סקר סיכונים

גלופת לימוד

סקר הסיכונים הינו תהליך הכרחי להגדרת מדיניות אבטחת מידע משמעותית התואמת את מטרות הארגון. הסקר כולל אוסף של פעילויות המפורטות להלן

תוכן העניינים

1. כללי

התהליך של סקר סיכונים נועד לזהות סיכונים קיימים לנכסי המידע ולמערכות המחשב של הארגון, בהתבסס על איומים ידועים, חולשות במערכות ואמצעי אבטחה קיימים. לאחר זיהוי הסיכונים, מתבצעת הערכה של השפעתם לדרישות העסקיות של הארגון בהיבט אמינות (Integrity), חיסיון (Confidentiality) וזמינות (Availability) המידע. במסגרת התהליך נערך תיעדוף (Prioritization) של הנכסים בהתאם לערכם העסקי ורמת ההגנה הנדרשת.

סקר הסיכונים הינו תהליך הכרחי להגדרת מדיניות אבטחת מידע משמעותית התואמת את מטרות הארגון. הסקר כולל אוסף של פעילויות, כמפורט להלן:

- מיפוי תהליכים ארגוניים.
- מיפוי וניתוח מערכת.
- מיפוי וניתוח אבטחה.
- סיכום והמלצות.

1.1 מיפוי תהליכים ארגוניים

מטרת מיפוי התהליכים הארגוניים היא לתת תמונה מדויקת ככל שניתן לתהליכים הארגוניים הנתמכים ע"י מערכות המחשוב. ניתוח זה מתבצע באמצעות ראיונות של אנשי הארגון האמונים על תחום זה.

1.2 מיפוי וניתוח מערכת

מטרת ניתוח המערכת היא לזהות ולתעד את משאבי המחשוב של הארגון, את הישויות ואת הפעילויות אותן הן מבצעות. ניתוח זה מתבצע באופן הבא:

- מיפוי וניתוח תשתיות.
- מיפוי וניתוח יישומים.

1.3 מיפוי וניתוח תשתיות

מיפוי תשתיות יבוצע באופן הבא:

- מיפוי מערכות התקשורת.
- מיפוי שרתים.
- מיפוי מערכות קצה.
- מיפוי תוכנות תשתית.
- מיפוי ממשקים.
- מיפוי מערכות ניטור ובקרה.
- מיפוי מערכות אבטחה.

1.3.1 מיפוי מערכות תקשורת

מטרת מיפוי מערכות התקשורת היא לתת תמונה מדויקת של מבנה ואופי מערכות התקשורת בארגון. מיפוי זה יתבצע באמצעות ראיונות עם אנשי התקשורת של הארגון. תוצר המיפוי יהיה שרטוטי רשתות התקשורת וסוגי הציודים המחוברים.

1.3.2 מיפוי שרתים

מטרת מיפוי השרתים היא לתת תמונה מדויקת של ה-"קופסאות" המותקנות בארגון, של אופיין ומיקומן ברשת. מיפוי זה יתבצע באמצעות ראיונות עם אנשי ה- System של הארגון. תוצר המיפוי יהיה רישום התחנות, מערכות ההפעלה שלהן, תפקידיהן ומיקומן ברשת.

1.3.3 מיפוי מערכות קצה

מטרת מיפוי מערכות הקצה היא לתת תמונה מדויקת של סוגי מערכות הקצה (מחשבים אישיים, מחשבים נישאים וכו'), אופיים ומיקומם ברשת. מיפוי זה יתבצע באמצעות ראיונות עם אנשי ה- System של הארגון. תוצר המיפוי יהיה רישום התחנות, מערכות ההפעלה שלהן, תפקידיהן ומיקומן ברשת.

1.3.4 מיפוי תוכנות תשתית

מטרת מיפוי תוכנות התשתית היא לתת תמונה מדויקת של תוכנות התשתית המותקנות על השרתים ומערכות הקצה השונות (מערכות הפעלה, שרתי דוא"ל, שרתי מסד נתונים וכו'). מיפוי זה יתבצע באמצעות ראיונות עם אנשי ה- System של הארגון. תוצר המיפוי יהיה רישום התוכנות התשתיתיות המותקנות על כל השרתים ומערכות הקצה.

1.3.5 מיפוי ממשקים

מטרת מיפוי הממשקים היא לתת תמונה מדויקת של הממשקים בין מערכות המחשוב בארגון למערכות מחשוב אחרות, פנימיות או חיצוניות. מיפוי זה יתבצע באמצעות ראיונות עם אנשי מערכות המידע של הארגון. תוצר המיפוי יהיה רשימה של הממשקים, אופיים, המערכות המשיקות והטכנולוגיה הכללית עליה הם מבוססים (למשל העברת קבצים באמצעות FTP).

1.3.6 מיפוי מערכות ניטור ובקרה (נו"ב)

מערכות ניטור ובקרה הן מערכות הממוקמות בלב תשתית המערכות. מטרת מיפוי מערכות הנו"ב היא לתת תמונה מדויקת לגבי מערכות הנו"ב המותקנות. מיפוי זה יבוצע באמצעות ראיונות עם אנשי ה- System של הארגון. תוצר המיפוי יהיה רשימה של מערכות נו"ב, אופיין, המערכות אותן הן מנטרות, הטכנולוגיה הכללית עליהן הן מבוססות ויכולותיהן.

1.3.7 מיפוי מערכות אבטחה

מטרת מיפוי מערכות האבטחה היא לתת תמונה מדויקת של מערכות האבטחה הייעודיות המיושמות בארגון. מיפוי זה יבוצע באמצעות ראיונות עם אנשי ה- System של הארגון. תוצר המיפוי יהיה רשימת מערכות האבטחה, אופיין והמקומות בהם הן מותקנות.

1.4 מיפוי וניתוח יישומים

ניתוח יישומים יבוצע לגבי יישומים מרכזיים בארגון. ניתוח זה יבוצע באופן הבא:

- מיפוי תהליכים מרכזיים.

- ניתוח זרימת המידע דרך רכיבי המערכת בתהליכים השונים.

1.4.1 מיפוי תהליכים מרכזיים

מטרת מיפוי התהליכים היא לתת תמונה של התהליכים העיקריים המבוצעים ע״י היישומים המרכזיים המופעלים בארגון. מיפוי זה יבוצע באמצעות ראיונות עם אנשי מערכות המידע של הארגון. תוצר המיפוי יהיה רשימת תהליכים עיקריים עבור היישומים המרכזיים בארגון.

1.4.2 ניתוח זרימת מידע

מטרת ניתוח זרימת המידע הוא לתת תמונה מדויקת של האופן בו מתבצעות הפעילויות של התהליכים. מיפוי זה יבוצע באמצעות ראיונות עם אנשי מערכות המידע של הארגון. תוצר המיפוי יהיה תיאור זרימת המידע בין המשאבים השונים בתהליכים שמופו.

2. מיפוי וניתוח האבטחה

ניתן להתייחס לתהליכי עבודה ממוחשבים כאל ישויות המבצעות פעילויות (גישות) על משאבים, כאשר:

- ישויות: מוגדרות כמשתמשים אינטראקטיביים או מודולי תוכנה (תהליכים וכו׳).
- פעילויות: מוגדרות כגישות לביצוע קריאה, כתיבה והרצה.
- משאבים: קבצים/נתונים, שיח (Session) ועיבוד (Processing).

אבטחת מידע, כשמירה על סודיות, זמינות ואמינות הנתונים, מבוצעת בפן הטכני, ע״י יישום מנגנוני בקרה על המשאבים והגישות אליהם:

- מנגנוני בקרת תצורה.
- מנגנוני אימות.
- מנגנוני בקרת גישה.
- מנגנוני תקפות.
- מנגנוני רישום.
- מנגנוני מעקב אבטחת מידע.
- מנגנוני המשכיות.

מטרת ניתוח האבטחה היא לתת תמונה מדויקת אודות אופן יישום מנגנוני הבקרה האבטחתיים (מנגנוני האבטחה) על הגישות למשאבים השונים.

ניתוח האבטחה ייעשה על מדגם מייצג של מערכות תקשורת, שרתים, מערכות קצה ויישומים.

2.1 מנגנוני בקרת תצורה (Configuration)

מנגנוני בקרת תצורה הם מנגנונים שתפקידם שמירה על עדכניות ותאימות של גרסאות התוכנה/הקושחה המותקנות במערכת.

2.2 מנגנוני אימות (Authentication)

מנגנוני אימות הם מנגנונים שתפקידם וידוא זהותה של ישות (משתמש או תהליך).

לדוגמא: מנגנון הקולט ממשתמש שם חשבון וסיסמא.

2.3 מנגנוני בקרת גישה (Access Control)

מנגנוני בקרת גישה הם מנגנונים המנהלים והמבצעים את פעולות מידור הגישה של ישויות למשאבים.

לדוגמא: מנגנון הממדר פעילויות שונות על קבצים (קריאה, כתיבה וכו') עפ"י מזהה חשבון, הקיים כחלק מובנה משרתי קבצים. דוגמא נוספת: Firewall הממדר פעילות של העברת נתונים בתקשורת בין ישויות עפ"י כתובת ה- IP של התחנות עליהן הן נמצאות.

2.4 מנגנוני תקפות (Validation)

מנגנוני תקפות הם מנגנונים המבצעים בדיקה ואישור תכונות של נתונים.

לדוגמא: מנגנון המאשר שקובץ הגיע בשלמותו ללא שינוי ושהוא נכתב ע"י מחבר מסוים - מנגנון חתימה אלקטרונית. דוגמא נוספת היא מנגנון המאשר שבקובץ לא קיים קוד עוין (אנטי-וירוס).

2.5 מנגנוני רישום (Logging)

מנגנוני רישום הם מנגנונים המבצעים תיעוד של ביצוע פעילויות או של ניסיונות כושלים לביצוען.

לדוגמא: מנגנון המבצע רישום גישות מוצלחות לקבצים שהוא חלק ממערכת ההפעלה Windows 2000.

2.6 מנגנוני מעקב אבטחת מידע (Auditing)

מנגנוני מעקב אבטחה הם מנגנונים המזהים פעילות החשודה כתקיפה של מערכת המידע ומעבירים הודעות על כך בצורות שונות (למשל שליחת ביפר או דואר אלקטרוני לאחראי האבטחה).

דוגמא למנגנון כזה הוא תוכנת Snort המבצעת זיהוי של פעילות חשודה על רשתות תקשורת.

2.7 מנגנוני המשכיות (Continuity)

מנגנוני המשכיות הם מנגנונים שתפקידם להבטיח פעילות רציפה של מערכות במקרה של בעיות. דוגמא למנגנון מסוג זה הוא מנגנון גיבוי המאפשר שיחזור מערכת והפעלתה מחדש במקרה של פגיעה בדיסק.

ניתוח האבטחה באמצעות ראיונות עם אנשי התקשורת, ה- System, אבטחת מידע ומערכות המידע של הארגון, וביצוע בדיקות אבטחה טכניות בהתאם לנושאים השונים.

3. סיכום ומסקנות - תוצרים

לאחר סיום שלבי המיפוי המפורטים לעיל, יתועדו וינותחו הממצאים, יגובשו המלצות ויוגשו המסמכים הבאים:

- תקציר מנהלים.
- מסמך ניתוח מערכת.
- מסמך ניתוח סיכונים.
- מסמך המלצות לשיפור רמת האבטחה עפ"י סדר עדיפות.

לאחר גיבוש מסמכים אלה, ניתן לגשת למלאכת עיצוב וכתיבת מדיניות אבטחת מידע המתאימה לארגון.

3.1 תקציר של תהליכי סקר הסיכונים

להלן תיאור תהליך העבודה לביצוע הפעילויות שתוארו לעיל:

פעילות	תת-פעילות
מנהלה	תכנון הפרויקט
	ניהול שוטף
איסוף נתונים	מיפוי תהליכים ארגוניים
	מיפוי תשתיות
	מיפוי מערכות תקשורת
	מיפוי שרתים
	מיפוי מערכות קצה
	מיפוי תוכנות תשתית
	מיפוי ממשקים
	מיפוי מערכות אבטחה
	מיפוי מערכות נו"ב
	ניתוח יישומים ארגוניים – מיפוי תהליכים
	ניתוח יישומים ארגוניים – מיפוי זרימת מידע
	מיפוי תהליכי אבטחה ארגוניים
ניתוח נתונים	איתור חולשות בארכיטקטורה
	איתור חולשות בתהליכים ארגוניים
	איתור חולשות ביישום מנגנוני אבטחה
	בניית מדגם לבדיקות טכניות
בדיקות טכניות	סריקת פורטים
	בדיקת מערכות תקשורת (מדגם מייצג)
	בדיקת שרתים (מדגם מייצג)
	בדיקת יישומים (מדגם מייצג)
תיעוד	תיעוד הניתוח
	תיעוד ממצאים טכניים
	כתיבת מסמך המלצות
	אפיון פתרונות טכניים
סיכומים	בנייה וביצוע מצגות