حملات سایبری چیست؟

حمله سایبری هرگونه تلاش مخرب برای دستیابی به دسترسی غیرمجاز به رایانه، سیستم محاسباتی یا شبکه رایانه ای با هدف ایجاد آسیب است. هدف حملات سایبری غیرفعال کردن، مختل کردن، تخریب یا کنترل سیستم های رایانه ای یا تغییر، مسدود کردن، حذف، دستکاری یا سرقت داده های موجود در این سیستم ها است. هر فرد یا گروهی می تواند با استفاده از یک یا چند استراتژی حمله از هر نقطه ای حمله سایبری را انجام دهد. مجرمان سایبری که حملات سایبری را انجام می دهند اغلب به عنوان بازیگران بد، بازیگران تهدید و هکرها شناخته می شوند. آنها شامل افرادی هستند که به تنهایی عمل می کنند و از مهارت های کامپیوتری خود برای طراحی و اجرای حملات مخرب استفاده می کنند. این گروه ها با دیگر بازیگران تهدید کار می کنند تا نقاط ضعف یا آسیب پذیری را در سیستم های رایانه ای پیدا کنند که می توانند از آنها برای سود بهره برداری کنند. گروه های متخصص کامپیوتر تحت حمایت دولت نیز حملات سایبری را انجام می دهند. آنها به عنوان مهاجمان دولت ملت شناخته می شوند و متهم به حمله به زیرساخت فناوری اطلاعات سایر دولت ها و همچنین نهادهای غیردولتی مانند مشاغل، مؤسسات غیرانتفاعی و خدمات عمومی شده اند.

چرا حملات سایبری اتفاق می افتد؟

حملات سایبری برای ایجاد آسیب طراحی شده اند. آنها می توانند اهداف مختلفی داشته باشند، از جمله:

سود مالی :

مجرمان سایبری بیشتر حملات سایبری، به ویژه حملات سایبری را علیه نهادهای تجاری، برای منافع مالی انجام می دهند. هدف این حملات اغلب سرقت داده های 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 می کنند.

سایر حملات با انگیزه مالی برای از کار انداختن سیستم‌های رایانه‌ای طراحی شده‌اند و مجرمان سایبری رایانه‌ها را قفل می‌کنند تا مالکان و کاربران مجاز نتوانند به برنامه‌ها یا داده‌های مورد نیاز خود دسترسی پیدا کنند. سپس مهاجمان از سازمان‌های هدف می‌خواهند که برای باز کردن قفل سیستم‌های رایانه‌ای به آنها باج بپردازند. با این حال، سایر حملات با هدف به دست آوردن داده های شرکتی ارزشمند، مانند اطلاعات اختصاصی، انجام می شود. این نوع حملات سایبری نوعی مدرن و کامپیوتری از جاسوسی شرکتی است.

اخلال و انتقام:

برخی نیز به طور خاص حملاتی را برای ایجاد هرج و مرج، سردرگمی، نارضایتی، ناامیدی یا بی اعتمادی انجام می دهند. آنها می توانند چنین اقداماتی را برای انتقام گرفتن از اعمالی که علیه آنها انجام می شود انجام دهند. هدف آنها ممکن است شرمساری عمومی برای نهادهای مورد حمله یا آسیب رساندن به اعتبار یک سازمان باشد. این حملات اغلب متوجه نهادهای دولتی می شوند، اما می توانند سازمان های تجاری یا غیرانتفاعی را نیز هدف قرار دهند. مهاجمان دولت ملت پشت برخی از این نوع حملات هستند. برخی دیگر که هکتیویست نامیده می شوند، ممکن است این نوع حملات را به عنوان نوعی اعتراض علیه نهاد مورد نظر انجام دهند. یک گروه غیرمتمرکز مخفی از فعالان انترناسیونالیست که به نام Anonymous شناخته می شوند، شناخته شده ترین این گروه ها هستند. تهدیدات داخلی حملاتی هستند که از سوی کارمندان با نیت مخرب انجام می شود.

جنگ سایبری :

دولت‌های سراسر جهان نیز در حملات سایبری دخیل هستند، به طوری که بسیاری از دولت‌های ملی به طراحی و اجرای حملات علیه سایر کشورها به عنوان بخشی از مناقشات سیاسی، اقتصادی یا اجتماعی مداوم اذعان دارند یا مظنون به طراحی و اجرای حملات هستند. این نوع حملات به عنوان جنگ سایبری طبقه بندی می شوند.

مطلب پیشنهادی: 7 روش متداول کلاه برداری در ارز دیجیتال

معرفی انواع حملات سایبری

حملات سایبری می‌توانند در اشکال مختلفی اتفاق بیفتند و به طرق مختلفی از جمله نفوذ به سیستم‌ها، دزدیدن اطلاعات، قربانی کردن سرویس‌ها و آسیب رساندن به زیرساخت‌های فناوری اطلاعات و ارتباطات (ICT) عمل کنند. در زیر، برخی از انواع رایج حملات سایبری را معرفی می‌کنم:

1. **فیشینگ (Phishing):** در این حمله، مهاجمان تلاش می‌کنند از طریق ایمیل‌ها، پیام‌های متنی یا تماس‌های تلفنی جعلی، اطلاعات حساس از کاربران را دریافت کنند. به طور معمول، این حملات به شکل صفحات وب جعلی یا درخواست‌های تقلبی ارائه می‌شوند.
2. **نفوذ (Hacking):** در حملات نفوذ، مهاجمان سعی می‌کنند از طریق شکاف‌ها و آسیب‌پذیری‌های موجود در سیستم‌ها، به سیستم‌ها و شبکه‌های مورد نظر نفوذ کنند. این حملات می‌توانند شامل نفوذ به سرورها، کنترل دستگاه‌ها، دسترسی به پایگاه داده‌ها و موارد مشابه باشند.
3. **رمزگشایی (Brute Force):** در این حمله، مهاجمان از تلاش مداوم برای حدس زدن رمزهای عبور استفاده می‌کنند. آن‌ها با استفاده از نرم‌افزارهای خاص، تعداد زیادی ترکیب ممکن را برای رمزعبورها امتحان می‌کنند تا به صورت خودکار رمزعبور را کشف کنند.
4. **نفوذ به شبکه (Network Intrusion):** در این حمله، مهاجمان تلاش می‌کنند به شبکه‌ها و سیستم‌های متصل به شبکه دسترسی یابند. آن‌ها می‌توانند از طریق ضعف‌ها در سیستم‌های متصل به شبکه یا بهره‌برداری از آسیب‌پذیری‌های شبکه، دسترسی نامشروع به داده‌ها را به دست آورند.
5. **رمزنگاری مخرب (Ransomware):** در این نوع حمله، نرم‌افزار مخربی بر روی سیستم قربانی قرار می‌گیرد و فایل‌ها را با استفاده از رمزنگاری رمزگذاری می‌کند. سپس، مهاجمان برای بازگشایی فایل‌ها و دسترسی به آن‌ها، مبلغی را در قادامه می‌دهند. درخواست می‌کنند. به عبارت دیگر، آن‌ها با خواسته‌های رمزگشایی پولی یا Bitcoin از قربانیان می‌خواهند.

6. **حملات DDoS (سرویس غیرمنتظره):** حملات سرویس غیرمنتظره اغلب با استفاده از شبکه‌های زامبی (به عنوان مثال، بات‌نت‌ها) که توسط مهاجم کنترل می‌شوند، صورت می‌گیرند. در این حملات، تعداد زیادی درخواست از یک سرویس یا سرور به طور همزمان ارسال می‌شود، که منجر به بارزایی بر روی سرور مورد هدف می‌شود و باعث اختلال در سرویس و عدم دسترسی کاربران می‌شود.
7. **حملات فیزیکی (Physical Attacks):** حملات فیزیکی به سخت‌افزارها و دستگاه‌ها مرتبط هستند. این حملات شامل دزدیدن یا تخریب دستگاه‌ها، نفوذ به ساختمان‌ها و مراکز داده، اشغال فضای فیزیکی سیستم‌ها و مورد تخریب سخت‌افزاری می‌شوند.
8. **حملات صفحه اصلی (Malware):** نرم‌افزارهای مخرب (مالوئر) از طریق نصب نرم‌افزارهای مشکوک یا فایل‌های پیوست شده به ایمیل‌ها و پیام‌های متنی، به سیستم‌ها نفوذ می‌کنند. این نرم‌افزارها می‌توانند اطلاعات را بدزدند، کنترل سیستم را به مهاجم منتقل کنند یا آسیب رساندن به سیستم‌ها را هدف قرار دهند.

مهاجمان سایبری همچنین از انواع دیگری از حملات مانند جاسوسی (Espionage)، حملات هدفمند (Targeted Attacks)، نفوذ به اینترنت اشیا (IoT) و حملات به ابر (Cloud) نیز استفاده می‌کنند. این لیست تنها چند مثال از حملات سایبری است و هر روزه روش‌های جدیدی توسط مهاجمان سایبری توسعه می‌یابد.

مهاجمان سایبری چه چیزهایی را هدف می‌گیرند؟

مهاجمان سایبری به طور کلی به دنبال بهره‌برداری از ضعف‌ها وآسیب‌پذیری‌های موجود در سیستم‌ها و شبکه‌ها هستند. آن‌ها می‌توانند برای دستیابی به اهداف مختلف از جمله زیر را هدف قرار دهند:

1. **دزدیدن اطلاعات:** یکی از هدف‌های اصلی مهاجمان سایبری، دستیابی به اطلاعات حساس و محرمانه است. آن‌ها می‌توانند به دنبال دزدیدن اطلاعات مالی، اطلاعات شخصی کاربران، اطلاعات مربوط به شرکت‌ها و سازمان‌ها، اسناد دولتی و سایر اطلاعات محسوب شوند.
2. **سوءاستفاده از حساب‌ها:** مهاجمان سعی می‌کنند به حساب‌های کاربری افراد یا سازمان‌ها نفوذ کنند و سپس از آن‌ها برای اهداف شخصی یا مالی خود استفاده کنند. آن‌ها می‌توانند از طریق دسترسی غیرمجاز به حساب‌های بانکی، حساب‌های رسانه‌های اجتماعی، ایمیل‌ها و سایر حساب‌های آنلاین استفاده کنند.
3. **نقض حریم خصوصی:** مهاجمان سایبری ممکن است به دنبال نقض حریم خصوصی فردی یا سازمانی باشند. آن‌ها می‌توانند اطلاعات شخصی را دزدیده یا منتشر کنند، دستگاه‌های حریم خصوصی را هدف قرار دهند و اطلاعات محرمانه را در دسترس عموم قرار دهند.

4. **قربانی کردن سرویس‌ها:** مهاجمان ممکن است به سرویس‌ها و برنامه‌های مختلف حمله کنند و آن‌ها را غیرفعال کنند یا از دسترس خارج کنند. این حملات می‌توانند منجر به اختلال در عملکرد و عدم دسترسی به سرویس‌های آنلاین، سیستم‌های بانکی، سایت‌های تجاری و سایر سرویس‌های مهم شوند.

حملات سایبری چگونه کار می کنند؟

عوامل تهدید از تکنیک‌های مختلفی برای راه‌اندازی حملات سایبری استفاده می‌کنند که تا حد زیادی بستگی به این دارد که آیا آنها به یک نهاد هدف‌دار یا غیرهدف حمله می‌کنند. در یک حمله غیر هدفمند، که در آن حمله کنندگان تلاش می‌کنند تا حد امکان به دستگاه‌ها یا سیستم‌ها نفوذ کنند، عموماً به دنبال آسیب‌پذیری‌هایی در کد نرم‌افزاری می‌گردند که آنها را قادر می‌سازد بدون شناسایی یا مسدود شدن، دسترسی پیدا کنند. یا ممکن است از یک حمله فیشینگ استفاده کنند و به تعداد زیادی از مردم پیام‌های مهندسی شده اجتماعی ارسال کنند که برای ترغیب گیرندگان به کلیک کردن روی پیوندی که کدهای مخرب را دانلود می‌کند، ارسال کنند.

در یک حمله هدفمند، عوامل تهدید به دنبال یک سازمان خاص هستند و روش های مورد استفاده بسته به اهداف حمله متفاوت است. به عنوان مثال، گروه هکریست Anonymous، پس از مرگ مردی در حین دستگیری توسط افسران مینیاپولیس، مظنون به یک حمله انکار خدمات توزیع شده (DDoS) در سال 2020 در وب سایت اداره پلیس مینیاپولیس بود. هکرها همچنین از کمپین‌های فیشینگ نیزه‌ای در یک حمله هدفمند استفاده می‌کنند و ایمیل‌هایی را برای افراد خاصی ایجاد می‌کنند که در صورت کلیک بر روی لینک‌های موجود، نرم‌افزار مخربی را دانلود می‌کنند که برای تخریب فناوری سازمان یا داده‌های حساس آن طراحی شده است. مجرمان سایبری اغلب ابزارهای نرم افزاری را برای استفاده در حملات خود ایجاد می کنند و اغلب آنها را در وب تاریک به اشتراک می گذارند. حملات سایبری اغلب به صورت مرحله‌ای اتفاق می‌افتند، با بررسی یا اسکن هکرها برای یافتن آسیب‌پذیری‌ها یا نقاط دسترسی، شروع به خطر افتادن اولیه و سپس اجرای حمله کامل – چه سرقت داده‌های ارزشمند، غیرفعال کردن سیستم‌های کامپیوتری یا هر دو. در واقع، اکثر سازمان ها ماه ها طول می کشند تا حمله ای را که در حال انجام است شناسایی کرده و سپس آن را مهار کنند.

مطلب پیشنهادی: مفهوم کلاه برداری پانزی

روند حملات سایبری

با افزایش فراوانی و پیچیدگی حملات سایبری، روندهای مختلفی ظاهر شده اند. به عنوان مثال، سه روند در حال حاضر ظاهر شده در حملات سایبری شامل موارد زیر است:

- **باج افزار(Ransomware):** این یک تهدید فزاینده و اساسی برای سازمان ها بوده است، زیرا این حملات پیچیده تر و رایج تر شده اند. مهاجمان تکنیک‌های باج‌افزاری را پیدا کرده‌اند که نتایج بهتری را برای مهاجمان به همراه دارد.
- **استفاده از هوش مصنوعی :** همراه مخرب از ابزارهای هوش مصنوعی برای کمک به تلاش های هک خود استفاده می کنند. به عنوان مثال، در سال 2019، مدیر عامل یک شرکت انرژی مستقر در بریتانیا زمانی هدف قرار گرفت که آنها معتقد بودند با رئیس خود که واقعاً صدای تولید شده توسط هوش مصنوعی بود، تلفنی صحبت می کردند. مدیرعامل دستوری مبنی بر انتقال 243000 دلار به حساب بانکی تامین کننده مجارستانی را دنبال کرد. از آن زمان تعداد حملات مشابه افزایش یافته است.
- **هکتیویسم Hacktivists :** سیستم ها یا شبکه های کامپیوتری را به دلایل اجتماعی یا سیاسی هدف قرار می دهند. هکتیویست ها و گروه های هکتیویست تهدیدی مداوم برای حملات بوده اند. به عنوان مثال، در طول درگیری اسرائیل و غزه، هکریست ها مدعی شده اند که مسئول حملات سایبری در هر دو طرف هستند.

چگونه از ایجاد حملات سایبری جلوگیری کنیم؟

1. **اطمینان از به‌روز بودن نرم‌افزارها و سیستم‌عامل‌ها:** برنامه‌ها و سیستم‌عامل‌های به‌روز، دارای بهبودهای امنیتی جدید و رفع آسیب‌پذیری‌ها هستند. بنابراین، اطمینان حاصل کنید که همیشه از آخرین نسخه‌های نرم‌افزارها و سیستم‌عامل‌ها استفاده می‌کنید و به‌روزرسانی‌های امنیتی را به موقع انجام دهید.
2. **استفاده از رمزنگاری قوی:** از رمزنگاری قوی برای اطلاعات حساس خود استفاده کنید. این شامل استفاده از رمزهای عبور قوی، استفاده از پروتکل‌های ارتباطی رمزگذاری شده (مانند HTTPS) و استفاده از رمزنگاری دیسک برای فایل‌ها و سیستم‌های خود است.
3. **آگاهی از فیشینگ و حملات جعل هویت:** آموزش خود و کارمندان در مورد روش‌های تشخیص فیشینگ و جعل هویت می‌تواند به جلوگیری از این نوع حملات کمک کند. آگاهی از نشانه‌ها و رفتارهای مشکوک، عدم اعتماد به ایمیل‌ها و لینک‌های مشکوک و اعتماد به منابع معتبر از موارد مهم در این زمینه است.
4. **استفاده از نرم‌افزارهای امنیتی:** استفاده از نرم‌افزارهای آنتی‌ویروس، آنتی‌مالور و فایروال، می‌تواند کمک کند تا نرم‌افزارهای مخرب و حملات را شناسایی و مسدود کنید. مطمئن شوید که این نرم‌افزارها به‌روزرسانی شده و به طور منظم اسکن و بررسی شوند.
5. **مراقبت از رمزعبورها:** استفاده از رمزهای عبور قوی و منحصر به فرد برای هر سرویس و حساب کاربری، می‌تواند از دسترسی غیرمجاز به حساب‌ها جلوگیری کند. همچنین، تغییر

دوره‌ای رمزعبورها و استفاده از ابزارهای مدیریت رمزعبور (مانند مدیر رمزعبور) می‌تواند به افزایش امنیت کمک کند.

6. **پشتیبانی منظم از داده‌ها:** ایجاد پشتیبان منظم از داده‌های مهم و حساس، به شما کمک می‌کند در صورادامه می‌دهم:
7. **پشتیبانی منظم از داده‌ها:** ایجاد پشتیبان منظم از داده‌های مهم و حساس، به شما کمک می‌کند در صورت بروز حملات سایبری، از اطلاعات خود دست ندهید. برای این منظور، می‌توانید از روش‌های پشتیبان‌گیری مانند استفاده از درایوهای خارجی، سرویس‌های ذخیره‌سازی ابری یا سیستم‌های پشتیبان‌گیری خودکار استفاده کنید.
8. **محدود کردن دسترسی‌ها:** محدود کردن دسترسی به سیستم‌ها و منابع حساس، می‌تواند در جلوگیری از حملات سایبری موثر باشد. از اصول اصلی امنیتی مانند حداقل دسترسی (Principle of Least Privilege) استفاده کنید و تنها به کاربران و دستگاه‌هایی که نیاز دارند، دسترسی لازم را ارائه دهید.
9. **آموزش و آگاهی کارکنان:** آموزش کارکنان در مورد مسائل امنیتی و رفتارهای امن، می‌تواند به جلوگیری از حملات سایبری کمک کند. اطمینان حاصل کنید که کارکنان آگاهی کافی در مورد فیشینگ، جعل هویت، رمزنگاری و سایر تهدیدات امنیتی دارند.
10. **مانیتورینگ و ثبت رویدادها:** رصد و ثبت رویدادها و فعالیت‌ها در سیستم‌ها و شبکه‌ها، امکان تشخیص زودهنگام حملات سایبری را فراهم می‌کند. استفاده از سیستم‌های رصد امنیتی و بررسی منظم لاگ‌ها و رویدادها می‌تواند به شناسایی و پاسخگویی سریع تر به حملات کمک کند.
11. **برنامه ریزی برای بحران:** ایجاد یک برنامه بحرانی و تعیین نقشه عمل در صورت بروز حملات سایبری، می‌تواند در مدیریت و کاهش اثرات این حملات مؤثر باشد. این برنامه باید شامل اقداماتی مانند قطع اتصال به اینترنت، استراتژی‌های پشتیبانی و بازیابی داده‌ها و اطلاعات، و اطلاع رسانی به تیم‌های مربوطه باشد.

مطلب پیشنهادی: راگ پول چیست؟

امنیت سایبری به چه معناست؟

امنیت سایبری به معنای حفاظت از اطلاعات، سیستم‌ها، شبکه‌ها و سرویس‌های مرتبط با فضای سایبری است. هدف اصلی امنیت سایبری، جلوگیری از دسترسی غیرمجاز، استفاده ناصحیح و سوءاستفاده از اطلاعات دیجیتالی و فناوری اطلاعات است.

امنیت سایبری شامل مجموعه‌ای از تدابیر، فرآیندها، فناوری‌ها و استراتژی‌ها است که به منظور محافظت از اطلاعات حساس و حفظ سازمان‌ها و افراد در برابر حملات سایبری طراحی می‌شود. این شامل موارد زیر می‌شود:

1. **شناسایی و پیشگیری:** شامل شناسایی و آنالیز آسیب‌پذیری‌ها، مانیتورینگ و تشخیص حملات و پیشگیری از وقوع حملات سایبری است.
2. **حفاظت:** شامل استفاده از روش‌ها و فناوری‌ها برای حفاظت از سیستم‌ها، شبکه‌ها و اطلاعات در مقابل حملات سایبری است. این شامل استفاده از رمزنگاری، فایروال‌ها، آنتی‌ویروس، نرم‌افزارهای محافظت از هویت و سایر فناوری‌های امنیتی است.
3. **تشخیص و واکنش:** شامل تشخیص سریع واقعه‌های امنیتی، پاسخ‌دهی به آن‌ها و بازیابی سریع از حملات است. این شامل استفاده از مانیتورینگ و رصد، تجزیه و تحلیل رویدادها، ایجاد خط‌مشی‌ها و فرآیندهای واکنش به حوادث است.
4. **آموزش و افزایش آگاهی:** شامل آموزش کاربران درباره مفاهیم امنیتی، رفع نقاط ضعف و افزایش آگاهی از رویکردها و تهدیدات امنیتی است.
5. **امنیت فیزیکی:** شامل محافظت از تجهیزات فیزیکی مرتبط با فضای سایبری مانند سرورها، دیتاسنترها و تجهیزات شبکه است.

امنیت سایبری در دنیای امروز بسیار مهم است، زیرا حملات سایبری روز به روز هوشمندانه‌تر و پیچیده‌تر می‌شوند و می‌توانند عواقب جدی برای سازمان‌ها و افراد داشته باشند.