מגישים : אלון טפליצקי 209198738 שגיא בירן 205620859

Cyber Risks Assessment Denial-of-Service Exercise

מתקפת DOS הינה מתקפה שנועדה "להקריס" מכונה או רשת, מה שהופך אותה לבלתי נגישה למשתמשים המיועדים לה. התקפות DoS משיגות מטרות אלה על ידי הצפת המטרה בתנועה (traffic), או שליחת מידע הגורם להתרסקות.

נציג וננתח הוכחת נכונות (POC) של שרת נתקף ושרת מוגן מפני התקפת DoS וזאת באמצעות Script אשר יסמלץ תקיפה לשרת באופן תדיר כדי להעמיס עליו ואף לגרום להפלתו.

השרת ממומש ב NodeJS ויכיל ספריות לצורך ביצוע ההגנה. בנוסף, שרת זה רץ ע"ג Docker אשר מסמלץ סביבה מבודדת, כדי שנוכל לבסוף להגביל את המשאבים בסביבה זו.

הערכת סיכוני סייבר:

נעריך את סיכוני הסייבר על השרת באמצעות 2 מאפיינים:

1. סבירות ההתקפה.
2. פוטנציאל הנזק.

לסיכום נבצע מכפלה בין ערכי המאפיינים ונסיק את ערכם של הסיכונים על השרת (לפי מדד NIST).

1. <u>שליחת מספר רב של בקשות לשרת</u>

<u>סבירות ההתקפה:</u>

השרת (כאשר אינו מכיל אמצעי הגנה) הוגדר לקבל כמות בקשות (Requests) שאינה מוגבלת ותלויה אך ורק במשאבי המערכת עצמה, לכן קיימת חולשה של מתקפת DoS כאשר תוקפים ינסו לשלוח מספר רב של בקשות אל השרת, תרחיש אשר עלול להוביל לקריסתו ואף מניעת מתן שירותים שונים ללקוחות.

לאור הנקודות שהועלו רמת הסבירות שמתקפה זו תתרחש במערכת היא **4**.

<u>פוטנציאל הנזק:</u>

המערכת שלנו מכילה שרת אחד שדרכו המשתמשים ניגשים לאתר ולכן הנזק שעלול להיגרם ע"י מתקפת DoS היא השבתת הפעילות התקינה של המערכת עד לביצוע אתחול של השרת.

בעקבות כך פוטנציאל הנזק הוא:

- פגיעה במוניטין של המערכת ונטישת לקוחות - משתמשים יחפשו חלופות אחרות לגשת למידע הדרוש.
- פגיעה בזמינות המידע במערכת- ע"י כך שמשתמשים לא יוכלו לגשת לאתר.

לאור הנקודות שהועלו פוטנציאל הנזק שמתקפה זו תגרום הוא **4**.

<u>לסיכום רמת הסיכון שמתקפה זו תתרחש לפי מדד NIST הינה - 16.</u>

1.1 <u>הגבלת מספר הבקשות על השרת</u>

<u>סבירות ההתקפה:</u>

השרת (כאשר מכיל אמצעי הגנה) הוגדר לקבל כמות בקשות (Requests) מוקצית מראש בחלון הזמן, בקשות שיחרגו מתנאים אלו ידחו אוטומטית ולא יוקצו להם משאבי מערכת. תוקפים אשר ינסו לשלוח מספר רב של בקשות אל השרת ייחסמו וגישתם למשאבי השרת תהיה בלתי זמינה.

לאור הנקודות שהועלו רמת הסבירות שמתקפה זו תתרחש במערכת היא **4**.

<u>פוטנציאל הנזק:</u>

המערכת שלנו מכילה שרת אחד שדרכו המשתמשים ניגשים לאתר ולכן הנזק שעלול להיגרם ע"י מתקפת DoS היא השבתת הפעילות התקינה של המערכת עד לביצוע אתחול של השרת.
בעקבות כך פוטנציאל הנזק הוא:

- פגיעה במוניטין של המערכת ונטישת לקוחות - משתמשים יחפשו חלופות אחרות לגשת למידע הדרוש.
- פגיעה בזמינות המידע במערכת- ע"י כך שמשתמשים לא יוכלו לגשת לאתר.

לאור הנקודות שהועלו פוטנציאל הנזק שמתקפה זו תגרום הוא **2**.

לסיכום רמת הסיכון שמתקפה זו תתרחש לפי מדד NIST הינה - 8.

2. שליחת בקשות ממדינות זרות

סבירות ההתקפה:
כיום, כל לקוח בעל חיבור אינטרנטי יכול לגלוש אל שרתים מחוץ למדינתו (בהנחה שאינו מוגבל ע״י ה-ISP) לכן, קיים חשש למתקפות סייבר על רקע פוליטי ו/או מדיני.
השרת (כאשר אינו מכיל אמצעי הגנה) חשוף לתקיפות מניעת שירות ע״י האקרים מרחבי העולם.
לאור הנקודות שהועלו רמת הסבירות שמתקפה זו תתרחש במערכת היא **3**.

פוטנציאל הנזק:
המערכת שלנו אינה מבצעת אימות בסיסי של לקוחות ומאפשרת לכל לקוח להיכנס למערכת, תרחיש אשר עלול להוביל לפוטנציאל נזק של:

- קריסת השרת ומניעת פעילותו התקינה.
- גניבת מידע חשוף והפצתו בעתיד.

לאור הנקודות שהועלו פוטנציאל הנזק שמתקפה זו תגרום הוא **4**.

לסיכום רמת הסיכון שמתקפה זו תתרחש לפי מדד NIST הינה - 12.

2.1 חסימה בקשות לפי כתובות IP ומיקום גאוגרפי

סבירות ההתקפה:
כיום, כל לקוח בעל חיבור אינטרנטי יכול לגלוש אל שרתים מחוץ למדינתו (בהנחה שאינו מוגבל ע״י ה-ISP) לכן, קיים חשש למתקפות סייבר על רקע פוליטי ו/או מדיני.
השרת (כאשר מכיל אמצעי הגנה) אינו חשוף לתקיפות ממדינות שונות (לאור העובדה כי מיפוי כתובות ה-IP ביחס למיקום הגיאוגרפי אינו תמיד עדכני/מדויק, ייתכנו מצבים שבהם יעשה שימוש בכתובות IP על-ידי גורמים מחוץ למדינות המוגדרות, למרות שהרישום יעיד כי כתובות אלו משויכות למדינות המוגדרות.)
לאור הנקודות שהועלו רמת הסבירות שמתקפה זו תתרחש במערכת היא **3**.

פוטנציאל הנזק:
המערכת שלנו מבצעת אימות בסיסי של לקוחות המבקשים להתחבר לשרת ומאפשרת ללקוח גישה רק במידה וכתובת ה IP שלו תואמת לרשימת כתובות (ע״פ כתובות של מדינה או רשימת כתובות ידנית) המאושרים בשרת.
אך קיימת סבירות לעקוף את אמצעי ההגנה הזה בכלים פשוטים כגון שירותי VPN, תרחיש אשר עלול להוביל לפוטנציאל נזק של:

- קריסת השרת ומניעת פעילותו התקינה.
- גניבת מידע חשוף והפצתו בעתיד.

לאור הנקודות שהועלו פוטנציאל הנזק שמתקפה זו תגרום הוא **4**.

לסיכום רמת הסיכון שמתקפה זו תתרחש לפי מדד NIST הינה - 12.

3. שימוש במשאבי מערכת מוגבלים

סבירות ההתקפה:
כיום כדי לתחזק מערכות בעלות משאבים רבים נדרשת יכולת כספית גבוהה, לכן חברות קטנות אינן יכולות להרשות לעצמן שימוש במשאבים רבים (לדוגמא: CPU, GPU, Memory …) תרחיש אשר "מעודד" תקיפת שרתים קטנים וחלשים אשר אינו דורש צריכת משאבים רבה מצד התוקף.
לאור הנקודות שהועלו רמת הסבירות שמתקפה זו תתרחש במערכת היא **3**.

פוטנציאל הנזק:
מערכות בעלות מספר מצומצם של משאבים אינן יכולות להתמודד עם הקצאה משאבים מרובה להתקפה ובעת מתקפה על שרתיהן הן נשארות חשופות, חדירות ללא אפשרות מענה כנגד תקיפות.
לאור הנקודות שהועלו פוטנציאל הנזק שמתקפה זו תגרום הוא **4**.

לסיכום רמת הסיכון שמתקפה זו תתרחש לפי מדד NIST הינה - 12.

3.1 שימוש במשאבי מערכת מוגדלים

סבירות ההתקפה:
במערכות בעלי משאבים מרובים התוקף יזדקק למס' משאבים זהה ואף גבוהה בשביל לגרום נזק לשרת הנתקף, כלומר ככל שהשרתים יהיו "חזקים" יותר תרחיש של ניצול משאבי מערכת יהיה קשה מצד התוקף אשר יזדקק למשאבים רבים דבר אשר יקשה על פעילותו.
לאור הנקודות שהועלו רמת הסבירות שמתקפה זו תתרחש במערכת היא **2**.

פוטנציאל הנזק:
מערכות בעלות מספר רב של משאבים יהיו מסוגלות להתמודד כנגד תקיפות מכיוון שלמרבית התוקפים יהיה מאוד קשה להתגבר על אותם מערכות (שרתים) דבר שעלול לגרור תהיות אצל התוקף האם כדאיות התקיפה משתלמת לו כלל.
לאור הנקודות שהועלו פוטנציאל הנזק שמתקפה זו תגרום הוא **3**.

לסיכום רמת הסיכון שמתקפה זו תתרחש לפי מדד NIST הינה - 6.