جمهوری اسلامی ایران
وزارت کشور
استانداری گلستان

تولید، دانش‌بنیان، اشتغال‌آفرین
سال ۱۴۰۱

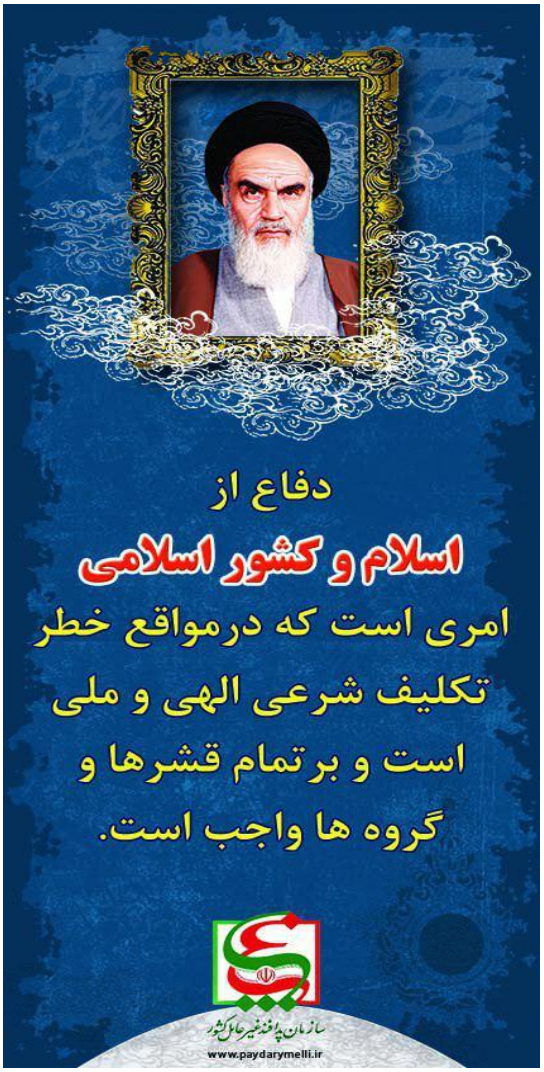
عنوان گزارش :

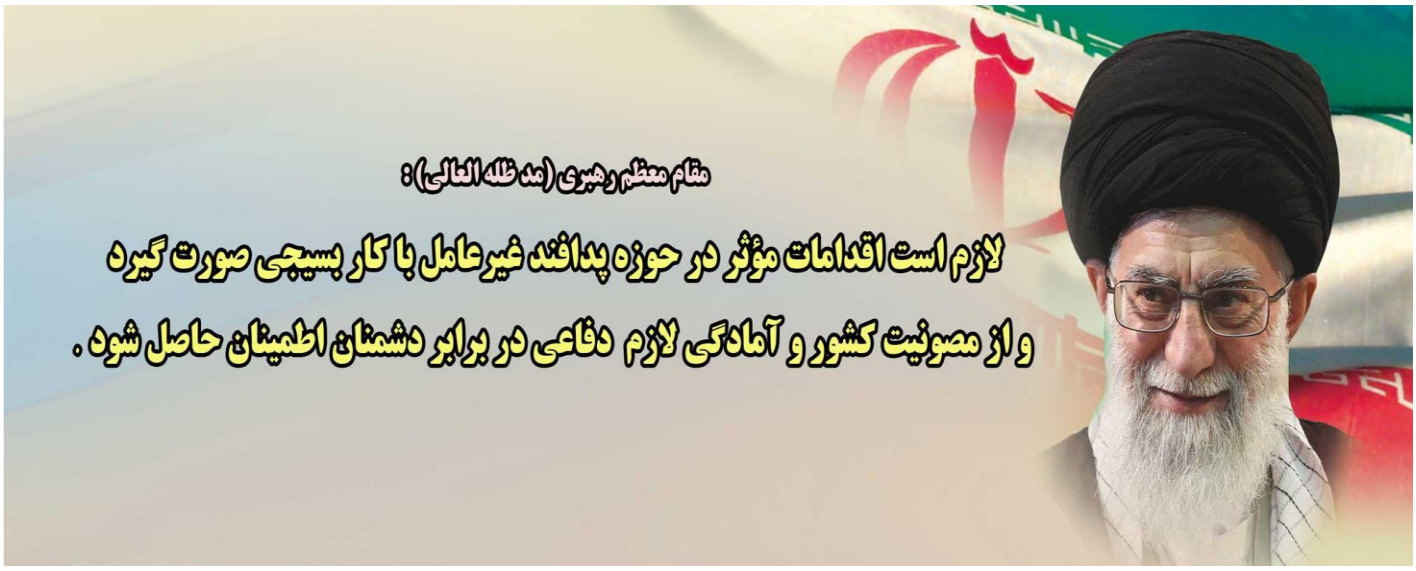
امنیت سایبری cybersecurity

مرداد ۱۴۰۱

سازمان پدافند غیرعامل کشور

وزارت کشور
استانداری گلستان
اداره کل پدافند غیرعامل


دفاع از
اسلام و کشور اسلامی
امری است که درمواقع خطر
تکلیف شرعی الهی و ملی
است و برتمام قشرها و
گروه ها واجب است.
سازمان پدافند غیرعامل کشور
www.paydarymelli.ir


مقام معظم رهبری (مد ظله العالی):
لازم است اقدامات مؤثر در حوزه پدافند غیرعامل با کار بسیجی صورت گیرد
و از مصونیت کشور و آمادگی لازم دفاعی در برابر دشمنان اطمینان حاصل شود .

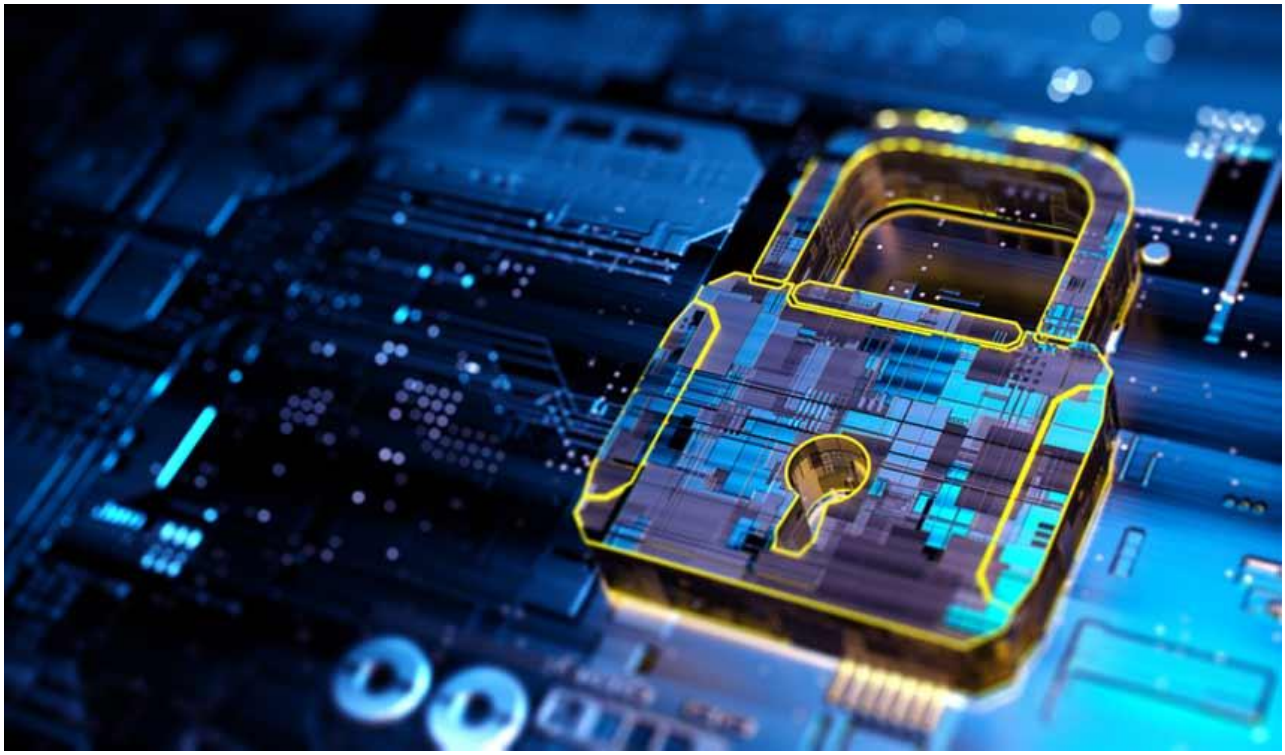
امنیت سایبری cybersecurity چیست؟

با گسترش دستگاه‌های مجهز به اینترنت، فرهنگ سایبری با سرعت بیشتری نسبت به امنیت سایبری در حال رشد است. هر چیزی که به فضای مجازی وابسته است به‌طور بالقوه در معرض خطر است. داده‌های خصوصی، مالکیت فکری، زیرساخت‌های سایبری و حتی امنیت نظامی و ملی می‌توانند با حملات عمدی، نقص‌های امنیتی سهوی و آسیب‌پذیری‌های اینترنت جهانی در معرض خطر قرار گیرند. این مجموعه مشکلات پرداختن به مسئلهٔ امنیت سایبری) cybersecurity یکی از ارکان انقلاب صنعتی چهارم (را ضروری می‌سازد. در ادامه ابتدا به این پرسش می‌پردازیم که cyber security چیست؟ یا همان امنیت سایبری چیست؟ و بعد به پرسش تهدیدات سایبری چیست؟ می‌پردازیم و در آخر وضعیت امنیت سایبری در ایران را بررسی می‌کنیم.

امنیت سایبری cybersecurity چیست؟

در پاسخ به این پرسش که امنیت سایبری چیست؟ یا cyber security چیست؟ می‌توان چنین گفت: امنیت سایبری cyber security عمل محافظت از سیستم‌های حیاتی و اطلاعات حساس در برابر حملات دیجیتالی است. اقدامات مبتنی بر امنیت سایبری cyber securityکه با عنوان امنیت فناوری اطلاعات (IT)نیز شناخته می‌شود، برای مقابله با تهدیدات علیه سیستم‌ها و برنامه‌های مبتنی بر شبکه طراحی شده‌اند، خواه این تهدیدات از داخل یا خارج از سازمان سرچشمه بگیرند.

طبق گزارشی ازIBM ، در سال ۲۰۲۰، میانگین هزینهٔ نقض داده‌ها 3.86 (data breach) میلیون دلار در سراسر جهان و ۸,۶۴ میلیون دلار در ایالات متحده بود. این هزینه‌ها شامل هزینه‌های کشف و پاسخ به نقض داده‌ها، هزینهٔ خرابی و درآمد از دست‌رفته، و آسیب بلندمدت به اعتبار کسب‌وکار و برند می‌شود. مجرمان سایبری اطلاعات شخصی مشتریان – (PII) نام، نشانی، کد ملی، و اطلاعات کارت اعتباری – را هدف قرار می‌دهند و سپس این سوابق را در بازارهای دیجیتالی زیرزمینی می‌فروشند. درز اطلاعات شخصی به ازدست‌دادن اعتماد مشتری، تحمیل جریمه‌های نظارتی و حتی پیگردهای قانونی منجر می‌شود. پیچیدگی سیستم امنیتی (ناشی از استفاده از فناوری‌های متفاوت) و فقدان تخصص درون سازمان‌ها می‌تواند این هزینه‌ها را افزایش دهد. اما سازمان‌هایی که دارای استراتژی جامع امنیت سایبری هستند، با بهترین شیوه‌ها اداره می‌شوند و با استفاده از تحلیل آماری پیشرفته، هوش مصنوعی (AI) و یادگیری ماشینی می‌توانند به‌طور مؤثرتری با تهدیدات سایبری مبارزه کنند و چرخهٔ حیات و تأثیر نقض داده‌ها را در صورت وقوع کاهش دهند.



حوزه‌های امنیت سایبری cybersecurity

استراتژی نیرومند امنیت سایبری **cybersecurity** دارای لایه‌های محافظتی متعددی برای دفاع در برابر جرایم سایبری است؛ علی‌الخصوص برای دفاع در برابر آن دسته از حملات سایبری که سعی دارند به داده‌ها دسترسی پیدا کنند، آن‌ها را تغییر دهند یا از بین ببرند تا از کاربران یا سازمان‌ها اخاذی کنند یا عملیات عادی کسب‌وکار سازمان‌ها را مختل کنند. اقدامات حفاظتی باید شامل موارد زیر باشد:

امنیت زیرساخت‌های حیاتی اقداماتی برای محافظت از سیستم‌های رایانه‌ای، شبکه‌ها و سایر دارایی‌هایی که جامعه برای امنیت ملی، سلامت اقتصادی یا امنیت عمومی به آن‌ها متکی است.

امنیت شبکه اقدامات امنیتی برای محافظت از شبکهٔ کامپیوتری، از جمله اتصالات سیمی و بی‌سیم-Wi Fi در برابر افرادی که قصد نفوذ به آن را دارند.

امنیت برنامه‌ها Applications فرایندهایی که به محافظت از اپلیکیشن‌هایی کمک می‌کند که درون سازمان و در فضای ابری اجرا می‌شوند. امنیت برنامه‌ها باید در مرحلهٔ طراحی، نحوهٔ مدیریت داده‌ها، احراز هویت کاربر و مواردی از این دست لحاظ شود.

امنیت فضای ابری به‌طور خاص، استفادهٔ محرمانه از کامپیوتر که داده‌های فضای ابری را در فضای ذخیره‌سازی، در حال انتقال (در حین انتقال به یا از فضای ابری) و در حال استفاده (در حین پردازش) رمزگذاری می‌کند تا از حریم خصوصی مشتری، الزامات کسب وکار و استانداردهای انطباق با مقررات حمایت کند.

امنیت اطلاعات اقدامات لازم برای حفاظت از داده‌ها، مانند مقررات عمومی حفاظت از داده‌ها یاGDPR ، که حساس‌ترین داده‌های شما را از دسترسی غیرمجاز یا سرقت محافظت می‌کند.

آموزش کاربر نهایی ایجاد آگاهی امنیتی در کل سازمان‌ها به‌منظور تقویت امنیت دستگاه‌هایی که در اختیار کاربر است. برای مثال می‌توان به کاربران آموزش داد پیوست‌های مشکوک ایمیل‌ها را حذف کنند یا از دستگاه‌های یواس‌بی (USB) نامعلوم استفاده نکنند.

جبران خسارات برنامه‌ریزی برای تداوم کسب و کار ابزارها و رویه‌هایی برای واکنش به رویدادهای برنامه‌ریزی‌نشده مانند بلایای طبیعی، قطع برق، یا حوادث امنیت سایبری، با حداقل اختلال در عملیات‌های کلیدی سازمان.

امنیت ذخیره‌سازی افزایش قابلیت تاب‌آوری داده‌ها با استفاده از حفاظ‌های متعدد. این حفاظ‌ها شامل رمزگذاری و تکثیر داده‌ها می‌شود. این داده‌های رمزگذاری‌شده و تکثیرشده همگی در کنار هم نگهداری می‌شوند و می‌توان آن‌ها را به‌سرعت بازیابی کرد و تأثیر حمله‌های سایبری را به حداقل رساند.

امنیت تلفن همراه ایمنی و مدیریت تلفن همراه با امنیت برنامه‌ها، امنیت برنامه‌های داخلی و ایمیل تلفن همراه.

افسانه‌های نادرست درباره امنیت سایبری

حجم حوادث امنیت سایبری در سرتاسر جهان در حال افزایش است، اما تصورات غلط همچنان پابرجاست، از جمله این باور که:

–**مجرمان سایبری خارجی هستند** در واقعیت، نقض امنیت سایبری اغلب نتیجهٔ سوءنیت افراد خودی است که یا برای خودشان یا هماهنگ با هکرهای خارجی کار می‌کنند. این خودی‌ها می‌توانند بخشی از گروه‌های سازمان‌یافته‌ای باشند که تحت حمایت دولت‌های خارجی هستند.

–**همهٔ خطرها شناسایی شده‌اند** در واقع، سطح خطر همچنان در حال گسترش است و آسیب‌پذیری‌های متعدد جدیدی در برنامه‌ها و دستگاه‌های قدیمی و جدید گزارش شده است و احتمال خطای انسانی همچنان در حال افزایش است.

–**مسیرهای حمله مسدود شده‌اند** مجرمان سایبری همیشه در حال یافتن مسیرهای جدیدی برای حمله هستند، از جمله بهره‌گیری از سیستم‌های لینوکس، فناوری‌های بهره‌برداری، دستگاه‌های مبتنی بر اینترنت اشیا (IoT) و محیط‌های ابری

–**صنایع تحت مدیریت من ایمن هستند** هر صنعتی سهمی از خطرات امنیت سایبری دارد، زیرا مجرمان سایبری از الزامات شبکه‌های ارتباطی موجود در تقریباً هر سازمان دولتی یا بخش خصوصی سوءاستفاده می‌کنند. برای مثال، حملات باج‌افزاری بیش از پیش بخش‌های اداری مختلف از جمله دولت‌های محلی و سازمان‌های غیرانتفاعی را هدف قرار می‌دهند و تهدیدها در زنجیره‌های تأمین، وب‌سایت‌های دولتی و زیرساخت‌های حیاتی نیز افزایش یافته‌اند.

تهدید سایبری چیست؟

اگرچه متخصصان امنیت سایبری cybersecurity سخت تلاش می‌کنند شکاف‌های امنیتی را ببندند، مهاجمان همیشه به‌دنبال راه‌های جدیدی برای فرار از نظارت‌های مبتنی بر فناوری اطلاعات و اقدامات دفاعی و نیز سوءاستفاده از نقاط ضعف در حال ظهور هستند. جدیدترین تهدیدات سایبری چرخش جدیدی در تهدیدات »شناخته‌شده» ایجاد کرده‌اند و از محیط‌های دورکاری، ابزارهای دسترسی از راه دور و خدمات ابری جدید سوءاستفاده می‌کنند. این مسئله باعث شده است پاسخ به این پرسش که «تهدید سایبری چیست؟» دستخوش تحول شود. این تهدیدات در حال تحول عبارت‌اند از:

بدافزار

اصطلاح "بدافزار" به انواع نرم‌افزارهای مخرب مانند کرم‌ها، ویروس‌ها، تروجان‌ها و جاسوس‌افزارها اشاره دارد که دسترسی غیرمجاز فراهم می‌کنند یا به کامپیوتر آسیب می‌رسانند. حملات بدافزار به‌شکل فزاینده‌ای «بدون فایل» شده است و برای دورزدن روش‌های کشف و شناسایی آشنایی مانند ابزارهای آنتی‌ویروس طراحی شده‌اند که پیوست‌های مخرب فایل‌ها را اسکن می‌کنند.

باج افزار

باج‌افزار نوعی بدافزار است که فایل‌ها، داده‌ها یا سیستم‌ها را قفل و تهدید می‌کند که داده‌ها را پاک یا نابود می‌کند – یا داده‌های خصوصی یا حساس را در اختیار عموم قرار می‌دهد – مگر اینکه به مجرمان سایبری که حمله را انجام داده‌اند، باج پرداخت شود. حملات باج‌افزاری اخیراً سازمان‌های دولتیِ استانی و محلی را هدف قرار داده‌اند، زیرا آن‌ها در مقایسه با سازمان‌های خصوصی راحت‌تر نقض (breach) می‌شوند و برای پرداخت باج به‌منظور بازیابی برنامه‌ها و وب‌سایت‌هایی که شهروندان به آن‌ها متکی هستند، بیشتر تحت فشار قرار می‌گیرند.

فیشینگ یا مهندسی اجتماعی

فیشینگ نوعی مهندسی اجتماعی است که کاربران را فریب می‌دهد تا اطلاعات شناسایی شخصی یا اطلاعات حساس خود را لو دهند. در کلاهبرداری‌های فیشینگ، علی‌الظاهر ایمیل‌ها یا پیام‌های متنی از طرف یک شرکت قانونی ارسال می‌شوند. این ایمیل‌ها یا پیام‌ها اطلاعات حساسی مانند اطلاعات کارت اعتباری یا اطلاعات ورود به سیستم را از کاربر درخواست می‌کند. در ایالات متحده، پلیس به افزایش کلاه‌برداری‌های فیشینگ مرتبط با بیماری کرونا اشاره کرده است که با رشد دورکاری مرتبط است.

تهدیدهای کارمندان و افراد خودی

کارمندان فعلی یا سابق، شرکای تجاری، پیمانکاران یا هرکسی که در گذشته به سیستم‌ها یا شبکه‌ها دسترسی داشته است، در صورت سوءاستفاده از مجوزهای دسترسی می‌تواند تهدیدی داخلی در نظر گرفته شود. تهدیدهای داخلی می‌توانند در برابر راه‌حل‌های امنیتی مرسوم مانند دیواره‌های آتش و سیستم‌های تشخیص نفوذ نامرئی باشند؛ زیرا این دسته از راه‌حل‌های امنیتی بر تهدیدات خارجی تمرکز دارند.

حملات توزیع‌شده بندآوری خدمات(DDoS)

حملهٔ DDoS سعی می‌کند سرور، وب‌سایت یا شبکه را با بارگذاری بیش از حد و ترافیک زیاد، معمولاً از طریق چندین سیستم هماهنگ، از کار بیندازد. حملات DDoS از طریق پروتکل مدیریت شبکهٔ ساده (SNMP)که برای مودم‌ها، چاپگرها، سوئیچ‌ها، روترها و سرورها استفاده می‌شود، پهنای باند شبکه‌های سازمانی را پر می‌کنند.

تهدیدات پیشرفته و مستمر(APT)

در تهدید پیشرفته و مستمرAPT ، مزاحم یا گروهی از مزاحمان به سیستم نفوذ می‌کنند و برای مدت زمانی طولانی شناسایی نمی‌شوند. نفوذی شبکه‌ها و سیستم‌ها را دست‌نخورده باقی می‌گذارد تا متجاوزان بتوانند از فعالیت‌های تجاری جاسوسی کنند و داده‌های حساس را بدزدند و درعین‌حال نفوذی از فعال‌سازی اقدامات متقابل دفاعی جلوگیری می‌کند.

حملات مرد میانی

حمله مرد میانی حمله‌ای با استفاده از استراق سمع است و در آن مجرم سایبری پیام‌های بین دو طرف را به‌منظور سرقت داده‌ها رهگیری و بازپخش می‌کند .برای مثال، در یک شبکهٔ وای‌فای ناامن مهاجم می‌تواند داده‌هایی را که بین دستگاه مهمان و شبکه ارسال می‌شود، رهگیری کند.

فناوری‌های کلیدی مرتبط با امنیت سایبری و بهترین شیوه‌ها

آن‌چه در ادامه می‌آید، بهترین روش‌ها و فناوری‌هایی هستند که می‌توانند به سازمان شما کمک کنند امنیت سایبری مطمئنی پیاده‌سازی کنید و به این وسیله آسیب‌پذیری شما را در برابر حملات سایبری کاهش می‌دهند و از سیستم‌های اطلاعاتی حیاتی شما محافظت کنند، بدون اینکه در تجربهٔ کاربر یا مشتری دخالت کنند:

مدیریت هویت و دسترسی (IAM) نقش‌ها و امتیازهای دسترسی را برای هر کاربر و همچنین شرایطی را تعریف می‌کند که تحت آن‌ها امتیازهایشان به آن‌ها داده یا از آن‌ها گرفته می‌شود. روش‌های IAM شامل

یک بار ثبت‌نام است که به کاربر امکان می‌دهد بدون واردکردن مجدد اطلاعات مورد نیاز برای اعتبارسنجی در همان جلسه وارد شبکه شود. همچنین احراز هویت چندعاملی، که نیاز به دو یا چند اعتبار دسترسی دارد، حساب‌های کاربری ویژه که فقط به کاربران خاصی امتیازات مدیریتی می‌دهند و مدیریت چرخه عمر کاربر، که هویت هر کاربر و امتیازات دسترسی آن‌ها را از ثبت نام اولیه تا زمان انقضای عضویت مدیریت می‌کند، از دیگر روش‌های IAM است. ابزار IAM همچنین می‌تواند به متخصصان امنیت سایبری دید عمیق‌تری دربارهٔ فعالیت‌های مشکوک در دستگاه‌های کاربر نهایی بدهد، از جمله دستگاه‌های آن دسته از کاربران نهایی که نمی‌توانند به‌صورت فیزیکی به آن‌ها دسترسی داشته باشند. این امر به تسریع بررسی و زمان لازم برای جداسازی و مهار آسیب ناشی از نقض (breach) کمک می‌کند.

پلتفرم جامع امنیت داده از اطلاعات حساس در چندین محیط از جمله محیط‌های چندابری ترکیبی محافظت می‌کند. بهترین پلتفرم‌های امنیت داده، دیدی خودکار و در لحظه نسبت به آسیب‌پذیری‌های داده‌ها فراهم می‌کنند و همچنین نظارت مستمری ارائه می‌کنند که آسیب‌پذیری‌ها و خطرات داده‌ها را قبل از نقض آن‌ها به پلتفرم‌های امنیتی هشدار می‌دهد. پشتیبان‌گیری و رمزگذاری نیز برای ایمن‌نگه‌داشتن داده‌ها حیاتی هستند.

اطلاعات امنیتی و مدیریت رویداد (SIEM) داده‌های به‌دست‌آمده از رویدادهای امنیتی را جمع‌آوری و تحلیل می‌کند تا به‌طور خودکار فعالیت‌های مشکوک کاربران را شناسایی کند و واکنشی پیشگیرانه یا اصلاحی به آن‌ها نشان دهد. امروزه راه‌حل‌های SIEM شامل روش‌های تشخیص پیشرفته مانند تحلیل رفتار کاربران و هوش مصنوعی (AI) است SIEM .می‌تواند به‌طور خودکار پاسخ مناسب برای تهدید سایبری را در راستای اهداف مدیریت ریسک سازمان شما اولویت‌بندی کند. بسیاری از سازمان‌ها ابزارهای SIEMخود را با پلتفرم‌های هماهنگ‌سازی امنیتی، اتوماسیون و پاسخ (SOAR)ادغام می‌کنند که واکنش سازمان‌ها به حوادث امنیت سایبری cybersecurity را بیش از پیش خودکار و تسریع می‌کند و بسیاری از حوادث را بدون دخالت انسان حل می‌کند.

استراتژی امنیتی با سطح اعتماد صفر

امروزه کسب وکارها طوری با هم مرتبط هستند که هیچ‌گاه سابقه نداشته است .سیستم‌ها، کاربران و داده‌ها همگی در محیط‌های مختلفی زندگی و کار می‌کنند .امنیت مبتنی بر محیط نه‌تنها دیگر کافی نیست، بلکه تعبیه کنترل‌های امنیتی در محیط پیچیدگی به بار می‌آورد و در نتیجه حفاظت از مهمترین دارایی‌ها را کاهش می‌دهد. «استراتژی سطح اعتماد صفر» به‌منظور بررسی اصالت و هدف هر کاربر یا دستگاه یا اتصال به هر کسب‌وکار، کنترل‌هایی را برای تأیید اعتبار آن‌ها به کار می‌گیرد. سازمان‌ها برای موفقیت در اجرای استراتژی سطح اعتماد صفر به روشی برای ترکیب اطلاعات امنیتی نیاز دارند تا زمینه‌ای (امنیت دستگاه، مکان و غیره) ایجاد کند که کنترل‌های اعتبارسنجی از آن‌ها خط بگیرد و به اجرا گذاشته شود.

امنیت سایبری cybersecurity در ایران

امروزه فضای مجازی به بخش تفکیک‌ناپذیری از زندگی انسان‌ها تبدیل شده و با سرعت شتابان، تمامی عرصه‌های زیست بشر را تحت تأثیر قرار داده است. از این رو ماهیت‌شناسی این فضا و تشخیص شرایط و الزام‌های تبدیل‌شدن به بازیگری توانمند در این عرصه، نخستین گام است و هرگونه بی‌توجهی و غفلت نسبت به این پدیده، صدمه‌ها و آسیب‌های خطرناکی را متوجه جامعه خواهد کرد.

سال 2019 را می‌توان یکی از پرالتهاب‌ترین سال‌ها از نظر امنیت سایبری در ایران و جهان دانست که شیوع کرونا و دورکاری در آن بی‌تأثیر نبوده است. مرکز تخصصی آپا وابسته به دانشگاه صنعتی اصفهان در جدیدترین گزارش سالانه خود مروری بر وضعیت امنیت سایبری ایران و جهان داشته است که برخی رخدادهای مهم در حوزه فضای مجازی کشور مثل نشت اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام و حمله به زیرساخت‌های ابرآروان پرداخته است. اگرچه به‌دلیل شیوع کرونا و شرایط دورکاری انتظار می‌رفت سال ۲۰۱۹ سالی پرهیاهو در حوزه فناوری اطلاعات باشد، اما شاید کمتر کسی حدس می‌زد که این سال حتی در نخستین روزهای خود در حوزه امنیت سایبری غوغا به پا کند. در اولین روزهای ۲۰۱۹، نه اخبار مربوط به کرونا بلکه خبر نشت اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام در فضای مجازی کشور سروصدای زیادی به پا کرد. این اطلاعات روی سامانه‌ای به نام «سامانهٔ شکار» قرار داشت که پایگاه داده‌های الاستیک جست‌وجوی آن، بدون کلمهٔ عبور یا سازوکار احزار هویت بود. باب دیاچنکو، کارشناس امنیت سایبری، این سرور را در ۲۶ مارس کشف کرد و تحلیل و بررسی کرد. سپس در ۲۹ مارس مشکل را به صاحبان این پایگاه گزارش کرد و اطلاعات در۳۰ مارس از این پایگاه حذف شد. اما حذف اطلاعات در آن زمان نتوانست جلوی انتشار عمومی داده‌ها را بگیرد و اطلاعات در فروم‌های هکری با قیمت ۵۰۰ دلار به فروش رفت.

اما یکی از بزرگ‌ترین حملات سایبری سال ۲۰۱۹ که سروصدای زیادی به پا کرد، حملهٔ گسترده به زیرساخت‌های ابر آروان بود . هدف از این حمله تخریب و حذف اطلاعات مشتریان گزارش شد. به گزارش وب‌سایت رسمی این شرکت، این حمله در حدود ۱۶ درصد از مشتریان غیررایگان ابرآروان را متأثر کرد. در این حمله، آن گروهی از مشتریان دچار مشکل اساسی شدند که از داده‌های خود نسخه پشتیبان نداشتند یا معماری آن‌ها به شکل ابرزی (Cloud Native) نبود.

سال‌هاست که متخصصان فضای سایبری در ایران متوجه حملات سایبری شده‌اند و به نهادهای مرتبط هشدارهای لازم را داده‌اند. در این رابطه، افزایش ضریب امنیت فضای سایبری و پیشگیری از حملات سایبری امری ضروری است.