מבקר העירייה

דוח ביקורת בנושא

אבטחת מידע והגנת הפרטיות

תוכן העניינים

1. מבוא

העירייה עושה שימוש נרחב במערכות מידע לניהול פעילותה השוטפת כאשר חלק ניכר מאספקת השירותים העירוניים תלוי במערכות המחשוב. חלק בלתי נפרד מהשימוש במערכות ממוחשבותף הינו שימוש ותחזוקה של מאגרי מידע על התושבים ועל הגורמים המקיימים קשר עם העירייה בתחומים רבים. מאגרי מידע אלו כוללים נתונים אישיים של תושבי הרשות , נכסים ובעלויות , אמצעי תשלום, מידע בתחומי רווחה ועוד. בנוסף, קיימים בעירייה נתונים בלתי מסוננים כדוגמת נתוני מערך המצלמות הכוללים לוחיות רישוי, תווי פנים, נתוני מיקום והרגלי תנועה.

ההתפתחות הטכנולוגית גרמה לארגונים רבים, ציבוריים ופרטיים, לעשות שימוש ברשת האינטרנט ובמכשירים ניידים. רשויות רבות ובכלל זה עיריית הרצליה משתמשות באתרי אינטרנט למתן שירותים ומידע באופן מקוון לרבות ביצוע תשלומים באמצעות האינטרנט.

עיריית הרצליה כמו ארגונים רבים חשופה למגוון סיכונים בקשר למאגרי ומערכות המידע ובכלל זה, דליפת מידע, איבוד מידע , השבתה של מערכות המחשוב, פגיעה ברציפות התפקודית של העירייה ועוד. מכאן נובע הצורך למסד ולתחזק מערך אבטחה שיגן על מאגרי המידע, ימנע דליפת נתונים ויבטיח פעילות תקינה של שירותי העירייה.

2. סיכונים במרחב הסייבר ברשות המקומית

מרחב הסייבר: כולל רשתות מחשוב, תקשורת מחשבים ומערכות מידע ממוחשבות והוא חלק אינטגרלי מחלק ניכר מפעילויות העירייה.

איום סייבר: מוגדר כצירוף של כוונות ויכולות לתקיפה במרחב הסייבר שטרם התממש.

אירוע סייבר: מוגדר כהתרחשות אשר מעידה על פגיעה אפשרית בפעילותה התקינה של מערכת מחשוב, שקיים יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר. אירועים אלו מבוססים על ניצול פגיעות או חולשה של הארגון, העלול לפגוע בו ברמות חומרה שונות.

אירועי סייבר ואבטחת מידע עלולים להיגרם בשוגג או במזיד, על ידי גורם פנימי או חיצוני, ולגרום לפגיעה ניכרת ברציפות התפקודית והעסקית של הארגון. בשנים האחרונות קיימת עלייה חדה במספרם ובחומרתם של אירועי סייבר המשבשים את פעילותם התקינה של ארגונים בארץ ובעולם. כך לדוגמה, בשנת 2020 חלה עלייה של 50% באירועי הסייבר שדווחו למרכז המבצעי של מערך הסייבר הלאומי, ביחס לשנה שקדמה לה.

רשויות מקומיות מתמודדות עם מגוון סיכונים, ואיומי סייבר, ומערכות המידע שלהן הפכו למוקד של עניין עבור האקרים ופושעי סייבר. התקפות סייבר ברשויות עלולות לגרום נזקים כדלהלן:

- פגיעה בתשתיות טכנולוגיה (חומרה, תוכנה ויישומים).
- פגיעה בשלמותו ובמהימנותו של המידע השמור במערכות המידע שבשימוש הרשות.

- דליפה של נתונים ומידע ממאגרי המידע שברשות הרשות וחשיפתם לגורמים שאינם מורשים לכך.
- שיבוש ואף מניעה של אספקת שירותים לתושבים ובמקרים חמורים אף פגיעה ברציפות התפקודית של הרשויות המקומיות.

ההנחיות המקצועיות של הביקורת הפנימית מחייבות עריכת סקר סיכונים לקביעת חשיבות נושאי הביקורת.

מרכיבי הסיכון חולקו עפ"י פרמטרים שנקבעו לסיכון גבוה, בינוי, נמוך.

פגיעה במערכות המידע כתוצאה מכשל באבטחת המידע מדורגת כסיכון גבוה לכל אחד ממרכיבי הסיכון הכלולים בסקר הסיכונים כדלהלן.

סיכון כספי: הפסד כספי מעל ל 15 מליון ₪.

סיכון תפעולי: פגיעה תפקודית הגורמת להשבתה של שירותים עירונים ולאי עמידה ביעדי הארגון.

ציות: אי עמידה בחוקים ובתקנות באופן שחושף את הארגון או עובדיו להליכים מנהליים או פליליים.

מוניטין: פגיעה במוניטין הרשות ברמה המקומית לתקופה של מעל חצי שנה.

בחינת הנזקים הפוטנציאלים כפי שתוארו לעיל כתוצאה מדלף מידע או איומי סייבר מעמידים את מכלול הסיכונים בדרוג "גבוה" ומכן החשיבות של גידור הסיכון. חוסנו של ארגון, עמידותו בפני אירועי סייבר ויכולתו להתמודד איתם, תוך שמירה על רציפות תפקודית, נגזרים מרמת ההיערכות להגנה בסייבר המיושמת בעת שגרה.

3. דוח הביקורת

במסגרת תוכנית העבודה של הביקורת לשנת 2022 נערכה ביקורת בנושא: התגוננות בפני איומי סייבר והגנת הפרטיות . הדוח נערך ע"י יועץ חיצוני המתמחה בתחום זה. להלן מפורטים פרקים מדוח הביקורת הכוללים את הנושאים שנבדקו במסגרתו ופעולות הביקורת , ופרטים אודות עורך הדוח.

יחד עם זאת הפרקים הכוללים פרטים אודות מערכות המחשוב ,תשתיות התקשורת ומאגרי המידע שבשימוש העירייה יחד עם פרוט מערכי ההגנה ,הוראות ההפעלה ואחזור המידע בשגרה ובעת אירועי סייבר, הושמטו מדוח הביקורת . אציין כי נערכו מספר דיונים על ממצאי הביקורת והמלצותיה עם מנהל מערכות המידע הקודם והנוכחית כמו גם עם מנכל העירייה.

4. פרקים מדוח אבטחת מידע והגנת הפרטיות

חלוקי נחל
פתרונות לעיר

דוח אבטחת מידע והגנת הפרטיות

עיריית הרצליה

ינואר 2022

חלוקי נחל
פתרונות לעיר

תכן עניינים

1. רקע מקצועי של עורך המסמך

מר דני בן שלום עוסק במתן שירותי תכנון, יעוץ, פיקוח, ידע ושירותים בתחום התקשוב, הכוללים בין היתר את תחום התקשורת, מחשוב, אבטחת מידע וסייבר, אינטרנט, תשתיות, טכנולוגיות מידע, ניהול סיכונים, מבדקי חדירה, המשכיות עסקית, שליטה ובקרה, תקינה ורגולציה וניהול פרויקטי סייבר ואבטחת מידע.

מר בן שלום מחזיק בהסמכות בין לאומיות רבות בתחומי אבטחת המידע והגנות הסייבר ובין היתר הינו בעל תעודות CISO ו CSSA. כמו כן מחזיק מר בן שלום בכתב מינוי כאודיטור חיצוני בתחומים אלה מטעם מכון התקנים.

העיסוק בסייבר ואבטחת מידע הנו אחד המרכזיים בפעילויות עורך המסמך. פעילותו מקיפה במגוון נושאי סייבר ואבטחת מידע תוך כיסוי כלל הפעילויות במחזור החיים של הפרויקט.

לעורך ניסיון רב בייעוץ בתחום, כולל תכנון, ארכיטקטורת אבטחת מידע, סקרי סיכונים, מבדקי חדירה, סיוע בגיבוש צרכים וארכיטקטורה, סיוע בהתמודדות עם איומים ותקיפות, הדרכה ומודעות, חקירות, אפיון, הכנת מכרזים, ליווי פרויקטים, כלי אבטחת מידע, מדיניות, נהלים, תקינה, יישום ובקרה על מערכות אבטחת מידע בהיבטים מגוונים וכד'. כל זאת לסביבות עבודה מגוונות, למערכות שונות, תשתיות, אינטרנט ועוד.

עורך הדוח פעיל במגזרים רבים כגון: תשתיות קריטיות, רשויות מוניציפליות, ביטחון, ממשלה, בריאות, אנרגיה, תחבורה ועוד.

2. מבוא

2.1 בשנים האחרונות אנו עדים לעליית היקף מתקפות הסייבר בעולם בעוצמות שהולכות וגוברות בכל שנה, עם נזקים משמעותיים לארגונים המותקפים. עיריית הרצליה מחויבת לכן להגן על הרציפות התפקודית של מערכות המחשוב שלה וכן להגן על מאגרי המידע שהיא מנהלת.

2.2 ארגונים מוסדיים בישראל, הן במגזר הממשלתי והן במגזר העירוני, נתונים למתקפות סייבר בלתי פוסקות מצד מדינות עויינות ובראשן איראן, מצד ארגוני טרור כמו משמרות המהפכה, החיזבאללה, והחמאס, מצד האקרים הפועלים מטעמי פשיעה כלכלית, ומצד האקרים הפועלים מטעמים אידיאולוגיים כנגד מדינת ישראל ומוסדותיה. ריבוי זה של הגורמים המעורבים בתקיפות סייבר על גורמים מוסדיים בישראל, מצריך התארגנות רבה יותר להגנה על מערכות המחשוב ומאגרי המידע של העירייה, ביחס להתארגנות הנדרשת לדוגמא מחברות קטנות ובינוניות במגזר הפרטי.

2.3 מניעת הצלחת מתקפות סייבר על רשתות העירייה תמנע את הנזקים הבאים:

- שיבוש או מניעה של שירותים חיוניים ואחרים של העירייה לתושבי העיר
- נזקים כלכליים לעירייה
- נזקים כלכליים לתושבי העיר ולקבלנים המועסקים ע"י העירייה.
- סיכון חיי אדם כתוצאה משיבוש שירותי העירייה
- כאוס בעיר כתוצאה מהשיבושים בשירותי העירייה
- אובדן אמון של תושבי העיר במוסדות העירייה ובסדר הציבורי

2.4 מניעת הצלחת מתקפות סייבר על מאגרי המידע של העירייה תמנע את הנזקים הבאים:

- פגיעה בצנעת הפרט כתוצאה מחשיפת מידע על תושבי העיר
- נזקים כלכליים כתוצאה מדלף מידע על חשבונות בנק וכרטיסי אשראי של תושבי העיר
- שיבוש או מניעת קבלת שירותים המגיעים לתושבי העיר, המותאמים למידע האישי שלהם במאגרי העירייה (שירותים סוציאליים, הנחות וכד').

2.5 עיריית הרצליה מחויבת על פי חוק להגן על מאגרי המידע שלה, משימוש לא תקין ודלף מידע האגור במאגרים שלה, וכתוצאה ממתקפות סייבר היכולות לגרום הן לשיבוש מידע והן לדלף מידע לגורם עוין. החוקים והתקנות להם כפופה העירייה בנושא מאגרי מידע הינם:

- חוק הגנת הפרטיות, תשמ"א-1981
- תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
- תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986

3. מטרת הביקורת

3.1 מטרת הביקורת העיקרית היא לוודא שהעירייה פועלת כראוי בכל הקשור להגנה על מערכות המחשוב ומאגרי המידע שלה מפני מתקפות סייבר, בכדי לשמור על הרציפות התפקודית של העירייה, בכדי לשמור על הפרטיות של תושבי העיר ועל שלומם ובכדי למנוע נזקים כלכליים מהעירייה , מתושבי העירייה ומקבלנים המועסקים ע"י העירייה.

3.2 הביקורת בחנה את התארגנות העירייה בהיבטים הבאים:

- קיום ויישום מסמכי מדיניות אבטחת מידע/ הגנת סייבר ורציפות תפקודית
- קיום ויישום נהלי אבטחת מידע/ הגנת סייבר ורציפות תפקודית
- קיום ופעילות צוות אבטחת מידע/ הגנת סייבר מקצועי ובראשו ממונה אבטחת מידע/ הגנת סייבר ופועל הן לסיכול אירועים אלו והן במתן מענה במקרה של זיהוי אירועים אלו.
- קיום ופעילות ועדת היגוי עירונית לאבטחת מידע
- רישום מאגרים אצל רשם המאגרים ומינוי מנהלי מאגרים
- קיום ופעילות וועדת העברת מידע בין גופים ציבוריים, בנוגע למאגרי המידע.
- קיום מערכות ואמצעי אבטחת מידע/ הגנת סייבר
- קיום מוקד אבטחת מידע/ הגנת סייבר המבצע ניטור שוטף של אירועי אבטחת מידע/ סייבר ופועל לסי
- קיום אמצעי הגנה פיזיים על מרכזי מחשוב ותקשורת עיקריים ועל מוקד אבטחת המידע/ הגנת הסייבר
- קיום תשומת לב ניהולית של הנהלת העירייה לנושאי אבטחת מידע/ הגנת סייבר והקצאת תקציבים לנושא
- קיום הדרכות לעובדים למודעות בנושאי אבטחת מידע/ הגנת סייבר
- ביצוע תרגילים לאימון העובדים וצוותי אבטחת מידע/ הגנת סייבר
- ביצוע ביקורות שוטפות לווידוא עמידה בדרישות אבטחת המידע/ הגנת הסייבר של העירייה

- ביצוע ביקורות עיתיות ע"י גורם מקצועי חיצוני מסוג סקרי סיכוני אבטחת מידע/ סייבר ומבדקי חדירות
- ביצוע פיקוח ובקרה על ספקי חוץ בנוגע לשירותי מחשוב, תקשורת ואבטחת מידע/ הגנת סייבר של מערכות העירייה ומאגרי המידע שלה.
- ביצוע ניהול סיכונים שוטף הכולל הערכות מצב ועבודה בתאם לתוכנית עבודה כוללת למזעור הסיכונים ולסגירת פערי אבטחה.
- קיום תכניות עבודה שוטפות ורב-שנתיות לקידום ולטיפול במערכות אבטחת המידע/ הגנת הסייבר
- ביצוע שיפור מתמיד של מערכות ואמצעי האבטחה/ הגנת הסייבר ושל הצוותים המקצועיים המפעילים אותם.

4. נושאים לבחינת הביקורת

4.1 לצורך בחינת המצב הקיים בנושאי אבטחת מידע/ הגנת סייבר נערכו שיחות לימוד ותחקור של מנהלי יחידות המחשוב, אבטחת המידע/ הגנת סייבר, ונדרשה סקירה של המסמכים הרלוונטיים הבאים (נמצא כי חלק מהמסמכים לא קיימים בידי העירייה):

- מסמך מדיניות אבטחת מידע/ הגנת סייבר של עיריית הרצלייה
- מסמך מדיניות המשכיות תפעולית של עיריית הרצליה
- נהלי אבטחת מידע/ הגנת סייבר של העירייה
- נהלי התאוששות מאירועים/ Disaster Recovery
- מסמך מינוי ממונה אבטחת מידע/ הגנת סייבר של העירייה
- מסמך מינוי וועדת היגוי עירונית לנושאי אבטחת מידע/ הגנת סייבר
- מסמך מינוי וועדת העברת מידע בין גופים ציבוריים
- מסמכי בקשה להקמת מאגרי מידע ברשם המאגרים
- שרטוטי ארכיטקטורת מערכות תקשורת נתונים ומערכות הגנת הסייבר שלהם
- רשימת נכסים עליהם נדרשת הגנה
- דרישות אבטחת מידע/ הגנת סייבר בהסכמים מול קבלני חוץ של מערכות מחשוב, תקשורת וסייבר של העירייה
- תוצאות סקרי סיכוני סייבר אחרונים
- תוצאות מבדקי חדירות אחרונים

- תכניות עבודה שוטפות ורב-שנתיות לקידום וטיפול בנושאי אבטחת/ מידע והגנת סייבר, ובכלל זה לטיפול בממצאי סקרי הסיכונים ובדיקות החדירות האחרונים.
- תיעוד הקצאות תקציב אחרונות לנושאי אבטחת מידע/ הגנת סייבר

4.2 בוצעה ביקורת בהיבט של עמידה בחוקים ובתקנות להגנת הפרטיות של מערכות המחשוב ואבטחת המידע של העירייה, בדגש על מאגרי המידע העירוניים והגורמים המטפלים בהם בעירייה. במסגרת זו נבדקו הנושאים הבאים:

- מסמכי הגדרות המאגרים
- מינוי ממונה אבטחת מידע
- נוהל טיפול במאגרים
- מיפוי נכסי המערכות של המאגרים
- ביצוע סקרי סיכונים
- הגנות פיזיות וסביבתיות על המאגרים
- אבטחת מידע בניהול כוח אדם המטפל במאגרים
- ניהול הרשאות גישה למאגרים
- זיהוי ואימות גישה למאגרים
- בקרה ותיעוד גישה למאגרים
- תיעוד של אירועי אבטחה במאגרים
- טיפול בהתקנים ניידים המתחברים למערכות המאגרים
- ניהול מאובטח ומעודכן של מערכות המאגר
- אבטחת מערכות התקשורת של המאגרים
- מיקור חוץ של שירותים לטיפול במאגרים
- ביקורות חוץ על המאגרים
- שמירת נתוני אבטחה של המאגרים
- גיבוי ושחזור נתוני אבטחה של מערכות המאגר
- קיום וועדה להעברת מידע בין גופים ציבוריים
- קיום אבטחת מידע בעת מסירה של מידע מהמאגרים
- קיום נוהל מסירת מידע מהמאגרים
- טיפול במידע עודף במאגרים
- טיפול בבקשות להעברת מידע מהמאגרים

4.3 הביקורת בחנה את היבטי אבטחת מידע/ הגנת סייבר כוללת בהתאם לעקרונות Best Practice המקובלים בישראל ובעולם. במסגרת ביקורת זו נבדקו הנושאים הבאים:

- קיום מערכת הגנה פיזית על מערכי המחשוב והתקשורת מרכזיים ועל מערכי הגנת הסייבר
- קיום מערכות ואמצעי הגנת סייבר הנותנים מענה לאיומים בפניהם ניצבות מערכות המחשוב של העירייה
- קיום מערכת בקרת גישה המבצעת ניהול משתמשים, משאבים, קבצים והרשאות.
- קיום הגדרות אבטחת מידע/ הגנת סייבר וחוקות התואמות את ההגנה הנדרשת ועומדות בקנה אחד עם הידע הקיים בעולם על סוגי פוגעני סייבר וסוגי תקיפות סייבר, ועם המלצות ההקשחה של היצרנים.
- ביצוע הקשחת הגנות סייבר של עמדות עבודה, שרתים, ציוד תקשורת וציוד הגנת סייבר.
- קיום גרסאות עדכניות של תוכנות מערכות הפעלה של מערכות המחשוב, התקשורת וציוד הגנת הסייבר, הכוללות את טלאי האבטחה האחרונים של היצרנים.
- קיום מערך עדכון גרסאות לתוכנות הנ"ל
- קיום מערך בקרת תצורה לתוכנות מערכות הפעלה, תוכנות ניהול קבצים, תוכנות הגנת סייבר ותוכנות ייעודיות אחרות, במטרה למנוע שינוי תצורה ע"י גורם עוין.
- בחינה של כשלים מובנים בארכיטקטורת המערכת ומערכות ההגנה שלה
- בחינה של עמידת המערכת ומערכות ואמצעי ההגנה שלה בדרישות החוקים והתקנות להגנת פרטיות.
- קיום הערכה שוטפת של יכולות וביצועי מערכות אבטחת המידע/ הגנת הסייבר אל מול לקח מצטבר ומודיעין סייבר, בנוגע לאירועי אבטחה בעירייה, בארץ ובעולם, וידע עולמי עדכני בנוגע להתמודדות עם תקיפות סייבר.
- קיום מוקד ניטור והגנת סייבר מרכזי מסוג SOC/SIEM בעל יכולות המתאימות לדרישות ההגנה של העירייה ולמערכות ואמצעי אבטחת המידע/ הגנת הסייבר של העירייה
- קיום אתר Disaster Recovery למרכז המחשבים המרכזי של העירייה

- תרגול תגובה לאירועי אבטחת מידע/ תקיפות סייבר, ובכלל זה תרגול נהלי דיווח, תגובה ואסקלציה לאירועי אבטחת מידע וסייבר
- תרגול תגובה לאירוע Disaster Recovery
- מידת העמידה של קבלני החוץ בדרישות אבטחת המידע/ הגנת הסייבר הנדרשת מהם ע"י עיריית הרצליה

4.4 בוצע מעבר על דוחות סריקת חולשות/ פגיעויות של מערכת Vulnerability Scanner של חב' Cybowall, לצורך מציאת גורמי החולשה/הפגיעות העיקריים במערכת. מערכת Vulnerability Scanner זו מבצעת סריקות מתמידות על רשתות עיריית הרצליה ומגלה חולשות/ פגיעויות אבטחת מידע ידועות שתוקף יכול לנצלם לחדירה עוינת קלה יחסית למערכות עיריית הרצליה, במטרה לפגוע במערכות המידע ולגרום לדלף מידע רגיש.

4.5 נכתב דוח סיכום ממצאים זה של מצב אבטחת המידע/ אבטחת הסייבר במערכות המחשוב של העירייה ובמאגרי המידע שלה, הכולל הצגת הסיכונים כתוצאה מפערי האבטחה הקיימים, והמלצות לטיפול בממצאים.

11. מתודולוגיה

מתודולוגית ביצוע הביקורת מבוצעת בהתאם למתודולוגיית אבטחת המידע בינלאומית. הביקורת בחנה ליקויים אשר עשויים לפגוע בסודיות, שלמות ו/או זמינות המערכת.

11.1 תהליך הביקורת

חלק זה מתאר את תהליכי הביקורת אשר חולק לשלושה חלקים:

11.1.1 שלב א' – הכנה לביקורת

משימה 1: איסוף נתונים

שלב איסוף הנתונים כולל זיהוי אנשי מפתח הקשורים למערכת וביצוע ראיונות מקדימים עמם. בנוסף, שלב זה כולל איסוף חומר אודות הארגון והמערכת הנבדקת. הראיונות מתמקדים בסביבה העסקית והתפעולית של המערכת. סקירת מסמכים מעניקה לצוות הביקורת כבסיס להערכה של תאימות אל מול מדיניות ונהלי הארגון, ורגולציות רלוונטיות.

משימה 2: חומרי עזר

חומרי העזר הבאים שימשו את צוות הביקורת:

- **שאלון בקרות אבטחת מידע במערכת** – שאלון שמולא ע"י הסוקרים בכדי לבחון את בקרות אבטחת המידע במערכת.
- **טבלת חישוב רמת סיכון** – הטבלה ממירה את הליקויים הגולמיים לסיכונים על בסיס התהליכים הבאים:
  - רשימת ליקויים
  - התאמה בין ליקויים לווקטור האיומים
  - הערכת סבירות המימוש והנזק הפוטנציאלי של מימוש האיום
- **טבלת הפחתת הסיכונים** – מכילה את הסיכונים העיקריים והבקרות המומלצות למזעורם. הטבלה מוגשת למנהל המערכת האחראי לקבלה ו/או דחייה של הבקרות באופן פורמאלי.

11.1.2 שלב ב' – ביצוע הביקורת

משימה 1 : סקירת מסמכים

הביקורת החלה עם סקירת מסמכים שסופקו לצוות הסוקרים ע"י מנהלי המערכת. ראיונות עומק שבוצעו עם מנהלי המערכת סייעו במילוי השאלונים וזיהוי איומים למערכת.

משימה 2 : ניתוח המערכת

בשלב זה, הסוקרים קבעו את גבולות המערכת לצד המשאבים המרכיבים את המערכת, ממשקיה עם מערכות חיצוניות, תלויות המערכת הובהרו לצד רגישות המידע במערכת, ונאספו כלל הפרטים אשר עשויים שעשוי להוביל לניתוח סביבתה.

משימה 3 : מתאר האיומים למערכת

מטרתו של שלב זה הנה לזהות את תרחישי האיומים ומקורותיהם העשויים לפגוע בסודיות, בשלמות ו/או בזמינות המערכת.

- **מקור איום** – הגורם הפוגע בערכי אבטחת המידע של המערכת (סודיות, שלמות, זמינות). מקור איום עשוי להיות אנושי, סביבתי או טבעי (איתני הטבע).
- **תרחיש איום** – הפעולה או הטכניקה שבה ממומשת ההתקפה.

מקורות איומים:

- **טעויות והשמטות** – שגיאות ופעולות שנגרמו ע"י אנשי המערכת (בד"כ פיתוח ותחזוקה) המביאות לנזק פיסי, הפרעות למערכת, ו/או חשיפה.
- **התקפות פנימיות** – פעולות הננקטות ע"י גורמים פנימיים לארגון ע"מ לפגוע בארגון ואנשיו, מערכותיו והמידע שלו. דוגמאות: חדירה למערכת, העלאת הרשאות במערכת, ציטוט למידע, ניחוש סיסמאות, מניעת שירות והנדסה חברתית.
- **פעילויות פנימיות בלתי מורשות (מעילות פנימיות)** – פעולות פנימיות בלתי מורשות ו/או לא חוקיות שמטרתן לגרום נזק. דוגמאות: הפצה של חומר שמור, זליגת מידע של לקוחות ופגיעה בפרטיות, הטרדה של אחרים ע"י שימוש במשאבי מחשוב, גניבת כסף ועוד.
- **התקפות חיצוניות** – פעולות הננקטות ע"י גורמים חיצוניים לארגון ע"מ לפגוע בארגון ואנשיו, מערכותיו והמידע שלו. דוגמאות: חדירה למערכת,

העלאת הרשאות במערכת, ציטוט למידע, ניחוש סיסמאות וחשבונות, מניעת שירות והנדסה חברתית, Phishing, Pharming ועוד.

- **קוד זדוני** – פעולות ממוכנות הנגרמות ע"י קוד המזיק לארגון, למערכותיו ולמידע שלו. דוגמאות: וירוסים, תולעים, סוסים טרויאניים, Rootkits, Spyware.

משימה 4 : זיהוי ליקויים

בשלב זה, צוות הסוקרים מגבש רשימה של ליקויים (פגיעויות או חולשות) במערכת שעשויים להיות מנוצלים על ידי גורמים איומים. את רשימת הליקויים גיבש צוות הסוקרים ע"י:

- ביצוע בדיקות Hands-On של רכיבי המערכת (אפליקציה, בסיס נתונים, מערכת הפעלה, תקשורת).
- ראיונות מעמיקים עם מנהלי המערכת.

משימה 5 : ניתוח הסיכונים

בשלב זה, צוות הסוקרים העריך את רמת הסיכון הנובעת משילובם של תרחישי האיומים והליקויים השונים במערכת. במקרים מסוימים, שילוב של קבוצת ליקויים יצרו סיכון ספציפי. במקרים אחרים, ליקוי ספציפי יצר סיכון ספציפי. קביעת רמת הסיכון עבור איום ספציפי כוללת התייחסות לפרמטרים הבאים:

- **קביעת הסבירות**: מידת הסבירות שבה עשוי איום לנצל ליקוי הקיים במערכת נקבעת ע"י הגורמים הבאים:
  - מוטיבציה ויכולות של מקור האיום.
  - אפקטיביות הבקרות למזעור האיום.

משימה 6: המלצות למזעור הסיכונים

בשלב זה, יומלצו בקרות שעשויות להפחית את סבירות מימוש הסיכון ו/או את עוצמת הנזק בעקבות מימושו.

מטרת שלב זה הנה להוריד את רמת הסיכון של המערכת לרמה המקובלת על ההנהלה והארגון. צוות הביקורת התחשב בגורמים הבאים במתן ההמלצות לגבי יישום הבקרות למזעור הסיכונים:

- רגישות המידע במערכת.
- אפקטיביות של הפתרונות המוצעים.

- דרישות רגולציה וחקיקה.
- מדיניות הארגון וממשל תאגידי.
- השפעה תפעולית.
- בטיחות ומהימנות.

ההמלצות הנן פרי ניתוח הסיכונים ומשמשות כבסיס להנהלת הארגון לגבש החלטות וסדרי עדיפויות לגבי מזעור הסיכונים. באחריות הארגון לגבש החלטה בגין קבלת ההמלצות, מציאת חלופות למזעור הסיכונים ו/או דחיית ההמלצות וקבלת הסיכונים באופן רשמי. ההחלטות שיגובשו בשלב זה יהוו בסיס לשלב גידור הסיכונים.

11.1.3 שלב ג' – לאחר הביקורת

משימה 1 : גידור הסיכונים

בשלב זה תבנה תכנית עבודה למזעור הסיכונים שנתגלו במהלך הביקורת תוך כדי מימוש הבקרות הנבחרות. התוכנית תכלול גורמים אחראים, שלבים עיקריים, עלויות צפויות ועוד.

משימה 2 : בקרה שוטפת

באחריות הנהלת הארגון לבקר ולנטר את פרויקט גידור הסיכונים. יש להקים ועדת היגוי מטעם ההנהלה שמטרתה לעקוב אחר יעדי הפרויקט ומזעור הסיכונים.