هدف امنیت سایبری محافظت از اطلاعات در برابر سرقت و آسیب است. این اطلاعات شامل داده‌های حساس، اطلاعات قابل شناسایی و تشخیص هویت افراد، سوابق پزشکی، اطلاعات شخصی، مالکیت معنوی، داده‌های مرتبط با فعالیت آژانس‌های دولتی و صنعتی می‌شود

پیاده‌سازی امنیت سایبری به صورت موثر و درست از چالش‌های دنیای امروز است، چون هم تعداد دستگاه‌ها بیشتر شده و هم هکرها خلاق‌تر شده‌اند

آنتی‌ویروس‌های معمولی دیگر جواب نمی‌دهد

چالش واقعی امنیت مجازی

سیده‌زهرا حسینی
خبرنگار

کمتر کسی پیدا می‌شود که این روزها از IT و اینترنت استفاده نکند؛ بسیاری از بخش‌های خدماتی و صنعتی مثل بانکداری، سرگرمی، رسانه‌ها حتی حمل‌ونقل و خرده‌فروشی نیز به تداوم دسترسی خود متکی هستند. این جمله‌ها را بارها شنیدیم اما غیرقابل کتمان است که استفاده از دنیای مجازی یا فضای سایبری زندگی همه ما را متحول کرده، زندگی ما تمام و کمال در گروی فضای مجازی است و حالا امنیت اطلاعات فضای سایبر، به‌شدت حیاتی است. این جمله نیز غیرقابل کتمان است که تهدیدها برای امنیت داده‌ها و اطلاعات واقعی همیشه وجود دارد و باید امیدوار باشیم به انواع مختلف امنیت سایبری تا بتواند برای مقابله با این تهدیدها استفاده شود.

سال ۱۹۸۲ بود که برای اولین بار ویلیام گیبسون از اصطلاح «فضای مجازی» در داستانی در مجله Omni استفاده کرد و بعد از چاپ کتاب Neuromancer این اصطلاح رایج شد. گیبسون در این رمان علمی-تخیلی، فضای مجازی را برآیند شکل‌گیری شبکه‌ای رایانه‌ای در جهانی مملو از موجودات هوشمند مصنوعی تعبیر کرد. امروزه اما از فضای سایبری به‌عنوان محیطی برای انتقال داده‌ها و اطلاعات یاد می‌شود و تنها شامل اینترنت نیست بلکه شامل تمام شبکه‌ها و سیستم‌های ارتباطی-اطلاعاتی است.

چرا امنیت سایبری مهم است؟

امنیت سایبری از این جهت مهم است که سازمان‌های دولتی، نظامی، شرکتی، مالی و پزشکی حجم گسترده‌ای از اطلاعات را در رایانه‌ها و سایر دستگاه‌ها جمع‌آوری، پردازش و ذخیره می‌کنند. هدف امنیت سایبری محافظت از اطلاعات در برابر سرقت و آسیب است. این اطلاعات شامل داده‌های حساس، اطلاعات قابل شناسایی و تشخیص هویت افراد، سوابق پزشکی، اطلاعات شخصی، مالکیت معنوی و داده‌های مرتبط با فعالیت آژانس‌های دولتی و صنعتی می‌شود.

اهمیت امنیت سایبری چیست؟

در طول چند سال اخیر تهدیدات سایبری و تعداد حمله‌ها با سرعت زیادی رشد کرده است. شرکت‌های امنیتی هشدار داده‌اند حملات سایبری و جاسوسی دیجیتال مهم‌ترین تهدید برای امنیت کشورها هستند و حتی از اصطلاح «تروریسم» برای خطرناک بودن این تهدیدات استفاده کردند. گزارش‌ها حاکی از آن است که تا پایان سال ۲۰۲۱ حمله‌های سایبری حدود ۶ میلیون دلار به اقتصاد جهانی آسیب وارد می‌کنند و پیش‌بینی شده تا سال ۲۰۲۲ حدود ۱۳۴ میلیارد دلار باید صرف امنیت سایبری شود. معمولا بیشتر حمله‌ها به سرویس‌های پزشکی و سرویس‌های عمومی است چراکه در جرایم سایبری بیشتر به‌دنبال اطلاعات پزشکی و مالی هستند.

گزارش‌ها حاکی از آن است که تا پایان سال ۲۰۲۱ حمله‌های سایبری حدود ۶ میلیون دلار به اقتصاد جهانی آسیب وارد می‌کنند و پیش‌بینی شده تا سال ۲۰۲۲ حدود ۱۳۴ میلیارد دلار باید صرف امنیت سایبری شود

انواع تهدیدات سایبری

تهدیدات در برابر امنیت سایبری به سه دسته تقسیم می‌شود:

- **جرایم سایبری:** Cybercrime در این مورد تهدید فرد یا گروهی سیستم‌ها را هدف قرار می‌دهند تا درآمد کسب کنند یا خرابکاری کنند.
- **حمله سایبری:** Cyber Attack این تهدید اغلب با هدف جمع‌آوری هدفمند اطلاعات، با انگیزه سیاسی است.
- **تروریست سایبری:** Cyber Terrorism تهدیدی که با هدف ایجاد رعب و وحشت با خراب کردن سیستم‌های الکترونیکی ایجاد می‌شود.

مهم‌ترین امنیت‌های سایبری کدامند؟

- **امنیت زیرساخت‌های حیاتی:** تامین امنیت سایبری زیرساخت‌های حیاتی به معنای محافظت از شبکه‌های ارتباطی، شبکه انتقال انرژی، تصفیه آب، چراغ‌های راهنمایی، پایانه‌های فروش و مراکز بهداشتی است. این مراکز ممکن است به‌طور مستقیم با حمله‌های سایبری مرتبط نباشند، اما می‌توانند به عنوان بستری برای ورود بدافزارها به نقاط پایانی سامانه‌هایی که به آنها متصل می‌شوند، استفاده شوند.
- **بهبود امنیت با اتکا به ابر:** بیشتر سازمان‌ها به‌دنبال استفاده از هوش مصنوعی برای بهبود مشاغل خود، افزایش تجربه مشتری و بهبود عملکردها هستند. شرکت‌های فعال در زمینه خدمات ابری با پیاده‌سازی راهکارهای امنیتی بالقوه هم به سازمان‌ها اجازه می‌دهند این حجم عظیم از داده‌های مستعد چالش‌های امنیتی را در فضای خارج از شبکه سازمانی ذخیره‌سازی و مدیریت کنند.
- **امنیت شبکه:** امنیت شبکه مجموعه راهکارهایی است که سازمان‌ها را قادر می‌سازد تا شبکه‌های رایانه‌ای را از دسترس افراد متجاوز، مهاجمان سازمان یافته و بدافزارها دور نگه دارند.

برای مقابله با حملات سایبری به شبکه‌ها چه‌کارهایی باید انجام داد؟

۱. برای بهبود امنیت شبکه لاگین‌های اضافی را محدود کنید.
۲. برنامه تعویض منظم رمزهای عبور را تدوین کنید.
۳. برنامه‌های ضدویروس قدرتمند نصب کنید.
۴. دیوارهای آتش را به‌درستی پیکربندی کنید.
۵. دسترس مهمان یا ناشناس را محدود کنید.
۶. ترافیک ورودی از اینترنت را ارزیابی کنید.

چند نکته برای حفظ امنیت در فضای سایبری

واقعیت این است که تمام کاربران فضای سایبری برای انجام فعالیت‌های روزمره از سیستم‌های کامپیوتری استفاده کرده و به آنها اعتماد می‌کنند. به همین دلیل مهم‌ترین نکات امنیت سایبری را که باید دقت ویژه‌ای به آنها داشته باشید، آورده‌ایم:

۱. نقض داده‌ای را اعلام کنید.
۲. کارشناس امنیت برای محافظت از اطلاعات استخدام کنید.
۳. برای کاربردهای تجاری که نیازمند داده‌های کاربران هستند از آنها کسب اجازه کنید.
۴. داده‌ها را برای حفظ حریم خصوصی افراد ناشناس کنید.
۵. در صورت نقص داده‌ای در اسرع‌وقت به مقامات مربوط گزارش دهید.
۶. روی خرید و به‌کارگیری ابزارهایی که دسترسی به اطلاعات را محدود می‌کنند سرمایه‌گذاری کنید، دسترسی افراد ثالث یا پیمانکاران به اطلاعات سازمانی را محدود کنید.
۷. از گذرواژه‌های پیچیده و طولانی همراه با احراز هویت دو عاملی یا چند عاملی برای ایمن‌سازی دسترسی به حساب‌های کاربری استفاده کنید.
۸. بهتر است برای اتصال به شبکه‌های سازمانی یا ارسال اطلاعات حساس از وای‌فای عمومی استفاده نکنید.
۹. نرم‌افزارها و سیستم عامل خود را آپدیت کنید. بهتر است از جدیدترین وصله‌ها - Patch استفاده کنید.
۱۰. پیوست ایمیل‌های دریافتی از فرستنده ناشناس را باز نکنید، چون ممکن است بدافزار داشته باشند.
۱۱. روی لینک‌های موجود در ایمیل که از فرستنده ناشناس یا وبسایت ناآشناست، کلیک نکنید.