סייבר ישראל
מערך הסייבר הלאומי

תבנית סקר סיכונים

מגזר קמעונאי

סייבר ישראל
מערך הסייבר הלאומי

תבנית סקר סיכונים

מגזר קמעונאות

מרץ 2020

מסמך זה פותח על ידי מערך הסייבר הלאומי לטובת הציבור בישראל. המסמך מהווה המלצה לאנשי הגנת סייבר, מערכות מידע ולאנשי IT במגזר הקמעונאי בישראל. ניתן להשתמש בו באופן חופשי לטובת העלאת החוסן בסייבר במשק הישראלי.
המסמך מציג רשימה של המלצות ליישום בארגון, ומוצע כי ארגונים יבצעו תהליך הערכת סיכונים לשם בחינה האם נדרש להחיל המלצות מחמירות מהאמור במסמך זה, וכן האם ניתן ליישם באופן אופרטיבי את ההמלצות.
המסמך נכתב בלשון זכר מטעמי נוחות בלבד והוא פונה לשני המינים.
התייחסויות והערות לתוכן המסמך ניתן להעביר במייל ל-tora@cyber.gov.il.

תוכן עניינים

1 מבוא...... 5

1.1 רקע...... 5
1.2 מטרה...... 5

2 הנחיות לשימוש בתבנית העבודה...... 7

2.1 רכיבי תבנית העבודה...... 7
2.2 שלבי ביצוע סקר סיכוני סייבר...... 8
2.3 אופן ביצוע סקר הסיכונים...... 9

3 דוגמה סקר סיכוני סייבר לדוגמה...... 14

1. מבוא...... 2

1.1. רקע...... 2

1.2. מטרות...... 2

1.3. תיחום הסקר...... 3

1.4. אופן ביצוע הסקר...... 3

1.5. תרחיש ייחוס...... 4

1.6. סיכונים מרכזיים שזוהו...... 5

1.7. סביבת הבקרה...... 6

1.8. תובנות מרכזיות...... 8

2. פירוט הסיכונים...... 11

2.1. יעד הגנה אופייני- עמדות מכירה (POS)...... 11

2.2. מערכת ניהול מלאי...... 15

2.3. אתר אינטרנט מכירתי...... 20

2.4. מערכת CRM - מועדון לקוחות...... 23

3. אפקטיביות בקרות...... 26

3.1. אפקטיביות ממוצעת של משפחות בקרה אשר יושמו בכלל התהליכים שנסקרו...... 26

נספח א'- אודות מערך הסייבר הלאומי...... 28

נספח ב'- רשימת ראיונות שנערכו במסגרת הסקר...... 29

נספח ג'- גיבוש תרחיש ייחוס במרחב הסייבר...... 30

נספח ד"- רשימת מסמכים אשר נסקרו במסגרת הסקר...... 36

נספח ה'- מיפוי נכסי מידע ומאגרי מידע...... 37

נספח ו'- סיכוני סייבר אופייניים לבחינה בסקר בהיקף בסיסי...... 41

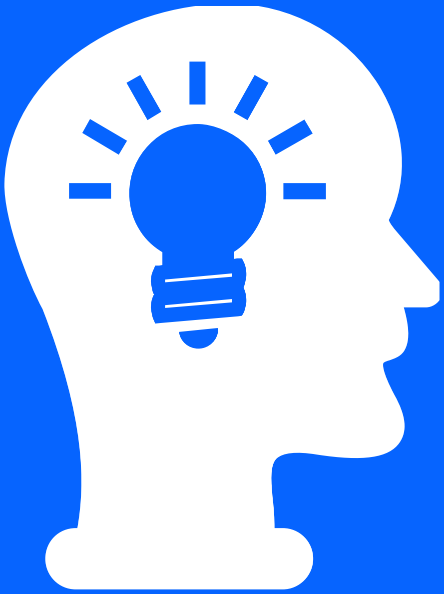
נספח ז'- סיכוני סייבר אופייניים לבחינה בסקר בהיקף מתקדם...... 42

נספח ח'- הערכת עוצמה, סבירות וחישוב רמת סיכון...... 44

נספח ט'- מילון מונחים...... 46

סייבר ישראל
מערך הסייבר הלאומי

תבנית עבודה לביצוע סקר סיכוני סייבר במגזר הקמעונאי



1 מבוא

1.1 רקע

סיכוני סייבר מהווים חלק משמעותי מכלל הסיכונים התפעוליים אליהם חשופות חברות ולהתממשותם עלולות להיות השלכות עסקיות שונות, לרבות: פגיעה במוניטין, אובדן הכנסות, חשיפה משפטית וכו'.

מטרות העל של תהליך ניהול סיכוני סייבר הן הפחתת הסבירות לפגיעה בתהליכים העסקיים ובמידע של הארגון כתוצאה מהתממשות סיכונים אשר מקורם במרחב הסייבר, וצמצום ההשפעה עליהם, במקרה שהתממשו סיכונים אלו.

תבנית העבודה לביצוע סקר סיכוני סייבר במגזר הקמעונאי (להלן "תבנית עבודה") מתבססת על תורת ההגנה בסייבר לארגון (להלן: "תוה"ג") אשר פורסמה ביוני 2017 על ידי מערך הסייבר הלאומי (לפירוט אודות המערך, ראה נספח א'). כדי להתאים אותה למאפייני המגזר הקמעונאי, נערכו, בין היתר, סקרים מקיפים במספר גופים מובילים במגזר הקמעונאי בישראל, במסגרתם התקיימו בין השאר ראיונות עם גורמי הנהלה ועם גורמי מערכות מידע והגנת סייבר.

נוכח השונות בין ארגונים שונים במגזר הקמעונאי, נבנתה תבנית העבודה ככלי דינמי אותו ניתן להתאים לכל ארגון, כך שיתאים ליעדיו, צרכיו וליכולותיו. תבנית העבודה כוללת הנחיות לשלבי עבודה מומלצים, התייחסות לסיכונים מגזריים אשר ייתכן ורלוונטיים לארגון, ודוגמאות מעשיות אשר חלקן עשויות להימצא רלוונטיות לארגון וחלקן עשויות להוות בסיס לסיעור מוחות, בעת זיהוי סיכונים ובחינת השפעתם על הארגון ובעת הערכת סביבת הבקרה.

1.2 מטרה

תבנית העבודה גובשה במטרה להוות כלי פרקטי המוביל באופן שיטתי את תהליך ביצוע סקר סיכוני סייבר, ומאפשר:

- לזהות את סיכוני הסייבר העלולים לפגוע בהשגת היעדים העסקיים;
- להעריך את רמת הסיכון תוך שקלול מרכיבי עוצמה וסבירות;
- להעריך את אפקטיביות סביבת הבקרה של מערכות המידע התומכות בתהליכים עסקיים;

- להציג בפני הנהלה ודירקטוריון תמונת מצב עדכנית לשם קבלת החלטות.

הנחיות לשימוש בתבנית העבודה

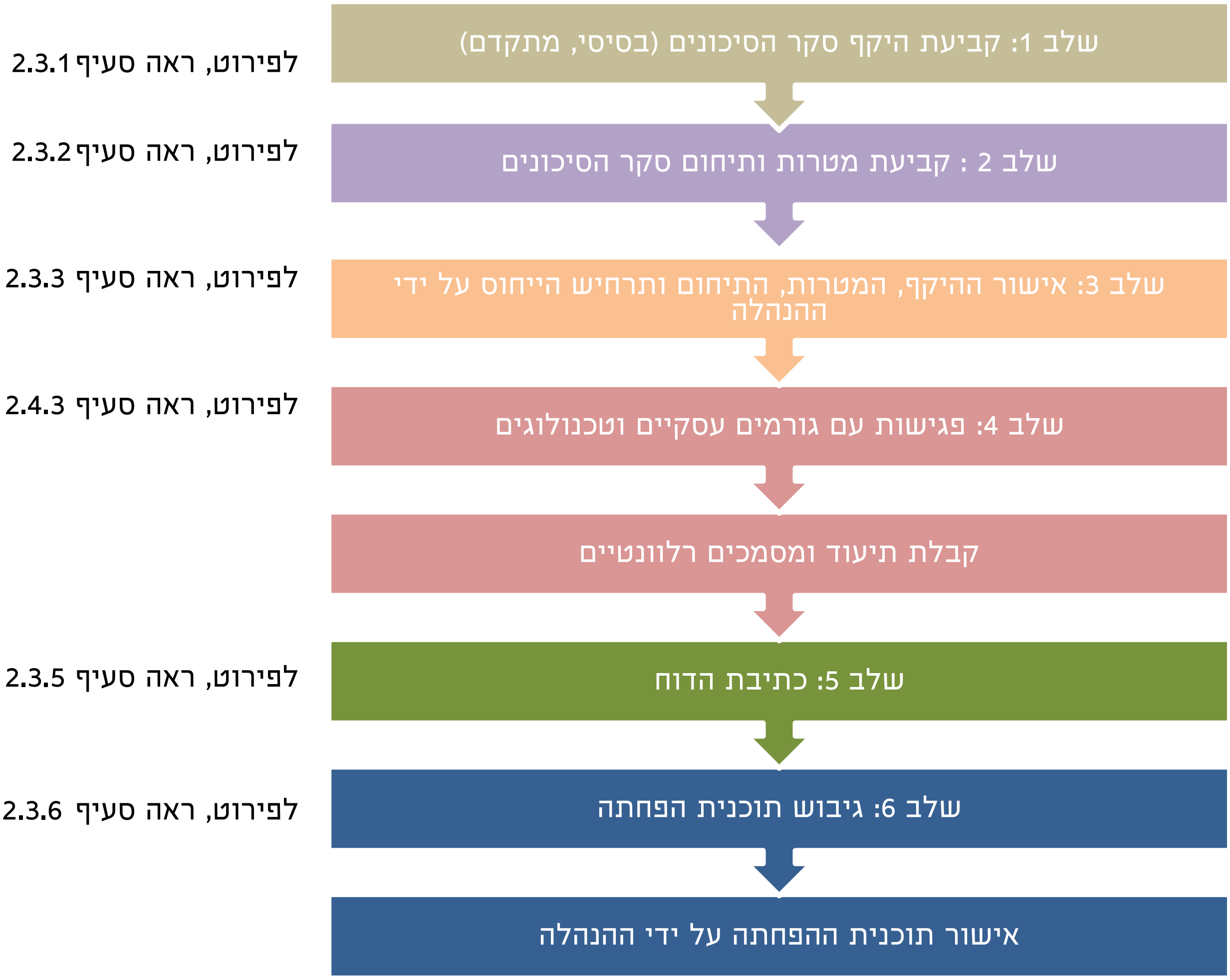
1.3 רכיבי תבנית העבודה

התבנית בנויה משני רכיבים:

- **קובץ לחישוב יעילות בקרות וגיבוש המלצות לשיפור** - קובץ אקסל אליו מרוכז המידע הגולמי שנאסף במסגרת הסקר אודות אפקטיביות בקרות תוה"ג. הקובץ כולל חישובים המהווים מקור מידע חשוב לדוח המסכם. כמו כן, בהתאם לפערים שזוהו, נדרש לגבש המלצות לתוכנית פעולה לשיפור אפקטיביות הבקרות.
- **תבנית דוח מסכם** - מסמך אקסל הכולל הנחיות לביצוע סקר הסיכונים, מוביל את כותב הדוח ומאפשר את הצגת תוצאות סקר הסיכונים באופן מובנה ועקבי. המסמך כולל הנחיות פרטניות לכתיבת הדוח וכן דוגמאות לתכנים מקצועיים רלוונטיים למגזר הקמעונאי, דוגמת סיכונים ומערכות מידע אופייניות. דוגמאות אלו מסייעות בשלב הערכת הסיכונים, וככל שהן רלוונטיות לארגון בו מתבצע סקר הסיכונים, ניתן לעשות בהן שימוש בעת כתיבת הדוח המסכם.

Retail Cyber Controls
Template_May 2019 V

1.4 שלבי ביצוע סקר סיכוני סייבר



1.5 אופן ביצוע סקר הסיכונים

לשם ביצוע סקר הסיכונים, יש לפעול בהתאם להנחיות המופיעות להלן, הכוללות בין היתר הפניות לסעיפים הרלוונטיים בתבנית הסקר. הנחיות מפורטות מופיעות בתחילת כל סעיף בתבנית הסקר.

<u>שלב ראשון - קביעת היקף סקר הסיכונים</u>

תבנית סקר הסיכונים נבנתה באופן המאפשר לארגון לבחור בין שתי רמות היקף, על מנת להתאים את סקר הסיכונים לצרכי הארגון:

היקף בסיסי: מאפשר לארגונים לבצע סקר מהיר יחסית המתמקד בסיכונים המאפיינים את המגזר הקמעונאי אליו משתייכת החברה. במסגרת סקר בהיקף בסיסי מזוהים הסיכונים העלולים להשפיע על יעדי ההגנה המאפיינים את המגזר הקמעונאי, מוערכת עוצמתם וכן נבחנת אפקטיביות הבקרות המרכזיות שנועדו להפחית סיכוני סייבר מהותיים אליהם חשופים יעדי הגנה אלו.

במסגרת סקר בהיקף בסיסי, נבחנת גם האפקטיביות של מספר מצומצם של בקרות-מפתח כלליות, אשר נועדו להפחית את סיכוני הסייבר אליהם חשופים תהליכים העסקיים ומערכות מידע.

ביצוע סקר סיכונים ברמה בסיסית יאפשר הצגת תמונת מצב חלקית בפני הנהלת החברה, באשר לסטטוס סיכוני הסייבר לתהליכים מרכזיים וגיבוש תוכנית להפחתתם.

לפירוט הבקרות והסיכונים הרלוונטיים לשלב זה, ראה **נספח ו'** וקובץ האקסל, גיליון "סביבת הבקרה", עמודות **N** (סינון "בסיסי"), **Q, T, W, Z**.

היקף מתקדם: מספק לארגונים תמונה רחבה יותר אודות סיכונים לתהליכים נוספים. ניתן לבצע סקר בהיקף מתקדם, לאחר סיום ביצוע סקר סיכונים בהיקף בסיסי, או לחלופין, כחלק מסקר רחב יותר, הכולל את תכולת הסקר הבסיסי ותכולה נוספת, הכלולה בסקר בהיקף מתקדם. התכולה הנוספת תקבע בהתאם למאפיינים ולצרכים הייחודיים של כל חברה, לרבות אסטרטגיית החברה, יעדיה העסקיים, תכניות להרחבת שירותים דיגיטליים ועוד. הרחבת היקף הסקר תאפשר להקיף תהליכי עבודה ונכסי מידע נוספים ולבחון את האפקטיביות של בקרות נוספות, המשפיעות על מוכנות הסייבר של החברה.

לפירוט הבקרות והסיכונים הרלוונטיים לשלב זה, ראה **נספח ז'** וקובץ האקסל, גיליון "סביבת הבקרה", עמודה **N** (סינון "מתקדם").

<u>שלב שני - קביעת מטרות ותיחום סקר הסיכונים</u>
במטרה לקבוע את תכולת הסקר ומשך ביצועו, יש לבצע את הפעולות המפורטות להלן :

- הגדרת הגורם אשר יוביל את ביצוע הסקר, כמו גם גורמים מהחברה ומחוצה לה שיסייעו לו בכך.
- הגדרת מטרות הסקר, בהתאם להנחיות המופיעות בסעיף 1.2 בתבנית הדוח.
- קביעת תיחום הסקר, בהתאם להנחיות המופיעות בסעיף 1.3 בתבנית הדוח.
- גיבוש תרחיש ייחוס, בהתאם להנחיות המופיעות בסעיף 2.1 בתבנית הדוח.

<u>שלב שלישי- קביעת מטרות ותיחום סקר הסיכונים</u>
יש לקבל את אישור ההנהלה באשר לכל אחד מהמרכיבים הבאים:

- ביצוע הסקר בהתאם לרמה הבסיסית או הרמה המתקדמת.
- מטרות הסקר.
- תיחום הסקר.
- תרחיש הייחוס.

<u>שלב רביעי- ביצוע הסקר</u>
בהתאם למטרות הסקר ותיחומו כפי שאושרו על ידי ההנהלה, יש לקבוע פגישות עם גורמים עסקיים וטכנולוגיים. מטרת הפגישות הינה קבלת הפרטים הנדרשים לשם זיהוי הסיכונים הרלוונטיים, מיפוי מערכות מידע ומאגרי מידע והערכת אפקטיביות בקרות כמפורט להלן.
פגישות עם גורמים עסקיים: במסגרת זאת, יש להיפגש עם עובדים בדרגים השונים הנוטלים חלק בתהליכים העסקיים שנכללים בסקר. כך, למשל, סקירת תהליך רכש יכולה לכלול פגישות עם מנהל מחלקת רכש, קניין האמון על בחינת ספקים וביצוע הזמנות, מנהלת חשבונות שאחראית על אישור הזמנות, מחסנאי האמון על קליטת סחורה וכו'. רצוי לקבוע פגישות ממוקדות של כשעה, ובמהלכן מומלץ להתייחס להיבטים הבאים:

- תיאור התהליך העסקי מקצה לקצה.

- קבלת מידע כללי על מערכות מידע המעורבות בתהליך, לשם מיפוי מערכות המידע בחברה בהתאם לתבנית המופיעה בנספח ה..

- קבלת מידע על מאגרי המידע בהם נעשה שימוש בתהליך, לשם מיפוי מאגרי המידע בחברה בהתאם לתבנית המופיעה בנספח ה'

- קבלת מידע על הסיכונים הרלוונטיים, בהתאם לתבנית המופיעה בפרק **2.**

- הבנת ההשלכות העסקיות במקרה של התממשות כל אחד מהסיכונים, בהתאם לתבנית המופיעה בפרק **2.**

פגישות עם גורמים טכנולוגיים: במסגרת זאת, יש להיפגש עם הגורמים הרלוונטיים בתחום טכנולוגיות המידע והגנת סייבר, האמונים על מערכות המידע השונות התומכות בתהליכים העסקיים שנכללים בסקר. במידת הצורך, יש לתאם פגישות גם עם ספקים וגורמי צד ג' רלוונטיים. כך, למשל, סקירת מערכות התומכות בתהליך הרכש יכולה לכלול פגישה עם נציג של יצרן מערכת הרכש בכל הנוגע לתמיכה ופיתוחים חדשים, עם הגורם המתפעל את המערכת באופן שוטף, עם גורם אבטחת המידע המנטר את פעילותה בהיבטי סייבר וכו'. רצוי לקבוע פגישות ממוקדות של כשעה עד שעה וחצי, ובמהלכן נדרש להתייחס להיבטים הבאים, לרבות קבלת תיעוד טכני ו/או בדיקה בפועל של מערכת המידע ככל שרלוונטי:

- קבלת מידע טכני על מערכות מידע המעורבות בתהליך, לשם מיפוי מערכות המידע בחברה בהתאם לתבנית המופיעה ב**נספח ה'.**

- קבלת מידע על מאגרי המידע בהם נעשה שימוש בתהליך, לשם מיפוי מאגרי המידע בחברה בהתאם לתבנית המופיעה ב**נספח ה'**

- קבלת מידע אשר יסייע בהערכת אפקטיביות הבקרות המגינות על מערכות מידע ומאגרי מידע, כמופיע בגיליון "סביבת הבקרה" בקובץ האקסל בעמודות המסומנות בצבע תכלת.

במטרה להבטיח אפקטיביות מקסימאלית של הפגישות:
מומלץ להזין לנספח ב'- רשימת ראיונות שנערכו במסגרת הסקר את הפגישות המתוכננות להתבצע, ובסיום הסקר, יש לוודא כי רשימה זו עדכנית ומשקפת את הפגישות אשר בוצעו בפועל.

מומלץ לקבוע פגישות ממוקדות בנות כשעה-שעה וחצי לכל היותר. במהלך הפגישות, יש להציג לבעל התפקיד שאלות ממוקדות, ולמלא, כאמור, את הטבלאות המפורטות לעיל.
מומלץ לבקש במסגרת הפגישות מסמכים ותיעוד רלוונטי, ולתעד אותם במסגרת הטבלה המופיעה בנספח ד'- רשימת מסמכים אשר נסקרו במסגרת הסקר.

לאחר השלמת הפגישות עם כלל הגורמים, על הסוקר:

לגבש המלצות לסגירה פערי אפקטיביות הבקרות כפי שזוהו, ולהשלימן בעמודה AC- המלצות לתכנית פעולה, המסומנת בצבע סגול בגיליון "סביבת הבקרה" בקובץ האקסל.
לגבש המלצות לסיכונים שזוהו, כמפורט בפרק 2.
לגבש תובנות מרכזיות על בסיס הסיכונים שזוהו ואפקטיביות הבקרות השונות.

<u>שלב חמישי- כתיבת דו"ח</u>

הדו"ח נועד לסייע לארגונים להציג את תוצאות סקר סיכוני הסייבר באופן שיספק תועלת לגורמים עסקיים ולגורמים טכנולוגיים כאחד, ולהניע לגיבוש תוכנית עבודה להפחתת הסיכונים אשר זוהו. מצורפת להלן תבנית לכתיבת הדוח המסכם, אותה ניתן לערוך ולהתאים, בהתאם לצרכי הארגון.

הנחיות כלליות

הדוח כולל הבנייה לוגית של פרקים וסעיפים.
הנחיות לכתיבת כל סעיף מופיעות בתחילת כל סעיף, באופן הבא:
יש למחוק את תיבות הטקסט עם סיום כתיבת הדוח.

ⓘ תיבת טקסט המפרטת את מטרת הסעיף וסוג המידע שיש לשלב בו.

מרבית הסעיפים כוללים דוגמאות רלוונטיות בפונט כחול כפי שמופיע בפסקה זו. דוגמאות אלו נמצאו רלוונטיות למגזר הקמעונאי, ניתן להתאים אותן לממצאי הסקר או למחוק במידה ואינן רלוונטיות לארגון.

לאחר מילוי הנתונים המפורטים לעיל, יש לערוך את הסעיפים הבאים:

- פילוח הסיכונים שזוהו, כמופיע בסעיף 1.6 במסמך הסקר לדוגמה המופיע בהמשך.
- תובנות מרכזיות והשלכות עסקיות, כמופיע בפרק 2.

בעת עריכת סקר הסיכונים, חשוב לזכור: מטרת תבנית העבודה היא לסייע בביצוע סקר סיכוני סייבר העלולים לפגוע בהשגת היעדים העסקיים של הארגון. תבנית הדוח המסכם והתכנים הכלולים בה מוגשים לעורך הסקר במטרה להציג סיכונים אופייניים למגזר הקמעונאי ולעורר חשיבה מוטת סיכונים אשר תסייע בזיהוי הסיכונים הקונקרטיים החלים על הארגון. על כן, אין לראות בדוגמאות הכלולות בתבנית הדוח "כזה ראה וקדש"; עורך הסקר נדרש להתאים דוגמאות רלוונטיות ולהסיר דוגמאות שאינן רלוונטיות לארגון בהתאם לסיכונים אשר זוהו.

<u>שלב שישי- גיבוש תכנית הפחתה</u>

לאחר השלמת הדוח, יש לגבש תכנית הפחתה, שהינה תכנית עבודה שמטרתה להקטין את הסבירות להתממשות הסיכון או את נזקיו במידה ויתממש, ולהעביר אותה לממונה הגנת הסייבר, לגורמי ההנהלה בארגון ולכל גורם רלוונטי אחר.

גיבוש תוכנית ההפחתה ראוי כי יתבצע בהתבסס על רמות הסיכונים שזוהו, ובהתייחס לאפקטיביות סביבת הבקרה - יש לתעדף את הטיפול בפערי הבקרה שזוהו, המפורטים במסגרת קובץ האקסל בגיליון "סביבת הבקרה". עבור כל פער, נדרש:

- לגבש המלצה קונקרטית וברת ביצוע (עמודה **AC** בגיליון);
- להמליץ על גורם אחראי לביצוע ההמלצה (עמודה **AD** בגיליון);
- להמליץ על תאריך יעד לסיום יישום ההמלצה (עמודה **AE** בגיליון).

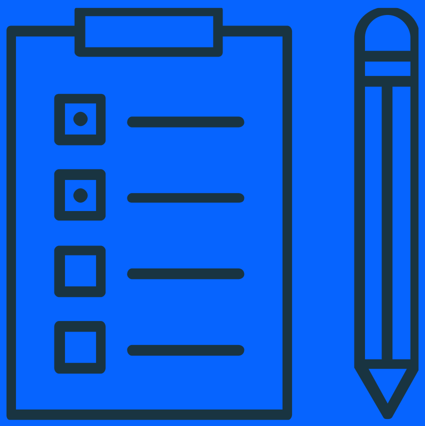
כחלק ממחזור חיי ניהול הסיכון יש לנקוט בצעדים הבאים:

- קיום דיון בהנהלה ו/או פורום אבטחת מידע (ככל שקיים) לשם הצגת הסקר וממצאיו.
- אישור ההנהלה ו/או פורום אבטחת מידע (ככל שקיים) לתוכנית הפחתה לסיכונים שזוהו והמשאבים הנדרשים לשם כך.
- גיבוש תכנית עבודה הכוללת אבני דרך ולוחות זמנים ליישום תכנית ההפחתה.

- מעקב אחר סטטוס יישום ההמלצות (עמודה **AF** בגיליון "סביבת הבקרה בקובץ האקסל").

סייבר ישראל
מערך הסייבר הלאומי

דוח סקר סיכוני סייבר לדוגמה



סקר סיכוני סייבר בחברת _____

[לוגו החברה]

נערך על ידי [שם, תפקיד]

מוגש ל: [שם, תפקיד]

תאריך: [dd.mm.yyyy]

תוכן עניינים

1. מבוא 2
1.1. רקע 2
1.2. מטרות 2
1.3. תיחום הסקר 3
1.4. אופן ביצוע הסקר 3
1.5. תרחיש ייחוס 4
1.6. סיכונים מרכזיים שזוהו 5
1.7. סביבת הבקרה 6
1.8. תובנות מרכזיות 8
2. פירוט הסיכונים 11
2.1. יעד הגנה אופייני- עמדות מכירה (POS) 11
2.2. מערכת ניהול מלאי 15
2.3. אתר אינטרנט מכירתי 20
2.4. מערכת CRM - מועדון לקוחות 23
3. אפקטיביות בקרות 26
3.1. אפקטיביות ממוצעת של משפחות בקרה אשר יושמו בכלל התהליכים שנסקרו 26
נספח א'- אודות מערך הסייבר הלאומי 28
נספח ב'- רשימת ראיונות שנערכו במסגרת הסקר 29
נספח ג'- גיבוש תרחיש ייחוס במרחב הסייבר 30
נספח ד"- רשימת מסמכים אשר נסקרו במסגרת הסקר 36
נספח ו'- סיכוני סייבר אופייניים לבחינה בסקר בהיקף בסיסי 41
נספח ז'- סיכוני סייבר אופייניים לבחינה בסקר בהיקף מתקדם 42
נספח ח'- הערכת עוצמה, סבירות וחישוב רמת סיכון 44
נספח ט'- מילון מונחים 46

1. מבוא

1.1. רקע

סיכוני סייבר מהווים חלק משמעותי מכלל הסיכונים התפעוליים אליהם חשופה חברת ABC (להלן: "החברה") ולהתממשותם עלולות להיות השלכות עסקיות שונות, לרבות: פגיעה במוניטין, אובדן הכנסות, חשיפה משפטית ועוד.

על פי מחקרים שנערכו בשנים האחרונות, המגזר הקמעונאי מהווה יעד מועדף לפעילות האקרים וגורמים זדוניים מסוגים שונים. לפי חלק מההערכות,, כ-75% מהחברות הקמעונאיות חוו אירוע של גניבת מידע במהלך פעילותן.

כדי להפחית סיכוני סייבר באופן שיטתי, יעיל ואפקטיבי, נדרש למפות נכסי מידע ותהליכים עסקיים, ולזהות את סיכוני הסייבר אליהם הם חשופים. לאחר מכן יש לגבש תוכנית הפחתה, תוך תעדוף הטיפול בסיכונים, בהתאם לעוצמתם ולמידת השפעתם על השגת יעדי החברה. **גישה זו תסייע גם בתהליך קבלת ההחלטות באשר למשאבים אותם נדרשת החברה להשקיע בהגנת סייבר**.

במהלך החודשים XY-XY 20XX נערך בחברה **סקר סיכוני סייבר**, במסגרתו מופו והוערכו סיכוני סייבר העלולים לפגוע **בסודיות, שלמות וזמינות** (Confidentiality, Integrity, Availability) תהליכים עסקיים ונכסי מידע מרכזיים של החברה.

1.2. מטרות

ⓘ עם תחילת התהליך, יש לקבוע את מטרות סקר הסיכונים ולהביאן לאישור גורמי ההנהלה המתאימים. קביעת מטרות הסקר תסייע הן לתיחום הפרויקט והן לניהול השוטף. ראוי לזכור כי לסטייה מהמטרות שנקבעו, עלולה להיות השפעה על תקציב ותוצרי הסקר ועל כן ראוי לאשר באופן פורמאלי שינויים במטרות העשויים להתרחש במהלכו.

מטרות הסקר הינן כדלקמן:

- זיהוי והערכת סיכוני סייבר אשר התממשותם תפגע בהשגת יעדי החברה.
- גיבוש תמונת מצב באשר לקיום בקרות הגנת סייבר בחברה ומידת האפקטיביות שלהן.
- יצירת תשתית לגיבוש תכנית להפחתת סיכוני סייבר.

1.3.תיחום הסקר

ⓘ לאחר קביעת מטרות סקר הסיכונים, יש לקבוע את היקפו וכפועל יוצא, את המשאבים הנדרשים הן מהצוות המבצע את הסקר והן מיתר הגורמים בחברה. בנוסף, יש לציין תחומים מרכזיים שאינם נכללים במסגרת הסקר. שיקולים להחרגה עשויים להיות קשורים לשינוי מהותי הצפוי בתחומי פעילות, תהליכים עסקיים או מערכות מידע, כמו גם אתרים גיאוגרפיים של החברה אשר הוחלט שלא לכלול בשל מורכבות לוגיסטית או תרומה שולית לסקר.

חברות בת/התהליכים/האתרים הבאים **נבדקו** במסגרת הסקר:

- חברה בת א'/ תהליך א'/ אתר א'.
- חברה בת ב'/ תהליך ב'/ אתר ב'.

חברות הבנות/התהליכים/האתרים הבאים **לא נבדקו** במסגרת הסקר:

- חברה בת א'/ תהליך א'/ אתר א'.
- חברה בת ב'/ תהליך ב'/ אתר ב'.

1.4.אופן ביצוע הסקר

במסגרת הסקר, נערכו ראיונות עם בעלי תפקידים בחברה ועם גורמי מערכות מידע (לפירוט, ראה נספח ב'- רשימת ראיונות שנערכו במסגרת הסקר), במטרה לזהות את סיכוני הסייבר והשפעתם על הפעילות העסקית. בנוסף, נסקרו תהליכי עבודה

ⓘ בסעיף זה יש לציין בקצרה את אופן ביצוע הסקר. מטרת הסעיף הינה הקניית ביטחון לקורא הדוח באשר לתהליך אשר בוצע ולתוצריו. מומלץ לבצע את כלל הפעילויות המפורטות להלן במטרה לבצע את התהליך באופן אפקטיבי ויעיל.

קיימים בחברה במטרה לזהות את מערכות המידע התומכים בהם, כמו גם, אפקטיביות בקרות אבטחת המידע הקיימות, שנועדו לסייע בהפחתת סיכוני הסייבר.

הסקר בוצע באופן התואם את מסמך תורת ההגנה בסייבר של מערך הסייבר הלאומי (לפירוט אודות מערך הסייבר הלאומי, ראה נספח א').

1.5. תרחיש ייחוס

ⓘ תרחיש הייחוס נגזר מאופי החברה ומתחומי פעילותה והוא מהווה בסיס לתהליך הערכת הסיכונים ולקביעת היקף ומטרות תוכנית הפחתת הסיכונים. בעת גיבוש התרחיש, יש לשקול מיהם השחקנים שעלולים לפעול כנגד החברה, מהי המוטיבציה לפעילותם, מטרות התקיפה והשלכותיה.
לגיבוש התרחיש ניתן להסתייע בנספח ג', גיבוש תרחיש ייחוס במרחב הסייבר.

מניתוח אופי החברה ותחומי פעילותה, אשר התבצע עם תחילת סקר הסיכונים, גובש תרחיש הייחוס המתואר להלן:

- איום ייחוס (שחקנים)- פושעי סייבר, ריגול תעשייתי, האקרים, האקטיביסטים, גורמים פנימיים.
- מוטיבציית השחקן- רווח פיננסי, השבתה/הפרעה/חבלה, יתרון תחרותי, נקמה/מרמור, אנרכיה/כאוס, טקטיקה/אסטרטגיה, חברתית/מוראלית, פרסום הצהרה.
- מטרות- חשיפת/הדלפת מידע רגיש, שיבוש/פגיעה במידע, פגיעה בזמינות מידע, פגיעה בתדמית ומוניטין.
- השפעה- אובדן הכנסה/נזק כלכלי, פגיעה במוניטין, הפללה/תביעה, סנקציות והגבלות, אובדן אמון ציבור/משקיעים, איכות הסביבה, תודעתית.

ההמלצות המופיעות במסמך זה, נכתבו בהלימה לאיום ייחוס זה.

ⓘ להלן תרחיש ייחוס אופייני לחברות במגזר הקמעונאי, עליו ניתן להתבסס בעת ביצוע הסקר, או, לחלופין, לבצע את ההתאמות הנדרשות לחברה.

תוקף חיצוני המבקש להשיג רווח כספי או יתרון תחרותי באמצעות חדירה בלתי מורשית לעמדות המכירה (PoS) או למסדי הנתונים של החברה לשם גניבת פרטי כרטיסי אשראי או נתונים עסקיים אודות ספקים ולקוחות. לחילופין, גורם פנימי, בדגש על עובד ממורמר, המבקש לנקום בחברה או להשיג רווח כספי עלול לנצל את הגישה שלו למערכות המידע לשם שיבוש תהליכים עסקיים או ביצוע הונאה.

1.6.סיכונים מרכזיים שזוהו

ⓘ יש לעדכן את התרשים שלהלן בהתאם לתוצאות שהתקבלו בסקר הסיכונים.

להלן פילוח סיכוני הסייבר שזוהו במסגרת סקר הסיכונים בהתאם לרמת החומרה שלהם:

ⓘ במטרה לסייע להנהלת החברה להתמקד בסיכונים המרכזיים שזוהו במסגרת הסקר, מומלץ לרכז בסעיף זה את 7-15 הסיכונים בעלי רמת החומרה הגבוהה ביותר, מתוך אלו המופיעים בפרק 2 להלן. ראוי כי הנהלת החברה תדון בהשלכות העסקיות במקרה של התממשות סיכונים אלו ותקיים מעקב אחר התוכנית להפחתתם. בהתאם לצורך ולשיקול הדעת של עורך הסקר, ניתן לצמצם או להגדיל את מספר הסיכונים אשר יופיעו בסעיף זה.

להלן תמצית הסיכונים אשר זוהו במהלך הסקר:

מס"ד	תיאור הסיכון	רמת הסיכון	המלצות
1.	גישה בלתי מורשית לעמדות מכירה כתוצאה ממערכות הפעלה בעלות חולשות אבטחה ידועות.		
2.	דלף כרטיסי אשראי של לקוחות מעמדות מכירה (PoS).		
3.	היעדר יכולת לשייך פעילות למשתמש ייחודי עקב שימוש בחשבון משתמש גנרי.		
4.	אי זמינות עמדות המכירה כתוצאה ממתקפת מניעת שירות.		
5.	גישה לא מבוקרת של ספקים חיצוניים למערכת המלאי.		
6.	רשת אלחוטית (Wi-Fi) לא מאובטחת בעלת קישור ישיר לרשת הפנימית (LAN) של החברה.		

מס"ד	תיאור הסיכון	רמת הסיכון	המלצות
7.	דלף נתוני לקוחות מאתר האינטרנט המכירתי.		
8.	אי זמינות אתר האינטרנט עקב תקיפת מניעת שירות.		
9.	השחתת (Defacement) אתר האינטרנט.		
10.	דלף פרטי חברי מועדון הלקוחות.		

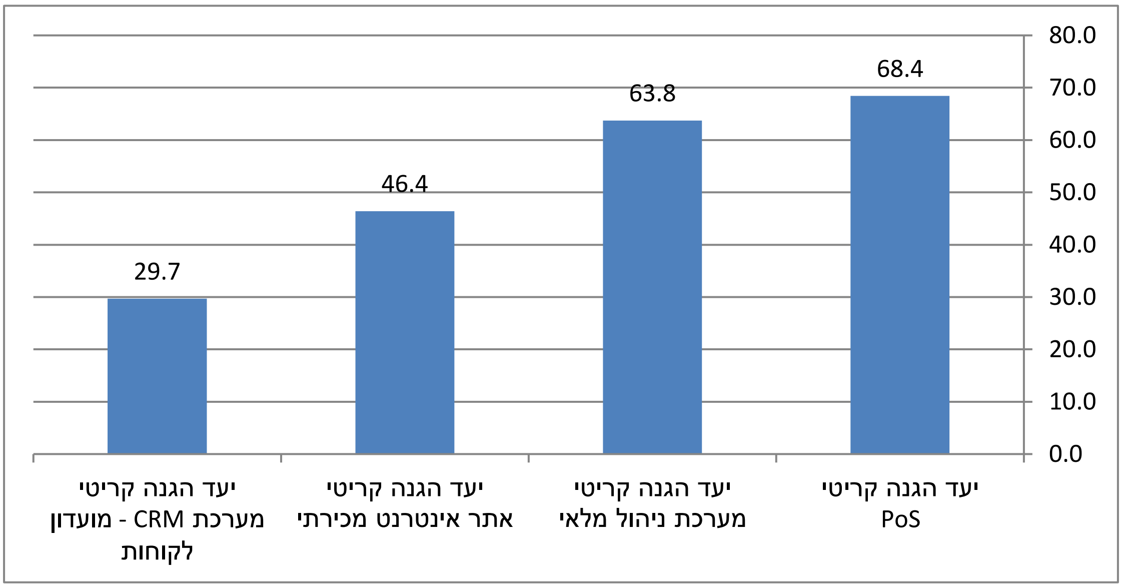
פירוט הסיכונים מופיע בפרק 2 להלן.

1.7 סביבת הבקרה

בקרות מצמצמות את החשיפה לסיכוני סייבר העלולים לפגוע ביעדי הארגון. נוכח זאת, קיימת חשיבות לעצם קיום הבקרות השונות, כמו גם ביישומן הנכון, וזאת במטרה להשיג אפקטיביות מירבית בהפחתת רמת הסיכון.

להלן תוצאות חישוב האפקטיביות הממוצעת של סביבת הבקרה, בפילוח ליעדי הגנה אופייניים ותהליכים כלליים:

ⓘ יש להעתיק את גרף 1 המופיע בגיליון "עיבודים" שבקובץ אקסל.



ⓘ בטבלה שלהלן מופיעה רמת האפקטיביות הממוצעת של הבקרות השונות שיושמו בפילוח ליעדי הגנה קריטיים ובקרות כלליות.
יש להעתיק את טבלה 1 המופיעה בגיליון "עיבודים".

יעדי הגנה	אפקטיביות ממוצעת בערך כמותי	אפקטיביות ממוצעת בערך איכותני
יעד הגנה אופייני עמדות מכירה (PoS)	68.4	גבוה מאוד
יעד הגנה אופייני מערכת ניהול מלאי	63.8	גבוה מאוד
יעד הגנה אופייני אתר אינטרנט מכירתי	46.4	גבוה
יעד הגנה אופייני מערכת CRM - מועדון לקוחות	29.7	בינוני
תהליכים כלליים	43.8	בינוני

1.8. תובנות מרכזיות

ⓘ מטרת סעיף זה הינה יצירת זיקה בין סיכוני סייבר שזוהו לבין השלכות אפשריות על הפעילות העסקית של החברה. ראוי כי המידע המופיע בסעיף זה יהווה מצע לדיון משותף של גורמי הגנת הסייבר עם הנהלת החברה, אשר במסגרתו יוקצו המשאבים הנדרשים להפחתת הסיכונים. להלן מספר דוגמאות של השלכות אופייניות למגזר הקמעונאי.

1.8.1. דלף מידע מעמדות המכירה - במהלך סקר הסיכונים, נוכחנו כי עמדות המכירה בסניפים מהוות יעד קל לתקיפה, כתוצאה משימוש במערכות הפעלה מיושנות בעלות חולשות אבטחה ידועות. להלן השלכות אפשריות, כתוצאה מתקיפה ופגיעה בעמדות מכירה:

- חשיפה לאחריות פלילית של נושאי משרה בחברה, כתוצאה מגניבת פרטי לקוחות לרבות פרטי אשראי וכפועל יוצא, אי עמידה בתקנות הגנת הפרטיות;
- פגיעה בהיקף הפדיון בסניף, כתוצאה מהשבתת עמדות מכירה וכפועל יוצא היעדר יכולת לחייב לקוחות;
- פגיעה במוניטין, כתוצאה מהיעדר יכולת לשרת לקוחות בסניף.

תקיפה בו זמנית של מספר סניפים, תוך ניצול אותן החולשות בעמדות המכירה, עלולה להוביל להד תקשורתי ולפגיעה משמעותית במוניטין החברה, ובמידה ומדובר במספר רב של סניפים, גם לנזק כספי משמעותי.

נוכח זאת, קיימת חשיבות בניטור של עמדות המכירה, וזאת במטרה לזהות מהר ככל שניתן פעילות חריגה שעלולה להעיד על אירוע סייבר. בנוסף, מומלץ להימנע משמירה מקומית של מידע רגיש, דוגמת פרטי אשראי, ובמידה והדבר לא ניתן לביצוע, ראוי להצפין את המידע. (למידע נוסף, ראה סיכונים xx-yy)

1.8.2. היעדר שליטה של אגף מערכות מידע על מערכות תפעוליות - נוכחנו כי מערכות טכנולוגיות תפעוליות (Operational Technology) בסניפים דוגמת מוני חשמל, מצלמות אבטחה ושעוני נוכחות, אינן מנוהלות על ידי אגף מערכות מידע ולעיתים אף מותקנות ללא ידיעתו. כתוצאה מכך, נמצאו מערכות אשר הגדרות האבטחה שלהן אינן תואמות את מדיניות החברה ועלולות להוות נקודת תורפה ברשת החברה.

במהלך הסקר התברר כי רשת התקשורת המשמשת את מצלמות האבטחה, אשר אינה כוללת בקרות אבטחת מידע נאותות, קושרה לרשת המנהלית של החברה, ללא ידיעת אגף מערכות מידע, באופן החושף את הרשת המנהלית לסיכון של חדירת גורם חיצוני עוין. עוד נמצא, כי גישה למערכות תפעוליות

שונות, לרבות מוני החשמל ומערכות ניהול בניין (BMS) מבוצעות ללא בקרה וניטור. חולשות אלו נובעות במידה רבה נוכח העובדה כי אגף מערכות מידע אינו מעורב בחלק מהפעילויות הנוגעות לתחום טכנולוגיות המידע המתקיימות בסניפים ועל כן אין באפשרותו להוות מנחה מקצועי וגורם בקרה על פעילויות אלו.

במטרה להפחית את הסיכון הזה, ראוי כי מחלקת מערכות מידע וממונה הגנת הסייבר יערכו בהקדם סקר סיכונים מקיף ברשתות התפעוליות של החברה, בדגש על זיהוי סיכוני סייבר וגיבוש תוכנית הפחתה (למידע נוסף, ראה סיכונים xx-yy)

1.8.3. <u>פגיעה באספקת סחורה בשל אי זמינות מערכות מידע ותשתית - מבדיקתנו עולה כי קיימים סיכונים שונים אשר עלולים להוביל לפגיעה בתהליך אספקת הסחורה. במסגרת זאת, נמצא כי רשת המסופונים המשמשת לצורך ניהול מלאי החברה מתבססת על רשת אלחוטית בלתי מאובטחת אשר הינה בעלת קישור ישיר לרשת הפנימית (LAN) של החברה. עוד עולה כי גישת יצרן מערכת המלאי לשם תמיכה במערכת המותקנת בחברה מבוצעת באופן בלתי מבוקר (ראה גם להלן).</u>

<u>מאחר והחברה תתקשה לקיים לאורך זמן את תהליך ניהול המלאי - קליטה, מיון והפצה - ללא מערכות המידע, קיימת חשיבות רבה לזמינות מערכות אלה. לאי זמינות של מערכות אלה, עלולות להיות השלכות שונות, דוגמת: (למידע נוסף, ראה סיכונים xx-yy)</u>

- נזק כספי כתוצאה מחוסר יכולת לקלוט מלאי למחסנים;
- מלאי חסר בסניפים כתוצאה מפגיעה בתהליך ההפצה;
- פגיעה במוניטין כתוצאה מאי אספקת סחורה ללקוחות.

1.8.4. <u>היעדר מנגנון אחיד ומאובטח לגישה מרחוק - נוכחנו כי גישה מרחוק למערכות המידע של החברה על ידי ספקים חיצוניים וגורמי צד ג' אחרים, מתאפשרת במספר דרכים ובאופן שאינו עומד בסטנדרטים מקובלים של הגנת סייבר- לרבות גישה שאינה מוגבלת מבחינת מועד ההתחברות, שימוש בשם משתמש גנרי לצורך התחברות, והיעדר רישום של פעולות המבוצעות מרחוק. גישה מרחוק לרשת החברה מהווה בהגדרה חולשה דרכה עלולים לחדור גורמים בלתי מורשים לרשת החברה.</u>

על כן קיימת חשיבות רבה לאפשר גישה מרחוק דרך מערכת מרכזית אחת, ליישם מנגנוני הזדהות חזקה והצפנת תווך התקשורת, וכן לקיים בקרה שוטפת על השימוש במערכת. לאור המספר הרב של ספקים חיצוניים והגישה המתאפשרת לחלקם למערכות מידע רגישות של החברה, ראוי לשקול שימוש במערכות להקלטת פעילות ספקים חיצוניים. למערכות אלו ערך הרתעתי והן עשויות לסייע בתחקור אירועי סייבר. למידע נוסף, ראה סיכונים (XX-YY)

2. פירוט הסיכונים

בסעיף זה יש לפרט את סיכוני הסייבר אשר זוהו במהלך סקר הסיכונים. הדוגמאות להלן מתייחסות לסיכונים אליהם חשופים יעדי ההגנה האופייניים למגזר הקמעונאי.

בהתאם להיקף הסקר, ניתן להסתייע בנספחים ו או ז הכוללים רשימת סיכוני סייבר אופייניים למגזר הקמעונאי. ככל שזוהו במסגרת הסקר סיכונים נוספים, יש להוסיפם

ⓘ עבור כל סיכון, נדרש:
א. לקבוע את הסבירות להתממשותו ועוצמתו, בהתאם למדדים המופיעים בנספח ח'.
ב. לחשב את רמת הסיכון (גבוהה, בינונית, נמוכה) בהתאם לנספח ח' בהתאם לעוצמתו והסבירות להתרחשותו.
ג. לתאר תרחיש להתממשות הסיכון, התואם את תרחיש הייחוס של החברה.
ד. לתאר השלכות עסקיות במקרה של התממשות הסיכון.
ה. לגבש המלצות ליישום לשם הפחתת הסיכון, בהתבסס על תקנים מקובלים דוגמת תוה"ג

בהתאם לדוגמאות להלן.

2.1. יעד הגנה אופייני- עמדות מכירה (PoS)

רקע: עמדות מכירה (Point of Sale) הינן הפלטפורמה המשמשת את החברה לגביית תשלום לקוחות בגין מוצרים שנרכשו. מטבע הדברים, מעובד ונשמר בעמדות מכירה מידע פיננסי רגיש ופרטי כרטיסי אשראי, המהווים יעד לתקיפה.

נוכח זאת, גישה בלתי מורשית למערכות אלה, בדגש על חשיפת המידע הפיננסי השמור בהן, מהווה סיכון שיש לפעול להפחתתו.

ⓘ בפסקה להלן יש לציין את האפקטיביות הממוצעת של הבקרות השונות שיושמו עבור יעדי ההגנה האופייני עמדות מכירה (PoS).
יש להעתיק את הערך המופיע בתא B3 בגיליון "עיבודים" בקובץ האקסל.

אפקטיביות סביבת הבקרה: במהלך סקר הסיכונים, נסקרה סביבת הבקרה של עמדות המכירה. מסקירה זו עולה כי ממוצע אפקטיביות הבקרות הינו XY%.

2.1.1. סיכון 1: גישה בלתי מורשית לעמדות מכירה כתוצאה מניצול חולשות אבטחה ידועות במערכות הפעלה.

ⓘ נא למחוק את המיותר עבור רמת הסיכון, הסתברות הסיכון ועוצמת הסיכון.

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- תוקף הפורץ לעמדות המכירה של החברה באמצעות ניצול חולשות אבטחה ידועות במערכות ההפעלה, תוך שימוש בכלי תקיפה הזמינים לכל דורש ברשת האינטרנט.

השלכות עסקיות פוטנציאליות

- פריצה לעמדות המכירה והשבתתן או פגיעה במידע המצוי בהן עלולה לגרום לפגיעה במוניטין החברה ואף לנזקים כספיים. .

מצב קיים

- נמסר לנו, כי גרסת מערכת ההפעלה של עמדות המכירה והשרתים המשמשים אותן אינן נתמכות יותר על ידי היצרן. מבדיקתנו עולה, כי גרסה זו כוללת פגיעויות אבטחת מידע ידועות.
- מבדיקתנו עולה כי גרסת מערכת ההפעלה של חלק מעמדות המכירה והשרתים אינה הגרסה העדכנית ביותר האפשרית.

המלצות

- מומלץ לבחון את האפשרות לשדרג את מערכות ההפעלה לגרסה הנתמכת על ידי היצרן, וזאת בתיאום עם יצרן תוכנת עמדות המכירה.
- במידה ולא ניתן לשדרג את מערכת ההפעלה של עמדות המכירה, ראוי לבחון בקרות מפצות, דוגמת:
  - סגמנטציית רשת;
  - Virtual Patching;
  - Personal Firewall.

2.1.2. סיכון 2: דלף מידע כרטיסי אשראי של לקוחות מעמדת המכירה

ⓘ נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- דלף פרטי כרטיסי אשראי כתוצאה מתקיפת עמדות מכירה תוך ניצול העובדה כי פרטי כרטיסי האשראי נשמרים באופן לא מוצפן בעמדות המכירה.

השלכות עסקיות פוטנציאליות

- דלף מידע רגיש דוגמת פרטי כרטיסי אשראי, צפוי לפגוע במוניטין החברה ועלול להוביל לחשיפה משפטית ורגולטורית עקב אי עמידה בדרישות חוק הגנת הפרטיות והנחיות תקן PCI.

מצב קיים

- נמסר לנו, כי פרטי כרטיסי אשראי המשמשים לתשלום בעמדות מכירה מאוישות או בשירות עצמי, נשמרים באופן זמני בעמדת המכירה, עד להשלמת שידורם לשב"א; לאחר מכן נמחקים נתונים אלו מעמדת המכירה.
- עוד נמסר שהחברה בתהליכי רכש של מוצר אבטחת מידע אשר מטרתו, בין היתר, הינה הצפנת פרטי כרטיסי האשראי, מיד עם שמירתם בעמדת המכירה.

המלצות

- מומלץ לבחון את מחויבותה של החברה ליישום תקן ה-PCI.
- מומלץ לקדם את הטמעת המוצר הטכנולוגי המאפשר להצפין נתוני כרטיסי אשראי הנשמרים באופן מקומי בנקודות המכירה.

2.1.3. סיכון 3: היעדר יכולת לשייך פעולות המבוצעות בעמדת המכירה לעובד מסוים, עקב שימוש בחשבון משתמש גנרי בעמדות המכירה.

ⓘ נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- חשיפה של סיסמת גישה למערכת של החברה, לעובדים לא מורשים או לגורמים זרים.

השלכות עסקיות פוטנציאליות

- חשבון משתמש גנרי פירושו שימוש באותו חשבון על ידי מספר עובדים בארגון. הקצאת חשבון גנרי פוגעת באחד העקרונות המרכזיים בכל הקשור לבקרת גישה- אחריותיות (Accountability).
- מצב זה מעלה את הסבירות להתממשות סיכון של הונאות ומעילות, עקב חוסר יכולת לשייך פעולות המבוצעות בעמדת המכירה או חריגה ממדיניות הגנת הסייבר, לעובד מסוים.

מצב קיים

- נמסר לנו כי במוקדי המכירה לסוגיהם (חנויות, עמדות מכירה במרכזים מסחריים וכו'), השימוש בעמדות המכירה מתבצע באמצעות חשבון משתמש גנרי המשותף לכלל העובדים.
- מבדיקתנו עולה כי ההרשאות לכלל החשבונות הגנריים הינן זהות, וכוללות הרשאות חזקות מבחינה עסקית, לרבות שינוי ומחיקה של עסקאות בהיקף כספי גבוה.
- נמסר לנו כי כלל החשבונות הגנריים מוגדרים כ-Local Admin.

המלצות

- מומלץ, ככל הניתן, להימנע מכל שימוש בחשבונות משתמש גנריים.
- במידה וקיים אילוץ עסקי/תפעולי בחשבון משתמש גנרי, מומלץ ליישם את הצעדים הבאים:

❖ להקצות לחשבון המשתמש הגנרי הרשאות מוגבלות ככל שניתן, בהתאם לתפקידו- מוכרן, מנהל סניף וכו'
❖ להגדיר כי החשבון הגנרי יכול להיות פעיל רק בעמדת מכירה אחת, בכל רגע נתון.
❖ לנטר את הפעילות המבוצע בעמדות המכירה במטרה לזהות חריגות, דוגמת: היקף עסקאות גבוה מהרגיל, ריבוי פעילות זיכוי לקוח וכו'.
❖ מומלץ שלא להגדיר חשבונות גנריים כ-Local Admin.

2.2. מערכת ניהול מלאי

רקע

כל עסק קמעונאי נדרש לניהול מלאי, בין אם מדובר בחומרי גלם או תוצרת גמורה. לניהול שוטף ואמין של מלאי חשיבות רבה לשם תמיכה בפעילות העסקית, כמו גם כמרכיב מרכזי בדוחות הכספיים של החברה.

הגישה למערכת ניהול המלאי נעשית באמצעות התקני קצה מסוגים שונים, לרבות מחשבים נייחים, מחשבים ניידים, מסופונים, טאבלטים ועוד. אמצעי גישה אלו משמשים הן עובדים פנימיים של החברה והן ספקים חיצוניים. כפועל יוצא, קיימת חשיבות בניהול בקרת הגישה וביישום בקרות על התקני הקצה השונים בהתאם לסיכונים אליהם הם חשופים.

ⓘ בפסקה להלן יש לציין את האפקטיביות הממוצעת של הבקרות השונות שיושמו עבור יעדי ההגנה האופייניים למערכת ניהול מלאי.
יש להעתיק את הערך המופיע בתא B4 בגיליון "עיבודים" בקובץ האקסל.

הערה:

אפקטיביות סביבת הבקרה: במהלך סקר הסיכונים, נסקרה סביבת הבקרה של מערכת ניהול המלאי. מסקירה זו עולה כי ממוצע אפקטיביות הבקרות הינו XY%.

ⓘ נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.

2.2.1. סיכון 4: גישה לא מבוקרת של ספקים חיצוניים למערכת המלאי

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- שיבוש נתונים או פגיעה בזמינות מערכת מלאי כתוצאה מגישה לא מאובטחת מרחוק של גורם צד ג' המספק שירותי תמיכת IT או, לחלופין, כתוצאה מהיעדר ניטור על פעולות המבוצעות במערכת על ידי גורמי צד ג' המספק מלאי לחברה.

השלכות עסקיות פוטנציאליות

- תוקף עלול לנצל גישה לא מאובטחת מרחוק של אחד מספקי החברה, או לחלופין, ספק בעל הרשאות כתיבה לצורך שיבוש נתוני המלאי של החברה. בעקבות כך, החברה עלולה לספוג נזקים כספיים, כתוצאה מאי זמינות מוצרים ללקוחותיה.

מצב קיים

- נמסר לנו כי מנגנון הגישה מרחוק של ספק מערכת המלאי לשם תמיכה בה מבוסס על אימות באמצעות סיסמה סטטית, קרי, סיסמה שאינה משתנה.
- מבדיקתנו עולה כי הגישה מרחוק של הספק מתאפשרת לכל אורך ימי השבוע ושעות היממה.
- עוד נמסר כי החברה אינה מסדירה במסגרת חוזה ההתקשרות, את דרישות הגנת סייבר ואבטחת המידע שלה מספקים חיצוניים.
- כמו כן, מבדיקתנו עולה כי החברה אינה מתעדת ומנטרת את פעילותם של גורמי צד ג' שהינם ספקי סחורה של החברה ובעלי הרשאות כתיבה למערכת המלאי.
- במענה לבקשתנו לקבל תיעוד בנושא, נמסר לנו כי תהליכי תיקוף משתמשים והרשאות של משתמשים בעלי גישה מרחוק אינם מבוצעים.

המלצות

- מומלץ כי הגישה מרחוק למערכות החברה תבוצע תוך שימוש בשמות משתמש ייחודיים, הזדהות חזקה והצפנת תווך התקשורת.
- מומלץ, ככל שהדבר אפשרי, לצמצם את חלון הזמן בו יותר לגורם חיצוני לגשת למערכות החברה.
- מומלץ לגבש סט דרישות להגנת סייבר ואבטחת מידע ולכלול אותן בחוזי ההתקשרות עם ספקים חיצוניים וגורמי צד ג'.
- מומלץ לאכוף תיעוד של כלל הפעולות המבוצעות במערכת המלאי על ידי גורמי צד ג'.

- ככל אשר קיימת מערכת ניטור, מומלץ להגדיר חוקים שמטרתם לזהות פעילות חריגה המבוצעת על ידי גורמי צד ג' במערכת המלאי של החברה.
- מומלץ לשקול רכש מערכת הקלטה לשם תיעוד מפורט של פעולות המבוצעות במערכות החברה, בדגש על פעולות המבוצעות בגישה מרחוק ועל ידי גורמי צד ג'.
- מומלץ לבצע תהליך תיקוף משתמשים והרשאות עתיים לבעלי גישה מרחוק, בדגש על ספקים וגורמי צד ג', אחת לשנה לכל הפחות.

2.2.2. סיכון 5: רשת אלחוטית (Wi-Fi) לא מאובטחת בעלת קישור ישיר לרשת הפנימית (LAN) של החברה

ⓘ נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.

2.2.3.

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- ניצול הגדרות לקויות וחולשות אבטחת מידע על ידי גורם זדוני, לצורך פריצה לרשת אלחוטית, המשמשת לקישור מסופונים למערכות המידע של החברה.

השלכות עסקיות פוטנציאליות

- חדירה לרשת האלחוטית עלולה להוות פלטפורמה לחדירה לרשת הארגון הפנימית (LAN). נוכח זאת, תוקף עלול להשיג גישה למערכת ניהול המלאי של הארגון, ולשבש את המידע שבה, דבר שביכולתו לפגוע בתהליך המכירות של החברה ולהסב נזק כספי.
  יתרה מכך, הוא עלול להרחיב את תקיפתו למערכות נוספות של החברה, ולהוביל לפגיעה ברמה כלל ארגונית, דוגמת: הצפנת המידע השמור במערכות החברה.

מצב קיים

- נמסר לנו כי המסופונים בהם נעשה שימוש במחסן הלוגיסטי בחברה מקושרים לרשת אלחוטית (Wi-Fi) ללא אימות וללא הצפנת התווך. רשת זו מקושרת באופן ישיר לרשת הפנימית (LAN) של החברה ללא כל הגנות.
- במצב זה, גורם זדוני עלול להתחבר בקלות יחסית לרשת האלחוטית ומִמנה לדלג לרשת הפנימית של החברה ולחדור למערכת ניהול המלאי ולמערכות מידע אחרות.

המלצות

- יש ליישם פרוטוקולים דוגמת WPA2 ומנגנוני הגנה אחרים אשר יאפשרו שימוש מאובטח ברשת האלחוטית - לגורמים מורשים בלבד.

- במטרה להגן על הגישה לרשת הפנימית, מכיוון הרשת האלחוטית מומלץ ליישם בקרות אבטחה דוגמת: firewall, IPS וכו'.
- מומלץ לבצע בדיקת חדירות חיצוניות ופנימיות עתיות במטרה לוודא את רמת האבטחה של הרשת האלחוטית.

2.3. אתר אינטרנט מכירתי

אתר האינטרנט של החברה משמש הן כאתר תדמיתי והן כאתר אינטרנט מכירתי. ככזה, הוא חשוף לתקיפות שונות מרשת האינטרנט, אשר עלולות לגרום לנזקים לחברה, דוגמת אלה המפורטים להלן.

הערה

> ⓘ **בטבלה שלהלן מופיעה האפקטיביות הממוצעת של הבקרות השונות שיושמו עבור יעדי ההגנה האופייניים לאתר אינטרנט מכירתי.**
> **יש להעתיק את הערך המופיע בתא B5 בגיליון "עיבודים" בקובץ האקסל.**

אפקטיביות סביבת הבקרה: במהלך סקר הסיכונים, נסקרה סביבת הבקרה של אתר האינטרנט המכירתי. מסקירה זו עולה כי ממוצע אפקטיביות הבקרות הינו XY%.

2.3.1. סיכון 6: דלף מידע רגיש מאתר האינטרנט המכירתי

> ⓘ **נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.**

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- תוקף המנצל חולשות באבטחת אתר האינטרנט לשם גישה בלתי מורשית לנתונים השמורים בו, דוגמת לקוחות, קמפיינים עתידיים של החברה וכו'.

השלכות עסקיות פוטנציאליות

- חשיפת נתוני לקוחות או כל מידע רגיש אחר השמור באתר האינטרנט עלולה להוביל לנזק מהותי למוניטין החברה, ולנזק פיננסי בעקבותיו.

מצב קיים

- לא מתקיים תהליך פיתוח מאובטח בחברה, וכן לא מתקיים code review, מצב המעלה את הסבירות לקיום חשיפות אבטחה בקוד אתר האינטרנט.
- לא מתבצעים סקרי סיכונים ומבדקי חדירה (Penetration Tests) עתיים לאתר האינטרנט.

- לא הוטמעו כלי אבטחה ייעודיים להגנה על אתר האינטרנט.

המלצות

- מומלץ כי תיושם מתודולוגיית פיתוח מאובטח באתר האינטרנט.
- מומלץ לבצע סקרי סיכונים ו-code review טרם העברה לייצור של פיתוחים ושינויי תוכנה.
- מומלץ לקיים מבדקי חדירה עתיים לאתר האינטרנט.
- מומלץ לשקול הטמעת כלי אבטחה וניטור רלוונטיים לאתר האינטרנט, דוגמת Web Application Firewall.

2.3.2. סיכון 7: שיבושים בפעילות אתר האינטרנט עקב תקיפת מניעת שירות מבוזרת (DDoS) או השחתתו (Defacement)

ⓘ נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- תוקף היוצר עומס על משאבי האתר, למשל באמצעות שימוש ברשתות מחשוב שבשליטתו (Botnets) היוצרות היקף חריג של פניות לאתר, או, לחילופין, השחתת האתר באופן המונע אפשרות של שימוש.

השלכות עסקיות פוטנציאליות

- אי זמינות אתר האינטרנט של החברה יוביל לפגיעה ביכולת לספק שירות ללקוחותיה ולפגיעה בהיקף המכירות. יתרה מכך, השחתת אתר אינטרנט מתפרסמת בתוך פרק זמן קצר יחסית בכלי התקשורת ופוגעת במוניטין החברה,, פגיעה העלולה לגרום ללקוחות לעבור ולהשתמש באתר מכירות של מתחרה.

מצב קיים

- נמסר לנו כי החברה אינה מנטרת את אתר האינטרנט, לרבות בהיבטי היקף תעבורה.

- מבדיקתנו עולה כי החברה טרם יישמה מנגנון להתמודדות עם מתקפות מניעת שירות מבוזרות (Anti-DDoS).
- עוד עולה, כי לא מבוצעים מבדקי חדירה עתיים (Penetration Tests) לאתר האינטרנט, שמטרתם לזהות פגיעויות אבטחה ופערים בבקרה אשר עלולים להיות מנוצלים על ידי גורם זדוני.

המלצות

- מומלץ לנטר באופן שוטף את אתר האינטרנט, לרבות בהיבט היקף תעבורה שוטפת, ריבוי ניסיונות גישה כושלים לאזור אישי (ככל שקיים) וכו'.
- מומלץ לשקול הטמעת מנגנון להתמודדות עם מתקפות מניעת שירות מבוזרות.
- מומלץ לבצע מבדקי חדירה עתיים לאתר האינטרנט ולטפל בליקויים, ככל שיתגלו.

2.4. מערכת CRM - מועדון לקוחות

כחלק מפעילותה העסקית, מנהלת החברה מועדון לקוחות בן למעלה מ-200,000 לקוחות. נתוני החברים במועדון הלקוחות כוללים על פי רוב את שמו המלא של הלקוח, מספר תעודת זהות, כתובת, מספר טלפון, רכישות שביצע ותובנות עסקיות (BI) נוספות. כל אלה, הופכות את המידע במערכת ה-CRM ליעד מועדף עבור גורמים זדוניים פנימיים וחיצוניים.

הערה

> **ⓘ בטבלה שלהלן מופיעה האפקטיביות הממוצעת של הבקרות השונות שיושמו עבור יעדי ההגנה האופיינים למערכת CRM - מועדון לקוחות.**
> **יש להעתיק את הערך המופיע בתא B6 בגיליון "עיבודים" בקובץ האקסל.**

אפקטיביות סביבת הבקרה: במהלך סקר הסיכונים, נסקרה סביבת הבקרה של מועדון הלקוחות. מסקירה זו עולה כי ממוצע אפקטיביות הבקרות הינו XY%.

2.4.1. סיכון 8: דלף פרטי נתוני חברי מועדון הלקוחות

> **ⓘ נא למחוק את המיותר עבור רמת הסיכון, סבירות הסיכון ועוצמת הסיכון.**

- רמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- סבירות הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה
- עוצמת הסיכון: גבוהה מאוד / גבוהה / בינונית / נמוכה

תרחיש

- עובד או תוקף חיצוני המנצל חשבון בעל הרשאות גישה מתאימות או חולשות אחרות של מערכת המידע, לצורך פריצה למערכת מועדון הלקוחות של החברה המובילה לדלף המידע הרגיש השמור בה.

השלכות עסקיות פוטנציאליות

- דלף פרטי לקוחות של החברה עלול להוות הפרה של תקנות הגנת הפרטיות.
- זליגת מידע עסקי רגיש למתחרים אשר יוביל לפגיעה במכירות החברה.
- פגיעה במוניטין החברה כתוצאה מפרסום אירוע.

מצב קיים

- מבדיקתנו עולה כי לא קיים יומן רישום מערכת (Log File) על הפעילות המתבצעת במערכת ניהול מועדון הלקוחות.
- עוד עולה, כי לכלל עובדי החברה הרשאות צפייה במערכת ה-CRM, כאשר אין כל מערכת לניטור פעילותם.

המלצות

- מומלץ לבצע אחת לשנה לכל הפחות תהליכי תיקוף משתמשים והרשאות למשתמשים בעלי הרשאות למערכת ה-CRM.
- מומלץ לשקול רכש מערכת לניטור טרנזקציות עסקיות ותפעוליות.
- מומלץ לאכוף ניהול יומן רישום מערכת על הפעולות המבוצעות במערכת ניהול מועדון הלקוחות, שתכלול, לכל הפחות, את השדות הבאים:
  - המשתמש שביצע את הפעולה.
  - כתובת העמדה ממנה בוצעה הפעולה.
  - תאריך הפעולה.
  - שעת הפעולה.
  - מהות הפעולה.

3. אפקטיביות בקרות

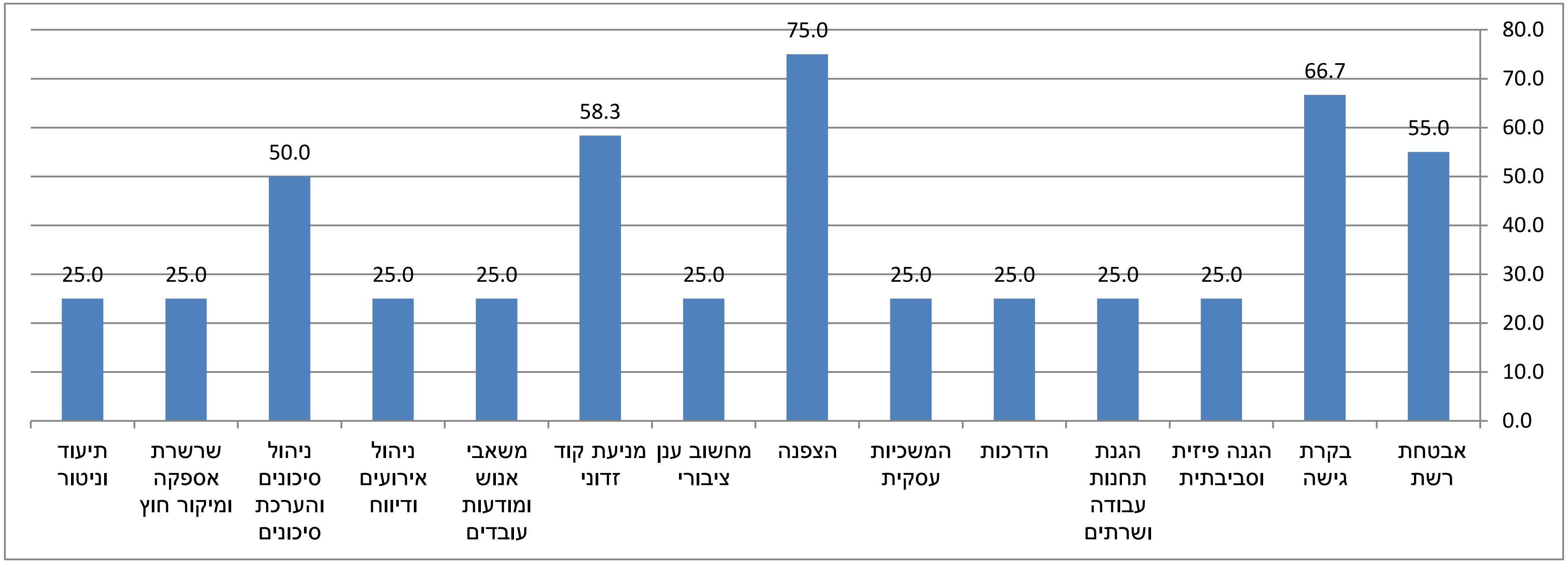
3.1.אפקטיביות ממוצעת של משפחות בקרה אשר יושמו בכלל התהליכים שנסקרו

ⓘ בטבלה שלהלן מופיעה האפקטיביות הממוצעת של הבקרות השונות שיושמו בפילוח למשפחות בקרה בתוה"ג.
יש להעתיק את טבלה 2 המופיעה בגיליון "עיבודים" שבקובץ אקסל.

הערה

משפחת בקרה	אפקטיביות ממוצעת בערך כמותי	אפקטיביות ממוצעת בערך איכותני
אבטחת רשת	55.0	גבוה
בקרת גישה	66.7	גבוה
הגנה פיזית וסביבתית	25.0	בינוני
הגנת תחנות עבודה ושרתים	25.0	בינוני
הדרכות	25.0	בינוני
המשכיות עסקית	25.0	בינוני
הצפנה	75.0	גבוה מאוד
מחשוב ענן ציבורי	25.0	בינוני
מניעת קוד זדוני	58.3	גבוה
משאבי אנוש ומודעות עובדים	25.0	בינוני
ניהול אירועים ודיווח	25.0	בינוני
ניהול סיכונים והערכת סיכונים	50.0	גבוה
שרשרת אספקה ומיקור חוץ	25.0	בינוני
תיעוד וניטור	25.0	בינוני
כלל משפחות הבקרה	**43.8**	**בינוני**

ⓘ יש להעתיק את גרף 2 המופיעה בגיליון "עיבודים".



נספח א'- אודות מערך הסייבר הלאומי

ב-7 באוגוסט 2011 החליטה ממשלת ישראל על הקמתו של מטה הסייבר הלאומי (במקור המטה הקיברנטי הלאומי) בכפיפות לראש ממשלת ישראל. על המטה הוטלה האחריות לבניית המדיניות והאסטרטגיה הלאומית בתחומי הסייבר ונקבע כי הוא יקדם ויסדיר תהליכי הגנה לאומיים, יפתח את היכולות הלאומיות בסייבר ויבסס שיתופי פעולה בין-לאומיים בתחום.

על בסיס האסטרטגיה שגיבש המטה עם כלל הגופים הרלוונטיים לתחום קיבלה ממשלת ישראל ב-15 בפברואר 2015 שתי החלטות. הראשונה, עוסקת באסטרטגיית בניין העמידות והחוסן בסייבר של המשק האזרחי, ובפרט בהיערכות הממשלתית מול המשק ובתוך הממשלה. השנייה, קבעה כי יוקם גוף נוסף בשם הרשות הלאומית להגנת הסייבר, שייעודו הגנת מרחב הסייבר האזרחי. תפקידיו העיקריים של הגוף החדש הינם ניהול כלל מאמצי ההגנה האופרטיביים במרחב הסייבר, הפעלת מרכז לסיוע בהתמודדות עם איומי סייבר (ה-CERT הלאומי) וחיזוק החוסן של כלל המשק בתחום.

הרשות הלאומית להגנת הסייבר החלה לפעול בשנת 2016 כגוף בעל מאפיינים ביטחוניים-אופרטיביים לצד מאפיינים אזרחיים שמוביל את מאמצי ההגנה בשטח כנגד תקיפות סייבר על המשק האזרחי. בין היתר, הרשות מנחה את גופי תשתיות המדינה הקריטיות, את המגזרים החיוניים במשק ופועלת לקידום העלאת העמידות בכלל המרחב האזרחי.

בשלהי 2017 החליטה ממשלת ישראל לאחד את שני הגופים, מטה הסייבר והרשות להגנת הסייבר, לכדי יחידה אחת - "מערך הסייבר הלאומי". בהחלטת הממשלה נקבע, כי יחידה זו תהיה אחראית על כלל היבטי הגנת הסייבר במרחב האזרחי, החל מגיבוש מדיניות ובניין כוח טכנולוגי, ועד הגנה מבצעית בסייבר.

כל אזרח או גורם שחושב שהוא מותקף בסייבר יכול להתקשר ולקבל תגובה טלפונית ראשונית בטלפון 119.

נספח ב'- רשימת ראיונות שנערכו במסגרת הסקר

נספח ז'ה משמש בתחילת הסקר לגיבוש רשימת הפגישות הנדרשות עם הגורמים העסקיים וגורמי המחשוב השונים בחברה. בהתאם לפגישות שהתקיימו בפועל, לרבות פגישות שנוספו או נגרעו, נדרש לעדכן את הטבלה שלהלן:

מס"ד	שם	תפקיד	מועד הפגישה
1.	גברת ישראלה ישראלי	סמנכ"לית כספים	9.5.2018
2.	מר ישראל ישראלי	מנהל רכש	17.8.2018
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

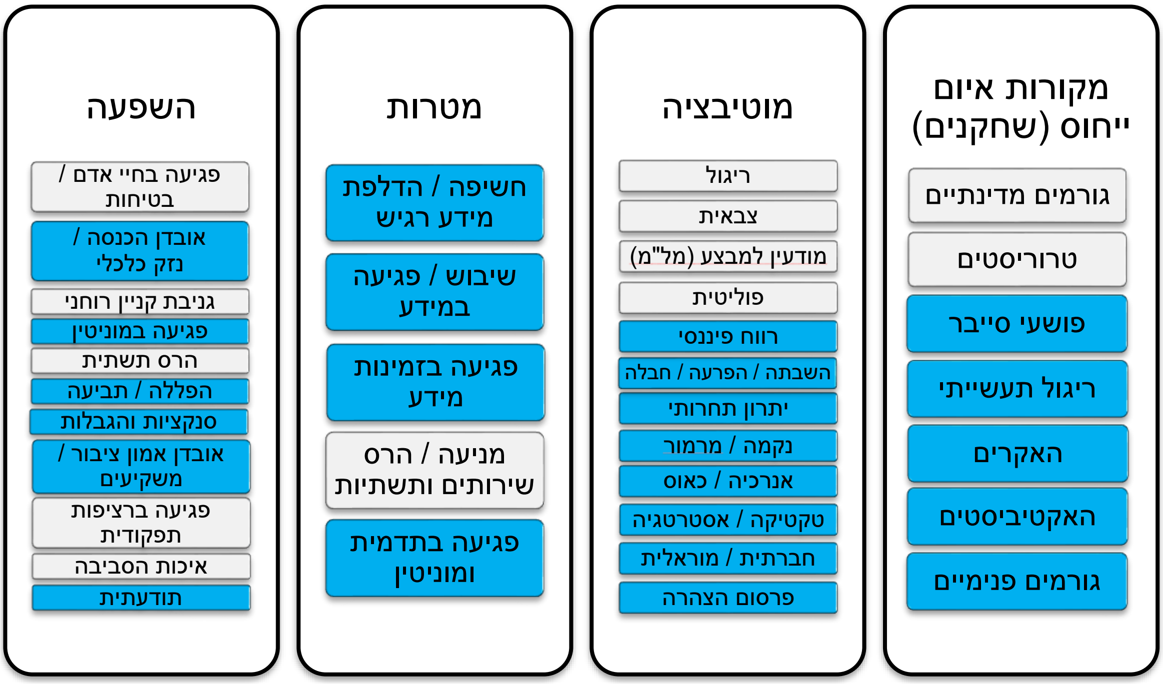
נספח ג'- גיבוש תרחיש ייחוס במרחב הסייבר

נספח זה משמש לגיבוש תרחיש ייחוס במרחב הסייבר, המוצג בסעיף 1.5 לעיל. על מנת לגבש את תרחיש הייחוס של החברה, יש לקיים תהליך חשיבה בהשתתפות גורמי הגנת הסייבר וגורמים עסקיים אשר יבחן את הרלוונטיות של הרכיבים השונים הנכללים במסגרת ארבעת הממדים המרכיבים את תרחיש הייחוס:

- מקורות איום ייחוס (שחקנים);
- מוטיבציה;
- מטרות;
- השפעה.

רכיבים בעלי מידת רלוונטיות נמוכה למגזר הקמעונאי מסומנים באפור.

בעת גיבוש תרחיש ייחוס לארגון יש להתייחס לממדים הבאים:



ממד ראשון - מקורות איום ייחוס (שחקנים)

כדי לאפיין את מקורות האיום, יש לבחון את הרשימה הבאה ולזהות מתוכה מקורות איום הרלוונטיים לחברה. לצורך שלמות התמונה האפשרית, נכללים ברשימה זו גורמים רלוונטיים למגזר הקמעונאי לצד גורמים רלוונטיים פחות, המופיעים בטקסט אפור. יש לשלב את מקורות האיום הרלוונטיים בסעיף 2.1 לעיל.

- גורמים מדיניתיים- עלולים להוציא לפועל מנעד רחב של איומים, שיובילו לנזקים שונים, החל מהשחתת אתר אינטרנט ועד לנזק נרחב לתשתית.
- טרוריסטים- גורמים אלה מעוניינים להפיץ טרור באוכלוסייה האזרחית, בין היתר באמצעות תקיפות פישינג לשם גניבת כספים או איסוף מידע רגיש, כמו גם על ידי תקיפות סייבר כנגד מתקני תשתית קריטיים.
- ריגול תעשייתי ופושעי סייבר- המניע לפעילות גורמים אלה הינה כספית. במסגרת זאת, הם נוקטים בשיטות שונות במטרה לגנוב מידע מסחרי רגיש, לסחוט ארגונים ואף לגנוב פרטי זהות של משתמשים ולקוחות.
- האקרים- חברי קבוצה זו מעוניינים לפרוץ לרשתות מחשוב ואפליקציות, בין היתר, במטרה לרכוש לעצמם מוניטין. ההאקרים נבדלים ברמת המיומנות שלהם, כאשר חלקם מבצעים תקיפות על בסיס כלים הזמינים באינטרנט, וחלקם בעלי יכולות גבוהות של תכנות ו/או הכרת תשתית.
- האקטיביסטים- האקרים בעלי רמת מיומנות מגוונת, אשר המוטיבציה לפעילותם הינה פוליטית-אידיאולוגית. כפועל יוצא, הם מעוניינים בפרסום ובהפצת תעמולה. חברה ישראלית עלולה להוות מטרה להאקטיביסטים אנטי-ישראליים.
- גורמים פנימיים- עובדי הארגון, לרבות עובדי קבלן ומיקור חוץ, שהינם בעל גישה למערכות ולמשרדים. בחלק מהמקרים, לעובדים אלה ידע רב על מערכות הארגון ובקרות האבטחה, ופעילותם נובעת מרצון לנקמה או רווח פיננסי שיושגו באמצעות פגיעה במוניטין הארגון או גניבת סודותיו. יצוין, כי בחלק מהמקרים, אירועי אבטחת מידע הנגרמים על ידי עובדים פנימיים מקורם בשל פעילות שגויה שלא בכוונת זדון.

מימד שני - מוטיבציה

כדי לאפיין את המוטיבציה המניעה את התוקף (שחקן) לבצע את פעילותו הזדונית, יש לבחון את הרשימה הבאה ולזהות מתוכה את סוגי המוטיבציה הרלוונטיים. לצורך שלמות התמונה האפשרית, נכללים ברשימה זו סוגי המוטיבציה הרלוונטיים למקורות איום אופייניים במגזר הקמעונאי לצד סוגים רלוונטיים פחות, המופיעים בטקסט אפור. יש לשלב את סוגי המוטיבציה הרלוונטיים בסעיף 2.1 לעיל.

- ריגול- המניע לפעילות תוקף מסוג זה הוא השגת גישה למידע בעל השלכות ברמת הבטחון הלאומי.

- צבאית- תקיפה מסוג זה מבוצעת לשם השגת יעדים בעלי אופי צבאי.
- מודיעין למבצע (מל"מ)- במקרה זה, מבקש התוקף להשיג מידע ונתונים שיסייעו לו לבצע פעילות מבצעית או תקיפת סייבר עתידית.
- פוליטית- תקיפה מסוג זה תתבצע נוכח מניע פוליטי של התוקף ו/או שולחיו, שמטרתו נעה מהכפשת יריב פוליטי ספציפי, דרך רצון להשפיע על דעת הקהל ועד ניסיונות להטיית בחירות.

- רווח פיננסי- במרבית הארגונים, החל מחברות עסקיות מובהקות דרך עמותות ועד משרדים ממשלתיים, קיים מידע אשר מכירתו על ידי התוקף לגורם שלישי יכולה להניב לו רווח כספי. יתרה מכן, לעתים, רווח זה יכול להגיע על ידי מניעת גישה למידע מהארגון (דוגמת תרחיש של תוקף המצפין את הקבצים ודורש כופר לשם פתיחתם) או שימוש של התוקף עצמו במידע למטרותיו (דוגמת תרחיש של יריב עסקי החושף הצעה למכרז של חברה מתחרה לשם גיבוש הצעה זולה יותר ובעקבות כך זוכה במכרז).
- השבתה/ הפרעה/ חבלה- תוקף המונע על ידי גורמים אלו יבקש לפגוע בתקינות פעילות מערכות המידע לשם עצם גרימת נזק או סחיטה. היעד של תקיפה שבבסיסה מוטיבציה זו יכולה להיות מערכת ספציפית, או, לחלופין, המערכת הראשונה אליה יצליח התוקף לחדור.
- יתרון תחרותי- תקיפה מסוג זה תבוצע, ברוב המקרים, על ידי יריב עסקי או מי שנשכר על ידו. יעדיה של תקיפה זו יכולים להיות מגוונים, בהתאם לטיבו של היתרון המבוקש, ויכולים לכלול גניבת מידע רגיש והשבתת מערכות.
- נקמה / מרמור- תקיפה המונעת מנסיבות אלה מבוצעת לעתים על ידי גורם פנימי לארגון, שמבקש להרע לארגון מסיבותיו, דוגמת- פיטורין, אי קבלת קידום בתפקיד וכו'. במקרים אחרים, התוקף הינו לקוח או מי שרואה את עצמו כנפגע מהתנהלות הארגון ו/או אנשיו.
- אנרכיה / כאוס- תקיפה מסוג זה נועדה לייצר שיבוש בפעילות מערכות החברה, וכפועל יוצא, בפעילותה. על פי רוב, היעד של תקיפה זו הוא נזק מקסימלי באשר הוא.
- טקטיקה / אסטרטגיה- מניע זה פירושו כי התקיפה מבוצעת לצורך השגת יעד ספציפי ממוקד וקצר טווח, או, לחלופין, כחלק מקמפיין מורכב ורחב בעל מטרות ארוכות טווח.
- חברתית / מוראלית- תוקף מסוג זה מעוניין ליצור נזקים מסוגים למערכות המידע לארגון הנתפס כעוין את ערכיו האישיים ו/או ערכי קבוצה אידיאולוגית אליה הוא משתייך.
- פרסום הצהרה- תוקף בעל מוטיבציה זו יבקש לנצל את מערכות הארגון במטרה להעביר את מסריו, לרבות בהיבט הפוליטי, הכלכלי וכו'.

מימד שלישי - מטרות

כדי לאפיין את סוגי המטרות בחברה בהן יבקש התוקף (שחקן) לפגוע במסגרת תקיפתו, יש לבחון את הרשימה הבאה ולזהות מתוכה את הרלוונטיות. לצורך שלמות התמונה האפשרית, נכללים ברשימה זו סוגי מטרות הרלוונטיות לתקיפות סייבר במגזר הקמעונאי, לצד סוגים רלוונטיים פחות, המופיעים בטקסט אפור. יש לשלב את סוגי התקיפות הרלוונטיות בסעיף 1.5 לעיל.

- חשיפה / הדלפת מידע רגיש- קרי, השגת גישה למידע ושימוש בו לצרכיו ו/או פרסומו בפומבי.
- שיבוש / פגיעה במידע- במקרה זה, ישאף התוקף לפגוע בנתונים עצמם, באופן שיוביל לשיבוש פעילות מערכת המידע והתהליכים בהם היא תומכת.
- פגיעה בזמינות מידע- היעדר זמינות חלקית או מלאה למידע פירושה חוסר פעילות מערכות ותהליכים, דבר שמוביל בעקבותיו נזקים מסוגים שונים, לרבות נזק כלכלי, תפעולי, פגיעה במוניטין ועוד.
- מניעה / הרס שירותים ותשתיות- מטרה מסוג זה פירושה תוקף המבקש לייצור נזק משמעותי ואף בלתי הפיך לחברה, ולעתים, לגורמים הקשורים לה.
- פגיעה בתדמית ומוניטין- פירושה של מטרה זו הוא יצירת נזקים מסוגים שונים, החל מחשיפה מידע ועד להשבתת מערכות, אשר יקבלו פומבי.

מימד רביעי - השפעה

כדי לאפיין את סוגי ההשפעות האפשריות של תקיפת סייבר על החברה, יש לבחון את הרשימה הבאה ולזהות מתוכה את הרלוונטיות. לצורך שלמות התמונה האפשרית, נכללים ברשימה זו סוגי השפעות הרלוונטיות לתקיפות סייבר במגזר הקמעונאי, לצד סוגים רלוונטיים פחות, המופיעים בטקסט אפור. יש לשלב את סוגי התקיפות הרלוונטיות בסעיף 1.5 לעיל.

ויודגש, לכל תקיפת סייבר עלולות להיות השלכות מסוגים שונים, אשר את חלקן קשה לחזות מראש. למשל, נזק כלכלי שנגרם כתוצאה מאי זמינות מערכת שהותקפה עלול להוביל לפגיעה במוניטין ואף לסנקציות ותביעות במידה וזמינות תהליך זה מחויבת על פי הרגולציה. נוכח זאת, יש לשקול את מגוון ההשלכות האפשריות של תקיפת סייבר, בהתאם למקורות האיום, המניעים האפשריים שלהם ומטרותיהם:

- פגיעה בחיי אדם / בטיחות- מדובר בנזק החמור ביותר שעלול להתרחש כתוצאה מתקיפת סייבר. במקרים אלה, ההשלכה הישירה או העקיפה מהפגיעה במערכת הינה פגיעה ואף סיכון לחיי אדם. למשל: נוזקת כופר שמצפינה קבצים בבית חולים.

- אובדן הכנסה / נזק כלכלי- במקרים אלה, התקיפה גורמת לאובדן הכנסה ישיר ו/או נזק כלכלי עקיף. למשל, בחברה למכירת מזון, אי זמינות אתר הקניות במשך שבוע תוביל לכך שכ-1,000 לקוחות לא ירכשו את מוצרי החברה (אובדן הכנסה) דבר שיגרום לכך שהחברה תצטרך להשמיד מלאי של מוצר מזון שלא נמכרו (נזק כלכלי).
- גניבת קניין רוחני- נזק מסוג זה נובע מגניבת מידע ייחודי ברמה עסקית ו/או תפעולית. כפועל יוצא, עלולה החברה להיות חשופה לנזקים כלכליים נרחבים ולפגיעה במוניטין. לדוגמה: גניבת מפרט הייצור של מוצר שתאפשר את הפקתו על ידי גורם מתחרה.
- פגיעה במוניטין- ברוב המקרים, פגיעה במוניטין הינה תוצאה של כל תקיפת סייבר, ככל שזו מתפרסמת. יודגש כי תוקף המעוניין בנזק זה ידאג לפרסום מעלליו במידה והארגון הנתקף לא יעשה זאת.
- הרס תשתית- על פי רוב, נזק מסוג זה הינו תוצר של תקיפות סייבר מתקדמות. נזק זה יכול להיגרם הן באופן ישיר, על ידי תקיפה של תשתית המחשוב עצמה, או, באופן עקיף, על ידי שיבוש פעילות מערכות המידע עצמן, אשר יוביל להרס תשתית המחשוב. לדוגמה, הרס מנגנון האחסון בשרת כתוצאה מכתיבה במהירות גבוהה של נתונים במקרה של תקיפת נתוני השרת, או, כתוצאה מהצפת מערכת המידע המבוססת על השרת בהיקף חריג של נתונים.
- הפללה / תביעה- ככל אשר הארגון הנתקף כפוף לרגולציה מחייבת, הוא עלול למצוא את עצמו חשוף להליכים משפטיים מסוגים שונים. בהקשר זה, יש לקחת בחשבון גם תביעה ייצוגית מצד לקוחות או כל גורם אחר אשר עלול לראות את עצמו נפגע כתוצאה מתקיפת סייבר שפגעה באותו ארגון.
- סנקציות והגבלות- השלכה מסוג זה הינו המשך של האמור לעיל, ומתרחשת כאשר הגוף הרגולטורי בוחר להפעיל את סמכות האכיפה שלו, דוגמת: המדינה, רשות ממשלתית וכו'.
- אובדן אמון ציבור / משקיעים- נזק מסוג זה הינו פועל יוצא של תקיפת סייבר מהותית, אשר הסבה נזק מהותי לארגון ו/או הציגה פער מהותי ביכולת ההתמודדות שלו למולה.
- פגיעה ברציפות תפקודית- במקרים אלה, מבקש התוקף למנוע מהארגון יכולת להתאושש מהתקיפה, וזאת על ידי פגיעה בתשתית ההתאוששות מאסון, למשל: מערכת הגיבוי.
- איכות הסביבה- בדומה לפגיעה בחיי אדם, מדובר בנזק חמור ביותר, שעלול להיגרם הן לסביבה עצמה ו/או לחיי אדם. למשל, שיבוש מערכת SCADA שמנהלת טיפול בשפכים עלולה לייצר מפגעים תברואתיים מסוגים שונים.
- תודעתית- בדומה למוניטין, פגיעה תודעתית נועדה לייצר השפעה ציבורית תקשורתית נרחבת ועמוקה.

נספח ד'- רשימת מסמכים אשר נסקרו במסגרת הסקר

יש לציין בטבלה להלן את המסמכים בהם נעשה שימוש במסגרת הסקר. מסמכים אלו עשויים להיות סיכומי דיון הנהלה, תוכניות עבודה, מסמכי מדיניות ונהלים וכו':

מס"ד	שם המסמך	סימוכין	תאריך פרסום
1.	נוהל ניהול משתמשים	נה-50	9.5.2018
2.	סיכום ישיבת דירקטוריון אפריל 2018	2018/115	22.4.2018
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

נספח ה' - מיפוי נכסי מידע ומאגרי מידע נכסי מידע שזוהו

ⓘ להלן רשימת מערכות מידע אופייניות בחברות במגזר הקמעונאי. יש לעדכן את הרשימה בהתאם לרשימת נכסי מידע הקיימים בחברה בפועל, לרבות נכסים שאינם כלולים בתיחום הסקר. גיבוש רשימה זה יתבצע על בסיס תיעוד קיים בחברה ו/או במסגרת פגישות המתקיימות במסגרת הסקר.

להלן רשימת מערכות המידע בחברה. המערכות המופיעות בסעיפים 10-14 לא נכללו במסגרת תיחום הסקר הנוכחי וראוי לבחון את סקירתן בעתיד.

מס"ד	סוג המערכת	שם המערכת	תצורת פריסה	ייעוד המערכת	רגישות המידע[1]
1.	עמדות מכירה (PoS)	•	מקומית	ניהול מכירת מוצרי החברה באתרים פיזיים (חנויות, ירידים וכו').	**רגיש- צנעת הפרט** מידע לקוחות: נתוני טרנזקציות, המכילים בין היתר נתוני כרטיסי אשראי, נתונים אישיים של לקוחות החברים במועדון לקוחות וכו'.
2.	אתר קניות מכירתי	• כתובת אתר האינטרנט	ענן	אפליקציה לרכישה מקוונת של מוצרי החברה.	**רגיש- צנעת הפרט** מידע לקוחות: נתוני טרנזקציות, המכילים בין היתר נתוני כרטיסי אשראי, נתונים אישיים של לקוחות החברים במועדון לקוחות וכו'.

[1] רגישות המידע:
א. רגיש-צנעת הפרט: מידע שהינו מידע רגיש לפי חוק הגנת הפרטיות.
ב. רגיש-עסקי: מידע שאינו חוסה תחת חוק הגנת הפרטיות, אך דליפתו תפגע כספית בחברה.
ג. פנימי: מידע שעוסק בתהליכי תפעול וארגון פנימיים של החברה שאינם נחלת הכלל.
ד. בלתי מסווג: מידע הנעדר כל רגישות שהיא.

מס"ד	סוג המערכת	שם המערכת	תצורת פריסה	ייעוד המערכת	רגישות המידע[1]
.3	מסופונים	•	משולבת	פלטפורמה ניידת המשמשת לצורך ניהול מכירות, מלאי ושרשרת האספקה.	**רגיש עסקי** מחירונים: המכילים, על פי רוב, את מחיר הבסיס של המוצר, כמו גם מבצעים עתיים, הנחות ייעודיות וכו'.
.4	מערכת ניהול מחסן ממוחשב (WMS)	•	מקומית	ניהול אחסנת וניפוק מלאי הסחורה של החברה, לרבות: קטלוג, מיקום פריטים וכו'.	**פנימי** תפעול: קטלוג הפריטים, אופן אחסון הסחורה, ניפוקה וכו' בהתאם לתנועות מלאי נכנס ויוצא.
.5	מערכת ניהול כספים	•	מקומית	ניהול התקציב, התזרים והתמחיר של החברה.	**רגיש עסקי** נתונים כספיים: נתונים חשבונאיים ופיננסים פנימיים המעידים על ביצועי החברה, דוגמת דוחות שנתיים, דוח נכסים וכו'.
.6	מערכת ניהול מלאי	•	מקומית	ניהול קבלה, אחסון וניפוק של מוצרים וסחורות.	**פנימי** נתוני מלאי: נתונים בדבר רמות מלאי הסחורה של החברה, דוגמת מלאי מוצרים גמורים, מלאי מוצרי גלם, מלאי מת ועוד.
.7	מערכת ניהול רכש	•	מקומית	ניהול תהליכי הרכש השונים המבוצעים בחברה למול ספקים.	**רגיש עסקי** נתוני רכש: חוזים והתקשרויות, לרבות עלות חומרי גלם, עלות מוצרים מוגמרים ועוד.
.8	BI/DW	•	מקומית	שמירה של נתונים עסקיים ועיבודם לשם הפקת תובנות.	**רגיש עסקי** מידע עסקי ותפעולי מסוגים שונים: נתונים גולמיים של מכירות, תמחיר, מלאי מת וכו', אשר עיבודם מאפשר זיהוי פערים עסקיים ושיפור תהליכים.

מס"ד	סוג המערכת	שם המערכת	תצורת פריסה	ייעוד המערכת	רגישות המידע[1]
.9	מערכת CRM- מועדון לקוחות	•	ענן	תמיכה בשירות לקוחות ובהבנת צרכיהם.	רגיש עסקי מגמות וניתוחים של לקוחות החברה: נתונים שונים אודות היקף מכירות, החזרות, שירות לקוי בסניפים וכו' המהווים רכיב מרכזי בשיפור המכירות, שמירה על מוניטין החברה ועוד.
	מערכות **שלא** נכללו בתיחום הסקר הנוכחי				
.10	דוא"ל	•	ענן	שליחה וקבלה של הודעות וקבצים ממוחשבים.	**רגיש- עסקי** מידע עסקי ותפעולי מסוגים שונים: מערכת הדואר האלקטרוני הינה פלטפורמה קריטית לפעילות הארגון, ומכילה מידע רב, ברמות רגישות שונות- מבלמ"ס ועד מידע רגיש לסוגיו.
.11	אפליקציות מובייל	•	ענן	הנגשת מוצרים ושירותים ללקוחות.	**רגיש- צנעת הפרט** מידע לקוחות: נתוני טרנזקציות, המכילים בין היתר נתוני כרטיסי אשראי, נתונים אישיים של חברי מועדון הלקוחות וכו'.
.12	שרת קבצים	•	מקומית	אחסון קבצים מסוגים שונים הנדרשים לחברה.	**רגיש- עסקי** • מידע הנהלה: סיכומי דיוני הנהלה ודירקטוריון, אסטרטגיה עסקית, מיזוגים ורכישות (M&A) וכו'. • פיתוח עסקי: פעילות המבוצעת הן במישור השיווקי, דוגמת זיהוי שווקים חדשים למוצרי החברה, והן במישור הייצורי-טכנולוגי, למשל, פיתוח מוצר חדש, שיפור תהליכי ייצור קיימים ועוד.

מס"ד	סוג המערכת	שם המערכת	תצורת פריסה	ייעוד המערכת	רגישות המידע[1]
					• תפעול שוטף של החברה, לרבות קווי אספקה, שמות העובדים, מיקום אתרי החברה וכו'.
13.	מערכת ניהול משאבי אנוש	•	מקומית	ניהול תהליכי משאבי האנוש, לרבות: גיוס, הדרכה, הערכה וכו'.	**רגיש- צנעת הפרט** מידע עובדים: נתונים שונים הקשורים לעובדים לאורך מחזור העסקתם, דוגמת- תוצאות מבחני מיון מועמדים, חוזי העסקה, חוות דעת תקופתיות וכו'.
14.	שכר	•	מקומית	ניהול שכר והטבות לעובדי החברה.	**רגיש- צנעת הפרט** מידע פיננסי אישי: נתונים שונים הקשורים לתגמול כלל עובדי החברה, מהעובד הזוטר ועד להנהלה הבכירה והדירקטוריון.

נספח ו'- סיכוני סייבר אופייניים לבחינה בסקר בהיקף בסיסי

להלן סיכונים אופייניים ליעדי ההגנה האופייניים במגזר הקמעונאי. מומלץ להיעזר ברשימה זו בעת ביצוע סקר סיכונים בסיסי.

מס"ד	יעדי הגנה אופייניים	תיאור הסיכון
.1	עמדות מכירה (PoS)	דלף כרטיסי אשראי של לקוחות מעמדות מכירה (PoS).
.2		גישה בלתי מורשית לעמדות מכירה כתוצאה ממערכות הפעלה בעלות חולשות אבטחה ידועות.
.3		היעדר יכולת לשייך פעילות למשתמש ייחודי עקב שימוש בחשבון משתמש גנרי.
.4		אי זמינות עמדות המכירה כתוצאה ממתקפת מניעת שירות.
.5	מערכת ניהול מלאי	גישה לא מבוקרת של ספקים חיצוניים למערכת המלאי.
.6		רשת אלחוטית (Wi-Fi) לא מאובטחת בעלת קישור ישיר לרשת הפנימית של החברה (LAN).
.7	אתר אינטרנט	דלף נתוני לקוחות מאתר המכירות המקוון.
.8		אי זמינות אתר האינטרנט עקב תקיפת מניעת שירות.
.9	מועדון לקוחות - מערכת CRMC	שיבושים בפעילות אתר האינטרנט עקב תקיפת מניעת שירות או השחתתו (Defacement).
.10		דלף פרטי חברי מועדון הלקוחות.

נספח ז'- סיכוני סייבר אופייניים לבחינה בסקר בהיקף מתקדם

להלן סיכוני סייבר אופייניים לתהליכים עסקיים ומערכות מידע, חלקם מאפיינים את המגזר הקמעונאי וחלקם רלוונטיים לכלל סוגי החברות. מומלץ להיעזר ברשימה זו בעת ביצוע סקר סיכונים מתקדם.

מס"ד	סיכון אב	סיכון
.1	גישה בלתי מורשית למערכות החברה	הקצאה עודפת של הרשאות גישה למשתמשים.
.2		אי ביצוע תהליכי תיקוף משתמשים והרשאות על בסיס עתי.
.3		מדיניות סיסמאות בלתי מוקשחת.
.4		פער באבטחת גישת ספקים מרחוק לרשת החברה.
.5		רשת אלחוטית (Wi-Fi) לא מאובטחת בעלת קישור לרשת הפנימית (LAN) של החברה.
.6		שימוש בחשבונות משתמש גנריים.
.7	דלף מידע עסקי	דלף נתוני לקוחות מאתר המכירות המקוון.
.8		דלף פרטי חברי מועדון הלקוחות.
.9		דלף תכניות עסקיות של החברה.
.10		חשיפת נתוני התמחיר של החברה לגורם חיצוני.
.11	מענה לקוי לאירוע סייבר	היעדר כלי שו"ב לזיהוי אירועי סייבר.
.12		היעדר תהליך מענה לאירוע אבטחת מידע.
.13		היעדר עדכון מצד ספקי צד ג' של החברה בהתרחש אירוע סייבר במערכותיהם.
.14	פגיעה במכירות/ תפעול	אי זמינות אתר האינטרנט עקב תקיפת מניעת שירות.
.15		אי זמינות עמדות המכירה כתוצאה ממתקפת מניעת שירות.
.16		אי זמינות מידע ושרתים כתוצאה מתקיפה המנצלת חולשות ידועות ו/או לא ידועות (Zero Day).
.17		הצפנת מערכות החברה כתוצאה מחדירת נוזקת כופר.
.18		השבתת אתר המכירות המקוון.
.19		מחיקה ו/או שינוי בלתי מורשה של נתוני טרנזקציות עסקיות.
.20		שיבוש נתוני מערכת ניהול מלאי.
.21	פערים בממשל אבטחת מידע	היעדר מדיניות ונהלי אבטחת מידע.
.22		היעדר מיפוי ובעלות על נכסי מידע.
.23		היעדר תוכנית המשכיות עסקית.
.24		מודעות לא מספקת של עובדים בהיבטי אבטחת מידע.
.25	תפקוד לקוי של תשתיות ומערכות מידע	אובדן מידע לצמיתות כתוצאה מתהליכי גיבוי לא אפקטיביים.
.26		הקצאה נרחבת של הרשאות Local Admin בעמדות קצה.
.27		פערים בנראות ושליטה על רשת התפעול (OT).
.28		פערי אבטחה אצל ספק צד ג' שנותן שירות לחברה ינוצלו לשם חדירה לרשת החברה ופגיעה במערכותיה.

מס"ד	סיכון אב	סיכון
.29		שיבושים בפעילות מערכות המידע בשל כשל בתשתיות תומכות ובקרות סביבתיות (חשמל, קירור, כיבוי אש).

נספח ח'- הערכת עוצמה, סבירות וחישוב רמת סיכון

קביעת סבירות

בעת הערכת הסבירות להתחרשות הסיכון יש להתחשב בפרמטרים שונים דוגמת: היקף המשתמשים בעלי גישה למערכת, האם המערכת נגישה מהאינטרנט וכו'. להלן קריטריונים שונים שיכולים לסייע בתהליך, התואמים את תוה"ג:

סבירות / שאלה	1 (נמוכה)	2 (בינונית)	3 (גבוהה)	4 (גבוהה מאוד)
1. כמה משתמשים קיימים במערכת?	10-1	50-11	500-51	יותר מ-500
2. מי הם משתמשי המערכת?	עובדים פנימיים בלבד	ספקים חיצוניים קבועים	ספקים חיצוניים מזדמנים	הציבור הרחב
3. כמה ממשקים קיימים למערכת	ללא ממשקים	5-1	10-6	יותר מ-10
4. מהו אופי ממשקי המערכת?	ללא ממשקים	ממשקים פנים-ארגוניים	ממשקים חיצוניים מול ספקים	ממשקים לציבור הרחב
5. מהו סוג המידע הקיים במערכת?	ללא רגישות עסקית	מידע פנימי של החברה	מידע רפואי או מידע של לקוחות	מידע עסקי רגיש
6. האם קיימת גישה מרחוק למערכות?	לא	באמצעות FA2	באמצעות ערוץ מוצפן	תוכנת השתלטות מסחרית
7. מהי רמת מידור ההרשאות במערכת?	מידור מלא (הרשאות לפי קבוצות/תפקידים)	מידור פרטני (הרשאות פרטניות לעובד)	מידור בסיסי (מנהל ומשתמש)	ללא מידור (הרשאות זהות לכולם)
8. מהי רמת העדכניות של המערכת?	גרסה עדכנית ביותר	עד 3 גרסאות אחורה	מעל 3 גרסאות אחורה	גרסאות שאינן נתמכות עוד על-ידי היצרן
9. מהי מדיניות העדכונים וטלאי האבטחה?	התקנת עדכונים מלאה לפחות אחת לרבעון	התקנת עדכוני אבטחה בלבד לפחות אחת לרבעון	עדכוני אבטחה קריטיים בלבד לפחות אחת לרבעון	ללא תהליך עדכונים מסודר
10. מהי רמת האבטחה הפיזית של המערכת?	נגישה לגורמים מורשים בלבד	נגישה לכלל עובדי הארגון	נגישה לקבלנים חיצוניים	נגישה לכלל המבקרים בארגון

קביעת עוצמה

הערכים המפורטים להלן תואמים לתוה"ג. יש לבחור את רמת העוצמה הגבוהה ביותר אשר עלולה להיגרם במידה והסיכון יתממש

עוצמה / קריטריון	**1 (נמוכה)**	**2 (בינונית)**	**3 (גבוהה)**	**4 (גבוהה מאוד)**
פגיעה בחיי אדם	בלתי ישים	קיימת סכנה ברורה לבריאות הציבור	קיימת סכנה ברורה לחיי אדם	קיימת סכנה ברורה ומיידית לחייהם של אנשים רבים
נזק ציות	קיימת חשיפה להליך מינהלי/אזרחי/פלילי העלולה להוביל לנזק לא מהותי	הנכס מוגדר כמאגר מידע שחלה עליו רמת האבטחה הבינונית על פי תקנות אבטחת המידע של הרשות להגנת הפרטיות	הנכס מוגדר כמאגר מידע שחלה עליו רמת האבטחה הגבוהה על פי תקנות אבטחת המידע של הרשות למשפט וטכנולוגיות מידע	קיימת חשיפה להליך מינהלי/פלילי/אזרחי שעלול להוביל להפסקת פעילות החברה
נזק כספי	נזק של עד 0.5% מהמחזור השנתי	נזק של בין 0.5% ל-1% מהמחזור השנתי	נזק של בין 1% ל-3% מהמחזור השנתי	נזק של מעל 3% מהמחזור השנתי
נזק למוניטין	חשיפה ללקוחות של מוצר ו/או שירות אחד	חשיפה ללקוחות של תחום פעילות	חשיפה בפני לקוחות של מספר תחומי פעילות ו/או חשיפה מצומצמת לקהל הרחב	חשיפה נרחבת ללקוחות החברה ולקהל הרחב

<u>**חישוב רמת הסיכון**</u>

יש להצליב את ערכי הסבירות ועוצמת הסיכון במטרה לחשב את רמת הסיכון. המטריצה ואופן החישוב להלן תואמים לתוה"ג

עוצמה/ הסתברות	**4 (גבוהה מאוד)**	**3 (גבוהה)**	**2 (בינונית)**	**1 (נמוכה)**
4 (גבוהה מאוד)	**גבוהה מאוד (16)**	**גבוהה (13)**	**בינונית (10)**	**נמוכה (7)**
3 (גבוהה)	**גבוהה מאוד (16)**	**גבוהה (12)**	**בינונית (9)**	**נמוכה (6)**
2 (בינונית)	**גבוהה (14)**	**בינונית (11)**	**בינונית (8)**	**נמוכה (5)**
1 (נמוכה)	**גבוהה (13)**	**בינונית (10)**	**נמוכה (7)**	**נמוכה (4)**

נספח ט'- מילון מונחים

להלן המונחים המרכזיים בהם נעשה שימוש בסקר זה:

- **איום סייבר (Cyber Threat)** - צירוף של כוונות ויכולות של תקיפה במרחב הסייבר, שטרם התממש.
- **אירוע סייבר (Cyber Incident)** - התרחשות אשר מעידה על נזק אפשרי לפעילותו התקינה של נכס סייבר, שיש יסוד להניח, כי היא נובעת מפעילות מכוונת במרחב הסייבר.
- **הגנת סייבר (של ארגון) (Cyber Defense)** - כל הפעולות שתכליתן להגן על נכסי הסייבר של הארגון מפני תקיפת סייבר.
- **ממונה הגנת סייבר (CISO - Chief Information Security Officer)** - בעל תפקיד המתכלל את מאמצי ההגנה על מערכות התקשוב הארגוניות בסייבר בארגון.
- **מרחב הסייבר הגלובאלי (Global Cyberspace)** - המצרף של כל נכסי הסייבר בעולם (ביבשה, בים, באוויר ובחלל).
- **מרחב הסייבר הישראלי (Israeli Cyber Space)** - מכלול נכסי הסייבר במרחב הסייבר העולמי, שלמדינת ישראל יש זיקה כלשהי אליהם.
- **נכס סייבר (Cyber Asset)** - מערכת תקשוב.
- **סבירות (Likelihood)** - ההסתברות שאירוע (תרחיש) יתממש בפועל.
- **סיכון (Risk)** - התרחשות עתידית לא ודאית עם השפעה שלילית.
- **סיכון שורשי (Inherent Risk)** - רמת הסיכון או החשיפה המובנית בתהליך/בפעילות, וזאת ללא נקיטה בפעולות תגובה מצד הארגון.
- **השפעה (Impact)** -הנזק העלול להיגרם במקרה של התממשות הסיכון.

*** סוף מסמך ***