קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר

הצעה להחלטה

בהמשך להחלטת ממשלה מספר 3611 מיום 07.08.2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי" (להלן – החלטה 3611), בהתאם לתפיסה הלאומית להגנת הסייבר, לטובת העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר במדינת ישראל, ובכפוף להחלטת ממשלה מִספר 2118 מיום 22.10.14, בנושא "הפחתת הנטל הרגולטורי – דיון בהחלטת ועדת השרים לענייני חברה וכלכלה מס. חכ/39 מיום 14.19.14".

מחליטים,

לקדם אסדרה לאומית בהגנת הסייבר ולפעול להובלה ממשלתית בהגנת הסייבר, כחלק מיישום האסדרה הלאומית וכמהלך של דוגמה לציבור ולמשק.

החלטה זו לא תחול על הגופים המיוחדים כפי שהוגדרו בהחלטה 3611.

הגדרות:

1. שוק שירותי הגנת הסייבר – חברות, יצרנים, ספקים, מוסדות הכשרה והסמכה ובעלי מקצוע העוסקים בהספקת ידע, מוצרים ושירותים בהגנת הסייבר לארגונים.

2. מגזר – כלל הגופים הפועלים במסגרת תחום מקצועי של משרד ממשלתי ובמסגרת אחריותו הרגולטורית.

1. <u>בתחום האסדרה הלאומית בהגנת הסייבר</u>:

א. לאמץ את עקרונות תפיסת האסדרה הלאומית בהגנת הסייבר (להלן – תפיסת האסדרה) שגיבש המטה הקיברנטי הלאומי (להלן – המטה), הכוללת את אסדרת שוק שירותי הגנת הסייבר לצד אסדרת היערכות הארגונים במשק בתחום זה, כמפורט בנספח א'.

ב. בהתאם לתפיסה, לקבוע כי אסדרת היערכות הארגונים במשק בתחום הגנת הסייבר תיעשה מתוך כוונה שלא להוסיף למשק עוד רגולטורים, אלא באמצעות העצמה של הרגולטורים הקיימים, וזאת באמצעות מגוון הכלים העומדים לרשותם וחיזוק כלים אלה ככל הנדרש, על מנת להעלות את רמת החוסן של המגזר האזרחי לאיומי סייבר, ובכלל זה באמצעות היערכות וכשירות.

ג. להטיל על המטה להקים יחידה שייעודה להסדיר את שוק שירותי הגנת הסייבר, לרבות אנשי מקצוע, שירותים ומוצרים, וזאת בהתאם לתפיסת האסדרה ובכפוף לכל דין, כמפורט בנספח ב'. היחידה תוקם במסגרת הרשות הלאומית להגנת

הסייבר שעתידה לקום במשרד ראש הממשלה בכפוף להחלטת ממשלה (להלן – הרשות הלאומית להגנת הסייבר).

ד. להטיל על המטה לבחון בניית תשתית לבדיקות ולאישור מוצרי הגנת הסייבר, לרבות בחינה של הקמה והפעלה של מעבדה לצורך כך, כמפורט בנספח ג'.

ה. להטיל על המנכ"לים של משרדי הממשלה שבמסגרתם מופעלות סמכויות רגולציה כלפי גופים או פעילויות החשופים לאיומי סייבר, לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים כדלקמן:

1) להקים יחידה להכוונה מקצועית בתחום הגנת הסייבר, כמפורט בנספח ד'. זאת בהתאם לסמכויות הרגולציה המופעלות על ידם או במסגרתם.

2) לפעול לקידום הגדרת המדיניות ודרישות האסדרה למימוש החלטה זו במסגרת המגזר עליהם אחראים.

3) לבצע, בתיאום עם המטה, עבודת מטה שתוגש לראש הממשלה, הבוחנת את התיקונים והשינויים הנדרשים מבחינה משפטית למימוש אפקטיבי של האמור.

במגזרים שבהם יותר ממשרד ממשלתי אחד האחראי להפעלת סמכויות רגולציה ביחס לגופים או לפעילויות, להטיל על ראש המטה לקבוע את המשרד המוביל לעניין פעילות זו.

ו. להנחות את מנכ"ל משרד הכלכלה, בתיאום עם המטה ומשרד האוצר, להציג לממשלה בתוך 120 יום מהחלטה זו תכנית להפעלת מנגנוני סיוע ותמרוץ לארגונים במשק שיפעלו להעלאת רמת המוכנות לאיומי סייבר, כפי שיוגדר בתכנית.

ז. להטיל על הלשכה המשפטית במשרד ראש הממשלה והמטה, בשיתוף משרד המשפטים, להכין תזכיר לחוק, אשר יוגש על ידי ראש הממשלה, ולרכז את תיקוני החקיקה הנדרשים למימוש האמור בתוך 180 יום מהחלטה זו.

2. <u>בתחום ההובלה הממשלתית בהגנת הסייבר</u>:

א. להקים יחידה להגנת הסייבר בממשלה (להלן – יה"ב) שייעודה להוות גוף הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך, למעט הגופים המיוחדים, ולהקים מרכז שליטה ובקרה ממשלתי למול איומי סייבר (להלן – ה-SOC ממשלתי), כמפורט בנספח ה'.

ב. להטיל על המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך לפעול לשיפור רמת הגנת הסייבר, ולשם כך למנות ממונה הגנת הסייבר, להקים ועדת היגוי משרדית, להסדיר את אנשי המקצוע בתחום הגנת הסייבר המועסקים במשרד, להקצות תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של המשרד, ולקדם עמידה של המשרד בתקני אבטחת מידע ארגוניים, כמפורט בנספח ו'.

ג. להטיל על מנהל הרכש הממשלתי ועל המנכ"לים של משרדי הממשלה, לפי העניין, להטמיע במסגרת הליך הרכש המרכזי או במסגרת הליך הרכש המשרדי דרישות הולמות בתחום הגנת הסייבר, כמפורט בנספח ז'.

ד. להטיל על ראש המטה להקים ועדת היגוי לקידום ההובלה הממשלתית בהגנת הסייבר (להלן – ועדת ההיגוי הממשלתית) ולגבש מנגנוני סיוע למשרדי הממשלה למימוש פתרונות טכנולוגיים מתקדמים לצרכים ייחודיים, כמפורט בנספח ח'.

להטיל על יה"ב לעקוב אחר קיום האמור בסעיפים 2.ב.-2.ג. בהחלטה זו, ולדווח על כך לוועדת ההיגוי הממשלתית.

נספח א' – עיקרי תפיסת האסדרה הלאומית בהגנת הסייבר

1. מטרת האסדרה: העלאה שיטתית ורציפה של רמת הגנת הסייבר במדינת ישראל באמצעות מימוש סטנדרטים מקצועיים בארגונים, וכן הסדרה של שוק שירותי הגנת הסייבר (אנשי מקצוע, שירותים ומוצרים) במגוון כלים.

2. פעילות האסדרה הלאומית עוסקת בעיקר בשכבה הראשונה בתפיסה הלאומית להגנת הסייבר, כמפורט בהצעה להחלטת ממשלה בנושא "קידום ההיערכות הלאומית להגנת הסייבר".

3. האסדרה תוכן כך שתיקח בחשבון את ההיבטים הבאים:

א. האסדרה תאמץ, ככל האפשר, רעיונות, תכניות ופעילויות מוצלחות שנעשו בעולם, תוך התאמתם למציאות הישראלית.

ב. האסדרה תסתמך, במידה רבה, על תקינה בינלאומית.

ג. האסדרה תקיים שותפות והתעדכנות בתהליכי פיתוח רגולציה בעולם.

ד. האסדרה תהיה מידתית.

ה. האסדרה תאפשר, במקרים מסוימים, מרחב גמישות למגזרים ולארגונים על מנת לממש ייעודם.

ו. האסדרה תמנף ותסתייע בגורמים הקיימים הפועלים בתחום אבטחת המידע והגנת הסייבר.

ז. האסדרה תגדיר רמות שונות של הגנה והסמכה ותיצור מנגנונים להתאמה והלימה ביניהן, לדוגמה בארגונים שבהם נדרשת הגנה ברמה גבוהה יועסקו חברות הנותנות שירותי הגנת הסייבר שהוסמכו לרמה זו.

ח. האסדרה תניע, תאפשר ותעודד פעילויות רצויות בתחום במשק הישראלי, כגון הכשרות, שיתוף מידע ופעילויות פנים-מגזריות, ולא תבלום את היזמות ואת פוטנציאל הייצוא.

ט. האסדרה תאפשר ותציע נגישות לכלים ולמתודות לשימוש ארגוני.

4. האסדרה תתמקד בארגונים ובמערכותיהם, כך שיתקיימו הנושאים הבאים:

א. בארגונים יעבדו אנשי המקצוע המתאימים.

ב. הארגונים יקבלו שירותים מקצועיים ברמת האיכות המתאימה להם.

ג. במערכות הארגון יוטמעו מוצרים מאושרים ומתאימים.

ד. הארגונים יפעלו בהתאם לתקינה מתאימה הן בהיבט הארגוני-תהליכי והן בהיבט הטכנולוגי להגנת המערכות הממוחשבות שלהם.

נספח ב' – יחידה להסדרת שוק שירותי הגנת הסייבר

הגדרות:

"Common Criteria" – תקן (ת"י ISO 15408) העוסק באישור ובהסמכת מוצרי אבטחת מידע והגנת הסייבר בהתאם לדרישות מוגדרות ולתהליך הכולל בדיקות מעבדה מוסמכת. אישור והסמכת המוצרים מתבצעים בהתאם למדרג של רמות בדיקה.

1. ייעוד: הסדרה של שוק שירותי הגנת הסייבר במדינת ישראל.

2. תפקידים

א. בתחום אנשי המקצוע – לקדם את העמידה בסטנדרטים המקצועיים של אנשי המקצוע ושל מוסדות ההכשרה וההסמכה בתחום הגנת הסייבר, באמצעות עיסוק בנושאים הבאים ובחינה עיתית שלהם ובשים לב ל-"דו"ח הוועדה הציבורית להגדרת מקצועות ההגנה בסייבר" (להלן – הדו"ח):

1) הגדרת תחומי הידע הנדרשים למקצועות הגנת הסייבר.

2) בחינה של מסלולי ההכשרה וההסמכה.

3) שיתופי פעולה עם מוסדות ההכשרה וההסמכה.

4) מתן חוות דעת ואישורים מקצועיים ביחס לעמידה של מסלולי ההכשרה וההסמכה ושל אנשי המקצוע בדרישות המקצועיות.

5) הסמכת אנשי המקצוע ומסלולי ההכשרה וההסמכה, בכפוף לכל דין.

ב. בתחום המוצרים – הקמה והפעלה של מנגנון לאישור מוצרי הגנת הסייבר לעמידה בתקנים, כגון תקן Common Criteria, ובכלל זה:

1) בניית סכימה לאומית, בהתאם לתקן, לבדיקה ולאישור מוצרי הגנת הסייבר בישראל, זאת בתיאום עם המטה.

2) קבלת בקשות לאישור מוצרים, לרבות מיצרנים.

3) הפניית בקשות בדיקה למעבדות מוסמכות.

4) הנפקת אישורים למוצרים העומדים בדרישות.

ג. בתחום השירותים – לקדם את העמידה בסטנדרטים מקצועיים של חברות הייעוץ ושירותי הגנת הסייבר (להלן – ספקי השירות) ובכלל זה:

1) הגדרת השירותים הנדרשים להסדרה.

2) קביעת מדרג איכות לכל שירות.

3) קביעת הדרישות המקצועיות לעמידה ברמות השונות של מדרג האיכות לכל שירות.

4) מתן חוות דעת ואישורים ביחס לעמידה של ספקי השירות בדרישות המקצועיות שהוגדרו לרמת האיכות של השירות הניתן על ידם.

5) הסמכה של ספקי השירות, בהתאם לסוג השירות ולרמתו המקצועית, ובקרה על כך, בכפוף לכל דין.

3. כ"א ותקציב

א. היחידה תוקם במסגרת הרשות הלאומית להגנת הסייבר, וסמכויותיה יעוגנו בחקיקה בהתאם לצורך, כאמור בסעיף 1.ז. להחלטה זו.

ב. תקני היחידה יסוכמו בין המטה לבין משרד האוצר ונציבות שירות המדינה כחלק מהרשות הלאומית להגנת הסייבר.

ההסדרה תבוצע תוך בחינת חלופות למימוש ובהתייעצות עם גופים ומשרדים רלוונטיים. היבטי אסדרת המקצועות ופעילות בעלת השפעה על עסקים קטנים ובינוניים יתואמו עם משרד הכלכלה.

נספח ג' – קידום בניית תשתית מדינתית לאישור מוצרי הגנת הסייבר

1. המטה יבחן הקמה והפעלה בישראל של מעבדה שייעודה בדיקות ואישורים של מוצרי הגנת הסייבר, בהתאם לתקן Common Criteria, ובאופן שתוצריה יוכרו בעולם.

2. החלטה על הקמה והפעלה של מעבדה, לרבות התקציב למימוש, יסוכמו בין המטה לאגף התקציבים במשרד האוצר.

3. המטה ומשרד הכלכלה יקדמו במשותף סיוע ליצרנים שהינם עסקים קטנים ובינוניים, בהתאם להגדרות משרד הכלכלה, המעוניינים לעמוד בתקן Common Criteria.

התקציב לטובת מענקי הסיוע יתוקצב ממקורות המטה בין השנים 2015-2019.

נספח ד' – יחידות להכוונה מקצועית מגזרית בתחום הגנת הסייבר במשרדי הממשלה

1. ייעוד: הכוונה והנחיה מקצועית בתחום הגנת הסייבר בהתאם לסמכויות הרגולציה המופעלות על ידי המשרד הממשלתי או במסגרתו.

2. כפיפות

א. היחידה תפעל בכפיפות למשרד הממשלתי שאליה היא שייכת.

ב. היחידה תפעל בהנחיה מקצועית של הרשות הלאומית להגנת הסייבר.

3. תפקידים

א. הכוונה והנחיה בהיבטי הגנת הסייבר, לרבות הגדרת המדיניות ודרישות האסדרה, ליווי מקצועי שוטף ומענה לפניות מקצועיות, בהתאם למאפיינים של הגופים אשר ביחס אליהם מתבצעת הפעילות (להלן – המגזר). ככל שיידרש, בנושאים שחל עליהם החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק), ובנושאים שחל עליהם חוק הגנת הפרטיות, התשמ"א-1981, תתבצע ההנחיה בתאום עם הגורם המוסמך לפי חוקים אלה.

ב. בקרת ביצוע הדרישות המקצועיות בהתאם לאסדרה וברמה המקצועית הנדרשת, לרבות הכרת הפערים והצורך בהתאמות.

ג. בניה והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר, לרבות דיווח אודות אירועים, איומים, חולשות, פוגענים ונוזקות למרכז לסיוע בהתמודדות עם איומי סייבר (להלן – ה-CERT הלאומי) וכן הגדרת נהלי ושיטות הדיווח בין הגופים במגזר.

ד. ייזום ומימוש פעילות רוחבית, לרבות הקמת תשתיות והפעלת מנגנונים, שתכליתם שיפור הגנת הסייבר במגזר.

4. כ"א ותקציב

א. המטה יסווג בתוך 90 יום מהחלטה זו, את היקף הפעילות הנדרשת של המשרדים בתחום הגנת הסייבר, בהתאם לנזק הפוטנציאלי כתוצאה מפגיעה במערכות הממוחשבות של הגופים במגזרם. זאת בהתאם לקטגוריות: גדול, בינוני, קטן.

ב. בהתאם לסיכום בין המטה לבין נציבות שירות המדינה, המשרדים יאיישו את התפקידים האמורים לעיל, בהתאם למפתחות המפורטים להלן:

היקף פעילות/תפקיד	מנהל	תחום הכוונה	תחום בקרה
גדול	1	2	2
בינוני	1	1	1
קטן	1	-	-

ג. במשרדים המבצעים כיום הנחיה מקצועית בתחום הגנת הסייבר של גופי מגזר, הקצאת כוח האדם, כאמור בנספח זה, תיעשה כהשלמה לאמור ועל פי הצורך, תוך מניעת כפילויות ובתאום עם אגף התקציבים במשרד האוצר.

ד. מקורות לטובת איוש התפקידים:

1) איוש התפקידים יבוצע באמצעות תקני כוח אדם ועובדים ממיקור חוץ למשרדי הממשלה.

2) תקציב בשנים 2015-2016 – התקציב לאיוש התפקידים יתבסס על מקורות המטה, בסכום שלא יעלה על 500 אש"ח בשנה לתפקיד.

3) תקציבי השנים 2017-2019 – מחצית מהתקציב תתוקצב ממקורות המטה ומחציתו ממקורות המשרד הממשלתי הרלוונטי. המטה ישתתף בתקציב עד לתקרה של 500 אש"ח בשנה ליועץ.

4) המטה ייבחן בעוד 5 שנים מקבלת החלטה זו את מנגנון איוש ותקצוב התפקידים.

ה. התקצוב כאמור יעשה על מנת לאפשר עמידה בלוחות הזמנים של האיוש המפורטים להלן, אשר הינם באחריות המנכ"לים של משרדי הממשלה:

1) איוש משרת מנהל היחידה עד תום המחצית הראשונה של שנת 2015.

2) איוש יתר המשרות, במשרדים שסווגו בהיקף פעילות בינוני או גדול, יבוצע בתיאום בין המטה לבין כל אחד מהמשרדים.

5. <u>בקרה</u>: להטיל על המטה לבצע בקרה על מימוש נספח זה.

המטה, נציבות שירות המדינה ומשרד האוצר בסיכום ביניהם יהיו רשאים לשנות את המפתחות המפורטים בסעיף 4 ב'.

נספח ה' – הובלה ממשלתית בהגנת הסייבר – היחידה להגנת הסייבר בממשלה ומרכז שליטה ובקרה ממשלתי למול איומי סייבר

1. ייעוד היחידה להגנת הסייבר בממשלה (להלן – יה"ב): הכוונה והנחייה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך.

2. כפיפות

א. יה"ב תפעל בכפיפות לממונה על התקשוב הממשלתי.

ב. יה"ב תפעל בהנחייה מקצועית של הרשות הלאומית להגנת הסייבר.

3. תפקידים

א. הכוונה והנחיה של משרדי הממשלה ויחידות הסמך בהיבטי הגנת הסייבר, לרבות בתחומים הבאים:

1) מיפוי מושאי ההגנה.

2) ניהול סיכונים.

3) הכנת תכנית להגנת הסייבר והקצאת משאבים למימושה.

4) גיבוש מדיניות ארגונית, נהלים ושיטות עבודה.

5) היערכות להתמודדות עם אירועים, לרבות ניהול אירועים, תהליכי התאוששות ושיקום.

ככל שיידרש, בנושאים שחל עליהם החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק), ובנושאים שחל עליהם חוק הגנת הפרטיות, התשמ"א-1981, תתבצע ההנחיה בתאום עם הגורם המוסמך לפי חוקים אלה. כמו כן, ככל הניתן, ההנחיה תיעשה בשים לב לצרכים ולמאפיינים הייחודיים של משרדי הממשלה ויחידות הסמך.

ב. בקרת ביצוע הדרישות המקצועיות בהתאם להכוונה ולהנחיה.

ג. בניית תהליכי שיתוף מידע בתוך הממשלה, לרבות דיווח ל-CERT הלאומי.

ד. ייזום פעילות רוחבית ומימושה.

ה. מעקב אחר קיום הדרישות לעניין ההובלה הממשלתית בהגנת הסייבר, ודיווח לוועדת ההיגוי הממשלתית, כמפורט בנספח ח'.

4. כ"א ותקציב

לשם הקמת היחידה תקצה רשות התקשוב הממשלתי 2 תקנים בשנת 2015 ממקורותיה, ומשרד האוצר יקצה 2 תקנים בשנת 2015 ו-3 תקנים בשנת 2016 בהתאם לסיכום עם משרד ראש הממשלה. תנאי ההעסקה של עובדי היחידה יסוכמו בין רשות התקשוב הממשלתי לבין הממונה על השכר במשרד האוצר, בתיאום עם המטה ונציבות

שירות המדינה. כמו כן, יקצה משרד האוצר ליחידה תקציב בסך 1.5 מלש"ח לשנת 2015, 2 מלש"ח לשנת 2016, 0.5 מלש"ח לשנת 2017, ותקציב שוטף בסך 4 מלש"ח החל משנת 2017.

<u>מרכז שליטה ובקרה ממשלתי למול איומי סייבר</u>

5. להטיל על המטה ועל יה"ב להקים ביחד מרכז שליטה ובקרה ממשלתי למול איומי סייבר (להלן – ה-SOC הממשלתי) אשר יעסוק בגיבוש תמונת מצב ממשלתית שוטפת בהיבטי הגנת הסייבר ומתן מענה לטיפול באירועי סייבר.

6. להקים את ה-SOC הממשלתי במסגרת ה-CERT הלאומי על בסיס תשתיותיו הטכנולוגיות והאופרטיביות ותוך בניית יכולות ייעודיות לממשלה.

7. להנחות את משרדי הממשלה, ובכללם את ממשל זמין, להעביר ל-SOC הממשלתי דיווחים הקשורים בהגנת הסייבר, לרבות אירועים, איומים, חולשות, פוגענים ונוזקות.

תקצוב ה-SOC הממשלתי יסוכם בין המטה, רשות התקשוב הממשלתי ומשרד האוצר.

נספח ו' – הובלה ממשלתית בהגנת הסייבר – פעילות לקידום הגנת הסייבר במשרדי הממשלה

הגדרות:

"ת"י ISO 27001" – תקן ישראלי שאומץ מתקן ISO בינלאומי העוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ולתהליך השוטף של הקמת המערכת ושיפורה השיטתי.

1. מינוי ממונה הגנת הסייבר במשרד ממשלתי

א. המנכ"לים של משרדי הממשלה ימנו בכל משרד ממשלתי בעל תפקיד האחראי על הגנת הסייבר במשרד (להלן – ממונה הגנת הסייבר). בעל תפקיד זה יפעל בכפיפות ישירה למנכ"ל או מטעמו.

1) תפקיד הממונה ימולא, ככל הניתן, על ידי בעל תפקיד בדרג ניהולי קיים.

2) בכל משרד ממשלתי ימונה ממונה אחד בלבד לשם מניעת כפילויות.

ב. תפקיד ממונה הגנת הסייבר:

1) גיבוש מדיניות הגנת הסייבר במשרד, בהתאם לתהליך ניהול סיכונים ארגוני.

2) בניית תכנית עבודה להגנת הסייבר על פי המדיניות.

3) ניתוח והערכה שוטפים של תכנית הגנת הסייבר והמדיניות בהתאם לצרכים, לאיומים ולמענים, וכן של ההיערכות הארגונית להתמודדות עם אירועי סייבר.

4) גיבוש תכנית תקציבית לטיפול בהגנת הסייבר ולניהולה השוטף.

5) בקרה על יישום וניהול הגנת הסייבר בהיבט הארגוני הרחב ובהתאם למדיניות.

ג. גורם זה יהיה נציג המשרד בוועדת ההיגוי הממשלתית (אם המשרד מיוצג בוועדת ההיגוי), כמפורט בנספח ח' להחלטה זו.

ד. מנהלי יחידות הסמך במשרד הממשלתי ימנו, בתיאום עם המשרד הממשלתי ועם יה"ב, ממונה הגנת הסייבר ביחידת הסמך או לחילופין אחראי הגנת הסייבר. במידה ויוחלט כי ימונה אחראי הגנת הסייבר, הוא יפעל בכפיפות מקצועית לממונה הגנת הסייבר של המשרד הממשלתי.

2. הסדרת מינוי אנשי המקצוע בתחום הגנת הסייבר המועסקים בממשלה ועל ידי הממשלה

א. ועדת ההיגוי הממשלתית תגדיר בתוך 120 יום את הדרישות להעסקת אנשי מקצוע בתחום הגנת הסייבר בממשלה ועל ידי הממשלה. זאת בהתאם לעקרונות שייקבעו על ידי המטה, בשים לב לדו"ח.

ב. בתוך 90 יום מהגדרת הדרישות על ידי ועדת ההיגוי הממשלתית, יבחנו המשרדים

את מידת עמידתם של המועסקים אצלם בתחום הגנת הסייבר בדרישות. מיפוי זה יוגש לוועדת ההיגוי הממשלתית.

ג. המשרדים ימנו "אחראי על הגנת הסייבר ביחידת מערכות המידע" (להלן – האחראי):

1) האחראי יעמוד בדרישות של "מגן קיברנטי בכיר", בהתאם להמלצות הדו"ח.

2) האחראי יהיה כפוף ישירות למנמ"ר ויפעל בהתאם להנחיות מקצועיות של יה"ב בהיבטי הגנת הסייבר.

ד. כל עובד חדש שיועסק בתחום הגנת הסייבר בממשלה יעמוד בדרישות המקצועיות שהוגדרו לעיל.

ה. ועדת ההיגוי הממשלתית תגדיר את שלבי המימוש של הדרישות המקצועיות, ובכלל זה ביצוע הכשרות והשתלמויות מקצועיות, כך שבתוך חמש שנים, לכל היותר, כלל העובדים העוסקים בתחום הגנת הסייבר בממשלה יעמדו בדרישות המקצועיות. חריגים יאושרו על ידי ועדת ההיגוי הממשלתית בלבד.

3. <u>הקמת ועדת היגוי משרדית</u>

א. הוועדה תפעל לשיפור רמת הגנת הסייבר של המשרד, לרבות הפעילויות המפורטות בהחלטה זו, ותפקח על הפעילות השוטפת המבוצעת במשרד בנושא זה.

ב. ראש הוועדה: מנכ"ל המשרד הממשלתי, חברים בה: נציגים בכירים במשרד בעלי אחריות לתחום הגנת הסייבר, לרבות אחריות בהיבטים טכנולוגיים, אבטחתיים ותפעוליים, מנהל התקציבים, מנהל משאבי אנוש, יועמ"ש, נציג יה"ב ונציגים נוספים לפי שיקול דעתו של המנכ"ל.

ג. הוועדה תתכנס לכל הפחות פעם בחציון.

4. <u>הקצאת תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של משרדי הממשלה</u>

א. המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך, במסגרת סמכותם ואחריותם הקיימת, יסדירו את מבנה התקציב השנתי של משרדם כך שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר.

ב. מנכ"ל משרד ממשלתי או מנהל יחידת הסמך, לפי העניין, יוכל בנסיבות מיוחדות לאשר הפחתה מהאמור, בהחלטה מפורטת ומנומקת שתדווח לוועדת ההיגוי הממשלתית, כמפורט בנספח ח' להחלטה זו, ובלבד שלפחות 6% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר.

ג. בתום שנתיים ממועד החלטה זו, ועדת ההיגוי הממשלתית תבחן את הצורך בהעלאת אחוז התקציב הייעודי להגנת הסייבר.

5. <u>עמידה של משרדי הממשלה וגופיה בתקני אבטחת מידע ארגוניים</u>

א. המנכ"לים של משרדי הממשלה יגדירו בתוך 120 יום מהחלטה זו תכנית מדורגת להטמעה, התעדה והסמכה לתקן אבטחת מידע ארגוני ממשפחת ת"י ISO 27001, כמפורט להלן:

1) מטה המשרד ומחוזות המשרד – בתוך שנתיים. ועדת ההיגוי הממשלתית מוסמכת להאריך את התקופה האמורה בשנה נוספת.

2) גופים נוספים במשרד – בהתאם לתכנית עבודה רב-שנתית, שתגובש בתוך שנתיים, לביצוע בתוך חמש שנים לכל היותר.

ב. תכנית ההסמכה תוגש לאישור ועדת ההיגוי הממשלתית, כמפורט בנספח ח' להחלטה זו, בתוך 120 יום מהחלטה זו. אחריות ביצוע התכנית המאושרת תחול על המנכ"לים של משרדי הממשלה.

ג. משרדי הממשלה ידווחו מדי שנה לוועדת ההיגוי הממשלתית על יישום התכנית, ולא יאוחר מיום 30 ביוני בכל שנה אזרחית.

המטה יקדם הליך תחרותי לשירותי ייעוץ שילוו את משרדי הממשלה באופן מקצועי פרטני במימוש תכנית היישום ויתקצב את הפעלתם.

נספח ז' – הובלה ממשלתית בהגנת הסייבר – רכש

1. רכש ממשלתי של שירותים ושל מוצרי הגנת הסייבר מאושרים בהתאם לתקינה

א. המטה יקים תת ועדה בהשתתפות נציגים מהחשב הכללי, יה"ב ושירות הביטחון הכללי, שתגבש מתווה ועקרונות בנוגע לאופן רכישת שירותים ומוצרים תוך שימוש בתקינת אבטחת מידע (כגון Common Criteria) במערכות הממשלתיות, בתוך 180 יום מהחלטה זו.

ב. מנהל הרכש הממשלתי והמנכ"לים של משרדי הממשלה, לפי העניין, אחראים לכך שרכש שירותים ומוצרים בתחום הגנת הסייבר, יבוצע בהתאם למתווה ולעקרונות שיגובשו על ידי תת הוועדה. ועדת ההיגוי הממשלתית, כמפורט בנספח ח', תוכל לאשר חריגים לאמור.

2. דרישות לעמידה בתקני אבטחת מידע ארגוניים, כתנאי לרכש מגורמים המעבירים מידע ממוחשב אל הממשלה או ספקים של מערכות מחשוב

א. גורמים המעבירים מידע ממוחשב או ספקים של מערכות מחשוב, המוטמעות או מקושרות למערכות מחשוב ממשלתיות, המבקשים למכור לממשלה שירותים הקשורים בכך, יחויבו לעמוד בתקן אבטחת מידע ארגוני ממשפחת ת"י ISO 27001, החל מתום שנתיים להחלטה זו. יה"ב תוכל להאריך התקופה האמורה במקרים פרטניים, לתקופה של שנה נוספת.

ב. הטיפול בחריגים, מעבר להארכת תקופת המימוש בשנה נוספת, יתואם בין המטה, יה"ב ומנהל הרכש הממשלתי.

ככל הנדרש, יבוצעו תיקונים בתקנות חובת המכרזים ובהוראות התכ"מ למימוש האמור.

נספח ח' – הובלה ממשלתית בהגנת הסייבר – מנגנוני ניהול, תיאום וסיוע

1. הקמת ועדת היגוי ממשלתית לקידום ההובלה הממשלתית בהגנת הסייבר (להלן – הוועדה)

א. הוועדה תפעל לקידום רמת הגנת הסייבר במשרדי הממשלה וביחידות הסמך, בהתאם למפורט בנספחים ה', ו', ז' להחלטה זו, ותפקח על הפעילות השוטפת המבוצעת בנושאים אלו, מתוך ראייה כוללת של קידום ההובלה הממשלתית בהגנת הסייבר.

ב. ראש הוועדה: ראש המטה הקיברנטי הלאומי.

ג. נציגי הוועדה ממשרדי ממשלה: ממוני הגנת הסייבר, כמפורט בנספח ו', ממשרדי התשתיות הלאומיות, האנרגיה והמים, התקשורת, הבריאות, התחבורה והבטיחות בדרכים, האוצר, הכלכלה, החוץ, הפנים, ביטחון הפנים, וכן נציגי המטה הקיברנטי הלאומי, החשב הכללי ואגף התקציבים במשרד האוצר, יה"ב, נציבות שירות המדינה, שירות הביטחון הכללי והרשות למשפט טכנולוגיה ומידע במשרד המשפטים. ראש הוועדה יוכל להוסיף נציגים נוספים על פי שיקול דעתו.

ד. ועדה זו תתכנס לכל הפחות פעם ברבעון.

ה. הוועדה תדווח לממשלה על פעילותה, ההתקדמות והפערים ביישום, אחת לשנה.

2. גיבוש מנגנוני סיוע למשרדי הממשלה למימוש פתרונות טכנולוגיים מתקדמים לצרכים ייחודיים

א. המטה יקים תת ועדה בהשתתפות יה"ב, שירות הביטחון הכללי ומשרד האוצר למיפוי צרכים ייחודיים במשרדי הממשלה בתחום הגנת הסייבר ולגיבוש מנגנוני סיוע לפיתוח, להצטיידות ולהטמעת פתרונות טכנולוגיים מתקדמים לצרכים אלו.

תקציב לסעיף זה יוקצה ממקורות המטה.

דברי הסבר

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 מאד, 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.

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.

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 בתוכו, 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.

אשר לאומדן הנזקים הכלכליים הנובעים מתקיפות סייבר למדינות ולארגונים – אמנם, קיים קושי אובייקטיבי לאמוד נזקים אלו, אך ממחקרים רבים עולה כי מדובר בנזקים משמעותיים מאוד הן ברמת מדינות והן ברמת ארגונים. כך לדוגמה, עולה מן המקורות הבאים:

א. דו"ח ה-IC3 האמריקני, גוף מדינתי הכולל מרכז לקבלת תלונות על הונאות מסוגים שונים באינטרנט[1], קובע כי בשנת 2013 הנזק המצרפי מן התלונות עמד על יותר מ-780 מיליון דולר.

[1] http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

ב. דו"ח של ממשלת בריטניה בשיתוף חברת Detica[2], העוסקת בייעוץ טכנולוגי ופיננסי, משנת 2011 קובע כי עלויות פשיעת הסייבר בבריטניה מוערכות בכ-27 מיליארד לישי"ט בשנה.

ג. דו"ח של איגוד הקמעונאים הבריטיים (British Retail Consortium) לשנת 2012[3] קובע כי סוג הפשיעה המזיק ביותר לסקטור הקמעונאי הוא תחום תקיפת המחשבים והמרמה המקוונת. הערכת הנזק לסקטור הקמעונאי מתקיפת המחשבים והמרמה המקוונת בשנת 2012 בבריטניה עמדה על 205.4 מיליון לישי"ט.

ד. דו"ח של חברת אבטחת המידע McAfee משנת 2009[4] ניסה להעריך את עלויות ההשבתה של מחשבים במגזר הממשלתי ובמגזר האנרגיה, כתוצאה מהתקפות מניעת שירות באמצעות האינטרנט (DoS – Denial of Service). על פי הדו"ח, תקיפת סייבר על מחשבי מערכות ממוחשובת חיוניות עלולה להסב נזק המוערך בכ-6.3 מיליון דולר (בממוצע למדינה) עבור כל 24 שעות של השבתת המערכת, כאשר ההשבתה אף עלולה לגרום לאובדן חיים.

ה. דו"ח של חברת אבטחת המידע Norton משנת 2013[5] ניסה לכמת את נזקי פשיעת הסייבר ברמה העולמית. ממצאי המחקר הראו כי הנזק הישיר אשר נגרם בעולם כולו מפשעי מחשב, ובעיקר עקב הונאות מקוונות, תוכנות זדוניות ווירוסים, חדירות למחשב וגניבות מידע, הינו כ-113 מיליארד דולר.

ו. הדו"ח של שחר ארגמן וגבי סיבוני, שפורסם בשנת 2014[6], סקר את תופעת הריגול העסקי בסייבר מהפן הכלכלי, והציג את נזקיה הישירים ברמה העולמית על בסיס מחקרים קיימים. הדו"ח מעריך שנזקי הריגול העסקי המקוון במדינת ישראל הינם גבוהים ביותר ונעים בין 1-3 מיליארד דולר בשנה. להלן ריכוז הנתונים שהציגו:

	הנזק השנתי המוערך כתוצאה מגניבת מידע מסחרי וקניין רוחני	
המדינה הנתקפת	במיליארדי דולרים	כאחוז מהתמ"ג
ארה"ב	250-300	1.67-2
דרום קוריאה	82	7.3
גרמניה	28-71	0.8-2
אנגליה	34	1.4

מרחב הסייבר, כפי שהתפתח, הינו במידה רבה מרחב אזרחי. נדרש להגן על מרחב זה ולהעלות את רמת החוסן שלו לאיומי סייבר, ובכלל זה באמצעות היערכות וכשירות, אולם

[2] https://www.baesystemsdetica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf
[3] http://www.brc.org.uk/downloads/brc_retail_crime_survey_2012.pdf
[4] http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf
[5] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013
[6] "חשיפת המשק הישראלי לריגול סייבר עסקי", צבא ואסטרטגיה 6, 39 (2014).

תוך שמירה על חיוניותו כמנוע צמיחה וכמאפשר זרימה חופשית, ככל הניתן, של מידע, שירותים ומסחר.

מדינות נדרשות להיערך לאתגר ההגנתי המתפתח בסייבר במספר צירי פעולה כחלק ממענה שלם ורב מימדי (בהיבטים מדיניתיים, משפטיים, טכנולוגיים, כלכליים, מודיעיניים ועוד).

אחד מצירי הפעולה הינו מיסוד סטנדרטים מקצועיים בתחום הגנת הסייבר והחלת אסדרה שתכליתה העלאה שיטתית ורציפה של רמת ההגנה במדינה. זאת על מנת למנוע, או לפחות לצמצם, את פגיעותה לתקיפות סייבר וכחלק מהמאמץ להובלה עולמית בתחום הסייבר.

מורכבותו והיקף השפעתו של הנושא, רמת הביזור הגבוהה שבו, החשיבות והצורך במענה משולב, מתואם ורב-שכבתי מחייבים ראייה מערכתית-אסטרטגית.

עם זאת, ראוי לזכור כי הטיפול בנושא במדינה, ברמות וברבדים שונים, לא החל כעת והעיסוק בו אינו מצוי בחלל ריק. האסדרה אינה מתעלמת מהקיים, אלא מתחשבת בו ונוקטת גישה משלבת ומתכללת. יתרה מזאת, למגזרים ולארגונים עצמם יש רצון ומחויבות להסדרת הסייבר בתחומם, הן נוכח המוטיבציה למניעה או לצמצום נזקים ומשיקולי הגנה מפני תביעות, והן לאור השאיפה למתן שירות טוב ואמין ולשמירה על לקוחות ותדמית.

במדינת ישראל פועלים כיום מספר גורמים בתחום אסדרת הגנת הסייבר ואבטחת המידע כלפי המגזר האזרחי וכן רגולטורים מגזריים.

א. גורמי האסדרה העיקריים בתחום הגנת הסייבר ואבטחת המידע כלפי המגזר האזרחי (בדגש על פעילות מול ארגונים במגזר זה ומשרדי ממשלה), הם הרשות הממלכתית לאבטחת מידע בשירות הביטחון הכללי והרשות למשפט מידע וטכנולוגיה במסגרת משרד המשפטים.

ב. הרגולטורים המגזריים (בתחומים כגון בריאות, בנקאות, תקשורת ואנרגיה) פועלים, מכוח חוקים, תקנות והחלטות, כלפי הגופים במגזר שלהם. כך לדוגמה, המפקח על הבנקים בבנק ישראל מגדיר רגולציה מחייבת (גם בתחום הגנת הסייבר) עבור הבנקים, ומשרד הבריאות מגדיר רגולציה להגנת הסייבר עבור מערכת הבריאות.

למרות שקיימים גורמים העוסקים בפועל בתחום, אף גורם מביניהם לא שימש, ולא נדרש לשמש, כגורם לאומי מרכזי המתכלל ומוביל את התחום בראייה לאומית ובדגש על אסדרת שוק שירותי הגנת הסייבר (בניגוד לאסדרת הגנת הסייבר במגזרים ובארגונים עצמם). כפועל יוצא, אף גורם מביניהם לא התמקד ולא היה אחראי על קידום פעילויות מדינתיות כלליות ותשתיתיות בתחום זה, כגון חקיקה, הסדרת המקצועות, תקינה, ייצוג המדינה מול גורמי רגולציה ותקינה בעולם וכדומה.

במסגרת החלטת ממשלה מספר 3611 בנושא "קידום היכולת הלאומית במרחב הקיברנטי" מיום 07.08.2011 (להלן – החלטה 3611) הוחלט על הקמת המטה הקיברנטי הלאומי (להלן – המטה). לפי החלטה זו, אחד מתפקידי המטה הוא לקדם חקיקה ותקינה בתחום הסייבר.

קידום החקיקה והתקינה ברמה הלאומית בתחום הגנת הסייבר יהווה פעילות מרכזית

ומשמעותית לבניה ולמיסוד מנגנוני האסדרה הלאומית לתחום הגנת הסייבר על ידי המדינה, כאשר הרשות הלאומית להגנת הסייבר תהווה גורם מסדיר בתחום זה, בדגש על הסדרת שוק שירותי הגנת הסייבר. בתוך כך, יקודמו ויתואמו שיתופי פעולה מקצועיים בגיבוש הרגולציה עם רגולטורים וגורמים מנחים בתחום הסייבר, רגולטורים ומובילים מגזריים, מכון התקנים, חברות ויועצים וגופי רגולציה ותקינה בעולם.

יצוין כי האסדרה, שאותה המדינה מעוניינת ליצור בתחום הגנת הסייבר, אינה שונה בבסיסה מאסדרות בנושאים אחרים, כגון בטיחות ואיכות סביבה. האסדרה המדינתית מהווה מחויבות של המדינה כלפי הציבור והמשק לאיזון הנדרש בין מרכיבים שונים, לרבות מניעת סיכון לחיי אזרחים, יציבות כלכלית, טובת וזכויות האזרח, מניעת נזק מדינתי מערכתי, קידום ושיפור הרמה המקצועית, מניעת כשלי שוק וכדומה.

מטרת הצעת ההחלטה הנוכחית הינה לקדם אסדרה לאומית בהגנת הסייבר ולפעול להובלה ממשלתית בהגנת הסייבר, כחלק מיישום האסדרה הלאומית וכמהלך של דוגמה לציבור ולמשק.

ההצעה מורכבת משני סעיפים ראשיים –

סעיף 1 – האסדרה הלאומית בהגנת הסייבר.

סעיף 2 – ההובלה הממשלתית בהגנת הסייבר.

להלן פירוט דברי ההסבר בהתאם לסעיפי הצעת ההחלטה:

<u>סעיף 1 – האסדרה הלאומית בהגנת הסייבר</u>

האסדרה הינה אחד המאמצים המרכזיים בהגנה הלאומית בסייבר.

תפיסת האסדרה הינה תפיסה לאומית כוללת לתחום הגנת הסייבר, שתכליתה לתת מענה למצב הקיים בו כל אדם יכול להציג ולהגדיר את עצמו כמומחה להגנת הסייבר או למכור מוצר המוצג כמוצר להגנת הסייבר או להציע שירותים המוצגים כשירותי הגנת הסייבר. כמו כן, לתת מענה לכך שלמעט תחומים כגון תשתיות קריטיות ומגזרים וארגונים ספציפיים, רוב המשק פועל בתחום הגנת הסייבר באופן לא מוסדר ולא מחייב.

על מנת להסדיר את הפעילות המדינתית, ייעשה שימוש בכלי רגולציה מגוונים, לרבות חוקים, החלטות ממשלה, הוראות ותקנות, תקנים, מנגנוני הסמכה, תמריצים ישירים ועקיפים, מנגנוני הטלת אחריות אזרחית ופלילית ומנגנוני פיקוח ואכיפה.

השימוש במגוון רחב של כלים למימוש האסדרה יאפשר מתן מענה מקיף, בהיבט כיסוי מושאי הרגולציה ופעילויות ההסדרה הרלוונטיות עבורם. יודגש כי השימוש בכלי הרגולציה ייעשה, בין היתר, בהתאם לחשיבות הנושא, היקפו, הדינאמיות וקצב השינויים בתחום, שיטת היישום ואפשרויות האכיפה. בנוסף, הרגולציה תפותח על בסיס תשתית עובדתית

מקצועית שתבחן את הצורך ואת שיטת ומידת ההתערבות היעילה ביותר.

הרגולציה תחול על ארגונים בישראל וכן על מוצרים ושירותים המיובאים לישראל או ניתנים בה. הרגולציה תאומץ על ידי משרדי הממשלה וגופי הסמך שלה ותחול על ארגונים וחברות, על נותני שירותים בתחום הגנת הסייבר ועל ספקים של מוצרי הגנת הסייבר. מאחר שהרגולציה חלה על גורמים מחוץ למגזר הממשלתי, הפעילות העוקבת להחלטת ממשלה זו, והנגזרת גם היא מן התפיסה, הינה חקיקת חוק.

החוק הינו המהלך המרכזי והמחייב בתחום אסדרת הגנת הסייבר אשר יהווה מעטפת מקצועית רחבה לתחום זה, תוך הסתמכות על מהלכי חקיקה בעולם ותוך מניעת כפילויות וסתירות עם תקנות, הנחיות ותקנים הקשורים לתחום הגנת הסייבר. החוק יהיה "קו פרשת מים" שלאחריו העיסוק והטיפול הרגולטורי-מערכתי בהגנת הסייבר במדינת ישראל יהיה מוסדר, ברור ומחייב.

היות שהעיסוק בתחום הרגולציה מחייב הסתמכות על ידע מקצועי רחב, עמוק ומעודכן, נדרש לבנות במדינה בסיס ידע תשתיתי ועל-מגזרי התומך בפעילות הרגולטורית ובקביעת המדיניות המקצועית התומכת באסדרה כלפי שוק הגנת הסייבר מחד גיסא וכלפי הארגונים ומערכותיהם, מושאי ההגנה, מאידך גיסא. בסיס ידע זה יהווה תשתית לעיצוב מדיניות וכן ישמש גורמים רבים נוספים, לרבות גורמי ההכוונה, חברות, יצרנים, ספקים וכלל הגורמים העוסקים בהגנת הסייבר ברבדים השונים.

אכיפת האסדרה כלפי אנשי המקצוע[7], השירותים המקצועיים ומוצרי הגנת הסייבר, דורשת הקמת יחידה להסדרת שוק שירותי הגנת הסייבר שתפעל ותסמיך בתחום זה באופן רוחבי כלפי שוק זה (ספקים, יצרנים, חברות ייעוץ, אנשי מקצוע, מוסדות הכשרה והסמכה וכדומה). היחידה תפעיל סטנדרטים ראויים בתחום הגנת הסייבר ותוודא מימושם כלפי הגורמים הפועלים בשוק שירותי הגנת הסייבר, תוך קידום השקיפות ושיתוף המידע לציבור באשר לרמת האיכות המקצועית של השירות הניתן, על בסיס מנגנוני מדרוג מוגדרים ונגישים. יחידה זו תפעל בכפיפות לרשות הלאומית להגנת הסייבר ותפעל בתיאום ובשיתוף עם גופים ומשרדים רלוונטיים (כגון משרד הכלכלה). סמכויותיה יוגדרו ויוסדרו במסגרת החקיקה הצפויה שתאפשר הרחבת פעילותה כגורם לאומי הפועל באופן רוחבי מול שוק שירותי הגנת הסייבר.

הארגונים נדרשים לקיים הגנה הולמת בסייבר כלפי מערכותיהם באופן מידתי ומותאם לרמת הנזק שעלולה להיגרם כתוצאה מהפגיעה בהן. לשם כך, הם זקוקים לכח אדם מקצועי, מוצרים מאושרים להגנת הסייבר ושירותים מקצועיים המוצעים בשוק שירותי הגנת הסייבר.

הארגונים במשק משוייכים בחלקם למגזרים (בית חולים לדוגמה משוייך למגזר הבריאות), ובחלקם אינם משוייכים באופן מובהק למגזר. על מנת ליישם הגנה הולמת בסייבר בכלל המגזר, נדרש לחזק את משרדי הממשלה ולשם כך יוקמו או יחוזקו (היכן שקיימות) יחידות

---

[7] לצורך הגדרת המקצועות בתחום הגנת הסייבר הוקמה ועדה ציבורית בראשות האלוף (במיל.) עמי שפרן אשר המליצה להגדיר ארבעה מקצועות (מגן קיברנטי בכיר, מגן קיברנטי, מומחה חדירה קיברנטית ומומחה תחקור קיברנטי).

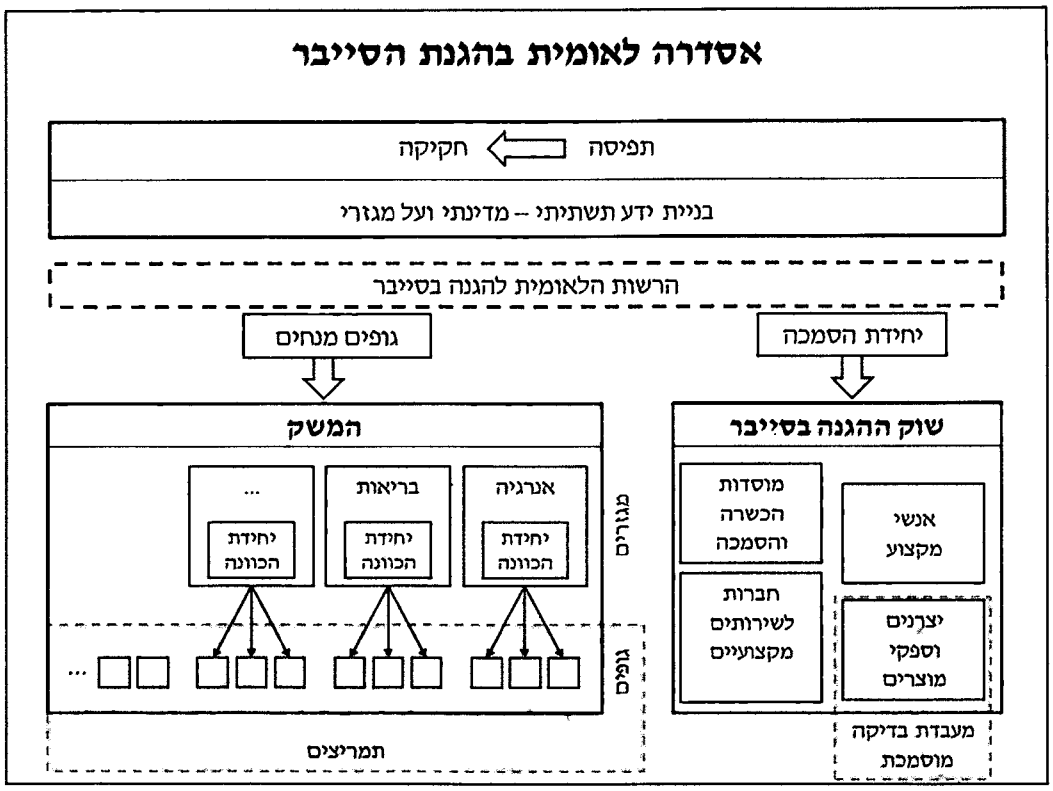
להכוונת הגנת הסייבר במשרדים הממשלתיים שיכווינו ויפקחו על מימוש הגנת הסייבר בגופים המשוייכים למגזרם. כדי שיחידות אלו יוכלו להסדיר באופן יעיל את הגנת הסייבר של הגופים המצויים בתחום אחריותם, נדרש לחזקם בהיבטי ידע וכח אדם מקצועי ולהגדיר באופן ברור את סמכויותיהם.

על המשרדים לקיים תהליך סדור של מיפוי מושאי ההגנה, תכנון תכנית להגנה, מימוש ובקרה על התכנית, הפעלת מנגנוני פיקוח ותמרוץ פנים מגזריים וכן בנייה והפעלת תהליכי שיתוף מידע פנימיים וחיצוניים.

בהקשר זה, יוזכר כי למשרדי הממשלה סמכויות חוקיות כלפי הגופים שבתחום אחריותם בהיבט המקצועי. כדוגמה לכך, רגולטורים רשאים להתקין תקנות למגזר הרלוונטי וכן להפעיל, בחלק מהמקרים, מנגנוני רישוי לחברות. במסגרת זו, רגולטורים אלו יכולים להתנות רישוי חברות בעמידה ברגולציית הגנת הסייבר.

יודגש כי היקף הפעילות בתחום הסייבר אינו אחיד בין המגזרים השונים. רמת האיום הנשקפת למגזר מסויים אינה בהכרח דומה למגזר אחר. כפועל יוצא, נדרש לבנות את יחידות הכוונת הגנת הסייבר במשרדים הממשלתיים בהתאמה להיקף פעילותן הנדרש בתחום הגנת הסייבר.

על מנת להטמיע במשק את האסדרה בתחום הגנת הסייבר ובמקביל לתהליך החקיקה, ישנה חשיבות לבניית מנגנוני סיוע, עידוד ותמרוץ ממשלתיים לארגונים שיקדמו ויטמיעו באופן הולם את הרגולציה (לדוגמה יתרון במכרזים וסובסידיות). על אף העובדה כי הארגונים מעוניינים, על פי רוב, לטפל בהגנת מערכותיהם, הרי שהדבר כרוך בעלויות. מאחר שקיים גם אינטרס מדינתי רחב בכך שהארגונים ומערכותיהם יקיימו רמת הגנה הולמת (בהיבטים כגון – שמירה על יציבות כלכלית, טובת וזכויות האזרח ושמירה על פרטיות המידע הנוגע אליו, מניעת כשלי שוק וכדומה), ראוי שהמדינה תיבנה מנגנוני סיוע ותמרוץ לקידום האסדרה ולהטמעתה.



תרשים 1 – תיאור סכמטי של מרכיבי האסדרה הלאומית בהגנת הסייבר

<u>סעיף 2 – ההובלה הממשלתית בהגנת הסייבר</u>

ממשלת ישראל, על משרדיה השונים ויחידות הסמך בה, מהווה גורם מרכזי ובעל חשיבות במשק הישראלי.

לפיכך, ההובלה הממשלתית בהגנת הסייבר תהווה קטר למשק ותשמש גורם ראשון ומוביל ביישום האסדרה הלאומית בסייבר. זאת, הן כמהלך של דוגמה לציבור והן מכיוון שהפעילות במגזר זה (בזכות גודלו ומרכזיותו) צפויה להניע פעילויות נוספות במשק ולגרור אחריה גורמים נוספים במגזר הציבורי והפרטי.

פעילות הממשלה בתחום הגנת הסייבר כלפי משרדיה וגופיה, דורשת הקמת יחידה להגנת הסייבר בממשלה והגדרה ברורה של סמכויותיה כלפיהם. יחידה זו תפעל כגורם מכוון ומנחה כלפי המגזר הממשלתי, תבקר ותוודא מימוש הנחיותיה במשרדי הממשלה וביחידות הסמך, תוודא קיום מנגנוני דיווח והעברת מידע ותיזום פעילויות תשתיתיות ורוחביות לקידום הגנת הסייבר במגזר זה.

ההובלה הממשלתית בהגנת הסייבר תיושם באופן הדרגתי ומותאם במשרדי הממשלה.

משרדי הממשלה שונים זה מזה ברמת המענה הניתן בהם כיום לתחום הגנת הסייבר. ישנם משרדים שהתהליך אצלם, בהיבטי תקינה ארגונית לדוגמה, כבר בעיצומו. מנגד ישנם משרדים שעדיין לא הניעו פעילות משמעותית בהיבט ההיערכות לאיומי הסייבר.

כדי לקדם את ההובלה הממשלתית בהגנת הסייבר יש לטפל בהעלאה ובחיזוק רמת הגנת הסייבר במשרדי הממשלה השונים.

לפיכך, כשלב התחלתי הכרחי, על כל משרד לבנות אצלו תשתית ארגונית התומכת בפעילות ההגנה.

פונקציה מרכזית ובעלת משמעות רבה בהקשר זה, הינה נושא משרה שיוגדר כממונה על הגנת הסייבר במשרד הממשלתי, אשר ינהל וירכז את מכלול הפעילויות הארגוניות בתחום הגנת הסייבר. גורם זה צריך להיות בעל מעמד ארגוני, כדי שמידת השפעתו הארגונית תהיה הולמת וכדי שתהיה לו היכולת לתאם בין הגורמים השונים העוסקים והמשפיעים בהיבטים של קידום הגנת הסייבר בארגון. גורם זה אינו בהכרח בעל הידע המקצועי הטוב ביותר בארגון, אך הוא צריך להכיר את הפעילות הארגונית הנעשית בתחום זה ולוודא כי היא מתקיימת בהתאם למדיניות ולתכניות העבודה שאושרו על ידי המנכ"ל.

נדבך נוסף, בהקשר של בניית התשתית הארגונית התומכת בפעילות ההגנה, הינו הקמת ועדת היגוי משרדית, בראשות המנכ"ל, שתתכנס באופן עיתי ושתהווה את הסמכות הגבוהה ביותר במשרד הממשלתי, המבקרת את הפעילות הנעשית בתחום הגנת הסייבר במשרד. ועדה זו יכולה להוות כר מתאים לתיאום בין גורמים ארגוניים שונים, לפתרון מחלוקות מקצועיות, לקבלת החלטות עקרוניות ולהכוונת מדיניות ארגונית.

לא ניתן לקיים הגנה יעילה בסייבר ללא הקצאת תקציב הולמת. נדרש כי חלק מוגדר משיעור התקציב המוקצה לפעילות ה-IT הארגוני, יוקצה עבור אבטחת המידע והגנת הסייבר[8]. ללא הקצאה סבירה ומתאימה לנושא, קיים תמיד הסיכון כי הארגון לא יממש פתרונות IT הולמים לאיומי הסייבר עקב תעדוף פנימי בתחומי ה-IT השונים.

בהקשר זה יצויין כי יש צורך גובר בהשקעה ייעודית ובשריון משאבים בשל מתאר האיומים על המגזר הממשלתי, בשל הצורך בריכוז מאמץ כדי לשפר את המצב בחלק ממשרדי הממשלה, ובשל הצורך ליצור שינוי משמעותי במסגרת ההובלה הממשלתית.

עוד יצויין כי במסגרת התקציב המשוריין לנושא זה הכוונה היא לכלול את כל ההשקעה הישירה והעקיפה שיש בה כדי לתרום להגנת הסייבר, ובכלל זה העסקת יועצים לצורך הסמכה ארגונית, ביצוע ביקורות אבטחת מידע וכדומה, בין אם מדובר ברכש IT ובין אם באמצעים משלימים.

לאחר הנחת התשתית הארגונית, ניתן לקדם בפועל את הגנת הסייבר בארגון ולקיים תהליך שיטתי ורציף של שיפור רמת הגנת הסייבר.

אחת הפעילויות המרכזיות בתחום זה הינה קידום תהליך להסמכה ארגונית בהתאם לתקינה הקיימת בתחום אבטחת המידע הארגוני. מהלך זה יחייב את הארגון לבצע תהליך מתודולוגי מוגדר ושקוף, לניהול מערכת אבטחת המידע אצלו. כך לדוגמה, על הארגון להגדיר מדיניות,

---

[8] בהתאם לסקר של GARTNER משנת 2013, טווח ההשקעה באבטחת מידע ממכלול תקציב ה- IT הממוצע הוא 5.1% כאשר, הוא עשוי להגיע גם עד 12%.
Measures: Current Year IT Key Metrics Data 2014: Key IT Security

לקיים תהליכי הגדרת נכסי מידע, ניהול סיכונים ובניית תכניות עבודה להגנה מתוך גישה הממוקדת בטיפול בפערים ובשיפור תהליכים. העמידה בתקנים ארגוניים תגרום למצב שבו המשרדים והגופים בממשלה ימסדו ויסדירו את פעילויותיהם בתחום אבטחת המידע ובכך יטפלו באופן שיטתי ומוסדר יותר בסיכוני אבטחת המידע ובמענים הארגוניים הנדרשים.

משפחת ת"י ISO 27001 הינה אוסף של תקנים בינלאומיים שאומצו גם כתקינה ישראלית הניתנים להתעדה גם במדינת ישראל. תקנים אלו מוכרים בעולם ובעלי יכולת התאמה לארגונים רבים. יישום תקינה זו מאפשר שימוש במנגנונים קיימים במשק הישראלי (תקינה ישראלית, יועצים המתמחים בהכנה לתקן, מערכת בדיקה והתעדה וכדומה) וכן מאפשר פעילות מקבילה ומותאמת למשרדי הממשלה השונים וליחידות הסמך.

אנשי המקצוע המועסקים בממשלה ועל ידי הממשלה בתחום הגנת הסייבר צריכים להיות ברמה מקצועית גבוהה, על מנת שיוכלו למלא את תפקידם באופן מיטבי. לפיכך, ברי כי איוש אנשי מקצוע ברמה גבוהה בתחום זה ומתן סמכויות ומרחב פעולה מקצועי בתוך הארגונים הינו מרכיב קריטי במימוש הגנת הסייבר הארגונית. בתוך כך, חשוב שיוגדר ויפעל הגורם בעל הידע, היכולות והסמכות לתכנן את מערכי הגנת הסייבר בארגון, לצידו יפעלו הגורמים בעלי ההתמחות ביישום ההגנה בפועל ברכיבי החומרה והתוכנה המוטמעים במערכות הארגון. גורמים בעלי כישורים מקצועיים ספציפיים (כגון מומחה בדיקות חדירת מערכות או מומחה לתחקור אירועי סייבר), יפעלו בגופים בהתאם לצורך.

בהתאם לדו"ח הוועדה הציבורית להגדרת מקצועות הגנת הסייבר, אשר הגישה את המלצותיה למטה, הידע של מגן קיברנטי בכיר צריך ליצור בסיס תיאורטי איתן לתכנון מערכות הגנת הסייבר ולהתעדכנות מקצועית בלימוד אישי, שכן מדובר בנושא דינמי ומתפתח, המשתנה לבקרים. הדרישות המוצעות בדו"ח הוועדה למקצוע "מגן קיברנטי בכיר" כוללת דרישה להכשרה אקדמית שתבטיח העמקה מקצועית, היכרות מעמיקה וידע תיאורטי מקיף.

מרכיב נוסף ובעל חשיבות גבוהה הינו איכות מוצרי הגנת הסייבר המוטמעים במערכות הארגון.

מוצרי הגנת הסייבר המוטמעים במערכות המחשוב של הממשלה צריכים לעמוד בסטנדרטים מקצועיים שיאפשרו הגנה טובה והולמת על מערכות הממשלה, לרבות על המערכות שהוגדרו כמערכות רגישות או בעלות חשיבות. לפיכך, הממשלה צריכה לרכוש מוצרי סייבר המספקים רמת אבטחה הולמת על פי תקן מקצועי, היכן שהדבר הוגדר.

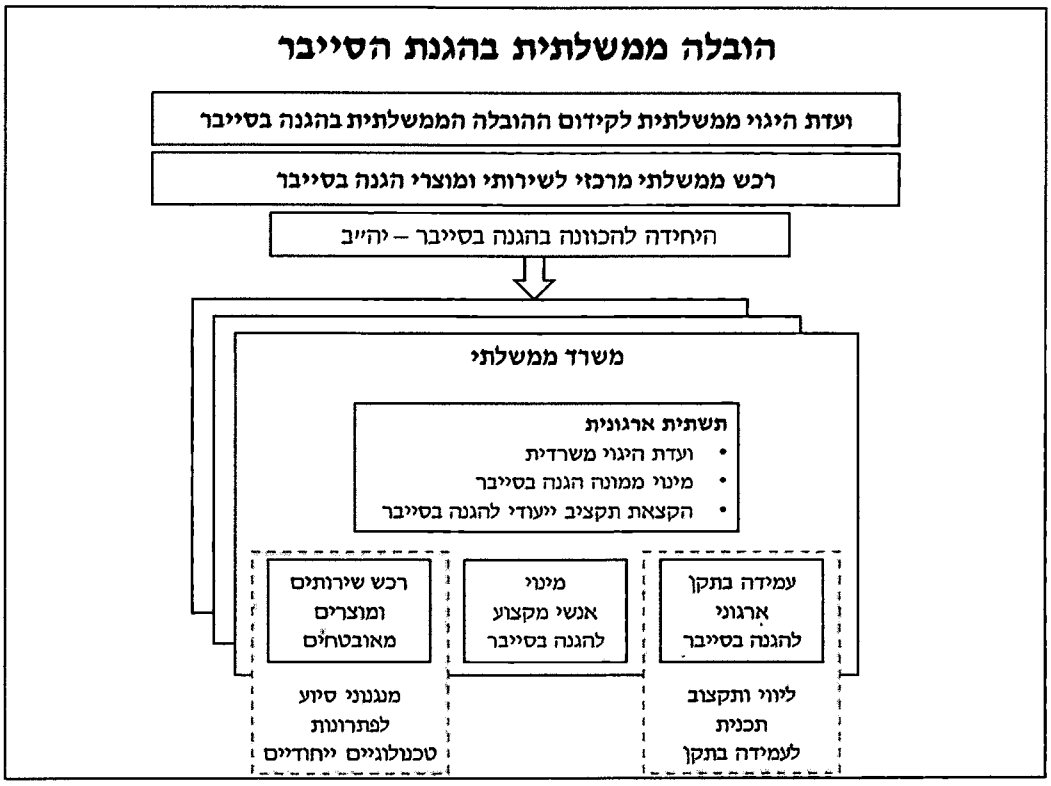
תקן מקצועי נפוץ בעולם בתחום הינו תקן Common Criteria (שאומץ גם כתקן ישראלי – ת"י ISO 15408) העוסק בהסמכת מוצרי אבטחת מידע והגנת הסייבר בהתאם לדרישות מקצועיות מוגדרות ולתהליך הכולל בדיקות מעבדה מוסמכת. הסמכת המוצרים מתבצעת בהתאם למדרג של רמות בדיקה. יצרני תוכנה וחומרה המעוניינים בקבלת התקן נדרשים לפעול בהתאם לתהליך מוסדר ושיטתי מול גורמי הסמכה במדינות בהם קיימת מערכת לטיפול בתקן ומול מעבדות מוסמכות הבודקות את המוצרים בהתאם להגדרת דרישות אבטחה ברורות ובמתודה מוגדרת ומתועדת היטב. קבלת התקן מעידה כי המעבדה שבדקה

את המוצר מאשרת כי התכונות האבטחתיות הנדרשות במפרט הבדיקה נבדקו בהתאם להגדרה של השיטה ופרוטוקול הבדיקה.

גורמים המעבירים מידע ממוחשב או ספקים של מערכות מחשוב לממשלה והמשתתפים במכרזים בתחום זה, צריכים גם הם לעמוד בתקני אבטחת מידע ארגוניים. על מנת שמערכות הממשלה תהיינה מוגנות, נדרש כי התוצרים המסופקים לממשלה לא יהוו סיכון כלפי מערכות הממשלה וייוצרו בסביבה מוגנת. למותר לציין כי בהקשר זה מערכות ממוחשבות המקושרות למערכות הממשלה צריכות גם הן לפעול בתוך מערכת מוגנת ברמה הולמת.

יודגש כי הדרישות המפורטות בהחלטת ממשלה זו הינן בבחינת רמה בסיסית בהגנת הסייבר. פעילויות נוספות במשרדי הממשלה, ראוי שתבוצענה בהתאמה לצרכים ולאיומים הייחודיים במשרדים השונים.

מאחר שהפעילות בממשלה צריכה להיות מבוקרת גם בראייה ממשלתית כוללת, נדרש למסד מנגנון מרכזי שיתכנס באופן עיתי שתפקידו לעקוב ולבקר את פעילות הממשלה בתחום זה. בהקשר זה, הצעת החלטה זו עוסקת גם בהקמת ועדת היגוי ממשלתית, בראשות ראש המטה הקיברנטי הלאומי, המורכבת מנציגי משרדים ממשלתיים ומגופים מקצועיים העוסקים בתחום. הוועדה תדווח לממשלה על פעילותה, על מימוש תכניות העבודה, על הפערים ועל צירי הפעילות במשרדים השונים ותפעל באופן שיטתי ורציף לקידום ההובלה הממשלתית בהגנת הסייבר. בתוך כך, תפעל הוועדה גם לסיוע למשרדי הממשלה למימוש פתרונות טכנולוגיים מתקדמים לצרכים ייחודיים.



תרשים 2 – תיאור סכמטי של מרכיבי ההובלה הממשלתית בהגנת הסייבר

תקציב

כמפורט בגוף ההחלטה.

עמדת שרים אחרים שההצעה נוגעת לתחום סמכותם

שר הכלכלה – תומך

שר האוצר – תומך

החלטות קודמות של הממשלה בנושא

החלטה מספר 3611 מיום 07.08.11 בנושא "קידום היכולת הלאומית במרחב הקיברנטי"

החלטה מספר 1886 בק/9 מיום 20.3.1997 בנושא "הקמת ועדת היגוי לנושאי מחשוב בכל משרד ממשלתי"

החלטת מספר 2118 מיום 22.10.14 בנושא "הפתתת הנטל הרגולטורי – דיון בהחלטת ועדת השרים לענייני חברה וכלכלה מס. חכ/39 מיום 14.19.14"

סיווגים

סיווג ראשי: 01ביצועי

סיווג משני: 02הצהרתי

תחום פעולה עיקרי: 01חוץ וביטחון

מוגש על ידי ראש הממשלה

י' בטבת התשע"ה
01 בינואר 2015

Prime Minister's office

משרד ראש הממשלה

היועצת המשפטית

ירושלים, ט' טבת, התשע"ה

31 בדצמבר, 2014

מזהה מלי: D355683

חוות דעת משפטית הנלווית להצעת החלטה לממשלה ולוועדות השרים

נושא הצעת ההחלטה: קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר

תמצית ההצעה בהתייחס להיבטיה המשפטיים:

רקע

1. בהחלטת ממשלה 3611 מיום 07.08.2011 (להלן – החלטה 3611) הוקם המטה הקיברנטי הלאומי (להלן – המטה), במשרד ראש הממשלה. בהמשך להחלטה זו ובמסגרת תפקידיו, גיבש המטה תפיסה לאומית להגנה בסייבר.
2. עבודת מטה זו הבשילה לשתי הצעות החלטה לממשלה שמטרתן המשך קידום ויישום נושאים אלה. נושא ההיערכות האופרטיבית כלול בהצעת החלטה בנושא "קידום ההערכות הלאומית להגנה בסייבר" המובאת לממשלה במקביל להצעת החלטה זו.
3. מטרת הצעת ההחלטה הנוכחית הינה לקדם אסדרה לאומית בהגנה בסייבר ולפעול להובלה ממשלתית בהגנה בסייבר, כחלק מיישום האסדרה הלאומית וכמהלך של דוגמה לציבור ולמשק. זאת בכפוף להחלטת ממשלה מס' 2118 מיום 22.10.14, בנושא "הפחתת הנטל הרגולטורי – דיון בהחלטת ועדת השרים לענייני חברה וכלכלה מס. חכ/39 מיום 14.9.14".

האסדרה הלאומית בהגנה בסייבר

4. מרחב הסייבר הינו מרחב אזרחי ברובו, ולכן רכיב מרכזי וראשון בהעלאת החוסן בו הינה חיזוק והעלאה של ההגנה בסייבר בארגונים.
5. השיטה המוצעת לביצוע, בדומה לתחומים אחרים בהם יש סיכונים הנשקפים לפעילות, הינה באמצעות מימוש סטנדרטים מקצועיים בארגונים, ולצדם הסדרה של השירותים בתחום ההגנה (אנשי מקצוע, שירותים ומוצרים) במגוון כלים, על מנת להבטיח כי מימוש הסטנדרטים מיושם ברמה הנדרשת.
6. פעילות זאת משתלבת במגמה של השנים האחרונות של פיתוח יכולות מקצועיות ומוסדיות בקרב רשויות הרגולציה במשק לטיפול במערכות מידע ובסיכוני סייבר. המטה מלווה ומחזק מגמות אלה, ומסייע במסגרת פעילותו לפיתוח יכולות אלה.

7. על רקע זה, הצעת ההחלטה, ותפיסת הרגולציה שגיבש המטה הקיברנטי, מבקשת להתבסס על **הסדרה מגזרית** בעת הטיפול בסיכוני סייבר. זאת על בסיס עמדת מדיניות לפיה הרגולטור המגזרי המסדיר סיכוני פעילות, הינו הגורם המתאים להסדיר גם את הטיפול בסיכונים לפעילות הנובעים ממערכות ממוחשבות במגזר. יתרה מזו, יש חשיבות בעידן של ייעול הליכי הרגולציה בהפחתת של מספר רשויות ההנחיה והפיקוח הפועלות מול עסק או ארגון, בהקשר לאותה פעילות.

8. לצד הטיפול בארגונים, נדרשת העלאה רציפה של **רמת השירותים** הניתנת, על מנת שלרשות הארגונים יעמדו הכלים להיערכות. בהתאם לכך הצעת ההחלטה ממקדת את הטיפול בנושא זה באמצעות הקמה של יחידה ייעודית שמטרתה קידום סטנדרטים ראויים בתחום ההגנה בסייבר, ומימושם כלפי הגורמים הפועלים בשוק שירותי החגנה בסייבר, תוך קידום השקיפות ושיתוף המידע לציבור באשר לרמת האיכות המקצועית של השירות הניתן, על בסיס מנגנוני מדרוג מוגדרים ונגישים. יחידה זו תוקם על ידי המטה ותפעל בכפיפות לרשות הלאומית להגנה בסייבר.

9. ממשלת ישראל, על משרדיה השונים ויחידות הסמך בה, מהווה גורם מרכזי ובעל חשיבות במשק הישראלי. לפיכך, החובלה הממשלתית בהגנה בסייבר נועדה לממש את התפיסה ביישום האסדרה הלאומית בסייבר. זאת, הן כמהלך של דוגמה לציבור והן מכיוון שהפעילות במגזר זה (בזכות גודלו ומרכזיותו) צפויה להניע פעילויות נוספות במשק ולגרור אחריה גורמים נוספים במגזר הציבורי והפרטי.

10. פעילות הממשלה בתחום ההגנה בסייבר כלפי משרדיה וגופיה, דורשת הקמת יחידה להגנה בסייבר בממשלה שתפעל כגורם מכוון ומנחה כלפי המגזר הממשלתי.

11. בנוסף, כמפורט בהצעה, מוצע להניע שורה של פעולות ארגוניות, ובהן הקמת ועדת היגוי משרדית, מינוי נושא משרה בכיר האחראי לכך, שיריון תקציב לתחום ההגנה בסייבר במסגרת תקציב מערך המיחשוב, הערכות להסמכה לתקינה ארגונית בתחום ההגנה בסייבר, וכן בתחום העסקת אנשי מקצוע ורכש מוצרים.

<u>היבטים משפטיים של אסדרת ארגונים באמצעות רגולציה מגזרית</u>

12. הצעת ההחלטה נועדה לממש את התפקיד שהוטל על המטה הקיברנטי בעת הקמתו, של מימוש תקינה והסדרה לטובת העלאת החוסן במרחב האזרחי. טיפול במרחב האזרחי נעשה, בהגדרה, בדרך של הפעלת כלי אסדרה ותמריצים שמטרתם השפעה על פעולתם של הארגונים במרחב זה. בהתאם לכך, תפיסת האסדרה מבקשת לממש את ההפנמה של הצורך לטפל באיומים הנשקפים ממרחב הסייבר, בדרך של מגוון כלים רגולטורים. באופן כללי, רכיב מרכזי בתפיסת ההסדרה, כנגזרת של האמור, הוא הצורך בהסדר חקיקתי כולל. מטרת ההחלטה הנוכחית להניע את הפעילות הממשלתית לקראת הסדרה כאמור, ותוך ביצוע עבודת מטה נדרשת לכך.

13. תפיסת האסדרה מבקשת להתבסס על פעילויות רגולציה קיימות כלפי ארגונים ופעילותם במגוון תחומים שנועדו למניעה או צמצום נזקים הנשקפים מפעילותם. בנוסף היא מתבססת על מחזור החיים הרגולטורי שהינו מגזרי באופיו, הכולל את איתור הסיכונים הנשקפים, ובהתאם לכך עיצוב נורמות מתאימות, הטמעתן, ולבסוף ביצוע הליכי פיקוח ואכיפה.

14. יעד מרכזי של עבודת המטה שמבקשת ההחלטה להניע היא מיפוי משפטי וארגוני מדויק יותר, באשר לאחריות ולסמכות של כל משרד ויכולת המימוש של המשרדים את הנדרש מהם בתחום אחריותם, הקיים או העתידי, במסגרת מכלול ההסדרים החלים במגזר, ומערכת היחסים המשפטית והכלכלית המאפיינת אותו.

15. הגם שאין כל מניעה לכך שהממשלה תנחה את הרגולטורים להביא בחשבון היבטים הקשורים במימוש ההחלטה, ככל שהם בסמכותם, הרי שהיישום בפועל והמשקל שיינתן לכך לפי העניין כפוף לתכלית הרגולציה, והכל בהתאם ובמסגרת הוראות הדין הרלוונטיות.

16. בנוסף, במסגרת עבודת המטה שמבקשת ההחלטה להניע, ייבדקו מכלול ההיבטים הנוספים, כגון הפעלת סמכויות מקבילה בידי רשויות פיקוח.

17. יובהר כי אין בהחלטה כשלעצמה, בטרם קביעת רגולציה ייעודית על ידי הרגולטור הרלבנטי בהתאם לסמכויותיו, משום הטלת חובות ישירה על גופים במרחב האזרחי.

<u>היבטים משפטיים של אסדרת שוק שירותי ההגנה בסייבר</u>

18. אסדרת מקצועות, שירותים ומוצרים, צריכה להיעשות בהתאם למסגרת החוקתית החלה על חופש העיסוק בחוק יסוד: חופש העיסוק, ובחוק יסוד: כבוד האדם וחירותו.

19. לצורך בחינה יסודית ומקדמית של הצורך בטיפול בתחום מקצועות האבטחה בסייבר, מינה ראש המטה ועדה ציבורית בראשות האלוף (מילו) עמי שפרן. הועדה קובעת בהמלצותיה, בין היתר, כי:

> "הרמה המקצועית של כוח האדם שיעסוק בהגנה קיברנטית היא שתקבע את רמת ההגנה ואת היכולת להתמודד עם אירועי הגנה קיברנטית, ולכן נודעת לה חשיבות מיוחדת."
>
> ...
>
> "הוועדה הגיעה למסקנה כי העדר הכשרה מסודרת ברמה גבוהה של בעלי מקצוע והעדרה של הסמכה מקצועית המציגה וודאות באשר לרמת הכשרתם של בעלי מקצוע אלה היא כשל המהווה מכשול בפני שדרוג רמת ההגנה הקיברנטית של ארגונים בישראל. הוועדה בדעה כי נדרש לטפל בנושא זה, שכן הרמה המקצועית הגבוהה של כוח האדם היא נדבך חשוב בפיתוח יכולת ההגנה הלאומית בתחום הקיברנטי".
>
> ...
>
> "לדעת הוועדה יש בהחלט מקום שהמדינה תפעל כדי להבטיח כי המומחיות הנדרשת תעמוד לרשות המשק, כי ייבנה מערך מקצועי ברמה שתאפשר להתמודד עם האתגרים העתידיים בתחום וכי לא יחסרו בעלי מקצוע בתחום."

20. בהמשך למגמה המפורטת בדוח הוועדה הציבורית (כמתואר בדברי ההסבר להחלטה), מטרת הצעת ההחלטה הנוכחית להניע את הפעילות בתחום זה, וזאת תוך מיקוד במיסוד יחידה מקצועית לנושא זה, שתפעל לקידום המקצועות במכלול הכלים העומדים לרשותה. בהקשר זה יובהר כי יש מגוון שיטות טיפול בהעלאת רמת בעלי המקצוע, החל בהגדרת המקצועות, קביעת מסלולי הכשרה, הגדרת דרישות מקצועיות, וכמובן רישוי.

21. הפעילות שתניב החלטה זו נועדה להיות בסיס מקצועי לקידום הנושא, במגוון אפיקים, ובכפוף למגבלות המשפטיות החלות על כל אחד מהם. במסגרת זו ייבחן הצורך בתיקוני חקיקה מתאימים, ובכלל זה השלמה של המהלכים ההסדרתיים במסגרת חוק ייעודי.

<u>הובלה ממשלתית, יחידת הגנה בסייבר</u>

22. הצעת ההחלטה נועדה להניע סדרת תהליכי עבודה במסגרת משרדי הממשלה, שמטרתן מימוש התפיסה במימד הארגוני והתהליכי, כדי להעלות בצורה ניכרת את רמת החוסן של משרדי הממשלה לסיכונים קיברנטיים.

23. במימד הארגוני, מדובר בנושאים המוסדרים במסגרת כללי הפעולה ונהלי העבודה של המשרדים פנימה.

24. בנוסף, תוקם יחידה מקצועית מרכזית להכוונה והנחייה מקצועית בתחום זה עבור הממשלה, וזאת במסגרת רשות התקשוב הממשלתי.

25. מאחר שבתחום אבטחת המידע והסייבר יש גם גורמים מנחים ביחס לחלק מהפעילויות, ככל שיידרש, בנושאים שחל עליהם החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק), ובנושאים שחל עליהם חוק הגנת הפרטיות, התשמ"א-1981, תתבצע ההנחיה בתאום עם הגורם המוסמך לפי חוקים אלה.

26. במסגרת ההצעה מוטל על היחידה לבנות תהליכי שיתוף מידע בעל ערך הגנתי, וזאת במסגרת ההגנה הכוללת של מגזרי הממשלה.

27. בתחומים בהם חלים דינים ספציפיים, כגון רכש לפי דיני המכרזים, מובן כי מימוש ההחלטה ייעשה בהתאם לשיקול הדעת המנהלי והמנגנונים הקיימים ובמסגרתם ועל פי הוראות כל דין.

<u>קשיים משפטיים, ככל שישנם, ודרכי פתרונם:</u>

<u>החלטה לאחר חוק התפזרות</u>

28. הצעת ההחלטה מוגשת לאחר שהתקבל בכנסת חוק התפזרות הכנסת התשע עשרה, התשע"ה-2014 (להלן – חוק ההתפזרות). הצעת ההחלטה נבחנה בהתאם למסגרת המשפטית החלה על קבלת החלטות ממשלה לאחר קבלת חוק ההתפזרות. במסגרת זו נדרשת הממשלה לאיפוק הראוי לממשלה יוצאת, אולם עליה להבטיח יציבות והמשכיות. יש לאזן איזון כולל – בהתחשב במכלול הנסיבות – האם נדרשים איפוק או עשייה.

29. במכלול הנסיבות הקשורות בצורך הדחוף בקידום הנושא, בפערים הידועים בטיפול במרחב הסייבר האזרחי, ולנוכח היקפה של עבודת המטה שקדמה להצעת ההחלטה, נראה כי מכלול הנסיבות מניעות לעשייה, וכי הממשלה מוסמכת ויכולה לקבל את ההחלטה בעת הזו.

30. יתרה מזו, כמפורט להלן, ההחלטה עצמה מסדירה מסגרת שלמה להמשך עבודת המדיניות, ובכלל זה הכנת חקיקה מתאימה, שבתורה תובא כנדרש לאישור הממשלה בעתיד. ההחלטה נדרשת כעת על מנת להמשיך את רצף הפעילות הממשלתי ולכוונו ולא לקטוע אותו. הדברים פורטו בחוות דעת אל היועץ המשפטי לממשלה מיום 16.12.14.

<u>עמדת היועצים המשפטיים של משרדים אחרים שהצעת ההחלטה נוגעת להם:</u>

הצעת ההחלטה נוגעת לכלל משרדי הממשלה, והיא גובשה לאחר עבודת מטה במהלכה הוטמעו הערות שהתקבלו ממשרדים שונים. הנוסח העדכני של טיוטת הצעת ההחלטה, הכולל את התיקונים שנערכו, הופץ ליועצים המשפטיים לקראת הבאתה לממשלה.

עמדת היועצת המשפטית למשרד להגנת הסביבה היא כי ההצעה מעלה קשיים משפטים בשל כך שהיא מטילה על רשויות פיקוח קיימות לעסוק גם בסייבר, בעוד שאין להם את הכלים הארגונים והטכנולוגים לכך.

מוקד ההחלטה הינו בהתנעת תהליך מדיניות, שבמסגרתו ממילא ייבחנו ההיבטים המשפטיים והארגונים שאליהם מתייחסת היועצת המשפטית למשרד להגנת הסביבה.

עמדת נציג היועץ המשפטי לשירות הביטחון הכללי היא כי לא קיבל במועדה את הצעת ההחלטה. עקב כך הפנה את הח"מ להערות שנשלחו לגרסה קודמת.

הערות אלה, ככל שהן רלבנטיות להחלטה זו, עוסקות בפרק העוסק בהקמת יחידת הגנה בסייבר. לפיהן, בנוסח המוצע לא בא לידי ביטוי מעמדו של הגורם המוסמך לפי חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, בהנחיה של מערכות ממוחשבות המכילות **מידע מסווג** או הינן **תשתיות קריטיות**, ואשר פועלות במסגרת משרדי הממשלה. בהתאם לכך עולה מהערות אלה כי יש לקבוע בהחלטה כי הגורם המוסמך להנחיית יחידת ההגנה בסייבר הינו הגורם המוסמך לפי חוקים אלה. לשיטתו של נציג יועמ"ש שב"כ, על מנת לממש את תפקידו של שב"כ, עליו להנחות את כלל המערכות הממשלתיות.

לעניין הערתו של נציג יועמ"ש שב"כ, יודגש כי מירב המערכות הממוחשבות הפועלות כיום במסגרת שירות המדינה אינן מכילות מידע מסווג, ואינן תשתיות קריטיות. בהתאם לכך, אין קושי משפטי בכך שרק מקום שבו יש סמכות לגורם המוסמך, כמפורט בהחלטה, פעילותה של יה"ב תיעשה בהתאם להנחייתו. למעלה מכך, בהחלטת הממשלה בנושא "קידום ההערכות הלאומית להגנת הסייבר" מוקמת רשות לאומית להגנת הסייבר, אשר תהא אחראית על פעילות מול כלל המערכות הממוחשבות במרחב האזרחי ובכלל זה משרדי הממשלה.

<u>עמדת היועץ המשפטי של המשרד שהשר העומד בראשו מגיש את ההצעה:</u>

לאור האמור לעיל, אין מניעה משפטית לקבלת ההחלטה.

עמית אשכנזי, עו"ד

יועץ משפטי
המטה הקיברנטי הלאומי