۷) شرح و توجیه اهداف حملات

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

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

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

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

باج افزارها (Ransomware) و سایت‌های جعلی صیادی (Fishing) ابزارهایی برای چنین حملاتی به‌شمار می‌آیند.

نکته: نحوه برخورد با کسی که پتانسیل حمله را کشف کرده (آسیب‌پذیری در سیستم رایانه) می‌باشد با توجه به موارد زیر به‌طور مناسبی (گاه تند و گاه آرام) صورت گیرد.

1. سازمان کر آسیب‌پذیری در آن کشف شده،
2. مزدی کر آسیب‌پذیری را کشف کرده و واکنش آن به سازمان،
3. اهمیت آسیب‌پذیری و خاطرات ناشی از آن و ...

۸) ارایه گزارش‌های مختصر (موضوع)

ارایه گزارش‌های مختصر به سازمان‌ها می‌تواند اهمیت این موضوع را برای آنها شفاف کند. در ادامه برخی از عناوین هم برای تهیه چنین گزارش‌هایی را ذکر می‌کنیم.

① توجیه اینکه حوادث می‌توانند در سازمان دو دسته حوادث بدخواهانه/عمدی یا غیر بدخواهانه/غیر عمدی باشند و در این راستا حوادث بدخواهانه برای سازمان‌ها با مقیاس‌های مختلف (بزرگ، متوسط، کوچک) را در سال‌های متوالی بر اساس منابع معتبر ارایه کنیم.

② انواع حوادث امنیتی بدخواهانه صورت پذیرفته در سازمان‌ها را رتبه‌بندی کرده و بر اساس چندین سال متوالی ارایه کنیم. با این کار سازمان‌ها می‌توانند برای حوادث امنیتی محتمل در سازمان خود برنامه‌ریزی کنند.

③ هزینه‌های محتمل برای یک حادثه سنگین امنیتی را در سال‌های مختلف برای شرکت‌های با مقیاس بزرگ، کوچک و متوسط برآورد کرده و دلایل آن را به طور شفاف بررسی کنیم.

هزینه محتمل شده می‌تواند از مجموع هزینه‌های زیر حاصل شود:

* هزینه فرار و زیان به برند شرکت،
* هزینه رفع مشکل،
* دارایی‌هایی که ممکن است از دست بروند و ...

⑨ 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 طراحی شده است، اطلاق می‌شود. انواع بدافزارها عبارتند از: ویروس‌های رایانه‌ای، کرم‌ها، تروجان‌ها، باج‌افزارها، جاسوس‌افزارها، آگهی‌افزارها و ...

انواع بدافزارها بر اساس پارامترهایی نظیر نحوه عملکرد، نحوه توزیع، محیط هدف و ... (مستقل از رایانه) دسته‌بندی می‌شوند.