סקר סיכונים

מסגרת זו תוחלף בהבהקים העיקריים של ה...., לפי שיקול דעת כותב המסמך ובהתאם לכללים הנהוגים בארגון.

**שימוש בגלופה זו מותנה ברישוי מפת"ח**

תוכן העניינים

[1. כללי 2](#_Toc416255824)

[1.1 מיפוי תהליכים ארגוניים 2](#_Toc416255825)

[1.2 מיפוי וניתוח מערכת 2](#_Toc416255826)

[1.3 מיפוי וניתוח תשתיות 2](#_Toc416255827)

[1.4 מיפוי וניתוח יישומים 2](#_Toc416255828)

[2. מיפוי וניתוח האבטחה 3](#_Toc416255829)

[2.1 מנגנוני בקרת תצורה (Configuration) 3](#_Toc416255830)

[2.2 מנגנוני אימות (Authentication) 3](#_Toc416255831)

[2.3 מנגנוני בקרת גישה (Access Control) 3](#_Toc416255832)

[2.4 מנגנוני תקפות (Validation) 3](#_Toc416255833)

[2.5 מנגנוני רישום (Logging) 3](#_Toc416255834)

[2.6 מנגנוני מעקב אבטחת מידע (Auditing) 3](#_Toc416255835)

[2.7 מנגנוני המשכיות (Continuity) 3](#_Toc416255836)

[3. סיכום ומסקנות 4](#_Toc416255837)

[3.1 תקציר של תהליכי סקר הסיכונים 4](#_Toc416255838)

[3.2 תוצרי הסקר 4](#_Toc416255839)

[3.3 הפקת לקחים 4](#_Toc416255840)

# 1. כללי

## 1.1 מיפוי תהליכים ארגוניים

## 1.2 מיפוי וניתוח מערכת

## 1.3 מיפוי וניתוח תשתיות

### 1.3.1 מיפוי מערכות תקשורת

### 1.3.2 מיפוי שרתים

### 1.3.3 מיפוי מערכות קצה

### 1.3.4 מיפוי תוכנות תשתית

### 1.3.5 מיפוי ממשקים

### 1.3.6 מיפוי מערכות ניטור ובקרה (נו"ב)

### 1.3.7 מיפוי מערכות אבטחה

## 1.4 מיפוי וניתוח יישומים

### 1.4.1 מיפוי תהליכים מרכזיים

### 1.4.2 ניתוח זרימת מידע

# 2. מיפוי וניתוח האבטחה

## 2.1 מנגנוני בקרת תצורה (Configuration)

## 2.2 מנגנוני אימות (Authentication)

## 2.3 מנגנוני בקרת גישה (Access Control)

## 2.4 מנגנוני תקפות (Validation)

## 2.5 מנגנוני רישום (Logging)

## 2.6 מנגנוני מעקב אבטחת מידע (Auditing)

## 2.7 מנגנוני המשכיות (Continuity)

# 3. סיכום ומסקנות

## 3.1 תקציר של תהליכי סקר הסיכונים

להלן תיאור תהליך העבודה לביצוע הפעילויות שתוארו לעיל:

| פעילות | תת-פעילות | לו"ז לביצוע | סטטוס/לקחים |
| --- | --- | --- | --- |
| 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 |  |  |

## 3.2 תוצרי הסקר

## 3.3 הפקת לקחים