סייבר ישראל
מערך הסייבר הלאומי

הגנת סייבר שרשרת אספקה

צד לקוח

סייבר ישראל
מערך הסייבר הלאומי

הגנת סייבר שרשרת האספקה
דגשים עבור צד לקוח
הרחבה מקצועית

מאי 2022
גרסה 1.2

תוכן עניינים

1. הקדמה

שרשרת אספקה, מאפשרת לארגון להתמקד בפעילות הליבה, ולהוציא לצד ג' את הפעילויות (מוצרים ושירותים), בהם אין לו יתרון תחרותי.

הוצאת פעילות זו, כוללת בין היתר רכש של תכנות ייעודיות, קבלת שירותי ייעוץ ושירותי תמיכה, רכש של פתרונות אחסון ועוד.

- מספר העסקים הכולל במגזר העסקי בישראל עומד על 542 אלף עסקים; 99.5% מהם, עסקים קטנים ובינוניים עד גודל של 100 שכירים לעסק.
- עסקים אלו אחראים על יותר ממחצית מהתוצר הלאומי.

לצד היתרונות הברורים, הגלומים בגישה זו, מצויים לא מעט סיכוני סייבר אשר על הארגון להביא בחשבון. מאחר ולארגון גדול, דוגמת בית חולים, עירייה, בנק, חברת ביטוח יש מאות ואלפי ספקים - הדבר מייצר מספר אתגרים. מסמך זה, מציג מתודה לאומית לניהול סיכוני סייבר שמקורם בשרשרת האספקה. ככלל, ניתן לחלק את סיכוני הסייבר של ארגון לסיכונים שמנצלים פגיעויות ופערי אבטחה בנכסי הארגון, ולסיכונים אשר נגרמים כתוצאה מפגיעה בצדדים שלישיים של הארגון (שרשרת אספקה ומיקור חוץ).

עבור הסיכונים התלויים בפעילויות ההגנה הישירות של הארגון, כתב מערך הסייבר מתודה לאומית בשם תורת ההגנה בסייבר לארגון (תוה"ג ארגוני). מסמך זה **משלים** את המתודה הלאומית באמצעות הצגת הצעדים המומלצים לטובת מזעור הסיכונים, אשר לרוב נשענים על פעילויות הגנה של צדדים שלישיים.

2. קהל יעד

מסמך זה מהווה כלי עזר בידי ממונה הגנת מידע וסייבר (CISO) ו/או מנהל אבטחת מידע או בידי גורם חליפי האחראי על הנושא בארגון. המסמך מהווה כלי עזר מסדיר ומכווין במסגרת בניית תכנית ניהול סיכוני הסייבר בשרשרת האספקה.

3. מטרת המסמך

להציג מתודה סדורה, לניהול יעיל ולצמצום של איומי סייבר שכיחים אשר מקורם בשרשרת האספקה.

4. הנחות יסוד

4.1. בחלק מהמקרים ניהול סיכוני הסייבר בשרשרת האספקה מתנהל מחוץ לכותלי הארגון, ולפיכך יכולת האכיפה והבקרה של הארגון תהיה פחותה יותר.

4.2. רמת הגנת המידע של חלק מהספקים אינה מספקת, וההתקשרות עם ספק זה הינה הכרחית/לא ניתנת לשינוי מסיבות שונות. דבר זה, עלול לעלות את רמת הסיכון לאיומי סייבר של הארגון מצד אותו ספק ולהצריך שימוש בבקרות מפצות ייעודיות מול הספק.

4.3. ישנם מקרים הארגון יידרש להתייחס למצבים יחודיים במסגרת תהליך ניהול הסיכון. לדוגמה:

4.3.1.1. ספקים אשר לא יוכלו לעמוד בדרישות ההגנה המצופות מהם, אך מסיבות מסוימות הארגון מעוניין להתקשר עימהם. לדוגמה, בשל התחייבות חוזית קיימת, ידע ומומחיות ספציפית שלו או מסיבות נוספות. במקרים אלו, נדרש לבצע תהליך של ניהול הסיכון מול הספק הספציפי, ולהחליט על אופן מזעור הסיכון. לדוגמה, באמצעות יישום בקרות מפצות, פיתוח תהליך עבודה שונה מול הספק ועוד.

4.3.1.2. קיימים ספקים אשר אין ביכולת הלקוח הממוצע להשפיע על רמת ההגנה שלהם. לעיתים הדבר נובע מיחסי "הכוחות" שבין הספק ללקוח, לעיתים מקור הבעיה בספק שאיננו ממוקם בישראל ואין לנו יכולת לבצע לו ביקורות ולדרוש ממנו עמידה בדרישות פרטניות וכו' במקרים אלו, ניתן לנסות לייצר לחץ על הספק באפיקים אחרים, כגון באמצעות הפניה לרגולציה/התאגדות של מספר לקוחות מול אותו הספק. כמו"כ, ניתן לעיתים (בהיעדר יכולת אפקטיבית לוודא את רמת ההגנה של הספק), להסתמך על הסמכה בינלאומית קיימת (כגון SOC2) ולדרוש בחוזה ההתקשרות את היכולת לבצע ביקורת/לקבל נתונים. לא פעם, ספקים אלו מאפשרים ללקוחותיהם לקבל גישה לתוצאות סקר סיכונים שהם ביצעו באמצעות גורם צד ג' בלתי תלוי. עיון בדו"חות סקר עשוי ללמד את הלקוח פרטים חשובים. בפרט חשוב לוודא במקרים אלו את התיחום (Scope) של המבדק, שכן לעיתים ניתנה הסמכה עבור שירות/מוצר מסוים ולא עבור כל פעילות הספק. בנוסף, **חשוב להבין את מטריצת חלוקת האחריות שבין הספק ללקוח בהיבטי ההגנה**. לדוגמה, העובדה שספק שירותי ענן בינלאומי עומד בדרישות תקן מקובל בתחום

(כגון CSA[1]), איננה מעידה בצורה אוטומטי על אופן חלוקת האחריות[2] לעניין ניהול עדכוני תוכנה, ניהול משתמשים, הקשחות, גיבויים, ניטור וכו'. מומלץ להגדיר במסגרת הסכם ההתקשרות עם הספק את הנושא.

4.3.1.3. שמירה על יתירות בין ספקים, כך שתקיפת סייבר כנגד ספק פלוני, לא תשפיע באופן מהותי על מדדי המשכיות עסקית של הארגון.

4.3.2. ספקים אשר פגיעה בהם תהווה נזק גבוה מאוד לליבת העשייה של הארגון. במקרים אלו, מומלץ לבצע, בנוסף על סקר הערכת רמת ההגנה של הארגון בהתאם למתודה זו, גם סקר הערכת סיכונים פרטני. סקר זה יביא בחשבון את סוג המידע, תהליכים עסקיים תלויים, מיפוי איומים, איום ייחוס וכו'.

4.4. במקרים אלו, מומלץ להביא את הנושא לדיון ואישור של הנהלת הארגון ולידיעת גורמי ניהול הסיכונים בארגון (כגון מנהל סיכונים תפעוליים, CRO אם ישנו וכו').

[1] https://cloudsecurityalliance.org/
[2] ראה לדוגמה https://www.cloudsecurityalliance.no/2019/02/mapping-of-on-premises-security-controls-vs-major-cloud-providers-version-3-2-feb-2019 /

5. מונחים והגדרות

5.1. ספק - גורם שאינו מתוך הארגון, אשר נותן לו את אחד מאלו או יותר בחצרות הארגון או חצרות הספק:

5.1.1. מתן שירות בתחומים שונים ומגוונים (כגון תמיכה מקצועית, סליקה, ייעוץ, ניהול תוכן, ניטור וכיו"ב)

5.1.2. מספק ציוד, אמצעים ומערכות, תומך ומאחזק אותם

5.1.3. מפתח עבור הארגון מערכות ייעודיות בהתאם לצרכיו

5.1.4. מפעיל כ"א או מספק שירותים אנושיים

5.2. **ספק מהותי\קריטי** - ספק שנקבע ע"י הארגון או הרגולטור הרלוונטי, שהוא חיוני להתנהלות העסקית התקינה, וקיימת בו תלות הדוקה להשגת ייעדי הארגון ועמידה במשימותיו. החלטה על הגדרת ספק כמהותי נתונה לשיקול דעתו של הארגון. חריג לכך, כאשר מגדיר רגולטור מראש עבור הגורמים במשק עליהם הוא אמון כי ספק מסוים, או ספק שעומד בקריטריונים מוגדרים - יהווה ספק מהותי בכל מקרה.

5.3. **סיכוני סייבר בשרשרת האספקה** - סיכונים לארגון או לקוח (הנהנה משירותי הספק), הנובעים מעצם העסקיים-טכנולוגיים הטכנולוגיים בינו לבין הספק, העלולים לפגום באפקטיביות הארגון, יעדיו, משימותיו או לפגוע ברציפותו התפקודית.

5.4. **התקשרות עם ספק:** תהליך עסקי - ארגוני, הקובע את מסגרת הפעילות, החובות והזכויות ההדדיים במסגרת חוזית בין הארגון/ לקוח לספק. בהיבטי אבטחת מידע וסייבר יש לסכם את התנאים הנדרשים לעמידה מטעם הספק במהלך תקופת ההתקשרות ואת אסטרטגייה סיום ההתקשרות.

5.4.1. **אסטרטגיית סיום התקשרות עם ספק (Exit Strategy Plan)** - נועדה לזיהוי של סיכוני הגנת מידע וסייבר פוטנציאליים ואבטחת המשכיות עסקית של שירותים עם מינימום פגיעה תפעולית בעסקי החברה השוטפים בעת סיום ההתקשרות של הארגון עם ספק. נושא זה לרוב איננו בתחום האחריות הישירה של גורמי הגנת מידע וסייבר בארגון, אך יש לוודא חוזית ונהלית את היכולת לממש אסטרטגיה זו במידה ויעלה צורך כזה מטעמי חשיפה לסיכוני סייבר אשר חורגים מתיאבון הסיכון של הארגון. מומלץ לוודא במסגרת הסכם ההתקשרות, כי קיימת הזכות של הלקוח לדרוש מהספק למחוק את המידע, להחזיר אמצעים וקניין ארגוני, לנתק קישורים

וכו' בסיום ההתקשרות, או בכל נקודת זמן שקודמת לה (לדוגמה במקרה של חשד לפריצה ו/או דלף מידע אצל הספק).

4.3 **"מערכת יוב"ל" (יעדים ובקרות לארגון)** -מערכת לניהול סיכוני הגנת מידע וסייבר. המערכת פותחה באמצעות המערך הלאומי להגנת הסייבר, לטובת הציבור. המערכת מורכבת ממספר מודולים, כגון מודול שרשרת אספקה, מודול התעדה, מודול תורת הגנה ועוד. מודול שרשרת אספקה במערכת, מסייע לאבחן את רמת הגנת המידע המיושמת על ידי הספק.

4.4 רמת הגנת המידע נקבעת על ידי מילוי שאלון סגור הכולל שאלות ממגוון תחומים באבטחת מידע. לאחר מילוי השאלון הספק יקבל ציון המשקף את רמת הגנת המידע של שירות/מוצר ספציפי. במקרים מסוימים, יידרש הספק לעבור בדיקת התעדה, באמצעות גורם בדיקה מורשה, אשר רק לאחריה יקבל אישור על רמת ההגנה בארגונו. המערכת מסייעת בין היתר בדברים הבאים:

- הנגשת שאלון רמת ההגנה לספקים במשק. השימוש באקסל בקרות מתודה עדכני הוא חובה. המילוי שלהן יכול להיות באמצעות מערכת GRC כזו או אחרת, וביניהן מערכת "יובל".
- מערכת ההתעדה שתועמד לרשות הציבור באתר מערך הסייבר הלאומי, מאפשרת את הנגשת רשימת הגורמים במשק אשר סיימו את תהליך ההסמכה בהתאם למתודה הלאומית בנושא (ספקים, ובודקים מאושרים). כל ארגון במשק יוכל לבצע חיפוש במערכת, ולקבל פילוח מתאים של חברות העומדות בסף הסיכון שקבע הארגון. על סמך מידע זה יוכל הארגון לבחור את הספק המתאים ולחתום עמו חוזה התקשרות להבטחת עמידת הספק ברמת הסיכון שנקבעה.
- פלטפורמה עבור הספק להפיק דו"חות להצהרה על רמת העמידה שלו בדרישות ההגנה של מתודה זו, לצד יכולת לנהל את הליקויים שעלו אצלו בתהליך (Remediation). בנוסף, הספק רשאי בכל זמן נתון לעדכן את פרטיו במערכת ובהתאם יופק למוצר/שירות ציון חדש.

המערכת זמינה למשק באתר מערך הסייבר ובאמצעות הקישור הבא:https://grc.cyber.gov.il

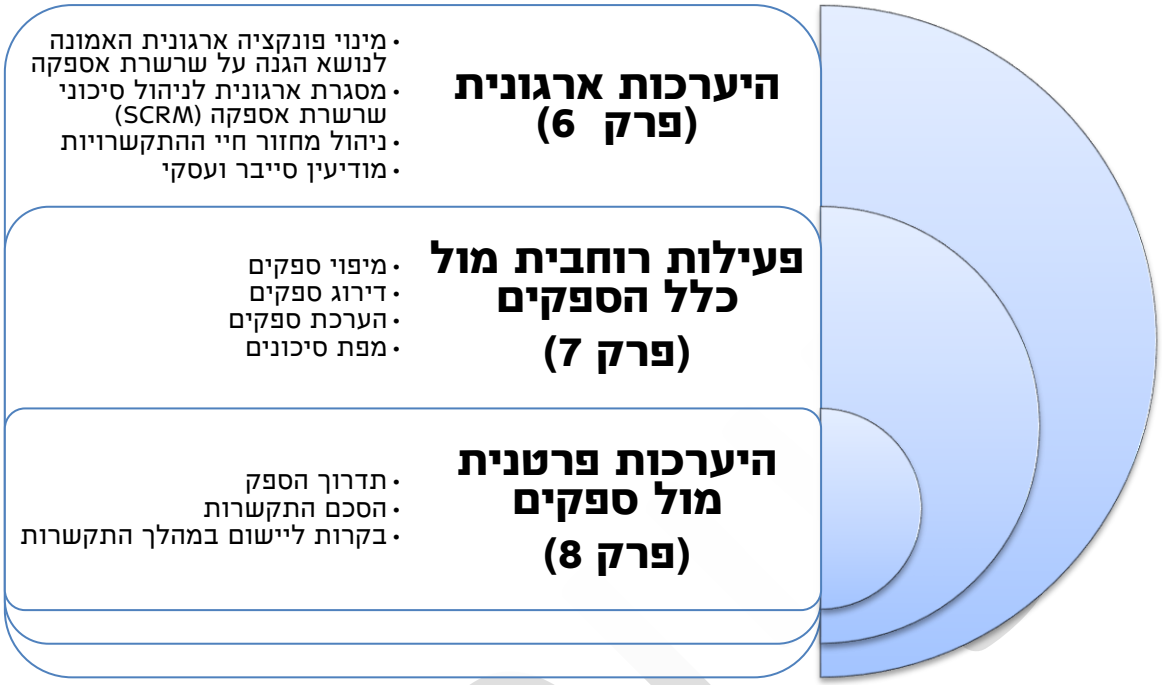
יצוין, כי אין חובה לעשות שימוש במערכת "יובל", וכי פלטפורמה זו לא באה להחליף את מערכות ניהול הסיכונים של לקוחות במשק (תוכנות VRM - Vendor Risk Management), והיא באה לתת מענה לספקים אשר נדרשים למלא שאלון שונה עבור עשרות ומאות לקוחות.
להבנת ההבדלים בין ייעוד המערכות, ראה נספח א'.

4.5 **בודקים מאושרים** – רשימה מנוהלת ע"י מערך הסייבר הלאומי המכילה את פרטי הקשר של בודקים שהוכשרו לבדיקת ספקים. הרשימה מצוייה באתר מס"ל בכתובת לינק

4.6 "**ספקים בטוחים**" - רשימה מנוהלת ע"י מערך הסייבר הלאומי, המכילה את רשימת הספקים, אשר ביצעו תהליך בדיקה מלא ע"י בודק מוסמך וקיבלו אקרדיטציה להיות עומדים בדרישות מתודת ההגנה לסיכוני הסייבר בשרשרת האספקה. התקשרות ארגון/ לקוח עם ספק בטוח יכולה לקצר באופן משמעותי את לוחות הזמנים לבדיקת הספק, ואף להוזיל עלויות עבור הארגון.

6. פעילות ההגנה בראי הארגון

ניתן לחלק את פעילויות ההגנה של ארגונים מפני סיכוני שרשרת האספקה כך:



תרשים 3: מיפוי פעילויות ההגנה של ארגונים מפני סיכוני שרשרת האספקה

יישום השלבים הנ"ל, מצריך משאבים וידע רב מהארגון. לטובת התמודדות עם אתגרי המשק בנושא, הוגדרו מספר כלים ומענים מטעם מערך הסייבר הלאומי בנושא. לקריאה אודות האתגרים והמענים אותם פיתח המערך ברמה הלאומית, ראה נספח ב'.

7. היערכות ארגונית

7.1. מינוי פונקציה ארגונית האמונה לנושא הגנה על שרשרת אספקה

7.1.1. על הנהלת הארגון למנות פונקציה ארגונית האמונה לנושא הגנה על שרשרת אספקה.

7.1.2. פונקציה זו צריכה להיות בעלת הבנה מקצועית מתאימה בתחום ניהול סיכונים, הגנת מידע וסייבר, מכרזים והתקשרויות.

7.1.3. ככלל, יש להעדיף כי פונקציה זו תהיה כפופה לממונה הגנת מידע וסייבר (CISO).

7.2. מדיניות הערכת סיכונים בשרשרת האספקה (SCRM - Supply Chain Risk Management)

7.2.1. יש לכתוב נוהל עבודה אשר יאושר על ידי ההנהלה ויתוקף לפחות אחת לשנה.

7.2.2. התייחסות לבקרות מפצות בהתקשרויות בהן לא ניתן להביא את הספק אל רמת ההגנה הנדרשת. בקרות אלו עשויות לכלול לדוגמה הקמת סביבת ספקים בתוך הארגון, אספקת מחשבים וציוד מוקשח לספקים, החלטה על ביצוע העבודה של הספק במקרים מסוימים אך ורק בתוך חצרות הארגון וכו'.

7.2.3. התייחסות לכלי ניהול הבקרה אחר התהליך. כלים אלו עשויים לסייע לארגון הן בשלב מיפוי והערכת הספקים והן בשלב המעקב אחר מימוש ההמלצות והמשימות הפתוחות מול הספקים השונים. כלים אלו, לרוב מוכרים במשק ככלי GRC (Governance, Risk Compliance) , או ככלי VRM (Vendor Risk Management). היתרון שבשימוש בכלים אלו, טמון ביכולת לקבל תמונה הוליסטית של מצב הספקים, לצד התראות, הצגת תמונת מצב השוואתית (בנצ'מרק) , אוטומציה של הפניה אליהם ושל הערכת רמת ההגנה של הספק ועוד.

7.2.4. מדיניות הארגון, תכלול בין היתר התייחסות להיבטים הבאים: מיפוי דרישות הגנת ומידע וסייבר שעל הארגון וספקיו לעמוד בהם, שיקולים במכרזים והתקשרויות לבחירה בספק שירותים או במוצר, שינויים בסוג ההתקשרות עם הספק ובמבנה הארגוני/טכנולוגי של הספק, היבטי ביקורת ובקרה, אופן הגישה מרחוק של ספקים, היבטי הוצאת מידע לספק או לספקי המשנה שלו (דוגמת ספק ענן ציבורי או מרכז נתונים שיתופי), טיפול באירוע הגנת מידע וסייבר אצל הספק, אופן סיום התקשרות עם ספק ולתדירות ואופן ביצוע הפניה אל הספקים השונים בהתאם לדרישות מתודה זו.

7.2.5. מדיניות תכלול התייחסות לתהליכים משיקים בארגון, דוגמת שילוב ממונה הביטחון (מנב"ט) במקרה של מכרזים והתקשרויות שאין לחשוף אותם לנחלת הכלל או במקרה שבו הספק ייחשף במסגרת פעילותו למידע מסווג.

7.2.6. מדיניות הארגון תגדיר על מי חלה האחריות להגנה על המידע שאצל הספק (לכל אורך נתיב המידע, כולל ספקים וצד ג' של ספקים).

7.2.7. אחריות הנהלה - הקצאת משאבים נדרשים לטובת ביצוע ביקורות לספקים מהותיים בהתאם להגדרתם על ידי הגורם העסקי בארגון ולפוטנציאל הנזק שלהם.

7.3. ניהול מחזור החיים של ההתקשרויות

7.3.1. לפני יציאה למכרז או התקשרות חדשה או חידוש התקשרות קיימת, יש ליידע את ממונה הגנת מידע וסייבר באופן אוטומטי.

7.3.2. במידת האפשר, מערכת ניהול הספקים תכלול אוטומציה של התהליך והוספת שדות עבור מאפיינים של הספק בהיבטי הגנת מידע וסייבר (דוגמת איש קשר, סיווג הספק, שירותים אותם הוא מספק וכו'). במידת הניתן, לא יתאפשר תהליך הקמת הספק במערכת, ללא אישור ממונה הגנת מידע וסייבר בארגון.

7.3.3. יש להגדיר את היבטי הגנת מידע וסייבר החוזיים מול הספק, כגון התחייבות לחתימה על הסכם סודיות, חתימה על הסכם ניגוד עניינים, דרישה לערבות בנקאית ושיפוי במקרה של אירוע הגנת מידע וסייבר, סמכות/רשות לבצע ביקורות סייבר בחצרות הספק, הזכות לאסוף מידע פורנזי (ראיות דיגיטליות) ממערכות הספק, החלת דרישות הגנת מידע וסייבר על ספקי המשנה, חובת הספק לידע את הארגון תקופה של X חודשים לפני ביצוע שינויים מהותיים דוגמת העברת מידע לחו"ל או לספק משנה, חובת הספק לעדכן מידית את הארגון במקרה של אירוע סייבר אשר עשוי להשפיע על הארגון ו/או לקוחותיו, חובת שקיפות מצד הספק ועוד. מומלץ לוודא כי בכל הסכם התקשרות ובכל מכרז של הארגון ישנו סעיף מובנה אשר מגדיר את דרישות הגנת מידע וסייבר בהתקשרות.

7.3.4. בעת בחינת התייחסות הספק לעמידתו בדרישות המתודה, יש לוודא כי **התיחום**, **תחומי ההתמחות**, **עדכניות המענה** ו**אופן ההוכחה** המוצהרים על ידו עונים לצורכי הארגון. כמו כן, יש לוודא כי קיימת הקבלה בין המוצהר על ידי הספק, למידע המפורסם במאגר המידע אודות ספקים הזמין באתר האינטרנט של מערך הסייבר הלאומי. במקרה שבו ישנו שוני בין הרישומים, יש לפנות לספק לשם קבלת הבהרות.

7.3.5. בעת חידוש התקשרות עם ספק קיים, יש לוודא כי חידוש החוזה מביא בחשבון את רמת ההגנה הנוכחית של הספק ואת אופן מימוש ההמלצות וסגירת הפערים שהוצפו על ידי הארגון אל מול הספק. חידוש חוזה, הינו חלון זמן, שמהווה

הזדמנות לשלב בחוזה היבטי הגנה נוספים, אשר נדרשים, אך לא נכללו בהסכם ההתקשרות הקודם.

7.3.6. **<u>סיום התקשרות עם ספק</u>**

7.3.6.1. יש לוודא כי הסדרים עם הספק שנקבעו במסגרת הסכם ההתקשרות, מתקיימים. בפרט חשוב לוודא עמידה בכל הקשור למחיקת נתונים של הארגון המאוחסנים בחצרי הספק בתום ההתקשרות בין הצדדים. בין היתר ניתן לבדוק את הדברים הבאים:

7.3.6.2. יש לוודא החזרת כלל הרשומות, המדיה, הציוד והרכיבים השייכים לארגון אשר נעשה בהם שימוש לצורך עבודת הספק. כל זאת, לרבות פריטים הנמצאים בקרב כלל עובדי הספק וספקי המשנה שלו.

7.3.6.3. בנוסף, הספק יחתום על הצהרה בה הוא מתחייב שלא נשארו ברשותו רכיבים כלשהם הנוגעים למערכת ו/או מידע אודות הארגון וכי הוא לא יעשה שום שימוש במידע על הארגון, אליו הוא נחשף במסגרת ההתקשרות.

7.3.6.4. יש לוודא השמדת מדיה מגנטית מכל ציוד אשר שימש את הספק במהלך ההתקשרות עם הארגון (כגון: במקרה שמדובר במחשבים של הספק ששימשו לעיבוד ו/אחסון של מידע של הארגון). כמו כן, נדרש לוודא מחיקת עותקים של קבצים ומידע של הלקוח ממערכות המידע ונכסי ה IT של הספקים לאחר סיום הצורך העסקי באחזקתו.

7.3.6.5. יש לוודא כי לספק לא נותרות הרשאות גישה, אמצעי הזדהות וגישה פיזית ו/או לוגית למידע של הארגון.

7.3.6.6. יש לוודא הנחיה לעניין המותר והאסור אודות פרסום פרטי הפרויקט/התקשרות לגורמי צד ג'.

מומלץ לשלב את היבטי הגנת הסייבר בהיבטי רכש מתחילת התהליך, ראה איור בנספח ג.

7.3.7. **<u>מודיעין סייבר ועסקי</u>**

7.3.7.1. על הארגון לשקול שימוש במודיעין סייבר ועסקי לשם בחינת מצב הספק בטרם התקשרות, ובמהלך ההתקשרות.

7.3.7.2. הממצאים עשויים לסייע לארגון להעריך האם רמת הגנת מידע וסייבר של הספק סבירה, ולפיכך ניתן להתקשר עמו או לחדש מולו הסכם התקשרות. כמו כן, הממצאים יכולים לסייע לארגון לאתר קיומו של אירוע סייבר בספק אשר עשוי להשפיע עליו או על לקוחותיו.

8.פעילות רוחבית עבור כלל הספקים

8.1. **<u>מיפוי ספקים</u>:**

8.1.1. יש לייצר רשימה של ספקי הארגון, כאשר ספקים אלו כוללים נותני שירות מסוגים שונים, כגון: פיתוח תוכנה, רכש חומרה ותקשורת, יישום והטמעה של מערכות בארגון, חברות ייעוץ וסקרי סיכונים, נותני שירות כגון רואה חשבון, עריכת דין, שרותי דפוס, עריכה, מיתוג, תמיכה טכנית, אינטגרציה וכו'.

8.1.2. את הרשימה יש לתקף מול גורמים עסקיים בארגון, אשר יש להם היכרות עם סוג הפעילות אל מול הספקים הנ"ל. מומלץ להיעזר באנשי הרכש בנושא וברשימה של אגף מערכות מידע (לטובת איתור תוכנות חיצוניות, ספקי שירותי IT, בעלי גישה מרחוק לארגון וכו').

8.1.3. יש לייצר תהליך ארגוני אשר מוודא כי גורמי הגנת מידע וסייבר בארגון יהיו מיודעים על הוספת ספק חדש לארגון/התקשרות חדשה/יציאה להתקשרות חדשה/מכרז חדש. לדוגמה, ניתן ליישם זאת הן כחלק מנוהל עבודה בארגון והן כחלק משילוב של מחלקת הגנת מידע וסייבר בתהליך הקמת ספק חדש במחלקת הכספים/במערכת המידע וכו'.

8.1.4. המיפוי יכלול התייחסות לסוג השירות אותו מספק הספק. מיפוי זה יתייחס לקטגוריות הבאות:

- <u>גישה מרחוק</u> – ספקים אשר נדרשים, כחלק מחוזה ההתקשרות מולם, לטובת אספקת המוצר/שירות להתחבר למשאבי הארגון. במקרים אלו, מצופה מהספק לעבוד בהתאם למדיניות האבטחה של הארגון[3] בנושא חיבוריות מרחוק. יחד עם זאת, לא פעם ישנם מצבים בהם הספק מגדיר את אופן ההתחברות שלו מרחוק אל לקוחותיו. במקרים אלו, נדרש לוודא כי אופן ההתחברות מתבצע בצורה בטוחה. בהרבה מקרים, ספקים אלו הינם אנשי מחשוב/IT/תקשורת/פיתוח וכו' אשר יש להם פוטנציאל נזק גדול לארגון. עבור שירותים אלו, ישנן בקרות/ דרישות הגנה ייעודיות בשאלון הספקים.
- <u>מרכז נתונים שיתופי (Colocation)</u> - מרכז נתונים המשכיר שטח רצפה לארגונים. ספקים אלו מאפשרים לארגון להעביר את חוות השרתים שלו או אתר הגיבוי (DR) לסביבה של ספק מתמחה.
- <u>פיתוח תוכנה</u>- ספקים אשר מפתחים תוכנה שמותקנת אצל הלקוח. ספקים אלו עשויים להוות פירצת אבטחה. רמת ההגנה של הלקוח, תלויה במידה רבה ברמת

[33] ראו תורת ההגנה בסייבר לארגון

https://www.gov.il/he/departments/general/cyber_security_methodology_2

ההגנה הקיימת בתהליכי הפיתוח וניהול מחזור החיים של הספק מפתח התוכנה. עבור שירותים אלו, ישנן בקרות/דרישות הגנה ייעודיות בשאלון הספקים.

- אחסון אתרים (Website Hosting) – ספקים אשר מפתחים ו/או מאחסנים אתרי אינטרנט עבור לקוחותיהם. ספקים אלו, עשויים לכלול אירוח של אתר אותו בנה הלקוח, כמו גם הנגשה ושימוש במערכות מסוג מחוללי אתרים (CMS). ספקים אלו מהווים לא פעם יעד לתקיפה, בשל כמות הלקוחות שלהם, משטח החשיפה הרחב והיכולת לייצר נזק לארגונים גדולים באמצעות פגיעה בספקי האירוח שלהם. עבור שירותים אלו, ישנן בקרות/דרישות ייעודיות אשר מספקות את המענה ההגנתי המצופה אל מול איומים כגון: מתקפת מניעת שירות, השחתה ודלף מידע.
- אבטחת OT – ספקים אשר מפתחים ו/או מספקים שירות ו/או מוצרים בעולם ה-OT. . ספקים אלו, עשויים לכלול יצרני בקרים, חברות אינטרציה, מומחי יישום.
- דרישות רוחביות -כל ספק נדרש לרמת הגנה בסיסית בנושאים השונים, כמעט ללא תלות בסוג השירות אותו הוא מספק. דרישות אלו, מייצגות את המינימום המצופה מכל ספק איתו הארגון מתקשר, בהתאם לרמת הסיכון שנגזרת מההתקשרות עימו (ספק מהותי/לא מהותי). ספקים בקטגוריה זו יכולים לכלול לדוגמה: חברת מיתוג, חברות סקרים, חברות ייעוץ בנושאים השונים (ייעוץ סייבר, ייעוץ תפעולי, ייעוץ אסטרטגי וכו') , עורכי דין, רואי חשבון, חברת שירותי תרגום, בית דפוס וגורמים נוספים אשר התקפת סייבר עליהם, תסכן את לקוחותיהם בחשיפת מידע ובסיכונים נוספים.

בסוף שלב זה, בידי הארגון תהיה טבלה עם מיפוי אשר כולל לפחות את ההיבטים הבאים:

מיפוי ספקים				
שם הספק	**סוג השירות/מוצר אותו הוא מספק**	**איש קשר מהצד העסקי בארגון אל מול הספק**	**פרטי התקשרות מול נציג הספק לשאלות בנושא סייבר**	**סוג השירות הניתן (שירות מבוסס מרכז נתונים שיתופי/פיתוח תוכנה/גישה מרחוק/דרישות רוחביות/ אחסון אתרים/אבטחת OT)**

טבלה 1: דוגמה לטבלת מיפוי ספקים

8.2. **דירוג ספקים:**

8.2.1. יש לדרג את הספקים לשלוש רמות סיכון.

8.2.2. דירוג הספקים יביא בחשבון את השלכות/פוטנציאל הנזק שעלול להיגרם לארגון, כתוצאה מאירוע סייבר אצל הספק. לטובת חישוב פוטנציאל הנזק, ניתן לעשות שימוש במספר קריטריונים, כגון אלו המוצגים בטבלה הבאה:

דירוג הספק	רמת הנזק הצפוי לארגון מהספק	האם מדובר "בספק מהותי" בהתאם להנחיית רגולטור	נזק כלכלי לארגון (כולל עלויות כתוצאה מאובדן הכנסה/מוניטין/רגולציה וכו')	פגיעה ברציפות עסקית	רגישות המידע הנגיש לספק	סבירות להתממשות אירוע כתוצאה מההתקשרות
C	נמוך	לא	עשרות אלפי שקלים	התאוששות מאירוע אצל הספק תיקח מספר שעות	מידע בעל רמת רגישות נמוכה	תלות נמוכה בסייבר. לדוגמה, ספק של ציוד משרדי, שירותי מומחה שאינם כוללים מידע של הלקוח, ללא הרשאות ונגישות למערכות הלקוח וכו'
B	בינוני	לא	מאות אלפי שקלים	התאוששות מאירוע אצל הספק תיקח מספר ימים	מידע בעל רגישות בינונית	תלות בינונית בסייבר בהתקשרות עם הספק
A	גבוה	כן	מעל מיליון ₪	התאוששות מאירוע אצל הספק תיקח מספר שבועות	מידע רגיש עסקית כגון פטנטים, סודות מסחריים וכו'	ספק בעל תלות גבוהה בסייבר. לדוגמה: ספק אשר מספק שירותי IT, בעל הרשאות גישה מרחוק, ספק תוכנה מהותית, מחזיק מידע רגיש בענן או במערכות שבחצרות הספק

טבלה 2: דוגמה לטבלת מיפוי ספקים הכוללת פרמטרים לחישוב פוטנציאל הנזק

יש לבצע התאמה של הערכים בהתאם לגודל הארגון, מאפייניו ודרישות החוק,הרגולציה, דרישות חוזיות וצרכים עסקיים. טבלה זו נועדה לתת המחשה לשיקולים וערכים מולם יכול ארגון לבנות את תכנית ההגנה שלו. תיקוף קריטריון פוטנציאל "נזק כלכלי לארגון" עשויה לעבור התאמות לדוגמה אל מול המחזור הכספי של הארגון ותיקוף קריטריון

"פגיעה ברציפות עסקית" עשוי לעבור התאמות אל מול תכנית המשכיות עסקית (בדגש על BIA, RPO, RTO ופרמטרים נוספים).

8.2.3. עבודה עם הטבלה הנ"ל, תסייע לסווג את הספקים על פי הקריטריונים השונים. הציון הסופי של ספק (מבין שלוש הרמות C/B/A) , ייגזר מפוטנציאל הנזק המירבי. כך לדוגמה, ספק אשר בקריטריון אחד נמצא ברמה A, וביתר הקריטריונים נמצא ברמה C, יסווג כספק ברמת פוטנציאל נזק A. חריג לכלל הינה קביעה של רגולטור כי מדובר ב"ספק מהותי", ולפיכך חלה חובה על הארגון להגדיר אותו כספק ברמת פוטנציאל נזק A.

8.2.4. לאחר דירוג פוטנציאל הנזק המירבי, יש לשקלל את מידת הסבירות להתממשות אירוע סייבר כתוצאה מההתקשרות עם הספק. סבירות זו עשויה להיגזר מתוך:

8.2.4.1. **מאפייני הספק**, כגון רמת ההגנה שלו, כפי שהיא עולה מהמענה על שאלון הספקים ו/או מהפעלת כלים טכנולוגים לדירוג הספק, מידת המוטיבציה של יריב לתקוף ספק זה ועוד.

8.2.4.2. **מאפייני ההתקשרות**, כגון סוג המידע עימו עוסק הספק, ממשקים פתוחים מולו, תלות טכנולוגית בתוצר המתקבל ממנו ועוד. שקלול זה יסייע לארגון לתעדף את המשאבים המוקצים לטובת ניהול סיכוני שרשרת האספקה.

- **ספקים אשר דורגו ברמה A** - יידרשו להוכיח את רמת ההגנה שלהם בדרישות שאלון הספקים (ראה נספח ד') באמצעות בודק ספקים/גורם בדיקה מאושר. לצפייה ברשימת גורמי הבדיקה המאושרים, ראה רשימה באתר המערך[4] ובמודול האסדרה.
- **ספקים אשר דורגו ברמה B** - יידרשו לענות על השאלון לרבות צירוף הראיות הנדרשות בשאלון. את הראיות הספק יעביר ללקוח בערוץ בטוח שיסוכם בין הצדדים.
- **ספקים אשר דורגו ברמה C** - ימלאו את שאלון הספקים ויחתימו עורך דין או את מנכ"ל החברה על הצהרת הספק לגבי רמת עמידתו בדרישות ההגנה שבשאלון.

[4] בודקי ובודקות ספקים
https://www.gov.il/he/departments/general/bodkim_2019

בסוף שלב זה, בידי הארגון תהיה טבלה של מיפוי ספקים עם דירוג רמת הסיכון/מידת הקריטיות של כל אחד מהם. ראה טבלה לדוגמה:

מיפוי ספקים					**דירוג ספקים**
שם הספק	**מאפייני ההתקשרות**	**איש קשר מהצד העסקי בארגון אל מול הספק**	**פרטי התקשרות מול נציג הספק לשאלות בנושא סייבר**	**קטגוריית השירות הניתן (שירות מבוסס מרכז נתונים שיתופי /פיתוח תוכנה/גישה מרחוק/ אחסון אתרים/ שירות שכולל חשיפת מידע של הלקוח/אבטחת OT)**	**רמת הסיכון של הספק (ספק מהותי/לא מהותי)**
ישראל ישראלי ייעוץ אסטרטגי	ליווי הנהלת הארגון בבניית תכנית אסטרטגית	ענת	XYZ	דרישות רוחביות - כתיבת מסמכים רגישים עבור הארגון. הספק מחזיק בתכניות רגישות להנהלה בנושא תחומי העיסוק אליהם הארגון מתכוון לפנות בשנים הקרובות.	כן
ישראל כהן - מיישם ERP	יישום המערכת מול מחלקת תפעול	ישראל	ABC	דרישות רוחביות. פיתוח תוכנה - מלווה את אגף מערכות מידע ביישום המערכת.	לא
ישראלי פיתוח ואחסון אתרים	אחסון אתר החברה (כולל שדרוגים, תחזוקה וכו')	אור	AAA	דרישות רוחביות. אחסון האתר וניהולו.	כן

ישראל אינטגרציה	תמיכה בציוד התקשורת	אלי	BBB	דרישות רוחביות - לספק אין גישה מרחוק ועבודתו מתמקדת בליווי אנשי התקשורת שלנו.	לא
ישראלי משרד עו"ד	עורך פטנטים	ישראל	CCC	דרישות רוחביות - הספק מחזיק במחשבו האישי ובאמצעים נתיקים מידע רגיש של החברה.	כן

טבלה 3: דוגמה לטבלה של מיפוי ספקים הכוללת דירוג רמת הסיכון/מידת הקריטיות

8.3. **<u>הערכת רמת ההגנה של הספק בהתאם לדירוג הספק</u>**:

8.3.1. לטובת הערכת רמת ההגנה של הספק, הארגון יפנה אל ספקיו בדרישה לקבל מענה אודות דרישות ההגנה בהתאם למתודה זו. לטובת כך, על הלקוח להגדיר לספק את ארבעת הפרמטרים הבאים:

- ✓ **האם הספק מהותי בעיני הלקוח** - לטובת מתן חליפת הגנה אשר מותאמת לסיכון אשר נגזר מההתקשרות עם הספק הספציפי, נדרש להגדיר לספק האם הוא מהותי מבחינת הלקוח. הגדרה זו משפיעה על כמות ועומק יישום הבקרות הנדרשות ממנו. כך לדוגמה, ספק אשר איננו מוגדר מהותי, יידרש לניהול היבטי גיבוי בסיסיים, בעוד ספק שהוגדר כמהותי יידרש ליותר בקרות וליישומן באופן מתקדם יותר תוך אימוץ תפיסת הגנה מכוונת איומים (Threat-Based Defense), ואבטחה מבוססת ראיות (Evidence-Based Security).
- ✓ **האם הספק מהותי בעיני הרגולטור** - לטובת מתן חליפת הגנה אשר מותאמת לסיכון אשר נגזר מההתקשרות עם הספק הספציפי, נדרש להגדיר לספק האם הוא מהותי מבחינת רגולטור. הערה: יש לשים לב כי בתקנים וברגולציות מסוימות, ישנה הגדרה של הרגולטור עבור מיהו ספק מהותי. במקרה של ספק יש להתייעץ עם הרגולטור הרלוונטי.
- ✓ **מהו סוג השירות הרלוונטי** - על הספק לדעת האם מצופה ממנו במסגרת ההתקשרות להתחבר מרחוק, לפתח תוכנה וכו'. אמנם ישנן דרישות מינימום אשר נדרשות בכל התקשרות (דרישות רוחביות) , אך במקרים בהם ההתקשרות כוללת מאפיינים ספציפיים כגון תהליכי פיתוח, הספק

נדרש להתייחס להיבטי הגנה נוספים אשר מפורטים בשאלון הספקים שבמתודה זו.

- ✓ **אופן המענה המצופה** - על הספק לדעת האם עליו למלא את הדו"ח באמצעות הצהרה עצמית אותה הוא מפיק מהמערכת, האם עליו לצרף ראיות נדרשות בהתאם לדרישות השאלון או שעליו להוכיח את אופן עמידתו בדרישות המתודה באמצעות גורם בלתי תלוי (כגון גורם בדיקה מאושר).

במידה והספק כבר מאושר, ייתכן והלקוח יסתפק בבקשה מהספק להמציא לו את תוצאות הסקר או בהשלמה נקודתית של מספר דרישות מסוימות.

מומלץ לבנות תכנית עבודה שנתית אשר תציג מתי פונים ולאיזה ספק, לרבות נוסח פניה קבוע אשר יקל על מימוש התהליך בצד הלקוח ואשר תוודא סגירת מעגל אשר מכסה את כלל הספקים הרלוונטיים (בהתאם לניהול הסיכון של הארגון).

⚠ יש לשים לב, כי רמת הסיכון של חלק מהספקים עשויה להיות מושפעת מהיבטים רגולטוריים וכן מעובדת היותם ספקי מל"ח (משק לשעת חירום).

8.4. **קבלת החלטה על אופן ניהול הסיכון בהתקשרות עם הספק:** במקרים מסוימים, על אף הצורך להתקשר עם ספקים אשר יש להם רמת הגנה בסייבר נאותה, ייתכן והנהלת הארגון תדרוש לבצע את ההתקשרות בכל מצב. לטובת ניהול נכון של הסיכון, מומלץ לזכור את ארבע האפשרויות הקיימות בעולם ניהול הסיכונים:

- **קבלת הסיכון** - במקרה זה נדרש להציג להנהלת הארגון את הסיכון הפוטנציאלי ואת העובדה כי הוחלט שלא לנקוט באמצעים מיוחדים בהתקשרות עם ספק זה. מקרה זה יכול להיות במקרים בהם הספק לא מספיק מהותי, ואז הארגון מחליט שלא לפנות אליו כלל עם דרישות הגנה, במקרים בהם ישנה תלות גדולה בספק והוא איננו מוכן לענות על דרישות ההגנה, אך הארגון מעוניין בהתקשרות עימו בשל אילוצים אחרים ובמקרים נוספים.
- **העברת הסיכון** - לדוגמה באמצעות ביטוח הלקוח מפני נזקים מסוג זה.
- **הפחתת הסיכון** - לדוגמה באמצעות הוספת בקרות מפצות מול הספק.
- **דחיית הסיכון** - לדוגמה באמצעות המלצה להנהלה שלא לחדש את ההתקשרות או המלצה להפסיקה לאלתר.

8.5. יש לבנות מפת סיכונים הנגזרת מההתקשרויות הקיימות מול ספקי הארגון. מפה זו תהיה מתוחזקת על ידי הגורם האמון על הגנת הסייבר בארגון. מפה זו תעודכן באופן שוטף ותאושר על ידי הנהלת הארגון בצורה עיתית.
שים לב: סיכוני הסייבר בשגרה ובחירום עשויים להיות שונים. התקשרות עם

ספקים בשגרה, מתבססת רוב על מספר הנחות עבודה, אשר לעיתים משתנות במעבר לחירום במידה והוא ברמה לאומית ו/או בינלאומית.

לצפייה ברשימת סיכונים לדוגמה ראה נספח ה'.

9. היערכות פרטנית מול הספקים השונים

9.1. **הסכם ההתקשרות** - יש לחתום מול הספק על הסכם התקשרות ובו כלל היבטי ניהול סיכוני סייבר בשרשרת אספקה. שילוב היבטי ההגנה בסייבר, אל מול החוזים וההסכמים יעוגן בנוהל עבודה מתואם עם גורמי הרכש בארגון. יש לשים לב למקרים בהם ישנו חוזה התקשרות קיים, ארוך טווח. במקרים אלו, לא פעם קשה יותר לרתום את הספק להעלות את רמת ההגנה שלו בסייבר. מומלץ לבחון מול אנשי הרכש את היכולת של הארגון להניע את הספק לממש את דרישות ההגנה המצופות.

9.2. **תדרוך הספק**

9.2.1. עם תחילת עבודתו של הספק או חשיפתו למערכת באופן פיזי או לוגי, יתודרך כל אחד מעובדי הספק המשתתף בהתקשרות בנושאים הבאים:

9.2.1.1. האיומים הרלוונטיים למערכת ולתהליך העסקית.

9.2.1.2. הנזקים הפוטנציאליים מתקיפת סייבר של המערכת.

9.2.1.3. פירוט ההנחיות בהן הם נדרשים לעמוד וליישם.

9.2.1.4. התדרוך יועבר על ידי גורם מאושר מהארגון הבקיא בדרישות הגנת המידע הנדרשות על מנת להפחית את חשיפת הארגון לסיכון ככל הניתן.

9.2.1.5. בהמשך לתדרוך יחתום העובד על הצהרה בה הוא מתחייב ליישם את דרישות האבטחה.

9.2.1.6. מסמכי ההצהרה יישמרו בחזקת הארגון עד לפרק זמן מוגדר בהתאם לכל הוראת חוק ורגולציה, מיום הפסקת עבודתו של הספק.

9.3. **בקרות ליישום במהלך ההתקשרות**

9.3.1. במקרה בו הספק פועל במתחמי הארגון יש לוודא כי הפעילות המתבצעת הינה בכפוף להנחיות המחייבות את עובדי הארגון.

9.3.2. במקרה בו הספק פועל ממתקניו, החברה תעביר מסמך דרישות אבטחה לספק, טרם תחילת עבודתו או חשיפתו למערכת פיזית או לוגית.

9.3.2.1. עבור ספקים מהותיים, יש לתקף אחת בשנה לפחות את עמידת הספק בהתחייבויותיו שבחוזה התקשרות.

9.3.2.2. עבור ספקים מהותיים, מומלץ לבחון שימוש בכלי ניטור אשר מספקים יכולת קבלת אינדיקציה בזמן אמת וביקורת רציפה אחר רמת ההגנה של הספק (Continuity Control Monitoring)

9.3.2.3. על הארגון להגדיר את הפעילויות עבורן נדרש הספק לעשות שימוש באמצעי זיהוי חזקים.

9.3.2.4. על הארגון להיות ערוך לתפעל אירוע אבטחת מידע - חוזית, תהליכית וטכנולוגית.

9.3.2.5. נוכח הסיכונים הגלומים בגישה מרחוק של פעילות ספק (במידה ורלוונטי) , חובת הארגון לקיים מנגנוני אבטחה ובקרה שיסייעו להפחתתם כדוגמת:

- סביבה מבודדת, ייעודית ובתצורה וירטואלית.
- ההתקשרות מהאינטרנט אל מערכות הארגון תתבצע בפרוטוקול תקשורת (Session) שונה מזה שבו תבוצע ההתקשרות בין הסביבה המבודדת למערכות הארגון.
- הגישה לסביבה זו תהיה במתכונת Allowlist ותגביל את התחנות והכתובות המורשות לגישה, הפרוטוקולים, זמני התחברות, משך התחברות פעיל וניתוק לאחר אי-פעילות ויישומים מורשים לגישה.
- הסביבה תוחזר למצב מאובטח (Steady State) בסיום השימוש.
- יש להגביל את זמן החיבור הפעיל וזמן לניתוק לאחר חוסר פעילות בחיבור.
- חשבון המשתמש לגישה מבחוץ יהיה שונה מזה המשמש לגישה מבפנים ובעל נתוני זיהוי ואימות שונים.
- האימות יתבסס על אימות רב-גורמי (MFA).
- החשבון וההרשאות ברמת היישום עבור גישה מרחוק יהיו שונות מאלו המשמשות לגישה פנימית.
- יש למנוע מהמשתמש להיות מחובר בו זמנית לרשתות או למערכות הגוף באופן מקומי ומרוחק. יש לייצר התרעה על כל מקרה כזה.
- כלל היישומים בתחנה יופעלו במתכונת Allowlist ולא תתאפשר הפעלת יישומים לא מורשים.
- נתוני האימות והזיהוי לחשבון ניהול מרחוק יהיו שונים מאלו של חשבונות הניהול הפנימיים וינוהלו בקבוצה ייעודית.
- יש להגדיר כי המשתמש המתחבר מרחוק יקבל רק את הרשאות הגישה הנדרשות לפעולות ניהול המותרות לביצוע מרחוק, כפי שיוגדר על ידי גורם מאושר מטעם הארגון.

- יש לבצע הקלטת תעבורה וניטור כל זמן ההתקשרות ולאתר אנומליות וחריגות מהפעולות המורשות לצרכי ניהול וחריגה ממדיניות האבטחה (יש לעדכן את הספק כי כל פעולותיהם במערכות החברה יוקלטו).
- מניעת גישת הספק למערכות הארגון ללא אישור, בדגש על סביבת היצור.
- הבטחת גישה מאובטחת ומסביבת פעילות נפרדת מיתר סביבות העבודה של הספק.

9.3.2.6. יש להגדיר בנוהל כתוב את תהליך ההתחברות של הספק לצורך תחזוקת/ניהול רכיבי המערכת ברשת תוך התייחסות לדברים הבאים:

- ייזום ההתחברות ואישור הפעילות - רק על ידי גורם מאושר מטעם הארגון.
- אופן הניטור וההקלטה.
- קבלת התרעות וטיפול בחריגות.
- הפסקת הפעילות וסגירת ההתחברות.
- בדיקת סיום ההתחברות והניתוק ממערכות הארגון.

9.3.2.7. יש ליצור יכולת לנתק באופן מיידי את הקישור במקרה שמזוהה אירוע חריג.

9.3.2.8. יש למנוע אפשרות להכנסת ו/או הוצאת קבצים בערוץ זה, אלא בערוץ הלבנה/השחרה / DLP נפרד.

9.3.2.9. נוכח הסיכונים הגלומים בספק חיצוני עם גישה למתקני הארגון (במידה ורלוונטי), חובת הארגון לקיים מנגנוני אבטחה ובקרה שיסייעו להפחתתם כדוגמת:

- עבור פעילות של ספק קבוע, יש להתקין מחשב ייעודי של הארגון ועליו יהיו מותקנים כל היישומים הנדרשים לספק לפעילותו.
- עבור פעילות אד-הוק כגון מבדק חדירה, סקר פגיעויות וכדומה יש לקבוע מראש את היקף הפעילות של הספק באופן ברור ומפורט ולקבוע מדדים להצלחה וכישלון, מקרים ותגובות במקרה של תקלה ולהגדיר גורם פנימי המלווה באופן אפקטיבי את הבודק.
- אין למסור סיסמאות ניהול קיימות לספק. במידת הצורך, יש להקים חשבון ייעודי, זמני, עם ההרשאה הנדרשת בלבד לפעילות.
- במקרה של מסירת הרשאות ניהול במסגרת הפעילות יש לשנותם במיידי.
- יש לעדכן את הגורמים הרלוונטיים לגבי תחילת וסיום הפעילות לצורך הגברת ערנותם והעלאת סף הרגישות לאירועים חריגים.

- כל פעילות המבוצעת על ידי הספק במערכות הארגון (כגון מבדק חדירה, סקר פגיעויות) יבוצעו תוך פגיעה מינימלית ברמת האבטחה וניתוח משמעויות מהסיכונים הנגזרים מפעילות כגון זו.
- בסיום הפעילות יש לבצע בדיקה מהן הפעילויות שבוצעו בפועל ולסגור חשבונות והרשאות זמניות אשר הוקצו לטובת הפעילות.

9.3.3. **הגנת מידע תפעולי רגיש**

מידע תפעולי רגיש הינו מידע אשר נוגע לתפעול/ תחזוקת/ אבטחת/ ניהול המערכות, שבמקרה ויגיע לידי תוקף, עלול לאפשר קיצור שלבים בתהליך תקיפת מערכות קריטיות ו/או הזלגת מידע רגיש כדוגמת:

- שמות משתמשים, אמצעי הזדהות דוגמת סיסמאות.
- טופולוגיה של רשתות (כגון תרשימי רשת הכוללים כתובות IP).
- פרמטרים של ציוד אבטחה ותקשורת (כגון חוקים של FW והגדרות תקשורת).
- תרשימים הנדסיים של בניינים ומתחמי עבודה.
- מפרט רכש של אמצעיים מיוחדים.
- רשימת ספקים.
- מידע טכני/ תפעולי על המערכת (כגון ספים תפעוליים, קוד מקור).
- תצלומים של מתחמים ורכיבים רגישים (כגון חדרי שרתים וציוד תקשורת).
- גיבויים הכוללים קבצים ובסיסי נתונים.
- מידע אודות הורדה זמנית של רמת האבטחה במערכת, לצורך ביצוע פעילות תחזוקה/ עדכון.

9.3.4. מידע רגיש יאוחסן בצורה מאובטחת הכוללת הצפנה ובקרת גישה למורשים בלבד.

9.3.5. יש להפעיל ניטור על כל ניסיונות הגישה והשימוש במידע, לרבות ניסיונות לא מוצלחים.

9.3.6. יש לחסום את האפשרות של גורמים לא מורשים לשלוח מידע מסווג מחוץ לרשת הארגונית בעזרת אמצעים ייעודיים לכך (כגון DLP). יש לוודא כי האיתור של מידע רגיש/חסוי כולל גם התייחסות למידע תפעולי רגיש.

9.3.7. מידע תפעולי מסווג יועבר לגורם חיצוני בתצורה מאובטחת בלבד (דוא"ל מוצפן או באמצעות מנגנון העברת קבצים מאובטח (כגון כספות).

9.3.8. יש להצפין את הדיסק הקשיח ואת ה- BIOS/UEFI של מחשבים ניידים עם מידע זה.

9.3.9. **הגנת מידע בבקרים תעשייתיים OT (Operational Technology)**

מרבית רשתות הבקרים התעשייתיים תוכננו לפני זמן רב, בטרם הייתה מודעות לאיומי סייבר. לפיכך, חסרות ברשתות אלו בקרות הגנת מידע. עם עליית האיומים החיצוניים והפנימיים המכוונים לתשתיות תעשייתית וקריטיות, יש צורך בבקרות המספקות חשיפה בזמן אמת והגנה תוך עמידה בדרישות הטכניות והתפעוליות הייחודיות של עולם הבקרים התעשייתיים.
לבקרות ספציפיות הנוגעות בעולם הבקרים התעשייתיים, יש לעיין במסמכים מקובלים של גופי תקינה מובילים בתחום.

9.3.10. בקרות מפצות וסנקציות

9.3.10.1. לעיתים יש צורך בבקרות מפצות בהתקשרות עם ספק, במקרים בהם לא ניתן לסמוך או להשפיע באופן משביע רצון על רמת הגנת המידע של הספק, להלן דוגמאות לבקרות מפצות שניתן ליישם בעת התקשרות:

- על הארגון לספק מחשב נייד מוקשח או עמדה ייעודית מוקשחת לצורך פעילות הספק.
- ככל הניתן, יש לוודא כי עבודת הספק תעשה מתוך חצרות הארגון.
- במידה והספק אינו מיישם הפרדת סביבות, על הארגון לספק סביבה בטוחה שדרכה הספק יספק את שירותיו.
- הארגון יבדוק את המערכת/השירות של הספק באמצעות כלים פנימיים וכן שימוש במבדקי חדירה טרם עליית המערכת/השירות לשלב הייצור.

לעיתים יש צורך בהפעלת סנקציות אל מול פעילויות הספק, להלן דוגמאות לסנקציות:

- במידה והספק לא עומד בקריטריונים אותם הגדיר הארגון כקריטיים לצורך התקשרות, יש להתנות את ההתקשרות בביצוע סקר ספק ובמסגרת זו הארגון (או גורם אחר מטעמו) יבצע סקר אודות אופי והתנהלות הספק טרם חתימת החוזה.
- במידה והספק חורג מהנחיות האבטחה של הארגון, יש לפעול בשיקול דעת ובמידת הצורך להפסיק את ההתקשרות או להפעיל סנקציות כספיות (בהתאם ובכפוף לעיגון הנושא בחוזה ההתקשרות מול הספק).
- אם במהלך תקופת ההתקשרות עלה חשד כי הספק המהותי חושף את הארגון לסיכוני סייבר משמעותיים יש לבחון הפסקת ההתקשרות באופן מיידי.
- דרישה מהספק לרכוש ביטוח סייבר אשר כולל בין היתר שיפוי לנזקים עבור צד ג'.

יש לשים לב, תורת ההגנה בסייבר לארגון בגרסה העדכנית מהווה את למקור לפרשנות דרישות המתודה.

10. סיכום

מסמך זה נועד לשמש ארגונים (בייחוד את ממונה הגנת מידע וסייבר) כמתודה לניהול סיכוני הגנת מידע וסייבר בשרשרת אספקה. המסמך מספק מתודה סדורה וישימה לניהול ההגנה בסייבר על שרשרת האספקה, לצד סט בקרות מפורטות ומומלצות ליישום על ידי כלל הארגונים במשק, לצורך ניהול שוטף ואפקטיבי של שרשרת האספקה.

ניהול שרשרת האספקה מייצג את מחזור החיים של פעילויות הארגון אל מול ספקי שירות ומוצרים. הניהול מתחיל בשלב מקדים של מיפוי וסיווג נכסי המידע הארגוניים לאחר מכן מיפוי הספקים עמם הארגון יחליט להתקשר.

יש להעריך את הספק באופן תקופתי ומתמשך, באמצעות מערכת קריטריונים ואופן מדידה קבוע מראש. כמו כן, במהלך ההתקשרות על הארגון לבצע הערכת סיכונים מתמדת ולפעול בהתאם לסיכונים אלו.

חשוב להדגיש את החשיבות בחוזה התקשרות מקיף הכולל את כל התנאים ורמת השירות הנדרשים לעמידה ברמת הגנת מידע וסייברמספקת עבור כל שירות/מוצר. על הארגונים לעבוד עם נהלים מסודרים ולתעד את תהליך בחירת הספק וניהולו במהלך ההתקשרות. בנוסף, על הארגון לבצע תדרוך מקיף בהיבטי הגנת מידע וסייבר לכלל עובדי הספק הצפויים להוות חלק מההתקשרות עם הארגון.

כמו כן, גם תהליך סיום ההתקשרות הינו מהותי ויש לוודא כי הסדרים עם הספק שנקבעו בהתקשרות מתקיימים בכל הקשור למחיקת נתונים וביטול הרשאות.

דגשים המופיעים לעיל יחד עם סט הבקרות, מהווים מתודה מסודרת לניהול שרשרת האספקה הארגונית.

נספח א - אבחנה בין תוכנות ניהול סיכוני סייבר לארגון לבין מודול שרשרת אספקה

תהליך ניהול סיכוני סייבר בשרשרת האספקה, מציב אתגרים הן לספקים והן ללקוחות. עבור כל צד בתהליך, ישנם פתרונות שונים לאתגרים השונים. לטובת הבנת ההבדלים שבין תוכנות וכלים ממשפחת VRM ו/או כלי GRC שונים, לבין מודול שרשרת אספקה של מערך הסייבר, נדרש לחדד את הפערים שבין האתגרים.

האתגר	משמעות בעיני הלקוח	משמעות בעיני הספק
שאלון עם דרישות הגנה - חוסר אחידות	מה לבקש מהספקים? כיצד לרתום אותם לענות על השאלון הייחודי של הלקוח?	הספק מקבל עשרות שאלונים **שונים** בשנה
ניהול התהליך שבין הספק ללקוח	נדרש לעקוב אחר סטטוס המענה ואחר פערי ההגנה של כל אחד ממאות/אלפי הספקים	נדרש להפיץ את המענה שלו בעשרות מערכות שונות ומול עשרות ומאות לקוחות שונים
כיצד לאמת את הצהרת הספק?	נדרש לבצע עשרות ולעיתים מאות ביקורות בשנה	הספק עובר עשרות ביקורות בשנה

טבלה 4: אבחנה בין תוכנות ניהול סיכוני סייבר לארגון לבין מודול שרשרת אספקה

מודול שרשרת אספקה במערכת יוב"ל, קם **במטרה לסייע לספקים** במשק לבצע את התהליך בצורה יעילה ומועילה.

עיקרי התועלות של המודול בעיני הספק:

- ✓ קבלת הגרסה העדכנית של השאלון הלאומי במקום זמין, בפשטות ובחינם.
- ✓ קבלת יכולת להפיק דו"חות בפורמט מוסדר ומקובל מטעם מערך הסייבר הלאומי, איתו ניתן לגשת לתהליך ההסמכה מול גוף התעדה מאושר.
- ✓ קבלת יכולת לנהל את תהליך תיקון הליקויים והפערים אל מול דרישות מערך הסייבר משרשרת האספקה.
- ✓ חיבור לתוצרים נוספים של מערך הסייבר, כגון מודול תורת ההגנה, מסמכי המלצות הגנה ועוד.

לטובת סיוע לארגונים אשר מהווים את "צד הלקוח", אשר מנהלים פעמים רבות מאות ואלפי ספקים, קמו בשנים האחרונות פתרונות מסוגים שונים. ספקים אלו,

נכנסים לקטגוריה הולכת ומתרחבת בארץ ובעולם של תוכנות אשר נקראות: Vendor Risk Management או 3rd party risk assessment.

חלק מספקים אלו, ייעודיים לעולם ניהול פתרונות אלו, מאפשרים פעמים רבות לארגונים בין היתר את הדברים הבאים:

- ✓ ניהול "מאגר הספקים" של הארגון, לרבות אנשי קשר, תאריך ביצוע סקר אחרון, מאפייני ההתקשרות, לקוח פנימי של הספק בתוך הארגון ועוד.
- ✓ יכולת שליחה אוטומטית של השאלון אל הספקים בצורה מתוזמנת למייל של הספק.
- ✓ יכולת קבלת דשבורד אשר מציג את דירוג הספקים על פי מידת הסיכון הגלומה בהתקשרות עימם ובהתאם לרמת ההגנה שלהם ("מפת חום" לספקים).
- ✓ יכולת ניהול השיח עם הספק על גבי הפלטפורמה, לרבות העלאת צרופות, התכתבות במקום מרכזי, התייחסות לפרטים שהוזנו על ידי הספק ועוד.
- ✓ יכולת הערכת סיכון של הספק בצורה אוטומטית (מלאה או חלקית) בהתבסס על כלי סריקה חיצוניים או פנימיים לספק (rating) + יכולת להעלות צרופות למערכת.
- ✓ יכולת קבלת מודיעין על חולשות ופגיעויות אצל ספקיו (לדוגמה, על בסיס מידע שאותר בדארקנט, מנועי איתור חולשות ועוד) ושקלול הציון בהתבסס על המענה של הספק ועל איום ייחוס/מאפיינים מגזריים ועוד.
- ✓ שירות מומחה (MSSP/MDR) אשר נלווה לתוכנה במטרה לנהל את התהליך בהיבטי סייבר מול הספקים עבור הלקוח.
- ✓ ממשק מול מערכות פנימיות בארגון, כגון מערכת לניהול משימות, מערכת לניהול קשרי לקוחות, מערכת ERP, שרת AD ועוד.

יכולות אלו אינן נכללות במודול שרשרת האספקה של מערך הסייבר הלאומי.

נספח ב - אתגרים ומענה לאומי

בבחינה שנערכה במשק הישראלי במהלך שנת 2018, לצד בחינת המתודות המקובלות בעולם, עולה התמונה הבאה:

- **לא קיים תקן/שפה מקובלת "דה פקטו" של ארגונים במשק אל מול הספקים שלהם.** למעשה, המשק מתחלק ברובו, לארגונים שאינם מבצעים שום פעילות הגנה אל מול שרשרת האספקה שלהם, כאלו שפיתחו בעצמם שאלון (לרוב איננו מותאם לסוגי התקשרויות שונות) ולכאלו שדורשים מהספק לעמוד בדרישות תקן דוגמת ISO 27001. הדבר יוצר קושי על ארגונים והשקעת משאבים בפיתוח ותחזוקת השאלון.
- **קיים קושי לנהל את תהליך ההפצה, תמיכה בשאלות הספק ובניתוח הממצאים.** ארגונים נדרשים להפיץ את השאלון לעשרות, מאות ולעיתים לאלפי ספקים (לרוב באמצעות דוא"ל). לאחר מכן, על הארגון לוודא כי הספק שקיבל את השאלון אכן מבין מה מצופה ממנו וכיצד להשיב על השאלון הספציפי של הארגון הספציפי. לבסוף, על הארגון לנתח את השאלונים ולקבל החלטה על סמך התוצאות שנשלחו אליו. פעילות זו דורשת זמן רב של איש הגנת המידע/סייבר שלרוב הינו משאב מוגבל.

- **ארגונים לא מצליחים לכסות את היקף הביקורת על הספקים שלהם מבחינת כמות והיקף הבדיקות.**

בשיחות שנערכות עם ספקים, לקוחות, רגולטורים ויועצים במהלך שנת 2018, עולה כי

1. שפה אחודה -

פיתוח של "תקן" לדרישות מהספק, עשוי לסייע לארגונים (ספקים ולקוחות) לחסוך זמן בפיתוח מסמך כזה, בתמיכה בשאלות ועוד. המצב הנוכחי, לפיו כל ארגון מפתח בעצמו שאלון מקשה הן על הלקוחות והן על הספקים. יצירת שפה משותפת למשק, תפחית את הנטל בשלב התכנון ובשלב הבקרה והביקורת.

2. בניית מנגנון אמון-

לטובת חסכון בזמן ובכסף של ארגונים, משני צדדי ההתקשרות (ספק ולקוח), נדרש לוודא כי רמת ההוכחה ואופן הבדיקה שלה התבצעה בצורה מקצועית. המצב הנוכחי, לפיו ארגונים רבים מבצעים מבדק/סקר לאותו הספק מקשה הן על הספק והן על הלקוח. מה גם, שניתן לייצר את המכנה המשותף הרחב שמעניין לקוחות רבים במשק (כגון קיומם של לוגים, עמידה בתקנות הגנת הפרטיות, גיבויים, כלי הגנה להגנה על עמדות קצה ועל הרשת ועוד). למרות שהספקים לא פעם "ביצעו את התהליך" עבור לקוח מסוים, ואפילו באמצעות יועץ/גורם בלתי תלוי, פעמים רבות הם נדרשים לבצע מענה מחדש על כל השאלון עבור לקוחות אחרים במשק. בשל הקושי של גופים לבצע סקרים עבור ספקים רבים, פעמים רבות הלקוחות מסתפקים בשליחת שאלון והסתמכות על צורת עבודה של "קרא וחתום".

לטובת הקלה על ארגונים במשק לנהל את התהליך בצורה מיטבית, נדרש לקדם בעיקר שני נושאים:

בהינתן שארגון א' ידע כי ספק מסוים, נשאל את השאלות שחשובות לו, והספק אף הוכיח זאת באמצעות בדיקה מקצועית של צד ג' (Certified auditor), ייתכן שארגון ב' לא יידרש לבצע פעילויות מול ספק זה. גם במקרים בהם ארגון ב' ירצה לבדוק נושאים נוספים, הרי שאת המכנה משותף הרחב עבור חלק ניכר מהמשק - הספק הוכיח בצורה טובה ומקצועית.

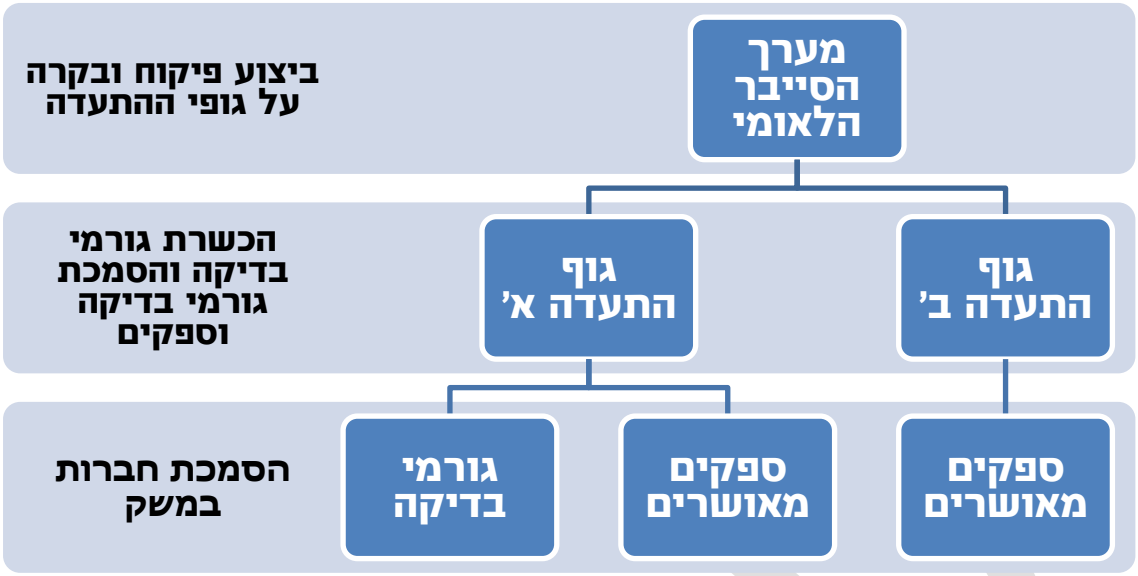
לטובת מתן מענה לצורך זה, פיתח מערך הסייבר את הכלים הבאים לטובת אסדרת המשק:

א. **שאלון ספקים** - סט דרישות מודולרי לספקים במשק. דרישות אלו, מחולקות בהתאם לרמת הסיכון שמהווה הספק לתהליכים העסקיים של הארגון ומערכותיו (ספק מהותי/לא מהותי) וכן מאופי ההתקשרות (ספק מרכז נתונים שיתופי, ספק מפתח תוכנה, ספק שמקבל גישה מרחוק/ ספק אחסון אתרים וכו').

ב. **פירמידת הכשרה והסמכה של גורמי בדיקה מאושרים** - מערך הסייבר פיתח מסלול להכשרה ולבקרה אחר בעלי המקצוע אשר עוסקים בתחום ביקורת ספקים. גורמים אלו, עברו סינון מקדים מבחינת תנאי קדם וכן עברו תהליך של ראיון מקצועי והכשרה מקצועית אשר התבצעו בהתאם לסילבוס שהוגדר על ידי מערך הסייבר הלאומי. בודקי הספקים המאושרים, הינם אנשי מקצוע אשר מסייעים להסמכת ספקים במשק באופן בו ניתן לדעת כי הסקר שהתבצע לספק נעשה על ידי איש מקצוע בעל רמה גבוהה.

ג. **פירמידת הכשרה והסמכה של ספקים -** ספקים במשק אשר עברו תהליך סקר סיכונים באמצעות גורם בדיקה מאושר, מוגשים על ידו לגוף התעדה (Certification Bodies) אשר מורשה להנפיק לספק תעודת "ספק מאושר". לטובת וידוא שמירה על רמת ביקורות נאותה במשק, מתבצעת בקרה על תקינות פעילותם של גופי ההתעדה.

לפיכך, ניתן לתאר באופן סכמתי את פירמידת ההסמכה בהתאם לתרשים הבא:



תרשים 4: פירמידת ההסמכה

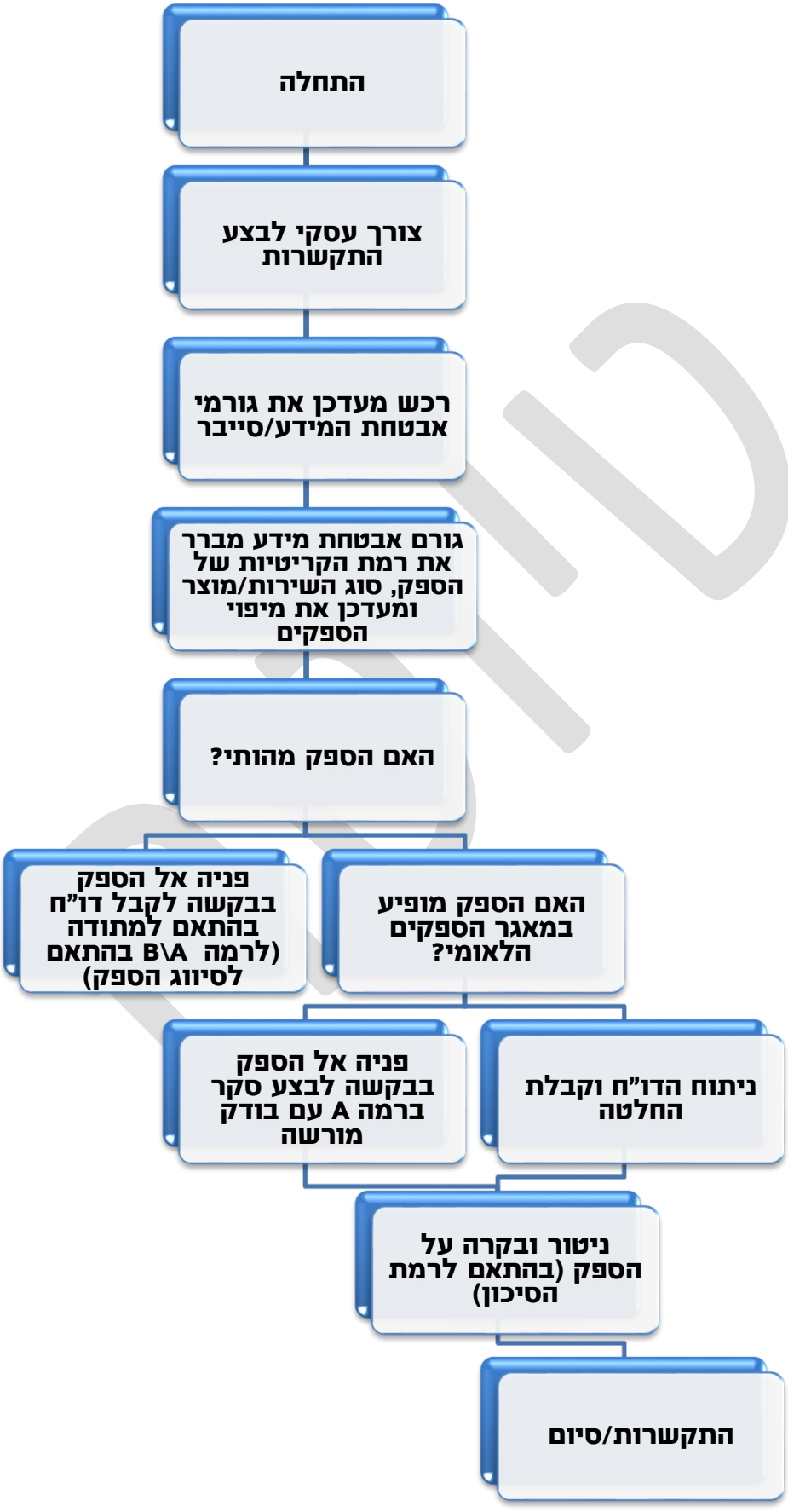
ד. **מערכת מידע** - מערכת יוב"ל (יעדים ובקרות לארגון) הינה פלטפורמה לאומית אשר מורכבת ממספר מודולים. בין המודולים של המערכת, ישנו מודול אשר מספק מענה לכמה מהאתגרים שקשורים לניהול סיכוני הסייבר של שרשרת האספקה. בין אתגרים אלו ניתן למנות:

1) **משאבים מועטים לתמיכה בשלב הפצת השאלון לספקים רבים** - כיום, לקוחות נדרשים לשלוח את השאלון שלהם לכל ספק וספק. לרוב הדבר נעשה באמצעות דואר אלקטרוני. תהליך זה, מצריך מהלקוח להחזיק רשימה עדכנית של אנשי הקשר אצל הספקים השונים, תשומות לשליחה ווידוא קבלת השאלון/דרישות הגנה בצד השני, ניהול גרסאות של השאלון ועדכון הספקים במידה והשתנו שאלות ועוד. לאחר מיכון השאלון, יכול כל ארגון להפנות את ספקיו למערכת, ולדעת כי הוא ימצא בה את השאלון הרלוונטי בגרסתו העדכנית.
2) **משאבים מועטים לשלב התמיכה בשאלות ספקים אודות אופן המענה** - עבודה עם המערכת, מסייעת לספק לקבל מידע עשיר אודות השאלות/דרישות ההגנה, לצד מסמכים נלווים ועזרים מרוכזים בפלטפורמה אחת.
3) **היעדר אחידות במבנה התוצר של תהליך הסקר** -לטובת תמיכה בתהליך הביקורות והבקרה של גורמי הבדיקה, כמו גם של גופי ההתעדה, המערכת מכוונת את ממלא הסקר בתהליך מובנה עד להפקת דו"ח מוגדר בסוף התהליך. דו"ח זה יכול להוות הצהרה עצמית, במקרה של ביצוע התהליך ללא גורם בדיקה מאושר ויכול להוות הבסיס איתו מגיע גורם הבדיקה אל גוף ההתעדה, במקרה של צורך בקבלת תעודת הסמכה מאושרת לספק.
4) **קושי של ספקים לנהל את הממצאים שעלו במהלך הסקר** - עבודה עם יישומים שונים והתכתבויות מקשים על שלב תיקון הליקויים ושיקוף המצב העדכני

ללקוח. המערכת מאפשרת לספק לקבל בצורה גרפית וטבלאית, (אותה ניתן לייצא בקלות) את תמונת המצב שלו, לצד יכולת לצלול לתוך נושא מסוים, לעדכן את רמת ההגנה הנוכחית ולהפיק דו"ח עדכני בהתאם.

5) **יישום עקרון אי ההכחשה** - כיום, פעמים רבות תהליך המענה על דרישות ההגנה מתנהל ביישומים שונים כגון תכתובות מייל, אקסל וכו'. עבודה עם מערכת מובנית, מסייעת למקבל הדו"ח לדעת מי ביצע את המענה על הדו"ח, מתי הופק הדו"ח, מי הגורם שחתם עליו ולדעת שהדו"ח נמסר בצורה שאיננה קובץ פתוח (כגון אקסל, אשר לא ניתן לדעת בקלות האם ערכים בו שונו, מתי, על ידי מי, מה היה הערך המקורי, היכן הגרסה העדכנית וכו').

נספח ג - שילוב היבטי הגנת סייבר בתהליך הרכש



תרשים 5: שילוב היבטי הגנת סייבר בתהליך הרכש

נספח ד - שאלון מתודת שרשרת אספקה צד הספק

שאלון הספקים מהווה את הבסיס הרחב הנדרש מהספק לטובת ההתקשרות. שאלון זה מהווה רף מקצועי מינימאלי, בהתאם לסוג ההתקשרות (כגון אחסון מידע במרכז נתונים שיתופי, פיתוח, גישה מרחוק, ספק אחסון אתרים וכו') וכן בהתאם למידת הרגישות של ההתקשרות (ספק מהותי/לא מהותי).

שאלון זה כולל דרישות הגנה שונות בהתאם למבנה הבא:

סוג התקשרות	מהותיות	מזהה נושא	נושא	דיוחי בקרה	בקרה	דגשים ליישום הבקרה	עומק יישום הבקרה	ראיות נדרשות	דגשים לבדיקה חיצונית	סף מעבר	תאימות לתקנים

טבלה 5: עמודות לדוגמה משאלון המתודה

קישור לשאלון בגרסתו העדכנית ניתן למצוא באתר מערך הסייבר (https://www.gov.il/he/departments/news/querysupply)

- **סוג התקשרות** -סוגי ההתקשרות השונים, כגון מרכז נתונים שיתופי, פיתוח תכנה וכו'.
- **מהותיות** - הגדרה האם דרישת ההגנה הספציפית מצופה מכל ספק, או רק מספק מהותי. האפשרויות בעמודה זו הינן כן/לא, כאשר במקרה בו כתוב "כן", אזי הדרישה שבשורה זו מצופה ליישום רק מהספקים המהותיים.
- **מזהה נושא** - מספר סידורי עבור נושאי הדרישות השונים.
- **נושא** - תיאור הנושא הכללי, תחתיו מאוגדות מספר דרישות הגנה (כגון: הגנה היקפית, גיבויים ושחזורים, הגנה על תחנות קצה וכו').

- **זיהוי בקרה** - מספר סידורי עבור דרישות ההגנה השונות.
- **בקרה** - תיאור הדרישה הספציפית המצופה מהספק ליישום.
- **דגשים ליישום הבקרה** - הכוונה כללית, אשר מסייעת לתאם ציפיות בין הספק ללקוח ולהסביר באמצעות דוגמאות ודגשים נוספים את מהות הבקרה.
- **עומק יישום הבקרה** - פירוט על אופנים שונים ליישום הבקרה, כאשר המענה נע בין "לא קיימת "ועד ל"קיימת בצורה אפקטיבית ומלאה" (כולל הטווח שבאמצע). עמודה זו נועדה לתאם ציפיות באשר לעומק יישום הבקרה/דרישה אצל הספק בפועל. כך לדוגמה, לא מצופה מהספק לענות "האם יש לוגים" או "האם ישנם גיבויים" במענה של כן/לא, אלא ניתנת לו האפשרות להסביר עד כמה הבקרה מוטמעת בארגון.
- **ראיות נדרשות** - הסבר על אופן ההוכחה ללקוח כי המענה שהוגדר אכן מיושם בפועל. ראיות אלו יועברו ללקוח בהתאם לסיכום בין הצדדים.
- **דגשים לבדיקה חיצונית** - דגשים עבור גורם הבדיקה אשר יש לוודא לפני מתן "ציון" לעומק ההטמעה. עמודה זו הינה חובה עבור בדיקה באמצעות גורמי בדיקה מאושרים.
- **סף מעבר** - הגדרת עומק ההטמעה המינימאלי הנדרש עבור כל בקרה, תוך הבחנה בין ספק מהותי לספק שאיננו מהותי. כך לדוגמה, ייתכן שעבור נושא הגיבויים עומק הבקרה המינימאלי הנדרש מספק שאיננו מהותי יהיה "1" ואילו עבור ספק מהותי, המינימום הנדרש הינו "3". ספק שאיננו עומד ברמת עומק יישום הבקרה בהתאם לדרישת הסף, איננו עומד בציפייה של הלקוח בנושא הספציפי.
- **תאימות לתקנים** - הצגת מראה מקום לתקנים ורגולציות אשר דורשות מהספק ליישם דרישה זו.

נספח ה' - סיכוני סייבר בשרשרת אספקה

בניהול שרשרת האספקה הארגון עלול להיחשף למגוון סיכונים פוטנציאליים, מצד ספקים וספקי משנה המספקים לארגון שירות או מוצר. לכן, על הארגון להיות מודע לסיכונים ולנהל אותם באופן מתמיד. ניהול הסיכונים כולל מיפויים, סיווגם (מבחינת רמת קריטיות) , הגדרת אחראי לטיפול בסיכון והבקרה הנדרשת להטמעה על מנת לצמצם את הסיכון ככל הניתן או לחילופין קבלת הסיכון או העברתו. במידה והספק או ספק משנה הנותן שירות או מספק מוצר לארגון ,מנהל את מערך אבטחת המידע שלו באופן לקוי, הדבר עלול לסכן את החברה.

ניתן לסווג את איומי הסייבר בהתאם לקטגוריות הבאות[5]:

מס'	הקטגוריה	דוגמה לתרחישים
1.	איום המכוון ישירות כנגד הארגון	החדרת נוזקה בערוץ דוא"ל. הדלפת מידע ע"י עובד הארגון. דליפת מידע של הארגון אשר אוחסן בענן בצורה לא ראויה (לדוגמה, כתוצאה מ- Misconfiguration).
2.	איום מצד ספק של הארגון	השתלטות על עמדת תמיכה של ספק, ושימוש ב-VPN לשם החדרת נוזקה לארגון. ביצוע הטמנה מכוונת ספציפית כנגד הארגון בסביבת הפיתוח של ספק (לרבות קוד פתוח), כאשר הארגון מתקין לאחר מכן את המוצר "המטופל" בחצרותיו. תוקף המנצל לרעה פגיעות תוכנה הקיימת במוצר שהארגון רכש מגורם חיצוני. גיום עובד פנימי בספק על-ידי מתחרה עסקי.

[5] ראוי לציין כי ישנם מודלים שונים לביצוע סיווג לתקיפות סייבר

		דלף מידע עסקי, כתוצאה מעזיבת עובד את הספק ללא הקפדה על תהליכי ניהול העסקה תקינים בצד הספק. פגיעה בפרטיות עובדי החברה, כתוצאה מפריצה לערוץ התקשורת באמצעותו הספק מעביר תוצרים ללקוח. פגיעה ביעדים עסקיים, עקב אי זמינות משאבי המחשוב של הספק (לדוגמה כתוצאה מפגיעת כופרה ברשת של הספק). פגיעה ביעדים עסקיים, כתוצאה מגניבת פטנטים או תכניות עסקיות אשר נשמרו בשרתי החברה שמלווה את הארגון בתהליך. דלף מידע כתוצאה מאובדן ציוד כגון מחשבים או מדיה נתיקה של הספק. קיומן של פגיעויות בקוד מקור עקב אי החלת תהליך פיתוח מאובטח הולם בצד הספק.
3.	שימוש בארגון ("הלקוח") כצינור לשם הגעה לארגון אחר	השתלטות על עמדת תמיכה של הארגון, ושימוש ב-VPN לשם החדרת נוזקה ללקוח של הארגון.
4.	נתזים מתקיפה כנגד ארגון אחר	תקיפת מניעת שירות מבוזרת (DDoS) כנגד אתר אינטרנט של ארגון אחר המאוחסן בסביבת אירוח (Hosting) המשרתת את אתר האינטרנט של הארגון.

		ביצוע הטמנה שאינה מכוונת ספציפית כנגד הארגון בסביבת הפיתוח של ספק (לרבות קוד פתוח), כאשר הארגון מתקין לאחר מכן את המוצר "המטופל" בחצרותיו.
5.	תקיפה שאינה מכוונת כנגד הארגון	תקיפת מניעת שירות מבוזרת (DDoS) אשר בוצעה עקב טעות נגד שם מתחם (Domain) של ארגון שאינו היעד האמיתי.

טבלה 6: סיווג תקיפות בהתאם לקטגוריות שכיחות

ניתן לראות כי תקיפות העונות לקטגוריה "2" אופייניות לתקיפות מסוג שרשרת אספקה כנגד צד לקוח. כמו כן, שכיח לראות תקיפות העונות לקטגוריות "4" ו"5" עשויות במקרים מסוימים לענות להגדרה זו.

כמו כן, יש גם סיכונים תפעוליים הנובעים משרשרת האספקה שעל הארגון לנהל:

- פגיעה במוניטין כתוצאה מתקלה המביאה לידי שיבוש נתונים של החברה אשר אוחסנו בענן.
- פגיעה בשירות הניתן לארגון מצד ספק עקב תקלה בספק משנה שלו
- העדר זמינות בשוק של חלקי חילוף המשרתים מערכות תקשוב
- רכישה של הספק על-ידי מתחרה עסקי של הארגון
- החלפת בעלים/קיומה של שליטה זרה בספק אשר עשויה לפגוע ביכולת הארגון להשיג את יעדיו

במצבי חירום לאומי, נדרשת היערכות שונה של ארגונים. במצב זה, על ארגונים לבחון את המשמעות שבמעבר מעבודה מול ספק אשר עובדיו נמצאים תחת מעטפת הגנת סייבר ידועה ומוכרת, למצב בו עובדיו אינם יכולים לגשת לחצרות הלקוח ו/או למשרדים שלהם.

במצבים אלו, יש לוודא מול הספק את חידוד הבקרות בהתאם לסיכונים מהם חוששים לאור השינוי החדש.

לדוגמה, ייתכן וכפועל יוצא מהמציאות החדשה, עשויים להתקיים מצבים שאינם שגרתיים, דוגמת:

✓ פיתוח תוכנה מהבית שלא בסביבה בטוחה, ועם תיעוד חלקי.

- ✓ שימוש נרחב במחשבים וציוד פרטי של עובדי הספק, לרבות MDM שלא קיים לרוב הספקים, ועובדי הספק שולחים לעצמם מידע רגיש/חסוי למייל הפרטי/לנייד.
- ✓ חלק ניכר ממנגנוני האבטחה של הספק אינם רלוונטיים לתצורת העבודה החדשה, וזאת לאור העובדה כי המימוש השכיח של ה-DLP הינו בכניסה/ביציאה לרשת הספק, ולפיכך אין אכיפה וניטור של פעילות עובדים המספקים שירות ללקוח.
- ✓ חוסר אמצעי הגנה מפני מניעת שירות/כופרה על מחשבי עובדי הספק.
- ✓ ייתכן והספק מעביר קבצים עם מידע רגיש למייל הפרטי ולא באמצעות כספות (או אמצעי מקביל).
- ✓ אי הקפדה על עקרונות המידור, דוגמת הפרדת מידע של לקוחות שונים ועוד.

לטובת כך, ניתן להסתייע במיפוי הבקרות שדורשות חידוד עם הסיכונים הרלוונטיים. דוגמה למפת סיכונים של ארגון לאור מציאות כזו יכולה להיראות כך:

מס'	תיאור הסיכון
.1	השתלטות זדונית על ממשק גישה מרחוק או דילוג נוזקה לרשת הארגון באמצעות ממשק גישה מרחוק
.2	ניצול לרעה של חולשות תוכנה בשירותים עסקיים חדשים באתר האינטרנט או באפליקציית מובייל של הארגון
.3	ניצול לרעה של טעות אנוש בהגדרת תצורה (System Configuration) של מערך ההגנה בסייבר/IT של הארגון
.4	אי זמינות שירותים עסקיים/מידע ארגוני בעקבות פעילות כופרה (Ransomware)
.5	השתלטות על חשבון/עמדת משתמש לשם הדלפת מידע (Data Leakage)

טבלה 7: דוגמה למיפוי בקרות שדורשות חידוד עם הסיכונים הרלוונטיים

***** סוף מסמך *****