چتری برای محافظت از شبکه‌های ارتباطی و دستگاه‌های متصل به شبکه

در تمامی ادوار، از اولین ویروس سکتور راه‌انداز سیستم‌ها تا تهدیدات پیشرفته و پیچیده‌ای که سازمان‌ها، کاربران و حتی دولت‌ها را هدف قرار داده‌اند، هدف سرقت یا امحاء اطلاعات بوده است.

کامپیوترها بیش از نیم قرن است که به پیشرفت انسان‌ها کمک کرده‌اند. به‌تدریج با فراگیرتر و پیچیده‌تر شدن این سامانه‌ها، تهدیدات پیرامون آن‌ها نیز به شکل فزاینده‌ای رشد کرده‌اند. این دستگاه‌های پردازشگر هوشمند همواره از سوی افرادی تهدید می‌شوند که سعی دارند در روند فعالیت سازمان‌ها خللی ایجاد کرده و عملکرد این سامانه‌ها را متوقف کنند. در تمامی ادوار، از اولین ویروس سکتور راه‌انداز سیستم‌ها تا تهدیدات پیشرفته و پیچیده‌ای که سازمان‌ها، کاربران و حتی دولت‌ها را هدف قرار داده‌اند، هدف سرقت یا امحاء اطلاعات بوده است. سازمان‌های امروزی با تهدیدات کاملا پیچیده‌ای روبه‌رو هستند که هر یک خطر واقعی برای یک سازمان به شمار می‌روند. یک حمله موفق و حساب شده هکری با اتکا بر چهار عامل کاربران نهایی (کارمندان یک سازمان)، کیت‌های بدافزاری، رخنه‌های مستتر در نرم‌افزارها و پیکربندی اشتباه تجهیزات شبکه به مرحله اجرا در می‌آید. گزارش‌های منتشر شده از سوی شرکت‌هایی همچون کسپرسکی، مک‌آفی و... نشان می‌دهند که هر ساعت یک تهدید جدید ظاهر می‌شود که شرکت‌های امنیتی را مجبور می‌کند برای مقابله با آن تهدید و محافظت از کامپیوترها و شبکه‌ها در حال آماده‌باش کامل قرار داشته باشند.

یک کارشناس امنیتی برای آن‌که بتواند از زیرساخت‌های یک شبکه محافظت کند، چاره‌ای ندارد جز این‌که درباره تهدیدات پیرامون روترها، سوییچ‌ها، شبکه‌های ارتباطی بی‌سیم و مهم‌تر از آن سامانه‌هایی که برای پیشگیری یا به دام انداختن هکرها از آن‌ها استفاده می‌شود، اطلاعاتی به دست آورد. برای کاربران نهایی یا همان مصرف‌کنندگان، یک شبکه تنها ابزاری است که برای انجام کارهای خود از آن استفاده می‌کنند، در نتیجه اگر تیم مدیریت امنیت اطلاعات یک سازمان تصور کند زیرساخت ارتباطی سازمان هیچ‌گونه مشکلی نداشته و بی‌تفاوت به مسائل امنیتی، ارزیابی‌های هفتگی یا ماهانه را انجام ندهد، ناگهان با حمله غیرمنتظره‌ای روبرو می‌شود که سرقت اطلاعات یا از دست رفتن رکوردهای اطلاعاتی تنها بخشی از پیامدهای زیان‌بار این قصور خواهد بود.

محرمانگی، دسترس‌پذیری و یکپارچگی سه اصل اساسی امنیت شبکه را تشکیل می‌دهند؛ به عبارت دقیق‌تر، اخباری که در ارتباط با انتشار بدافزارها یا حمله به شبکه یک سازمان در رسانه‌ها منتشر می‌شود، همگی حول این سه محور قرار دارند. حملاتی که سعی دارند سه اصل فوق را نقض کنند. اصل محرمانگی به حفاظت از داده‌ها در شبکه اشاره دارد. داده‌ها در شبکه باید از دسترس کاربران غیرمجاز به دور باشند و به‌هیچ‌عنوان به افراد غیرمجاز اجازه داده نشود به داده‌ها دسترسی پیدا کنند. در این زمینه، الگوریتم‌های رمزنگاری کمک فراوانی به ما می‌کنند تا از داده‌ها محافظت کنیم. اصل یکپارچگی به این موضوع اشاره دارد که تغییرات روی‌داده باید تنها توسط کاربران مجاز انجام شود. اگر داده‌هایی که درون یک شبکه باید انتقال داده شوند، خراب شوند، اصل یکپارچگی داده‌ها نقض می‌شود.

اصل دسترس‌پذیری به این موضوع اشاره دارد که داده‌ها باید بدون مشکل در اختیار کاربران مجاز قرار داشته باشند. هر عاملی که باعث شود، اصل دسترس‌پذیری نقض شده و دسترسی به سرویس‌های مبتنی بر شبکه، سامانه‌ها و داده‌ها با اختلال روبه‌رو شود باعث ضرر و زیان‌های مالی سنگینی می‌شود. یک کارشناس امنیت شبکه‌های کامپیوتری برای آن‌که بتواند از زیرساخت‌های ارتباطی یک سازمان به‌درستی محافظت کند، مجبور است دانش خود را در ارتباط با اصول اولیه امنیت شبکه‌های کامپیوتری، ترمینولوژی‌های مختلف امنیتی، انواع مختلف حملات و ابزارهای امنیتی ارتقا دهد. هر چه سطح دانش یک کارشناس امنیت شبکه‌های کامپیوتری بیشتر باشد، به همان نسبت در تشخیص به‌موقع یک حمله سریع‌تر بوده و می‌تواند اقدامات مقتضی را در زمان درستی انجام دهد. به‌طور طبیعی یک کارشناس امنیت شبکه‌های کامپیوتری مجبور است در ارتباط با مباحث زیربنایی و مهم شبکه‌ها اطلاعات کافی داشته باشد. به‌عنوان‌مثال، او باید بداند لایه‌های مختلف مدل OSI یا TCP/IP چگونه کار می‌کنند و چه ابزارها و دستورات خط فرمانی برای بررسی وضعیت شبکه‌ها به کار گرفته می‌شوند. به همین دلیل است که افراد مسئول برقراری امنیت شبکه‌های کامپیوتری در ارتباط با مباحث شبکه، دانشی در سطح مدرک CCNA R&S دارند.

امنیت شبکه‌های کامپیوتری درست به همان اندازه تسلط بر پیاده‌سازی شبکه‌ها حائز اهمیت است. بر همین اساس، پرونده ویژه شماره 218 ماهنامه شبکه را به مبحث امنیت در شبکه‌های کامپیوتری اختصاص دادیم. در این پرونده سعی کردیم گلچینی از مهم‌ترین، کاربردی‌ترین و البته ساده‌ترین مباحثی را که هم مخاطبان عام و هم متخصصان به آن‌ها علاقه‌مند هستند، گردآوری کنیم. در پرونده ویژه این شماره با بهترین ابزارهای محافظت از نقاط پایانی در سال 2019، انواع مختلف دیواره‌های آتش که برای محافظت از شبکه‌ها و سامانه‌های انفرادی قابل استفاده است، مفهوم امنیت در شبکه‌های کامپیوتری، آشنایی با گونه‌ها و طبقه‌بندی‌های رایج حاکم بر دنیای امنیت شبکه‌ها که ممکن است کمتر در مورد آن‌ها مطلب خوانده باشید، چگونگی محافظت از شبکه‌های بی‌سیم خانگی و سازمانی، لزوم به‌کارگیری ظرف عسل برای به دام انداختن هکرها، تفاوت‌ها و مزایای به‌کارگیری سامانه‌های تشخیص نفوذ و پیشگیری از نفوذ آشنا خواهید شد و هدف اصلی این بوده تا اطلاعاتی مهم و هرچند مختصر در ارتباط با مفهوم امنیت در شبکه‌های کامپیوتری را به سمع و نظر مخاطبان برسانیم

تاریخ انتشار:

21 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16006/%DA%86%D8%AA%D8%B1%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D8%B1%D8%AA%D8%A8%D8%A7%D8%B7%DB%8C-%D9%88-%D8%AF%D8%B3%D8%AA%DA%AF%D8%A7%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AA%D8%B5%D9%84-%D8%A8%D9%87-%D8%B4%D8%A8%DA%A9%D9%87