סיכום שנה 2025

מערך הסייבר הלאומי

יוסי כראדי

דברי ראש מערך הסייבר הלאומי

שנת 2025 עמדה בסימן מלחמה רב זירתית עבור מדינת ישראל. החזיתות הפיזיות ידעו תנודות בעצימות הלחימה, החל משיא הלחימה ב'עם כלביא' ועד לתום מלחמת 'חרבות ברזל', אך חזית הסייבר נותרה פעילה.

היקף האיומים, קצב ההתרחשות והמורכבות המבצעית של אירועי הסייבר ההולכים וגוברים המחישו ביתר שאת כי במרחב הסייבר אין 'הפסקת אש' וכי זוהי **חזית אסטרטגית מרכזית בביטחון הלאומי.**

מדינת ישראל היא **המדינה השלישית בעולם** בהיקף תקיפות הסייבר נגדה (דו"ח מיקרוסופט לשנת 2025). במהלך השנה דווחו למערך הסייבר הלאומי למעלה מ־**26,000** אירועי סייבר המהווים עלייה של כ־**55%** בהשוואה לשנת 2024.

המסקנה העולה מהנתונים ברורה: במרחב הסייבר אין קו חזית ברור - **כל ארגון, כל מערכת וכל אזרח הם יעד למתקפה** ומטרתה היא פגיעה ברציפות התפקודית, באזרחי המדינה, מתוך רצון לערער את החוסן הלאומי וליצור תחושת איום מתמדת.

אל מול מציאות זו, פעל מערך הסייבר הלאומי לחיזוק ההגנה הלאומית ולהעמקת החוסן של המשק כולו, לשפר את מנגנוני התיאום בין הגופים השונים ולהעמיק את שיתופי הפעולה עם משרדי הממשלה, המגזר הפרטי והקהילה הבינלאומית.

פרסום תזכיר חוק הגנת הסייבר בתחילת 2026 מהווה ציון דרך היסטורי: לראשונה מוגדרת בישראל תפיסת הגנת סייבר לאומית, נקבעים סטנדרטים מחייבים לארגונים חיוניים ולספקי שירותים דיגיטליים, ומוסדרים מנגנוני דיווח, פיקוח ואכיפה על אירועי סייבר משמעותיים. החוק יעגן את הגנת הסייבר כאינטרס לאומי, ויהווה יישור קו עם הסטנדרטים הבינלאומיים.

במקביל, השקנו את התוכנית הרב־שנתית להגנת הסייבר של מדינת ישראל לשנים הקרובות שאושרה עקרונית ע"י ראש הממשלה ותעוצב יחד עם האוצר בשנת 2026. התוכנית מתמקדת בשלושה צירים מרכזיים: אבטחת ענן, שילוב הסייבר עם הבינה המלאכותית והיערכות לעידן הקוונטי.

למול האיומים הרבים בכלל הזירות ומתקפות הסייבר לאורך כל השנה ולמרות הצלחות של אויבנו בסייבר במקומות מסוימים, מערך הסייבר הלאומי עמד במשימתו הראשית - **הגנה על התשתיות הקריטיות והבטחת רציפות התפקוד הלאומית של מדינת ישראל.** עשינו זאת באמצעות שיתופי פעולה עמוקים בארץ ובעולם, מקצוענות, מסירות ובעיקר האנשים המצוינים אשר עומדים על המשמר.

נמשיך לפעול ללא לאות במאמץ ההגנה הלאומית בסייבר מתוך הבנה כי לא לעולם חוסן.

איננו יכולים לבחור מתי תפרוץ המערכה הבאה, אך אנו בוחרים להיות מוכנים אליה.

אירועי סייבר מרכזיים בעולם

שנת 2025 מסמנת שלוש מגמות משמעותיות במתקפות הסייבר:

- מתקפות סייבר מבוססות AI, שמסוגל לייצר נוזקות ומתקפות הנדסה חברתית שנראות אמינות.
- מתקפות שמתחילות בגניבת פרטי התחברות של עובדים, מה שמאפשר לתוקפים להיראות כמשתמשים לגיטימיים.
- תקיפת חברות דרך חדירה לספקים בשרשרת האספקה שלהן.

אירועי סייבר מרכזיים בעולם

בשנת 2025

שדות תעופה באירופה

Collins Aerospace - תקיפה על מערכות הצ'ק אין בשדות התעופה של ברלין, היתרו, דאבלין ובריסל, שגרמה לביטול של 217 טיסות. כ-10,000 אנשים לא הגיעו ליעדם ונגרם נזק המוערך בכ-**150 מיליון יורו.**

(ספטמבר 25')

שדות תעופה בצפון אמריקה

סדרת פריצות סייבר שהתמקדו במערכות הכריזה ומסכי המידע לציבור במספר שדות תעופה. האקרים השתלטו על המערכות ושידרו מסרים פוליטיים אנטי-ישראלים ואנטי-אמריקאים, התומכים בחמאס.

(אוקטובר 25')

חברת F5

חברת F5 היא אחת מספקיות היישומים ותשתיות תקשורת החשובות בעולם. התוקפים הצליחו לגנוב קוד מקור ומידע על פגיעויות במוצרי החברה, ולהשיג גישה לליבת מוצרי החברה, המשמשים ממשלות ותאגידי ענק בכל העולם וגם בישראל.

(אוקטובר 25')

Jaguar Land Rover

אחת מתקיפות הסייבר החמורות בתולדות בריטניה שבוצעה נגד יצרנית הרכב Jaguar Land Rover. התקיפה השביתה את מערכות המידע ותשתיות ה-IT של החברה והיא נאלצה לעצור לחלוטין את הייצור במפעליה המרכזיים עד ינואר 2026. הנזק הכלכלי הישיר של התקיפה נאמד בכ-**1.9 מיליארד ליש"ט** והיא יצרה 'אפקט דומינו' שהסב נזקים לכ-**5,000 ארגונים נוספים** שהיו בקשרים עם החברה.

(אוגוסט '25 - ינואר 26')

אירועי סייבר מרכזיים בישראל

בשנת 2025

אירועי סייבר מרכזיים בישראל

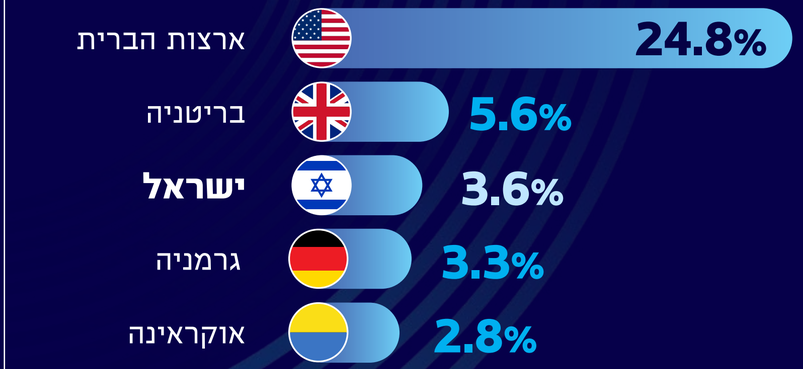
היקף מתקפות הסייבר נגד ישראל - מהגבוהים בעולם

לפי דו"ח ההגנה הדיגיטלית של מייקרוסופט ל-2025,
ישראל היא המדינה השלישית בעולם במספר המתקפות שהיא חוותה
במחצית הראשונה של השנה, ומופנות בראש ובראשונה כלפי מגזר ה-IT.
התקיפות התמקדו בתשתיות מדינה קריטיות ובמגזרים חיוניים נוספים
כמו: מגזרי האנרגיה, הרשויות מקומיות, הממשלה והבריאות.

על פי הדו"ח, כשני שלישים **(64%)** מכלל פעילות הסייבר של קבוצות
תקיפה מדינתיות איראניות מופנית נגד ישראל.

Microsoft

דירוג המדינות המותקפות ביותר בסייבר (ינואר-יוני 2025):



דירוג המדינות המותקפות ביותר על ידי קבוצות תקיפה איראניות:

אירועי סייבר מרכזיים בישראל

בשנת 2025

במהלך השנה האחרונה, טיפל המערך במספר אירועי סייבר משמעותיים שסיכנו **שירותים חיוניים לאזרח ולמשק.**

מאי 2025

- חדירה לחברת אחסון - סיכון לתשתית קריטית

יוני 2025

- פריצה לספק פתרונות דיגיטליים שהובילה להפצת מאות אלפי שיחות הפחדה לאזרחים

יולי 2025

- דלף מידע מחברה בתחום הכשרה לתעופה

אוגוסט 2025

- ניסיון למחיקת מידע בחברה בתחום התקשורת

ספטמבר 2025

- דלף מידע מחברת הנגשת מסמכים

אוקטובר 2025

- כופרה בחברת הסעות
- חדירה לתיבות דוא"ל בחברת מים וביוב
- גניבת מידע מתיבות דוא"ל של בית חולים וניסיון לשבש את תפקודו

נובמבר 2025

- ניסיון להשחית מסופונים של חברה המספקת פתרונות תשלום
- דלף מידע מחברה בתחום פתרונות דיגיטליים לתחום התיירות

דצמבר 2025

- חשד לאירוע בספק שירותים דיגיטליים בתחום השכר

- קוד זדוני באיזור אישי באתר של חברה בתחום המים והביוב
- מחיקת שרתים של לקוחות של חברת מחשוב ענן
- פריצה לתיבות דוא"ל של תאגיד בתחום התעסוקה, שהובילה להפצת הודעות דוא"ל זדוניות
- מחיקת מידע בחברה בתחום הפיננסי
- דלף מידע בחברת החזקות בתחומי האנרגיה
- הקרנת מסרי תודעה על מסכים של תחנות תחבורה ציבורית
- חשד לדלף מידע מחברה המספקת פתרונות דיגיטליים למגזר הבריאות
- דלף מידע ממכון מחקר

אירועי סייבר מרכזיים בישראל

תובנות ממבצע "עם כלביא" בהיבטי הגנת הסייבר

עם פרוץ מבצע "עם כלביא" ביוני 2025, העלה מערך הסייבר הלאומי את רמת הכוננות, פתח חמ"ל לאומי ייעודי למבצע בהיבטי הגנת סייבר, ופעל לסנכרון בין יחידות ממשלתיות וחברות טכנולוגיה בינלאומיות כדי לספק הגנה אקטיבית ובניית תמונת מצב.

פעילות תוקפי הסייבר התרחבה משמעותית לצד שליחת עשרות אלפי הודעות השפעה לאזרחי ישראל. התקיפות כוונו למגוון רחב של מגזרים אזרחיים, תוך שילוב בין תקיפות סייבר להשפעה פסיכולוגית ולעיתים אף במטרה לשרת ישירות פעילות קינטית נגד יעדים בישראל.

15
קבוצות תקיפה

423
פניות על הנדסה חברתית

84
אירועים ואינדיקציות

שילוב בין סייבר ללוחמה קינטית ("קינטי קיברנטי"):
חיבור בין פעולות איסוף וסייבר לפגיעה בעולם הפיזי ובכלל זה פריצה למצלמות ואיסוף מידע על יעדי איש.

שימוש נרחב בלוחמת תודעה מבוססת סייבר להעצמת הבהלה:
התוקפים ניצלו פריצות לשירותים להפצת הודעות ושיחות תוך התחזות לגורמים רשמיים ככלי לייצור פחד המוני ולפגיעה במורל של האזרחים. המערך בלם את הרחבת התפוצה והוציא הודעות אזהרה.

פגיעה רוחבית במגוון מגזרים אזרחיים:
התוקפים מיקדו מאמצים בטווח רחב של מגזרים המספקים שירותים חיוניים לאזרח וכן ספקי שירותים דיגיטליים, אך לא הצליחו לייצר הפרעה לרציפות התפקודית.

חקיקה בחירום:
לאור חומרת האיומים, המערך קידם חקיקת חירום למגזר השירותים הדיגיטליים שהיו שרשרת אספקה למגוון שירותים וחברות במשק, שנועדה לבלום מתקפות בטרם התפשטותן.

דיווחים שהתקבלו במרכז המבצעי 119

במהלך השנה האחרונה, טיפל מרכז 119 של מערך הסייבר הלאומי ביותר מ-**26,000** פניות ודיווחים על אירועי סייבר במגוון רמות חומרה, החל מהודעות פישינג ועד לפריצות מורכבות למערכות מחשוב.

לצד הטיפול בפניות הנכנסות, פעל המערך באופן יזום ופנה לכ-**2,300** ארגונים שונים שעלו לגביהם סימנים המצביעים על מתקפת סייבר אפשרית, במטרה לסייע להם להתגונן מבעוד מועד ולצמצם נזקים פוטנציאליים.

דיווחים שהתקבלו במרכז המבצעי 119

26,498
דיווחים בשנת **2025**

יותר **55%** דיווחים
בהשוואה לשנת **2024**

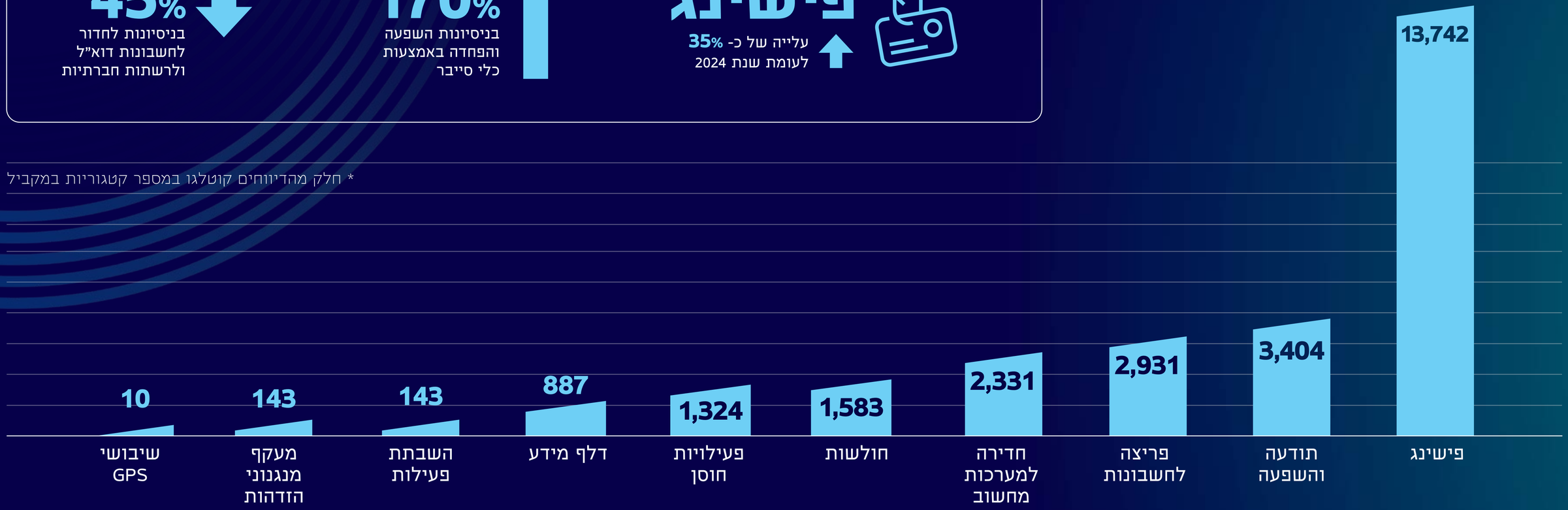
שלוש סוגי המתקפות הנפוצות ביותר

הדיווח השכיח ביותר השנה:
פישינג
עלייה של כ- **35%** לעומת שנת 2024

עלייה חדה של מעל
170%
בניסיונות השפעה והפחדה באמצעות כלי סייבר

ירידה של כ-
45%
בניסיונות לחדור לחשבונות דוא"ל ולרשתות חברתיות

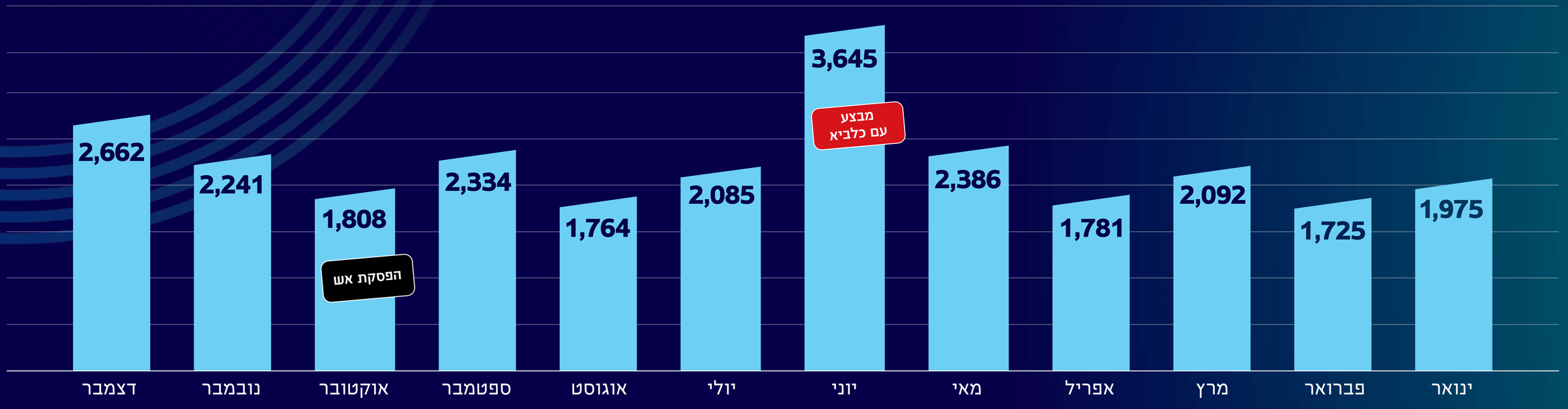
* חלק מהדיווחים קוטלגו במספר קטגוריות במקביל



דיווחים שהתקבלו במרכז המבצעי 119

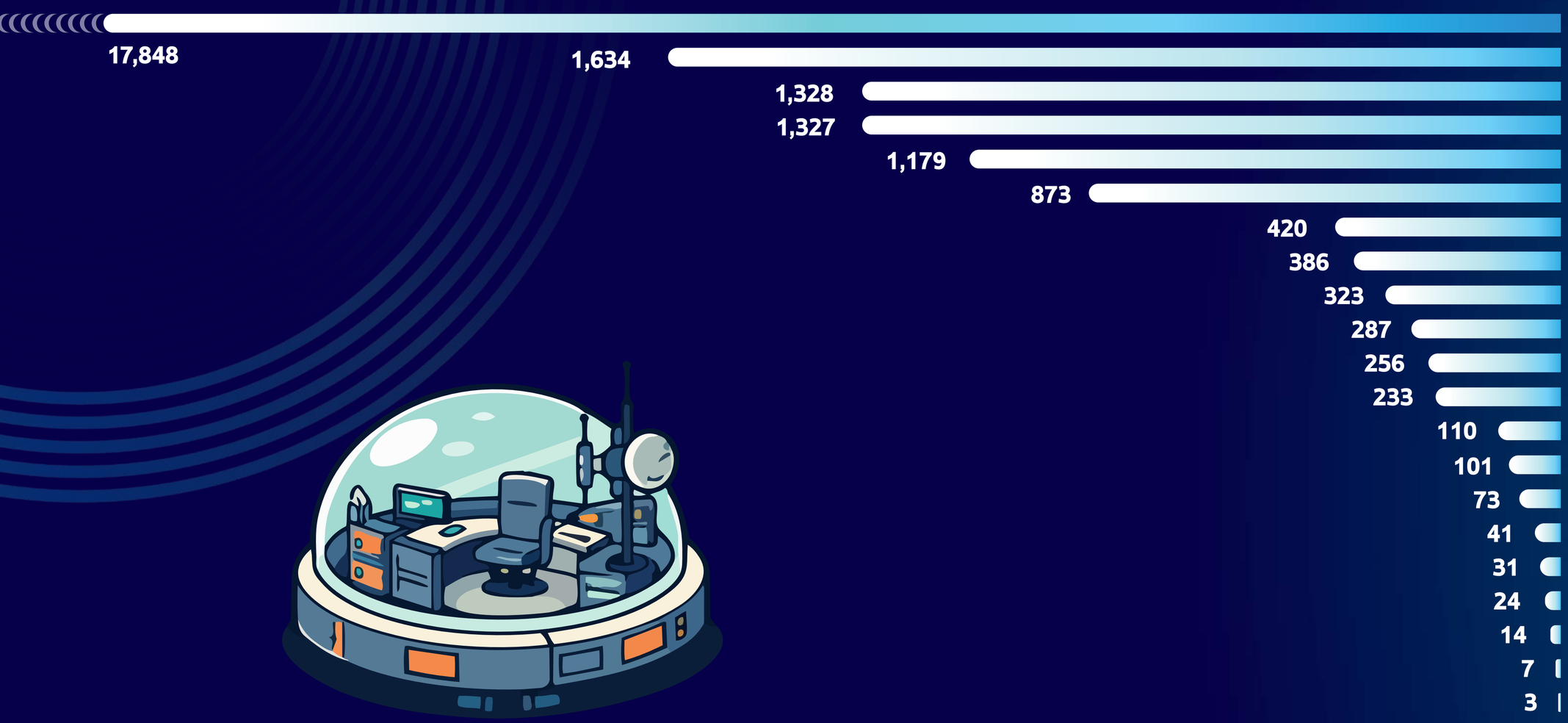
התפלגות הפניות והאירועים לאורך השנה

במהלך מבצע "עם כלביא" בחודש יוני, נרשמה עלייה משמעותית במספר הפניות ואירועי הסייבר שטופלו על ידי מרכז 119.
מגמה זו נבעה משילוב של הסלמה בניסיונות התקיפה, שכללו בעיקר הודעות ושיחות הפחדה לצד הפצת מידע עוין והודות לערנות גבוהה ורגישות מוגברת של הציבור, שהובילו לגידול בשיעור הדיווחים על ניסיונות אלו.



דיווחים שהתקבלו במרכז המבצעי 119

התפלגות הדיווחים והאירועים לפי מגזרים



התרעות למשק

במהלך 2026 הוציא מערך הסייבר הלאומי **2,482** התרעות למשק - חלקן לכלל הארגונים והחברות במשק, חלקן למגזר מסוים וחלקן לארגון ספציפי.

מדובר בהכפלה של פי **2.5** במספר ההתרעות לעומת 2024, בעיקר בשל הגידול בהתרעות היזומות של המערך לארגונים ספציפיים. התרעות מגיעות ממידע שעולה במגוון טכנולוגיות הניטור והזיהוי של המערך.

התרעות למשק

בשנת 2025

התרעות לציבור (כחולות)

התרעות על ניסיונות פישינג והפחדה

51 — 2025

42 — 2024

התרעות פומביות (לבנות)

התרעות לכלל המשק

92 — 2025

150 — 2024

התרעות לקבוצת עניין מוגדרת (צהובות)

התרעות למגזר ספציפי

35 — 2025

26 — 2024

התרעות לארגון ספציפי (אדומות)

התרעות לארגון שלגביו התקבלה אינדיקציה לניסיון תקיפה

2,304 — 2025

518 — 2024

* הצבעים הם לפי פרוטוקול TLP: White / Amber

סיכום שנה 2025

נתיבי תקיפה עיקריים שזוהו באירועי סייבר בישראל

חקירת עשרות אירועי סייבר בהיקפים שונים על ידי המערך וחברות IR (באמצעות פורום MIRROR) בשנה החולפת העלתה מספר נתיבי חדירה מרכזיים לארגונים.

המגמה של שימוש בשיטת דיוג (פישינג) וגניבת מידע התגברה השנה, לצד ניסיונות חדירה דרך שרשראות האספקה של הארגונים.

נתיבי תקיפה עיקריים שזוהו באירועי סייבר בישראל

חמשת נתיבי החדירה המרכזיים לארגונים בישראל

פישינג וגניבת זהויות
הודעות דוא"ל מתחזות שמובילות לדלף פרטי התחברות או לצרופה מזיקה ומביאים לחדירה למערכות ארגוניות.

מערכות חשופות ולא מעודכנות
חולשות במוצרי אבטחה וטכנולוגיות לחיבור מרחוק, ממשקי העלאת קבצים פתוחים שלא הוגדרו כראוי ו־FW/CRM לא מעודכנים.

Infostealer
דלף מידע שנגרם בשל נוזקות שאוספות סיסמאות ומידע רגיש ושולחות אותו ישירות לתוקף.

בקרי IoT ונכסים לא מנוהלים
ציוד מחובר לרשת ללא הקשחה מספקת המשמש כנקודת כניסה לארגון.

שרשרת אספקה וספקי שירות
תקיפה דרך ספקי צד שלישי, במיוחד IT, תקשורת ושירותים מנוהלים, כקיצור דרך לארגונים גדולים.

גילוי אחראי של חולשות

פעילות יזומה לזיהוי ולצמצום חולשות במרחב הישראלי

המערך פועל בצורה פרו-אקטיבית כדי לזהות ולהתריע על חולשות במשק ולהיות צעד אחד לפני התוקפים. לשם כך מפעיל המערך תוכנית לגילוי אחראי של חולשות, שבה חוקרים וחוקרות אבטחה מגלים חולשות במערכות של ארגונים, מדווחים עליהן למערך, והמערך מתריע על החולשה בפני הארגון כדי שיטפל בה. ההישגים של החוקרים והחוקרות מקבלים הכרה פומבית בהיכל התהילה של המערך.

גילוי אחראי של חולשות

פעילות יזומה לזיהוי ולצמצום חולשות במשק הישראלי

כחלק מהמאמץ לחזק את ההגנה של המשק מערך הסייבר מפעיל תכנית ייעודית לגילוי אחראי של חולשות:
קהילה של חוקרי אבטחה ומומחי סייבר שמדווחים על פרצות אבחה שמצאו במרחב הדיגיטלי.
המערך מנתח את הדיווחים וסוגר את החולשות כדי שגורמים עוינים לא יוכלו לנצל אותן.

658
דיווחי VDP שהתקבלו

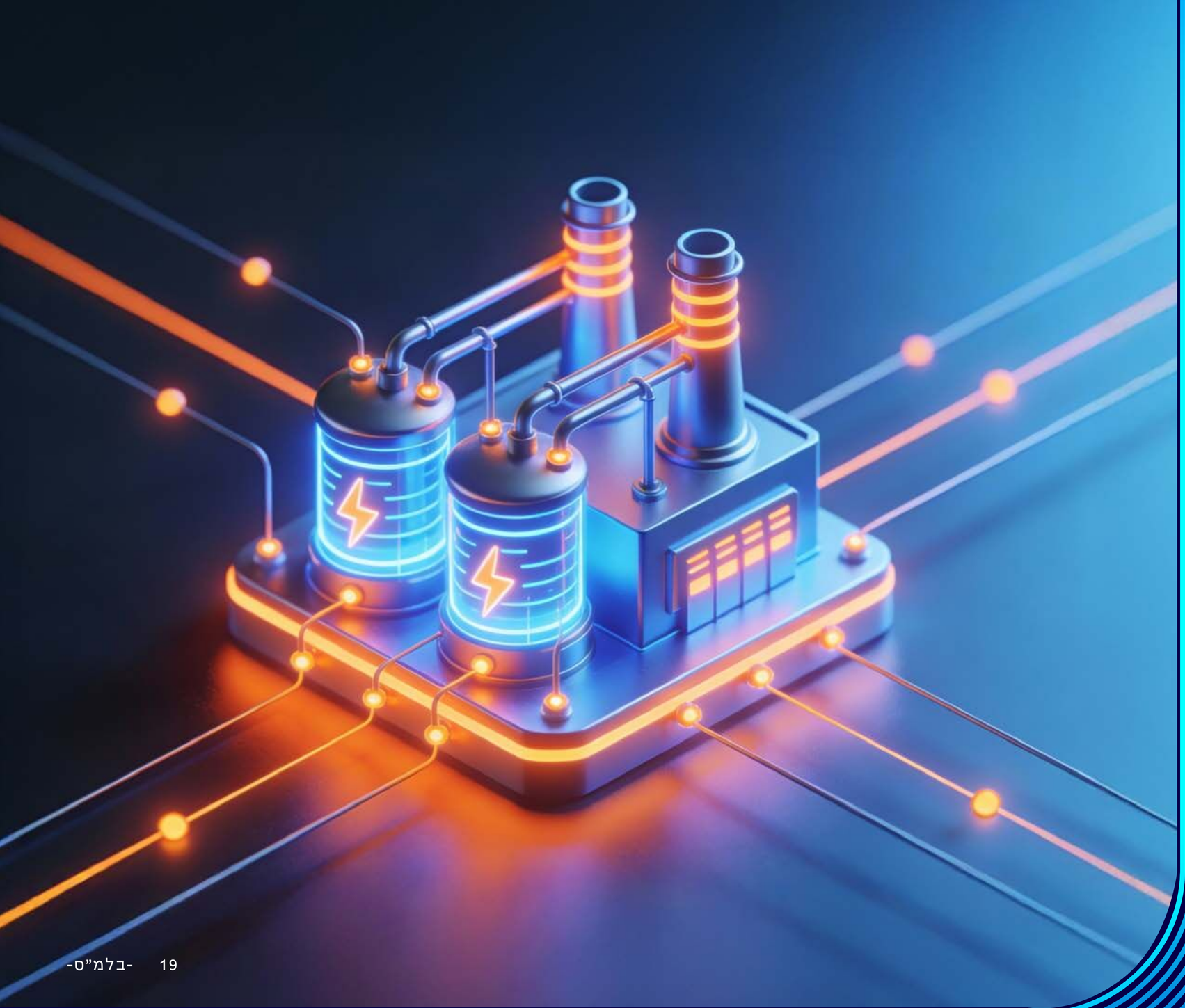
353
מדווחים בהיכל התהילה

32
מדווחים חדשים שהצטרפו השנה

39
חולשות CVE שנחתמו

CVE המערך שותף בתוכנית העולמית של ארגון MITRE לאסגרה ולחיתום חולשות והוסמך לרישום פגיעויות וחשיפות נפוצות.

VDP תוכנית ל"גילוי חולשות אחראי" (VDP - vulnerability disclosure program) על ידי חוקרים וחוקרות שמזהים חולשות במשק ומדווחים עליהן למערך הסייבר.



הגנה על תשתיות מדינה קריטיות

גופים המוגדרים כתשתית מדינה קריטית הם גופים אשר פגיעה בהם עלולה להסב נזק לאומי עצום. כדי לוודא שתשתיות אלו נמצאות במידת הגנת סייבר מרבית, המערך מלווה אותן באופן צמוד, מנחה ומבקר אותן.

הגנה על תשתיות מדינה קריטיות

בתקופת המלחמה, עלו הנסיונות מצד אויבינו לפגוע בתשתיות קריטיות כדי לשבש את שגרת החיים בישראל, אך גם בשגרה הן מהוות יעד תקיפה מרכזי.

נכון לשנת 2025 כ- **80%** מגופי התמ"ק נמצאים ברמת בשלות הגנה מתקדמת המצביעה על יכולת גבוהה להתמודדות עם מרבית מתקפות הסייבר השכיחות וגם עם תרחישים מורכבים יותר.

שאר הארגונים מצויים בשלבי הסמכה שונים, כאשר ארגונים שהצטרפו לאחרונה נמצאים בראשית ההסכמה ויתקדמו בתקופה הקרובה.

מיזמים טכנולוגיים לאומיים להעלאת החוסן

במסגרת מרכז הניטור והבקרה הלאומי (NSOC) מעניק המערך מענה לאיומי סייבר ייחודיים למגזרים שונים במשק, בהם הפיננסי, הממשלתי, בטחון, פנים, האנרגיה, תקשורת והגנת הסביבה.

באמצעות טכנולוגיות מתקדמות מבוססות אוטומציה וצוות אנליסטים בכירים, המרכזים מנתחים ידע שהתקבל מהגופים, משתפים מידע, מגבשים תמונת מצב, מונעים אירועי סייבר, מסייעים לרציפות תפקודית וכן מפיקים תובנות לאומיות.

במהלך המלחמה שם המערך כמטרה את נושא העלאת החוסן במשק, בניסיון להגיע לכמה שיותר ארגונים ומגזרים.

מיזמים טכנולוגיים לאומיים להעלאת החוסן

קהילות סייבר

TITAN

במטרה להעלות את החוסן הלאומי ולהגדיל את היכולת הלאומית להתמודד עם היקף נרחב של מתקפות, הקים מערך הסייבר הלאומי פורום חברות אשר מספקות שירותי אבטחה מנוהלים (MSSP), בדגש על שירות "SOC as a Service".

החברות בפורום מעניקות שירותי הגנה לאלפי ארגונים במשק. שיתוף מידע טכני מהיר בין המערך לחברות מאפשר זיהוי ומניעה מוקדמים של מתקפות באופן רחב, וממשם את היכולת המצרפית של קהילת הסייבר בישראל.

השנה גדל מספר החברות השותפות במיזם ב־**63%**.

26
חברות MSSP במיזם

125
חוקי ניטור אסטרטגיים

126
דוחות חקירה

57
שיתופים יזומים

פורום MIRROR

פורום MIRROR הוא שיתוף פעולה בין מערך הסייבר הלאומי לחברות IR לטיפול באירועי סייבר.

בין היתר הצליח הפורום לבלום את הנזק הפוטנציאלי מהתקיפה על המרכז הרפואי שמיר ביום כיפור השנה, ולהבטיח את רציפות הטיפול הרפואי.

30
אירועי סייבר טופלו על ידי החברות בפורום

45
חברות IR שמשתתפות בפורום

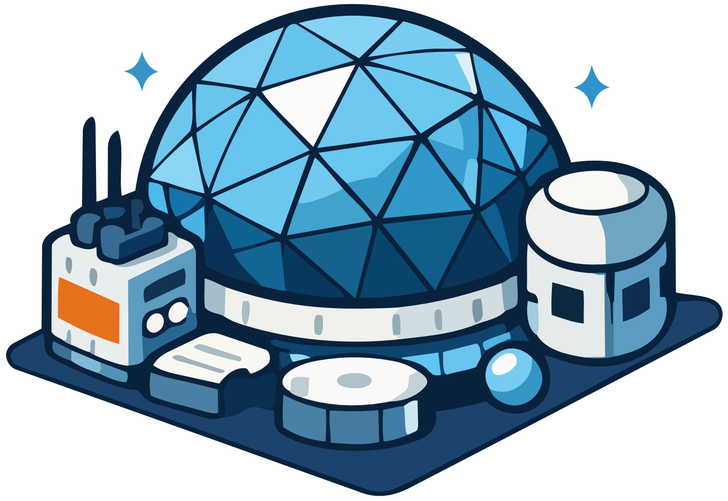
15
אירועי סייבר דווחו לראשונה באמצעות חברות בפורום

90
מומחים בקהילה

מיזמים טכנולוגיים לאומיים להעלאת החוסן

פרויקטים רב שנתיים בתשתית סייבר

מערך הסייבר הלאומי מפעיל מגוון מערכות ושירותים רב שנתיים שמטרתם צמצום יכולת התקיפה של ארגונים ותשתיות חיוניות בישראל. מערכות אלו מופעלות בשיתוף פעולה עם חברות טכנולוגיה במטרה לזהות ולבלום את התקיפות.



CYBERSHIELD

פרויקט ניטור לאומי. שיתוף פעולה אסטרטגי בין מערך הסייבר הלאומי וחברת Google כחלק מכיפת הסייבר הלאומית. המערכת הייחודית שפותחה, מייצרת תמונת מצב וניטור לאומיים המאפשרים זיהוי ותגובה אוטומטיים לאירועי סייבר בשילוב יכולות בינה מלאכותית (AI).

חיבור **25** גופים חדשים למערכת ושכלול יכולות הזיהוי הביאו השנה לעלייה של פי **7** במספר הנסיונות למתקפות שזוהו ונמנעו בהשוואה לשנה שעברה.

אירועים שזוהו ונבלמו באמצעות המערכת:

3
אירועי סייבר בעלי פוטנציאל אפידמי

126
אירועי סייבר משמעותיים

648
ניסיונות למתקפות

PDNS

מערכת PDNS (Protective DNS) לגלישה בטוחה הוא שירות המופעל במטרה לייצר "שומר סף" באינטרנט באמצעות חסימת גישה לדומיינים זדוניים, תוך שימוש בכלי AI ואנליטיקות שמדייקים את הזיהוי שלהם. מטרת השירות היא להקטין משמעותית את יכולת התקיפה של ארגונים ותשתיות קריטיות בישראל.

פורטל מערך סייבר לאומי להגברת החוסן

פורטל הסייבר הלאומי מסייע להגברת החוסן הלאומי בסייבר על ידי הנגשת כלים ושירותים לארגונים במשק הישראלי במטרה לצמצם את משטח התקיפה ולהגן מפני מתקפות סייבר.

קידום חוק הגנת הסייבר הלאומי

חוק הגנת הסייבר הלאומי נועד לתת מענה לאיומי הסייבר המתגברים, שהנזק השנתי שלהם לכלכלה מוערך בכ-**12 מיליארד** שקלים; לצמצם פערים רגולטוריים וליצור מסגרת חוקית אחידה וסטנדרטים מחייבים, בדומה למדינות מערביות אחרות; להגן על הרציפות התפקודית ולהבטיח את חוסנם של ארגונים חיוניים שבלעדיהם המדינה והמשק אינם יכולים לתפקד בשגרה ובחירום.

קידום חוק הגנת הסייבר הלאומי

נוסח החקיקה הוא תוצר של עשרות שיחות ותיאומים עם גורמים במשק ובממשל שנערכו במהלך שנת 2025.
מאמצים אלו הובילו לפרסום תזכיר החוק להערות הציבור בתחילת 2026.

החוק מייצר סטנדרט הגנה אחיד ורשת ביטחון לניהול סיכוני סייבר.

עיקרי החוק:

כפי שמובאים בתזכיר להערות הציבור שפורסם בתחילת 2026

החלת סטנדרטים
הגדרת רמת הגנה בסיסית מחייבת וניהול סיכונים לארגונים חיוניים וספקי שירותים דיגיטליים.

פיקוח ואכיפה
יצירת מסגרת לאומית לפיקוח על עמידה ביעדי האבטחה והבטחת החוסן של המשק הישראלי.

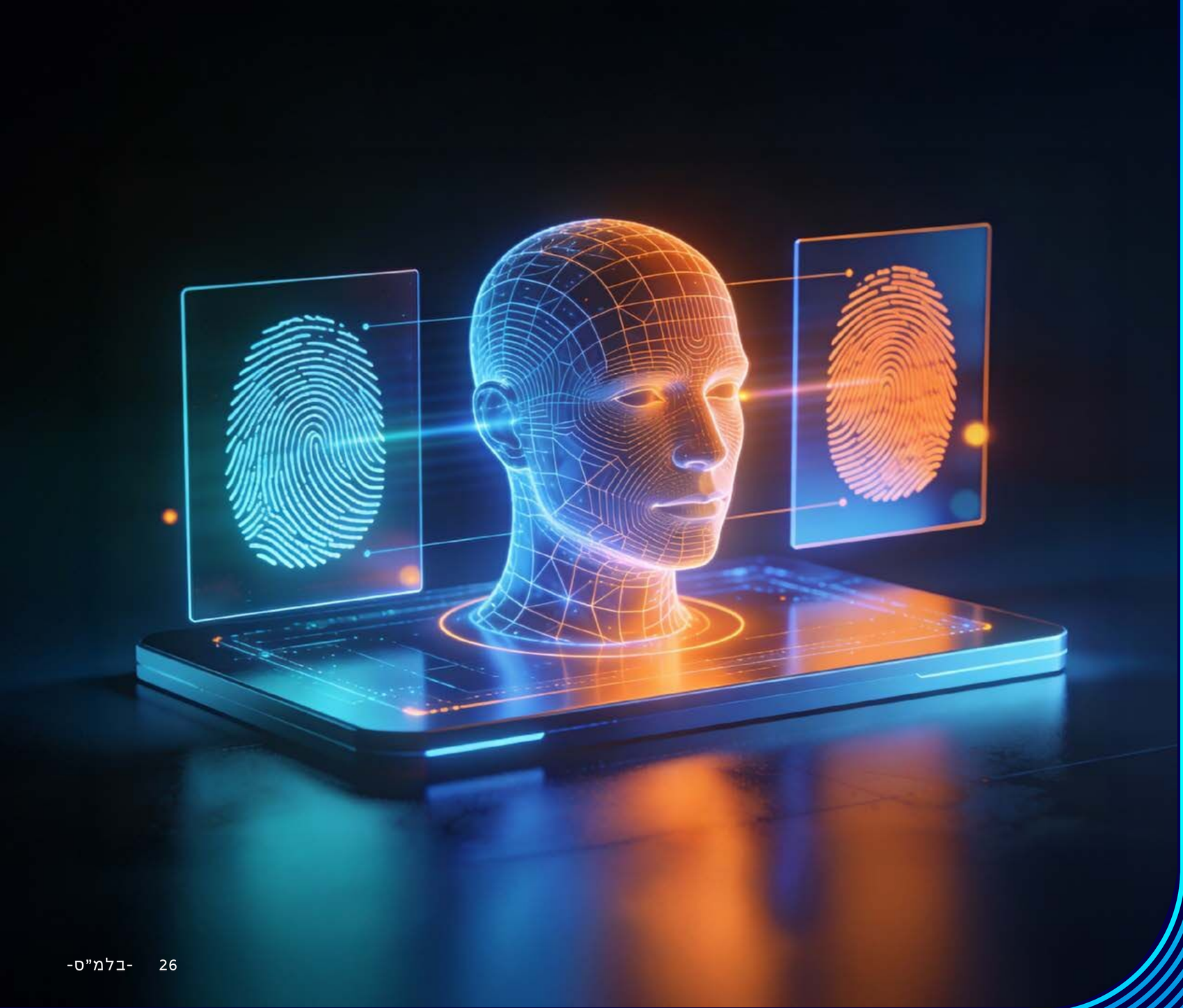
חובת דיווח
הטלת חובה על ארגונים לדווח באופן מיידי לרגולטור ומערך הסייבר הלאומי על אירועי תקיפה משמעותיים.

הסדרת סמכויות
הגדרה ברורה של תחומי האחריות של מערך הסייבר הלאומי מול משרדי הממשלה.

הזדהות בטוחה וביומטריה

פעילות תחום ההזדהות והיישומים הביומטריים בשנת 2025:

- מימוש סמכויות הפיקוח של הממונה על היישומים הביומטריים
- חיזוק החוסן של המשק בתחומי הביומטריה וההזדהות הדיגיטלית
- גיבוש ועדכון מתודולוגיה להזדהות דיגיטלית
- קידום מחקר יישומי וחדשנות בתחום הביומטריה



הזדהות בטוחה וביומטריה

פעולות מרכזיות:

פרסום **3 דו"חות פיקוח**:
1. פרויקט התיעוד הלאומי החכם
2. דו"ח מיוחד בנושא זיהוי חללים
3. פרויקט לחיזוק מערך ביקורת הגבולות לזרים (איסוף ושמירה של מידע ביומטרי)

פרסום **עבודת מטה לאומית**
ליישומים ביומטריים

דו"ח ייעודי על תפקידי המאגר הביומטרי ומאגרים ביומטריים בממשלה

ביצוע **מבדק חוסן** לאפליקציית הזיהוי מרחוק של רשות האוכלוסין

קבלת **3 סמכויות חדשות**
לניהול מידע ביומטרי בגופים ממשלתיים

עדכון **המתודולוגיה הלאומית**
להזדהות דיגיטלית בטוחה

ליווי והכוונה מקצועית
ל-**4 משרדי ממשלה**
בתחום ההזדהות הדיגיטלית

ליווי והכוונה ליישומים ביומטריים
ב-**6 גופים ציבוריים**

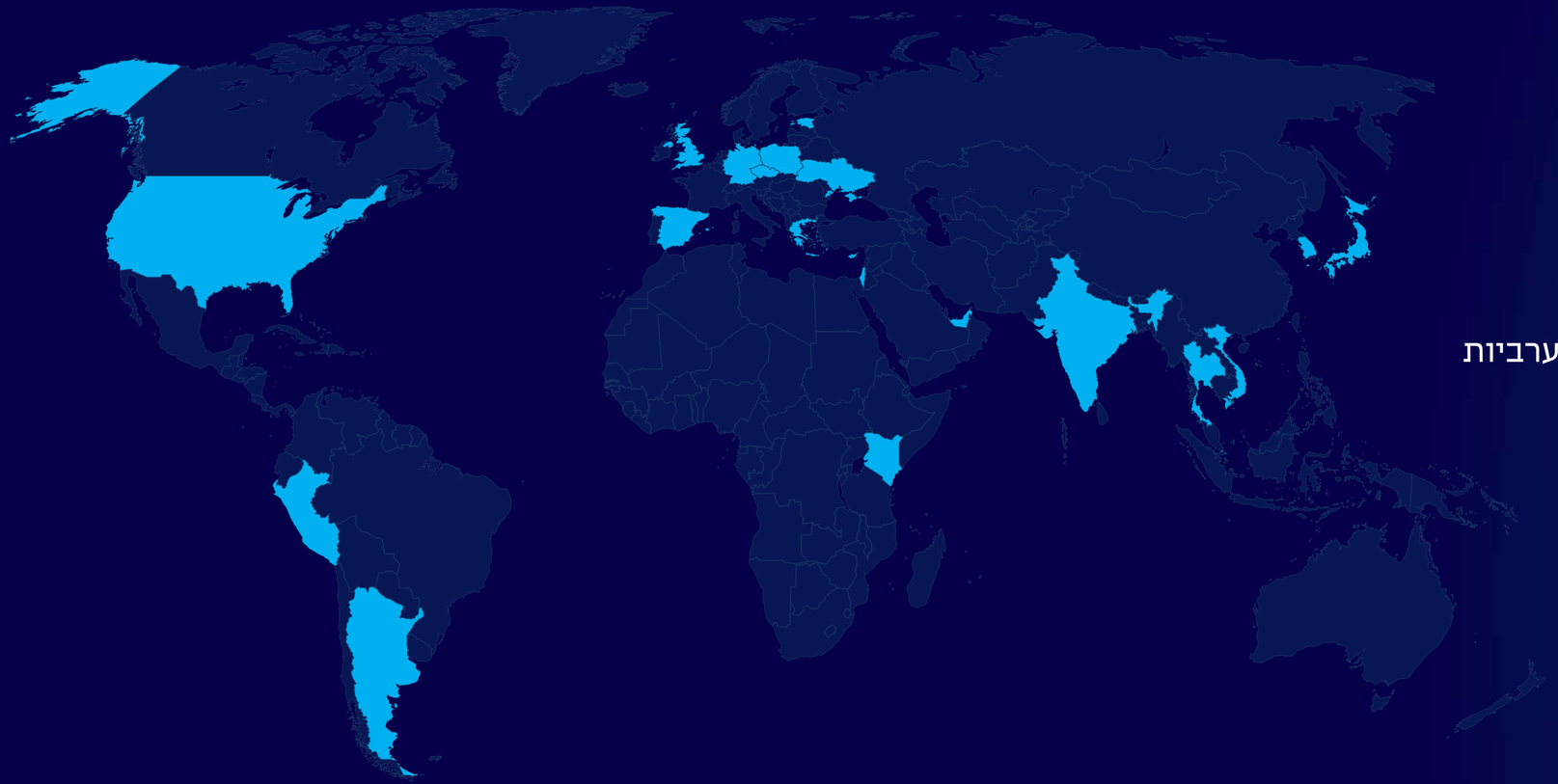
מימון **8 מחקרים**
בתחום הביומטריה והסייבר

שיתופי פעולה בין־לאומיים בתחום הסייבר

שיתוף פעולה בין-לאומי הוא בליבת אסטרטגיית הגנת הסייבר של ישראל מתוך תפיסה כי איומי הסייבר הם חוצי מדינות וגבולות.

שיתופי פעולה בין־לאומיים

הרחבת שיתופי הפעולה של המערך עם גופי הגנת סייבר בעולם בשנת 2025



- ארצות הברית
- בריטניה
- גרמניה
- יוון
- קפריסין
- צ'כיה
- ספרד
- אסטוניה
- פולין
- אוקראינה
- קנדה
- סינגפור
- קוריאה
- יפן
- תאילנד
- ויאטנם
- הודו
- איחוד האמירויות הערביות
- ארגנטינה
- פרו
- פיג'י
- קניה

מעל **20** משלחות זרות התארחו במערך בשנת 2025

הגברת שיתופי הפעולה האופרטיביים עם גופי הגנת סייבר, מודיעין ואכיפה זרים שסיפקו מודיעין איומים בזמן אמת במהלך מבצע "עם כלביא"

שיתופי פעולה בין־לאומיים

שיתופי פעולה אסטרטגיים עם ארצות הברית וגרמניה

ארצות הברית

יחסי ישראל וארצות הברית בתחום הגנת הסייבר מתבססים על שותפות אסטרטגית עמוקה, רבת שנים, המשלבת זרועות רבות בממשל, גופי ביטחון, סוכנויות, גופי מטה וחברות מסחריות משתי המדינות.

ממשל טראמפ החדש חיזק את המחויבות לשיתוף הפעולה האסטרטגי והאופרטיבי, שכלל השנה מאמצים מתואמים בהתמודדות עם פשיעת סייבר, הגנה על תשתיות קריטיות, שיפור מתמיד של הגנת סייבר והתמודדות מול אתגרים טכנולוגיים מתקדמים כגון: בינה מלאכותית, טיפול בחולשות, מעבר לתשתיות ענן מאובטחות והגנה על שרשראות אספקה.

גרמניה

השנה השר הגרמני לביטחון פנים חתם על ברית הגנה בין ישראל וגרמניה הכוללת נדבך משמעותי שמתייחס לתחום הסייבר ונחתם הסכם כוונות של המערך עם מנהלת הסייבר במשרד לבטחון פנים של גרמניה (BMI).

שיתוף הפעולה בין המדינות כולל 4 מרכיבים מרכזיים:

1. פיתוח כיפת סייבר הדור הבא
2. הקמת מרכז מצויינות משותף למחקרי סייבר לאומיים
3. הרמוניזציה בתחומי חקיקה ואסדרה בסייבר
4. הצבת נספח סייבר של המערך בגרמניה.

שיתופי פעולה בין־לאומיים

בונים קואליציות: מערך הסייבר השתתף במגוון פעילויות בינלאומיות

תרגילים ואימונים נבחרים

- תרגיל APEX הבינלאומי בדרום קוריאה
- תרגיל בילטלי בהגנת סייבר למגזר הימי עם קפריסין
- תרגיל תרחישי סייבר במגזר הפיננסי ביפן
- האקתון CyberSpirit בסינגפור
- אימון הגנת סייבר ל-OT ורשתות תעשיתיות במעבדת INL בארה"ב
- תרגיל Cyberfire לניהול אירועי סייבר בארה"ב
- תרגיל טרילטראלי בהיערכות סייבר בחירום עם יוון וקפריסין
- סדנאות משותפות במודיעין איומים עם גרמניה
- קבינט הסייבר הגלובלי (**GCC**) בהובלת ראש המערך התקיים וירטואלית והשתתפו בו בכירים מ-15 מדינות בעולם.

אירועים וכנסים מרכזיים

CYBERTECH GLOBAL TEL AVIV 2025

CYBERTECHNYC 2025 · CYBERTECH LATIN AMERICA · CYBERTECH SOUTH AMERICA

Cyber Week Dec. 8th-11th, 2025 Tel Aviv University, Israel

SICW Singapore International Cyber Week

CSK 2025 Cyber Summit Korea

CRI International Counter Ransomware Initiative

msc Munich Security Conference

World Economic Forum

RSAC 2025 Conference

CYBERUK

Osaka, Kansai, Japan EXPO2025

NATO OTAN

Eco-System מחקר וחדשנות בסייבר

Eco-System

מחקר וחדשנות בסייבר

בשנים האחרונות התחזקה פעילות המחקר שמייצר האקו־סיסטם בתחום הסייבר בבאר שבע. בין המיזמים של מערך הסייבר: המעבדה הלאומית לסייבר, בקרה תעשייתית, תשתיות קריטיות ואנרגיה (ICNL), שפועלת מזה כשנתיים בשיתוף פעולה עם משרד האנרגיה.

בשנת 2025 הובילה המעבדה שורה של מבדקים טכנולוגיים עם חברות הזנק וחברות בין־לאומיות בתחום סייבר ICS/OT, לצד מחקרים משותפים עם האקדמיה ועם מפא"ת. במקביל, קיימה המעבדה פעילות רחבה של חינוך, הדרכה ותרגול לגורמי ממשלה, ארגונים במשק והאקדמיה, באמצעות ימי עיון, קורסים, ווביינרים, ביקורים סקירות ומידעונים.

1,150 משתתפים בכנסים וימי עיון

870 משתתפים בהדרכות

18 ניסויים וסימולציות

4 מחקרים

תעשיית הסייבר הישראלית

בשנתיים האחרונות, למרות המלחמה ואי-יציבות גלובלית, תעשיית הסייבר הישראלית היוותה עוגן מרכזי בכלכלת ישראל והפגינה חסינות עם עלייה בהיקפי ההשקעות.

היקף ההשקעות הפרטיות בחברות ישראליות: **4.1 מיליארד $**

1 מכל 3 דולרים מכלל ההשקעות הגלובליות בסייבר הושקע בחברת סייבר ישראלית.

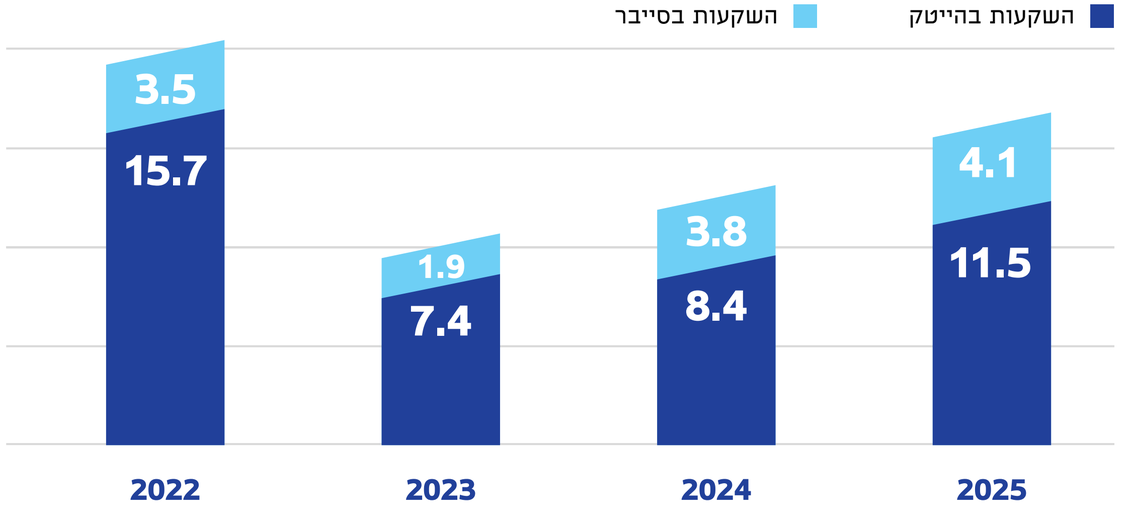
תעשיית הסייבר הישראלית

השקעות הון בהייטק ובתעשיית הסייבר הישראלית לשנת 2025 [1]:

תעשיית הסייבר משמשת עוגן של יציבות וצמיחה גם בתקופות של חוסר ודאות. הסייבר אחראי על כמעט שליש מהשקעות ההון בסטרטאפים ישראלים וכ-**80%** משווי האקזיטים ב-2025.

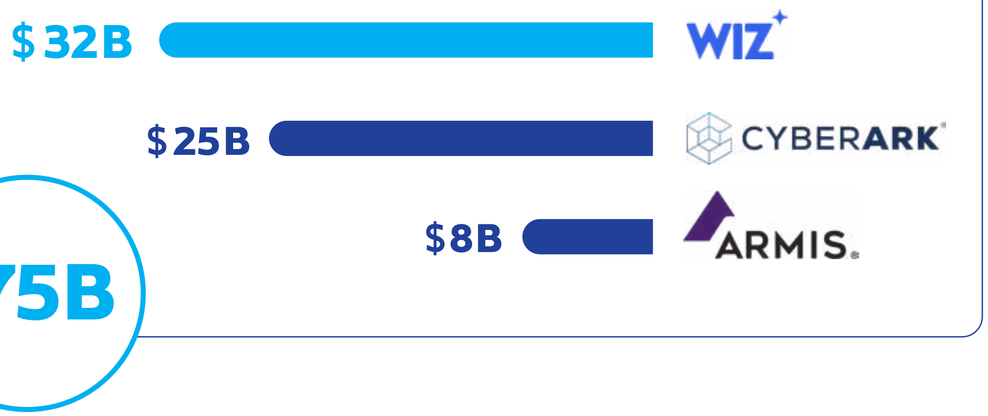
מעבר להזרמת הון זר לקופת המדינה, התעשייה מבצרת את מעמדה האסטרטגי של ישראל בעולם, משמרת את הכישרונות הטכנולוגיים במדינה ומבטיחה את חוסנו של המשק הישראלי בטווח הארוך.

השקעות הון בהייטק ובסייבר בישראל 2025



[1] לפי הדו"ח השנתי לשנת 2025 על האקוסיסטם הישראלי בהייטק של Startup Nation Central

3 האקזיטים הגדולים ב-2025:



טיפול במתקפות פישינג

מערך הסייבר הלאומי מקבל ובודק אלפי דיווחים על מתקפות פישינג (דיוג) שמגיעים ממקורות שונים. קישורים שמתגלים כמזיקים מטופלים כדי לצמצם את הנזק למשק.

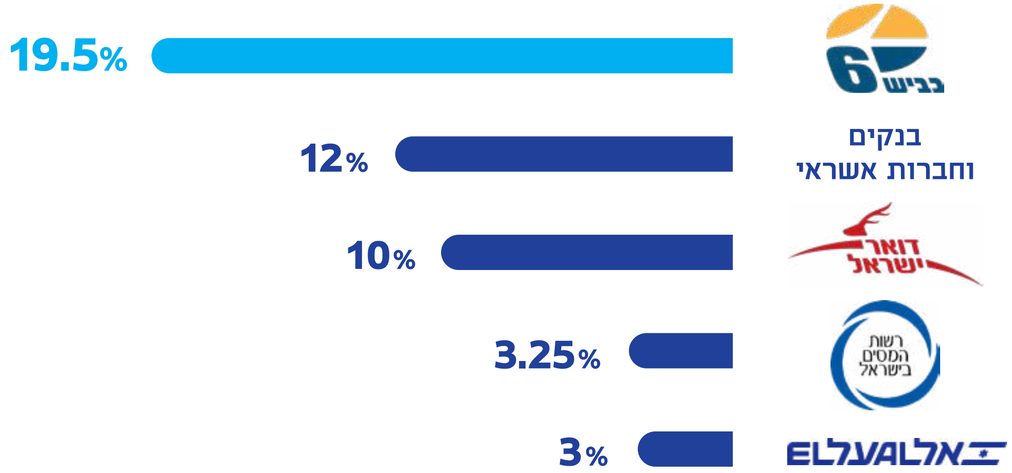
המערך עובד בשיתוף עם ספקיות הפצת המסרונים כדי לצמצם את ההפצה ולעצור אותה מיד כשהיא מתגלה.

השנה קיבל המערך **35,537** דיווחים ממקורות שונים על מתקפות פישינג ובלם **31,657** קישורים מזיקים - עלייה של פי **6** לעומת 2024.

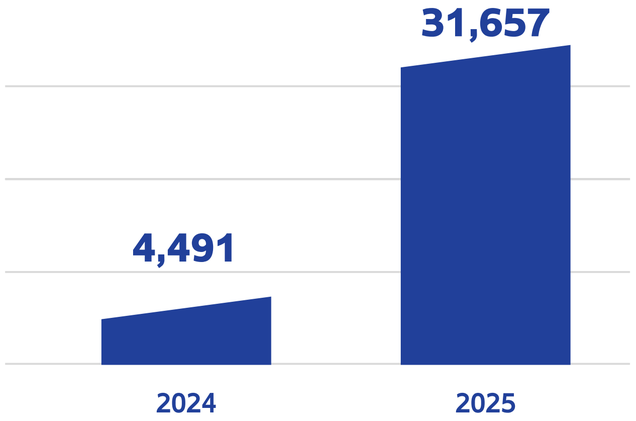
טיפול במתקפות פישינג

כלי ה-AI מקלים על תוקפי הסייבר לייצר הודעות פישינג ברמת אמינות גבוהה מאוד של עיצוב וכתיבה. ההודעות נראות אמינות ולעיתים קרובות קשה לזהותן. בנוסף, השנה נראתה עלייה נוספת במתקפות דיוג ממוקדות (ספיר פישינג) על בכירים במגזרי התקשורת, האקדמיה, הביטחון והממשל.

5 הגופים אליהם התחזו הכי הרבה בהודעות בשנת 2025:



מתקפות פישינג שטופלו ונבלמו:



הדהוד מתקפות ברשת הגלויה

האקרים משתמשים כיום ברשת הגלויה כזירה ללוחמה פסיכולוגית במטרה לנסות לפגוע בחוסן הלאומי באמצעות הדהוד מתקפות, פרסום מידע אישי על אישי ציבור והפצת מידע מוטעה.

הדהוד מתקפות ברשת הגלויה

מערך הסייבר הלאומי פועל כשכבת הגנה לאומית במרחב הדיגיטלי ולצורך כך עוקב אחר מגמות, שיח ודפוסי פעילות גלויים ברשת. המידע משמש לניתוח והערכת איומים, להבנת שיטות פעולה ויכולות של תוקפים ולהפקת תובנות הגנתיות.

באמצעות ניתוח זה, המערך מספק התרעות והכוונה מקצועית לארגונים בזמן אמת, במטרה לצמצם סיכונים, לחזק מוכנות, ולאפשר התמודדות מוקדמת ואף להזהיר את הציבור מפני מגמה מסוימת ומניסיונות השפעה.

765

קבצי דלף מידע הקשורים לישראל פורסמו ברשת ובדארקנט

גידול של **53%** משנת 2024

726

פרסומי תוקפים ברשתות החברתיות המתהדרים בתקיפות בישראל

ירידה של **19%** משנת 2024

הגברת מודעות וחוסן דיגיטלי בקרב הציבור

מערך הסייבר מפרסם חומרי הסברה וקמפיינים במטרה להעלות את המודעות הציבורית לאיומי הסייבר על אזרחים, עם כלים להתמודדות - במיוחד במצבי מלחמה וחירום.

במבצע "עם כלביא" ביוני 2025 נצפתה עלייה חדה במתקפות המיועדות להשפיע על המורל הציבורי, נסיונות להטעות ולגרום לפאניקה. המערך הגיב באופן מיידי עם אזהרות בזמן אמת, חומרי הסברה, כתבות וקמפיין רב ערוצי.

הגברת מודעות וחוסן דיגיטלי בקרב הציבור

קמפיינים ונתונים

8
קמפיינים

כ-200M
חשיפות

51
התרעות לציבור

קמפיין "אל תהיו שתפנים!"
במטרה להעלות מודעות למניעה של
הפצת טרור פסיכולוגי ברשתות

"אל תתנו להם לשחק לנו בראש"
קמפיין העלאת מודעות למתקפות פישינג
והשפעה במבצע "עם כלביא"

שבוע הגנת הסייבר
קמפיין הגנה ברשת לבני נוער

קמפיין הזדהות דיגיטלית
העלאת המודעות לחשיבות של
שמירה על הזהות הדיגיטלית

קמפיין כופרה
העלאת מודעות בקרב עסקים קטנים
למתקפות כופרה

119 מתקשר אליך
במטרה לעודד ארגונים לענות
לשיחות של 119

קמפיין דיווח לצ'ט בוט
הגברת הפניות ל-119 באמצעות
צ'אט בוט ייעודי בוואטסאפ

לחשוב כמו האקר
פודקאסט סיפורי סייבר והמלצות
הגנה לארגונים קטנים ולציבור

הגברת מודעות וחוסן דיגיטלי בקרב הציבור

תכנית "שגרירי סייבר"

השנה השיק המערך את תוכנית 'שגרירי סייבר', המכשירה בני ובנות נוער בגילי 12 עד 15 שסומנו כמובילים חברתיים להפוך למשפיעני סייבר ולהעביר את הידע בנושא לחבריהם ולמשפחתם. במסגרת התוכנית, עוברים המשתתפים הכשרה מקצועית במרכז המערך בבאר שבע ויום הכשרה נוסף באחת מחברות הייטק השותפות לפרויקט - צ'ק פוינט, מיקרוסופט או פאלו-אלטו.

מעבר לידע הטכני, התכנית מעניקה להם כלים להעברת מסרים והסברה אפקטיביים, וכן מציידת אותם במצגת להעברת הנושא בכיתות המקבילות במטרה לסייע בקהילות שלהם ולחזק את החוסן הלאומי.

CHECK POINT · Microsoft · paloalto NETWORKS

ברנקו וייס חינוך משנה חברה · בית הספר האקולוגי - יבנה ע"ש יצחק שמיר

התחלה:
אוקטובר 25

150
תלמידים סה"כ

6
בתי ספר

ציון ממוצע:
3.9 מתוך 5

מבט קדימה

מבט קדימה

חזית הסייבר תמשיך להוות זירה משמעותית בשנים הקרובות וההתפתחות המואצת משנה את העולם ומביאה אותנו לתלות מוחלטת ביכולות הדיגיטליות בכל תחום בחיינו, להעברת קבלת החלטות מהאדם לבינה המלאכותית ולהאצת יכולות עם הפריצה הצפויה של המחשוב הקוואנטי ממחקרי לתעשייתי. כל אלו יעמידו את החברה הגלובלית באתגר משמעותי ולשאלה - כיצד אנו נהנים מהיכולות המדהימות הללו בצורה בטוחה ומטמיעים אותן בצורה שלא תפגע באנושות ולא תערער את היסודות של חיינו?

ההגנה בסייבר היא המאפשר ולא החסם בדרך לאימוץ הטכנולוגיות המתקדמות לתכלית שיפור החיים של אזרחי מדינת ישראל. עלינו לנהל סיכונים בצורה מושכלת באמצעות הבנה עמוקה של האיומים, העלאת החוסן בכדי לצמצם את הסיכון, היערכות להתמודדות עם האירועים אשר בוא יבואו ("קו המגע לעולם ייפרץ") ותכנון ההתאוששות שלאחר האירוע מבעוד מועד.

מערך הסייבר הלאומי מוביל תוכנית לאומית שתכליתה הגנה חזקה על רציפות התפקוד והתשתיות הקריטיות, שיפור הגנת הסייבר הלאומית ושימור ישראל כמעצמת סייבר עולמית.

הדרך להשגת המטרות היא עבודה בשיתוף פעולה עם השותפים בארץ ובעולם, חיבור אמיתי לתעשייה ולשוק הפרטי, חתירה למצוינות ללא פשרות, מיסוד ההגנה בסייבר באמצעות חוק הגנת הסייבר הלאומי, תורת הגנה חדשה ועדכנית, קידום ופיתוח יכולות קצה והטמעתן בהגנת המדינה.

עיצוב והוצאה לפועל של התוכנית הרב שנתית להגנה הלאומית בסייבר הם העוגן שיאפשר לנו להביא את מדינת ישראל להיות ערוכה לאתגרי הסייבר בראי 2030.

מעל לכל תוכנית ישנה ההבנה העמוקה כי כוחה של מדינת ישראל בכלל ובסייבר בפרט טמון באנשיה. יש לנו את האנשים הטובים בעולם וההשקעה בהם היא הדבר הנכון והחכם ביותר שאנו צריכים לעסוק בו.

נמשיך לשקוד על משימת ההגנה בסייבר, לטפח את ההון האנושי ולהוביל את ההגנה תוך מיסוד ישראל כמעצמת סייבר עולמית.

מזמין אתכם להיות שותפים למאמץ ההגנה הלאומית בסייבר!

יוסי כראדי
ראש מערך הסייבר הלאומי

כתיבה ועריכה:
אגף דוברות
פרסום והסברה

מערך הסייבר הלאומי

119
119@cyber.gov.il
www.cyber.gov.il