31 בדצמבר 2015
י"ט בטבת התשע"ו

מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל

כתובת לקבלת דואר: משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450811, פקס 03-7450822

הקדמה

הגנת הסייבר של הארגונים במדינת ישראל מהווה אבן יסוד בתפיסה הלאומית להגנת הסייבר, כמשתקף בשתי החלטות ממשלה מפברואר 2015[1] שאותן קידם מטה הסייבר הלאומי.

כיום מועסקים בארגונים שונים במשק אנשי מקצוע במגוון דיסציפלינות של תחום הגנת הסייבר, עם שונות גבוהה ברמתם המקצועית וללא ודאות באשר לעמידתם בסטנדרטים מקצועיים שיאפשרו לארגונים להתמודד כנדרש עם איומי ואירועי סייבר. על רקע זה עלה הצורך להסדיר את מקצועות הגנת הסייבר בישראל, במטרה להבטיח את הרמה המקצועית, המהימנות והאתיקה של העוסקים בתחום.

נוכח מורכבות הנושא ורגישותו ועל מנת לבחון אותו בראייה משקית כוללת מינה ר' מטה הסייבר הלאומי, ד"ר אביתר מתניה, ועדה ציבורית להגדרת מקצועות הגנת הסייבר[2]. לאחר בחינה מקיפה של הנושא, הגישה הוועדה את עבודתה, אשר הובילה למסקנות הבאות:

1. קיימת **תכלית ראויה** לאסדרת מקצועות הגנת הסייבר – התמודדות עם האיומים על הביטחון, על בטיחות הציבור ועל כלכלת המדינה.
2. יש מקום **להגדרת מקצועות פרטנית** וקידום מערכי הכשרה והסמכה במקצועות הליבה.
3. יש מקום **שהמדינה תפעל** כדי להבטיח כי המומחיות הנדרשת תעמוד לרשות המשק.

יצוין כי הוועדה ביצעה אבחנה בין **מקצועות** לבין **תפקידים** בתחום הגנת הסייבר (ראו פירוט בנספח ב'). אבחנה זו מתבטאת בכך שבעל מקצוע הינו אדם המוסמך לתחום ידע ומיומנות ייחודית וזהו תחום התמחותו העיקרי. לעומת זאת, בעל תפקיד הינו מינוי ארגוני או, לחילופין, שילוב של תחומי התמחות המוכרים כמקצוע. בשלב זה, תבוצע אסדרה של המקצועות.

בהמשך לעבודת הוועדה, קידם מטה הסייבר הלאומי שורת פעילויות נוספות ומשלימות שכללו, בין היתר, לימוד אופן אסדרת מקצועות בתחומים שונים בישראל וכן לימוד אודות אסדרת מקצועות הגנת הסייבר בעולם. במקביל, התקיים תהליך רציף ומתמשך של היוועצות עם מספר רב של אנשי מקצוע מארגונים, מחברות שירותים וממוסדות הכשרה בתחום הגנת הסייבר.

מטרת מסמך זה הינה להציג את המקצועות שיוסדרו, את הידע הנדרש עבורם, את המנגנון לאסדרת המקצועות ב"מצב היציב"[3] (Steady State) ואת מתווה האסדרה.

המסמך יתוקף באופן עיתי ויעודכן במידת הצורך על ידי מטה הסייבר הלאומי.

---

[1] החלטות 2443 בנושא "אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" ו-2444 בנושא "קידום ההיערכות הלאומית להגנת הסייבר".

[2] בראש הוועדה עמד האלוף (מיל') עמי שפרן (לשעבר ר' אגף התקשוב בצה"ל) וחברי הוועדה היו (ע"פ סדר א"ב): עו"ד אייל ברנע (הלשכה המשפטית, משרד ראש הממשלה), אילן כרמית (מכון התקנים הישראלי), אמיל מלול (משרד הכלכלה), עו"ד דבורה האוסן-כוריאל (חוקרת דיני סייבר ישראליים ובינלאומיים), דניאל רוזן (יו"ר ודירקטור במספר חברות טכנולוגיות), זיו סולומון (מטה הסייבר הלאומי), עו"ד מיכאל אטלן (היועץ המשפטי, משרד הכלכלה), עו"ד צביה גרוס (לשעבר היועצת המשפטית למערכת הביטחון) ותא"ל (מיל') שלמה וקס (מנכ"ל איגוד תעשיות האלקטרוניקה והתוכנה).

[3] "המצב היציב" הינו המצב העתידי המתוכנן שבו כל מרכיבי מנגנון האסדרה יפעלו. לעניין מסמך זה הוא יוגדר החל משנת 2021.

תוכן העניינים

תמצית

הגדרת המקצועות בתחום הגנת הסייבר

1. במסגרת המאמץ לקידום ההגנה הלאומית במרחב הסייבר, יוסדרו מקצועות הגנת הסייבר בישראל.
2. המקצועות שיוסדרו הם:

א. **מיישם הגנת סייבר** – אדם בעל ידע תיאורטי בסיסי ויכולת יישומית (Hands-on) האחראי על יישום הגנת הסייבר בארגון.

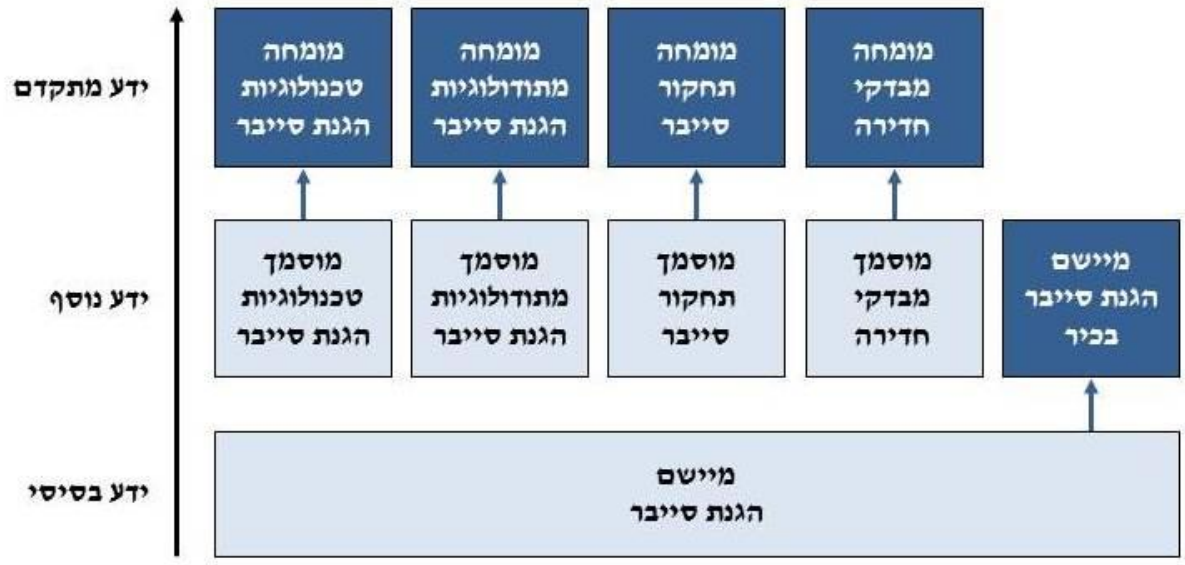
ב. **מוסמך מבדקי חדירה** – אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי איתור חולשות במערכי הגנת סייבר ובדיקת חדירות (Penetration Testing).

ג. **מוסמך תחקור סייבר** – אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי תחקור אירועים (Forensics).

ד. **מוסמך מתודולוגיות הגנת סייבר** – אדם בעל ידע תיאורטי מקיף ומעמיק במכלול נושאי מתודולוגיות הגנת הסייבר.

ה. **מוסמך טכנולוגיות הגנת סייבר** – אדם בעל ידע תיאורטי מקיף ומעמיק במכלול נושאי טכנולוגיות הגנת הסייבר.

3. לכל מקצוע יוגדרו שתי רמות הסמכה – רמה בסיסית ורמה מתקדמת המאפשרת הסמכה כמומחה (או כ"מיישם הגנת סייבר בכיר" למקצוע "מיישם הגנת סייבר").
4. להלן תרשים המתאר את המקצועות השונים ואת רמת הידע המקצועי הנדרש מהם:



<u>קווים מנחים לאסדרה</u>

5. מנגנון האסדרה ב"מצב היציב" יכלול את הרכיבים הבאים:
   א. חובת עמידה בתנאי סף הכוללים גיל (בגיר), אזרחות ישראלית והיעדר עבר פלילי.
   ב. חובת עמידה בבחינות תיאורטיות ומעשיות לבדיקת הידע הנדרש בכל אחד מהמקצועות.
   ג. קיום בחינות לרמת מומחיות גבוהה יותר בכל אחד מהמקצועות לכל המעוניין, לאחר קבלת ההסמכה הבסיסית וצבירת ותק מקצועי של 4 שנים.
   ד. חובת עמידה עתית, אחת ל-3 שנים, בדרישות לשמירת כשירות מקצועית בכל אחד מהמקצועות.
   ה. הקמת מרשם של בעלי המקצועות שהוסמכו.
6. יונפקו תעודות הסמכה לכל בעל מקצוע שיעמוד בדרישות.
7. מתווה האסדרה כולל את שלבי מימוש המנגנון, לרבות התייחסות נפרדת להסמכות "דור המדבר"[4].
8. בעלי המקצוע ישתלבו בארגונים שונים במגוון מגזרי המשק וענפיו (כגון משרדי ממשלה, גופים עסקיים, חברות ייעוץ ושירותים).
9. יצוין כי העיסוק במקצועות הגנת הסייבר לא יוגבל באופן גורף והחלת האסדרה במקומות שמוגדרים או שיוגדרו לכך, תבוצע באופן הדרגתי.
10. למימוש האסדרה תוקם ברשות הלאומית להגנת הסייבר יחידה שייעודה אסדרת שוק שירותי הגנת הסייבר (אנשי מקצוע, שירותים ומוצרים), אשר תהווה סמכות מקצועית בתחומי אחריותה.
11. בהיבטי אסדרת אנשי המקצוע, היחידה תפעל בהתאם למדיניות מטה הסייבר הלאומי ותטפל בכלל ההיבטים הנדרשים למימוש האסדרה, ביניהם:
    א. תיקוף המקצועות ותחומי הידע הנדרשים לכל מקצוע
    ב. הכנת המבחנים לבדיקת הידע הנדרש לכל מקצוע
    ג. הגדרת התנאים והתבחינים לפטור חלקי מבחינות
    ד. הגדרת התהליכים לקבלה, להקפאה ולחידוש התעודה
    ה. הגדרת רמות ההסמכה לכל מקצוע
    ו. הגדרת התבחינים לעמידה בכשירות מקצועית
    ז. קידום חקיקה ראשית/משנית בנושא

[4] "דור המדבר" – אנשים העוסקים בתחום הגנת הסייבר בהיקף ניכר במשך 4 שנים לפחות (שנתיים ל"מיישם הגנת סייבר"), אשר יוכרו ככאלה על ידי הרשות הלאומית להגנת הסייבר.

פרק א': מבוא

1. היווצרות מרחב הסייבר הינה תולדה של ההתפתחות הטכנולוגית המואצת של העשורים האחרונים ותרומתו להתפתחות האנושית אינה ניתנת לערעור. מרחב זה מאפשר זרימה חופשית של ידע, הון ושירותים, עם חסמי כניסה נמוכים מאוד, ובכך הוא משפר את הרווחה החברתית ומעודד חדשנות. התבססותן של פעילויות מסורתיות רבות על מרחב הסייבר הולכת ועולה (דוגמת תשלומים דיגיטליים או שליטה ובקרה בתהליכי ייצור ותפעול), במקביל לפיתוח מתמשך של פעילויות מרכזיות חדשות באמצעותו (דוגמת מסחר מקוון ורשתות חברתיות). כתוצאה מכך ונוכח השפעתו הנרחבת על פעילותם של פרטים, ארגונים ומדינות, הופך מרחב הסייבר לבעל חשיבות אסטרטגית.

2. לצד זאת, מרחב הסייבר טומן בחובו משרעת איומים ייחודית בהיקפה, בהיותו תווך פוטנציאלי לפעילויות עוינות, מוכרות וחדשות כאחד, אשר עשויות להביא הן לפגיעה בתוך המרחב (למשל במידע או בתפקוד) והן לפגיעה היוצאת ממנו (למשל פיזית או תודעתית). בין היתר, איומים אלה כוללים: השחתת אתרים וחסימת שירותים, סחיטה והטרדה של פרטים וארגונים, פגיעה בפרטיות ע"י גניבת מידע אישי, ריגול מסחרי, שיבוש או השבתה של תהליכים ושירותים חיוניים לאזרחים ולמשק, גניבת סודות מדינה, פגיעה בתשתיות ובמערכות חיוניות למשק ולגופי הביטחון, פגיעה בחיי אדם ועוד. מגוון גורמים עוינים עשויים לממש איומים אלה – יחידים, אסופות האקרים, קבוצות פשיעה, ארגוני טרור, תאגידים ומדינות – וזאת מתוך שורה ארוכה של מניעים – אישיים, אידיאולוגיים, כלכליים, ביטחוניים ואחרים.

3. בשנים האחרונות ניכרת עלייה משמעותית בשכיחותם של אירועי סייבר ובחומרתם, בעולם כולו ובישראל בפרט. מגמה זו מיוחסת במידה רבה למאפיינים הייחודיים של המרחב אשר מקלים על הפעילות העוינת בתוכו: קבועי הזמן הקצרים המאפיינים את השתנות המרחב ואת הנעשה בו, חוסר הרלוונטיות של המרחק הפיזי לפעילות במרחב וכתוצאה מכך חשיפה לאיומים מכל העולם בסבירות דומה, האנונימיות היחסית המתאפשרת בו, היעדר כוח ביטחוני החוצץ בין התוקף לנתקף, מחירי הכניסה הנמוכים לפיתוח יכולות פעולה במרחב ועליית "שטח הפנים" לתקיפה כתוצאה מהתרחבותו המהירה. הסיכון האמור במגמה מדרדרת זו לפגיעה בביטחון האישי, בפעילות המשק ובביטחון המדינה, חייב התייחסות ברמה הלאומית.

4. בחזית ההתמודדות עם איומי סייבר ניצבים ארגונים ממשלתיים ופרטיים[5], העושים שימוש במרחב הסייבר ואף תלויים בו לקיום פעילותם השגרתית. לרוב מופקדים על התמודדות זו בפועל אנשי טכנולוגיית המידע בארגונים, בעלי הכשרות בדיסציפלינות מקצועיות שונות.

5. על רקע מציאות חדשה זו של "חזית אזרחית רחבה", התקבלה החלטת ממשלה מס' 2443 מיום 15/02/2015 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", שתכליתה העלאה שיטתית ורציפה של רמת הגנת הסייבר בישראל באמצעות מימוש סטנדרטים מקצועיים בארגונים, וכן אסדרת שוק שירותי הגנת הסייבר (אנשי מקצוע, שירותים ומוצרים) במגוון כלים.

[5] לעניין מרכזיותם של הארגונים כמושאי ההגנה העיקריים באסטרטגיה לאומית להגנת הסייבר, ראו גם:
A Three Layer Framework for a Comprehensive National Cyber Security Strategy, E. Matania, L. Yoffe, M. Mashkautsan, Forthcoming in *Georgetown Journal of International Affairs: International Engagement on Cyber VI* (Spring 2016).

6. נדבך מרכזי באסדרה הלאומית בהגנת הסייבר הוא אסדרת אנשי המקצוע העוסקים בתחום זה, מתוך הנחה כי רמתם המקצועית מהווה מרכיב משמעותי ביותר בבניית החוסן של כלל המשק בסייבר, ולכן נודעת לה חשיבות מיוחדת.

7. בדומה לאסדרה ממשלתית בתחומים אחרים, אסדרת מקצועות נועדה להבטיח את האינטרס הציבורי במצב עניינים שבו קיים בכך כשל או פער משמעותי, דוגמת הצורך להגן על הציבור מפני בעלי מקצוע לא מיומנים, אשר עשויים להסב נזק כלכלי, פיזי או אחר, ולוודא רמת בסיס מקצועית מספקת של בעלי מקצוע שהשלכות פעילותם עשויות לחרוג מעבר למעסיקיהם וללקוחותיהם.

8. יחד עם זאת, חשוב לזכור כי חופש העיסוק הינו זכות יסוד חוקתית במדינת ישראל, ולכן אם וככל שמגבילים אותו, יש לעשות זאת באופן מידתי ובמשנה זהירות. בנוסף, יש להימנע מפגיעה לא הכרחית בפעילות החופשית במשק.

<u>מאפייני התחום והעיסוק בהגנת הסייבר</u>

9. התחום המקצועי של העיסוק בהגנת הסייבר הינו מורכב ומאתגר:

א. הוא מחייב ידע והבנה במגוון דיסציפלינות מקצועיות.

ב. הוא כולל מספר רב של התמחויות ספציפיות (כגון ניהול, ארכיטקטורה של מערכות מחשוב, הנדסה של מערכות מחשוב, יישום, בדיקות, חקירה, ניטור אירועים ועוד[6]). המומחים הספציפיים בתחום הגנת הסייבר מסתייעים בבעלי מקצוע בתחומי מחשוב מגוונים (כגון חומרה, תקשורת, מערכות הפעלה, בסיסי נתונים ויישומים ספציפיים). כמו כן, הוא מחייב הבנה באסדרה ותקינה.

ג. הוא חדש יחסית ונמצא בשלבי התפתחות מהירים.

ד. בנוסף ללימודים אקדמיים, פועלת בישראל מערכת הכשרה ענפה בתחום זה ברמות שונות. בפרט, צה"ל ומערכת הביטחון מקיימים מערך הכשרה נרחב בהתאמה לצרכיהם הייחודיים.

ה. כמו במקצועות רבים אחרים, ההתמחות הספציפית, הוותק והניסיון מהווים מרכיבים רבי ערך בבניית יכולת ההתמודדות.

<u>אסדרת מקצועות הגנת הסייבר בעולם</u>

10. בעולם מתפתחות מספר גישות לטיפול באסדרת מקצועות הגנת הסייבר, וכמה מדינות כבר החלו לנקוט בצעדים משמעותיים. ניתן להבחין במספר מגמות בהקשר זה:

א. **קביעת ידע וכישורים** – ישנן מדינות, ביניהן ארה"ב, סינגפור, אוסטרליה ובריטניה, אשר משקיעות מאמצים ניכרים בקביעת מפרטים אחידים לאנשי המקצוע בתחום הגנת הסייבר

[6] בעולם מקובלים מודלים שונים להגדרת תחומי העיסוק. לדוגמה, ה-NIST בארה"ב מבצע את האבחנה הבאה:
1. **פיתוח**: פיתוח, עיצוב ובניית מערכות טכנולוגיית מידע מאובטחות.
2. **פיקוח ותחזוקה**: מתן תמיכה, ניהול ותחזוקת המערכות כדי להבטיח ביצועי מערכות יעילים.
3. **אבטחה**: זיהוי, ניתוח ודיווח אודות סיכוני סייבר קיימים ברשת כדי שיהיה ניתן להגן על המערכות.
4. **חקירה**: תחקור פשעי טכנולוגיית מידע או פשעים המתבצעים באמצעות חדירה למערכות מידע.
5. **ניתוח נתונים**: ניתוח המידע המתקבל ממערכות אבטחת המידע וסיווגו בהתאם לצרכי מודיעין.
6. **תמיכה והדרכה**: הדרכה, פיתוח והכשרה של מנהלים ועובדים בארגון בנושא אבטחת המערכות.

ואבטחת המידע. הגורמים הרלוונטיים במדינות אלה מפרסמים כבר היום את המלצותיהם במטרה להניע את השוק לפעולה.

ב. **הסמכה** – קיימת מגמה, בעיקר במדינות בעלות אסטרטגיית סייבר מפותחת, להכרה בתעודות מקצועיות ואקדמיות ספציפיות כמעידות על כישורים ויכולות נדרשות. במדינות כמו בריטניה כבר מתקיימים מנגנוני הסמכה ציבוריים לאנשי מקצוע שונים, אשר מעניקים תעודות ואישורים בחסות ממשלתית. אף שאין מימוש של מנגנון רישוי גורף, מדובר בסימון מהותי של ההיצע המאפשר לרגולטורים ולארגונים גישה למאגר של בעלי מקצוע עם הסמכה ממשלתית.

ג. **החלה בממשלה** – מגמה בולטת נוספת היא אימוץ סטנדרטיזציה של אנשי המקצוע בממשלה. בעוד מדינות נוהגות משנה זהירות בהשפעה על המשק בכלל ועל השוק הפרטי בפרט, ממשלות (דוגמת בריטניה, גרמניה וסינגפור) מאמצות כבר היום סטנדרטים אחידים כלפי בעלי המקצוע.

11. להלן מספר דוגמאות:

א. **אוסטרליה** – קיימות תכניות התעדה, התמחות וליווי לאנשי מקצוע במגזר הציבורי. הממשלה גיבשה תכנית כוללת להכשרת כוח אדם במגזר הציבורי על בסיס המודל של ארגון ה-SFIA[7].

ב. **ארה"ב** – קיימת יוזמה פדראלית לקבוע מקצועות ליבה ומסלולי הכשרה. הממשל עורך פרויקט רוחב כדי לעדכן את ה-National Cybersecurity Workforce Framework, שיעסוק גם בטקסונומיה של המקצועות. עובדי הגנת סייבר בממשל הפדראלי נדרשים לעמוד בהכשרות ספציפיות.

ג. **בריטניה** – קיימת תכנית לאומית להתעדה ומעורבות ממשלתית בהסמכות מסוגים שונים. במסגרת התכנית, CESG Certification for IA Professionals, הוסמכו מאות אנשי מקצוע במגזר הציבורי. הוגדרו שבעה מקצועות כאשר ההסמכה מתבצעת על ידי שלוש חברות חיצוניות, והסטנדרט מחייב עבור הממשלה.

ד. **גרמניה** – קיימים מנגנוני הסמכה לכוח אדם בסייבר המשמשים סטנדרט מחייב עבור הממשלה. ה-BSI נדרש לספק מומחיות כזו לממשלה על פי חוק.

ה. **סינגפור** – קיימת תכנית לאומית להתעדה בהסמכות מסוגים שונים במסגרת ה-NICF (National Infocomm Competency Framework), אשר מחייב את הממשלה. הממשלה תומכת במסלולי קריירה ומפעילה תכניות תמרוץ לעובדים ולארגונים לרכישת ידע ומיומנות בנושא.

<u>פעילות הוועדה הציבורית להגדרת מקצועות הגנת הסייבר</u>

12. הוועדה, שמונתה על ידי מטה הסייבר הלאומי (להלן: המטה), הייתה הגורם הציבורי הראשון לעסוק בבחינת הנושא ברמה הלאומית. הוועדה דנה, בין היתר, בעוצמת ואופי שיטת האסדרה. במסגרת עבודת הוועדה נבחנו ארבע החלופות הבאות, הנבדלות זו מזו במידת ההתערבות בחופש העיסוק:

א. הימנעות מהתערבות כלשהי

ב. קביעה או המלצה וולונטרית של הידע והכישורים הנדרשים

ג. הנהגת מרשם לאומי והגנה על תארים

ד. הנהגה בחוק של חובת רישוי לשם עיסוק במקצועות המוגדרים

[7] SFIA – Skills Framework for the Information Age

13. **המלצת הוועדה, לאחר הערכת הסיכונים למול הפגיעה בחופש העיסוק ובפעילות החופשית במשק, הייתה למקד את האסדרה במרחב שבין חלופות ב' ו-ג'** (קביעה או המלצה וולונטרית של הידע והכישורים הנדרשים **או** הנהגת מרשם לאומי והגנה על תארים). **חלופת אי ההתערבות נמצאה כלא מספקת נוכח הסיכונים. חלופת חובת הרישוי הגורפת נדחתה אף היא, שכן היא נמצאה כלא מידתית בעת הזאת בהקשר לנסיבות השוק ולעולם התוכן המדובר**.

<u>עקרונות ושיטת האסדרה</u>

14. בהמשך לעבודת הוועדה, ביצע המטה בחינה שהתמקדה בגיבוש חלופה במרחב האפשרויות האמור, אשר תאזן באופן מיטבי בין הבטחת הרמה המקצועית, מזעור הפגיעה בחופש העיסוק והפחתת הנטל הרגולטורי והפגיעה בתחרות למינימום האפשרי.

15. להלן עקרונות האסדרה שסוכמו (ראו פירוט בפרק ג'):

א. הרשות הלאומית להגנת הסייבר (להלן: הרשות) תעניק תעודות אודות היותם של פרטים כשירים לעסוק במקצועות הגנת הסייבר כפי שהוגדרו. העיסוק במקצועות הגנת הסייבר לא יוגבל באופן גורף והאישורים האמורים לא יהוו תנאי לעיסוק במקצוע לכשעצמם. הנחת המטה, כחלק מתפיסת האסדרה הלאומית, היא שרגולטורים יעשו שימוש באישורים אלה בגזרתם ועל פי סמכותם החוקית בנסיבות המתאימות לכך, על מנת לחייב גופים מסוימים במשק להעסיק בעלי מקצוע מוסמכים. במקביל, האישורים שתנפיק הרשות יהוו סטנדרט מחייב בממשלה.

ב. מתן ההסמכות יתבסס על עמידה בתנאי סף (גיל, אזרחות, היעדר עבר פלילי) ועל עמידה במבחנים תיאורטיים ומעשיים כפי שתקבע הרשות.

ג. בעלי ההסמכות יידרשו לעמוד בבחינות כשירות מקצועית אחת ל-3 שנים.

ד. יתנהל מרשם של בעלי המקצוע המוסמכים, שנתוניו יהיו שקופים ונגישים לציבור, כך שניתן יהיה לבדוק האם אדם מסוים הוא בעל מקצוע מוסמך. גורמים שאינם רשומים במרשם יהיו רשאים לעסוק באותם עיסוקים ובלבד שלא ישתמשו בשמות המקצועות המופיעים במרשם.

ה. האסדרה לא תעסוק בפיקוח על מוסדות לימוד והכשרה. הנחת המטה היא שנושאי הבחינות שתפרסם הרשות יהוו "מצפן" עבור מוסדות הלימוד וההכשרה המבקשים לשלב את בוגריהם בשוק העבודה.

פרק ב': הגדרת המקצועות בתחום הגנת הסייבר

16. המקצועות שיוסדרו בתחום הגנת הסייבר הם (ראו פירוט בנספח א'):

א. **מיישם הגנת סייבר (Cyber Security Practitioner)**

אדם בעל ידע תיאורטי בסיסי ויכולת יישומית (Hands-on) האחראי על יישום הגנת הסייבר בארגון, בהיבטי:

1) התקנה, ניהול, תפעול ותחזוקה של מוצרי הגנת הסייבר (כגון אנטי-וירוס, Firewall, IPS, DLP, בקרת גישה, הגנת התקנים ניידים).
2) יישום תהליכי אבטחה שגרתיים (כגון ניהול חשבונות והרשאות משתמשים, ניהול סיסמאות, ניהול גישת משתמשים למחשבים ולמידע, ניהול ציוד קצה והתקנים ניידים בהיבטי אבטחה).
3) זיהוי וטיפול ראשוני / בסיסי באירועי אבטחה בהסתמך על הכרת סוגי איומים ותקיפות ואופן הטיפול בתקיפות שהתגלו.

כל זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

הערה: כל אחד מבעלי המקצועות הבאים יידרש לבסיס ידע מקצועי של "מיישם הגנת סייבר" בנוסף לידע מקצועי בהתאם לתחום הסמכתו.

ב. **מוסמך מבדקי חדירה (Cyber Penetration Testing Specialist)**

אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי איתור חולשות במערכי הגנת סייבר ובדיקות חדירות (Penetration Testing).

ג. **מוסמך תחקור סייבר (Cyber Forensics Specialist)**

אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי תחקור אירועים (Forensics).

ד. **מוסמך מתודולוגיות הגנת סייבר (Cyber Security Methodology Specialist)**

אדם בעל השכלה אקדמית וידע תיאורטי מקיף ומעמיק, האחראי על:

1) גיבוש, אפיון ומימוש תפיסות, שיטות ומתודולוגיות להגנת הסייבר בארגון.
2) הטמעת היבטי אסדרה ותקינה ישראלית ובינלאומית והיבטי הגנת הפרטיות.
3) ניהול סיכונים בהגנת הסייבר.
4) ליווי מתודולוגי של תהליכים ארגוניים בתחום הגנת הסייבר (כגון ליווי הקמת מערכת הגנת סייבר ארגונית, ליווי פרויקטים בהיבטי הגנת סייבר, אבטחת שרשרת האספקה, המשכיות עסקית, התאוששות מאסון וניתוח השפעות עסקיות).

כל זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

ה. **<u>מוסמך טכנולוגיות הגנת הסייבר (Cyber Security Technology Specialist)</u>**

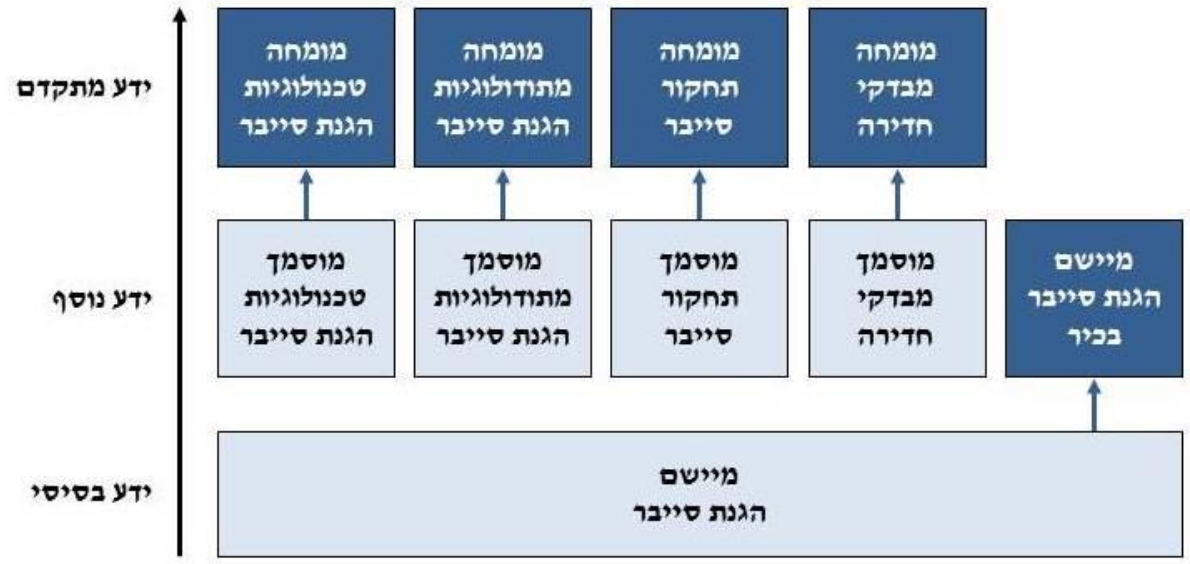
אדם בעל השכלה אקדמית וידע תיאורטי מקיף ומעמיק, האחראי על:

1) תכנון מענה טכנולוגי להגנת הסייבר בארגון, תוך שילוב טכנולוגיות ושיטות אבטחה.
2) התאמת מוצרי הגנה ושילובם בתשתיות המחשוב לרבות מערכי אחסון ושיטות גיבוי.
3) ליווי הטיפול באירועי סייבר בהיבט הטכנולוגי.

כל זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

17. לכל מקצוע יוגדרו שתי רמות הסמכה – רמה בסיסית ורמה מתקדמת המאפשרת הסמכה כמומחה (או כ"מיישם הגנת סייבר בכיר" למקצוע "מיישם הגנת סייבר").

18. להלן תרשים המתאר את המקצועות השונים ואת רמת הידע המקצועי הנדרש מהם:



תרשים 1 – המקצועות השונים בתחום הגנת הסייבר ורמת הידע המקצועי הנדרש מהם

פרק ג': מנגנון האסדרה ב"מצב היציב" (Steady State)

19. בהחלטת ממשלה 2443 נקבע כי במסגרת הרשות תוקם יחידה שייעודה אסדרת שוק שירותי הגנת הסייבר (אנשי מקצוע, שירותים ומוצרים), אשר תהווה סמכות מקצועית בתחומי אחריותה.

20. תפקיד היחידה בתחום אסדרת אנשי המקצוע יהיה לקדם את עמידתם בסטנדרטים מקצועיים. בתוך כך, היחידה תתקף את רשימת המקצועות המוסדרים לכל הפחות אחת לשלוש שנים ואת הידע המקצועי הנדרש במקצועות השונים אחת לשנה, על מנת לוודא עדכניות ורלוונטיות.

21. להלן עיקרי שיטת אסדרת המקצועות בתחום הגנת הסייבר:

א. במקצועות המחייבים תואר אקדמי (מומחה מתודולוגיות הגנת סייבר ומומחה טכנולוגיות הגנת סייבר), התארים יהיו בתחומים הבאים (כתחום מקצוע עיקרי / משני / התמחות / שילוב בין תארים): מדעי המחשב / מערכות מידע / הנדסת תוכנה / הנדסת מחשבים / הנדסת אלקטרוניקה / הנדסת תקשורת / הנדסת תעשיה וניהול / מתמטיקה או תואר אחר שיוגדר על ידי הרשות.
<u>הערה</u>: תואר אקדמי שונה ובנוסף הכשרות / הסמכות מקצועיות בהגנת הסייבר בהיקף משמעותי (400 שעות במצטבר) שיוכרו על ידי הרשות, יהוו תחליף לתואר אקדמי בתחומים שפורטו.

ב. הסמכת בעלי המקצוע תהיה מורכבת משלושה רכיבים:

1) עמידה בתנאי סף לכל המקצועות – בגיר, בעל אזרחות ישראלית והיעדר עבר פלילי.

2) עמידה בהצלחה בבחינות תיאורטיות ומעשיות (שיבוצעו, לדוגמה, באמצעות סימולטורים) לכל המקצועות, המוכיחות ידע מקצועי נדרש ויכולת מעשית בהתאם לתחומים שהוגדרו (ראו פירוט בנספח א'). הבחינות יתקיימו, לכל הפחות, בשני מועדים שונים בשנה.
לכל המקצועות תוגדר רמה בסיסית (Entry Level) שאליה יוסמך כל מי שיעמוד בהצלחה בבחינות. בנוסף, תהיה אפשרות להסמכה לרמת מומחיות גבוהה יותר (Advanced Level), כתלות בעמידה בבחינות נוספות ובצבירת ותק של ארבע שנים במשרה מלאה לאחר סיום ההסמכה ברמה הבסיסית.

3) עמידה בכשירות מקצועית – בעלי ההסמכות יידרשו לעמוד בבחינות כשירות מקצועית אחת ל-3 שנים, כדי לוודא את בקיאותם בעיקרי השינויים והמגמות העדכניים למקצועות השונים.

ג. מרשם והנפקת תעודות לבעלי המקצוע:

1) יתנהל מרשם של בעלי המקצוע המוסמכים, שיהיה שקוף ונגיש לציבור. הציבור יהיה רשאי להפנות שאילתות פרטניות אודות נתוני המרשם, כך שניתן יהיה לבדוק האם אדם מסוים הוא בעל מקצוע מוסמך. גורמים שאינם רשומים במרשם, יהיו רשאים לעסוק באותם עיסוקים ובלבד שלא ישתמשו בשמות המקצועות המופיעים במרשם.

2) יונפקו תעודות הסמכה לכל בעל מקצוע שיעמוד בדרישות. התעודה תהיה בתוקף לשלוש שנים, בהלימה לתדירות הנדרשת לשמירת הכשירות המקצועית.

3) גורם שלא יעמוד בדרישות הכשירות המקצועית או שחל שינוי לרעה בדרישות הבסיס (לרבות סוגיית העבר הפלילי), ייבחן מחדש חידוש תעודתו.

פרק ד': מתווה האסדרה

22. תהליך מימוש האסדרה עד להגעה ל"מצב היציב", ייפרס עד שנת 2021 (כמפורט בתרשים 2 להלן).

23. עמידה בבחינות מקצועיות

א. כאמור, יוגדרו שתי רמות הסמכה:

1) רמה בסיסית (Entry Level) – שאליה יוסמכו כל מי שיעמדו בהצלחה בבחינה המקצועית.

2) רמה מתקדמת (Advanced Level) – שאליה יוסמכו בעלי המקצועות השונים, כתלות בעמידתם בבחינות מקצועיות נוספות ובצבירת ותק של ארבע שנים במשרה מלאה לאחר סיום ההסמכה ברמה הבסיסית.

ב. להלן פירוט שמות המקצועות בשתי הרמות:

רמה בסיסית	רמה מתקדמת
מיישם הגנת סייבר Cyber Security Practitioner	מיישם הגנת סייבר בכיר Senior Cyber Security Practitioner
מוסמך מבדקי חדירה Cyber Penetration Testing Specialist	מומחה מבדקי חדירה Cyber Penetration Testing Expert
מוסמך תחקור סייבר Cyber Forensics Specialist	מומחה תחקור סייבר Cyber Forensics Expert
מוסמך מתודולוגיות הגנת סייבר Cyber Security Methodology Specialist	מומחה מתודולוגיות הגנת סייבר Cyber Security Methodology Expert
מוסמך טכנולוגיות הגנת הסייבר Cyber Security Technology Specialist	מומחה טכנולוגיות הגנת הסייבר Cyber Security Technology Expert

ג. קיום בחינות לכלל המקצועות יחל בשנת 2017.

ד. מימוש תהליך הבחינות לרמה מתקדמת יחל בשנת 2021 (ל"דור המדבר" – החל משנת 2017).

בתוך כך, יוגדרו התנאים והתבחינים לקבלת פטור חלקי מהבחינות, בדגש על השכלה / הכשרה / הסמכה קודמת (מטעם ארגונים דוגמת ISC^2 ו-ISACA).

24. עמידה בכשירות מקצועית

כאמור, לכלל המקצועות יתקיים תהליך לשמירת כשירות מקצועית בתדירות של אחת לשלוש שנים. על כן, תהליך שמירת הכשירות המקצועית לכל המקצועות יחל בשנת 2020.

בתוך כך, יוגדרו התנאים והתבחינים לעמידה בכשירות המקצועית, שתבטיח ידע עדכני ויכולת מעשית גבוהה במקצועות המחייבים זאת. מבחני הכשירות המקצועית יכילו את עיקרי השינויים והמגמות העדכניים לתחום ההתמחות.

25. מרשם והנפקת התעודות לבעלי המקצוע

א. המרשם יוקם בשנת 2017 ויכלול את כל אנשי המקצוע שהוסמכו החל ממועד הבחינות הראשון.

ב. יונפקו תעודות הסמכה לכל בעל מקצוע שיעמוד בדרישות המקצועיות.
בתוך כך, יוגדרו התהליכים לקבלה, להקפאה ולחידוש התעודה.

26. הסמכת "דור המדבר"

"דור המדבר", כאמור, מתייחס לאנשים העוסקים בתחום הגנת הסייבר בהיקף ניכר במשך 4 שנים לפחות (שנתיים ל"מיישם הגנת סייבר"), אשר יוכרו ככאלה על ידי הרשות. המשתייכים לאוכלוסייה זו ומעוניינים להשתלב בתהליך ההסמכה, יוכלו לבחור באחת משתי אפשרויות:

א. ניצול "חלון הזדמנות" של שנה, שבה יוכלו לקבל הסמכה למקצועות השונים (כולל לרמה מתקדמת), באמצעות מעבר בחינות המותאמות לאוכלוסייה זו.

ב. קבלת תעודות זמניות למשך שלוש שנים. לאחר פרק זמן זה יפוג תוקף התעודה הזמנית והמעוניינים בהסמכה יידרשו לבצע תהליך הסמכה מלא.

27. הדרישה מהמשק

תהליך החלת היישום במשק (עבודה בפועל של בעלי המקצוע המוסמכים במגזרי המשק והארגונים השונים) יתבצע באופן מדורג בהתאם לחשיבות ודחיפות, לסוג המגזרים והארגונים, לקיום תשתית משפטית מתאימה וכדומה. זאת תוך איזון הולם בין המרכיבים, האילוצים והסיכונים הרלוונטיים:

א. **במשרדי הממשלה** – העוסקים בהגנת הסייבר יידרשו לעמוד בהסמכות הרלוונטיות כפי שנקבע בהחלטת ממשלה 2443:

1) כל עובד חדש שיועסק בתחום הגנת הסייבר בממשלה יעמוד בהסמכות הרלוונטיות.

2) בתוך חמש שנים, לכל היותר, כלל העובדים העוסקים בהגנת הסייבר בממשלה יעמדו בהסמכות הרלוונטיות.

ב. **במגזרי המשק האזרחי (בכלל המגזר או בגופים מסוימים בו)** – העוסקים בהגנת הסייבר יידרשו לעמוד בהסמכות הרלוונטיות על פי הכוונת הרגולטורים הרלוונטיים בהתאמה למדיניות הרשות. זאת, בהלימה להחלטת ממשלה 2443, אשר הטילה על הרגולטורים המגזריים להכווין ולהנחות את גופי המגזר בהגנת הסייבר, לרבות הגדרת המדיניות ודרישות האסדרה בהתאם למאפיינים של הגופים אשר ביחס אליהם מתבצעת הפעילות.

ג. **בגופים ייחודיים שיוגדרו על ידי הרשות כבעלי נזק פוטנציאלי משמעותי כתוצאה מפגיעה במערכות הממוחשבות שלהם**[8] – העוסקים בהגנת הסייבר יידרשו לעמוד בהסמכות הרלוונטיות על פי החלטת הרשות, ובמידת הצורך תוך היוועצות עם הרגולטורים המגזריים הרלוונטיים.

[8] גופים אלה יוגדרו בהתאם לתבחינים שיתייחסו, בין היתר, להיקף פעילות הגוף, תלות תהליכי הליבה שלו במחשב, התלות של גופים אחרים בו ועוד.

28. להלן תרשים המתאר את מתווה האסדרה:

הנושא	המרכיב במימוש	2016	2017	2018	2019	2020	2021 ואילך (ה"מצב היציב")
הסמכה	קיום בחינות לרמה בסיסית	שנת היערכות	←	←	←	←	←
	קיום בחינות לרמת מתקדמת						←
	תהליך שמירת כשירות						←
"דור המדבר"	אפשרות א': תהליך חד פעמי מקוצר (שנה) – כולל לרמה מתקדמת			←			
	אפשרות ב': תעודה זמנית ל-3 שנים (וביצוע תהליך הסמכה מלא לאחר מכן)		←	←	←		
מרשם	הקמת מרשם		←	←	←	←	←
דרישה מהמשק	במשרדי הממשלה: 1. כל עובד חדש בתחום הגנת הסייבר בממשלה יעמוד בהסמכות הרלוונטיות 2. בתוך חמש שנים, לכל היותר, כלל העובדים העוסקים בהגנת הסייבר בממשלה יעמדו בהסמכות הרלוונטיות		←	←	←	←	←
	במגזרי המשק האזרחי (על פי הכוונת הרגולטורים המגזריים הרלוונטיים בהתאמה למדיניות הרשות)		←	←	←	←	
	גופים ייחודיים בעלי פוטנציאל נזק משמעותי כתוצאה מהפגיעה במערכות הממוחשבת שלהם (על פי החלטת הרשות, ובמידת הצורך תוך היוועצות עם הרגולטורים המגזריים הרלוונטיים)		←	←	←	←	

תרשים 2 – מימוש המתווה לאסדרת מקצועות הגנת הסייבר

נספח א' – מקצועות הגנת הסייבר – מהות והידע המקצועי הנדרש

מיישם הגנת סייבר (Cyber Security Practitioner)

מהות המקצוע

אדם בעל ידע תיאורטי בסיסי ויכולת יישומית (Hands On) האחראי על יישום הגנת הסייבר בארגון, בהיבטי:

1. התקנה, ניהול, תפעול ותחזוקה של מוצרי הגנת הסייבר (כגון אנטי-וירוס, Firewall, IPS, DLP, בקרת גישה, הגנת התקנים ניידים).
2. יישום תהליכי אבטחה שגרתיים (כגון ניהול חשבונות והרשאות משתמשים, ניהול סיסמאות, ניהול גישת משתמשים למחשבים ולמידע, ניהול ציוד קצה והתקנים ניידים בהיבטי אבטחה).
3. זיהוי וטיפול ראשוני / בסיסי באירועי אבטחה בהסתמך על הכרת סוגי איומים ותקיפות ואופן הטיפול בתקיפות שהתגלו.

כל זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

ידע מקצועי נדרש

1. **מבוא להגנת סייבר**: מונחים, איומים, סוגי יריבים והמוטיבציות שלהם, סוגי תקיפות (לרבות תקיפת מחשב מרחוק / מתוך הארגון, חדירה פיזית למתחמי מחשב, Social Engineering ותקיפות משולבות), סוגי פגיעות במערכות / במידע (לרבות בהיבטי זמינות, אמינות, שלמות וסודיות), השלכות ומשמעויות הפגיעה (כלכליות, מוניטין, משמעויות מעבר לרמת הארגון), דרכי התמודדות ארגוניות (מינוי בעלי תפקידים, הגדרת מדיניות ונהלים, הגדרת נכסי מידע ומערכות חיוניות, ניהול סיכונים, אבטחה פיזית, המרכיב האנושי ומהימנות עובדים, מודעות, הטמעה בתרבות הארגונית, דיווחים ובקרות), גופים לאומיים העוסקים בתחום בישראל.
2. **ידע בסיסי בחוקים, החלטות ממשלה, תקינה ואסדרה בנושאי הגנת הסייבר, אבטחת מידע ופרטיות** הנהוגים בישראל.
3. **היכרות עם הסביבה הטכנולוגית**: מבנה המחשב (לרבות CPU, ALU, ROM, RAM, אמצעי אחסון, BIOS, UEFI), מודל 7 השכבות (OSI), תקשורת מחשבים (כולל Wireless), רכיבי תקשורת (לרבות Switch, Router), רשתות (WAN/LAN), פרוטוקולים (לרבות SYSLOG, RADIUS, DNS, HTTP, HTTPS, FTP, TCP/IP, UDP, SSL, SIP, RIP, ARP, SSH, ICMP, SNMP, SNTP, IPSEC), מערכות הפעלה (לרבות Windows, Linux), בסיסי נתונים, מערכות SCADA, Virtualization, Mobile, מחשוב ענן, Hosting, Big Data, יישומים נפוצים (כגון יישומי ERP, CRM, BILLING), שיטות גיבוי ושחזור.
4. **היכרות טובה עם טווח רחב של מוצרים ושיטות אבטחה (לרבות אופן היישום, שגרות תפעול, קונפיגורציה, עדכוני תוכנה וחומרה, דרכי התחזוקה ודרכי הניהול)**: אנטי-וירוס, Firewall, DMZ, Proxy, הקשחת שרתים ומערכות הפעלה, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), DLP (Data Leakage Prevention), SBC (Session Border Controller),

Anomaly Detection (User / Network Behavior), NAC (Network Access Control), סגמנטציה (כולל VLAN), Encryption, ניהול זהויות (IAM / IDM), הגנת התקנים ניידים, EPS (Endpoint Security), MDM (Mobile Device Management), MAM (Mobile Application Management), שירותי Mail Relay, SOC (Security Operations Center), SIEM (Security Information Event Management), שיטות בקרת גישה (סיסמאות, Tokens, Smart Cards, ביומטריה, Multi-Factor), אותנטיקציה של משתמשים ושל התקנים, Data/Content Filtering, Remote Access, VPN, Wireless Security, אבטחת מערכות בסביבת WEB (לרבותWeb Filtering ו-WAF), אבטחת מערכות SCADA, הגנת בסיסי נתונים ומערכי אחסון מרכזיים, הלבנת / השחרת קבצים, BCP, DRP, Honey Pots.

5. **היכרות עמוקה עם תהליכי האבטחה השגרתיים בארגון**: ניהול חשבונות והרשאות משתמשים (לרבות Administrator, Guest, Privilege User), ניהול סיסמאות, ניהול גישת משתמשים למחשבים ולמידע, ניהול גיבויים, Patch Management (לרבות למערכות הפעלה, לרכיבי תקשורת, ליישומים, למוצרי אבטחה), ניהול ציוד קצה והתקנים ניידים, קבלה ומעקב אחר מידע (המתקבל מלוגים, Events, ומקורות חוץ) וחקירתו, ניטור מערכות, חיפוש וזיהוי אנומליות.
6. **ידע בסיסי באופן הטיפול באירועי אבטחה**: הכרת סוגי תקיפות מוכרות (כגון DOS/DDOS, Spear Phishing) ואופן הטיפול בתקיפות שהתגלו (גישות וכלים).
7. **אתיקה מקצועית**.

מוסמך מבדקי חדירה (Cyber Penetration Testing Specialist)

מהות המקצוע

אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי איתור חולשות במערכי הגנת סייבר ובדיקת חדירות (Penetration Testing).

ידע מקצועי נדרש

בנוסף לבסיס הידע של מיישם הגנת סייבר, יחויב גם בידע מקצועי בנושאים הבאים:

1. **תקיפה**: תהליך התקיפה (כגון Kill Chain של Lockheed Martin), שיטות וכלים לתקיפה, שיטות וכלים לזיהוי תקיפות, שיטות תקיפה משולבות (לדוגמה טכנולוגי ואנושי), APT (Advanced Persistent Threat).
2. **הכרת חולשות**: חולשות אפליקטיביות (כולל OWASP Top 10 Vulnerabilities, בהקשר של Web applications), חולשות תשתיתיות.
3. **כלים לביצוע מבדקי חדירה**: הכרת כלים, הפעלת כלים, קריאת דו"חות המופקים מהכלים.
4. **סוגי בדיקות חדירה**: Black Box, White Box, Gray Box.
5. **בדיקת חדירה ברמה תשתיתית**: חדירה למערכות הפעלה (לרבות Windows, Linux), חדירה לציוד תקשורת ולבקרים, הכרה בסיסית של שפות רלוונטיות (לדוגמה Python, Perl).
6. **בדיקת חדירה ברמה אפליקטיבית**: חדירה לממשקי WEB, חדירה למערכות ייעודיות, Code Review (הכרה בסיסית), הכרה בסיסית של שפות רלוונטיות (כגון .NET, PHP, ASP), הכרה בסיסית של SQL.
7. **כתיבת דו"ח בדיקה מסכם**: אופן הכתיבה, פורמט, רמת הפירוט, המחשת הסיכון הארגוני, הערכת יכולת המימוש, המלצות לארגון על הפעולות הנדרשת לשיפור ההגנה והתעדוף לביצוען.

מוסמך תחקור סייבר (Cyber Forensics Specialist)

מהות המקצוע

אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי תחקור אירועים (Forensics).

ידע מקצועי נדרש

בנוסף לבסיס הידע של מיישם הגנת סייבר, יחויב גם בידע מקצועי בנושאים הבאים:

1. **שחזור מידע ונתונים**, לרבות מהרכיבים הבאים: שרתים, תחנות קצה, התקנים ניידים (כולל טלפונים סלולאריים), רכיבי זיכרון, התקני אחסון.
2. **פענוח אירועים**: שיטות וכלים לגילוי, זיהוי, פענוח ושחזור אירועים; ניתוח נתונים, הצלבת נתונים וקורלציה בין נתונים לשם הרכבת תמונה שלמה.
3. **Reverse Engineering** (הכרה בסיסית): לשם תחקור אחר מתווה התקיפה.
4. **שימור ראייתי**: איתור ושימור ממצאים וראיות דיגיטליות כך שיוכלו לשמש בידי גורמי אכיפה להוכחת ביצוע התקיפה, אופן ביצוע התקיפה ולפענוח זהות התוקף.
5. **חקירת זמן אמת לעומת חקירת אקס פוסט.**
6. **הכרת כלים**: כלי שכפול, כלי שחזור, כלי חיפוש, כלי ניטור, כלי פיצוח סיסמאות.
7. **היבט משפטי**: הכרת פסיקות ותקדימים בנושא, דיני ראיות.
8. **הכרת גופי חקירה רלוונטיים בישראל וסמכויותיהם**: משטרת ישראל, מצ"ח, רשות המיסים, רשות לניירות ערך, הרשות למשפט, טכנולוגיה ומידע.
9. **כתיבת דו"ח בדיקה מסכם**: אופן הכתיבה, פורמט, רמת הפירוט, המחשת אופן התרחשות האירוע, המלצות לארגון על הפעולות הנדרשות לשיפור ההגנה והתעדוף לביצוען.

מוסמך מתודולוגיות הגנת סייבר (Cyber Security Methodology Specialist)

מהות המקצוע

אדם בעל השכלה אקדמית[9] וידע תיאורטי מקיף ומעמיק, האחראי על:

1. גיבוש, אפיון ומימוש תפיסות, שיטות ומתודולוגיות להגנת הסייבר בארגון.
2. הטמעת היבטי אסדרה ותקינה ישראלית ובינלאומית והיבטי הגנת הפרטיות.
3. ניהול סיכונים בהגנת הסייבר.
4. ליווי מתודולוגי של תהליכים ארגוניים בתחום הגנת הסייבר (כגון ליווי הקמת מערכת הגנת סייבר ארגונית, ליווי פרויקטים בהיבטי הגנת סייבר, אבטחת שרשרת האספקה, המשכיות עסקית, התאוששות מאסון וניתוח השפעות עסקיות).

כל זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

ידע מקצועי נדרש

בנוסף לבסיס הידע של מיישם הגנת סייבר, יחויב גם בידע מקצועי בנושאים הבאים:

1. **הכרת חוקים והחלטות ממשלה**: לרבות חוק המחשבים, חוק הסדרת הביטחון בגופים ציבוריים, חוק הגנת הפרטיות, החלטות ממשלה רלבנטיות.
2. **תקינה ואסדרה**: ישראלית ובין-לאומית, בנושאי הגנת סייבר ואבטחת מידע, לרבות: סדרת 27000 ISO, PCI DSS, SOX, באזל, סדרת 800 של NIST, HIPAA, IEC 62443, Common Criteria, ISO 31000, הוראות המפקח על הבנקים, הוראות המפקח על הביטוח ושוק ההון.
3. **ארגונים בעולם העוסקים בתקינה ובהסמכות**: ISO, IEC, ANSI, NIST, IEEE, ITU, BSI, DIN,AFNOR, CEN, CENELEC, ENISA, ETSI, NERC, ISC^2, ISACA, SANS, ISA.
4. **תפיסות וגישות בהגנת סייבר**: מעגלי הגנה, Defense in depth, No single point of failure, Least privilege, Need to know, הלימה בין רמת הגנה לרמת סיווג (כולל אבחנה בין סיווג למידור), מימוש בקרות מפצות כמנגנון משלים.
5. **מתודולוגיות ומסגרות עבודה בתחום טכנולוגיות המידע**: ITIL, COBIT.
6. **מדיניות ונהלים**: מטרת המדיניות, בניית מדיניות, הקשר בין מדיניות לנהלים.
7. **GRC (Governance, Risk management and Compliance)**:
   א. **ממשל הגנת סייבר (Governance)** – ניהול הגנת סייבר ברמת הארגון, מבנים ארגוניים תומכים, מימוש מדיניות הגנת סייבר ארגונית, בעלי תפקידים, תקצוב, שליטה ובקרה ארגונית, הקצאת משאבים, מחויבות הנהלה ודירקטוריון.

[9] התארים יהיו בתחומים הבאים (כתחום מקצוע עיקרי / משני / התמחות / שילוב בין תארים): מדעי המחשב / מערכות מידע / הנדסת תוכנה / הנדסת מחשבים / הנדסת אלקטרוניקה / הנדסת תקשורת / הנדסת תעשיה וניהול / מתמטיקה או תואר אחר שיוגדר על ידי הרשות.
הערה: תואר אקדמי שונה ובנוסף הכשרות / הסמכות מקצועיות בהגנת סייבר בהיקף משמעותי (400 שעות במצטבר) שיוכרו על ידי הרשות, יהווה תחליף לתואר אקדמי בתחומים שפורטו.

ב. **ניהול סיכונים (Risk management)** – מתודולוגיות ניהול סיכונים (כגון מתודולוגיית COSO), סוגי סיכונים, זיהוי הסיכונים, ניתוח הסיכונים, השפעת הסיכונים על הארגון, דרכי התמודדות, סיכונים שיוריים.

ג. **תאימות (Compliance)** – תאימות לדרישות חוק, רגולציה, תקינה, חוזים, מדיניות ונהלים ארגוניים, דרישות פנים ארגוניות וחוץ ארגוניות (כגון דרישות לקוח).

8. **ביקורת (Audit) בתחום הגנת סייבר**: בקרות טכנולוגיות ומתודולוגיות נדרשות, וכן הכנת וליווי ארגונים למבדקי תאימות לתקינה.

9. **ליווי הקמת מערכת הגנת סייבר ארגונית**: הגדרת היעדים, הגדרת נכסי המידע / המערכות החיוניות, זיהוי וניהול הסיכונים, הגדרת תהליכי טיפול ומניעה, הגדרת ובחירת הבקרות הנדרשות, מיקוד בתהליכי עבודה אפקטיביים, שילוב ההגנה כחלק מהתהליכים הארגוניים, הנעת תהליכי לימוד, הפקת לקחים ושיפור.

10. **ליווי פרויקטים בהיבטי הגנת סייבר**: שילוב נושאי ההגנה במכלול מחזור החיים של מערכות ממוחשבות (SDLC).

11. **אבטחת שרשרת האספקה.**

12. **המשכיות עסקית (BCP), התאוששות מאסון (DRP), Incident Response Plan וניתוח השפעות עסקיות (BIA).**

מוסמך טכנולוגיות הגנת סייבר (Cyber Security Technology Specialist)

מהות המקצוע

אדם בעל השכלה אקדמית[10] וידע תיאורטי מקיף ומעמיק, האחראי על:

1. תכנון מענה טכנולוגי להגנת הסייבר בארגון, תוך שילוב טכנולוגיות ושיטות אבטחה.
2. התאמת מוצרי הגנה ושילובם בתשתיות המחשוב, לרבות מערכי אחסון ושיטות גיבוי.
3. ליווי הטיפול באירועי סייבר בהיבט הטכנולוגי.

זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

ידע מקצועי נדרש

בנוסף לבסיס הידע של מיישם הגנת סייבר, יחויב גם בידע מקצועי בנושאים הבאים:

1. **תכנון מענה טכנולוגי להגנת סייבר בארגון**: טופולוגיה / ארכיטקטורה תשתיתית מאובטחת, תכנון מערכים אפליקטיביים ומערכי WEB מאובטחים.
2. **מוצרי הגנה**: הכרת מגוון מוצרי הגנה וחלוקתם למשפחות, השוואה בין מוצרים בהתאם לצרכי הארגון, השפעת הטמעת המוצרים על הארגון ועל מערכי המחשוב שלו.
3. **תקינה טכנולוגית**: לרבות הכרת Protection Profiles ורמות הסמכה (EAL) של Common Criteria.
4. **אחסון**: מערכות אחסון ושיטות גיבוי ושחזור של מידע.
5. **קריפטוגרפיה ונושאים משיקים**: שיטות קריפטוגרפיות נפוצות (הצפנה סימטרית וא-סימטרית), PKI, CA (Certificate Authority), Challenge Response, Digital Signatures, Hash function, סטגנוגרפיה.
6. **הכרה בסיסית של שיטות ותהליכים לפיתוח קוד מאובטח (Secure Coding)**: לדוגמה Secure Coding Guidelines ב-MSDN של Microsoft, וכן שילוב כלים אוטומטיים לבדיקות אבטחה בתהליך הפיתוח.

[10] התארים יהיו בתחומים הבאים (כתחום מקצוע עיקרי / משני / התמחות / שילוב בין תארים): מדעי המחשב / מערכות מידע / הנדסת תוכנה / הנדסת מחשבים / הנדסת אלקטרוניקה / הנדסת תקשורת / הנדסת תעשיה וניהול / מתמטיקה או תואר אחר שיוגדר על ידי הרשות.
הערה: תואר אקדמי שונה ובנוסף הכשרות / הסמכות מקצועיות בהגנת סייבר בהיקף משמעותי (400 שעות במצטבר) שיוכרו על ידי הרשות, יהווה תחליף לתואר אקדמי בתחומים שפורטו.

נספח ב' – אבחנה בין מקצועות לבין תפקידים בתחום הגנת סייבר

1. הוועדה הציבורית לאסדרת מקצועות הגנת הסייבר הבחינה בין **מקצועות** לבין **תפקידים** בתחום זה.
2. אבחנה זו מתבטאת בכך שבעל מקצוע הינו אדם המוסמך לתחום ידע ומיומנות ייחודית וזהו תחום התמחותו העיקרי. לעומת זאת, בעל תפקיד הינו מינוי ארגוני או, לחילופין, שילוב של תחומי התמחות המוכרים כמקצוע. בשלב זה, תבוצע אסדרה של המקצועות.
3. בהתייחס לתפקידים בתחום הגנת הסייבר ובהמשך לעבודת הוועדה הציבורית, בוצע במטה תהליך של חשיבה ראשונית בנושא ואובחנו, בשלב זה, שני תפקידים:

א. **ממונה הגנת סייבר ארגוני**

1) גורם ניהולי בכיר, הממונה על ידי המנכ"ל (על פי רוב בנוסף על תפקידו העיקרי), אשר משימתו ואחריותו הינן להוביל את ההיערכות הארגונית ולבקר את מימוש המדיניות בתחום הגנת הסייבר ובכלל זה: ניהול אסטרטגיה, תשתיות, כוח אדם, מדיניות, אכיפה, מודעות ארגונית לנושאי אבטחה ונושאים נוספים.
2) ממונה הגנת סייבר ארגוני יידרש לידע בסיסי (בהיקף מצומצם יותר מבסיס הידע המקצועי בהגנת סייבר הנדרש מבעלי המקצוע המוסמכים), בהיבטים רלוונטיים של מתאר האיומים, תפיסות ההגנה, שיטות תקיפה, ניהול סיכונים והצורך בהכרת התהליכים העסקיים והמקצועיים של הארגון כבסיס לפעילות הארגונית בתחום הגנת הסייבר.
3) גורם זה לא יהיה כפוף, במישרין או בעקיפין, למנהל ה-IT הארגוני.

ב. **מנהל הגנת סייבר**

1) גורם מקצועי בדרג ניהולי, האחראי על ניהול כלל היבטי הגנת הסייבר בארגון.
2) גורם זה הינו מוסמך/מומחה במתודולוגיות הגנת סייבר אשר השלים את הידע הנדרש בטכנולוגיות הגנה או, לחילופין, מוסמך/מומחה בטכנולוגיות הגנת סייבר אשר השלים את הידע הנדרש במתודולוגיות הגנת סייבר.
3) מומלץ כי גורם זה לא יהיה כפוף, במישרין או בעקיפין, למנהל ה-IT הארגוני.

4. העקרונות והמנגנונים לאסדרת התפקידים בארגונים יוגדרו ויאופיינו בהמשך ע"י המטה והרשות.