امنیت سایبری :

همزمان با گسترش تعداد کاربران، افزایش حجم داده‌ها و نیاز به برقراری امنیت در فضای مجازی، بیش از پیش ما با مفاهیمی مانند هک، امنیت و دیوارهای امنیتی روبرو شده‌ایم.

یکی از این اصطلاحات، مفهومی به نام امنیت سایبری (Cyber Security) است که نقطه مقابلی برای هک و حملات مخرب در فضای دیجیتال محسوب می‌شود .

منظور از امنیت سایبری چیست؟

امنیت سایبری به معنای محافظت از سیستم‌های متصل به اینترنت شامل سخت‌افزار، نرم‌افزار و داده‌ها در برابر تهدیدات دیجیتال است.

این روش هم توسط افراد و هم توسط سازمان‌ها برای جلوگیری از نفوذ غیرمجاز به پایگاه‌های داده و سایر سیستم‌های دیجیتال مورد استفاده قرار می‌گیرد.

حملات هکرها یکی از مهم‌ترین تهدیداتی است که معمولاً برای نفوذ، اصلاح، پاک کردن، تخریب یا باج‌گیری سیستم‌ها و داده‌های محرمانه کاربر یا سازمان طراحی شده‌اند.

یکی از روش‌هایی که برای کنترل و خنثی کردن حملات هکرها می‌تواند استفاده شود، بکارگیری رویکردهای تدافعی در امنیت سایبری است.

انواع امنیت سایبری

امنیت سایبری را می‌توان به دسته‌های مختلفی تقسیم کرد که هماهنگی مشترک آنها جهت تامین امنیت سایبری در یک سازمان ضروری است.

این دسته‌بندی‌ها شامل موارد زیر هستند:

- امنیت برنامه‌ها
- امنیت اطلاعات یا داده‌ها
- امنیت شبکه‌ها
- امنیت برنامه‌هایی برای بازیابی بلایا و تداوم کسب‌وکار
- امنیت عملیاتی
- امنیت ابری
- امنیت زیرساخت‌های حیاتی
- امنیت فیزیکی
- آموزش کاربران نهایی

حفظ امنیت سایبری در میان سناریوهای تهدید، همیشه در حال تحول نوعی چالش بزرگ برای سازمان‌ها است.

برای مثال در گذشته رویکردهای واکنشی سنتی که در برابر تهدیدات کمتر شناخته‌شده رویکرد تدافعی در نظر گرفته نمی‌شد، امروزه کارآمد نیست و می‌بایست برای برقراری امنیت در فضای سایبری، رویکردهای فعال‌تر و سازگارتر ارائه کرد.

مزایای امنیت سایبری

از مهم‌ترین مزایای امنیت سایبری می‌توان به موارد زیر اشاره کرد:

- محافظت از کسب‌وکارها در برابر حملات سایبری و نقض اطلاعات
- حفاظت از داده‌ها و شبکه‌ها
- جلوگیری از دسترسی غیرمجاز کاربران
- ایمن‌سازی کاربران نهایی و دستگاه‌های نقطه پایانی
- رعایت استانداردهای نظارتی
- تداوم عملیات تجاری کسب‌وکارها
- افزایش اعتماد و شهرت به شرکت در بین توسعه‌دهندگان، شرکا، مشتریان، ذینفعان و کارمندان

اشکال مختلف تهدیدات امنیت سایبری

همگام با فناوری‌های در حال تحول، انواع تهدیدات مختلف و جدیدی در حوزه امنیت سایبری به وجود می‌آیند یا به شکل پیشرفته‌تری تبدیل می‌شوند. در حال حاضر تهدیدات امنیتی مختلفی وجود دارد که در ادامه برخی از رایج‌ترین این تهدیدات مورد بحث قرار خواهند گرفت.

بدافزارها

بدافزارها (Malware) دسته‌ای از نرم‌افزارهای مضر هستند که در آن هر فایل یا برنامه‌ای می‌تواند برای آسیب رساندن به کاربر کامپیوتر به سلاحی خطرناک تبدیل شود .

این شامل انواع مختلفی از بدافزارها مانند کرم‌ها، ویروس‌ها، تروجان‌ها و جاسوس‌افزارها است.

باج افزارها

باج‌افزارها (Ransomware) نوعی بدافزار هستند که در آن یک مهاجم یا به اصطلاح یک هکر، فایل‌های سیستم کامپیوتری شخص یا سازمان قربانی را معمولاً از طرق مختلفی رمزگذاری می‌کند و به دنبال آن در ازای رمزگشایی و انتشار این فایل‌ها، از کاربر باج‌خواهی می‌کند.

مهندسی اجتماعی

مهندسی اجتماعی (Social Engineering) نوعی روش حمله است که بر تعامل انسان با انسان متکی است و کاربران را فریب می‌دهد تا با دور زدن پروتکل‌های امنیتی، اطلاعاتی که معمولاً ایمن هستند را بدست آورند.

فیشینگ

فیشینگ (Phishing) نوعی مهندسی اجتماعی محسوب می‌شود که شامل ارسال ایمیل‌ها یا پیام‌های متنی جعلی است که به نظر می‌رسد منشا آن از منابع قانونی باشد.

این پیام‌ها معمولاً مخاطبان گسترده‌ای را هدف قرار می‌دهند. هدف این پیام‌ها سرقت اطلاعات حساس، مانند جزئیات کارت اعتباری یا اعتبار ورود به سیستم است.

تهدیدهای داخلی

تهدیدهای داخلی مربوط به نقض یا ضررهای امنیتی است که توسط عوامل انسانی مانند کارمندان، پیمانکاران یا مشتریان ایجاد می‌شود. این تهدیدها می‌توانند مخرب یا غیرعمدی باشند.

حملات انکار سرویس

حملات انکار سرویس توزیع شده (DDoS) زمانی اتفاق می‌افتد که چندین سیستم مانند سرور، وب‌سایت یا سایر منابع شبکه بر ترافیک یک سیستم هدف غلبه می‌کنند. این حملات با پیام‌ها یا درخواست‌های اتصال، سیستم را کند یا خراب می‌کنند و مانع از ایجاد ترافیک قانونی می‌شوند.

تهدیدهای پایدار پیشرفته

تهدیدهای پایدار پیشرفته (APT) به حملات هدفمند و پایداری گفته می‌شود که در آن مهاجم، شبکه‌ای را با هدف سرقت داده‌ها مورد حمله قرار می‌دهد و تا مدت زمان طولانی شناسایی نمی‌شود.

حملات مردمیانی

حملات Man-in-the-Middle (MitM)یا حملات مردمیانی، حملات نظارتی هستند که در آن مهاجم، پیام‌ها را بین دو طرف که مستقیماً با یکدیگر در ارتباط هستند، ره‌گیری و ارسال می‌کند.

سایر حملات رایج عبارت‌اند از باتنت‌ها، کیت‌های بهره‌برداری، تبلیغات بد، vishing، حملات پر کردن اعتبار، حملات اسکریپت بین سایتی(XSS) ، حملات تزریق SQLو به خطر انداختن ایمیل‌های تجاری.(BEC)

چالش‌های امنیت سایبری

امنیت سایبری به طور مداوم با مسائلی مانند هکرها، از دست دادن داده‌ها، حریم خصوصی، مدیریت ریسک و تکامل استراتژی‌های امنیت سایبری دست و پنجه نرم می‌کند. پیش‌بینی می‌شود که تعداد حملات سایبری در طول سال‌های آینده افزایش یابد.

چالش‌های کلیدی امنیت سایبری که مستلزم توجه مداوم‌اند شامل موارد زیر هستند:

- سازگاری با تهدیدات در حال تغییر
- مدیریت حجم داده‌ها
- ارتقاء آگاهی و آموزش امنیت سایبری
- رفع کمبود نیروی کار و شکاف مهارتی
- مدیریت حملات زنجیره تأمین و ریسک‌های شخص ثالث

سازگاری با تهدیدات در حال تغییر

یکی از مهم‌ترین موانع در امنیت سایبری، تغییر مستمر چشم‌انداز خطرات امنیتی است .

ظهور فناوری‌های جدید و کاربردهای بدیع یا متفاوت آن‌ها، راه را برای روش‌های جدید حمله هموار می‌کند. به‌روز ماندن با این تغییرات و پیشرفت‌های مکرر در حملات و اقدامات حفاظتی، کاری اساسی و در حین حال سخت محسوب می‌شود.

یکی از مسائل مهم این است که اطمینان حاصل شود تمام جنبه‌های امنیت سایبری به طور مداوم به‌روز می‌شوند تا از آسیب‌پذیری‌های احتمالی دفاع کنند. این می‌تواند به‌ویژه برای سازمان‌های کوچک‌تر با کارکنان محدود یا منابع داخلی، چالش‌برانگیز باشد.

مدیریت حجم داده‌ها

سازمان‌ها معمولاً با حجم زیادی از داده‌ها سروکار دارند که ریسک به سرقت رفتن داده‌ها توسط مجرمان سایبری را افزایش می‌دهد.

به عنوان مثال، سازمانی که اطلاعات شخصی پرسنل را در فضای ابری ذخیره می‌کند، ممکن است مورد هدف حمله باج‌افزار قرار گیرد. به همین خاطر سازمان‌ها باید اقدامات پیشگیرانه‌ای را برای جلوگیری از چنین نقض‌هایی انجام دهند.

ارتقاء آگاهی و آموزش امنیت سایبری

برنامه‌های امنیت سایبری باید آموزش کاربران نهایی را در اولویت قرار دهد. کارمندان ممکن است ناخواسته تهدیدها و آسیب‌پذیری‌هایی را از طریق لپ‌تاپ یا دستگاه‌های تلفن همراه خود وارد فضای کار کنند. آن‌ها همچنین ممکن است رفتارهای ناامن مانند کلیک کردن بر روی لینک‌های مخرب یا دانلود پیوست‌ها از ایمیل‌های فیشینگ را خواسته یا ناخواسته انجام دهند. آموزش منظم

آگاهی از امنیت می‌تواند کارمندان را توانمند کند تا نقش موثری در محافظت از شرکت خود در برابر تهدیدات سایبری ایفا کنند.

رفع کمبود نیروی کار و شکاف مهارتی

یکی دیگر از چالش‌های امنیت سایبری، کمبود پرسنل امنیت سایبری ماهر است. همان‌طور که کسب‌وکارها داده‌های بیشتری را جمع‌آوری و استفاده می‌کنند، نیاز به کارکنان امنیت سایبری برای تجزیه‌وتحلیل، مدیریت و پاسخ به حوادث افزایش می‌یابد.

مدیریت حملات زنجیره تأمین و خطرات شخص ثالث

سازمان‌ها ممکن است پروتکل‌های امنیتی سخت‌گیرانه‌ای را درنظر بگیرند اما اگر شرکا، تأمین‌کنندگان و فروشندگان شخص ثالثی که به شبکه‌های آنها دسترسی دارند؛ ایمن نباشند، تمام این تلاش‌ها ممکن است به هدر برود. در این حال حملات زنجیره تأمین مبتنی بر نرم‌افزار و سخت‌افزار به چالش‌های امنیتی پیچیده‌ای تبدیل می‌شوند. به همین دلیل سازمان‌ها باید به ریسک شخص ثالث در زنجیره تأمین رسیدگی کنند و مشکلات عرضه نرم‌افزار را به حداقل برسانند.

نقش اتوماسیون در امنیت سایبری چیست؟

اتوماسیون (خودکار سازی وظایف) به عنصری حیاتی در ایمن‌سازی کسب‌وکارها همگام با افزایش تعداد روزافزون و پیچیدگی تهدیدات سایبری تبدیل شده است. استفاده از هوش مصنوعی و یادگیری ماشین در بخش‌هایی که داده‌های با حجم بالا را مدیریت می‌کنند، می‌تواند امنیت سایبری را در زمینه‌های کلیدی زیر افزایش دهد :

- شناسایی تهدیدات سیستم‌های هوش مصنوعی می‌تواند حجم وسیعی از داده‌ها را پردازش کرده، تهدیدات شناخته شده را شناسایی و تهدیدات جدید بالقوه را پیش‌بینی کند.
- واکنش به تهدیدات سیستم‌های هوش مصنوعی می‌توانند اقدامات امنیتی را به صورت خودکار طراحی و اجرا کنند.

از جمله دیگر مزایای اتوماسیون در این حوزه می‌توان به امنیت سایبری طبقه‌بندی حملات، شناسایی بدافزار، تجزیه‌وتحلیل ترافیک و بررسی انطباق اشاره کرد.

تامین‌کنندگان و ابزارهای امنیت سایبری

تامین‌کنندگان امنیت سایبری مجموعه‌ای از محصولات و خدمات امنیتی را ارائه می‌دهند. بطور کلی ابزارها و سیستم‌های امنیتی رایج عبارت‌اند از:

- مدیریت هویت و دسترسی(IAM)
- دیوارهای امنیتی
- حفاظت نقطه پایانی
- آنتی‌ویروس
- سیستم‌های تشخیص/جلوگیری از نفوذ(IPS/IDS)
- پیشگیری از دست دادن داده(DLP)
- اطلاعات امنیتی و مدیریت رویداد(SIEM)
- ابزارهای رمزگذاری
- اسکنرهای آسیب‌پذیری
- شبکه‌های خصوصی مجازی(VPN)
- پلتفرم محافظت از بار کاری ابری(CWPP)
- کارگزار امنیتی Cloud Access (CASB)

فرصت‌های شغلی در رشته امنیت سایبری چیست؟

با گسترش چشم‌انداز تهدیدات سایبری و تهدیدات نوظهور مانند موارد مرتبط با اینترنت اشیا، نیاز روزافزون به افرادی با آگاهی از امنیت سایبری و مهارت‌های سخت‌افزاری و نرم‌افزاری وجود دارد. وظایف متخصصان فناوری اطلاعات و سایر متخصصان کامپیوتری در زمینه امنیت عبارت‌اند از:

- **مدیر ارشد امنیت اطلاعات :(CISO)** این نقش شامل اجرای برنامه امنیتی در سراسر سازمان و نظارت بر عملیات بخش امنیت فناوری اطلاعات است.
- **افسر ارشد امنیت :(CSO)** این فرد مسئول اجرایی امنیت فیزیکی یا سایبری یک سازمان است.
- **مهندسین امنیت** :این متخصصان با تمرکز بر کنترل کیفیت در زیرساخت فناوری اطلاعات، از دارایی‌های سازمان در برابر تهدیدات محافظت می‌کنند.
- **معماران امنیتی** :این افراد مسئول برنامه‌ریزی، تجزیه‌وتحلیل، طراحی، آزمایش، نگهداری و پشتیبانی از زیرساخت‌های حیاتی یک سازمان هستند.
- **تحلیل‌گران امنیتی** :مسئولیت‌های آن‌ها شامل برنامه‌ریزی اقدامات و کنترل‌های امنیتی، حفاظت از فایل‌های دیجیتال و انجام ممیزی‌های امنیتی داخلی و خارجی است.
- **متخصص تست نفوذ** :این افراد به عنوان هکرهای اخلاقی، امنیت سیستم‌ها، شبکه‌ها و برنامه‌ها را آزمایش می‌کنند و به دنبال آسیب‌پذیری‌هایی می‌گردند که می‌تواند توسط عوامل مخرب مورد سوءاستفاده قرار گیرند.

- **شکارچیان تهدید** :به عنوان تحلیل‌گران تهدید، هدف آن‌ها کشف آسیب‌پذیری‌ها حملات و کاهش آن‌ها قبل از به خطر افتادن یک کسب‌وکار است.

سایر مشاغل امنیت سایبری شامل مشاوران امنیتی، افسران حفاظت از داده‌ها، معماران امنیت ابری، مدیران و تحلیل‌گران مرکز عملیات امنیتی(SOC) ، محققان امنیتی، رمزنگاران و مدیران امنیتی است.

نقش ما در امنیت سایبری چیست؟

به عنوان کاربران اینترنت، نقش ما در برقراری امنیت سایبری شامل اجرای عادات اینترنتی ایمن برای محافظت از خود و شبکه‌هایمان در برابر تهدیدات سایبری بالقوه است. برای مثال استفاده از رمز عبورهای قوی و منحصربه‌فرد، فعال کردن احراز هویت دومرحله‌ای، به‌روزرسانی منظم و اصلاح نرم‌افزار، اجتناب از کلیک روی لینک‌ها یا وب‌سایت‌های مشکوک و توجه به اطلاعاتی که به‌صورت آنلاین به اشتراک می‌گذاریم، از جمله راهکارهایی است می‌توان در راستای تامین امنیت در فضای سایبری به کار برد.

همچنین وظیفه ما شامل آموزش خود در مورد تهدیدات سایبری مختلف و مطلع ماندن از آخرین اقدامات امنیت سایبری است. در مفهوم وسیع‌تر، شرکت‌ها و سازمان‌ها مسئولیت حفاظت از سیستم‌ها و داده‌های خود را دارند که شامل حفظ قدرتمند زیرساخت امنیت سایبری و آموزش کارکنان در مورد بهترین شیوه‌های امنیت سایبری است.

امنیت سایبری یا Cyber Security چیست؟

امنیت سایبری یک موضوع بسیار حیاتی و با اهمیت است که در دنیای امروزه مورد توجه ویژه‌ای قرار گرفته و با پیشرفت فناوری و ارتباطات، حملات سایبری نیز به شدت افزایش یافته که گاها عواقب جدی برای افراد و سازمان‌ها در پی دارند؛ لذا برای دستیابی به امنیت سایبری، باید به مسائل مربوط به امنیت داده‌ها، شبکه‌ها، نرم‌افزارها و... توجه نمود؛ محافظت از منابع محرمانه و مهم در برابر دسترسی غیرمجاز و هکرها، استفاده از رمزنگاری قوی، بروزرسانی سیستم‌های امنیتی، آموزش کارکنان در حوزه امنیت سایبری و... مواردی از اقداماتی حفاظتی جهت پیشگیری و مقابله با حملات سایبری هستند.

امنیت سایبری (cybersecurity) به مجموعه اقدامات و تدابیری اشاره دارد که برای حفاظت از اطلاعات و داده‌های ما در فضای اینترنتی لازم است؛ این اقدامات امنیتی از طریق تدابیر، تکنیک‌ها و فناوری‌هایی مانند: رمزگذاری، دیواره آتش، نرم‌افزارهای ضد ویروس، به‌روزرسانی‌های امنیتی و آموزش کاربران به منظور شناسایی و پیشگیری از تهدیدات مجازی اجرا می‌شوند.

با توجه به فضاهای کاربری نامحدود و گسترده‌ای که هر روزه بیش از پیش در اختیار کاربران مجازی قرار می‌گیرد؛ دامنه فعالیت و ایمن‌سازی سایبری نیز وسعت یافته و نیازمند رایزنی، علم و تخصصات متنوع جهت پیشگیری از وقوع جرایم سایبری و اجرای پروتکل‌های مناسب در برخورد با هر تهدیدی است؛ که در سطح فردی و اجتماعی کاربران یا امنیت ملی را با مشکل روبرو می‌سازد؛ لذا در ادامه به کلیت این سیستم حفاظتی و نحوه عملکرد آن می‌پردازیم.

امنیت سایبری در واقع حفاظت از اطلاعات و سیستم‌های کامپیوتری در مقابل تهدیدات و حملات اینترنتی در دنیای مدرن ارتباطات است.

تهدیدات سایبری می‌توانند شامل: حملات هکرها، نفوذ به سیستم‌ها، سرقت اطلاعات، بدافزارها (ویروس‌ها و نرم‌افزارهای خبیث) و دیگر نقض‌های امنیتی باشند .لذا مراحل کلی امنیت سایبری به شرح زیر تدوین اجرا می‌گردند.

پروتکل‌های امنیتی :استفاده از پروتکل‌های امنیتی مانند HTTPS :برای ارتباطات آنلاین با وبسایت‌ها و سرویس‌ها مهم است؛ لذا این پروتکل‌ها اطمینان می‌دهند که ارتباطات شما رمزنگاری و امن است.

رمزنگاری :استفاده از رمزنگاری برای محافظت از اطلاعات شخصی و حساس مانند: رمزهای عبور و اطلاعات بانکی که اهمیت دارند؛ در نتیجه با استفاده از الگوریتم‌های رمزنگاری، اطلاعات شما به صورت مخفی ذخیره می‌شوند.

به‌روزرسانی نرم‌افزارها :آپدیت نرم‌افزارهای مورد استفاده ازجمله سیستم‌عامل، مرورگر و... این به‌روزرسانی‌ها اغلب شامل اصلاحات امنیتی هستند که با نصب آن‌ها، ضعف‌ها و آسیب‌پذیری‌های احتمالی در سیستم شما کاهش می‌یابد.

رمزهای عبور قوی :استفاده از رمزهای عبور قوی و یکتا برای هر حساب که ترکیبی از حروف بزرگ و کوچک، اعداد و نمادهای خاص باشد؛ تا از نفوذ به حساب شما جلوگیری کند (از رمزهای عبور متفاوت) برای هر حساب استفاده کنید.

آگاهی از تهدیدات :آگاهی از تهدیدات سایبری رایج مانند فیشینگ، نرم‌افزارهای مخرب و نفوذ ممکن است به شما کمک کند تا اقدامات لازم برای جلوگیری از آن‌ها را انجام دهید؛ پس همواره مراقب پیام‌ها و لینک‌های مشکوک باشید.

پشتیبان‌گیری منظم :در صورت بروز مشکلاتی مانند هک یا از دست رفتن داده‌ها، می‌توانید با تهیه نسخه پشتیبان از اطلاعات، در صورت لزوم به حالت قبلی بازگردید.

نرم‌افزارهای امنیتی :استفاده از نرم‌افزارهای آنتی‌ویروس، فایروال و ضد جاسوسی می‌تواند از حملات مخرب مانند نفوذ و نصب برنامه‌های آفت‌زا جلوگیری کند، این نرم‌افزارها به تشخیص و مسدود کردن فعالیت‌های مشکوک در سیستم شما کمک می‌کنند.

آموزش و آگاهی :به دست آوردن آموزش‌های مربوط به امنیت سایبری و آگاهی از روش‌های حفاظت در برابر تهدیدات، می‌تواند به شما در مقابله با خطرات سایبری کمک کند؛ بنابراین آشنایی با مباحث رمزنگاری، فیشینگ، نفوذ و... کمک می‌کند تا در برابر این تهدیدات اقدامات مناسبی را انجام دهید.

به طور کلی Cybersecurity برای محافظت از اطلاعات امنیتی شامل سه عنصر اصلی است: سیستم‌ها، شبکه‌ها و افراد، لذا اقداماتی برای حفاظت از سیستم‌ها و شبکه‌ها در برابر حملات مجازی انجام می‌شود و آموزش کاربران به منظور پیشگیری از تهدیدهای سایبری نیز بسیار مهم است.

تاریخچه امنیت سایبری(cyber security)

تاریخچه امنیت سایبری به اوایل دوران شبکه‌های کامپیوتری برمی‌گردد؛ در ابتدا هدف اصلی شبکه‌های کامپیوتری اشتراک منابع و ارتباط بین کامپیوترها بود و امنیت سایبری چندان مهم نبود؛ اما با گسترش اینترنت و افزایش تعداد کامپیوترها و سرویس‌ها ،نیاز به محافظت از اطلاعات حساس در برابر تهدیدات سایبری رو به افزایش رفت.

در دهه ۱۹۹۰ با گسترش اینترنت و استفاده گسترده از وب، تهدیدات سایبری به طور قابل توجهی افزایش یافتند و اینترنت به عنوان شبکه با وسعت جهانی مورد استفاده قرار گرفت و این امر به تهدیدات جدیدی مانند: ویروس‌ها، کرم‌ها، تروجان‌ها و حملات دیده‌بانی (DoS) منجر شد؛ که در این دوره، توسعه رمزنگاری و تکنیک‌های امنیتی دیگر نیز در حال انجام بود.

در سال‌های ۲۰۰۰ با رشد سریع تجارت الکترونیک و انتقال اطلاعات حساس از طریق اینترنت، نیاز به امنیت سایبری بیشتر و حملات سایبری نیز پیچیده‌تر شدند و تکنیک‌های جدیدی مانند: فیشینگ ،نفوذ و سرقت هویت ظاهر شد و حملات به نظام‌های مختلف، شبکه‌های بزرگ و حتی دولت‌ها نیز رخ داد.

امروزه حفظ امنیت اطلاعات (سایبر سکوریتی) در فضای مجازی یکی از اولویت‌های اصلی برای سازمان‌ها، دولت‌ها و کاربران عادی است. توسعه تکنولوژی‌های جدید مانند: هوش مصنوعی و یادگیری ماشینی و... باعث بروز چالش‌ها و تهدیدات جدید در حوزه امنیت سایبری شده است.

بسیاری از حوادث سایبری مشهور در تاریخ حملاتی همچون Wannacry و NotPetya در سال ۲۰۱۷ نشان دادند که نقص‌های امنیتی در سیستم‌ها و شبکه‌ها می‌توانند عواقب جدی برای سازمان‌ها و جوامع داشته باشند؛ از آن زمان به بعد، آگاهی و آموزش درباره امنیت سایبری در حال افزایش است و بسیاری از سازمان‌ها و افراد تلاش می‌کنند تا از تهدیدات سایبری محافظت کنند و اقدامات امنیتی مناسب را انجام دهند.

اهمیت امنیت سایبری برای کشورها

این امکانات برای سازمان‌ها و شرکت‌ها نیز بسیار حیاتی است؛ زیرا سرقت اطلاعات می‌تواند عواقب جدی شامل از دست دادن اعتماد مشتریان، خسارت مالی و حتی خسارت به سابقه و اعتبار یک سازمان باشد.

ضمنا امنیت سایبری به ما امکان استفاده ایمن و مطمئن از خدمات آنلاین را می‌دهد؛ لذا با تضمین امنیت در فرآیندهای مختلف مانند: تراکنش‌های بانکی، خرید آنلاین و ارتباطات ایمن، افراد می‌توانند با اطمینان بیشتری از خدمات اینترنتی و درگاه‌های آنلاین استفاده کنند.

با توجه به اینکه تهدیدات سایبری به طور مداوم در حال تغییر و تکامل هستند؛ بروزرسانی مداوم و آگاهی درباره راهکارها و تکنیک‌های جدید نقش مهمی دارد؛ لذا در ادامه به چند مورد از اصلی‌ترین فواید امنیت سایبری در سطح فردی و اجتماعی اشاره می‌کنیم.

۱. حفظ اطلاعات شخصی شامل اطلاعات حساب بانکی، رمز عبور، ایمیل‌ها و سایر اطلاعات حساس مخاطبان.
۲. حفاظت از اموال دیجیتال مانند: فایل‌های مهم، تصاویر، ویدئوها و...
۳. حفظ حریم خصوصی با جلوگیری دسترسی غیرمجاز به اطلاعات شخصی با توجه به رشد روز افزون تکنولوژی و فضای آنلاین

٤. حفظ امنیت سازمان‌ها و نهادها با بهبود امنیت سایبری، در بخش عمومی و خصوصی که منجربه حفاظت از اطلاعات و اعتماد عامه کاربران به آن‌ها می‌شود.

٥. پیشگیری از جرائم سایبری با توجه به میزان روزافزون استفاده از اینترنت و سیستم‌های دیجیتال

انواع امنیت سایبری

اگرچه امنیت سایبری برحسب نوع جرایم، نوع حملات و... در هر کشوری طبق الگوریتم و قوانین خاص خود اجرا می‌شود؛ اما به طور کلی این سیستم با هدف پیشگیری از نفوذ عوامل غیرمجاز و جلوگیری از دسترسی چنین مجرمانی به داده‌های محرمانه، انواع ترفندهای امنیتی، استراتژی و تکنیک‌های حفاظتی خود را به شیوه‌های فنی، هوشمند، نرم‌افزاری و تحت وب به کار می‌گیرد؛ تا از هر نوع تعدی به حریم خصوصی سازمان‌ها و صفحات کاربری پیشگیری کند؛ لذا انواع اصلی امنیت سایبری برای تحقق این اهداف به صورت زیر هستند.

امنیت شبکه و امنیت سایبری

شامل تدابیر و روش‌هایی است که برای محافظت از شبکه‌های کامپیوتری و جلوگیری از دسترسی غیرمجاز، مهاجمان و جاسوسان سایبری استفاده می‌شود؛ این شامل استفاده از فایروال‌ها، شبکه‌های خصوصی مجاز، رمزنگاری اطلاعات و تشخیص حملات شبکه است.

امنیت سایبری در برنامه‌ها

برای محافظت از نرم‌افزارها و برنامه‌های کامپیوتری در برابر نفوذ و حملات زیانبار از امنیت سایبری برنامه‌های استفاده می‌شود که شامل: استفاده از آزمون امنیتی و استفاده از کدهای امن، روش‌های تست نفوذ و آموزش توسعه‌دهندگان در زمینه امنیت است.

امنیت داده

این نوع امنیت سایبری بر عملیات محافظت از داده‌های حساس و مهم تمرکز دارد و به مقابله با هرگونه نفوذ، تخریب، مختومه سازی، پردازش، ریست و تغییر غیرمجاز داده‌ها توسط عوامل بیگانه می‌پردازد؛ امنیت داده حاوی استفاده از رمزنگاری داده‌ها، سیاست‌های مدیریت دسترسی، پشتیبان‌گیری منظم و حفاظت از داده‌ها در مقابل سرقت و نفوذ عوامل غیرمجاز است.

امنیت فیزیکی

مجموعه اقداماتی که جهت حفظ دارایی‌های یک سازمان در برابر حملات سایبری صورت می‌گیرد؛ در حیطه امنیت فیزیکی قرار دارد؛ لذا محافظت از تجهیزات فیزیکی مرتبط با فضای سایبری مانند: سرورها، روترها، سوییچ‌ها و تجهیزات شبکه، با استفاده از سیستم‌های کنترل دسترسی فیزیکی، توسط این نوع از امنیت سایبری انجام می‌شود.

امنیت رمزنگاری

رمزنگاری اطلاعات یکی از اصلی‌ترین روش‌ها برای محافظت از دیتاها در ارتباطات سایبری است و طی این فرآیند، اطلاعات قابل خواندن به یک فرمت رمزی و ناشناخته تبدیل می‌شود؛ لذا در این در این نوع امنیت سایبری استفاده از روش‌ها و استانداردهای امنیتی به عنوان یک استراتژی کلی در طراحی و پیاده‌سازی سیستم‌های رمزنگاری بسیار مهم است.

امنیت سایبری با هوش مصنوعی: هوش مصنوعی بخش عمده‌ای از سایبری سکوریتی را ساپورت کرده و شامل: تشخیص سریع حملات، پیشگیری از حملات جدید، پاسخ سریع با تهدیدات، تقویت سیستم امینی و... است؛ این تشخیص هوشمند و به تبع اقدامات سریع و خودکار به میزان قابل ملاحظه‌ای بر سرعت‌عمل در پاسخ‌دهی و مختل سازی حملات سایبری تاثیرگذار خواهد بود.

امنیت سایبری همچنین شامل آموزش و آگاهی کاربران درباره تهدیدات گروه‌های سایبری و روش‌های پیشگیری و پاسخ به این ابهام است؛ که گروه‌های سایبری یعنی چه؛ یا سایبری‌ها چه کسانی هستند؟

گروه سایبری به معنی یک گروه از افراد یا سازمان‌هایی است که با هدف انجام فعالیت‌های مرتبط با تکنولوژی اطلاعات، ارتباطات (IT) و فضای سایبری به صورت تخطی از قوانین و محدودیت‌ها، به سیستم‌ها و شبکه‌های سایبری حمله می‌کنند.

اعضای گروه سایبری می‌توانند از هکرها، کریمینال‌های کامپیوتری، هکتیویست‌ها، جاسوس‌های سایبری و... با اهداف سوء جهت برداشت اطلاعات، آسیب‌رسانی به ساختارهای اقتصادی و سیاسی، تخریب سرویس‌های آنلاین، تهدید امنیت فردی و اجتماعی کاربران فضای مجازی تشکیل شود.

تفاوت امنیت اطلاعات و امنیت سایبری در چیست؟

امنیت اطلاعات و امنیت سایبری هر دو به حفاظت از سیستم‌های اطلاعاتی و داده‌های می پردازند؛ اما امنیت اطلاعات به مجموعه‌ای از تدابیر فنی، فیزیکی و سازمانی اشاره دارد و هدف آن حفاظت از داده‌ها و اطلاعات در مقابل دسترسی غیرمجاز، نشت یا تغییر آن‌ها است؛ در حالی که امنیت سایبری به مباحث مرتبط با اینترنت، شبکه‌های کامپیوتری و دنیای دیجیتال ارتباط دارد و هدف آن جلوگیری از دسترسی غیرمجاز، تهدیدها و حملات اینترنتی به سیستم‌ها و داده‌ها است .

در کل، امنیت اطلاعات بیشتر به جنبه‌های فیزیکی و سازمانی توجه می‌کند، در حالی که امنیت سایبری بیشتر مرتبط با محافظت از فضای دیجیتال و شبکه‌های ارتباطی است؛ که هر دوی این مفاهیم شامل الزامات قانونی و امتیاز جنبه‌های اخلاقی نیز می‌شوند؛ لذا در ادامه جوانب و تفاوت‌هایی هریک را بیان می‌کنیم.

محدوده :امنیت اطلاعات عبارت است از مجموعه تدابیر و روش‌هایی که برای محافظت از اطلاعات مهم، حساس و گران‌بها در هر شکل و شیوه‌ای طراحی و پیاده‌سازی می‌شود؛ این شامل محافظت از اطلاعات فیزیکی و الکترونیکی مانند: اطلاعات روی کاغذ، فایل‌های الکترونیکی، داده‌های سازمانی و اطلاعات شخصی کاربران است.

اما امنیت سایبری بیشتر به محافظت از سیستم‌ها، شبکه‌ها، داده‌ها و فضای سایبری در برابر تهدیدات و حملات سایبری پرداخته شامل: محافظت از امنیت شبکه‌ها، اطلاعات آنلاین، سرورها، برنامه‌ها، امنیت اینترنت اشیا (IoT) و دیگر عناصر مرتبط با فضای سایبری است.

رویکرد :امنیت اطلاعات عموما بر تدابیر فیزیکی و الکترونیکی جلوگیری از دسترسی غیرمجاز، سرقت، از دست دادن و تخریب اطلاعات استفاده می‌شود و شامل :قفل‌های فیزیکی، کنترل دسترسی فیزیکی و روش‌های رمزنگاری است.

اما امنیت سایبری بیشتر بر تکنولوژی‌های مرتبط با فضای سایبری و ارتباطات الکترونیکی تمرکز دارد؛ این شامل تشخیص حملات شبکه، مدیریت دسترسی الکترونیکی، آگاهی از نقاط ضعف و تهدیدات سایبری و روش‌های پیشگیری از آن‌ها است.

تهدیدات :امنیت اطلاعات و امنیت سایبری با تهدیدات متفاوتی روبرو هستند؛ در امنیت اطلاعات، تهدیدات ممکن شامل: سرقت فیزیکی اطلاعات، دسترسی غیرمجاز به فایل‌ها، نفوذ به سیستم‌های فیزیکی و سوءاستفاده از اطلاعات شخصی می‌شود.

در مقابل تهدیدات امنیت سایبری به صورت نفوذهای نرم‌افزاری، ویروس‌ها، حملات دنباله‌دار، فیشینگ(DDoS) و سایر روش‌های مهاجمانه برای دسترسی غیرمجاز، تخریب داده‌ها، سرقت اطلاعات و تخریب سیستم‌ها باشد.

به طور کلی، امنیت اطلاعات بیشتر به جنبه‌های فیزیکی و الکترونیکی اطلاعات توجه دارد، در حالی که امنیت سایبری بیشتر به جنبه‌های فضای سایبری و شبکه‌های ارتباطی توجه می‌کند؛ با این حال هر دو مفهوم به یکدیگر مرتبط هستند و برای دستیابی به یک محیط امن باید هر دو را مد نظر قرار داد.

نقشه راه امنیت سایبری و اهداف آن

نقشه راه امنیت سایبری یک برنامه جامع است که برای تحقق اهداف امنیت سایبری در یک سازمان طراحی می‌شود؛ این نقشه شامل استراتژی‌ها، سیاست‌ها، فرآیندها، فناوری‌ها و تدابیر امنیتی است؛ که برای مقابله با تهدیدات سایبری و حفظ امنیت سیستم‌ها و داده‌ها در یک سازمان مورد استفاده قرار می‌گیرند و برخی از اهداف امنیت سایبری عبارتنداز:

۱) حفظ سلامت و یکپارچگی سیستم‌ها :هدف اصلی امنیت سایبری این است که سیستم‌های فناوری اطلاعات و ارتباطات (ICT)سازمان‌ها را در برابر حملات و نفوذهای سایبری محافظت کند؛ این شامل حفظ تمامیت داده‌ها، جلوگیری از تخریب سیستم‌ها و جلوگیری از دسترسی غیرمجاز به منابع سازمان است.

۲) مدیریت ریسک :امنیت سایبری باید به صورت مداوم ریسک‌های احتمالی را تشخیص دهد و برنامه و راهکارهای مناسب را برای کاهش آن‌ها اجرا کند؛ شناسایی آسیب‌پذیری‌ها، ارزیابی ریسک، پیاده‌سازی تدابیر امنیتی و مداومت فرآیندها مواردی از اقدامات مدیریت ریسک محسوب می‌شوند.

۳) حفاظت از داده‌ها و اطلاعات :یکی از اهداف مهم امنیت سایبری حفاظت از داده‌ها و اطلاعات حساس است به طور مثال: رمزنگاری، مدیریت دسترسی، پشتیبان‌گیری منظم، حفاظت از حریم خصوصی، اجرای سیاست‌ها و الزامات مربوط به حفاظت از داده‌ها را شامل می‌شود.

۴) آموزش و آگاهی کارکنان :یکی از عوامل مهم در امنیت سایبری، آگاهی و آموزش است؛ تا کارکنان در مورد خطرات سایبری، روش‌های پیشگیری، رفتارهای امن و استفاده صحیح از فناوری‌های آگاه شوند.

۵) مطابقت با قوانین و مقررات :سازمان‌ها باید با قوانین و مقررات مربوط به امنیت سایبری که توسط دولت یا نهادهای مربوطه تعیین می‌شوند هم راستا باشند؛ همچنین به رعایت قوانین حفاظت از اطلاعات شخص، استانداردهای امنیتی، گزارش‌دهی و تحقق از الزامات قانونی بپردازند.

این تنها چند مورد از اهداف امنیت سایبری هستند و برنامه نقشه راه برای هر سازمان با توجه به نیازها و شرایط خاص آن طراحی و اجرا می‌شود؛ این برنامه باید به صورت مداوم بروزرسانی و ارزیابی شود تا با تغییرات تهدیدات سایبری و فناوری‌های جدید همگام باشد و به حفظ امنیت سایبری سازمان کمک کند.

انواع تهدید های امنیت سایبری

تهدیدات امنیت سایبری می‌تواند از منابع مختلفی برخاسته و در مقیاس‌های مختلفی اتفاق بیفتند؛ با توجه به منبع حمله‌کننده و اهداف آن نیز دسته‌بندی مختلفی از موارد تخلف در حوزه امنیت سایبری وجود دارد که نمونه‌های زیر لیست خطرناک ترین حملات سایبری را نشان می‌دهند.

حملات نفوذکاران(Hackers)

این نوع حملات شامل تلاش‌های غیرمجاز برای نفوذ به سیستم‌ها یا شبکه‌ها با هدف دسترسی به اطلاعات حساس، تخریب سیستم‌ها یا سرقت منابع است.

حملات انکار سرویس(Denial of Service – DoS)

نوع حملات با اشغال منابع سیستم یا شبکه، سرویس اصلی را برای کاربران مختل می‌کند و آن‌ها را از دسترسی به سرویس موردنظر محروم می‌سازد.

حملات فیشینگ(Phishing)

در این نوع حملات، حمله‌کننده با استفاده از ارسال ایمیل‌ها یا صفحات وب تقلبی، کاربران را به افشای اطلاعات حساس مانند: رمز عبور یا شماره کارت اعتباری تشویق می‌کند.

نفوذ فیزیکی(Physical Intrusion)

حمله‌کننده با نفوذ به فضای فیزیکی سازمان، می‌تواند به تجهیزات فنی، سرورها، روترها و سایر دستگاه‌ها دسترسی پیدا کند و آن‌ها را تخریب یا مورد سوءاستفاده قرار دهد.

نفوذ داخلی(Insider Threats)

این نوع تهدیدات وقتی به وجود می‌آیند که کارمندان یا اشخاص داخلی با دسترسی مجاز به سیستم‌ها و اطلاعات، اقدام به سرقت اطلاعات، تخریب سیستم‌ها یا ایجاد آسیب می‌کنند.

حفره‌های امنیتی نرم‌افزاری(Software Vulnerabilities)

وقتی که نرم‌افزارها حاوی ضعف‌های امنیتی هستند؛ حمله‌کننده می‌تواند از آن‌ها بهره‌برداری کرده و به سیستم‌ها و داده‌ها دسترسی غیرمجاز یا کنترل داشته باشد.

حملات برداری بر پروتکل‌ها(Protocol Attacks)

یکی از شایع‌ترین چالش های امنیت سایبری، بهره‌برداری از ضعف‌ها و آسیب‌پذیری‌های موجود در پروتکل‌های شبکه است که منجربه نفوذ به سیستم‌ها یا دسترسی غیرمجاز به اطلاعات شود.

حملات از راه دور (Remote Attacks)

تلاش‌های نفوذ به سیستم‌ها و شبکه‌ها از راه دور که بدون دسترسی فیزیکی به دستگاه‌ها بوده و اغلب از طریق شبکه اینترنت، برقراری اتصالات ناامن، بهره‌برداری از ضعف‌های امنیتی و مکانیزم‌های شبکه صورت می‌گیرند.

این تنها چند مورد از انواع خطرات امنیت سایبری هستند و هر روزه تهدیدات جدیدی به وجود می‌آیند؛ برای مقابله با این تهدیدات معمولا ترکیبی از راهکارهای فنی، سیاست‌ها، آموزش امنیت سایبری به کاربران در قالب کتب امنیت سایبری، فیلم آموزشی امنیت سایبری و موارد تخصصی‌تری که در ادامه اشاره می‌کنیم ارائه می‌شوند.

قوانین امنیت سایبری

قوانین امنیت سایبری به عنوان مجموعه‌ای از مقررات و استانداردها توسط دولت‌ها، سازمان‌ها و سازمان‌های بین‌المللی تعریف می‌شود؛ این قوانین و مقررات از تهدیدات سایبری محافظت کرده و رفتارهای غیرمجاز را کنترل می‌کنند؛ با وجود قانون‌گذاری‌های متفاوتی که در هر دولتی رایج است؛ به چند مورد از مهم‌ترین قوانین سایبری اشاره می‌کنیم.

قوانین حفاظت از اطلاعات شخصی :این قوانین معمولا شامل محدودیت و الزاماتی برای سازمان‌ها و سرویس‌دهندگانی است که باید اطلاعات شخصی کاربران را حفظ کنند

قوانین مربوط به جرایم رایانه‌ای :این قوانین تعریف می‌کنند که چه نوع رفتارها و عملکردهایی در فضای سایبری ممنوع است و مجازات‌های قانونی را برای اینگونه جرایم تعیین می‌کنند؛ از جمله هکرهای نفوذکار، کلاهبرداری اینترنتی، سرقت هویت، تقلب الکترونیکی و...

قوانین حفاظت از اطلاعات حساس :این قوانین برای حفاظت از اطلاعات حساس و محرمانه مانند: اطلاعات تجاری، اطلاعات مالی و... برای رمزنگاری، دسترسی محدود، مانیتورینگ و سایر اقدامات امنیتی حساس اتخاذ می‌شوند.

قوانین حقوق تکنولوژی اطلاعات :این قوانین مربوط به مسائل حقوقی در حوزه فناوری اطلاعات و ارتباطات هستند که شامل: قوانینی درباره حقوق مالکیت فکری، نشر، دسترسی به اطلاعات، قوانین تجارت الکترونیک و... است.

قوانین و جرایم سایبری علیه امنیت ملی و اجتماعی تا حدودی بین کشورها متفاوت است و برخی از سازمان‌ها و شرکت‌ها نیز قوانین داخلی خود را برای حفاظت از امنیت سایبری اجرا می‌کنند .

شرکت‌های فعال سایبری سکوریتی (cyber security) در دنیا

امروزه تعداد زیادی شرکت فعال در زمینه حفاظت از امنیت سایبری و مبارزه با تهدیدات امنیتی وجود دارند که هر یک در حوزه‌ها و گرایش‌های خاصی از امنیت سایبری فعالیت می‌کنند و دارای سیستمی مجهز و هوشمند با قابلیت شناسایی تهدیدات بالقوه و مدیریت ریسک سایبری هستند.

برخی از این شرکت‌ها به تنهایی یا به صورت همکاری با دیگر شرکت‌ها، خدمات امنیتی ارائه می‌دهند؛ آن‌ها همچنین اقداماتی مانند: ردیابی تهدیدات سایبری، آزمون نفوذ، آموزش امنیتی و... را ارائه داده و بهبود امنیت سایبری را مدنظر خود قرار می‌دهند که در ادامه به معرفی چند مورد از بهترین‌های این صنعت می‌پردازیم.

شرکت سیمنتیک(Symantec Corporation)

یکی از شرکت‌های برتر و معروف در زمینه سایبر سکوریتی است؛ که به ارائه راهکارهای حفاظت از امنیت سایبری برای شرکت‌ها و مشتریان فردی می‌پردازند.

شرکت مک آفی(McAfee Inc)

مک آفی از شرکت‌های پیشرو در زمینه سایبر سکوریتی که راهکارهای مختلف امنیتی، ازجمله ضدویروس، فایروال و محصولات حفاظت از امنیت ابری را پوشش می‌دهد.

شرکت ترند میکرو(Trend Micro)

ترند میکرو بزرگترین شرکت امنیت سایبری در ژاپن و یکی از پیشروان جهانی در حوزه امنیت سایبری است و نرم‌افزارهای آنتی‌ویروس، آنتی‌اسپایوآر، جلوگیری از نفوذ، مدیریت آسیب‌پذیری‌ها و... در زمینه مبارزه با تهدیدات سایبری ارائه می‌کند.

شرکت سیسکو سیستم(Cisco Systems, Inc)

از بزرگترین شرکت‌های فناوری اطلاعات و شبکه‌های کامپیوتری جهان است که در حوزه تجهیزات شبکه نظیر امنیت سایبری، ابر، اینترنت اشیا، تجارت الکترونیک و... فعالیت دارد و موارد زیر نیز از بهترین مراکز فعال در زمینه امنیت سایبری محسوب می‌شوند.

- کروم(CrowdStrike)
- سایمانتک(Symantec)
- پالوآلتو(Palo Alto Networks)
- فورتینت(Fortinet)
- چک پوینت(Checkpoint)
- تنابل(Tenable)
- کاربون بلک(Carbon Black)
- رپید۷(Rapid7)
- جونیپر نتورکس(Juniper Networks)

مهارت هایی که یک متخصص امنیت سایبری باید بداند

تنوع شاخه‌ها و سطح حرفه‌ای این سیستم به قدری گسترده است که یک متخصص سایبری، جهت فعالیت و کسب مدارج بیشتر در این عرصه به طیف وسیعی از اطلاعات و مهارت در گرایش‌های مختلف نیازمند است؛ لذا فارق از داشتن روحیه کاری، قابلیت تعامل بالا و همکاری تیمی که نوعی مهارت برای کار در امنیت سایبری محسوب می‌شوند؛ کسب دانش و تسلط بر اصول کلی و قوانین جزئی به صورت مهارت‌های زیر نیز لازم است.

- آگاهی از آسیب‌پذیری‌ها و تهدیدات امنیتی مانند: حملات دیده‌بانانه، نفوذ به شبکه، نفوذ به برنامه و آسیب‌های مربوط به نرم‌افزار و سیستم‌عامل‌ها
- تجربه و توانایی انجام آزمون‌های نفوذ و امنیت بر روی سیستم‌ها و شبکه‌ها به منظور شناسایی آسیب‌پذیری‌ها و نقاط ضعف و در نهایت تقویت امنیت آن‌ها.
- درک، تسلط و مهارت در استفاده از راهکارهای امنیتی مانند فایروال، سیستم‌های تشخیص نفوذ (Intrusion Detection System – IDS) و سیستم‌های جلوگیری از نفوذ (Intrusion Prevention System – IPS)
- دانش فنی عمیق و شناخت کامل از عملکرد شبکه‌ها، پروتکل‌های شبکه و فناوری‌های مرتبط با امنیت سایبری مانند: رمزنگاری، امنیت ابری، امنیت موبایل و...
- توانایی برنامه‌نویسی در زبان‌های مختلف مانند Python ،: Javaیا C++ برای تحلیل و بررسی کد، ایجاد ابزارهای امنیتی و انجام آزمون‌های نفوذ

- تحلیل داده‌های امنیتی: توانایی تحلیل داده‌های امنیتی و شناسایی الگوها و رویدادهای مشکوک به منظور تشخیص و جلوگیری از تهدیدات امنیتی.
- توانایی برقراری ارتباط موثر با اعضای تیم و مدیران، توانایی توضیح مفاهیم امنیتی و مهارت نوشتن گزارش‌های فنی و توصیه‌های امنیتی
- توانایی شناسایی و ارزیابی ریسک‌های امنیتی و مدیریت آن‌ها، ارائه راهکارهای امنیتی مناسب و تعیین اولویت‌ها برای مقابله با ریسک‌های مختلف

همچنین جهت فعالیت در این حوزه باید تونایی یادگیری، مهارت کار تیمی، تحقیق و تجربه مداوم، به‌روزرسانی دانش و مهارت خود را ارتقا دهید تا در این حوزه بسیار گسترده است موفق و روبه رشد باشید.

با این وجود ممکن است حقوق امنیت سایبری در ایران یا دیگر کشورها برای شما هم سوال باشد؛ حقوق امنیت سایبری در ایران نظامی بوده و توسط لوایح و قوانین مختلف تنظیم می‌شود؛ لذا قوانین مختلفی که برای حفاظت از اطلاعات و امنیت سایبری وجود دارند سبب نوسانات مبلغ درآمد شغل امنیت سایبری در هر حوزه می‌شوند.

- قانون تامین امنیت و حفاظت از اطلاعات سایبری
- قانون تعارض منافع در فضای سایبری
- قانون مبارزه با جرایم سایبری
- قانون حفاظت از اطلاعات شخصی

این قوانین و مقررات در ایران با هدف حفاظت از امنیت و اطمینان شهروندان در فضای سایبری تنظیم شده‌اند؛ لذا بر حسب مهارت، رتبه شغلی و تسلط فرد در هر یک از این زمینه‌ها حقوق مشخصی تعیین می‌شود.

مسیر یادگیری امنیت سایبری

نوع کار و حساسیت خاص فعالیت در حوزه امنیت سایبری، افرادی را می‌طلبد که استمرار و انگیزه قوی جهت یادگیری در این عرصه گسترده را داشته و با مهارت عملی و دانش تئوری، به تبحر لازم برای حفاظت از حقوق مادی و معنوی کاربران مجازی در سطح فردی، اجتماعی و حتی ملی بپردازند؛ بنابراین جهت یادگیری امنیت سایبری می‌تواند از طریق مراحل زیر مسیر آموزشی تکنیکی و اصولی را طی کنید.

اکتساب مفاهیم و اصول امنیت سایبری :در این مرحله باید با مفاهیم و اصول اساسی آموزش امنیت سایبری آشنا شوید مانند: تهدیدات سایبری، نقاط ضعف امنیتی، روش‌های حمله و دفاع، رمزنگاری، حفاظت از اطلاعات شخصی و موارد مشابه.

مطالعه منابع آموزشی :برای یادگیری دقیق و کامل تر، می‌توانید به منابع آموزشی معتبر و انواع کتاب امنیت سایبری مرجع در زمینه حافظ اطلاعات مراجعه کنید؛ کتاب‌هایی مانند: یافتن و بهره برداری از نقص های امنیتی، هک: هنر بهره برداری، امنیت شبکه: ارتباطات خصوصی در دنیای عمومی، کریپتوگرافی کاربردی: پروتکل‌ها، الگوریتم‌ها و کد منبع به زبان C و...

شرکت در دوره های امنیت سایبری :برخی دوره‌ها و کارگاه‌های آموزشی امنیت سایبری راهی عالی برای یادگیری عملی و تجربه عملی از موارد امنیتی هستند. در این دوره‌ها، می‌توانید با ابزارها و تکنیک‌های امنیتی واقعی آشنا شوید و با تمرین‌هایی از پیش طراحی شده راهکارهای امنیتی را به کار بگیرید.

انجام آزمون‌ها و گواهینامه‌ها :انجام آزمون‌ها و دریافت گواهینامه‌های مرتبط با امنیت سایبری مهارت‌ها و استعداد شما را توسعه می‌دهند؛ لذا می‌توانید در آزمون‌هایی چون CompTIA Security+، Certified Ethical Hacker (CEH)، Certified Information Systems Security Professional (CISSP)و موارد مشابه شرکت کنید.

تمرین عملی و تست امنیتی :برای بالا بردن مهارت‌های خود، می‌توانید تمرین‌های عملی و تست‌های امنیتی مرتبط را انجام دهید؛ این تمرین‌ها شامل ساخت و تست پویای سایت‌ها، مسابقه‌های Capture The Flag (CTF) و تمرین سازمان‌های امنیتی معتبر می‌شوند.

فیلم‌های آموزشی امنیت سایبری :در این حوزه نیز اثار ارزشمندی برای آشنایی و آموزش در قالب فیلم‌های با سبک امنیت سایبری وجود دارند که فهم و کسب این اطلاعات را ساده‌تر می‌کنند مانند: مجموعه ضروری دانش (۲۰۱۷)، گواهی مدیریت امنیت اطلاعات (CISM2019) و...

رشته و گرایش های امنیت سایبری کدام اند؟

اگرچه صنعت امنیت سایبری بسیار وسیع است؛ اما افراد کمی در خصوص رشته‌ها و چگونگی کسب مدارج تحصیلی در این زمینه اطلاعات کافی را دارند و به نوعی در لیست شاخه‌های تحصیلی غیرعمومی قرار دارند؛ با این وجود بسیاری از افراد مایلند بدانند که امنیت سایبری چیست؟ و انواع گرایش امنیت سایبری کدامند؟ که در ادامه قصد داریم به این سوالات پرداخته و با کسب مدرک امنیت سایبری آشنا شویم.

- **امنیت شبکه :**در این گرایش روی امنیت شبکه‌های کامپیوتری، تجهیزات شبکه و پروتکل‌های مرتبط با آنها تمرکز می‌شود.
- **امنیت برنامه‌ها :**در این گرایش به امنیت نرم‌افزارها، برنامه‌های کاربردی، وبسایت‌ها و شناسایی و رفع آسیب‌پذیری‌ها و نقاط ضعف در برنامه‌ها پرداخته می‌شود.
- **امنیت سیستم عامل :**در این رشته امنیت سیستم‌عامل‌های مختلف مانند ویندوز، لینوکس و مکینتاش قرار دارد و بر تنظیمات امنیتی و مقابله با تهدیدات مرتبط با سیستم عامل‌ها تمرکز می‌کنند.
- **امنیت ابری :**با روند افزایش استفاده از سرویس‌های ابری مانند: آمازون وب سرویس و مایکروسافت آزور، امنیت ابری نیز بسیار حائز اهمیت شده است .

- **امنیت شبکه‌های بی‌سیم :**شبکه‌هایی مانند: وای فای امنیت خود را از این رشته می‌گیرند و متخصصان به شناسایی و مقابله با تهدیدات امنیتی و مقابله با نفوذ به شبکه‌های بی‌سیم می‌پردازند.
- **تحلیل امنیتی :**متخصصان این گرایش بر روی تحلیل تهدیدات، جمع‌آوری و تحلیل داده‌های امنیتی و تشخیص نقاط ضعف و آسیب‌پذیری‌ها تسلط دارند.
- **رشته امنیت فضای سایبری :**این شاخه مباحثی مانند: هوش مصنوعی، رمزنگاری، حفاظت از پایگاه‌های داده، تحلیل رفتاری، امنیت شبکه، مدیریت ریسک سایبری و قوانین و مقررات مرتبط را آموزش می‌دهد.

امنیت رویدادها، حفاظت از اطلاعات و امنیت اینترنت اشیا موارد دیگری از گرایش‌های حوزه پویا و پیچیده سایبری سکوریتی هستند و این رشته‌ها و گرایش‌ها ممکن است در دانشگاه‌ها و موسسات آموزشی مختلف با نام‌ها و جزئیات متفاوتی معرفی شوند.

در حال حاضر، رشته امنیت فضای سایبری در دبیرستان به عنوان یک رشته تحصیلی مجزا وجود ندارد؛ اما برخی از دبیرستان‌ها و مدارس فنی و حرفه‌ای دروس مرتبط با امنیت فضای سایبری را در برنامه‌های آموزشی خود قرار می‌دهند؛ همچنین دروس مرتبط با علوم کامپیوتر، شبکه‌ها، امنیت اطلاعات و فناوری اطلاعات را در قالب رشته‌هایی مانند: علوم رایانه و فناوری اطلاعات و ارتباطات ارائه می‌شوند.

اما برنامه‌های تحصیلی در رشته امنیت فضای سایبری در دانشگاه شامل: دروس تکنولوژی‌های امنیتی، مبانی کریپتوگرافی، تحلیل رفتاری، مدیریت ریسک سایبری، کاربرد ابزارهای امنیتی، امنیت شبکه، استراتژی‌های دفاعی و حملات سایبری می‌پردازند. همچنین، برنامه‌های آموزشی می‌توانند بر اساس مقررات و استانداردهای بین‌المللی مؤسسات امنیتی و صنعتی در این زمینه تدوین شده باشند.

علاوه‌بر دروس تئوری، رشته امنیت فضای سایبری در دانشگاه از جنبه‌های کاربردی و عملی نیز پشتیبانی می‌کند و این برنامه‌ها شامل: آزمایشگاه‌های عملی، پروژه‌های تکمیلی، کارگاه‌ها و آموزش‌های عملی در زمینه امنیت سایبری و همچنین ارائه فرصت‌های کارآموزی در صنعت امنیت سایبری را فراهم می‌کند.

امنیت سایبری در ایران و دیگر کشورها چگونه است؟

وضعیت امنیت سایبری در هر کشور به عوامل مختلفی ازجمله: سیاست‌ها و قوانین مربوط به امنیت سایبری، توانمندی‌های فنی، آموزش و آگاهی کاربران، نوع تهدیدات و حملات سایبری و... بستگی دارد؛ لذا هر دولتی برحسب استراتژی‌های امنیتی مختص به خود، پروتکل‌های ویژه‌ای را جهت مقابله با حملات سایبری در پیش می‌گیرد.

امنیت سایبری ایران :امنیت سایبری در ایران به عنوان یکی از اولویت‌های بالای دولت در نظر گرفته شده و دولت سیاست‌ها و قوانین مربوط به امنیت سایبری کشور را تدوین و اجرا می‌کند؛

همچنین سازمان‌های مختلفی مانند: سازمان تنظیم مقررات و ارتباطات رادیویی، سازمان اطلاعات و مدارک کشور و نیروی انتظامی در این زمینه فعالیت می‌کنند.

امنیت سایبری ایالات‌متحده آمریکا :ایالات متحده دارای یکی از پیشرفته‌ترین ساختارهای امنیت سایبری در جهان است؛ امنیت سایبری در امریکا متشکل از تیم‌های امنیتی و سازمان‌هایی مانند: سازمان امنیت ملی (NSA) و سازمان امنیت سایبری و زیرساخت‌های بحرانی (CISA)را برای مقابله با تهدیدات سایبری تشکیل داده است.

امنیت سایبری اسرائیل :سطح امنیت سایبری اسرائیل نسبتا قوی و پیشرفته است و سیستم‌ها و تجهیزات پیشرفته‌ای را برای مبارزه با تهدیدات سایبری توسعه داده؛ همچنین به دلیل موقعیت جغرافیایی این کشور و نیاز اسرائیل به حفاظت از امنیت ملی خود در برابر تهدیدات سایبری، این کشور یکی از رهبران جهانی در زمینه امنیت سایبری به شمار می‌رود.

امنیت سایبری انگلیس :وضعیت امنیت سایبری انگلیس نیز تا حد زیادی پیشرفت کرده و دولت بریتانیا سیاست‌ها و قوانین مشخصی را برای مقابله با تهدیدات سایبری تدوین نموده؛ همچنین قطب‌های امنیت سایبری در انگلستان مسئولیت برنامه‌ریزی، هماهنگی و پاسخگویی در مورد تهدیدات سایبری را بر عهده دارند.

معرفی سایت هایی که در ایران خدمات سایبری ارائه می‌دهند

سطح مطلوب امنیت سایبری در کشور، بخاطر تدابیر و زیرساخت‌های امنیتی ویژه‌ای است که توسط سایت‌ها و مراکز امنیتی رسمی، طراحی و اجرا می‌شوند؛ لذا با وجود تعداد زیادی سازمان و شرکت فعال در حوزه امنیت سایبری، برنامه‌ریزی و تحقق تمامی پلان‌های امنیتی به خوبی پیش رفته و خدمات مختلفی جهت حفظ امنیت مالی، جانی و حیثیتی کاربران و سازمان‌ها توسط سایت‌های معتبر و مجربی اجرا می‌شود.

سایبری پلیس امنیت

این سایت به عنوان یک کانال رسمی پلیس امنیت فعالیت می‌کند و اطلاعات مربوط به نحوه حفظ امنیت، اخبار و رویدادهای مربوط به این حوزه را منتشر می‌کند.

پلیس امنیت سایبریت

پلیس امنیت سایبریت عموما به عنوان نهاد مسئول بررسی و پیگیری جرایم مرتبط با فضای مجازی و امنیت سایبری در یک کشور عمل می‌کند؛ واحدهای پلیس امنیت سایبری معمولا تحت عنوان (سازمان امنیت سایبری یا واحد پلیس سایبری) فعالیت می‌کنند.

امنیت سایبری مرکزی

این سازمان مرکزی متخصص خدمات و محافظت در برابر تهدیدات امنیتی، حفاظت از تأمین تکنولوژی و فناوری اطلاعات (IT) است؛ لذا به طور عمومی و در سطح بین‌المللی فعالیت داشته و با هدف تعیین استانداردها، تدابیر امنیتی، آموزش‌ها، خدمات حفاظت و... در فضای سایبری عمل می‌کند.

پلیس فتا

پلیس فتا بخشی از پلیس امنیت سایبری است که مسئول بررسی و پیگیری جرایم سایبری و جنایات مرتبط با فضای مجازی بوده و منظور خود را از طریق وب‌سایت رسمی و سایر منابع مربوطه منتشر می‌کند.

گروه امنیت سایبری گرداب

یک شرکت که به عنوان یک شرکت امنیتی، در حوزه آسیب‌شناسی، پویایی‌سنجی امنیتی، پنتست، طراحی و پیاده‌سازی سیستم‌های امنیتی، مانیتورینگ و جوابگویی به حملات، مدیریت ریسک، آموزش سایبری و... فعالیت می‌کند؛ لذا تیم امنیت سایبری گرداب با استفاده از تکنولوژی‌ها و روش‌های پیشرفته سعی می‌کند تا مشتریان خود را در برابر حملاتی مانند: هک، نفوذ، جاسوسی، نرم‌افزارهای مخرب و حملات دیگر محافظت کند.

خطرناک ترین حملات سایبری که تاکنون در دنیا رخ داده است

در حوزه سایبری، تا به حال حملات زیادی اتفاق افتاده‌اند که بسیار خطرناک و تأثیرگذار بوده‌اند؛ اما تعیین خطرات امنیت سایبری می‌تواند مسئله‌ای نسبی باشد و به عوامل مختلفی مانند: تاثیرات آن، مقصد، اندازه و زمان برگزاری حمله بستگی دارد.

حملات رانتوم وان :در سال ۲۰۱۷ حملات واناکرای (WannaCry) با استفاده از نرم‌افزار رمزنگاری کننده ویروسی، به سرعت در سراسر جهان گسترش یافت؛ که این حملات بر روی سیستم‌های عامل ویندوز تاثیر گذاشت و هزاران سازمان در بیش از ۱۵۰ کشور را تحت تایر قرار داد.

حملات پتیا :حملات (Petya) نیز در سال ۲۰۱۷ که این حملات با استفاده از ضعف‌های امنیتی در سیستم‌عامل ویندوز کامپیوترها را رمزنگاری کرده و از کار انداختند؛ این حملات نیز در سرتاسر جهان تاثیر گذاشتند و بسیاری از سازمان‌ها را به مشکلات امنیتی بزرگی روبرو ساختند.

حملات :DdoS این حمله به عنوان یکی از خطرناک‌ترین حملات سایبری شناخته می‌شود و این نوع تهاجمات در زمان‌های معینی و با استفاده از نقاط ضعفی سیستم‌ها انجام می شود؛ سیستم هایی که می توانند به صورت تهاجمی عمل کنند از طریق شبکه های کامپیوتری به یکدیگر متصل شده اند و هر کدام از این سیستم ها می توانند اطلاعاتی را از یکدیگر بدزدند و یا باعث خرابی و اختلال در عملکرد آن ها شوند.

لیست حملات سایبری به ایران نیز شامل موارد زیر است .

–هک و غیرفعال کردن خبرگزاری فارس، ایمیل مدیران و کارکنان شبکه پرس تی وی، ایمیل مدیر و کارمندان سازمان انرژی اتمی ایران توسط گروه هکری بلک ریوارد

–هک سازمان فرهنگ و ارتباطات اسلامی و هک وزارت جهاد کشاورزی توسط گروه قیام تا سرنگونی

–هک شرکت فولاد مبارکه خوزستان توسط گروه گنجشک درنده

–هک ۵ هزار دوربین کنترلی و ۱۵۰ سایت و سامانه برای شهرداری تهران

–هک زندان قزلحصار، تلوبیون، صدا و سیما، وزارت فرهنگ و ارشاد توسط سازمان مجاهدین خلق ایران

خدمات امنیت سایبری و کاربرد آن در صنایع مختلف

خدمات امنیت سایبری شامل مجموعه‌ای از روش‌ها، فناوری‌ها و فرآیندهایی است که طراحی و پیاده‌سازی می‌شوند تا سازمان‌ها و افراد را در مقابل تهدیدات سایبری محافظت کنند؛ این خدمات در صنایع مختلف و در سطوح مختلفی از سازمان‌ها کاربرد دارند که در زیر به برخی از کاربردهای خدمات امنیت سایبری در صنایع مختلف اشاره می‌کنم:

امنیت سایبر بانک صنعت بانکداری و مالی در گروه امنیت سایبری زیرساختهای حیاتی قرار دارد و خدمات امنیت سایبری آن شامل: مانیتورینگ و تحلیل ترافیک شبکه، رمزنگاری اطلاعات حساس، حفاظت از شبکه‌های پرداخت الکترونیکی و مبارزه با کلاهبرداری اینترنتی است.

امنیت سایبری بیمارستان :در بخش بهداشت و درمان، امنیت سایبری برای حفاظت از داده‌های پزشکی حساس، سیستم‌های پزشکی، تجهیزات پزشکی هوشمند و حفظ حریم خصوصی بیمارستان و بیماران اهمیت دارد و شامل: مانیتورینگ و حفاظت از سیستم‌های پزشکی، رمزنگاری اطلاعات پزشکی و امنیت شبکه‌های بیمارستانی است.

امنیت سایبری خودرو :در صنعت خودرو، امنیت سایبری درباره خودروهای هوشمند و متصل به اینترنت اهمیت زیادی دارد؛ لذا خدمات امنیت سایبری این صنعت شامل: حفاظت از سیستم‌های رانندگی خودکار، جلوگیری از حملات به دوربین‌های خودرو، سیستم‌های ناوبری و حفاظت از اطلاعات شخصی رانندگان است.

امنیت سایبری اتوماسیون صنعتی :در این صنعت، امنیت سایبری برای حفاظت از شبکه‌های صنعتی، سیستم‌های کنترلی و داده‌های حساس نقش دارد؛ مانیتورینگ و دفاع در برابر تهدیدات سایبری، آزمون نفوذ در سیستم‌ها، مدیریت ریسک سایبری و... برخی از فرآیندهای امنیتی این عرصه هستند.

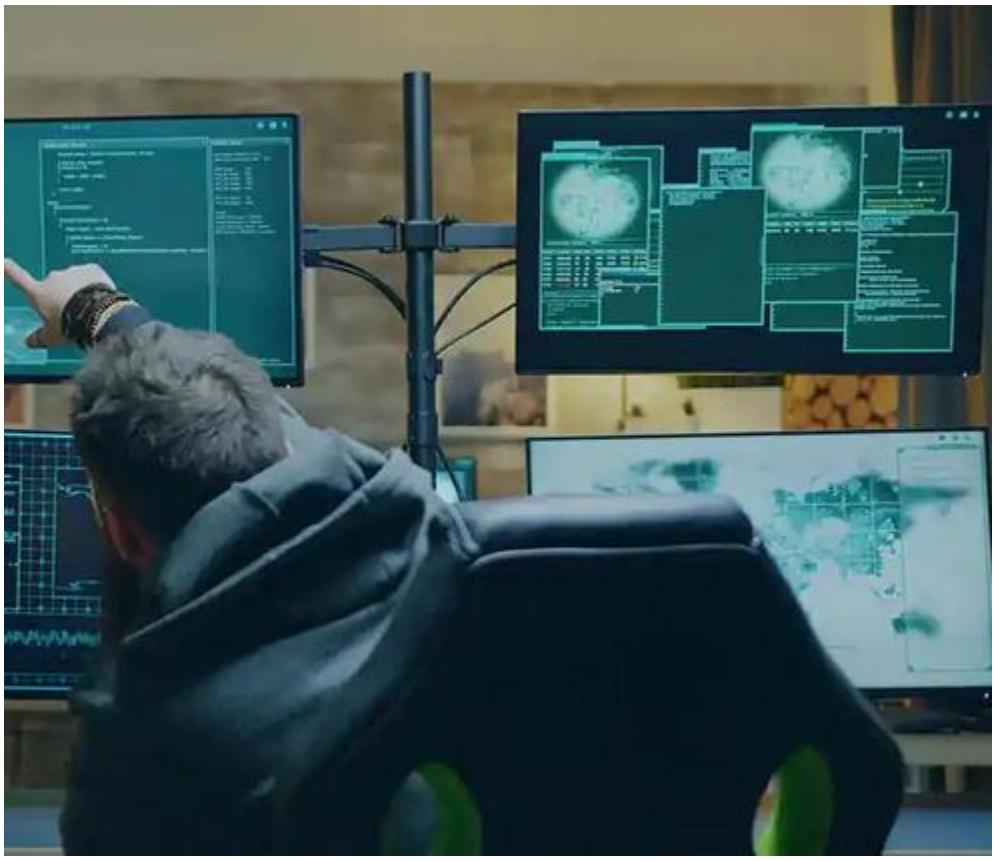
امنیت سایبری سپاه :وظایف سپاه در حوزه امنیت سایبری شامل آموزش پرسنل در زمینه امنیت سایبری، پایش و تشخیص حملات سایبری در شبکه‌های داخلی و خارجی، تحقیق و توسعه فناوری‌های امنیتی، تدوین و اجرای استانداردهای امنیت سایبری و همکاری با سازمان‌ها و نهادهای دیگر در حوزه امنیت سایبری است.

امنیت سایبری پدافند غیرعامل :مجموعه اقداماتی که به منظور حفاظت از منابع و ثروت‌های ملی در برابر حملات سایبری انجام می‌شود و شامل: بررسی، تحلیل، پیش‌بینی و سازوکارهایی است که طراحی شده‌اند تا سیستم‌ها، شبکه‌ها، داده‌ها و اطلاعات مربوط به یک نهاد، سازمان یا کشور را در برابر حملات سایبری محافظت کنند.

امنیت سایبری پهباد :امنیت سایبری پهباد شامل حفاظت از سیستم‌های کنترلی پهبادها، فرآیندها و ارتباطات آنها در برابر حملات سایبری است. این امنیت توسط تحلیل و ارزیابی ریسک امنیتی، شناسایی آسیب‌پذیری‌ها، پیشگیری از دسترسی غیرمجاز، مانیتورینگ ترافیک شبکه و... انجام می‌شود.

امنیت سایبری کودکان :آموزش و آگاه سازی کودکان در مورد مفهوم تهدیدات سایبری و راه‌های مدیریت و پیشگیری از آن‌ها شامل: آموزش اصول اساسی، نظارت و خرده‌گردانی، حفظ حریم خصوصی، بلایای آنلاین، استفاده مسئولانه از فناوری‌های ارتباط است.

این موارد تنها چند زمینه از خدمات امنیت سایبری در صنایع مختلف هستند؛ لذا امروزه با توجه به رشد روزافزون تهدیدات سایبری، نیاز به امنیت سایبری در تمامی صنایع و بخش‌ها اهمیت بیشتری پیدا کرده است؛



معرفی چند کتاب در زمینه امنیت سایبری

خوشبختانه همگام با پیشرفت علمی، دستاوردهای عملی و افزایش منابع آموزشی معتبر در این حوزه، کتب برجسته و غنی نیز ارائه می‌شوند و منابع مطالعه و آموزش سایبری را گسترده و جامع‌تر می‌سازند.

کتاب قوانین سایبری :این منبع غنی و برجسته به نویسندگی (حامد حاجی ملامیرزایی) به اهمیت ویژه صیانت از امنیت فردی و ملی در فضای نوپای سایبری سکوریتی پرداخته و شرایط سایبری ایران را با دیگر کشورها مطرح دنیا مقایسه می‌کند؛ همچین جوانب مختلف، چالش‌ها، نقاط قوت و ضعف‌های حقوقی و مدیریت امنیت سایبری کشور را نیز بررسی و تحلیل می‌کند.

کتاب هنر فریب :The Art of Deception نوشته کوین میتنیک و ویلیام سایمون است که به طور جذاب و قابل فهم، شیوه‌های متداول حملات سایبری و روش‌هایی که هکرها برای دریافت اطلاعات حساس استفاده می‌کنند را شرح می‌دهد؛ ازجمله مباحثی که در این کتاب مورد بررسی قرار می‌گیرند شامل: فرهنگ و روش‌های نفوذ، حملات فیزیکی و اجتماعی، فریب در حملات الکترونیکی و شبکه، تفهیم ضعف‌های مربوط به هویت و تأیید هویت است.

کتاب هنر نفوذ، هنر استفاده زورگویانه :Hacking The Art of Exploitation نوشته جان اریکسون، این کتاب به شما کمک می‌کند تا به شیوه‌ها و ابزارهایی که هکرها برای نفوذ به سیستم‌ها استفاده می‌کنند نگاهی دقیق داشته و به مباحثی مانند: نحوه عملکرد سیستم‌ها، بررسی استفاده از ابزارها، تکنیک‌هایی همچون buffer overflow وshellcode ، هک کردن سیستم‌ها با استفاده از تکنولوژی شبکه‌ها، وب، برنامه‌نویسی و... می‌پردازد.

کتاب راهنمای هکرهای برنامه‌های وب :The Web Application Hacker's Handbook نوشته دافید اشتوتارد و مارکوس پینتو: این کتاب به شما در مورد نحوه شناسایی آسیب‌پذیری‌ها و حملات رایج در برنامه‌های وب کمک می‌کند؛ لذا به تشریح الگوها و ضعف‌های امنیتی رایج در برنامه‌های وب مانند: حملات تزریق (Injection attacks)، حملات همسان سازی (Session hijacking)، حملات استفاده از اعتماد نادرست (Insecure Direct Object Reference) و راهکارهایی برای جلوگیری از آن‌ها پرداخته‌اند.

کتاب امنیت سایبری، راهنمای مبتدیان :Cybersecurity The Beginner's Guide نوشته اردال اوزکایا، این کتاب مخصوص مبتدیان است و مباحث اساسی و ابتدایی امنیت سایبری را به شما آموزش می‌دهد؛ که چگونه به صورت موثری از کلیه جنبه‌های امنیت سایبری مانند: حفاظت از داده‌ها، رمزنگاری، شبکه‌های بی‌سیم، هکرها و تهدیدات امنیتی، حملات DDoS و سایر مسائل امنیتی در دنیای دیجیتال مراقبت کنید.

جمع بندی چیستی امنیت سایبری

امنیت سایبری یک موضوع بسیار حیاتی و با اهمیت است که در دنیای امروزه مورد توجه ویژه‌ای قرار گرفته و با پیشرفت فناوری و ارتباطات، حملات سایبری نیز به شدت افزایش یافته که گاها عواقب جدی برای افراد و سازمان‌ها در پی دارند؛ لذا برای دستیابی به امنیت سایبری، باید به مسائل مربوط به امنیت داده‌ها، شبکه‌ها، نرم‌افزارها و... توجه نمود؛ محافظت از منابع محرمانه و مهم در برابر دسترسی غیرمجاز و هکرها، استفاده از رمزنگاری قوی، بروزرسانی سیستم‌های امنیتی، آموزش کارکنان در حوزه امنیت سایبری و... مواردی از اقداماتی حفاظتی جهت پیشگیری و مقابله با حملات سایبری هستند.

به طور کلی امنیت سایبری نیازمند روش‌ها و رویکردهای گوناگون و متعددی است که بسته به نوع سازمان، محیط کاری و نیازهای فردی متفاوت بوده و بهره‌برداری از روش‌های امنیتی مناسب،

آگاهی و آموزش کافی، همکاری با متخصصان و استفاده از ابزارهای مدرن می‌تواند به حفاظت در برابر تهدیدات سایبری و ایمنی اطلاعات کمک کند.

امنیت سایبری

امنیت سایبری در بیان ساده حفاظت از داده ها، سیستم‌ها، شبکه‌ها، برنامه‌ها و به طور کلی هر آنچه که در فضای دیجیتال دارایی ارزشمندی محسوب می‌شود، در برابر تهدیدات سایبری است. این حفاظت به بررسی **تهدیدات سایبری** و راه‌های مقابله با آن‌ها می‌پردازد. در این مقاله قصد داریم مهمترین **مفاهیم امنیت سایبری** را معرفی کنیم.

انواع امنیت سایبری

امنیت سایبری در بخش‌های مختلفی پیگیری می‌شود. در واقع گرچه هدف امنیت سایبری محافظت از دارایی ارزشمند در برابر تهدیدات است اما بسته به نوع دارایی، شکل تهدیدات و دفاع مقابل آن‌ها می‌تواند به طور کامل متفاوت باشد. امنیت سایبری به طور ویژه با عناوین امنیت شبکه، امنیت برنامه، امنیت اینترنت اشیا و امنیت فضای ابری پیگیری می‌شود که در ادامه به معرفی آن‌ها می‌پردازیم.

امنیت شبکه(Network Security)

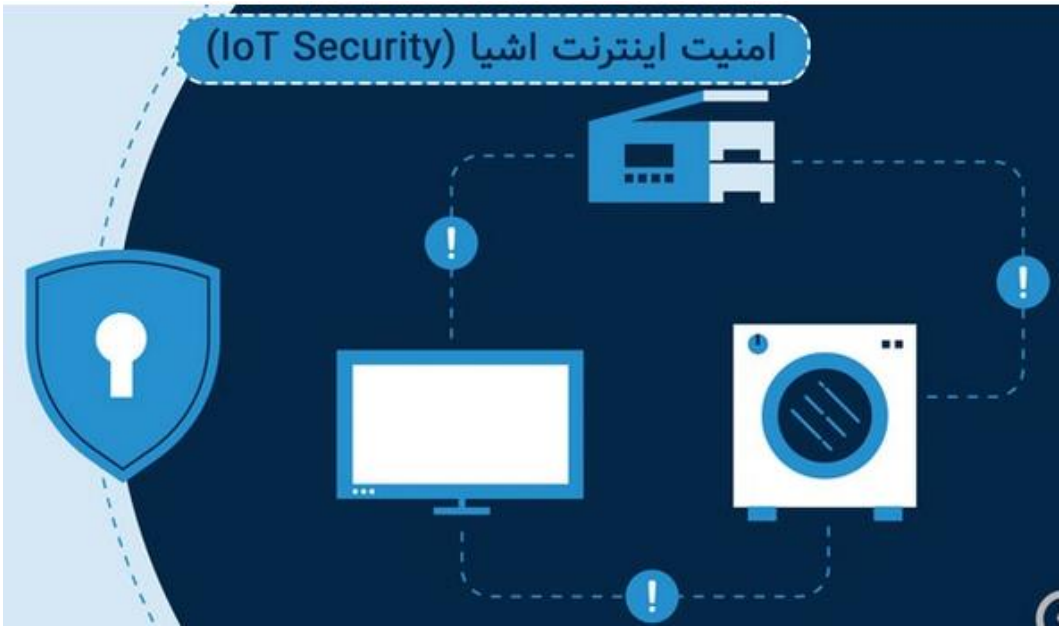
امنیت شبکه، محافظت از مجموعه‌ای از دستگاه‌های متصل به‌هم دربرابر اقدامات غیرمجاز است. این شبکه می‌تواند شامل کامپیوترها، موبایل‌ها، مسیریاب‌ها، دوربین‌های مداربسته و یا هر دستگاه دیگری با قابلیت اتصال به **شبکه** باشد. آلوده‌کردن کامپیوترهای شبکه به یک بدافزار، سواستفاده از آسیب‌پذیری‌های موجود و یا شنود اطلاعات کاربران شبکه از نمونه تهدیدات شبکه هستند.

به‌عنوان مثال، شبکه کامپیوترهای یک سازمان را درنظر بگیرید. در صورت آسیب پذیربودن **سیستم امنیتی** این شبکه، یک کارمند که به یک کامپیوتر درون شبکه دسترسی دارد یا مهاجمی که از طریق اینترنت به یک کامپیوتر داخل شبکه دست پیدا کرده‌است، می‌تواند با استفاده از این آسیب‌پذیری به کامپیوترهای دیگر نفوذ کند. این نفوذ دسترسی مهاجم را گسترش می‌دهد و در ادامه کامپیوترهای دیگر را نیز تحت کنترل مهاجم قرارمی‌دهد. این نفوذ می‌تواند باعث لورفتن اطلاعات حساس یا شخصی، **آسیب‌زدن به داده‌های مهم** و یا هر اقدامی که مهاجم نباید مجاز به انجام آن باشد می‌شود.

امنیت برنامه(Application Security)

این رویکرد از امنیت، با تمرکز بر یک برنامه خاص، نقاط ضعف و **آسیب پذیری‌های امنیتی** یک برنامه را کشف و رفع می‌کند. مهم‌ترین نمونه این نوع امنیت، امنیت برنامه‌های تحت وب یا **امنیت سایت (Web Application Security)** است. با وجود محبوب بودن برنامه‌های تحت وب، امنیت این برنامه‌ها با چالش‌های جدی روبرو است که باید مورد توجه توسعه‌دهندگان باشد.

امنیت اینترنت اشیا(IoT Security)



با فراگیرشدن استفاده از **اینترنت اشیا** به خصوص در موارد صنعتی و خانگی، نوع جدیدی از امنیت تعریف شد که تمرکز آن بر **تأمین امنیت** این گروه از دستگاه‌ها است. اینترنت اشیا به دستگاه‌های خاص‌منظوره اشاره دارد (مانند تنظیم کننده دما) که از طریق اینترنت قابل کنترل هستند. خلل در امنیت این نوع دستگاه‌ها می‌تواند باعث خسارت‌های قابل توجه در روند تولید صنعتی یا ایجاد مشکلات در دستگاه‌های خانگی شود .

امنیت فضای ابری(Cloud Security)

فضای ابری به شما این امکان را می‌دهد که از امکانات سخت‌افزاری و نرم‌افزاری، مانند فضای ذخیره‌سازی و یا برنامه‌ها، از طریق اینترنت بهره‌مند شوید. امنیت فضای ابری به **تامین امنیت داده‌های ذخیره شده** در این فضا و صحت عملکرد سرویس‌های ابری می‌پردازد.

جنگ سایبری

گسترش استفاده از سیستم‌های کامپیوتری با وجود تسهیل بسیاری از امور و ایجاد راه‌حل‌های انقلابی، تهدیدات جدیدی را معرفی کرد. یکی از مهمترین مفاهیمی که در فضای سایبر امروز وجوددارد، مفهوم **جنگ سایبری** است.

در **جنگ سایبری**، دشمن با به‌کارگیری حملات و تهدیدات در فضای سایبر، قصد آسیب‌زدن به کشور و نقض امنیت در ابعاد ملی را دارد. در واقع نتیجه مخرب این حملات بر یک کشور تاثیر می‌گذارد. جنگ سایبری انواع مختلفی دارد که در ادامه آن‌ها را به طور خلاصه بررسی می‌کنیم.

جاسوسی

این نوع از **حملات جنگ سایبری** با هدف دزدیدن و کسب اطلاعات محرمانه ملی طراحی و اجرا می‌شود.

خرابکاری

هدف این مورد ایجاد اشکال و خرابکاری در تاسیسات مهم و حیاتی یک کشور است .نمونه این حملات، کرم استاکس نت (Stuxnet) در سال ۲۰۱۰ است که در تاسیسات هسته‌ای ایران مشکلات جدی ایجاد کرد.

منع سرویس

حملات منع سرویس، با ایجاد ترافیک سنگین سایت‌های مهم و ملی یک کشور را از کار می‌اندازند و دسترسی کاربران عادی به آن را با مشکل مواجه کرده یا قطع می‌کنند.

آسیب به شبکه برق

شبکه برق یکی از نقاط مهم و استراتژیک کشور است که با استفاده از سیستم های کامپیوتری پیاده‌سازی و مدیریت می‌شود. در جنگ سایبری یکی از اهداف می‌تواند ایجاد آسیب و یا از کار انداختن شبکه برق در ابعاد مختلف باشد.

اخبار جعلی

این دسته از حملات فضای سایبر، با هدف تحت تاثیر قرار دادن افکار عمومی، به تولید و نشر اخبار کذب، شایعات و اطلاعات دروغ با هدف ایجاد بی‌اعتمادی در سطح ملی می‌پردازد.

اخلال در سامانه های اقتصادی

امروزه تمامی تراکنشات مالی و پولی از طریق سیستم‌های کامپیوتری و عمدتا اینترنت سازماندهی می‌شود. در **جنگ سایبری** خلل در سامانه اقتصادی می‌تواند دسترسی مردم به حساب‌های بانکی خود را دچار مشکل کند و یا از منابع مالی بانک ها دزدی کند.

مفاهیم امنیت سایبری

تامین امنیت سایبری با توجه به شرایط موجود پیگیری می شود. پیش از وقوع حمله یا نفوذ، لازم است اقدامات پیشگیرانه انجام شود. در حین حمله و پس از آن نیز باید اقدامات تشخیص و ردیابی و در نهایت واکنش مناسب صورت پذیرد. در ادامه این مفاهیم را معرفی می کنیم.

پیشگیری(Prevention)

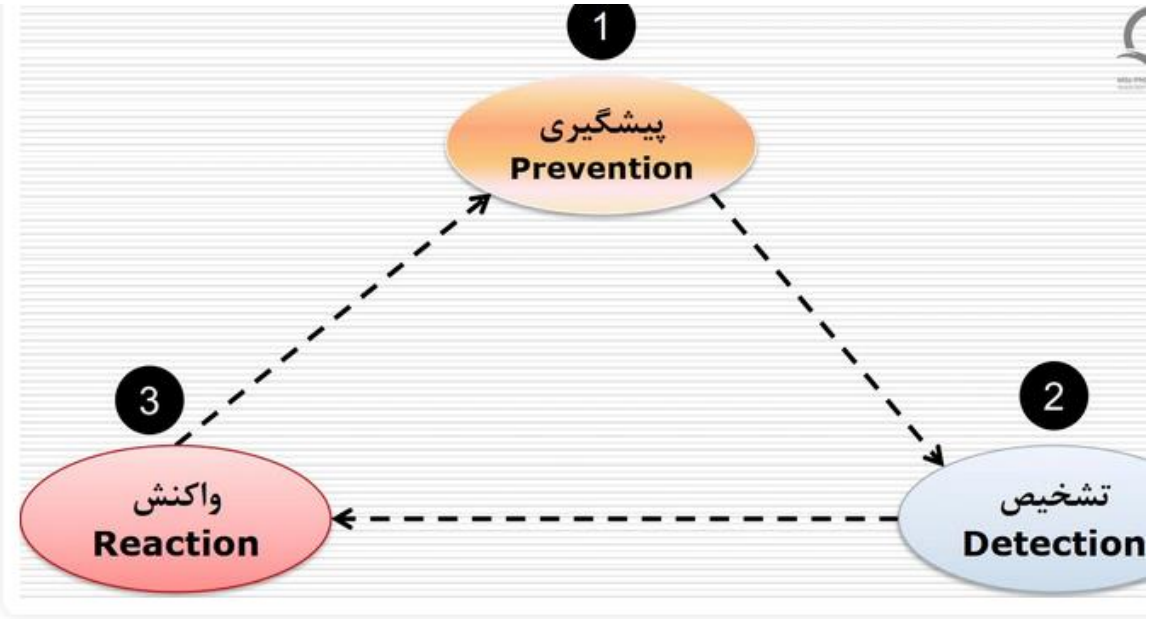
این رویکرد مربوط به زمان طراحی و پیاده‌سازی برنامه و یا شبکه است. پیش‌گیری با اتخاذ **سیاست‌های امنیتی** مناسب و بکارگیری مکانیزم‌های درست، از وقوع حمله و خسارت‌های متعاقب آن جلوگیری می کند.

تشخیص و ردیابی(Detection and Tracing)

تشخیص و ردیابی در زمان وقوع حمله و پس از آن صورت می‌گیرد. در زمان حمله، در صورت تشخیص باید پاسخ مناسب داده شود تا خسارت ناشی از حمله به حداقل برسد، به‌عنوان مثال دسترسی مهاجم قطع یا محدود شود. در موارد دیگر، شناسایی پس از وقوع حمله اتفاق می‌افتد. در این موارد باید زمان و علت حمله (آسیب پذیری‌های موجود)، میزان خسارت و هویت دشمن شناسایی شود.

واکنش(Reaction)

پس از شناسایی علل آسیب‌پذیری، باید در جهت رفع نقاط ضعف اقدام کرد تا از حملات مجدد جلوگیری شود. همچنین با استفاده از نسخه‌های پشتیبان، داده‌های آسیب‌دیده یا از بین رفته را ترمیم کرد و سیستم را به حالت درست قبلی برگرداند و یا نزدیک کرد.



مثلث امنیت سایبری (CIA) چیست؟

مثلث امنیت یا **CIA**به سه اصل برقراری امنیت سایبری اشاره دارد که با نقض هر یک از آنها امنیت نقض می‌شود. در ادامه به بررسی این سه اصل می‌پردازیم.

محرمانگی(Confidentiality)

محرمانگی به معنای عدم افشای اطلاعات محرمانه و خصوصی ذخیره شده و یا درحال انتقال، نزد افراد غیرمجاز است. به‌عنوان مثال، اگر پیام خصوصی شما به شخص A توسط شخص غیرمجاز Bخوانده‌شود نقض محرمانگی و در نتیجه نقض امنیت شده است. یکی از راهکارهای حفظ محرمانگی، رمزنگاری داده‌ها است.

صحت(Integrity)

صحت به معنای عدم دستکاری اطلاعات ذخیره شده و یا درحال انتقال توسط افراد یا برنامه‌های غیرمجاز و اطمینان از منبع ارسال اطلاعات است. به‌عنوان مثال، اگر پیام شما به شخص A در حین انتقال توسط شخص غیرمجاز B تغییر کند نقض صحت و در نتیجه نقض امنیت شده است. مثال دیگر نقض صحت می‌تواند جعل هویت باشد .شخص غیرمجاز B پیامی برای شما ارسال می‌کند و خود را شخص A جا میزند .امضای دیجیتال یکی از راهکارهای تأمین صحت است.

دسترس پذیری(Availability)

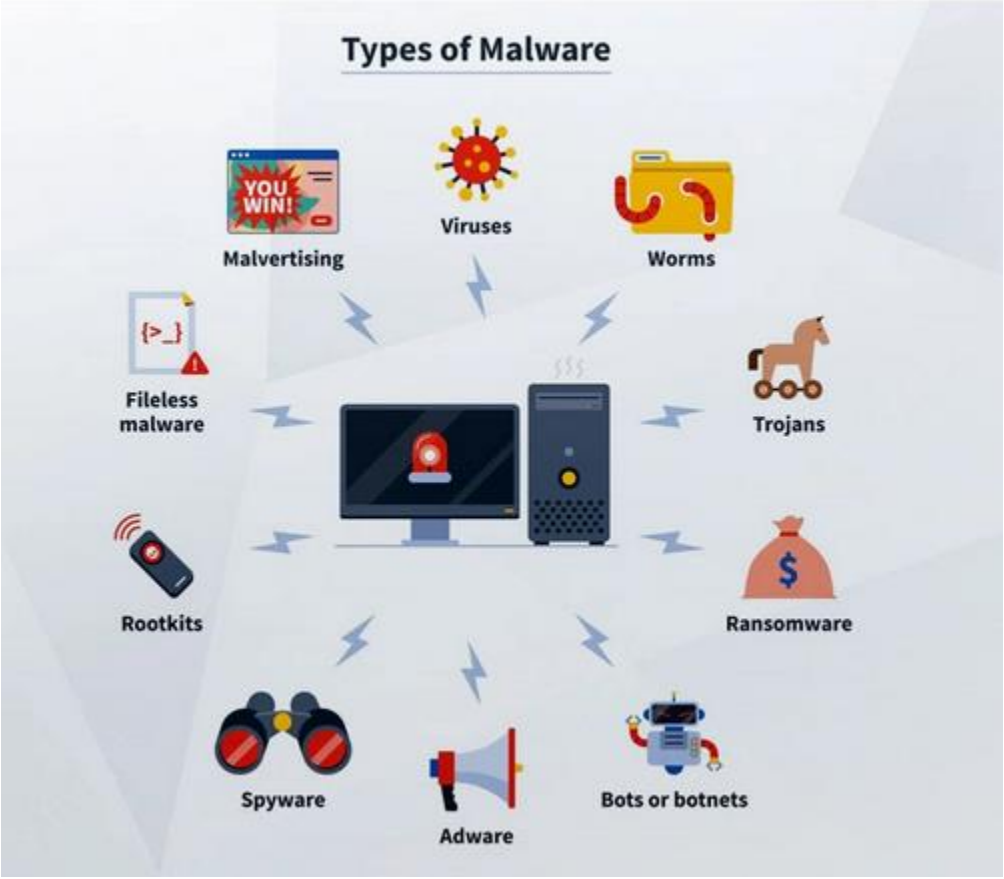
دسترس‌پذیری به معنای در دسترس‌بودن یک سرویس برای کاربران مجاز با کیفیت مورد انتظار است. به‌عنوان مثال اگر به دلیل یک حمله، صفحه وبی که مشاهده می‌کنید با کندی بارگذاری شود نقض دسترس‌پذیری و در نتیجه نقض امنیت اتفاق‌افتاده‌است .وجود پشتیبان از راهکارهای تأمین دسترس‌پذیری است.

حملات سایبری(Cyber Threats)

حملات سایبری انواع مختلفی دارند که در این بخش به برخی از معروف‌ترین آنها می‌پردازیم.

بدافزار(Malware)

بدافزارها به طور کلی به نرم‌افزارهایی اشاره دارد که مهاجم با قصد دزدیدن اطلاعات، کسب دسترسی‌های غیرمجاز و یا آسیب زدن به سیستم قربانی توسعه می‌دهد .معروف‌ترین انواع بدافزارها عبارتند از **باج‌افزارها**، کرم‌ها، **جاسوس‌افزارها** و **تروجان‌ها** که در ادامه بررسی می‌کنیم.



۱. **باج‌افزار : (Ransomware)** همان‌طور که از نام آن پیداست، به قصد باج‌گیری از قربانی ایجاد می‌شوند .به عنوان مثال، مهاجم با رمز کردن اطلاعات یک سیستم، برای رمزگشایی آن از قربانی باج می‌گیرد.

۲. **کرم‌کامپیوتر : (Worm)** کرم‌ها با هدف پخش‌شدن بین کامپیوترهای مختلف توسعه داده می‌شوند. به‌محض ورود کرم به سیستم کامپیوتر، بدون نیاز به دخالت شخص، تکثیر و به کامپیوترهای دیگر ارسال می‌شود. از تاثیرات ورود کرم به سیستم کامپیوتری می‌توان به پرشدن فضای خالی دیسک، کندشدن سیستم و حذف و تخریب فایل‌های میزبان اشاره کرد.

۳. **جاسوس‌افزار : (Spyware)** با هدف کسب اطلاعات محرمانه ساخته می شود. به‌عنوان مثال یک **جاسوس‌افزار** می‌تواند به‌طور مخفیانه در پس‌زمینه اجرا شود و همه کاراکترهای تایپ شده توسط قربانی را ذخیره و به مهاجم ارسال کند.

٤. **تروجان : (Trojan)** در ظاهر یک نرم‌افزار سالم است و یک عملیات مجاز انجام می‌دهد اما در واقع هدف مخربی دارد. به‌عنوان مثال یک نرم‌افزار تقویم که توسط مهاجم نوشته شده باشد می‌تواند در پس‌زمینه به جمع‌آوری و ارسال اطلاعات محرمانه مشغول باشد.

۵. **بات نت : (Botnet)** به شبکه‌ای از سیستم‌های کامپیوتر قربانی‌شده اطلاق می‌گردد که توسط مهاجم کنترل می‌شوند .در واقع مهاجم می‌تواند با صادر کردن یک فرمان همه سیستم‌ها را به عمل مشخصی وادارد. از شایع‌ترین خطرات بات‌نت‌ها شرکت در حملات منع سرویس (DoS) است که در ادامه بررسی می‌شود.

فیشینگ(Phishing)

حملات فیشینگ نوعی از **حملات مهندسی اجتماعی** هستند. مهندس اجتماعی با بررسی رفتار و نحوه فکر عموم افراد جامعه، می‌تواند رفتار آنها را پیش‌بینی کند .**حملات فیشینگ** با استفاده از این روش می‌تواند اطلاعات حساس افراد را سرقت کند. به‌عنوان مثال، زمانی که افراد به صفحه پرداخت راهنمایی می‌شوند، بیشتر به ویژگی‌های ظاهری صفحه دقت می‌کنند و به‌همین دلیل در یک سایت پرداخت تقلبی که شبیه به صفحات پرداخت معتبر است، اطلاعات حساب خود را وارد می‌کنند و مهاجم با این اطلاعات به حساب شخص قربانی دسترسی پیدا می‌کند.

مثال دیگر فیشینگ می‌تواند از طریق ایمیل‌های جعلی باشد. فرض کنید شما ایمیلی از شخص یا سازمان به ظاهر معتبر دریافت می‌کنید که برای یک روال سازمانی معقول از شما درخواست اطلاعات شخصی یا حساس می‌کند. با ارسال این اطلاعات حساس، شما قربانی فیشینگ می‌شوید.

حمله منع سرویس Denial of Service) یا(DoS

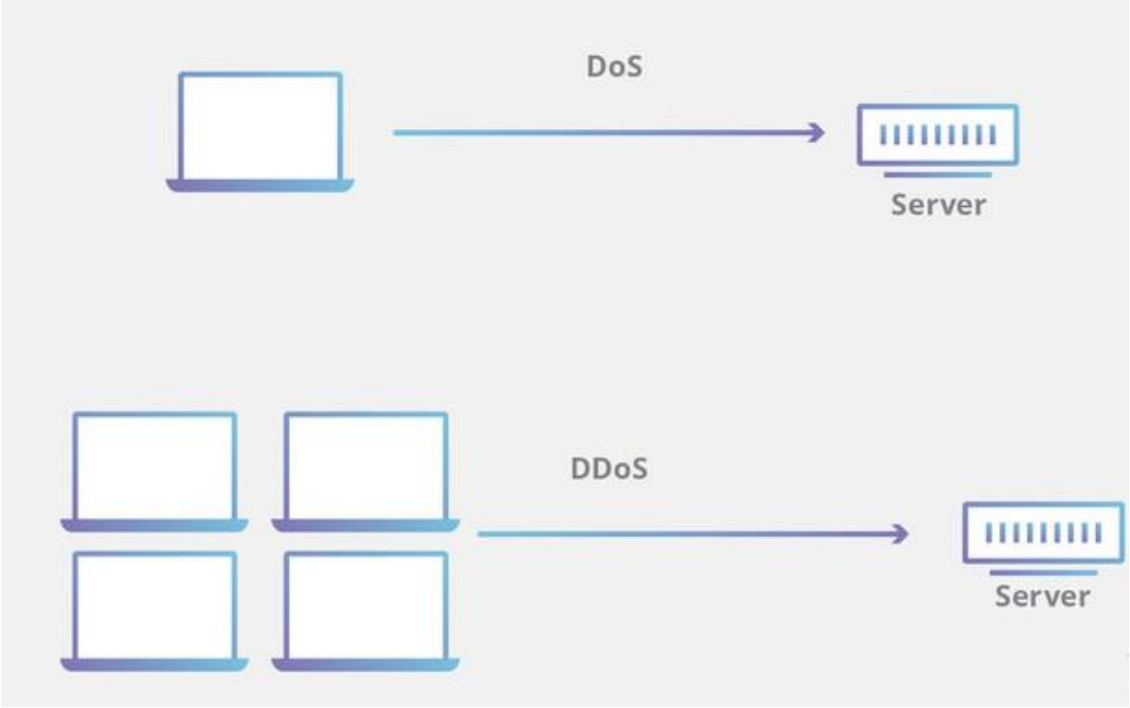
هدف این نوع حمله نقض امنیت از طریق نقض دسترس‌پذیری است. در این حمله دشمن با تعداد زیادی درخواست ترافیک زیادی ایجاد می‌کند و شبکه و یا سرور قربانی را تحت بار زیادی قرار می‌دهد. به این ترتیب، سیستم قربانی امکان ارائه خدمات به کاربران مجاز با کیفیت مورد انتظار را از دست می‌دهد و موجب نارضایتی کاربران می‌شود .

حمله توزیع شده منع سرویس Distributed Denial of Service) یا(DDoS

یک **حمله توزیع شده** که در جهت ایجاد اختلال در ترافیک عادی یک سرور، شبکه یا سرویس که توسط چندین سیستم کامپیوتری با سیل عظیمی از ترافیک ها انجام می‌شود. هنگامی که سرور یا شبکه قربانی مورد هدف قرار می‌گیرد، مهاجم توسط بات نت هایی که ایجاد کرده است به آدرس

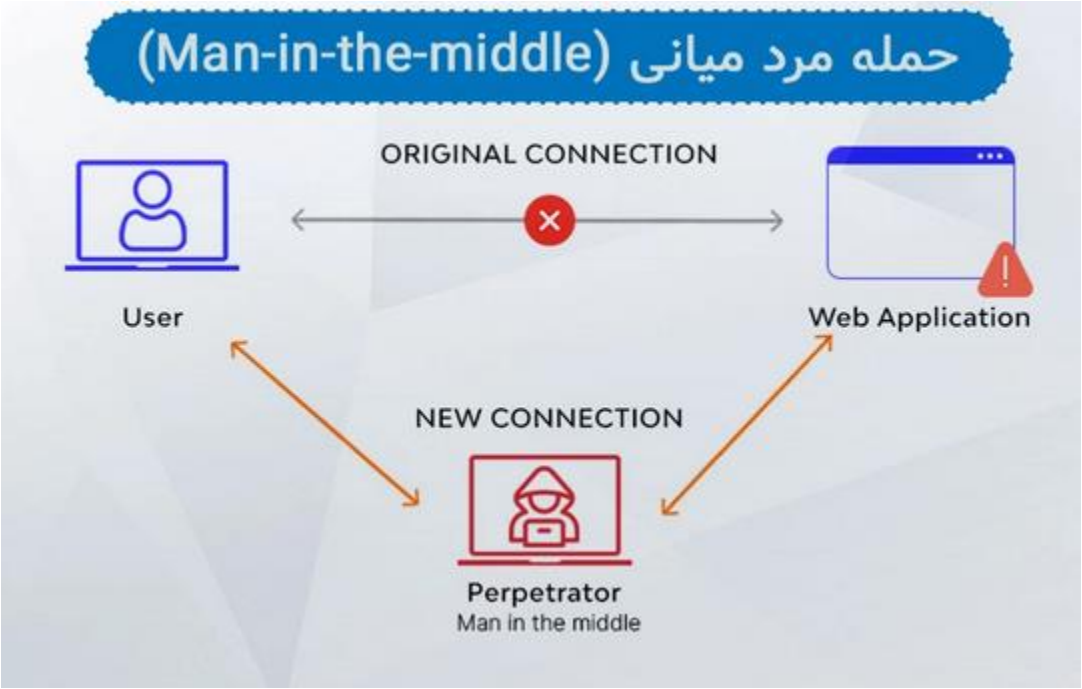
IPهدف درخواست‌هایی را ارسال می‌کند که باعث می‌شود شبکه تحت فشار قرار بگیرد و در نتیجه سرویس یا سرور از ترافیک عادی منع شود.

در تصویر زیر ماهیت **حمله DoS و DDoS** را می‌توانید مشاهده کنید:



حمله مرد میانی(Man-in-the-middle)

در این حمله مهاجم در بین ارتباط A و B قرار می‌گیرد و می‌تواند داده رد و بدل شده میان آن دو را شنود کرده و یا تغییر دهد. به‌عنوان مثال، در حالت عادی درخواست شما برای دیدن یک صفحه وب، به طور مستقیم به وب سرور مقصد می‌رود و پاسخ به طور مستقیم به کامپیوتر شما برمی‌گردد. اما در سناریو حمله، مهاجم درخواست شما را در میانه راه می‌گیرد و خود درخواست مشابهی به سرور ارسال می‌کند. در ادامه نیز پاسخ را از سرور دریافت می‌کند و برای شما ارسال می‌کند. به این صورت امکان شنود و تغییر درخواست‌های شما و سرور را خواهد داشت.



شغل های امنیت سایبری

با توجه به رشد چشم‌گیر **تهدیدات امنیتی** در سال‌های اخیر، در حوزه امنیت سایبری نیاز جدی به افراد متخصص برای جلوگیری و رفع این مخاطرات وجود دارد. در این بخش برخی از موقعیت‌های شغلی پرخواهان این حوزه را بررسی می کنیم.

کارشناس تست نفوذ(Penetration Tester)

وظیفه یک کارشناس تست نفوذ یا هکر اخلاقی، شبیه‌سازی یک مهاجم و تلاش برای نفوذ به **سیستم‌های تحت تست** است. با این شبیه‌سازی نقاط ضعف و آسیب‌پذیری‌های سیستم‌ها و شبکه مورد بررسی کشف و گزارش می‌شود.

مهندس امنیت(Security Engineer)

مهندس امنیت وظیفه طراحی امن مجموعه سیستم‌ها بر عهده دارد. به گونه‌ای که شبکه، سیستم های کامپیوتری و اطلاعات حساس از تهدیدات امنیتی مصون بمانند. این طراحی می‌تواند شامل دیواره‌های آتش (Firewall) و **سیستم‌های تشخیص نفوذ** (Intrusion Detection System)یا (IDS باشد .**مهندس امنیت سیستم‌ها** رو به طور مداوم مورد بازرسی قرار می‌دهد تا در صورت کشف احتمالی نفوذ غیرمجاز و یا آسیب پذیر بودن آن ها راه حل ارائه‌دهد.

تحلیل گر امنیت(Security Analyst)

تحلیل‌گر امنیت وظایف متنوعی دارد. با تسلط نسبت به انواع تهدیدات و راه‌حل‌های موجود، امن بودن سیستم‌ها را دربرابر این تهدیدات بررسی می‌کنند. تحلیل‌گر امنیت بررسی می‌کند که سیاست‌های امنیتی به خوبی پیاده‌سازی شده باشند .همچنین باید توانایی استفاده از ابزارهای مختلف حوزه امنیت سایبر را داشته باشد و سیستم‌ها را با این ابزار مورد وارسی قرار دهد و در صورت مورد حمله قرار گرفتن یک سیستم آن را شناسایی کند.

تحلیل گر بدافزار(Malware Analyst)

در بخش حملات متداول امنیتی به معرفی بدافزارها پرداختیم. یک تحلیل‌گر بدافزار وظیفه شناسایی بدافزارهایی مانند کرم‌ها، جاسوس افزارها، باج افزارها و تروجان‌ها را دارد. این شناسایی با بررسی کد برنامه‌ها و مشاهده رفتار آنها در حال اجرا انجام می‌شود و برنامه‌هایی که رفتار مخرب داشته باشند کشف و حذف می‌شوند.

یادگیری امنیت سایبری

برای **ورود به حوزه امنیت سایبری** و یادگیری آن، بهتر است با موضوعات و مهارت‌های امنیت سایبری آشنا شوید و با توجه به علاقه مسیر یادگیری خود را ترسیم کنید. در این بخش به معرفی این موضوعات می پردازیم.

رمزنگاری

رمزنگاری از جمله موضوعات مفصل امنیت است. هدف از رمزنگاری، محافظت از اطلاعات محرمانه در برابر افراد غیرمجاز است. در واقع با رمزنگاری فقط افرادی که کلید رمز را داشته باشند، امکان رمزگشایی اطلاعات را خواهند داشت.

در مبحث رمزنگاری، سیستم‌های رمزنگاری معرفی می‌شوند، شیوه رمز کردن اطلاعات بررسی می‌شود و راه های شکستن رمز و پی‌بردن به اطلاعات رمزشده آموزش داده می‌شود.

نفوذ به سیستم

یکی از مهمترین مهارت‌های موجود در حوزه **امنیت سایبری**، نفوذ به یک سیستم با استفاده از آسیب‌پذیری‌های نرم‌افزارهای در حال اجرای آن سیستم است.

به عنوان مثال، فرض کنید نرم‌افزار آسیب‌پذیر A از کاربر یک ورودی دریافت می‌کند. یک کاربر با مهارت‌های لازم، می‌تواند با ارسال یک ورودی مخرب به دقت تولید شده، روند اجرایی نرم‌افزار را تغییر داده و کنترل سیستم را به دست بگیرد و فرمان‌های غیرمجاز اجرا کند.

امنیت وب

یکی از **مسائل بسیار پرکاربرد در امنیت سایبری**، امنیت وب است. همه ما هر روز صفحات وب (سایت های اینترنتی) بسیاری را مشاهده می کنیم. در واقع حفظ امنیت این صفحات چالش های مختلفی دارد.

مهاجم می تواند با حمله به این صفحات اطلاعات کاربران را بدزدد و یا از طرف آن ها یک عملیات غیر مجاز انجام دهد. در موضوع امنیت وب، حملات وارد به این صفحات و راه مقابله با آن ها بررسی می شود. اصطلاح هک کردن (Hacking) عمدتا به این دسته از حملات اطلاق می شود.

مهندسی معکوس

یکی از تکنیک های مورد استفاده در **امنیت سایبری** جهت تحلیل عملکرد نرم افزار ها و بدافزارها مهندسی معکوس است. با استفاده از تکنیک های مهندسی معکوس کدهای اجرایی یک نرم افزار بررسی می شود.

به عنوان مثال، برخی با استفاده از این تکنیک ها، محدودیت های نرم افزارهای پولی را دور می زنند و به اصطلاح آن را کرک (Crack) می کنند. همچنین با تحلیل عملکرد بدافزارها، راه مقابله با آن ها را طراحی می کنند.

جرم‌شناسی دیجیتال

به عنوان یک قیاس، جرم‌شناسی دیجیتال مشابه کارآگاهی یک صحنه‌جرم است. تحت این عنوان مهارت‌های لازم جهت کسب اطلاعات در مورد یک جرم دیجیتال مانند باج‌گیری یا هک کردن، جهت شناسایی مجرم و نقاط ضعف سیستم‌ها آموزش داده می‌شود. یک تکنیک می‌تواند بررسی اطلاعات مشخصی از یک کامپیوتر برای تعیین میزان آسیب وارد شده، تشخیص فعالیت‌های مجرم و ردگیری وی باشد.

در کنار موضوعات معرفی شده، موضوعات مهم دیگری مانند امنیت موبایل، امنیت سخت‌افزار و عناوین دیگر نیز وجود دارد. قدم اول برای یادگیری و ورود به حوزه امنیت، بررسی بیشتر این موضوعات و انتخاب مسیر مورد علاقه است. منابع بیشماری به صورت مکتوب، ویدیویی و یا تعاملی وجود دارد که می‌توانید از آن‌ها استفاده کنید. همچنین یکی از راه‌های پر بازده برای **تقویت مهارت های حوزه امنیت**، شرکت و حل سوالات مسابقات امنیت موسوم به CTF یا Catch The Flagاست.

رشته امنیت سایبری

مباحث مرتبط با امنیت سایبری تحت عنوان گرایش رایانش امن در مقطع ارشد مهندسی کامپیوتر آموزش داده می‌شود. از دانشگاه های مطرحی که این گرایش را ارائه می‌دهند میتوان به دانشگاه صنعتی شریف، دانشگاه امیرکبیر، دانشگاه تربیت مدرس و دانشگاه اصفهان اشاره کرد. در بخش بررسی رشته رایانش امن به طور مفصل این گرایش بررسی شده است. یکی از پیش‌نیاز های قبولی در رشته رایانش امن و به طور کلی تخصص در امنیت سایبری، تسلط بر درس شبکه های کامپیوتری است که جزو دروس مهم مقطع کارشناسی رشته مهندسی کامپیوتر است .

همانطور که در بخش انواع امنیت سایبری بررسی شد یکی از شاخه های مهم این حوزه است.