משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

מיישם סייבר מא' עד ת'

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

תוכן העניינים

תקציר מנהלים	3
כשל השוק ותיקונו	5
תהליך בניית המקצוע	6
תיאור מקצוע המיישם	7
אשכולות ידע נדרשים	8
על מי חלה חובת ההסמכה	9
תהליך ההסמכה	9
כללים ותקנות בתחום הסייבר	10
שמירה על כשירות	10
הסמכות חיצוניות	11
תעודת הסמכה – מאגר נתונים	12
הקמת אתר תומך	12
עלויות	12
ותיקי התחום	13
ביצוע המבחן הלכה למעשה – שלבים	13

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

<u>תקציר מנהלים</u>

אסדרת מקצועות הסייבר נועדה להעלות את רמת הגנת הסייבר במדינת ישראל באמצעות קביעת רף מקצועי של העוסקים בתחום. מטרת ההסמכה להציב את ישראל בחזית העולמית של העוסקים במקצועות הסייבר.

בעקבות פרסום המסמך של מטה הסייבר הלאומי (דצמבר 2015) בנושא אסדרת מקצועות הסייבר, החלה הרשות הלאומית להגנת הסייבר להוציא לפועל את מבחני ההסמכה על פי העקרונות המופיעים מטה.

יש להדגיש כי תהליך אסדרת המקצועות בישראל בא לתקן כשל שוק במקצועות הסייבר כפי שעלה בעבודת מטה אותה הובילה הרשות.

תהליך ההסמכה הישראלי כולל שלושה נדבכים מרכזיים: מבחן עיוני, מבחן מעשי ושמירה על כשירות. הייחודיות בהסמכה הישראלית הוא הדגש על ההתנסות המעשית. בשלב הראשון ההתנסות תבוא לידי ביטוי במבחן מעשי כתנאי לקבלת ההסמכה ובעתיד השמירה על כשירות תחייב גם התנסות מעשית כתרגול ולא כמבחן.

בנוסף, תהליך ההסמכה נועד לוודא שהעוסקים בתחום הסייבר במדינה מכירים את הייחודיות של מימד הסייבר במדינת ישראל. לאור זאת תהליך ההסמכה יכלול מבחן בנושא הכולל בתוכו הכרת דיני הסייבר במדינת ישראל, האתיקה המקצועית, גופי הסייבר המדינתיים וכדי.

חובת ההסמכה הישראלית תחול בשלב הראשון על משרדי הממשלה, יחידות הסמך וגופי התמ"ק.

ובהמשך לאחר הצלחת השלב הראשון תיבחן האפשרות להרחיב את יישום ההסמכה הישראלית גם למגזרים נוספים ע"פ מדיניות שתקבע הרשות הלאומית להגנת הסייבר.

הרשות תקיים מבחני הסמכה לחמשת המקצועות המופיעים במסמך אסדרת המקצועות תוך בחינה מתמדת של מקצועות נוספים, תיקוף והתאמה לשינויים במרחב הסייבר.

<u>תהליך קבלת ההסמכה – מיישם סייבר</u>

ההסמכה בנויה ממבחן עיוני ומעשי המתקיימים ברצף כאשר חלוקת הניקוד היא:

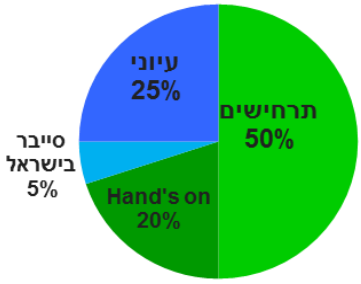
מבחן עיוני – 25%.

מבחן כללים ותקנות בתחום הסייבר בישראל – 5%.

תרחישי Hand's on – 20%

התמודדות עם תרחישים – 50%.

הציון העובר הוא 80%.



כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

<u>שמירה על כשירות</u>

שמירה על כשירות תתבצע אחת לשלוש שנים מתום מועד המבחן כאשר האפשרויות העומדות בפני בעל ההסמכה הן: מבחן שמירה על כשירות או צבירת "נקודות זכות" במשך שלוש השנים עד לרף שקבעה הרשות (כנהוג בהסמכות בינ"ל מובילות).

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

<u>הוכחת כשל שוק</u>

כחלק מתפיסת ההסמכה הובילה הרשות הלאומית להגנת הסייבר בדיקה עם מומחי סייבר ישראלים ועולמיים ברשויות השונות, באקדמיה, בתעשיה ובמחקר באשר לכשלי שוק. לאורך התהליך התקיימו פגישות עם גורמי חוץ המתמודדים עם אותו אתגר.

במחצית 2016 הוציאה מקאפי, בשיתוף מרכז המחקר CSIS מחקר בנושא חוסר בינ"ל במקצועיותם של אנשי אבטחת המידע ורגולציה שבוצעה במהלך המחצית הראשונה של 2016. המחקר נערך בקרב 8 מדינות מובילות בתחום הסייבר: ישראל, אוסטרליה, צרפת, גרמניה, יפן, מקסיקו, בריטניה וארה"ב. יש לציין כי המחקר התבסס על מידע זמין לציבור, ראיונות עם מומחים וסקרים במגזר הפרטי והממשלתי בכל מדינה.

מהמחקר עולה שישנו כשל שוק במקצועיות/ כשירות של האנשים העוסקים במקצועות הסייבר. לדעת עורכי המחקר בעיה זו רק הולכת ומחריפה. אחת הסיבות להמשך (והחרפת) הבעיה הביקוש מחד והמחסור מאידך באנשי הסייבר, מחסור אשר גדל והולך. כתוצאה ממצב שוק זה, ביקוש גדול לעומת היצע נמוך, יכנסו לשוק עובדים בעלי רמת ידע נמוכה בתחום. המחקר של מקאפי תומך את התפיסה של הרשות הלאומית להגנת הסייבר.

להלן מס' נקודות שעלו במחקר:

1. 82% מהנשאלים ענו שיש בעיה במקצועיותם של אנשי אבטחת המידע.
2. 25% מהנשאלים טענו שחוסר מקצועיות של אנשי אבטחת המידע הוביל לפגיעה במוניטין של הארגון ולאיבוד בסיסי נתונים במהלך תקיפות סייבר.
3. רובם המוחלט של הנשאלים טען כי טכנולוגיה יכולה לפצות חוסר מיומנות של אנשי אבטחת המידע.
4. חלק גדול מהחברות טענו כי נגרם להם נזק כבד מחוסר המיומנות של אנשי אבטחת המידע.
5. **75% מהנשאלים תלו את האשמה של חוסר המקצועיות של אנשי אבטחת המידע בממשלה.**

לדעת עורכי המחקר הפתרון נמצא באחריות הממשלות. **בין השאר דורש הפתרון התווית שיפורים בתוכניות הכשרה של אנשי מקצוע אבטחת המידע.** בראיית עורכי המחקר המדינה היא האחראית על הכשרת אנשי המקצוע העוסקים בתחום או לכל הפחות פיקוח על רמת הידע שלהם והתערבות במקרה הצורך.

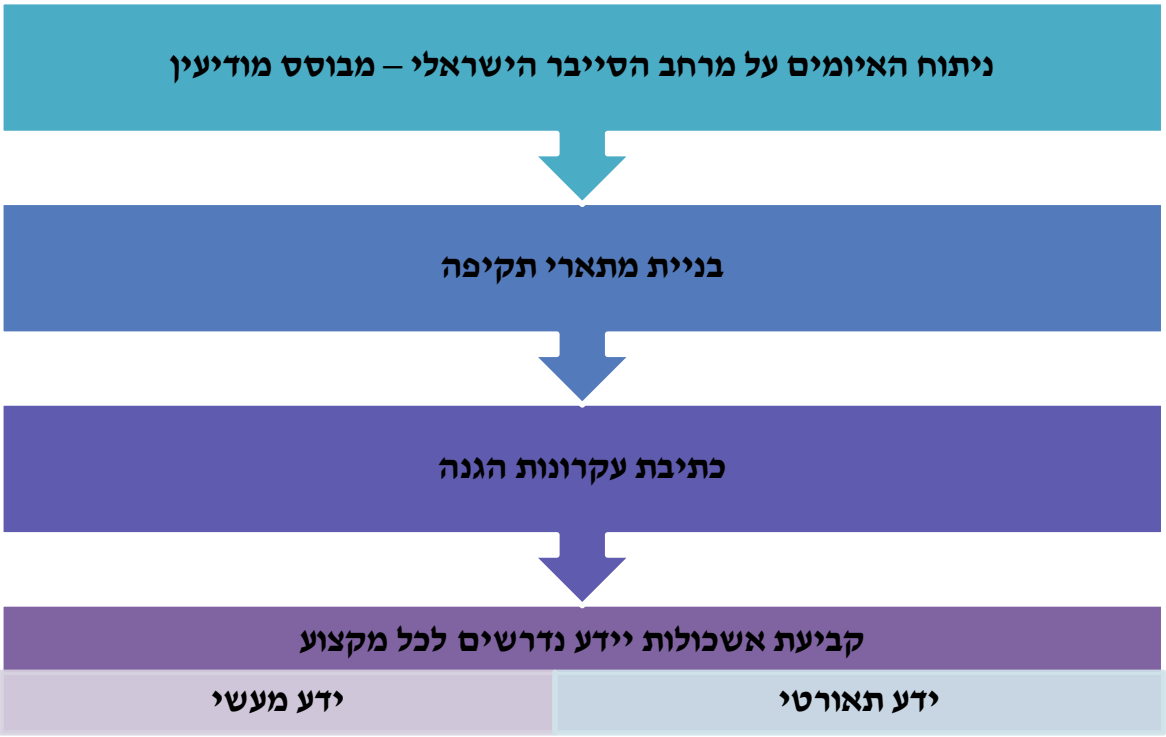
מחקר זה מתיישב עם תפיסת העבודה של הרשות הלאומית להגנת הסייבר. כחלק מתפיסת העבודה החלה הרשות הלאומית להגנת הסייבר תהליך של אסדרת המקצועות הבא לתת מענה על כשלי שוק אלו מכמה כיוונים:

1. הרשות הלאומית להגנת הסייבר תקיים מבחני הסמכה לבדיקת רף מקצועי לעוסקים במקצועות הסייבר ובכך תמנע כניסתם של אנשים בלתי מקצועיים לעיסוק בתחום.
2. כחלק מתהליך אסדרת המקצועות יידרשו העוסקים בתחום ל"שמירה על כשירות" על פי דרישות הרשות . בדרך זו מבטיחה הרשות הלאומית להגנת הסייבר שהעוסקים בסייבר יישארו מעודכנים ורלוונטיים להשתנות השוק המהירה המאפיינת את תחום הסייבר.

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

<u>תהליך בניית המקצוע</u>



האיומים על מרחב הסייבר האזרחי הישראלי נעים בתוך המנעד אשר בקצותיו יש מצד אחד הריגול העסקי ומהצד השני הרצון לפגיעה במדינת ישראל באמצעות הסייבר.

הרצון לפגוע במדינת ישראל יכול להתבצע בשני רבדים עיקריים:

1. פגיעה בתשתיות עד כדי השבתתם בדגש על תשתיות קריטיות וגורמי ממשל חיוניים.
2. פגיעה תודעתית שמטרתה ערעור תחושת הביטחון של האזרח בעיקר ע"י הדלפת מאגרי מידע וכד'.

יש להדגיש כי רובו של החומר עליו מתבצעת העבודה הינו חומר מודיעיני רגיש ולכן אין כאן המקום להרחיב עליו.

בשרשרת ההגנה על ארגון לכל אחד ממקצועות הסייבר יש תפקיד ייעודי.

את תפקידי ההגנה אפשר לחלק גם על ציר זמן התקיפה:

1) לפני התקיפה - ניהול שגרה המבוססת על שמירת ביטחון מידע מקסימלית אשר מאפשרת לארגון להתנהל בצורה מיטבית, טיוב מערכות ההגנה של הארגון לזיהוי תקיפה והכנת הארגון להתמודדות אתה.
2) במהלך התקיפה – זיהוי התקיפה בצורה המהירה ביותר, מניעת התפשטות התקיפה בארגון / לארגונים אחרים, הכלתה ועצירת התקיפה.
3) לאחר התקיפה – תחקור התקיפה, מציאת כשלי ההגנה אשר סייעו / אפשרו את התקיפה, תיקון הכשלים והפקת הלקחים.

יש להדגיש כי לכל מקצוע יש את מקומו הייחודי בציר הזמן ובהתאם לכך נגזר לכל מקצוע את אשכולות הידע הנדרשים לו באופן ספציפי.

<u>תאור מקצוע מיישם הסייבר</u>

מיישם הסייבר הוא האחראי בשגרה על תפעולן התקין של מערכות הגנת הסייבר בארגון. בארגון (כל ארגון) ישנם שני סוגי מיישמים.

1. מיישם טכני.
2. מיישם סייבר.

בעוד שהמיישם הטכני אחראי על מערכות ה-IT והתקשורת של הארגון, מיישם הסייבר אחראי על מערכות ההגנה שבו. אמנם, קיימות מערכות הגנה גם בשכבות התקשורת וה-IT של הארגון המגנות עד רמת הפרט, אולם מערכות ההגנה של מיישם הסייבר נמצאות ברובד הכלל ארגוני ומכאן נובעת חשיבותן הרבה.

הואיל וקיימים ארגונים (בעיקר ארגונים קטנים) בהם אותו אדם יעשה את שני התפקידים. יחד עם זאת ברמה התפיסתית שני התפקידים הם תפקידים שונים.

ייחודו של מיישם הסייבר הוא בכך שמחד הוא איש Hands-on המעורה בפרטים הקטנים ביותר של הארגון ומאידך צריך לראות את צרכי הארגון ואיך לצד אחריותו על שמירת אבטחת המידע הוא אינו מפריע להתנהלותו השוטפת והתקינה של הארגון.

לאור ייחודו של המיישם הוא נדרש להתמקצע במספר רבדים, האחד הוא היכולת להפעיל מערכות הגנה והשני הוא הכרה של כלל הארגון בהיבטי אבטחת מידע.

עבודתו של המיישם מחולקת לשני רבדי זמן עיקריים:

1. טרום התקיפה – בניית חוסנו של הארגון (כחלק מכלל בעלי התפקידים) תוך שימת דגש על טיוב מערכות ההגנה כחלק מתהליך העבודה השוטפת של הארגון.
2. במהלך התקיפה – זיהוי התקיפה בצורה המהירה ביותר, הכלתה ומניעת הדרדרות עד להגעת צוותי ההתערבות (במקרה הצורך).

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

<u>אשכולות ידע הנדרשים ממיישם הסייבר</u>

1 מבוא לאבטחת מידע והגנת הסייבר
2 תקני אבטחת מידע וניהול סיכונים
3 מבנה מחשב
4 יסודות מערכות הפעלה
5 יסודות תקשורת מחשבים
7 הגנת גישה בתקשורת ואינטרנט
8 בידול והפרדת רשתות תקשורת
9 היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע
10 הצפנה ואימות
11 בקרת גישה
12 היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים
13 היבטי אבטחת מידע במסדי נתונים
14 תוכנות זדוניות וזיהוי אנומליות
15 דלף מידע
16 ניהול ורישום אירועי אבטחת מידע (Audit)
17 טיפול באירועי אבטחת מידע
18 מחשוב ענן, שירותי אירוח, וירטואליזציה
19 שינוע מידע מ/אל הארגון
20 המשכיות עסקית (BCP/DRP)
21 אבטחה אפליקטיבית
22 מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה)
23 חוק ואתיקה
24 אבטחה פיסית
25 התנסות מעשית התומכת את הידע התאורטי

<u>על מי חלה חובת ההסמכה</u>

אסדרת המקצועות תחול בשלב הראשון על המגזר הממשלתי:

1. עובדי סייבר במשרדי הממשלה ויחידות הסמך וגופי התמ"ק.
2. דרישות סף במכרזים ממשלתיים – חשכ"ל.
3. חברות ממשלתיות[1].

בשלב השני (שנה – שנתיים) לאחר הכניסה למגזר הממשלתי והערכת מצב בנושא תחול האסדרה על התמ"ק.

לאחר שתערך בחינה בארגוני התמ"ק לתקף את הצורך והמידתיות.

הנחת העבודה – יישום תהליך האסדרה במגזר הממשלתי ישפיע בהדרגה על כל המשק כפי שקרה במקרים דומים בעבר.

<u>תהליך ההסמכה - מבחן מעשי ומבחן עיוני</u>

כאמור, תהליך ההסמכה כולל שני מבחנים: מבחן עיוני ומבחן מעשי. הצורך בשני המבחנים בא להבטיח כי בעל ההסמכה בקיא בשני הרבדים ולא בעל ידע תאורטי בלבד או להיפך.

המבחן העיוני יתקיים במתכונת של שאלות רב ברירה. אורך המבחן, כמות השאלות ורף המעבר ייקבע בכל מקצוע בנפרד. הרשות תעמיד לידי הציבור מבחנים לדוגמא בכדי לסייע לנבחנים פוטנציאלים להתכונן למבחן.

המבחן המעשי יהיה מותאם לכל מקצוע בנפרד. ישנם מקצועות בהם המבחן יעשה באמצעות סימולטור ובשאר המקצועות בדרכים אחרות (כגון במבחן למקצוע המתודולוג יידרש הנבחן להציג תרשים אבטחה לגוף מסוים בפני ועדת מומחים).

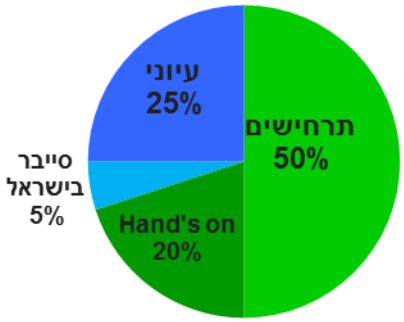
המבחן יהיה מורכב משני החלקים (העיוני והמעשי) ויתקיים באותו יום.

התפלגות ניקוד המבחן (בין החלק המעשי לעיוני) יהיה שונה בין מקצוע אחד למשנהו, ובד"כ יעמוד על 25% למבחן העיוני ו70% למבחן המעשי. 5% נוספים יהיו חלק חובה בנושא הכרת הסייבר במדינת ישראל (אתיקה מקצועית, חוקים וגופים).

[1] תאום מול רשות החברות הממשלתיות.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

התפלגות הסמכת מיישם סייבר



- המבחן העיוני יהיה מבוסס על רשימת אשכולות ידע נדרשים (והסילבוס) שהרשות תפרסם.
- תרחישי ה Hand's on יהיו מבוססים על כלי גנרי (או פתרון חלופי אחר) אשר ניתן יהיה להורדה באתר של הרשות.
- יפורסמו גבולות גזרה לתרחישים (עד איזה רובד המבחן בודק) בנוסף תרחישי המבחן יהיו מקבילים לתרחישים אשר יפורסמו באתר.
- הרשות תפרסם את החומר עליו יהיה המבחן של הכרת הסייבר בישראל.

בשלב ראשון יתקיימו מבחנים בין יום ליומיים בחודש (לכל מקצוע) ובהמשך יורחבו המועדים לפי דרישת השוק. המבחנים יתקיימו במרכז הארץ במקום נגיש לציבור אשר יעמוד בדרישות הטכנולוגיות הנדרשות לקיום המבחן.

<u>כללים ותקנות בתחום הסייבר</u>

נדרש לוודא כי כלל העוסקים בתחום מכירים את חוקי הסייבר והאתיקה המקצועית במדינת ישראל.
בנוסף יש צורך ליידע את אודות גופי הסייבר ותפקידם/אחריותם במרחב הסייבר של המדינה.
לצורך כך במבחן העיוני יוקדש פרק העוסק בתחום זה. את החומר תפרסם הרשות לציבור לצורך הכנה למבחן. פרק זה של המבחן יהיה אחיד לכלל המקצועות ואדם שעבר את הפרק במבחן הסמכה אחד יהיה פטור מפרק זה במבחן הסמכה למקצוע אחר.
ככלל פרק זה של המבחן יהיה אחד מהחלקים במבחן העיוני, לבעלי פטור מהמבחן העיוני תינתן אפשרות לשלב את הפרק הזה במבחן המעשי או לגשת למבחן זה בלבד.
הרשות רואה בהכרת הגופים הרלוונטיים בישראל והדרך לפעול מולם נדבך חשוב ביותר בהגנה על המרחב הקיברנטי של מדינת ישראל.

<u>שמירה על כשירות</u>

לאור הדינמיות והחידושים הרבים בתחום הסייבר רואה הרשות הלאומית להגנת הסייבר ערך עליון בשמירת הכשירות של העוסקים בתחום.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

שמירת הכשירות תתבצע באמצעות צבירת "נקודות זכות" אותם יצטרך בעל ההסמכה לצבור במהלך שלוש שנים כדי לשמור על תעודתו (כמקובל בהסמכות בינ"ל מובילות).
את נקודות הזכות אפשר לצבור ע"י השתתפות בכנסים (המאושרים ע"י הרשות), כתיבת שאלות למבחני ההסמכה והעברת הרצאות בנושא סייבר ע"פ קריטריונים ידועים מראש ובתיאום/ אכוונה של הרשות.
בעתיד הרשות לאומית להגנת הסייבר תעמיד לרשות הציבור סימולטורים לצורך תרגול במקצועות מסוימים. מעבר תרגול זה יזכה בנקודות זכות רבות (ביחס לנקודות זכות אותם יקבלו על השתתפות בכנסים). דירוג זה מבטא את החשיבות שהרשות נותנת לתרגול מעשי.
הרשות תפרסם את הדרכים בהם יועברו לראשות נקודות הזכות לצורך מעקב אחר שמירת הכשירות של בעלי המקצוע.

<u>הסמכות חיצוניות</u>

<u>הסמכות בינ"ל</u>

הרשות הלאומית להגנת הסייבר מכירה בקיומם של הסמכות הבינ"ל כהסמכות טובות המקיפות ידע רב (ברובו עיוני).
בתהליך אסדרת המקצועות קובעת הרשות את הרף (המינימאלי מבחינתה) שעל בעל ההסמכה לדעת.
לעיתים קיים פער בין הידע הנדרש ע"י הרשות במקצוע מסוים לבין מה שנלמד בהסמכה בינ"ל .
מכיוון שהרשות רוצה להכיר בהסמכות בינ"ל מחד ומאידך אין הרשות מעוניינת להתפשר על רמת הידע הנדרשת, אזי יקום מנגנון שתפקידו יהיה לגשר על הידע הנדרש ע"י הרשות במקצוע מסוים לבין הידע הנרכש בהסמכה בינ"ל מקבילה, ע"י בניית תוכנית לימודים אשר תגשר על פער זה.
אי לכך הרשות תפרסם בהמשך אילו הסמכות יכולות להוות תחליף לשלב המבחן העיוני ואיזה ידע נדרש להשלים לצורך קבלת הפטור ממבחן זה.
הרשות שומרת לעצמה את הזכות להחליט מהו הפער בין הסמכה מסוימת לבין מקבילתה הבין לאומית.
יש לציין כי ההחלטה תעשה בהתייעצות עם ועדה מקצועית (ועדת שקילות) הכוללת בתוכה את מיטב אנשי המקצוע המובילים בתחום זה.
כאשר מדובר בהסמכה ייחודית למוסד ספציפי, ולא הסמכה בינ"ל מוכרת, הרשות תיקח בחשבון את איכות המוסד הלימודי בבואה לאשר את ההסמכה (ולא רק את הסילבוס הנלמד).
למיטב ידעתנו, כיום אין כמעט מבחנים מעשיים בהסמכות בינ"ל ולכן רובם המוחלט של בעלי ההסמכות יידרשו לעבור את המבחן המעשי.
בנוסף בעלי ההסמכה הבינ"ל יעברו את המבחן בנושא "הסייבר במדינת ישראל" כחלק מתהליך ההסמכה.

<u>הסמכות ישראליות</u>

במדינת ישראל ישנם מס' גופים (בעיקר בקרב הקהילה הביטחונית בדגש על צה"ל) המכשירים את אנשיהם לעיסוק במקצועות הסייבר השונים.
הרשות מקדמת עבודת מטה למול גופים אלו בכדי לשלב תכנים רלוונטיים להסמכות (הנדרשים ע"י הרשות ולא מופיעים בתוכנית הלימודים של הגוף) ולאפשר לבוגרי הסמכות אלו לקבל תעודת הסמכה

ישראלית מיד עם סיום הסמכתם בגופים האמורים.
שילוב התכנים יעשה רק לאחר בדיקה לקיום זיקה עמוקה בין התכנים הנלמדים בגוף לבין המקצוע אותו הרשות מסמיכה.
יש לציין כי גם ללא ביצוע תהליך זה, של הוספת התכנים, יוכרו בעלי הסמכות אלו כבעלי הסמכות רלוונטיות וההתייחסות אליהם תהייה כמו לבעלי הסמכה בינ"ל (השוואת סילבוסים מתן פטורים / הקלות לאחר בדיקה של איכות הגוף המסמיך).
ככלל, רוב בעלי הסמכות ישראליות מקבילות יידרשו לעבור מבחן מעשי.

<u>מערך רישום ותיעוד</u>

הרשות תספק תעודה לכל מי שעבר בהצלחה את מבחני ההסמכה. התעודה אישית ואינה ניתנת להעברה.
בתעודה יצוינו פרטי זיהוי של בעל התעודה והמקצוע בו ניתנה ההסמכה. במקביל תעמיד הרשות לטובת הציבור מאגר מידע בו יהיה אפשר לראות את בעלי ההסמכה.
בכדי למנוע פרסום שמם של בעלי ההסמכה בפומבי, הבדיקה תעשה ע"י שאילתה בו יצטרך השואל למלא פרטי הזהות של בעל התעודה. התשובה שתתקבל תהייה לגבי אדם זה בלבד (האם הוא בעל הסמכה ישראלית). המאגר לא יכלול פרטים נוספים.

<u>הקמת אתר תומך</u>

הרשות תקים אתר אינטרנט התומך במבחני ההסמכה הישראלית. האתר יכלול את הסילבוסים שפורסמו, מבחנים לדוגמא לכל מקצוע, מועדי בחינות, מיקומם וכד'.
בנוסף יפורסם באתר כל נושא ההסמכות הבינ"ל ויפורט בו איזו הסמכה מקבילה למקצוע מסוים ומה נדרש להשלים.

<u>עלויות</u>

בשלב הראשון מבחן ההסמכה יהיה בחינם לסקטורים המונחים ע"י הרשות.
אדם אשר לא יגיע למבחן ללא סיבה מוצדקת (אשר תלווה באישור מתאים) תישלל אפשרותו לגשת למבחן בחודשיים העוקבים וזאת במטרה להבטיח ניצול מקסימלי של פלטפורמת הבחינה.

- הגופים המונחים (ממשל ותמ"ק) יהיו פטורים מתשלום.
- שאר הסקטורים תקבע העלויות ע"פ מודל ההפעלה שייקבע.

יש לציין כי במקרה של גביית תשלום מהנבחן נידרש להקים תהליך גביה מאובטח ופונקציית כ"א תומכות.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

<u>ותיקי התחום</u>

קיימים היום בישראל מס' גדול של אנשים העוסקים במקצועות הגנת הסייבר במשך מספר שנים. אנשים אלו מוגדרים כוותיקי התחום (במסמך אסדרת מקצועות הסייבר "דור המדבר").

מתוך ההבנה שניסיון מצטבר מביא גם לידע רב אותו לא לומדים בקורסי הכשרה רגילים, הרשות תקים מסלול הכשרה מיוחד לאנשים אלו.

ותיקי התחום מוגדרים כל מי שיש לו ניסיון מוכח של 7 שנים בתחום הסייבר מתוכם לפחות 3 שנים באותו מקצוע בו הם מבקשים לקבל הסמכה. הניסיון צריך להיות במקומות עבודה מוכרים (שאפשר יהיה לוודא את הניסיון המוצהר).

יחד עם הרצון "לבא לקראת" אותם אנשים אין כוונת הרשות להתפשר על המקצועיות אותה היא דורשת ולכן ותיקי התחום יידרשו להשלים ידע זה על בסיס מודל שייקבע ע"י הרשות.

בנוסף ותיקי התחום יידרשו להציג הסמכה בינ"ל בתוקף הקשורה למקצוע בו הם מבקשים הסמכה.

תחליף המבחן (מעבר לסדנאות) יהיה סיוע לרשות לקדם את הגנת הסייבר במדינת ישראל באמצעות מס' דרכים שיפורסמו בהמשך אשר יביאו לידי ביטוי את הניסיון הרב אותו צברו ותיקי התחום.

הרשות תפרסם בהמשך את הדרכים בהם ניתן להגיש בקשה להכרה כוותיקי התחום. בנוסף הרשות תקים גוף מיוחד שתפקידו יהיה לטפל במקרים חריגים הקשורים לוותיקי התחום.

<u>ביצוע המבחן הלכה למעשה – שלבים</u>

1. פרסום של מועדי המבחן באתר של הרשות.
2. רישום למבחן המבוקש.
3. קבלת הודעת אישור הרישום.
4. הגעה למבחן בהתאם לזמן והמקום שנבחרו וביצוע הבחינה.
5. קבלת אישור על מעבר הבחינה (ברוב הבחינות באופן אוטומטי ע"י הסימולטור).
6. הכנסת הנתונים למאגר המוסמכים.

כאמור, לצורך הכנה מיטבית למבחן הרשות מפרסמת לכל מקצוע מס' דברים האמורים להקל על הניגשים לבחינה:

1. סילבוס שעל בסיסו תתקיים הבחינה.
2. מבחנים עיוניים לדוגמא.
3. מבחנים מעשיים לדוגמא*

*במקצוע המיישם יופיעו דוגמאות לתרחישי הon hand's ודוגמאות לתרחישים כלליים בהתאם לפרוט הבחינה (כפי שהוסבר למעלה).