چارچوب امنیت سایبری ایالات متحده آمریکا

چارچوب امنیت سایبری ایالات متحده آمریکا (به انگلیسی: NIST Cybersecurity Framework)

سازمان استاندارد ملی ایالات متحده آمریکا در دوازدهم فوریه ۲۰۱۴ نسخه اول چارچوب بهبود امنیت سایبری زیرساخت‌های حیاتی را منتشر کرد. این چارچوب از طریق همکاری میان صنعت و دولت ایجاد شده‌است و شامل استانداردها، رهنمودها و اقداماتی است که برای بهبود حفاظت از زیرساخت‌های حیاتی استفاده می‌شود. رویکرد مقرون به صرفه، تکرار پذیر، منعطف و اولویت‌گذاری شده چارچوب به مالکان و گردانندگان زیرساخت حیاتی در مدیریت مخاطرات مرتبط با امنیت سایبری کمک می‌کند.[۱] به استثنای مطالبی که به عنوان کپی رایت بر آن‌ها حک شده باشد، کلیه اطلاعاتی که در صفحات وبسایت سازمان ملی استاندارد آمریکا منتشر می‌شوند اطلاعات عمومی محسوب(شامل) می‌شوند و قابل توزیع و کپی کردن هستند.[۲] بنابراین ترجمه و هرگونه استفاده از اطلاعات سازمان ملی استاندارد ایالات متحده آمریکا نقض کپی رایت محسوب نمی‌شود و می‌توان ترجمه عینی و بدون دخل و تصرف استاندارد امنیت سایبری را در ویکی‌پدیا استفاده کرد.

خلاصه چارچوب

امنیت ملی و اقتصادی ایالات متحده آمریکا به کارکرد مطمئن زیرساخت‌های حیاتی بستگی دارد. تهدیدات امنیت سایبری از اتصال‌پذیری و پیچیدگی فزاینده سامانه‌های زیرساختی حیاتی نشات می‌گیرد و امنیت ملی، سلامت و ایمنی عمومی را به خطر می‌اندازد. همانند مخاطرات مالی و شهرت، مخاطرات امنیت سایبری نیز بر بقای شرکت‌ها تأثیرگذار خواهد بود. تهدیدات امنیت سایبری می‌تواند هزینه‌ها را بالا ببرد و درآمد را کاهش دهد. تهدیدات امنیت سایبری می‌تواند بر توانایی شرکت‌ها در نوآوری، کسب و حفظ مشتریانشان آسیب وارد کند.

برای مواجهه با این مخاطرات، ریاست جمهور آمریکا فرمان اجرایی ۱۳۶۳۶ "بهبود امنیت زیرساخت‌های حیاتی" را در دوازدهم فوریه ۲۰۱۳ صادر کرد که تعیین کرد"این سیاست ایالات متحده برای بهبود امنیت و مقاومت زیرساخت‌های حیاتی ملت است که کارآمدی، نوآوری و موفقیت مالی محیط سایبری را حفظ می‌کند و ایمنی، امنیت، محرمانگی کسب و کار، حریم خصوصی و حقوق شهروندی را ارتقا می‌دهد ". در تصویب این سیاست‌ها، فرمان اجرایی به دنبال توسعه یک چارچوب امنیت سایبری مبتنی بر مخاطره داوطلبانه است- مجموعه‌ای از استانداردهای صنعتی و بهترین اقدام‌ها که به سازمان‌ها در مدیریت مخاطرات امنیتی کمک می‌کند. چارچوب منتجه از تعامل میان دولت و بخش خصوصی خلق شده‌است و به صورتی مقرون به صرفه مبتنی بر نیازهای کسب وکار و بدون تحمیل الزامات مقرراتی اضافی بر کسب و کارها از زبانی مشترک برای پرداختن و مدیریت مخاطرات امنیت سایبری بهره می‌گیرد.

چارچوب بر استفاده از محرک‌های کسب و کار برای هدایت فعالیت‌های امنیت سایبری و در نظر گرفتن مخاطرات امنیت سایبری به عنوان بخشی از فرایند مدیریت مخاطره سازمان تمرکز دارد. چارچوب شامل سه بخش می‌شود: هسته چارچوب، نمایه چارچوب و لایه‌های پیاده‌سازی چارچوب. هسته چارچوب مجموعه‌ای از فعالیت‌های امنیت سایبری، خروجی ¬ها و ارجاعات آگاهی بخش است که بین بخش‌های زیرساختی عمومیت دارند و رهنمودی تشریحی برای توسعه نمایه‌های سازمانی انفرادی ارائه می‌کنند. از طریق استفاده از نمایه‌ها، چارچوب به سازمان کمک خواهد کرد که فعالیت‌های امنیت سایبری خود را با نیازمندی‌های کسب و کار، تحمل خطا و منابع خود همراستا کند. لایه‌ها مکانیزم‌هایی برای سازمان پدید می‌آورند که بتواند ویژگی‌های رویکرد خود به مدیریت مخاطرات امنیت سایبری را مشاهده و درک کند.

فرمان اجرایی همچنین لازم می‌داند که هنگامی که سازمان‌های بزرگ با زیرساخت حیاتی فعالیت‌های امنیت سایبری انجام می‌دهند، چارچوب، روش‌شناسی حفاظت از حریم خصوصی افراد و حقوق شهروندی را نیز شامل شود. در حالی که فرایندها و نیازهای کنونی تغییر می‌کنند، چارچوب به سازمان‌ها در لحاظ کردن حریم خصوصی و آزادی‌های شهروندی به عنوان بخشی از یک برنامه امنیت سایبری جامع کمک می‌کند.

چارچوب سازمان‌ها را- فارق از اندازه، سطح مخاطره فضای سایبر یا پیشرفتگی امنیت سایبری آنها- قادر می‌سازد که اصول و بهترین اقدامات مدیریت مخاطره را برای بهبود امنیت و مقاومت زیرساخت‌های حیاتی بکاربگیرند. در رابطه با رویکردهای متعدد امروزی در امنیت سایبری، چارچوب با گردهم آوردن استانداردها، رهنمودها و اقداماتی که در صنعت امروز به خوبی عمل می‌کنند، به این استانداردهای پراکنده ساختار و سازمان می‌دهد. به‌علاوه از آنجا که چارچوب امنیت سایبری به

استانداردهای شناخته شده امنیت سایبری جهان ارجاع می‌دهد، چارچوب همچنین می‌تواند توسط سازمان‌هایی که خارج از ایالات متحده آمریکا واقع شده‌اند استفاده شود و به عنوان مدلی برای همکاری‌های بین‌المللی در زمینه تقویت زیرساخت‌های حیاتی خدمت کند.
چارچوب یک رویکرد یکسان برای مدیریت همه ابعاد زیرساخت‌های حیاتی به‌شمار نمی‌رود. سازمان‌ها مخاطراتی یکتا خواهند داشت-تهدیدهای مختلف، آسیب‌پذیری‌های مختلف و تحمل خطاهای مختلف- و نحوه پیاده‌سازی اقدام‌ها در چارچوب هم متفاوت خواهد بود. سازمان‌ها می‌توانند فعالیت‌هایی که برای عرضه خدمات حیاتی مهمند را تعیین و سرمایه‌گذاری‌ها را در جهت حداکثرسازی اثر هر دلاری که خرج می‌کنند اولویت بندی کنند. نهایتاً چارچوب به دنبال کاهش و مدیریت مخاطرات امنیت سایبری است.

چارچوب سندی زنده است و با توجه به بازخوردهای صنعت بروزرسانی خواهد شد. همانطور که چارچوب به ورطه عمل گذاشته می‌شود، درس‌های آموخته شده در نسخه‌های آینده لحاظ خواهند شد. این موضوع تضمین می‌کند که چارچوب امنیت سایبری با نیازهای اپراتورها و مالکان زیرساخت‌های حیاتی در محیط چالش‌برانگیز راهکارها، تهدیدات و مخاطرات جدید مطابقت داشته باشد.[۳]

منابع

۱. /Welcome (http://www.nist.gov/cyberframework)
۲. Disclaimer (http://www.nist.gov/public_affairs/disclaimer.cfm)
۳. Cybersecurity Framework (PDF) (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)