حملات سایبری چیست و چه انواعی دارد؟

هفته نامه آموزشی شنبه های سایبری شماره هفتاد و پنج

Cyber Saturdays No. 75

مدیریت آمار، فناوری اطلاعات و امنیت فضای مجازی

تلفن : ۰۵۱-۳۸۰۲۳۰۷۸ it.security@mums.ac.ir

حملات سایبری چیست و چه انواعی دارد؟

حملات سایبری چیست؟

این روزها که دنیای مجازی به بخش غیر قابل جداشدنی زندگی ما انسان‌ها تبدیل شده است باید مراقب داده‌هایمان باشیم تا مورد حملات سایبری قرار نگیرد. اطلاعات بانکی، نام کاربری، رمز عبور سایت، کیف پول‌های ارزی مجازی و غیره از جمله این موارد هستند که اطلاعات ارزشمندی را در خود جای می‌دهند.

حمله سایبری زمانی اتفاق می‌افتد که مجرمان سایبری سعی دارند به داده‌های الکترونیکی ذخیره شده در رایانه یا شبکه، دسترسی غیرقانونی پیدا کنند. هدف از این کار ممکن است وارد کردن صدمه به شهرت، آسیب رساندن به یک کسب‌وکار یا یک شخص یا حتی به سرقت بردن داده‌های ارزشمند باشد؛ این در حالی است که حملات سایبری می‌تواند افراد، گروه‌ها، سازمان‌ها یا دولت‌ها را مورد هدف قرار دهد.

حملات سایبری داده‌هایی را نشانه می‌گیرند که مهاجمان می‌توانند کنترل‌های امنیتی شناخته شده مانند احراز هویت دو مرحله‌ای را دور بزنند، بنابراین سازمان‌ها و شرکت‌های امنیتی باید بیشتر به رویکرد خود نسبت به امنیت سایبری فکر کنند.

حمله سایبری اغلب اولین گامی است که مهاجم برای دسترسی غیرمجاز به رایانه‌ها یا شبکه‌های فردی یا تجاری قبل از انجام نشت داده برمی‌دارد.

هدف حمله سایبری غیرفعال کردن رایانه موردنظر و آفلاین کردن آن یا دسترسی به داده‌های رایانه و نفوذ به شبکه‌ها و سیستم‌های متصل است.

انگیزه‌های حملات سایبری نیز متفاوت است اما به طور کلی، سه دسته اصلی کیفری، سیاسی و شخصی برای آنها وجود دارد.

مهاجمانی که با انگیزه مجرمانه وارد کار می‌شوند، به‌دنبال سود مالی از طریق سرقت پول، سرقت اطلاعات یا اختلال در تجارت هستند. افرادی که انگیزه شخصی دارند، مانند کارمندان ناراضی فعلی یا سابق یک نهاد به دنبال پول، داده یا فرصتی برای ایجاد اختلال در سیستم شرکت هستند. این درحالی است که بنا بر بررسی‌ها، انتقام، اصلی‌ترین انگیزه اغلب آنها است. اما مهاجمانی که انگیزه اجتماعی-سیاسی دارند، معمولا به دنبال جلب توجه برای علل خود هستند. در نتیجه، آنها حملات خود را در معرض دید عموم قرار می‌دهند.

البته انگیزه‌های دیگری هم برای حملات سایبری وجود دارد؛ از جمله آنها می‌توان به جاسوسی اشاره کرد.

امروزه اکثر حملات سایبری، به‌ویژه حملات علیه نهادهای تجاری برای منافع مالی انجام می‌شود. هدف این حملات اغلب سرقت داده‌های حساس مانند شماره کارت اعتباری مشتری یا اطلاعات شخصی کارکنان است که مجرمان سایبری از آنها برای دسترسی به پول یا کالا با استفاده از هویت قربانیان استفاده می‌کنند.

مهاجمان سایبری چه چیزهایی را هدف می‌گیرند؟

حملات سایبری معمولاً به این دلیل اتفاق می‌افتد که سازمان‌ها، فعالان دولتی یا اشخاص یک یا چند هدف (Target) را دنبال می‌کنند. مانند:

- داده‌های مالی کسب‌وکارها
- لیست مشتریان
- داده‌های مالی مشتری
- پایگاه‌های داده مشتری، از جمله اطلاعات شناسایی شخصی
- آدرس‌های ایمیل و اعتبار ورود به سیستم
- مالکیت معنوی، مانند اسرار تجاری یا طراحی محصول
- دسترسی به زیرساخت فناوری اطلاعات

حملات سایبری چیست و چه انواعی دارد؟

- خدمات فناوری اطلاعات، برای پذیرش پرداخت‌های مالی
- داده‌های شخصی حساس

سایبر تروریسم

سایبر تروریسم یکی از اشکال نوین ترور علیه منافع ملی است. در حملات تروریستی خشونت علیه اشخاص، دولت‌ها یا گروه‌ها برای پیشبرد اهداف سیاسی و عمومی به کار گرفته می‌شود. سایبر تروریسم هدف خود را روی منابع موجود در فضای مجازی متمرکز می‌کند. امروزه این نوع حملات سایبری بسیار خطرناک‌تر از تروریسم سنتی است؛ چرا که بسیاری از کشورها در زمینه فناوری اطلاعات رشد اقتصادی زیادی دارند و همین باعث ایجاد سایبر تروریسم‌ها در سراسر جهان شده است.

امنیت سیستم‌های کامپیوتری و شبکه‌های سایبری در هر کشوری از اهمیت بسیار زیادی برخوردار است. به همین خاطر است که تقویت زیرساخت‌های سایبری باید در اولویت کار هر سازمانی قرار بگیرد. یکی از مهم‌ترین اقدامات پیشگیرانه برای آسیب‌های احتمالی در زمینه فناوری کامپیوتری و سایبرنتیک، اتخاذ تدابیر امنیتی است. امروزه مهاجمان فقط با در دست داشتن یک کامپیوتر می‌توانند تهدیدی برای منافع یک کشور به حساب بیایند. باتوجه به اهدافی که تروریست‌ها به دنبال آن برنامه‌های خود را طراحی و سازماندهی می‌کنند باید که راه‌های پیشگیری از تروریسم سایبری اولویت همه افراد و سازمان‌ها باشد. اولین گزینه عاقلانه برای جلوگیری از این نوع حمله سایبری، اتخاذ تدابیر پیشگیرانه خواهد بود که پیشگیری وضعی و پیشگیری اجتماعی به عنوان جامع‌ترین راهکار موفقیت‌آمیز در این زمینه مورد توجه قرار گرفته است.

انواع حملات سایبری

یک حمله سایبری، به‌ویژه اگر توسط یک هکر ماهر انجام شود، ممکن است از مراحل مکرر تشکیل شده باشد؛ برای همین درک انواع حمله و مراحل مربوط، به شما کمک می‌کند تا بهتر از خود دفاع کنید.

بدافزار

بدافزار، اصطلاحی است که برای نرم‌افزارهای مخرب از جمله جاسوس‌افزارها، باج‌افزارها، ویروس‌ها و کرم‌ها به‌کار برده می‌شود. بدافزارها عموما از طریق یک آسیب‌پذیری به شبکه نفوذ می‌کند؛ معمولا این ورود هنگامی انجام می‌شود که کاربر روی لینک یا پیوست ایمیل آسیب‌زا کلیک کرده و نرم‌افزار مخربی را نصب می‌کند.

فیشینگ

فیشینگ، نوعی تهدید سایبری و روشی برای ارسال ارتباطات جعلی است که به نظر می‌رسد از طریق یک منبع معتبر یا از ایمیل ارسال می‌شود. هدف از این کار، سرقت یا دریافت اطلاعات مهم مانند کارت اعتباری و اطلاعات ورود به سیستم یا نصب بدافزار روی دستگاه فرد مورد نظر است.

حمله Man-in-the-middle

حملات Man-in-the-Middle (MitM) که به آن حملات «شنود» نیز می‌گویند، زمانی رخ می‌دهد که مهاجمان خود را وارد یک تراکنش دو طرفه می‌کنند، هنگامی که مهاجمان ترافیک را قطع می‌کنند، می‌توانند داده‌ها را فیلتر و سرقت کنند. در این نوع حملات دو نقطه مشترک برای ورود وجود دارد.

با استفاده از وای‌فای عمومی ناامن، مهاجمان می‌توانند خود را بین دستگاه بازدیدکننده و شبکه قرار دهند و بازدیدکننده بدون این‌که بداند، تمام اطلاعات را از طریق مهاجم منتقل می‌کند.

هنگامی که بدافزار به یک دستگاه نفوذ کرد، مهاجم می‌تواند نرم‌افزاری را برای پردازش تمام اطلاعات قربانی نصب کند.

حملات سایبری چیست و چه انواعی دارد؟

حمله Denial-of-service

این حمله سیستم‌ها، سرورها یا شبکه‌ها را پر از ترافیک و در نتیجه منابع و پهنای باند را تخلیه می‌کند. این کار باعث می‌شود سیستم قادر به انجام درخواست‌های قانونی نباشد. مهاجمان از چندین دستگاه در معرض خطر برای انجام این حمله استفاده می‌کنند.

حمله‌های سایبری کشورها علیه یکدیگر و بزرگ‌ترین حمله سایبری جهان

فناوری‌های جدید و پیشرفته همانند یک شمشیر دو لبه عمل می‌کنند. این فناوری‌ها هم به‌عنوان یک دارایی بزرگ برای سازمان‌ها به‌شمار می‌روند و روش‌های جدید پیشرفته امنیتی را برای آنها فراهم کرده و هم می‌توان با حمله‌های سایبری کشورها علیه یکدیگر از آن استفاده کرد.

در این بین بزرگ‌ترین حمله سایبری جهان علیه زیرساخت‌های اسرائیل رخ‌داده است. در نتیجه این حمله سایت موساد از دسترس خارج شد. در سال ۲۰۲۱ نیز بسیاری از شرکت‌ها و نهادهای حساس در سراسر جهان مورد حملات سایبری قرار گرفتند که این هکرها موفق شدند به نهادهای آمریکایی نفوذ کرده و اطلاعات میلیون‌ها کاربر را به سرقت ببرند. در این سال همزمان با شیوع ویروس کرونا، بیشتر شرکت‌ها مجبور شدند خدمات خود را به‌صورت آنلاین و اینترنتی ارائه دهند و همین به هکرها فرصت داد که خلاق‌تر شوند.

در این بازه زمانی حملات سایبری ۲۹ درصد افزایش پیدا کرد. حمله به خط لوله انتقال سوخت در آمریکا یکی از بزرگ‌ترین حملات سایبری جهان محسوب می‌شود که هکرها با استفاده از باج‌افزار دارک ساید موفق به نفوذ در این سایت شدند. کولون یال پایپ لاین یکی از بزرگ‌ترین شرکت‌های انتقال سوخت در آمریکا است که این حمله باعث شد انتقال سوخت چند روز با مشکل جدی مواجه شود.

حملات سایبری علیه ایران

بدافزارها در سال‌های ۲۰۰۹ و ۲۰۱۰ ساخته شدند. این روزها تروریسم سایبری چهارمین دهه خود را طی کرده و چنان گسترش‌یافته که از سال ۲۰۱۲ به بعد به عنوان سال جهنمی از آن یاد می‌شود. افرادی که در زمینه حملات سایبری مشغول به کار هستند با داشتن یک میلیارد دلار بودجه و پنجاه نفر نیروی متخصص، می‌توانند یک کشور را مختل کنند.

حملات سایبری علیه ایران نیز انجام شده و بخش‌های مختلفی مانند نفت، بانک، صنعت و غیره را از کار انداخته یا حداقل باعث بروز اختلال شده است. این حملات ریز و درشت چنان وسیع بوده که وزیر ارتباطات شمار این حملات را حتی تا ۱۴هزار نیز گزارش کرده است. یکی از جدیدترین حملات بدافزاری به نام «ناریلام» است که این روزها در فضای رسانه‌ای بیشتر در مورد آن صحبت می‌شود.

استاکس نت، حمله سایبری‌ای که علیه ایران در بخش صنعتی در سال ۱۳۸۹ صورت گرفت که آن زمان موضوع کرم جاسوسی پربحث و درخور توجه بود. این کرم به بخش صنعتی کشورها حمله می‌کرد و برخی از کامپیوترهای ایران را نیز تحت‌تاثیر خود قرار داده بود. عمده مراکزی که مورد هجوم این کرم قرار گرفته بود مربوط به بخش نفت و نیرو بوده که در همین راستا، IPهایی برای شناسایی آن و آنتی‌ویروس‌هایی برای مقابله با آن در برنامه دولت قرار گرفت.

حملات سایبری چیست و چه انواعی دارد؟

هک سایبری چیست؟

ممکن است بسیاری با کلمه هک سایبری آشنایی داشته باشند ولی ندانند این حمله دقیقا به چه صورتی انجام می‌شود. هک سایبری در اصل به حرکتی آگاهانه و غیراخلاقی در جهت تخریب یا سرقت اطلاعات شخص، سازمان یا یک دولت گفته می‌شود. هکرها معمولا برای حمله به یک سیستم دلایل خاص خود را دارند و برخی از آنها که به هکرهای کلاه‌سفید مشهور هستند اهداف مشخصی را دنبال می‌کنند و حمله آنها از نوع حملات سایبری نیست.

ولی هکرهای دیگری هستند که به قصد نقض سیستم اطلاعاتی سازمان یا شخصی اقدام به هک خواهند کرد و این نوع هک، حمله سایبری محسوب می‌شود. در یک هک سایبری ممکن است تمام اعتبار و ارزشی را که یک سازمان یا شخص به سختی به دست آورده از بین برود. این هک، حتی شرکت‌های بزرگ را می‌تواند ورشکسته کند و اعتماد مشتریان به این شرکت‌ها و موسسات را از بین ببرد. البته باید بگوییم که همه هکرها بد نیستند و برخی از آنها برای عیب‌یابی و از بین بردن فساد و مشکلی از پیش شکل گرفته اقدام به چنین کاری می‌کنند.

هک سایبری در جزئی‌ترین حالت خود نیز می‌تواند خسارت لازم را وارد کند، حتی اگر از نوع مالی نباشد. این هک‌ها مشکلاتی از قبیل مختل‌شدن سیستم، مشکلات مالی و ورشکستگی، از دست دادن اعتبار، مشکلات روحی و روانی و ضربه به کاربران را به دنبال خواهد داشت.

حملات سایبری و حقوق بین‌الملل

حملات سایبری به عنوان یک جنگ مدرن شناخته می‌شود و به خاطر ماهیت انتزاعی آن و مفاهیم ناملموس نسبت به فضای عینی برای حقوق بین‌الملل ناشناخته است. به همین خاطر شاید این سوال برای بیشتر افراد پیش بیاید که آیا حقوق بین‌الملل برای حملات سایبری قابل اجرا خواهد بود؟

برخی از محققان بر این باور هستند که اگر قصد این نوع حملات ایجاد صدمات فیزیکی یا خسارات باشد و به حمله‌های مسلحانه بینجامد باید مقررات و قوانین بین‌المللی دیگری را برای آن در نظر گرفت.

این مقررات که رفتار و عملکرد دولت‌ها را هنگام درگیری‌های مسلحانه به نظم در می‌آورد به حقوق بشردوستانه بین‌المللی یا حقوق حاکم در جنگ اطلاق می‌شود. در حال حاضر هیچ‌گونه حقوق بین‌المللی‌ای برای حملات سایبری وجود ندارد و این موضوع به‌خاطر قطعی نبودن جنگ سایبری سرچشمه می‌گیرد. پس در حال حاضر هیچ‌گونه قواعد و قوانین بین‌المللی‌ای برای اینکه حمله سایبری را ممنوع اعلام کند وجود نداشته و برخی محققان می‌گویند به دلیل این‌که در این نوع از حملات هیچ‌گونه برخورد فیزیکی صورت نمی‌گیرد؛ بنابراین نمی‌توان قانونی را هم برای آن وضع کرد.

حملات سایبری در پدافند غیرعامل

در قرن بیستم، فناوری دیجیتال توسعه زیادی پیدا کرد و جهان دچار تغییر شد. با این فناوری بسیاری از کارها ساده‌تر و بهینه‌تر شده است. در این بین پدافند سایبری یکی از مهم‌ترین مولفه‌ها در پدافند غیرعامل به شمار می‌رود. پدافند غیرعامل به نوعی از دفاع غیرنظامی و اقداماتی که بدون سلاح انجام

حملات سایبری چیست و چه انواعی دارد؟

می‌شود گفته می‌شود که با انجام‌دادن آن می‌توان زیرساخت‌های نظامی، غیرنظامی و جان انسان‌ها را با آن نجات داد و از آسیب رساندن به این زیرساخت‌ها جلوگیری کرد.

مهم‌ترین هدف پدافند غیرعامل حفاظت از جان مردم، حفاظت از زیرساخت‌های حیاتی، تامین نیازهای مردم، پایدارسازی مدیریت عالی کشور، استمرار خدمات ضروری، دفاع بیولوژیک از کشور و غیره است. به‌خاطر دیجیتالی شدن بسیاری از سازمان‌ها و زیرساخت‌های کشور، استفاده از پدافند غیرعامل در برابر حملات سایبری بسیار لازم و ضروری خواهد بود. سازمان‌ها و افراد برای رعایت کردن اصول امنیت سایبری از دسترسی غیرمجاز به داده‌ها، کامپیوترها و شبکه‌ها باید جلوگیری کنند. رعایت چنین اصولی باعث می‌شود از حذف داده‌ها و سرقت آنها جلوگیری شود.

حملات سایبری قابل پیشگیری است؟

کلید محافظت در برابر حملات سایبری، یک معماری امنیت سایبری سرتاسری چندلایه است و همه شبکه‌ها، نقطه پایانی و دستگاه‌های تلفن همراه و کلود را دربر می‌گیرد. با معماری مناسب می‌توانید مدیریت چندین لایه امنیتی را تجمیع کنید، این به شما امکان می‌دهد رخدادها را در تمام محیط‌های شبکه، سرویس‌های ابری و زیرساخت‌های تلفن همراه مرتبط کنید.

امنیت سایبری به چه معناست؟

امنیت سایبری عبارت است از برنامه‌ریزی و اقدام برای حفاظت از سیستم‌ها، دیتابیس‌ها، شبکه‌ها و برنامه‌ها از حملات سایبری و سازماندهی یک استراتژی دفاعی علیه مجرمان دنیای مجازی.

امنیت سایبری یک سری پروتکل است که فرد یا شرکت برای اطمینان از اطلاعات خود از آن استفاده می‌کند. در صورتی که زیرساخت‌ها و تجهیزات امنیتی مناسب و لازم به درستی برقرار باشد، در صورت قطعی برق و بروز هر گونه خطا و خرابی امکان بازیابی هارد وجود دارد و اطلاعات و داده‌ها در صحت کامل قابل دسترسی خواهد بود. نبود سیستم کارآمد امنیتی در این شبکه‌ها و نداشتن برنامه و طرح مدیریتی و نگهداری از اطلاعات در شرایط خطیر در برابر حملات سایبری و هکرها موقعیت و داده‌های فرد یا افراد و سازمان‌ها را با خطری جدی مواجه می‌کند.

تمامی سازمان‌ها و شرکت‌ها از داشتن آخرین استانداردها با امنیت بالا باید اطمینان حاصل کنند و کارمندان نیز باید در پروتکل‌های امنیت سایبری آموزش لازم را ببینند. بدون داشتن یک استراتژی امنیتی امکان وقوع اتفاقات ناگوار وجود دارد. هکرها به‌خوبی می‌دانند چگونه نقاط ضعف را پیدا کرده و از آنها بهره‌برداری کنند. به دلیل افزایش تعداد کاربران، برنامه‌ها، دستگاه‌ها و سیل عظیمی از داده‌ها که بسیاری از آنها محرمانه و حساس هستند، برخورداری از امنیت سایبری روز به روز اهمیت پیدا می‌کند. این نوع امنیت، سیستم‌های کامپیوتری، موبایل، سرورها و سیستم الکترونیکی را از حملات سایبری محفوظ نگه می‌دارد و وظیفه حفاظت از دستگاه‌هایی که افراد استفاده می‌کنند و حفاظت از هویت و اطلاعات آنها را بر عهده خواهد داشت.