ניתוח איומים
באמצעות מודל
STRIDE/DREAD

מגישים:

משה כרמל
מישל רם
שרון

מודל STRIDE/DREAD הוא שיטה לזיהוי וניתוח איומים פוטנציאליים על מערכת.

S - Spoofing
T - Tampering
R - Repudiation
I - Information Disclosure
D - Denial of Service
E - Elevation of Privilege

מודל DREAD הוא גרסה של STRIDE המתמקדת בהשפעה הפוטנציאלית של איומים אלו.

D - Damage - נזק
R - Reproducibility - יכולת שחזור
E - Exploitability - ניצול
A - Affected Users - משתמשים מושפעים
D - Discoverability - יכולת גילוי

Spoofing

תוקף יכול לנסות להתחזות למשתמש לגיטימי כדי לקבל גישה למשאבים מוגבלים, כגון מידע על לקוחות.

נזק: גבוה - אם תוקף מצליח לקבל גישה למידע רגיש של לקוחות, זה עלול להוביל לפגיעה כספית או מוניטין של החברה ולקוחותיה.

יכולת שחזור: נמוכה – סוג זה של תקיפה ידרוש כמות משמעותית של מאמץ לביצוע, שכן התוקף יצטרך לאסוף מספיק מידע על המשתמש הלגיטימי על מנת להתחזות לו באופן משכנע.

ניצול: בינוני - בעוד שהתוקף יצטרך לאסוף מידע על המשתמש הלגיטימי כדי לבצע את ההתקפה הזו, הוא עשוי לעשות זאת באמצעות טכניקות של הנדסה חברתית או על ידי השגת אישורי הכניסה של המשתמש באמצעים אחרים (כגון דיוג או תוכנות זדוניות).

משתמשים מושפעים: גבוה - אם תוקף מצליח להתחזות למשתמש לגיטימי, כל המשאבים שאליהם יש למשתמש גישה עלולים להיפגע.

יכולת גילוי: נמוכה - ייתכן שסוג ההתקפה הזה לא יהיה מורגש באופן מיידי, מכיוון שהתוקף ינסה להתחזות כמשתמש לגיטימי.

אמצעי נגד: הטמע אמצעי אימות חזקים, כגון אימות דו-גורמי, כדי להקשות על התוקפים להתחזות למשתמשים לגיטימיים. סקור ועדכן באופן קבוע את הרשאות המשתמש כדי להבטיח שרק למשתמשים מורשים תהיה גישה למשאבים רגישים.

Tampering

תוקף יכול לנסות לשנות נתונים או משאבים בתוך המערכת כדי להשיג מטרה זדונית כלשהי.

נזק: גבוה - בהתאם לנתונים או המשאבים המשתנים, לתקיפה מסוג זה עשויות להיות השלכות משמעותיות על החברה ולקוחותיה.

יכולת שחזור: נמוכה - סוג זה של תקיפה ידרוש כמות משמעותית של מאמץ לביצוע, שכן התוקף יצטרך לקבל גישה למערכת ולשנות את הנתונים או המשאבים המדוברים.

ניצול: בינוני - בעוד שהתוקף יצטרך לקבל גישה למערכת כדי לבצע את ההתקפה הזו, הוא עשוי לעשות זאת באמצעות פרצות באפליקציית האינטרנט או על ידי השגת אישורי כניסה באמצעים אחרים (כגון פישינג או תוכנות זדוניות).

משתמשים מושפעים: גבוה - אם תוקף מצליח לשנות נתונים או משאבים בתוך המערכת, זה עלול להשפיע על מספר רב של משתמשים.

יכולת גילוי: נמוכה - ייתכן שהתקיפה מסוג זה לא תהיה מורגשת מיד, מכיוון שהתוקף עשוי לבצע שינויים עדינים בנתונים או במשאבים על מנת להשיג את מטרתו.

אמצעי נגד: הטמעת אמצעי אבטחה חזקים כדי להגן מפני גישה לא מורשית למערכת, כגון חומות אש ומערכות זיהוי פריצות. סקור ועדכן בקביעות את בקרות הגישה כדי להבטיח שרק למשתמשים מורשים יש את היכולת לשנות נתונים או משאבים בתוך המערכת.

Repudiation

תוקף יכול לנסות להכחיש שהוא ביצע פעולה ספציפית בתוך המערכת, מה שמקשה להטיל עליו דין וחשבון.

נזק: גבוה - אם תוקף מצליח להכחיש שהוא ביצע פעולה ספציפית, זה עלול להקשות על להטיל עליו דין וחשבון על כל נזק שהוא עלול לגרום.

יכולת שחזור: נמוכה - סוג זה של תקיפה ידרוש כמות משמעותית של מאמץ לביצוע, שכן התוקף יצטרך לכסות בהצלחה את עקבותיו וליצור ראיות כוזבות כדי לתמוך בהכחשתו.

יכולת ניצול: נמוכה - סוג זה של התקפה ידרוש כמות משמעותית של ידע ומשאבים כדי לבצע בהצלחה.

משתמשים מושפעים: גבוה - אם תוקף מצליח להכחיש שהוא ביצע פעולה מסוימת, זה עלול להשפיע על מספר רב של משתמשים.

יכולת גילוי: נמוכה - ייתכן שהתקיפה מסוג זה לא תהיה מורגשת באופן מיידי, מכיוון שהתוקף עלול לטשטש את עקבותיו כדי ליצור ראיות כוזבות כדי לתמוך בהכחשתו.

אמצעי נגד: יישום אמצעים למעקב ורישום של פעילות המשתמשים בתוך המערכת, על מנת לספק ראיות לפעולות שנעשו. סקור ועדכן בקביעות את בקרות הגישה כדי להבטיח שרק למשתמשים מורשים יש את היכולת לבצע פעולות ספציפיות בתוך המערכת. עקוב אחר המערכת לאיתור פעילות חריגה ונקוט פעולה מתאימה במידת הצורך. זה עשוי גם להיות מועיל ליישם אמצעים לחינוך והכשרת עובדים לגבי הסיכונים של התנערות וכיצד למנוע זאת.

Information Disclosure

תוקף עלול לנסות להשיג גישה בלתי מורשית למידע רגיש, כגון נתוני לקוחות או מידע קנייני של החברה.

נזק: גבוה - אם תוקף מצליח לקבל גישה למידע רגיש, זה עלול להוביל לפגיעה כלכלית או במוניטין של החברה ולקוחותיה.

יכולת שחזור: נמוכה – סוג זה של תקיפה ידרוש כמות משמעותית של מאמץ לביצוע, שכן התוקף יצטרך לקבל גישה למערכת ולאתר את המידע הרגיש המדובר.

ניצול: בינוני - בעוד שהתוקף יצטרך לקבל גישה למערכת כדי לבצע את ההתקפה הזו, הוא עשוי לעשות זאת באמצעות פרצות באפליקציית האינטרנט או על ידי השגת אישורי כניסה באמצעים אחרים (כגון פישינג או תוכנות זדוניות).

משתמשים מושפעים: גבוה - אם תוקף מצליח להשיג גישה למידע רגיש, זה עלול להשפיע על מספר רב של משתמשים.

יכולת גילוי: נמוכה - ייתכן שהתקיפה מסוג זה לא תהיה מורגשת באופן מיידי, מכיוון שהתוקף עלול לגשת למידע מבלי להשאיר ראיות גלויות.

אמצעי נגד: הטמעת אמצעי אבטחה חזקים כדי להגן מפני גישה לא מורשית למערכת, כגון הצפנה ובקרות גישה. סקור ועדכן באופן קבוע את הרשאות המשתמש כדי להבטיח שרק למשתמשים מורשים תהיה גישה למשאבים רגישים.

Denial of Service

תוקף עלול לנסות לשבש את הזמינות של מערכת האינטרנט, ולהפוך אותה ללא זמינה למשתמשים לגיטימיים.

נזק: גבוה - אם מערכת האינטרנט אינה זמינה, עלולות להיות לכך השלכות משמעותיות על החברה ולקוחותיה.

יכולת שחזור: גבוהה – קל יחסית לשחזר סוג זה של התקפה, שכן התוקף יכול פשוט לשלוח מספר רב של בקשות לשרת האינטרנט על מנת להציף אותו ולשבש את זמינותו.

ניצול: גבוה - סוג זה של תקיפה קל יחסית לביצוע, שכן הוא דורש ידע או משאבים מינימליים.

משתמשים מושפעים: גבוה - אם מערכת האינטרנט אינה זמינה, כל משתמשי המערכת יושפעו.

יכולת גילוי: גבוהה - בדרך כלל קל לגלות סוג זה של התקפה, מכיוון שהיא גורמת למערכת האינטרנט להיות בלתי זמינה.

אמצעי נגד: הטמעת אמצעים להגנה מפני התקפות מניעת שירות, כגון הגבלת קצב והגנת מניעת שירות מבוזרת (DDoS). עקוב אחר מערכת האינטרנט לאיתור פעילות חריגה ונקוט פעולה מתאימה במידת הצורך.

Elevation of Privilege

תוקף יכול לנסות לקבל גישה להרשאות או משאבים שאינם מורשים לגשת אליהם.

נזק: גבוה - אם תוקף מצליח לקבל גישה להרשאות או משאבים לא מורשים, זה עלול להוביל לפגיעה כלכלית או במוניטין של החברה ולקוחותיה.

יכולת שחזור: נמוכה - סוג זה של תקיפה ידרוש כמות משמעותית של מאמץ לביצוע, שכן התוקף יצטרך לקבל גישה למערכת ולאתר את ההרשאות או המשאבים הלא מורשים המדוברים.

ניצול: בינוני - בעוד שהתוקף יצטרך לקבל גישה למערכת כדי לבצע את ההתקפה הזו, הוא עשוי לעשות זאת באמצעות פרצות באפליקציית האינטרנט או על ידי השגת אישורי כניסה באמצעים אחרים (כגון פישינג או תוכנות זדוניות).

משתמשים מושפעים: גבוה - אם תוקף מצליח להשיג גישה להרשאות או משאבים לא מורשים, זה עלול להשפיע על מספר רב של משתמשים.

יכולת גילוי: נמוכה - ייתכן שהתקיפה מסוג זה לא תהיה מורגשת באופן מיידי, מכיוון שהתוקף עלול לגשת להרשאות או משאבים לא מורשים מבלי להשאיר ראיות גלויות.

אמצעי נגד: הטמע אמצעי אבטחה חזקים כדי להגן מפני גישה לא מורשית למערכת, כגון חומות אש ובקרות גישה. סקור ועדכן באופן קבוע את הרשאות המשתמש כדי להבטיח שרק למשתמשים מורשים תהיה גישה להרשאות ולמשאבים הדרושים. עקוב אחר המערכת לאיתור פעילות חריגה ונקוט פעולה מתאימה במידת הצורך.