اهمیت امنیت سایبری برای دنیا

با گسترش اتصال جهانی و استفاده از خدمات ابری (ابر در اینجا استعاره از شبکه یا شبکه‌ای از شبکه‌های وسیع مانند اینترنت است که کاربر معمولی از پشت‌صحنه و آنچه در پی آن اتفاق می‌افتد اطلاع دقیقی ندارد) برای پردازش داده‌های حساس و اطلاعات شخصی، ریسک افشای آنها نیز گسترش می‌یابد. پیکربندی ضعیف سرویس های اینترنتی همراه با شرورهای سایبری که همیشه در حال تکامل هستند به معنای افزایش احتمال آسیب‌دیدن کسب و کارهاست. این معضل به قدری همپا با پیشرفت‌های فناوری اطلاعات پیش رفته است که اکنون امنیت سایبری یک اصل اساسی در این حوزه به حساب می‌آید. هر کارمند فناوری باید در ایمن سازی برنامه‌ها، دستگاه‌ها، داده‌ها، زیرساخت‌ها و افراد مشارکت داشته باشد. بنابراین، نیاز شرکت‌ها به اطمینان از به‌روزبودن پروتکل‌های امنیتی‌شان بسیار مهم است.

شکست امنیتی

اهمیت وجود امنیت سایبری را باید در شکست‌های امنیتی که می‌توانند زیرساخت‌های مهم دولتی از جمله بانک‌ها، وزارتخانه‌ها، پمپ‌بنزین ها و ... را برای خرابکاری‌هایی با منشا سیاسی سودجویانه هدف قرار دهند، جست‌وجو کرد. این معضلی فراگیر در سراسر جهان است و می‌توان گفت تقریبا هیچ کشور یا دولتی نیست که از آن در امان باشد. در هرکدام از این شکست‌های امنیتی که در نتیجه وجود یک یا چند نقص و عدم پایبندی به رویکردهای ایمنی رخ داده علاوه‌بر اینکه اطلاعات حیاتی میلیون‌ها کاربر در سطح اینترنت به سرقت رفته، به این سازمان‌ها نیز هم از بعد مالی و هم بعد اعتباری لطمات جبران‌ناپذیری وارد کرده است. آمارها نشان می‌دهد سطح حملات سایبری در جهان نه تنها روند کاهشی ندارد که به شدت در حال افزایش است.

روسیه در صدر جرائم سایبری

در یک مطالعه جدید که مهم‌ترین منابع تهدیدات جرائم سایبری را رتبه‌بندی می‌کند، روسیه به عنوان کانون اصلی جرائم سایبری در جهان نامگذاری شده است. شاخص جهانی جرائم سایبری پس از ۳ سال تحقیق توسط دانشمندان دانشگاه آکسفورد و دانشگاه نیو ساوت ولز منتشر شده است. براساس این شاخص، روسیه به عنوان کشوری با بیشترین تهدید جرائم سایبری در صدر لیست قرار گرفته است. پس از آن اوکراین، چین، ایالات‌متحده و نیجریه قرار دارند.

قفلی برای اطلاعات آنلاین

امنیت سایبری به ایمن نگه داشتن سیستم‌های کامپیوتری و داده‌های آنلاین کمک می‌کند

زهرا خلجی | روزنامه‌نگار

در سال‌های اخیر، واژه امنیت سایبری تبدیل به سرفصلی ثابت در حوزه فناوری اطلاعات شده است. بالا رفتن میزان تبادل داده‌ها در فضای مجازی فرصت را برای سودجویانی که از این اطلاعات سوءاستفاده می‌کنند فراهم کرده و اینجا دقیقا همان جایی است که پای امنیت سایبری را به میدان مبارزه با سارقان اینترنتی باز می‌کند. هکرها و سارقان آنلاین رمزهای عبور و اطلاعات شخصی را از سایت‌ها و شبکه‌های اجتماعی می‌گیرند یا اسرار شرکت را از فضای ابری آن خارج می‌کنند تا با سوءاستفاده یا فروش این اطلاعات پول هنگفتی به جیب بزنند. بنابراین برای هر شرکت و سازمانی در هر اندازه‌ای ایمن نگه داشتن اطلاعات نگرانی فزاینده‌ای است.

امنیت سایبری به زبان ساده چیست؟

خود واژه سایبری در معنای لغوی پیشوندی است که بر مجموعه فناوری‌های اطلاعاتی، ارتباطی، هوش مصنوعی و... اطلاق می‌شود. در زبان انگلیسی، سایبر یک پیشوند و در زبان فارسی، یک مضاف‌الیه است و بارها آن را در واژه‌هایی مانند فضای سایبری، جنگ سایبری، دولت سایبری، جامعه سایبری و امنیت سایبری شنیده‌ایم. امنیت سایبری شامل تمام فناوری‌ها و شیوه‌هایی است که سیستم‌های کامپیوتری و داده‌های الکترونیکی را ایمن نگه می‌دارد. در دنیایی که همه‌چیز ما، از کسب‌وکار تا زندگی اجتماعی، آنلاین است، انواع مختلفی از نقش‌های امنیت سایبری وجود دارد که باید در نظر گرفت. هدف امنیت سایبری محافظت از دستگاه‌ها، شبکه‌ها، نرم‌افزارها و داده‌ها در برابر تهدیدات سایبری خارجی است. این حفاظت با استفاده از شیوه‌ها و ابزارهایی است که می‌تواند تأثیر این تهدیدات را کاهش دهد.

امنیت اطلاعات چیست؟

امنیت اطلاعات و امنیت سایبری اغلب با هم اشتباه گرفته می‌شوند. این دو اصطلاح ارتباط نزدیکی با هم دارند و در طول مسیر به هم می‌رسند. شاید شما آنها را به جای یکدیگر استفاده کنید، اما باید بدانید که میان آنها تفاوت‌های کلیدی‌ای وجود دارد. امنیت اطلاعات گسترده‌تر است و رمزگذاری، امنیت نقطه پایانی و امنیت فیزیکی را شامل می‌شود. این حفاظت کلی از داده‌ها، از جمله محرمانه بودن، یکپارچگی و در دسترس بودن آنها را در محیط‌های مختلف تضمین می‌کند. در دنیای ماشینی امروز، همه‌چیز با کامپیوتر و اینترنت به هم متصل می‌شود، از جمله ارتباطات، سرگرمی، حمل‌ونقل، خرید، دارو و .... مقدار زیادی از اطلاعات شخصی در این سرویس‌ها و برنامه‌ها ذخیره می‌شود و به همین دلیل، امنیت سایبری و امنیت اطلاعات بسیار مهم است.

چرا امنیت سایبری اهمیت فزاینده‌ای دارد؟

هک شدن فقط تهدیدی مستقیم برای داده‌های محرمانه مورد نیاز شرکت‌ها نیست، بلکه می‌تواند روابط آنها با مشتریان را مخدوش کند و حتی آنها را در معرض مشکلات قانونی جدی قرار دهد. با فناوری جدید، از خودروهای خودران گرفته تا سیستم‌های امنیتی خانگی مجهز به اینترنت، خطرات جرائم سایبری حتی جدی‌تر می‌شود. بنابراین جای تعجب نیست که شرکت‌های تحقیقاتی و مشاوره بین‌المللی پیش‌بینی می‌کنند که هزینه‌های امنیتی در سراسر جهان در سال ۲۰۲۴ به ۲۱۰ میلیارد دلار رسیده است. طبق همین پیش‌بینی‌ها، بازار امنیتی تا سال ۲۰۲۸ به ۳۱۴ میلیارد دلار خواهد رسید.

نگرانی‌های روزافزون

این روزها نیاز به حفاظت از اطلاعات محرمانه نگرانی مبرمی در بالاترین سطوح دولتی و صنعتی است. هکرهای حرفه‌ای می‌توانند اسرار دولتی را از آن سوی دنیا به‌راحتی بدزدند. شرکت‌هایی که کل مدل‌های کسب‌وکارشان به کنترل داده‌های مشتری وابسته است پایگاه داده‌هایشان به‌راحتی در معرض خطر است. طبق گزارش کمیسیون تجارت فدرال آمریکا، تنها در یک مورد در سال ۲۰۱۷ اطلاعات شخصی ۱۴۷ میلیون نفر در یک شرکت گزارش‌دهی اعتباری به خطر افتاد.

> در دنیای ماشینی امروز، همه‌چیز با کامپیوتر و اینترنت به هم متصل می‌شود، ازجمله ارتباطات، سرگرمی، حمل‌ونقل، خرید، دارو و غیره. مقدار زیادی از اطلاعات شخصی در این سرویس‌ها و برنامه‌ها ذخیره می‌شود و به همین دلیل، امنیت سایبری و امنیت اطلاعات بسیار مهم است