مدرس: دکتر مجتبی رفیعی

نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۴: شرح و توجیه اهداف حملات

علی خرمشاهی

۲۷ اسفند ۱۴۰۰

فهرست مطالب

۱ شرح و توجیه اهداف حملات

حملات با اهداف مختلفی ممکن است صورت بپذیرد که در ادامه نمونه‌هایی از آنها ذکر شده است:

۱. **حملات با اهداف سیاسی:** در چنین حملاتی معمولا حمله کننده سعی در تضعیف رقیب سیاسی خود دارد. به عنوان مثال یک کشور میتواند با حمله سایبری به زیرساخت‌های حساس و حیاتی یک کشور، زمینه تضعیف دولت قربانی را فراهم آورد

۲. **حملات با اهداف اقتصادی:** برخی از اهداف حمله کننده در چنین حملاتی: ضربه زدن به رقیب، کسب اطلاع از دادههای محرمانه و یا حتی کسب درآمد از طریق نامشروع است.

۳. **حملات با اهداف شخصی:** این نوع حملات بیشتر به منظور انتقام جویی به دلیل خصومتهای شخصی یا ابراز توامندی و اثبات آن صورت میگیرد.

نکته: نحوه برخورد با کسی که پتانسیل حمله را کشف کرده (آسیب پذیری در سیستم را می داند) می‌بایست با توجه به موارد زیر به طور مناسبی (گاه تند و گاه آرام) صورت گیرد.

۱. سازمانی که آسیب پذیری در آن کشف شده،

۲. فردی که آسیب پذیری را کشف کرده و وابستگی آن به سازمان،

۳. اهمیت آسیب پذیری و مخاطرات ناشی از آن و ....

ارائه گزارش‌های متنوع امنیتی به سازمان‌ها می‌تواند اهمیت این موضوع را برای آنها شفاف کند. در ادامه برخی از عناوین مهم برای تهیه چنین گزارش‌هایی را ذکر می کنیم.

۱. توجیه اینکه حوادث امنیتی میتواند در دو رده حوادث بدخواهانه/عمدی یا غیربد خواهانه/غیرعمدی باشد و در این راستا حوادث بدخواهانه برای سازمانهای با مقیاسهای مختلف(بزرگ، متوسط، کوچک)را در سالهای متوالی بر اساس منابع معتبر ارائه کنیم.

۲. انواع حوادث امنیتی بدخواهانه صورت پذیرفته در سازمانها را رتبهبندی کرده و براساس چندین سال متوالی ارایه کنیم. با این کار سازمانها میتوانند برای حوادث امنیتی محتمل در سازمان خود برنامهریزی کنند

۳. هزینه‌های محتمل برای یک حادثه سنگین امنیتی را در سالهای مختلف برای شرکت های با مقیاس بزرگ، کوچک، متوسط به تصویر کشیده و دلایل آن را به طور شفاف بررسی کنیم.

هزینه محتمل شده میتواند از مجموع هزینههای زیر حاصل شود:

- هزینه ضرر و زیان به برند شرکت،
- هزینه رفع مشکل،
- دارایی‌هایی که ممکن است از دست بدهد و ...

حملات از طریق بدافزارها به سامانه‌ها تحمیل می‌شود. بدافزار (Malware) به هر نوع نرم‌افزاری که از روی عمد برای آسیب زدن به کامپیوتر، سرور، کلاینت، یا شبکه رایانه‌ای معرفی شده است، اطلاق می‌شود. بدافزارها براساس پارامترهایی نظیر: نحوه عملکرد، نحوه توزیع، محیط هدف و .... دسته بندی می‌شوند. برخی از این دسته‌ها عبارتند از: ویروس‌های رایانه‌ای، کرم‌ها، تروجان‌ها، باج افزارها، آگهی افزارها و ... .