



סיכום שנות ההקמה

2017-2016

תוכן עניינים

1. היכרות — עמ' 4

- תקציר מנהלים
- הרקע להקמת הרשות
- כוח האדם ברשות



2. מתמודדים עם איומי הסייבר — עמ' 11

- ניהול אירועים
- התמודדות עם איומים
- שת"פ בינלאומי
- פלטפורמות להנגשה
- מרכזים מגזריים



3. מגביהים את החומות — עמ' 24

- הגנת תשתיות מדינה קריטיות
- הגנת יתר המשק
- תורת הגנה לארגונים בישראל
- קידום כ"א מקצועי בתחום הגנת הסייבר



דבר ראש הרשות הלאומית להגנת הסייבר - בוקי כרמלי

ובין אחריותה להגנת הסייבר.

כשאדם פותח את ברו המים בביתו ושותה מים ישירות ממנו, הוא עושה זאת ביוזעו שהמדינה נטלה על עצמה את האחריות להבטיח שהמים נקיים ושהוא יכול לשתות אותם ללא חשש. כך, בהתאם, הציבה ממשלת ישראל לרשות מטרה לפיה כל אדם וארגון במדינה יוכל לעשות שימוש במרחב הסייבר ללא חשש.

באפריל 2016 החלה הרשות בפעילותה, תוך התבססות על שלוש אבני בניין מרכזיות:

- **פעילות הנחייתית** שייעודה הנחיית המשק כיצד להתגונן מפני מתקפות, כיצד להגן על נכסים קריטיים וכיצד לשמור על רציפות תפקודית גם בעת מתקפה. במסגרת זו הרשות אחראית על הגנת תשתיות המדינה הקריטיות, כגון חברת החשמל ונמלי הים, וכן מנחה באמצעות הרגולטורים השונים את יתר מגזרי המשק.
- **פעילות מבצעית** שייעודה סילוק מתקפות סייבר וסיוע למשק בהתגברות עליהן.
- **פעילות תשתיתית** שייעודה הרחבת מעגל העוסקים בהגנת הסייבר.

חרף הזמן הקצר שעבר מאז הקמתה, הרשות כבר הוכיחה את חזון ממשלת ישראל ואת נחיצותה למשק ותורמתה לחוסנו. הרשות היא נכס מדינתי שחשוב לשמור עליו.

במלאת שנתיים לפעילותה, אנו מבקשים לשקף לכם מקצת מהעשייה שלנו בתחום.

קריאה מהנה,

בוקי כרמלי

ראש הרשות הלאומית להגנת הסייבר

בשלהי המאה ה-19 הסופר

הידוע ז'ול וורן חזה בספרו

"פריז במאה העשרים"

עולם שכולו מרושת

בקווי טלגרף, במסגרתו

עיתונאי בפריז הכותב

כתבה על דף נייר, יוכל להזין

אותה למכונה גדולה השולחת

העתק שלו לקצה השני של האוקיינוס. הוא

קרא למכונה זו בשם "פקסימיליה". חלפו

מאה שנים ותקשורת זו נחשבה למתקדמת

שבנמצא. שלושים שנים לאחר מכן,

הטכנולוגיה הביאה אותנו למחוזות שפעם

נחשבו לבלתי אפשריים או דמיוניים לחלוטין.

לשמחתנו הטכנולוגיה לא עוצרת, אלא מסייעת לנו לייצר כלים, שיטות ומערכות שמזינים את ההאצה הטכנולוגית שמשפרת את איכות חיינו, אך בה במידה גם מגדילה את התלות שלנו, כחברה אנושית, בטכנולוגיה. כך, אנחנו מוצאים מערכות טכנולוגיות מורכבות המנהלות את שגרת חיינו במגוון רחב של תחומים: פיננסים, תחבורה, אנרגיה, רפואה, מזון ומגזרי עשייה נוספים.

ממשלת ישראל זיהתה את הפוטנציאל הנפיץ הטמון בהתפתחות זו, ובתום עיסוק רב שנים של המדינה בנושא – ובכלל זה של צוות שמינה ראש הממשלה, בראשות פרופסור אלוף (מיל') יצחק בן-ישראל ב-2010, ושל מטה הסייבר הלאומי שהוקם ב-2011 – התקבלה ההחלטה להקים את הרשות הלאומית להגנת הסייבר: גוף שייעודו הגנת מרחב הסייבר האזרחי. החלטה זו גזרה גזירה דומה בין אחריות המדינה להבטיח מים נקיים לכל תושביה



צילום: לע"מ

היכרות

CYBER SECURITY

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר



הערכים שלנו: מנהיגות, צניעות, שיתוף ומקצוענות

תקציר מנהלים

בתחילת 2016, לאחר עיסוק רב שנים של מדינת ישראל בנושא, הוקמה הרשות הלאומית להגנת הסייבר: גוף המשלב מאפיינים ביטחוניים-אופרטיביים לצד מאפיינים אזרחיים, המוביל בסינרגיה עם יתר גופי הביטחון את מאמצי ההגנה כנגד תקיפות סייבר על המשק האזרחי.

אחת ממשימות הליבה של הרשות היא **סיוע לציבור ולארגונים בהתמודדות עם איומי הסייבר - וזאת ללא קשר לשאלה מי עומד מאחוריהן**. סיוע זה מתממש באמצעות המרכז לניהול אירועי סייבר ברשות - ה-CERT הלאומי, הפעיל מתחילת אוקטובר 2016 בבאר שבע. הרשות פועלת לסייע לארגוני המשק בהתמודדות עם איומי הסייבר, ומאז תחילת פעילותה האופרטיבית **טיפול במאות רבות של איומים ואירועים במרחב בדרגות חומרה משתנות**. לצד מרכז הסיוע, הוקמו ברשות מרכזים מגזריים, המסייעים למשרדי הממשלה ולמגזר הפיננסי, שבפרק זמן קצר כבר הוכיחו את הערך ביצירת מומחיות מגזרית.

כיוון שהסייבר הוא מרחב גלובלי, הוא מחייב גם שיתוף פעולה בין-מדינתי. הרשות פעלה מיום הקמתה לביסוסה בקהילת גופי הגנת הסייבר העולמית, וכיום נמצאת בקשר עם גופים רבים ממדינות שונות על פני הגלובוס. קשר זה מוליד לא

מאז תחילת פעילותה האופרטיבית טיפלה הרשות במאות רבות של אירועים ואיומים במרחב.

רק תובנות משותפות ותהליכי עבודה סדורים, אלא גם נושא פירות ממשיים. בזכות קשר זה, **עשרות מדינות סייעו במאמץ הרשות לבלום תקיפות בינלאומיות על ארגונים בישראל**.

פעילות חשובה נוספת של הרשות מיום הקמתה היא **פעילותה להעצמת חוסן המרחב האזרחי**,

או בשפה פשוטה, "הגבהת החומות". פעילות זו נעשית בהסכמה, על ידי העלאת מודעות הארגונים לאיומי הסייבר, ובהנחיה, במידה שהאינטרס הציבורי מחייב זאת.

החל ממרץ 2017 הרשות אחראית מתוקף חוק להנחיית גופי תשתיות המדינה

הקריטיות, כגון חברת החשמל ורכבת ישראל, כיצד להתמודד עם סיכוני סייבר שעלולים להשבית מערכות קריטיות שבאחריותם. זוהי הנחיה ייעודית ישירה של הרשות שמעניקה "חליפת הגנה" מותאמת לכל גוף. במקביל להנחיית עשרות גופים אלה, הרשות החלה בעבודה מול הרגולטורים המגזריים, כגון המשרד להגנת הסביבה, על מנת להחיל נורמות מתחום הגנת הסייבר על מושאי ההגנה השונים. יחידות אלו, שאישו ע"י הרשות ומשרדי הממשלה בתוך הרשויות הרגולטוריות, כבר החלו להפיק תוצרים, כגון סקרי סיכונים למיפוי פערים וגיבוש "נספחי סייבר" במסגרת הסמכות הרגולטורית של המשרד.

על מנת לסייע למשק להיערך להתמודדות עם

האיומים, פרסמה הרשות בראשית 2017 את "תורת ההגנה בסייבר לארגון". עבודה על פי תורה זו מספקת לכל ארגון בישראל, קטן כגדול, כלים לניהול

ולטיוב ההגנה מפני הסיכונים הנגזרים מאיומי הסייבר, ומסייעת לארגון לבנות תכנית עבודה סדורה. אלפי ארגונים בישראל כבר פועלים כיום על פי תורה זו, הנגישה כשירות חינמי לכלל ארגוני המשק. [ניתן להוריד עותק של תורת ההגנה מאתר הרשות.](#)

במקביל, הרשות פעלה לקידום כח האדם המקצועי בתחום

הסייבר. פעילות זו נעשית במספר רבדים: על ידי התנעת תכנית אסטרטגית משותפת עם משרד החינוך להסמכת בני נוער בתחום, על ידי עידוד שוק התעסוקה בהסבה למקצועות ההגנה, ולבסוף, באמצעות קביעת רף מקצועי של העוסקים בתחום

במשרדי הממשלה.

בהקשר זה, הרשות פועלת לשילוב אוכלוסיות מגוונות בתעשייה ובגופי הממשלה. כך, במהלך 2017, נפתחו קורסים לציבור החרדי, נשים וגברים, במימון משרד העבודה והרווחה.

מקץ שנתיים לתחילת הקמתה של הרשות, ניתן לקבוע בהירות הנדרשת כי קיומו של גוף הגנה ממשלתי אובייקטיבי הנטול אינטרסים מסחריים ושכל ייעודו הגנת מרחב הסייבר האזרחי, יש בו כדי להוות

חידוש משמעותי המהווה קפיצת מדרגה לחוסן המשק. כל זאת, במטרה שכל אדם וארגון בישראל יוכל לעשות שימוש במרחב הסייבר **ללא חשש.**

על מנת לסייע למשק להיערך להתמודדות עם האיומים ול"הגבהת החומות", פרסמה הרשות את "תורת ההגנה בסייבר לארגון" - כלים ברורים לכל ארגון בישראל לטיוב ההגנה מפני הסיכונים הנגזרים מאיומי הסייבר.

על הרשות והרקע להקמתה

המרכיבים האזרחיים והביטחוניים במרחב הקיברנטי שזורים זה בזה ושחלקם לא ניתנים להפרדה, וכי נדרשת ראייה לאומית רחבה והבנה שהיערכות מדינת ישראל לאתגרי מרחב הסייבר הינם משימה לאומית.

בהמשך לכך, באוגוסט 2011 קיבלה ממשלת ישראל החלטה להקים את מטה הסייבר הלאומי, וזאת כיישום מהמלצות הדו"ח. ייעודו של גוף זה כפי שקבעה הממשלה הינו להוות גוף מטה לראש הממשלה, לממשלה ולוועדותיה, אשר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הקיברנטי. על מטה הסייבר הלאומי הוטל, בין היתר, לגבש תפיסת הגנה לאומית במרחב הסייבר.

מעת הקמת מטה הסייבר הלאומי וכתוצר של עבודת מטה שערך לגיבוש תפיסת הגנה לאומית במרחב הסייבר, התקיים דיון מקצועי, עקרוני וחשוב במדינת ישראל, שעסק באופן הקמת גוף אופרטיבי שאחראי על הגנת מרחב הסייבר האזרחי. הצורך בהגנה על המרחב האזרחי מעולם לא היה במחלוקת, אך אופן המימוש והאחריות שימשו בסיס למגוון רחב ונוקב של דיונים אשר הוכרעו לבסוף

הרשות החלה לפעול בתחילת שנת 2016, פרי עיסוק רב שנים של מדינת ישראל בצורך בהקמת גוף הגנה לאומי במרחב הסייבר.

הכל החל בנובמבר 2010, אז מינה ראש הממשלה מר בנימין נתניהו צוות מיוחד לגיבוש תכנית קיברנטית לאומית, שנודע גם בשם "המיזם הקיברנטי". הצוות, בראשו עמד פרופסור אלוף (מיל') יצחק בן-ישראל, עבד מספר חודשים, ונחלק למספר תתי ועדות ולעשרות אנשי מקצוע. הצוות בחן את המרכיבים החיוניים להתמודדותה של מדינת ישראל במרחב הסייבר, לרבות ניתוח תועלות לאומיות בהיבטי כלכלה, אקדמיה ובטחון לאומי. עבודת הצוות הושלמה במאי 2011 בדו"ח מיוחד לראש הממשלה.

מסקנת הצוות הייתה כי "מתקפות קיברנטיות הן בגדר פוטנציאל לאיום מהותי על הרצף התפקודי של המדינה, מוסדותיה ואזרחיה", וכי זוהי "פער מרכזי בהגנה קיברנטית על המרחב האזרחי הכולל".

בליבת הדו"ח, הוועדה המליצה על הקמת שני גופים, "מטה סייבר לאומי" ולצידו "גוף ביצוע לאבטחת המגזר האזרחי". כן המליצה הוועדה על הקמת מעטפת הגנת סייבר לאומית, הכוללת מערכות ממוחשבות אוטומטיות ומערכות אנושיות המספקות יחדיו הגנה על מערכות מחשב שהוגדרו מראש, לרבות הקמת מרכז תגובה וסיוע (CERT). הוועדה ציינה כי





ג. לבנות ולחזק את החוסן של כלל המשק

בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים ונופים במשק, הנחיית המשק בתחום הגנת הסייבר, אסדרת שוק שירותי הגנת הסייבר, רישוי, תקינה, עריכת תרגילים ואימונים, מתן תמריצים וכלים נדרשים נוספים.

ד. לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר.

ה. לבצע כל תפקיד אחר שיקבע ראש הממשלה, בהתאם לייעוד הרשות.

הרשות החלה לפעול בתחילת שנת 2016, עם מינויו של ראש הרשות הלאומית להגנת הסייבר, ומאז עוסקת בבנייה אינטנסיבית של יסודות הפעילות של הרשות, בגיוס כ"א, בבניית כלל התהליכים הארגוניים, בבניית והפעלת יכולות מבצעיות, בבניית והפעלת טכנולוגיות ייחודיות ועוד וכל זאת על מנת לממש את ייעודה להגן על מרחב הסייבר במדינת ישראל.

בהמשך מסמך סיכום זה, נפרט על פעילות זו וכיצד היא סייעה לשיפור מצב המשק בהיבטי הגנת הסייבר מיום הקמת הרשות.

בפברואר

2015 -

בהחלטת

הממשלה

2444 על הקמת גוף אזורי, יחידת סמך במשרד ראש הממשלה - **הרשות הלאומית להגנת הסייבר.**

במסגרת החלטה זו קבעה הממשלה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי.

בהתאם, נקבע כי ייעוד הרשות הלאומית להגנת הסייבר הינו הגנת מרחב הסייבר ובמכלול תפקידיה העיקריים נמנים:

א. לנהל, להפעיל ולבצע בהתאם לצורך את **כלל מאמצי ההגנה האופרטיביים** ברמה הלאומית במרחב הסייבר, בתפיסה מערכתית, לטובת מענה הגנתי שלם ורציף למול תקיפות סייבר.

ב. להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר (להלן – ה-CERT הלאומי) עבור כלל המשק, ובכלל זה **לפעול לשיפור החוסן ההגנתי בסייבר, לסייע בטיפול באיומי סייבר ואירועי סייבר.**

כח האדם ברשות

אודות האנשים שמאחורי המותג "הרשות הלאומית להגנת הסייבר" - אוכלוסייה מגוונת של נשים וגברים מקשת של קבוצות גיל.

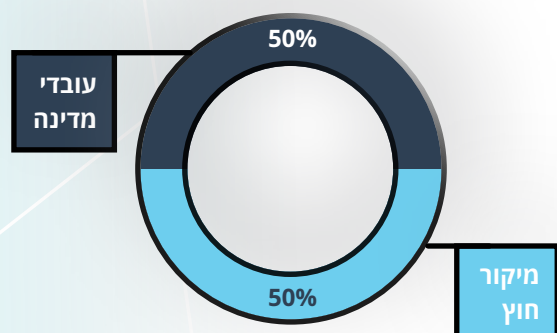
אחד האתגרים הגדולים בהקמת רשות מבצעית חדשה בישראל היה ונותר גיוס כוח אדם מקצועי ואיכותי. בחרנו להציג בפניכם בפרק זה מעט על

כוח אדם מיום הקמת הרשות*

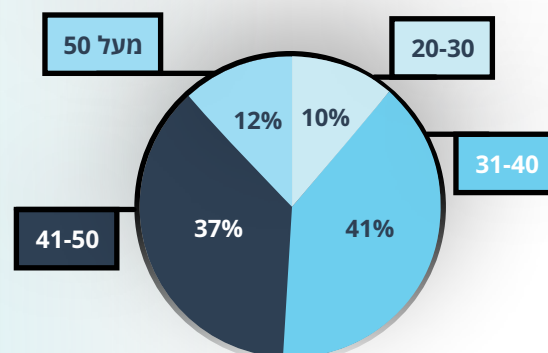


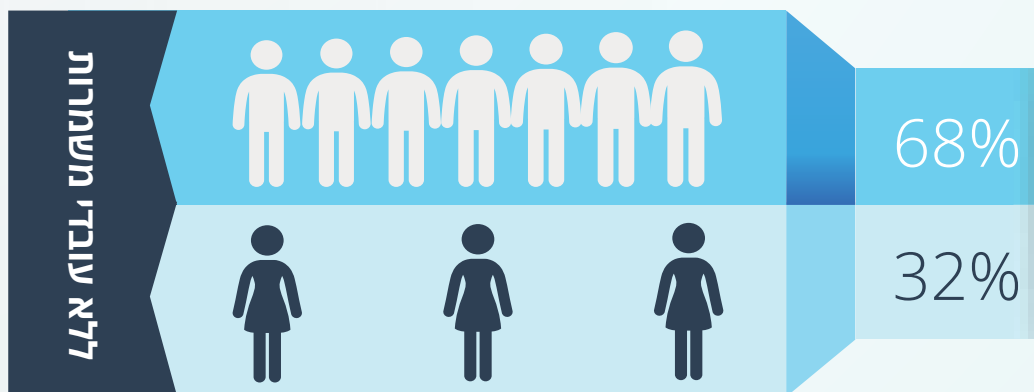
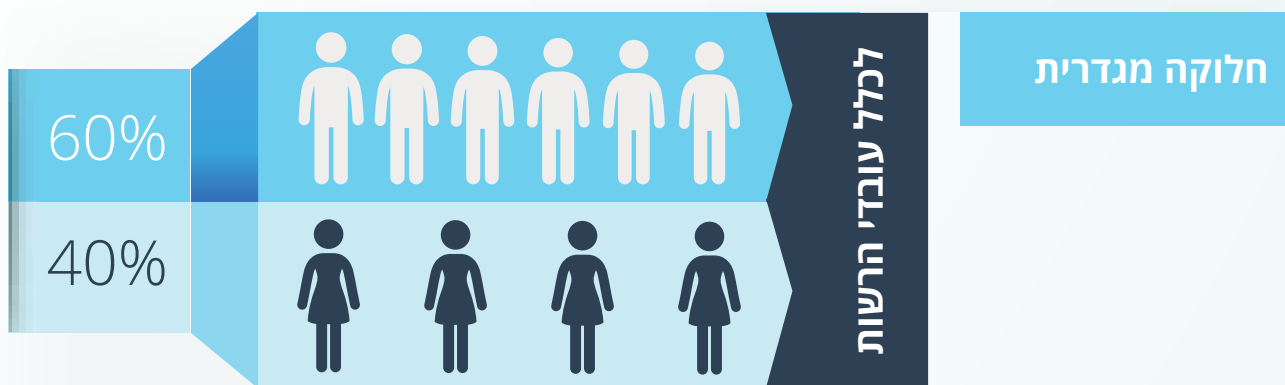
* המספרים מתייחסים לעובדי מדינה ולעובדים במסגרות אחרות

התפלגות כח אדם לפי סוגי העסקה



התפלגות גילאים (ללא עובדי משמרות)





בהי-טק הישראלי: 26% נשים ו-74% גברים, על פי נתוני הכלכלן הראשי במשרד האוצר, 2016



2.

מתמודדים עם איומי הסייבר



פעילות אופרטיבית

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר



הערכים שלנו: מנהיגות, צניעות, שיתוף ומקצוענות

מתמודדים עם איומי ואירועי הסייבר – פעילות אופרטיבית



מתמודדים עם האיומים

מרחב הסייבר כולל כיום איומים מסוגים שונים, על-ידי תוקפים שונים, אך לארגון הבודד אין זה משנה מיהו התוקף, אלא כיצד להתגונן בפניו או לסלקו.

התפיסה השלטת היא שבעוד זה כמעט בלתי אפשרי לעצור את התקפות הסייבר, המדינה תסייע אל מול האירועים השונים, ותפיץ הלאה את המידע ההגנתי הרלוונטי לטובת יתר המשק. תפקידה של הרשות בהקשר זה הוא לסייע לציבור ולארגונים בהגנת הסייבר להתמודד עם איומי הסייבר – ללא קשר לשאלה מי עומד מאחוריהן. סיוע זה מתממש באמצעות המרכז לניהול אירועי סייבר ברשות – ה-CERT (Cyber Emergency Response Team) הלאומי.



תגובה למתקפות – מהכרזה על חדירה ועד חזרה לשגרה

לרשות על תקיפתם בסייבר, בעשרות רבות של מקרים הוחלט, לאחר ניתוח מקצועי של משמעות

החל מהקמתה, פעילות הרשות עמדה בסימן בניין הפעילות המבצעית שלה. כך, הרשות מפעילה מבאר שבע את המרכז לניהול האירועים, המספק מענה ראשוני לטיפול בתקיפות ובאירועי סייבר במרחב האזרחי. מרכז זה, המאויש 24/7 באנליסטים מומחים בהגנת סייבר, עוסק יום יום שעה שעה בקליטה, ניטור וטיפול.

מתחילת 2017, הרשות ניהלה **מידי חודש עשרות אירועים** שבהם נחדרו ארגונים בידי תוקפי סייבר. בלשונה של הרשות מוגדר "אירוע" כחדירה וודאית לארגון בישראל. נכון לסוף שנת **2017**, ממוצע החדירות עומד על **כ-100 ארגונים בחודש**. זו מהווה עליה **בהשוואה ל-2016, אז טיפלה הרשות בכ-50 אירועים בחודש**. לאלה יש להוסיף תקיפות רבות, שלא בכולן התגלו חדירות לארגון. בעקבות פניות רבות של גופים אזרחיים



תקיפות סייבר במהלך 2017



לחקירת האירועים השונים ומערך אנליזה נלווה.

כגוף שמטרתו להיות עם הפנים למשק האזרחי, הרשות מודעת לכך שהמידע הנחלק עמה הינו בעל רגישות גבוהה, מסיבות כגון סודיות מסחרית, זכויות קנייניות, הגנת הפרטיות וכן הלאה, ועל כן פועלת הרשות בהתאם לעקרונות

האירוע לחוסן הלאומי, לשלוח לשטח צוותי תגובה של הרשות על מנת לסייע לארגון להכיל את התקיפה.

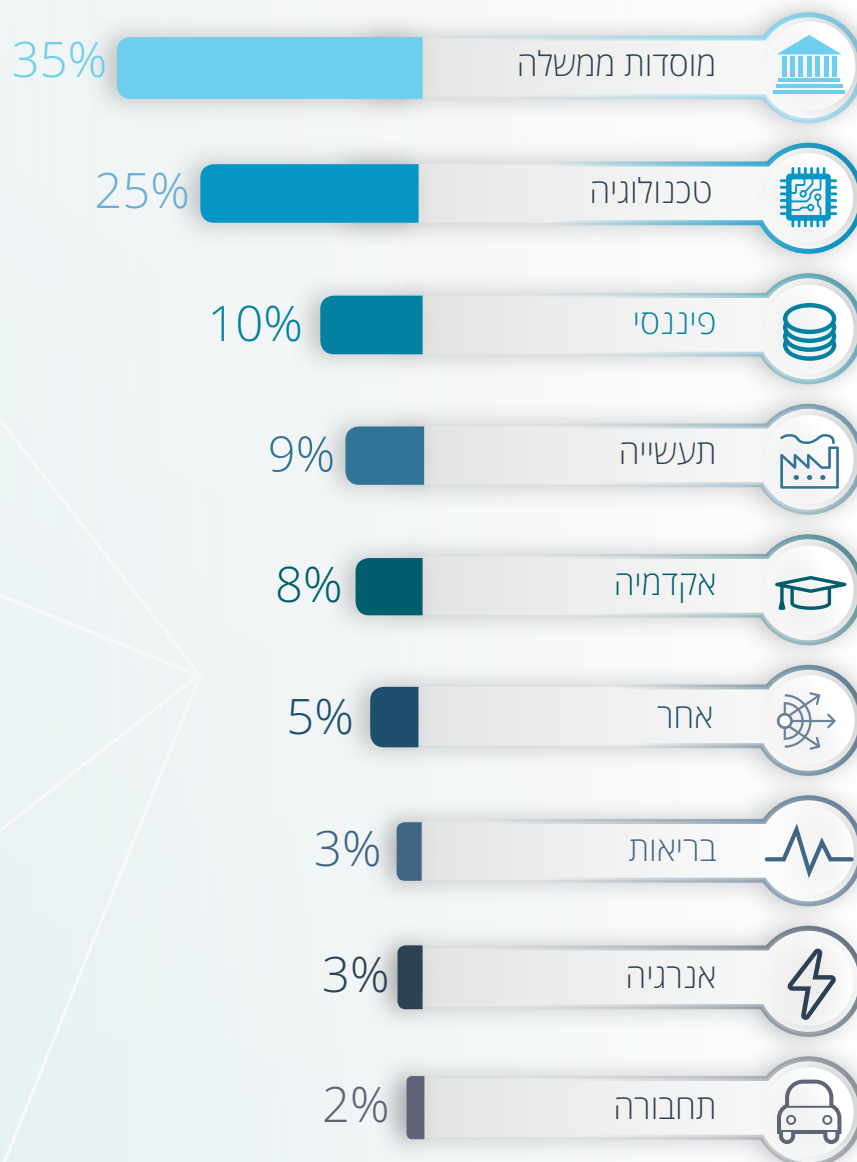
פעילויות התגובה לאירועי סייבר מתבססות על מתודולוגיה סדורה לניהול אירועי סייבר שפותחה ברשות הלאומית להגנת הסייבר ונתמכת בפיתוח ייעודי של כלים טכנולוגיים

קיומו של גוף הגנה ממשלתי אובייקטיבי, הנטול אינטרסים מסחריים, והפועל לטובת האינטרס הציבורי, מעורר התגייסות ונכונות של ארגונים נתקפים לחלוק מידע לצורכי הגנה.

כיום, לאחר תקופה ארוכה של פעילות אופרטיבית, ניתן לקבוע בזהירות כי קיומו של גוף הגנה ממשלתי אובייקטיבי הנטול אינטרסים מסחריים, הפועל למען האינטרס הציבורי, מעורר התגייסות ונכונות גבוהה של ארגונים נתקפים לחלוק מידע רגיש. זהו **חידוש משמעותי המהווה קפיצת מדרגה בהגנה על המשק**. בחרנו להציג בחוברת זאת שני אירועים על מנת לשקף כיצד פעלה הרשות וסייעה למשק.

שתואמו עם היועץ המשפטי לממשלה, שמטרתם מיקוד במידע המאפשר סילוק התקיפה תוך וידוא כי ננקטים כל הצעדים הנדרשים על מנת לשמור על זכויות הארגון הנתקף ועובדיו. בין היתר, הרשות מתחייבת שלא לחשוף את פרטי הארגונים הנתקפים. דיווחי הציבור מאפשרים לא רק לסייע לארגונים הנתקפים עצמם, אלא לזהות תקיפות מבעוד מועד ולבלום את התפשטותן של מתקפות גם לעבר ארגונים אחרים.

שיעור תקיפות בחלוקה למגזרים

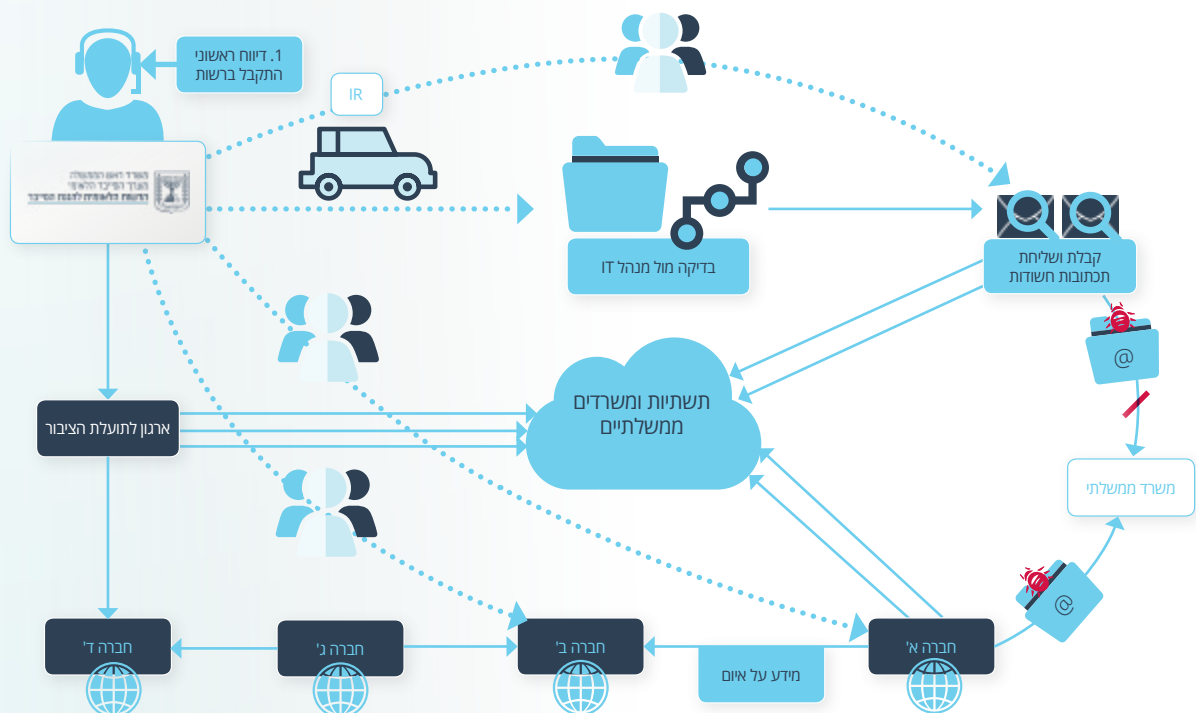


אירוע במגזר הטכנולוגיה:

מוסדות ציבור ואנשים פרטיים. מניתוח האירוע זוהו מספר חברות מרכזיות שנתקפו ושימשו פלטפורמה לתקיפת חברות וגופים נוספים. **הרשות יצרה קשר מידי עם עשרות הארגונים שהותקפו והפיצה התרעה רוחבית לטובת חיסון מידי ביתר המשק - מהלך שבלם חדירה למאות ארגונים בישראל.** זוהי דוגמה למתקפה שניתן להתמודד עמה באמצעות שיתוף פעולה במגזר האזרחי בהובלה של הרשות.

בתחילת 2017, התקבלו ברשות דיווחים רבים אודות מתקפת סייבר המתפשטת בגופים אזרחיים רבים במשק הישראלי. תוך זמן קצר מרגע זיהוי המתקפה, "הוקצו" צוותי תגובה של הרשות לאחד הארגונים שהותקף, וחשפו את מתווה התקיפה ואת נקודות האחיזה שבהן התוקף עשה שימוש. עבודת הניתוח לימדה כי התוקף התחזה לארגון לגיטימי ושלח הודעות דואר אלקטרוני בשם הארגון, תוך ניסיון לתקוף יותר מ-120 ארגונים, בהם: משרדי ממשלה,

תיאור האירוע





אירוע במגזר הבריאות:

בהכלת האירוע, ובמקביל הוחלט להפיץ את המידע ההגנתי לכלל הארגונים במגזר לטובת "חיסון" יתר בתי החולים ואיתור של נתקפים נוספים. **שיתוף פעולה זה עם מגזר הבריאות ובתי החולים סייע להכלת האירוע ולצמצום נזק פוטנציאלי הן במגזר הבריאות והן במגזרים נוספים.**

בחודש יוני 2017 התקבלה פניה ברשות אודות זיהוי קבצים חשודים ברשת מחשבים של מספר בתי חולים בארץ, בעקבותיה הוחלט על פתיחת חמ"ל ייעודי בשיתוף צוותים של משרד הבריאות ושל הרשות. לאחר הערכת מצב, הרשות שלחה לשני בתי חולים צוותי תגובה לטובת איסוף, חקירה וסיוע

התרעות – מזהוי לחיסון

TLP: אדום

TLP: צהוב

TLP: ירוק

TLP: לבן

אותו במהירות לטובת המרחב האזרחי.

כאן, בדומה לסיווג ביטחוני, כל מידע שהרשות מפיצה צבוע בצבע שמגדיר את רוחב ההפצה של המידע. כך למשל **לבן** משמעותו **הפצה פומבית**, ואילו

אדום הוא **הפצה רגישה לנמען בלבד**.

מיום התנעת פעילותה הרשות הפיצה למעלה מאלף "התרעות" מסוג זה, בדחיפה. זאת לצד הפצת מסמכי הגנה מעמיקים עבור מוצרים נפוצים והמלצות הגנה והתמודדות עם איומים כדוגמא נזקקות כופר, ציוד IoT, שימוש במנגנון DMARC ועוד. הפרסומים השונים מופצים בהתאם לרמת האיום והדחיפות באמצעות דוא"ל, אתר האינטרנט של הרשות ומערכת "סייברנט", עליה יפורט בהמשך.

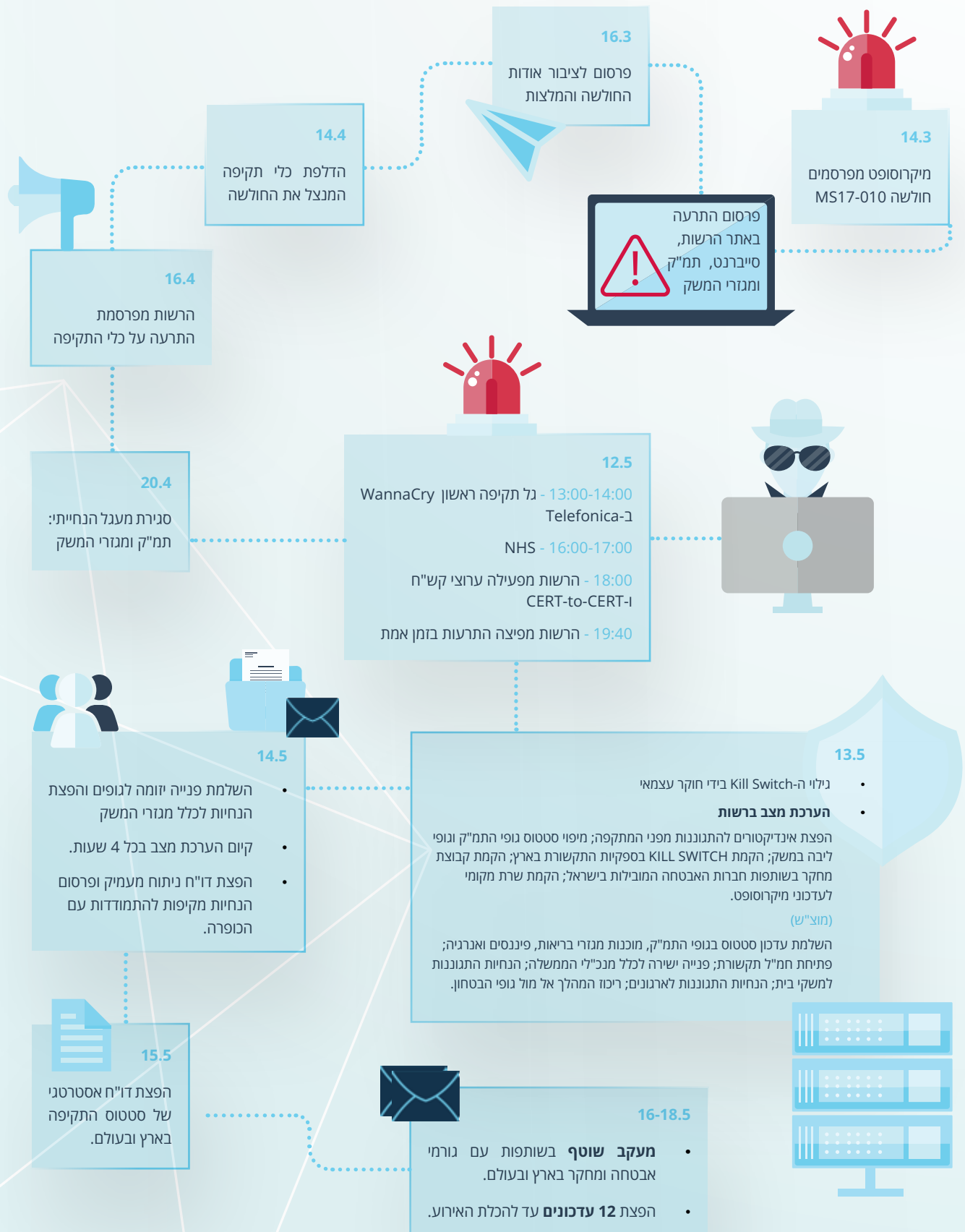
הרשות התמודדה עם עשרות רבות של איומי סייבר אלה, ובהם במהלך 2017 כגון Opisrael באפריל, NotPetya באוגוסט, CCleaner בספטמבר ו-Bad Rabbit באוקטובר. הגדול והמשמעותי מכולם היה ההתמודדות עם איום מתקפת הכופרה "חץ וקשת", הידוע גם בשמו הלועזי Wannacry. בחרנו לתאר לכם מעט כיצד ההתמודדות נראתה מהצד שלנו.

עולם ההתמודדות עם אירועי סייבר לא מתחיל בסילוק המתקפות מהארגונים לאחר שכבר נפגעו, אלא גם בהתמודדות מול איומים קונקרטיים בטרם הגיעו לפתחי הארגונים. זהו עולם ה"התרעות" – המלצות חוסן והתגוננות קונקרטיות מפני איום נקודתי. כאן, מושג המפתח הוא "**מיקור המונים**" (Crowdsourcing) - **חוכמת ההמון, כשהרשות משמשת כמוקד הידע הלאומי וכמי שמרכזת את המידע בנושא זה**: ארגון אחד שנפגע או שנחשף לאיום מהווה מקור שבו מסתייעת הרשות על מנת לעזור ליתר הארגונים להתחסן מפני אותו איום.

איך זה עובד? הרשות מזהה אינדיקציה ראשונית על אודות איום - ממקור מידע גלוי / מתוצר חקירה / משותף בינלאומי או ממקור אחר. הרשות מנתחת את האיום לצורך איסוף מזהים לזיהוי ולחיסון מידי, ומפיצה



השתלשלות אירוע WannaCry



שת"פ בינלאומי

שיתוף מידע הן בזמן התקיפות והן בשגרה, כבסיס להנחיית המשק ובניית החוסן הלאומי בתחום הסייבר.

כך נוצרה עם השנים קהילה מגובשת של גופי CERT (Cyber Emergency Response Team) בינלאומיים המהווה בסיס ישיר, אפקטיבי ומהיר להעברת מידע בזמן אמת בין ארגוני הסייבר העולמיים אודות איומים, שיטות תקיפה ומתן פתרונות יעילים להגנה מפני תקיפות סייבר. פיתוח הקשרים עם CERT של יותר מ-50 מדינות הינו בגדר חידוש ובשורה של ממש ותרם באופן דרמטי להגנת מרחב הסייבר הישראלי.

מרחב הסייבר הוא מרחב גלובלי, המתאפיין בכך שאין לו גבולות גיאוגרפיים ברורים. ככה, תקיפות הסייבר אינן בהכרח מזוהות עם מדינה מסוימת, ומהוות איום בינלאומי משותף על פעילות כלל המשתמשים. תקיפות סייבר יכולות להתחיל ממדינה מסוימת ולעבור דרך מדינות אחרות מסיבות שונות כגון הסוואת מקור התקיפה, התחמקות מהעמדה לדין ועוד.

אתגר הגנת מרחב הסייבר הינו אתגר עולמי המצריך שיתוף פעולה בין מדינות, ארגונים וחברות פרטיות. קשרי החוץ ושיתוף הפעולה מהווים מרכיב קריטי להבטחת



במקרים רבים הסתייעה הרשות בגופי הגנה מקבילים ברחבי העולם לטובת בלימת תקיפות סייבר על ארגונים בישראל מתוך המרחב הגלובלי. פיתוח הקשרים עם ארגוני CERT של יותר מ-50 מדינות הינו בגדר חידוש ובשורה של ממש, ותורם באופן דרמטי להגנת מרחב הסייבר הישראלי.

משותפים ונערכו קבוצות עבודה משותפות על מנת להמשיך ולקדם את יכולות ההגנה על המרחב האזרחי הישראלי.

במקביל, הרשות ממשיכה לפעול בסיוע מטה הסייבר הלאומי לקידום ולמיצוב מעמדה של מדינת ישראל בתחום **הגנת הסייבר** בקרב הקהילה הבינלאומית, ואירחה עשרות משלחות ממדינות וגופים מובילים בעולם, במטרה לחשפם לפעילות המדינה כמובילה בתחום הסייבר, ולחזון הציוני שקרם עור וגידים בבאר שבע, בהיותה קרית הסייבר העולמית המאגדת מובילים מעולם האקדמיה, התעשייה, צה"ל והרשות.

הרשות מפעילה קשרים עם ארגוני CERT מקבילים בעולם לטובת קבלת התרעות בזמן אמת על תקיפות ומידע מקדים לחיסון, סיוע במיגור תקיפות סייבר כנגד מטרות ישראליות, קבלת דו"חות חקירה על פוגענים וניתוחים של אירועי סייבר כלל עולמיים. בחלק מהמקרים, ה-CERT הישראלי הוא הראשון בקרב הקהילה הבינלאומית לשתף מידע על איומים גלובליים –

מה שהעלה את קרנה של המדינה בעולם בתחום הסייבר.

מיום הקמת הרשות נחתמו הסכמי הבנות לשיתוף פעולה עם גופים מובילים בעולם להסדרת תהליכי עבודה משותפים, התקיימו עימם תרגילים

פלטפורמות להנגשת מידע

הסייבר הלאומי, מאזנת בין שמירה על סודיות המידע העסקי של ארגוני המשק ובין שיתוף מהיר וקל של מידע הגנתי רלוונטי ופנייה קלה לרשות לצורכי סיוע.

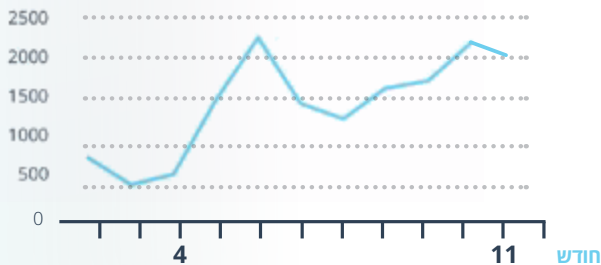
הרשות מפרסמת באופן תדיר התרעות והמלצות הגנה בפלטפורמה, שבפרק זמן קצר מתחילת הפעלתה ב-2017 הוכיחה את כוחה לשימוש המשק.

הגנת הסייבר דורשת שיתוף מידע רלוונטי בזמן אמיתי. אחת הדרכים לשיתוף מידע היא באמצעות פלטפורמה ייעודית, נגישה ומאובטחת, בה יוכלו ארגוני המשק האזרחי לקבל בצורה פשוטה, נהירה ומהירה מידע לצרכי הגנה ולשתף תובנות מתקיפות שאירעו אצלם.

לשם כך הוקמה מערכת הפצה בשם "סייברנט" - זירת הסייבר הישראלית. מערכת זו, יוזמה של מטה

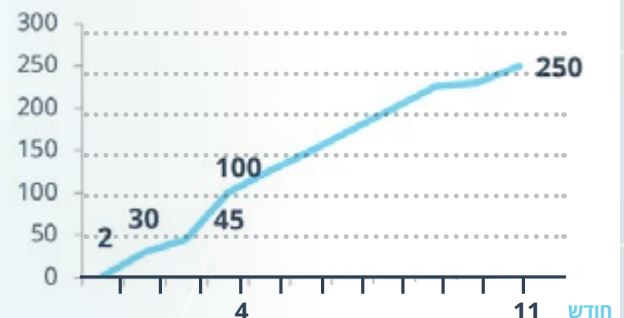
כניסות לסייברנט בחודש במהלך 2017

כניסות



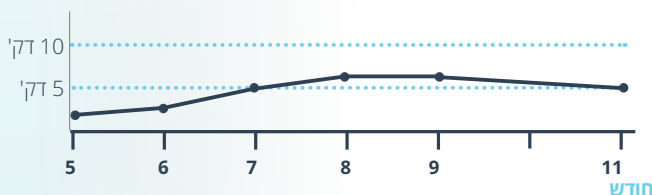
משתמשים רשומים בסייברנט - 2017

משתמשים



זמן ביקור ממוצע באתר הרשות

זמן ביקור



כניסות לאתר הרשות

2016

2,000 כניסות ייחודיות בחודש

2017

10,000 כניסות ייחודיות בחודש

מרכזים מגזריים במסגרת פעילות הרשות

ה-SOC הממשלתי

ה-SOC הממשלתי, שממוקם בתוך מתחם ה-CERT בבאר שבע, החל בפעילות מבצעית בקיץ 2017 ומנטר כיום את מערכותיהם של מספר משרדי ממשלה לצרכי הגנת הסייבר. עד לאמצע שנת 2018 צפוי ה-SOC הממשלתי לנטר ולשמור על בטחונם של 15 משרדי ממשלה שונים.

כבר בפרק הזמן הקצר מאז תחילת הפעילות, המערכת זיהתה איומים חדשים ואפשרה לחזק את הגנת הסייבר במשרדי הממשלה.

ה-SOC הממשלתי הוא מרכז הניטור הממשלתי להגנת הסייבר, פרי שיתוף פעולה בין רשות התקשוב הממשלתית והרשות הלאומית להגנת הסייבר. מערכת זו מהווה בשורה חדשה להגנת הסייבר במערכות משרדי הממשלה. המערכת, שהוקמה על בסיס תשתיותיו של המרכז לניהול אירועי סייבר של הרשות ומנוהלת בשיתוף היחידה להגנת הסייבר בממשלה (יה"ב) של רשות התקשוב הממשלתית, מנטרת את הרשתות ומערכות המידע במשרדי הממשלה, בחיפוש אחר מתקפות סייבר לשם איתורן, טיפול בהן, ניטרולן ומניעתן ברחבי המרחב הממשלתי.

מרכז הסייבר הפיננסי

בישראל. עם קבלת הדיווח הראשוני מלקוח של אחד הבנקים, תחקר המרכז את האירוע ובתוך 20 דקות שיתף את המידע עם כלל המערכת הפיננסית. בשלב הבא, פעל המרכז, בסיוע בינלאומי, להורדת האתרים המתחזים, והעביר את האירוע לגורמי האכיפה להמשך טיפול אל מול התוקף.

מרכז זה, לצד מרכז האנרגיה שהוקם ע"י משרד התשתיות הלאומיות, כבר מוכיח את הערך הרב ביצירת מומחיות מגזרית לטובת הגנת ארגוני המגזר הרלוונטי.



לצד מוקד הסיוע הראשוני, פועל מבאר שבע תחת ה-CERT הלאומי גם **מרכז הסייבר והרציפות הפיננסית**. המרכז, שהחל לפעול בראשית 2017 יחדיו עם משרד האוצר ובשיתוף הרגולטורים של המגזר הפיננסי, מתמקד בהגנה על התהליכים הפיננסיים המרכזיים: אספקת מזומנים, ביצוע עסקאות בכרטיסי חיוב, אספקת קצבאות, מסחר וסליקה בבורסה לני"ע. לקוחותיו הם ארגונים רבים ממגזר הבנקאות ושוק ההון.

אחד האירועים הבולטים שבהם טיפל המרכז הינו ניסיון הונאה מול לקוחות Paypal, במסגרתו הקים התוקף תשתית שלמה של אתרים מתחזים לבנקים

3.

מגבירים את החומות

פעילות להעצמת חוסן
המרחב האזרחי

משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר



הערכים שלנו: מנהיגות, צניעות, שיתוף ומקצוענות

תשתיות מדינה קריטיות

אחת ממשימות הליבה של הרשות, היא ההגנה על תשתיות המדינה הקריטיות.

ישראל הייתה מהראשונות בעולם, החל מתחילת שנות ה-2000, להכיר בצורך בהגנה על תשתיות מחשב חיוניות. בפברואר 2002, הטיל הקבינט המדיני-בטחוני את האחריות להגנה על תשתיות אלה על "היחידה הממלכתית להגנה על מערכות ממוחשבות חיוניות", יחידה שהוקמה במסגרת שירות הביטחון הכללי ופעלה על פי החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

תפקיד יחידה זו, שעם השנים שונה שמה ל"רשות לאבטחת מידע", היה להנחות את גופי תשתיות המדינה הקריטיות בענייני אבטחת המידע שלהן, ולפקח על ביצוען.

ועדת היגוי אובייקטיבית היא זו שאישרה את צירופו של גוף מסוים לרשימת גופי התשתית הקריטית של המדינה, וזאת על בסיס תבחיני נזק מוסכמים ועל בסיס אישור כנסת ישראל. גוף שהוכנס תחת מטריית ההנחיה קיבל בהתאם מעטפת הגנה מותאמת וייחודית.

עם השנים הוכנסו גופים שונים למסגרת אותו חוק, ובהם חברת החשמל, בנק

ישראל, רכבת ישראל, הבורסה לניירות ערך, וגופים חשובים נוספים.

כעשור וחצי לאחר מכן, עם השינויים הטכנולוגיים הרבים שהתרחשו ועל רקע חדירת הטכנולוגיה למרחב האזרחי, קם הצורך בהקמת גוף טכנולוגי-מבצעי ייעודי,

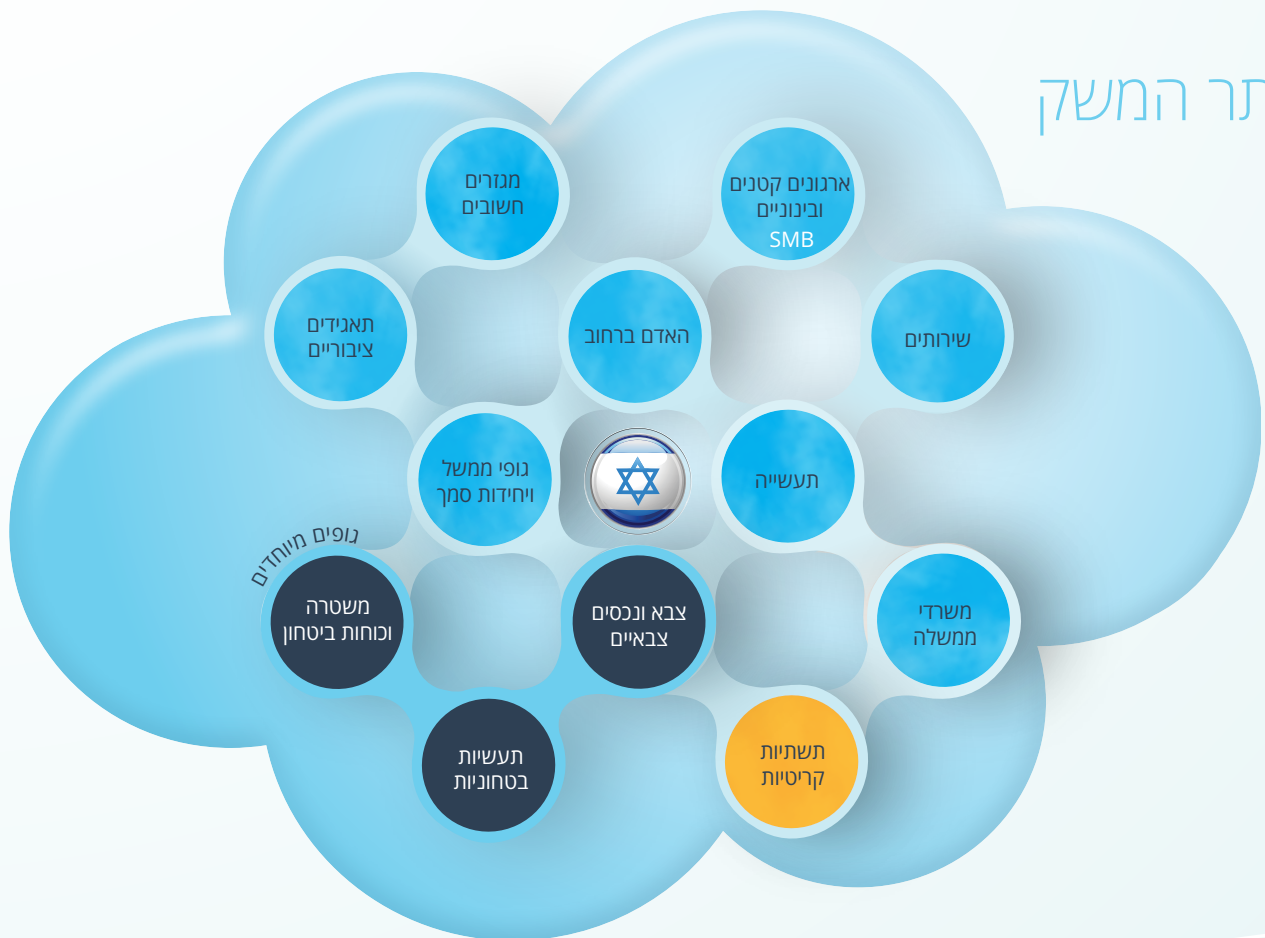


בעל מאפיינים אזרחיים ופתוחים לציבור, שיהיה אחראי על הגנת הסייבר המדינתית ובתוך כך, גם על הגנת תשתיות המדינה הקריטיות. גוף זה - הרשות הלאומית להגנת הסייבר - הוקם לבסוף באפריל 2016.

בהתאם, באוגוסט 2016 אישרה הכנסת את העברת האחריות על גופי התמ"ק, משירות הביטחון הכללי לרשות הלאומית להגנת הסייבר. ביולי 2017 הושלם המהלך, בשיתוף פעולה הדוק ופורה עם שירות הביטחון הכללי, ו-26 גופי תשתיות המדינה הקריטיות נמצאים כיום בהנחיה ייעודית ישירה של הרשות - הן לגבי הגנת מערכות המחשוב שלהם והן לגבי המידע המסווג המצוי בהם. ומה לגבי יתר המשק? על כך נרחיב להלן.

ישראל הייתה מהמדינות הראשונות בעולם, החל מתחילת שנות האלפיים, שהכירו בצורך להגן על תשתיות מחשב חיוניות.

יתר המשק



שישתמשו בסמכויותיהם על מנת להחיל נורמות בתחום הגנת הסייבר על מושאי ההגנה השונים, בהתאם לצורך הציבורי.

ההיגיון לכך היה שאמנם ממד הסייבר מוסיף תרחישי תקיפה נוספים, אולם מטרות הרגולציה – הגנה על חיי אדם, איכות הסביבה, רווחת הצרכנים ועוד – נותרו כשהיו. בהתאם, בשנתיים האחרונות עמלה הרשות

על הקמת "יחידות סייבר מגזריות" בממשלה, תוך מימון והכשרת אנשיהן. יחידות אלה אמונות על מיפוי הגופים מושאי ההגנה, מדידת מצב חוסנם ותיעדוף ההגנה בהם על פי האינטרס הציבורי ובהתאם להכוננת הרשות. בחרנו לתת לכם טעימה מפעילות זו:

מלבד כמה עשרות גופים שהוגדרו כתשתיות מדינה קריטיות ועל כן קיבלו מעטפת הגנה מדינתית, ברור היה שקיימים מגזרים וארגונים נוספים שפגיעה בהם בסייבר היא בעלת סיכון מובהק לאינטרס הציבורי.

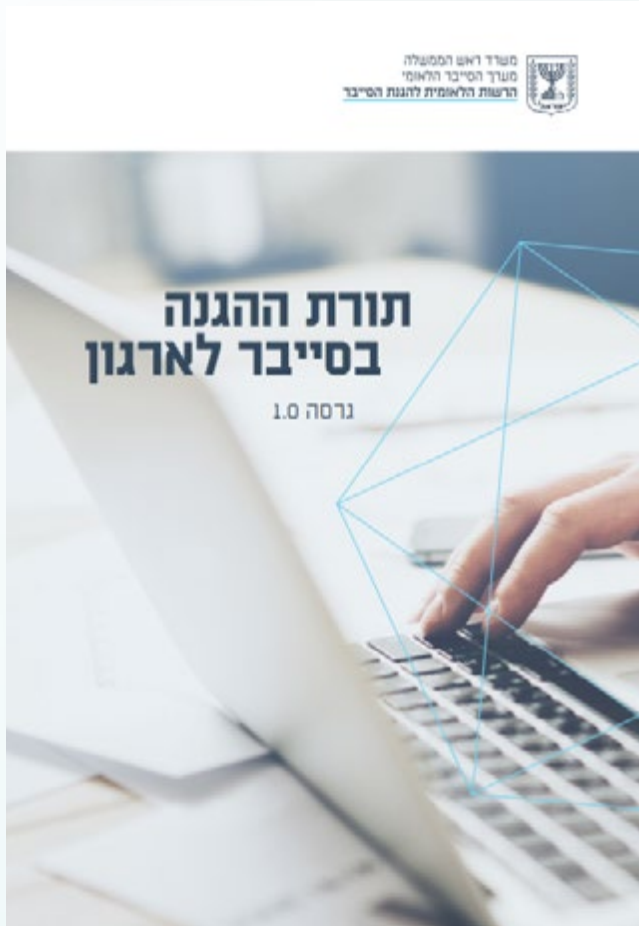
כאמור, המודל שבנתה מדינת ישראל להגנה על תשתיות מדינה קריטיות סיפק מענה מוצלח ומתקדם לזמנו. ואולם, ברקע הדברים ריחפה השאלה כיצד יגנו על עצמם יתר גופי המרחב האזרחי. שכן, מלבד כמה עשרות גופים שהוגדרו כתשתיות מדינה קריטיות ועל כן גם קיבלו מענה מדינתי, ברור היה שקיימים מגזרים וארגונים נוספים שפגיעה בהם בסייבר היא

בעלת סיכון מובהק לאינטרס הציבורי. הקמת הרשות הלאומית להגנת הסייבר חידדה את הצורך במענה לשאלה זו. הדרך שהתוותה ממשלת ישראל באמצעות החלטות הממשלה 2443 ו-2444 היא הכוונה מקצועית של הרשות את הרגולטורים השונים במשק,

דוגמאות לפעילות מול המשק האזרחי



תורת ההגנה בסייבר לארגון



כיום, העולם מתחיל את אט להבין כי מתקפות סייבר עלולות לפגוע בארגונים ואף להביא להפסקת תהליכי ייצור, לנזק כלכלי ולפגיעה במוניטין שלהם. כדי לסייע לממשק האזרחי בישראל להיערך להתמודדות עם איומים אלה, פרסמה הרשות בראשית 2017 את **"תורת ההגנה בסייבר לארגון"**. תורת ההגנה, שנכתבה מתוך היכרות עמוקה עם המאפיינים של המשק הישראלי ולאחר בחינה מעמיקה של מקורות רבים בארץ ובעולם, מחייבת את משרדי הממשלה ויחידות הסמך שלה ומומלצת עבור יתר הארגונים במשק.

עבודה על פי תורת ההגנה הארגונית מעמידה לרשות כל ארגון בישראל – קטן כגדול – כלים ברורים למימוש ההגנה מפני הסיכונים העסקיים הנגזרים מאיומי הסייבר, ומסייעת לו לבנות תכנית עבודה תחת תהליך סדור של ניהול סיכונים. לעבודה עם המסמך יתרונות נוספים, כגון מיפוי יעדי ההגנה, שהם קריטיים לתפקוד הארגון גם ללא הקשרי הסייבר; יכולת לתרום למוניטין הארגון בעולם מקוון, בו קיימת חשיבות רבה לעמידות הארגון מפני מתקפות סייבר; הקניית ידע לגבי דרישות הגנה שעל הארגון לדרוש מקבלני משנה שלו ועוד.

[מוזמנים להוריד את קובץ תורת ההגנה מאתר הרשות](#)



קידום כוח אדם מקצועי בתחום הגנת הסייבר

לאחר פרסום מסמך המדיניות בנושא מקצועות הסייבר על ידי מטה הסייבר הלאומי בדצמבר 2015, החלה הרשות בבחינה מעמיקה באשר לפער המקצועיות של ההון האנושי בתחום ובגורמים לתופעה זו. זאת, מתוך תפיסת עולם לפיה אין הרשות רוצה להתערב אלא

עם התגברות הצורך של העולם המודרני בטכנולוגיה, מתעצמים גם מקומם וחשיבותם של האנשים הנדרשים לתפעולה. לכן, כחלק מהפעילות של הרשות, אנו פועלים להגדלת כמות המועסקים בתחום, תוך הקפדה על רמת מקצועיות גבוהה.

דוגמאות לפעילות להעצמת כוח אדם מקצועי



מבחיני הסמכה לבדיקת הרף המקצועי של העוסקים בתחום. עם גיבוש התובנות מהפיילוט, ייבחן כיצד המהלך השפיע על כשירותם המקצועית של אנשי הגנת הסייבר, ובהתאם, תישקל האפשרות להרחיב את יישום ההסמכה הישראלית גם למגזרים נוספים, בהתאם למדיניות שתיקבע.

במקום שמוכח כי קיים בו "כשל שוק" – קרי, כוחות השוק עצמם נכשלו ביצירת תוצאה הרצויה חברתית. מבדיקה עם מומחי סייבר ישראלים ועולמיים ברשויות השונות, באקדמיה, בתעשייה ובמחקר, לא עלתה הוכחה מובהקת לכשל שוק בכשירות אנשי מקצועות הסייבר. בהתאם, התוותה הרשות פיילוט שבעיקרו



קידום נשים בסייבר

כולנו יודעים שתופעת המחסור של חלק מן האוכלוסייה הישראלית במגזר הטכנולוגי היא בעיה של ממש – וגם תחום הגנת הסייבר סובל מכך. כאן, משתלבים הן הרצון שלנו לקדם שוויון בתחום והן הצורך הממשי ברתימת כ"א מקצועי לתחום מחלקי אוכלוסייה שלא משתתפים בדרך כלל בו.

בשנת 2018 נתמקד בעידוד נשים להצטרף למאמץ זה.

המלאכה לא תמה. הרשות היא כאותו תינוק, שעם הזמן למד לעמוד ולאחר מכן לצעוד בזהירות ובמתינות בכוחות עצמו, עד שהוא מגביר את קצב מרוצו. עולם הסייבר הוא עולם דינמי שנע בעצמו במהירות גבוהה והדבר מחייב להמשיך ולגייס אנשים ומשאבים ולהשקיע תשומות על מנת להמשיך להיות רלוונטיים להגנת הסייבר המדינתית.

אם לא נעשה כן, היעדר תנועה קדימה משמעותה תהא נסיגה לאחור.

יצאנו לדרך עם אמירה ברורה ונחרצת לפיה **"זכותם של כל אדם וכל ארגון בישראל**

לעשות שימוש במרחב הסייבר ללא חשש". את הצעד הראשון, ההקמה, השלמנו בשנתיים. פנינו אל השנים הבאות, אל האתגרים שהעולם הטכנולוגי יציב בפנינו ואל יישום המשימה כבדת המשימה שעליה אנו אמונים.

"זכותם של כל אדם וכל ארגון בישראל לעשות שימוש במרחב הסייבר ללא חשש".

במובנים רבים, הקמת הרשות הלאומית להגנת הסייבר הייתה בבחינת ניסוי בהקמת "סטארט אפ" ממשלתי. האתגר היה גדול, מכל כיוון שרק ניתן היה לחשוב עליו: החל מהצורך בגיוס כ"א איכותי לגוף ממשלתי שהיה חסר כל מוניטין כלפי מועסקות ומועסקים רלוונטיים; דרך הכניסה הממשלתית הראשונית למרחב הסייבר,

תחום שמנוהל בעיקר על ידי גופים פרטיים ותחרותיים, והצורך ברתיעת "משקיעים" ו"סוכני שטח" רלוונטיים; וכמובן ההצטרפות למועדון החשוב של מה שקרוי "קהיליית הביטחון" במדינת

ישראל. בו בזמן, היה זה אקוטי לשמור ככל הניתן על חזית פתוחה לציבור, שכן בעולם האינטרנטי שעליו אמונה הגנת הרשות – חופש ואור השמש הם שמות המשחק.

כיום, שמונה רבעוני פעילות לאחר היציאה לדרך, ניתן לומר כי על אף כלל הקשיים שליוו את תהליך ההקמה, שתוכנן להתרחש בתהליך תלת-שנתי, מתייצב עתה על רגליו גוף נוסף בישראל, האמון על הגנת הסייבר של המרחב האזרחי של המדינה.

תהליך זה לא יכול היה להתבצע ללא הנשים והגברים הנפלאים שהצטרפו במעלה הדרך ל"הרפתקה" זו וללא התומכים הרבים בציבור, שהבינו שעל אף החששות מפני הקמת גוף ממשלתי נוסף, יש בהקמת גוף ייעודי להגנת הסייבר את הפוטנציאל לסייע לכלל המרחב האזרחי להגן על עצמו טוב יותר.



רוצים לדעת עוד? 
בואו לבקר אותנו ב-



הרשות הלאומית להגנת הסייבר | NCSA.GOV.IL
בפייסבוק ובלינקדאין

הותקפתם?

 *9344