Cyber Risk Assessment – DoS assignment

Home Assignment no 1

מגישות-

יובל אביטן- 319066007

ויקטוריה חליוסטוב- 320755481

בת חן אברהם- 316476985

Risk= likelihood \*impact

5- סבירות גבוהה ביותר

1- סבירות נמוכה ביותר

חלוקה למקרים:

1. נתונים:

שרת HTTP, וארגון עם מידע מסווג.

5\*5 = Risk

סבירות הסיכון הינה 5, מכיוון שזהו שרת HTTP שאינו מוגן.

ולכן הסבירות שההתקפה תתבצע גבוהה.

פוטנציאל הנזק הוא 5 מכיוון שמחשב יש מידע מסווג כגון: רפואי, ביטחוני, ממשלתי...

1. נתונים:

שרת HTTP, מחשב אישי ללא מידע מסווג.

5\*1 = Risk

סבירות הסיכון הינה 5 מכיוון שזהו שרת HTTP שאינו מוגן.

ולכן הסבירות שההתקפה תתבצע גבוהה.

פוטנציאל הנזק הוא 1 מכיוון שאין במחשב מידע מסווג.

במקרה ההתקפה שלנו מדובר במקרה מספר 2, מכיוון שהשתמשנו בשרת HTTP והקמנו אתר לוקאלית על המחשב שלנו שלא מכיל מידע מסווג.

הגנות:

1. הגבלת מספר הבקשות-

כאשר צמצמנו את מספר הבקשות סבירות ההתקפה ירדה מכיוון שהאתר הצליח לעלות.

על פי הערכתנו סבירות ההתקפה תרד ותהייה בין 2 ל-3 (תלוי במספר הבקשות שצמצמנו).

פוטנציאל הנזק לא ישתנה.

1. חסימת מספר הבקשות לפי IP-

כאשר יצרנו חסימה ל- IP מסוים אותו משתמש לא הצליח לגשת לאתר.

על פי הערכתנו סבירות ההתקפה תרד ותהייה בין 1 ל-2 (תלוי במיקום ובחיבור האינטרנט

מכיוון שה-IP של המחשב הוא דינאמי והתוקף יכול לשנות את הכתובת שלו).

פוטנציאל הנזק לא ישתנה.

1. חסימה על פי זמן-

כאשר יצרנו חסימה על פי זמן, באותה נקודת זמן מסוימת לא הייתה כלל גישה לאתר.

על פי הערכתנו סבירות ההתקפה תרד בין 3 ל-4 (תלוי בכמות השעות שהגדרנו לחסימת גישה לאתר).

פוטנציאל הנזק לא ישתנה.