خدمات ما داشته باشید، لطفاً با کارشناسان امنیتی ما تماس بگیرید تا یک مشاوره سریع رایگان دریافت کنید.