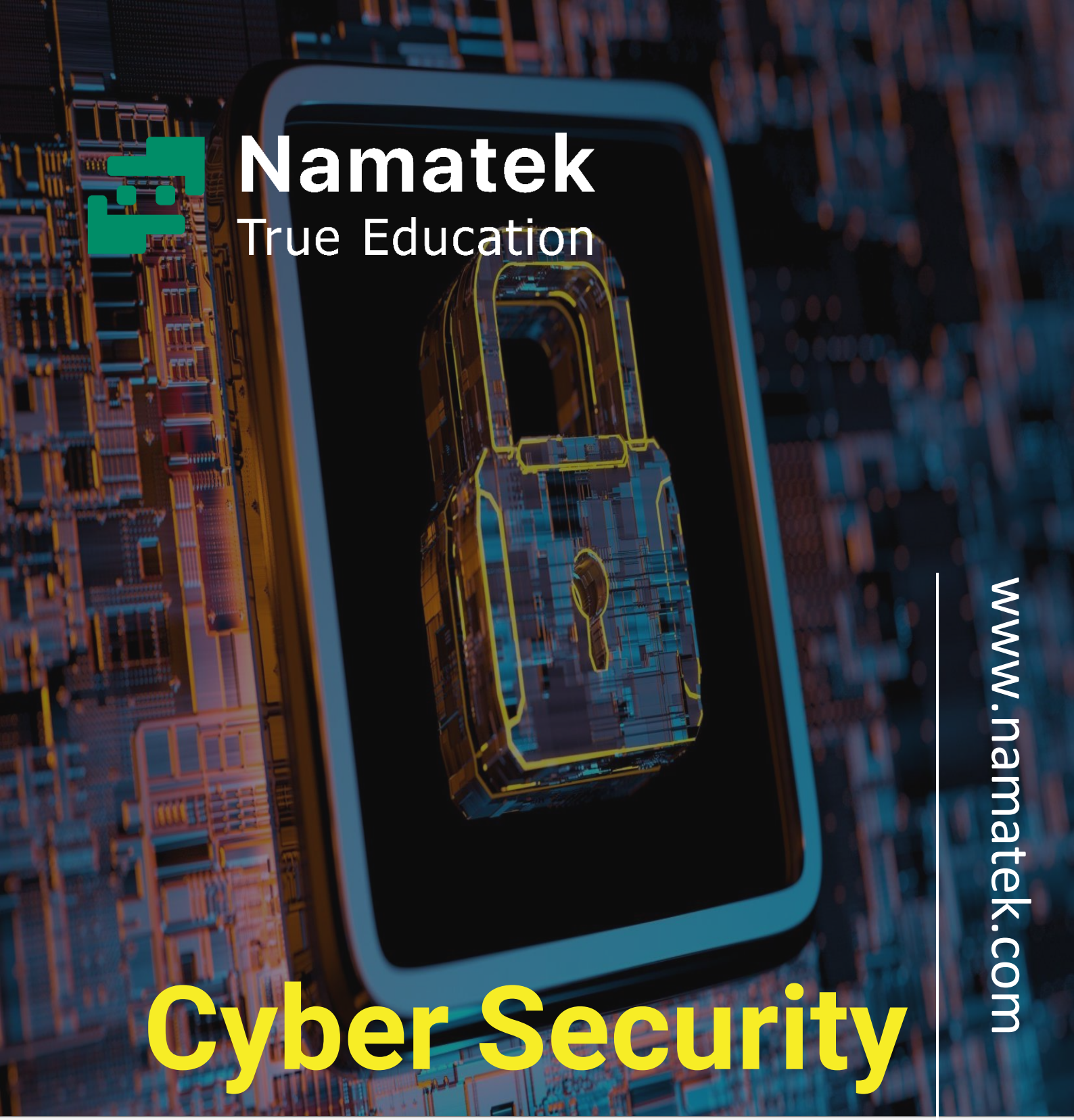


۹ روش تهدید امنیت سایبری و راه مقابله با آن ها

فهرست مطالب

امنیت سایبری از بروز حملات به شبکه ها، سیستم ها و داده ها جلوگیری می کند و در واقع سیستم ها و اطلاعات مهم یک سازمان را در برابر بروز چالش ها و مشکلات جدی محافظت می کند. حملات سایبری ممکن است در هر موقعیت زمانی علیه یک سازمان یا یک فرد صورت گیرند.

در این نوشتار به طور اختصاصی به تشریح امنیت سایبری پرداخته ایم. با ما همراه باشید.

#۱ امنیت سایبری چیست؟ (Cyber Security)

امنیت سایبری از دستگاه های متصل به دنیای اینترنت در مقابل حملات سایبری محافظت می کند. سیستم امنیتی برای محافظت از دستگاه ها و منابع اطلاعاتی باید از چندین لایه محافظتی برخوردار باشد تا امنیت

بالایی برای سیستم های یک سازمان ایجاد شود. این فرآیند توسط سازمان ها و افراد متخصص شکل می گیرد. در صورت طراحی و اجرای یک برنامه راهبردی قوی در این زمینه، دسترسی های مخرب و غیرمجاز، تغییر، تخریب، حذف و ویرایش غیرمنطقی اطلاعات محرمانه روی نخواهد داد.

#۲ اهمیت امنیت سایبری

با توجه به اینکه فعالیت در فضای دیجیتال و دنیای اینترنت روز به روز در حال گسترش است، اهمیت امنیت سایبری نیز افزایش یافته است؛ البته در زمینه خطرات، حملات و تهدیدات سایبری نیز تغییرات زیادی شکل گرفته و رویکردهای قدیمی و سنتی در این حوزه پاسخگوی امنیت فضای دیجیتال فعلی نخواهند بود. دلیل اهمیت امنیت سایبری این است که بسیاری از ارگان های دولتی، شرکت های خصوصی، مراکز علمی و اماکن

پزشکی حجم وسیعی از اطلاعات مهم را در سیستم های خود جمع آوری، پردازش و ذخیره می کنند. در صورت دسترسی غیرمجاز از طریق حملات سایبری یا هکرها بخش گسترده ای از این اطلاعات از بین می روند و شرکت ها و سازمان ها با خسارات جبران ناپذیری رو به رو می شوند.

#۳ انواع روش های تهدید امنیت سایبری (Cybersecurity Threats)

هدف اصلی از حملات سایبری از بین بردن اطلاعات مهم در سازمان ها است. حملات سایبری ممکن است از داخل یا خارج سیستم دیجیتال یا شبکه به یک فرد یا سازمان خسارت وارد کنند. در این بخش برخی از انواع حملات سایبری را که تهدیدی جدی برای تخریب امنیت سیستم ها هستند عنوان می کنیم.

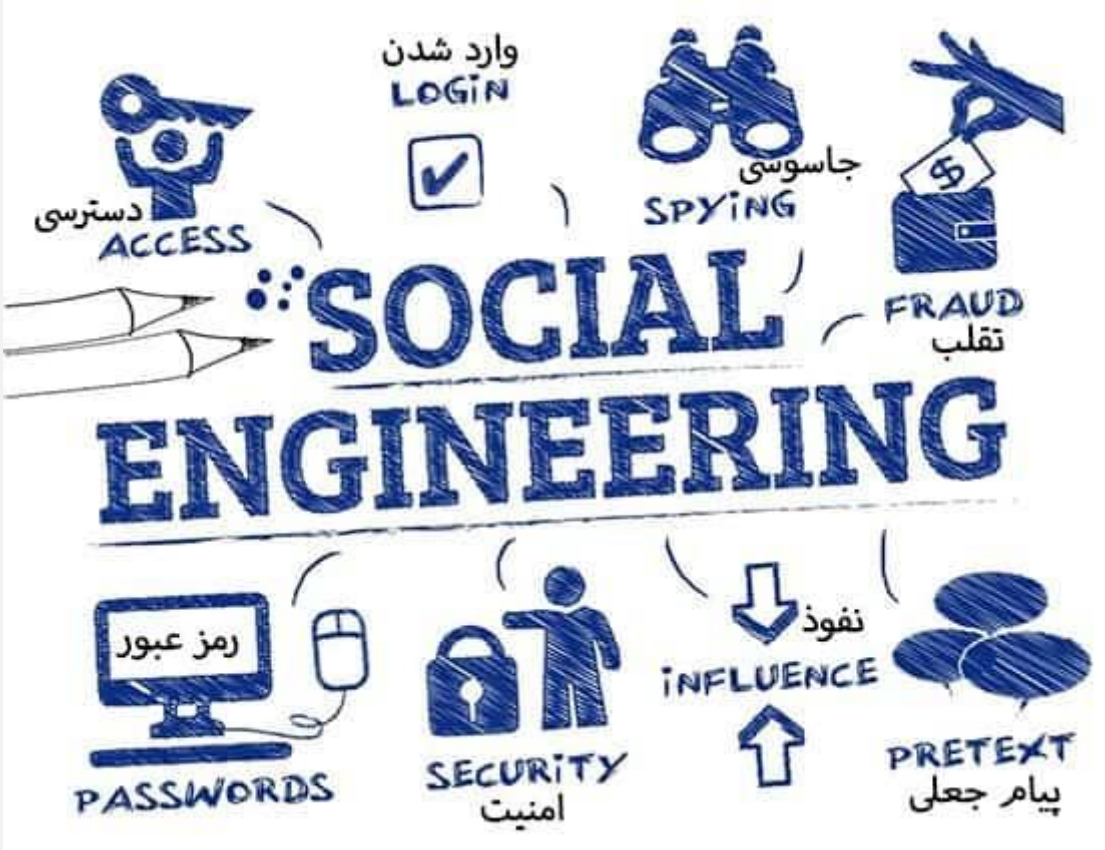
#۱-۳ بدافزارها (Malware)

یکی از حملات رایج سایبری، تهدید از طریق نرم افزار های مخرب است. این نوع از نرم افزار ها می توانند به هر نوع برنامه یا فایلی آسیب برسانند و یا آن را حذف کنند. هکرها از طریق بدافزارها به سیستم کاربران نفوذ می کنند و در برخی مواقع کنترل سیستم را بر عهده می گیرند. نفوذ بدافزارها از طریق باز کردن یک لینک، دانلود یک فایل از اینترنت و یا باز کردن یک ایمیل در سیستم مقصد صورت می گیرد.

#۲-۳ باج افزار ها (Ransomware)

همان طور که از نام آن مشخص است، هکرها پس از حمله به سیستم کامپیوتری یک فرد یا سازمان، امنیت سایبری را تخریب کرده، فایل ها و اطلاعات مهم را رمزگذاری می کنند و برای رمزگشایی فایل های قفل شده از کاربران سیستم های آسیب دیده باج دریافت می کنند.

#۳-۳ مهندسی اجتماعی (Social Engineering)



این نوع حمله مبتنی بر تعامل و ارتباط انسانی شکل می گیرد. بدین ترتیب که کاربران سیستم های مقصد با فریب خوردن بخش زیادی از اطلاعات مهم را در اختیار هکرها قرار می دهند. هکرها با نفوذ به لایه های امنیت سایبری، به اطلاعات محرمانه و مهم دست می یابند و کنترل سیستم در اختیار آن ها قرار می گیرد.

۳-٤# فیشینگ (Phishing)

حملات فیشینگ مشابه حملات مهندسی اجتماعی است. در این نوع حمله، هکرها با ارسال پیام یا ایمیل جعلی که شبیه به منابع و سازمان های معتبر است، به سیستم کاربران و لایه های محافظتی امنیت سایبری سیستم نفوذ کرده و اطلاعات مهم مانند رمز کارت اعتباری را دریافت می کنند.

#۳-۵ فیشینگ هدفمند (Spear Phishing)

در این مدل از فیشینگ، هدف اصلی تهدید یا حمله به امنیت سایبری یک سازمان، شرکت یا یک کاربر مشخص است.

#۳-۶ تهدیدهای داخلی امنیت سایبری (Insider Threats)

تهدیدها و حملات داخلی از سوی کارمندان، مشتریان یا سایر افراد فعال در یک سازمان و شرکت اتفاق می افتند. این دسته از تهدیدات می توانند به صورت غیرارادی یا سهوی روی دهند. در هر صورت خسارات زیادی از افشای اطلاعات و نفوذ به لایه های امنیت سایبری به جای می ماند.

#۳-۷ حملات دیداس (DDoS: Distributed Denial-Of-Service)

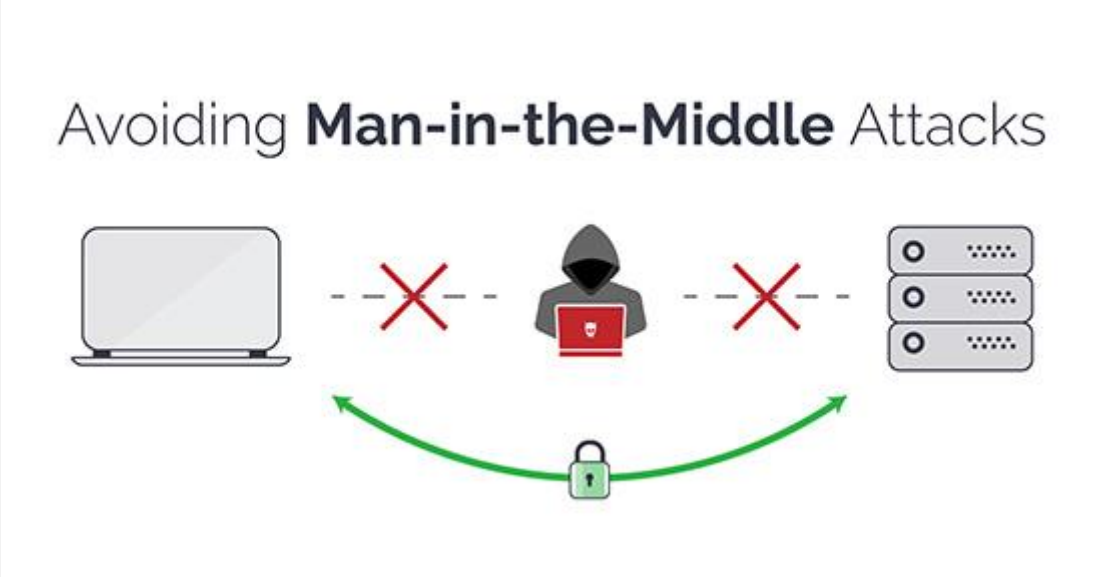
حمله دیداس سازمان یافته است و در آن چندین سیستم با تهدید یک سیستم، فعالیت آن را مختل می کنند و ترافیک سیستم هدف را مورد حمله قرار می دهند. این سیستم می تواند وب سایت، سرور، شبکه یا هر منبع مهم دیگری باشد. سیستم های حمله کننده با ارسال ایمیل و پیام زیاد، از سیستم مقصد درخواست های مختلف مانند اتصال یا باز کردن برخی برنامه ها و... را ارائه می کنند. بدین شکل فعالیت سیستم هدف کند می شود و یا به طور کلی از کار می افتد و از دسترسی به ترافیک های

رسمی و قانونی خارج می شود. در واقع تمام پروتکل ها و استراتژی های امنیت سایبری از بین می روند.

#۳-۸ تهدیدات پایدار پیشرفته (APTs: Advanced Persistent Threats)

این نوع حملات به صورت کاملاً هدفمند در مدت زمان طولانی صورت می گیرند. در واقع، هکرها با نفوذ به شبکه یک سازمان، اطلاعات آن ها را سرقت می کنند و به طور محرمانه به مدت طولانی در سیستم هدف باقی می مانند. آن ها در طول این مدت بخش زیادی از اطلاعات سیستم را حذف یا تخریب می کنند.

#۳-۹ حملات استراق سمع (MitM: Man-in-the-Middle)



حملات و تهدیدهای استراق سمع از طریق شکل گیری ارتباط بین دو طرف، یعنی پس از ارسال و دریافت پیام های مختلف بین دو طرف، صورت می گیرند. در نتیجه تمام قوانین و برنامه های راهبردی امنیت سایبری سیستم نیز تخریب می شوند.

#۴ افزایش امنیت سایبری

برای آن که سیستم از امنیت سایبری بالایی برخوردار باشد، بهتر است به نکات زیر بیشتر توجه شود. به خصوص اگر از آن دسته سازمان هایی هستید که اطلاعات مهم زیادی در سیستم های خود ذخیره می کنید، لازم است این موارد را حتما در نظر بگیرید:

- به روز رسانی نرم افزار ها و برنامه های کاربردی مهم
- استفاده از آنتی ویروس قوی و جدید
- فعال کردن فایروال
- رمزگذاری مطمئن و استفاده از ابزارهای مدیریت پسورد
- استفاده از سرویس تایید هویت چندعاملی
- پشتیبان گیری (Backup) از تمامی اطلاعات مهم
- ارزیابی ریسک
- ایجاد فضای امنیتی یکپارچه و قوی در سیستم
- بررسی منظم حساب های کاربری آنلاین

#۵ مهم ترین مزایای امنیت سایبری

با رشد فزاینده تعداد سیستم ها، کاربران و برنامه ها در سازمان های متعدد و مدرن، در کنار افزایش جامعه اطلاعاتی در فضای دیجیتال که اکثر آن ها بسیار محرمانه و حساس هستند، دستیابی به امنیت سایبری و اجرای پروتکل های آن بسیار مهم و پرسود است.

مزایای امنیت سایبری عبارت اند از:

- محافظت از اطلاعات مهم کسب و کار ها در برابر حملات سایبری
- مقابله با دسترسی های غیرمجاز و نفوذ هکرها
- تامین امنیت شبکه ها، داده ها، سرورها و دستگاه های دیجیتال
- ایجاد فضای مطمئن برای افزایش اعتبار برند یک شرکت
- بهبود و کاهش مدت زمان بازیابی اطلاعات