סיכום שנה 2024

בסימן מלחמת "חרבות ברזל"

מערך הסייבר הלאומי

גבי פורטנוי
דבר ראש מערך הסייבר הלאומי לשנת 2025

מלחמת 'חרבות ברזל' לא הייתה רק עימות צבאי קונבנציונלי - היא התנהלה גם במרחב הקיברנטי. אויבינו, בהובלת איראן, ניסו לפגוע ברציפות התפקודית של תשתיות חיוניות, לשבש את חופש הפעולה של צה"ל ואף לערער את המורל הציבורי ולהשפיע על דעת הקהל בעולם.

שנת 2024 הציבה בפנינו אתגרים חסרי תקדים. למדנו, התייעלנו והשתפרנו, תוך הפקת לקחים שהוטמעו בתוכניות העבודה שלנו לשנים הבאות.

<u>תובנות מרכזיות משנת 2024:</u>

- **מתקפות סייבר - חלק בלתי נפרד מהמלחמה המודרנית:** המערך פעל כזרוע לחימה לכל דבר, עם הכלים המתקדמים ביותר תוך שיתוף פעולה הדוק עם קהילת הביטחון, הממשלה והמגזר הפרטי.
- **הטכנולוגיה בשירות ההגנה:** עשינו קפיצת מדרגה משמעותית בהקמה של תשתיות טכנולוגיות שיעניקו הגנה רחבה ברמה הלאומית.
- **כוחנו באחדותנו:** שיתוף הפעולה בין כלל הגורמים הוא המפתח להצלחה. רק באמצעות פעולה משותפת - מקומית, אזורית ובין לאומית, נוכל לבנות חומת מגן אפקטיבית מול האיומים.
- **הון אנושי - הנכס החשוב ביותר:** מסירות, נחישות ויצירתיות שמאפיינים את 'הרוח הישראלית' הם שהובילו אותנו להישגים.
- **הגנה על התודעה הציבורית:** האויבים ניסו לנצל מתקפות דיוג, חדירה לרשתות חברתיות והפצת מידע שקרי כדי לערער את החוסן החברתי. בתגובה, המערך החל ביצירת "מרחב מוגן תודעתי" - מערך להגנה מפני מידע כוזב, סיוע בזיהויו והסרתו מהרשת
- **הציבור - קו ההגנה הראשון:** המלחמה הוכיחה כי הציבור אינו רק קהל יעד, אלא חלק בלתי נפרד ממערך ההגנה הלאומי. מתקפות סייבר עלולות לפגוע לא רק בארגונים קריטיים אלא גם באזרחים - וזו תובנה שתעמוד בבסיס האסטרטגיה הלאומית שלנו להמשך.

<u>אתגרים מרכזיים לשנת 2025:</u>

- חיזוק החוסן הלאומי בסייבר: היערכות לאיומים חדשים ומתפתחים.
- מימוש חזון 'כיפת הסייבר': הטמעת תשתיות לאומיות להגנה על הארגונים החיוניים.
- הסתגלות למציאות משתנה: השינויים במרחב הדיגיטלי מהירים ודורשים מאיתנו גמישות ודינמיות. עלינו להקדים תרופה למכה, לזהות את מוקדי העניין של התוקפים ולספק מענה מהיר ויעיל.

אני מלא גאווה בעובדי המערך, בקהילת הביטחון, במגזר הממשלתי והפרטי, ובטוח ביכולתינו להמשיך ולהוביל את ישראל להישגים נוספים בתחום הסייבר. המרוץ אינו נגמר - כל אתגר מחזק אותנו וכל הישג מראה לנו שאפשר להגיע רחוק יותר.

עיקרי פעילות התוקפים במרחב הסייבר

המגמות שזוהו בשנתיים האחרונות הלכו והתעצמו השנה ביתר שאת.

השנה נצפתה מגמה גוברת מצד איראן, חזבאללה ותוקפים נוספים לקידום פעילות סייבר תומכת לחימה, בין השאר זוהה מיקוד באיסוף מידע על יעדי איש ואזרחים ותהליכים בישראל.

עיקרי פעילות התוקפים במרחב הסייבר

ניצול חולשות 1-Day

קיצור משמעותי של זמן ניצול החולשה
מפרסומה ועד מימושה

שימוש בדלף פרטי התחברות

שימוש גובר של תוקפים בדלף פרטי התחברות
מאתרים ומארגונים וסחר בהם בדארקנט

תקיפות דיוג

התרחבות השימוש בפישינג כדרך לפרוץ לארגונים
ועליית מדרגה בכמות ובאיכות ההודעות שנראות
פעמים רבות לגיטימיות

שירותים דיגיטליים

שרשראות אספקה טכנולוגיות המשמשות
דרך לפרוץ לארגונים רבים במקביל

ניצול של ממשקים/בקרים פתוחים במרחב

מיקוד תוקפים בחיפוש מצלמות אבטחה פרטיות וציבוריות
בתקופת המלחמה

מתקפות DDoS בנפחים חריגים וגדולים במיוחד

מול אתרים רבים בישראל ומיקוד מיוחד במגזר הפיננסי

איסוף מידע ומיקוד ביעדי איש

מעבר ממתווים שמכוונים לגרימת נזק למתווים
שמתמקדים באיסוף מידע על ישראלים ויעדי איש

דיווחים שהתקבלו במרכז המבצעי 119

מרכז 119 של המערך מקבל אלפי דיווחים בשנה אודות מתקפות סייבר, חשדות וניסיונות. הדיווחים מגיעים מאזרחים או מארגונים, נבחנים ומקבלים את המענה המותאם - מסיוע ראשוני ועד להכוונה מקרוב באירוע סייבר משמעותי. אל המרכז ניתן להגיע בחיוג ישיר או באופן מקוון בכל שעה.

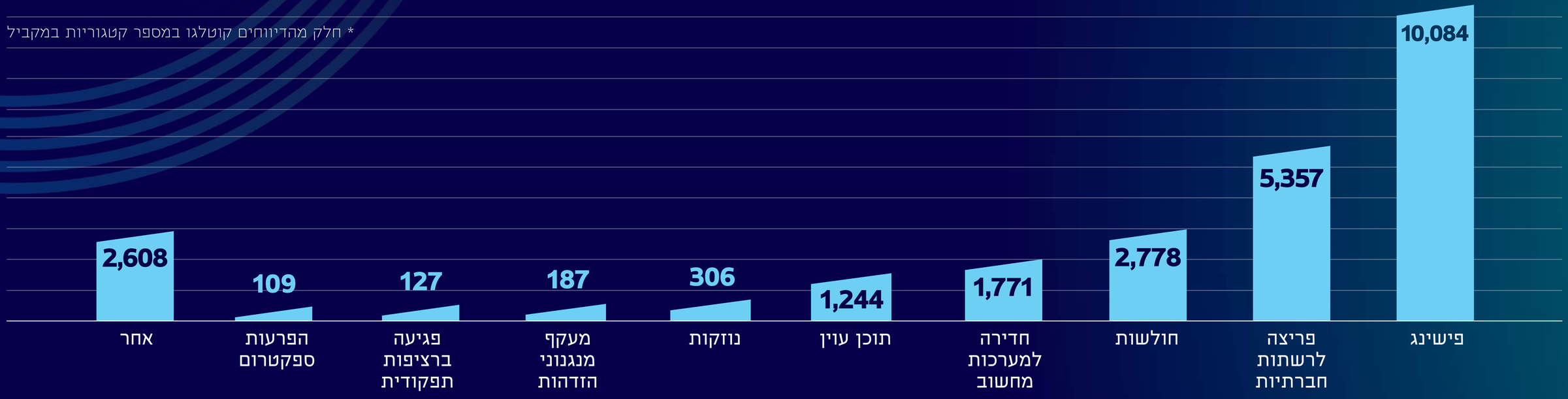
דיווחים שהתקבלו במרכז המבצעי 119

בשנת 2024 התקבלו **17,078** דיווחים מאזרחים ומארגונים שאומתו כאירועי סייבר. השנה התווספה קטגוריה חדשה לדיווחים:
תוכן עוין - הודעות ושיחות מפחידות, חדשות כזב ולוחמה פסיכולוגית ברשת וסרטוני "דיפ פייק". נושא שהתעצם בזמן המלחמה.

17,078
דיווחים בשנת **2024**

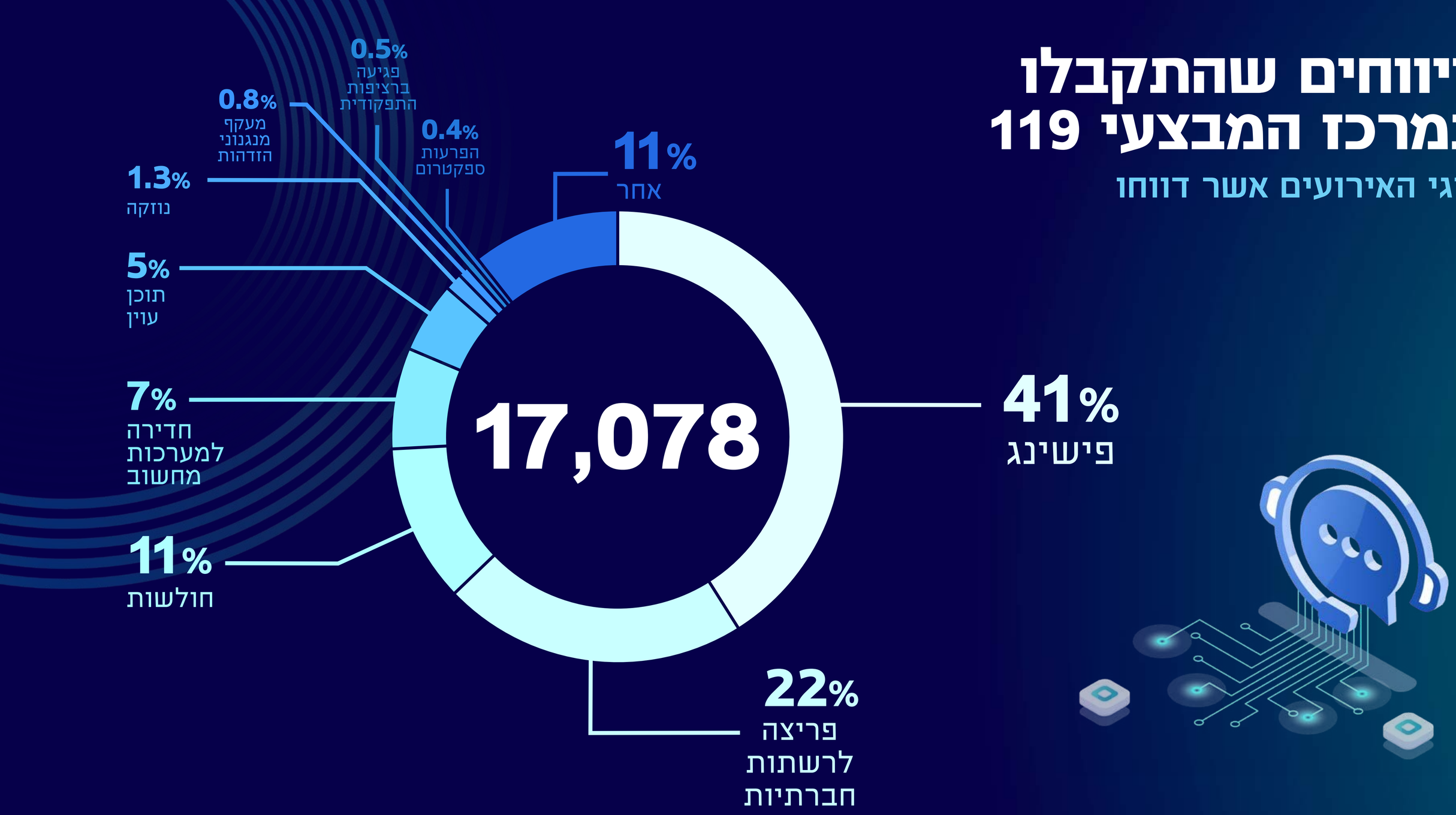
עלייה של **24%** במספר הדיווחים בהשוואה לשנת **2023**

פישינג
המתקפה הכי נפוצה שדווחה השנה.



דיווחים שהתקבלו במרכז המבצעי 119

סוגי האירועים אשר דווחו



דיווחים שהתקבלו במרכז המבצעי 119

חלוקת הדיווחים על פי סוגי מגזרים

טיפול במתקפות פישינג

הדיווחים המתקבלים ממגוון מקורות במערך הסייבר הלאומי אודות מתקפות דיוג (פישינג) פעילות נבחנים, וקישור שנמצא מזיק מועבר לטיפול הגורמים המתאימים, במטרה לצמצם את הנזק.

בנוסף, המערך פועל יחד עם הגורמים הרלוונטיים מול ספקיות הפצת המסרונים כדי לצמצם את היקף הפצת מסרוני הדיוג.

השנה טיפל המערך ב-**4,491** מתקפות דיוג שהופצו לציבור הרחב או לארגונים ונמצאו מזיקות - עלייה של כ-**80%** בהשוואה לשנה הקודמת שבה החלה הפעילות.

טיפול במתקפות פישינג

תשתיות דיוג שטופלו במערך

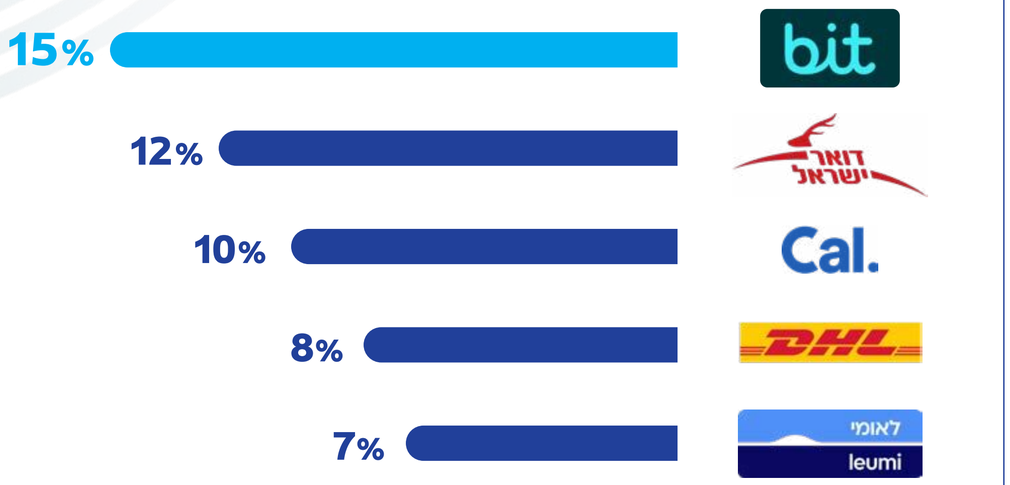
בחינת המגמות של הודעות הפישינג השנה מעלה כי נוסח הודעות הדיוג בשנה האחרונה הופיע לעיתים קרובות באופן שהקשה על זיהויין כזדוניות על ידי המשתמש.
ההודעות עשו שימוש בכלי בינה מלאכותית יוצרת ופעמים רבות הותאמו באופן ממוקד יותר לקהל היעד בצורה שנראית משכנעת.

4,491
תשתיות דיוג טופלו

זמן ממוצע להורדת תשתית:
5 שעות

80% מהבקשות להסרת תשתיות טופלו תוך
24 שעות

5 הגופים המרכזיים שהתחזו אליהם בהודעות



* אחוז מתוך סך הודעות הדיוג שטופלו במערך

טיפול במתקפות פישינג

תרגיל פישינג במשרדי ממשלה להעלאת מודעות

במהלך חודש אוקטובר 2024 יזמו מערך הסייבר הלאומי ורשות החירום הלאומית (רח"ל) שני תרגילי פישינג למשרדי הממשלה, במטרה להעלות את המודעות לסכנות הטמונות בלחיצה על קישורים חשודים.

כ-**20%** מהעובדים שקיבלו את ההודעה לחצו על הקישור - נתון שמשקף **שיפור משמעותי** בהשוואה לתרגילים קודמים, בהם שיעור ההקלקות עמד על כ-30%.

משתתפים ותוצאות:

20 **משרדי ממשלה** השתתפו בתרגילים

כ- **40,000** **עובדי מדינה** קיבלו את הודעות הפישינג כחלק מהתרגיל

כ- **20%** **מהעובדים** לחצו על הקישור

נסיונות השפעה על התודעה ברשת הגלויה

האקרים מנצלים את הרשת הגלויה ככלי ליצירת השפעה תודעתית על הציבור, באמצעות קריאות למתקפות, הדהוד מתקפות, פרסומים על גופים שכביכול נפגעו והפצת מידע אישי על ישראלים.

חלק מהתכנים המופצים מבוססים על עובדות, אך רבים מהם הם פרסומים כוזבים, המגיעים על רקע המלחמה ונועדו לזרוע בלבול וחוסר אמון.

נסיונות השפעה על התודעה ברשת הגלויה

מערך הסייבר הלאומי פועל באופן שוטף לגילוי, זיהוי וטיפול בתכנים אלה, כדי לצמצם את השפעתם ולחזק את החוסן הציבורי. כמו כן, המערך מתריע לארגונים על אינדיקציות למתקפות, כוונות ויכולות שעולות מפרסומים גלויים.

500

קבצי דלף מידע הקשורים לישראל פורסמו ברשת ובדארקנט

900

פרסומי תוקפים ברשתות החברתיות אודות תקיפות במשק הישראלי

התרעות למשק

במהלך שנת 2024 הוציא מערך הסייבר הלאומי **736** התרעות למשק - חלקן רחבות ורלוונטיות לכלל הארגונים, חלקן למגזר מסויים וחלקן לארגון ספציפי שבו התגלתה חולשה או אינדיקציה לתקיפה.

מדובר בהכפלה של מספר ההתרעות שהוציא המערך השנה בהשוואה ל-367 התרעות שיצאו בשנת 2023. ההכפלה מגיעה על רקע המלחמה והתעצמות האיומים.

התרעות למשק

בשנת 2024

150

התרעות פומביות

התרעות לבנות - מפורסמת באופן פומבי ומיועדת לכלל המשק.

26

התרעות לקבוצת עניין מוגדרת

התרעות צהובות - מפורסמת רק לקבוצות עניין מסוימות על פי מגזרים.

518

התרעות המיועדות לארגון ספציפי

התרעות אדומות - התרעות העולות ממגוון טכנולוגיות הניטור והזיהוי של המערך ומועברות לארגון ספציפי.

42

התרעות על פישינג ופייק ניוז לציבור הרחב

* הצבעים הם לפי פרוטוקול TLP: White / Amber

שימוש בחולשות נפוצות על ידי קבוצות תקיפה

מחקירת עשרות אירועי סייבר שנעשתה על ידי צוותי מערך הסייבר הלאומי בשנת 2024 עולים מספר נתיבי חדירה עיקריים לארגונים ששימשו את התוקפים לביצוע מתקפות סייבר.
לצד חולשות אבטחה חמורות שנוצלו השנה, נצפה שימוש גובר במיוחד גם בשיטות דיוג (פישינג) ושימוש בפרטי דלף של התחברות למערכות של ארגונים.
השנה נצפה קיצור משמעותי של זמני מימוש חולשות - מרגע שפורסמו ועד לרגע שמומשו לתקיפות חלפו שעות בודדות בלבד.
נתון זה מציב את האתגר של מגני סייבר להטמיע במערכותיהם את עדכוני האבטחה לחולשות קריטיות באופן מיידי.

שימוש בחולשות נפוצות על ידי קבוצות תקיפה

נתיבי חדירה עיקריים למערכות ארגונים שנצפו בישראל

חולשת Ivanti
ספקית VPN שבמוצריה התגלו חולשות חמורות.

הגדרה לקויה בשרתי Sharepoint
איפשרה לנצל מנגנון שהוגדר בצורה לקויה לטובת הרצת קוד מרחוק.

חולשות ישנות בשרתי דוא"ל (Exchange) כגון ProxyShell
שרשרת חולשות המאפשרות לתוקף להעלות קבצים זדוניים (Webshell).

חולשה בממשק ניהול PRTG
חולשה ברכיב PRTG לא מעודכן המאפשרת לתוקף "להזריק" פקודות לממשק הניהול של הרכיב ובכך לאפשר גישה לרשת הארגון.

שימוש בפרטי התחברות שדלפו
התחברות באמצעות שם משתמש וסיסמה שדלפו לרשת.

ממשק פתוח להעלאת קבצים
ממשק באתר web החשוף לעולם אשר מאפשר העלאת קבצים ללא ביצוע בדיקות קלט.

פישינג קלאסי
דוא"ל עם קובץ שמכיל תוכנה מזיקה או לחילופין קישור לעמוד בו יש להזין פרטים אישיים או פרטי התחברות למערכת.

Brute Force מוצלח
ניחוש סיסמאות אוטומטי בניסיונות רבים שעבד במקרים שבהם לא היו הגנות נוספות והסיסמה היתה קלה לניחוש.

הגנה אקטיבית

פעילות לצמצום חולשות במשק הישראלי

פעילות פרו-אקטיבית של המערך שמטרתה להיות צעד אחד לפני התוקפים ולזהות חולשות ומגמות במשק. המערך מפעיל את "התוכנית לגילוי אחראי של חולשות" שבה מוזמנים חוקרי וחוקרות אבטחה לדווח באופן דיסקרטי למערך על חולשות שמצאו במערכות של ארגונים. המערך מנהל את הממשק עם הארגון החשוף ומעניק למדווח הוקרה פומבית בהיכל תהילה.

הגנה אקטיבית

פעילות לצמצום חולשות במשק הישראלי

השנה חלה עלייה של כ-**22%** במספר דיווחי ה-VDP. השנה הדיווחים הפכו ממוקדים ואיכותיים יותר אודות חולשות משמעותיות.

ימים בממוצע לסגירת דיווחי VDP

כמות דיווחי CVE שנחתמו

מדווחים שהתווספו

מספר מדווחים בהיכל התהילה

כמות דיווחי VDP שהתקבלו

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

VDP תוכנית מיוחדת ל"גילוי חולשות אחראי" (VDP - vulnerability disclosure program) לקבלת דיווחים המסייעים באיתור ובזיהוי חולשות במשק הישראלי.

מיזמים טכנולוגיים לאומיים להעלאת חוסן

במסגרת מרכז הניטור והבקרה הלאומי (NSOC) מעניק מערך הסייבר הלאומי מענה לאיומי סייבר ייחודיים למגזרים שונים במשק, בהם הפיננסי, הממשלתי, בטחון פנים, האנרגיה, העורף, התקשורת והגנת הסביבה. באמצעות טכנולוגיות מתקדמות מבוססות אוטומציה וצוות אנליסטים בכירים, המרכזים מנתחים מידע שהתקבל מהגופים, משתפים מידע, מגבשים תמונת מצב, מונעים אירועי סייבר, מסייעים לרציפות תפקודית וכן מפיקים תובנות לאומיות.

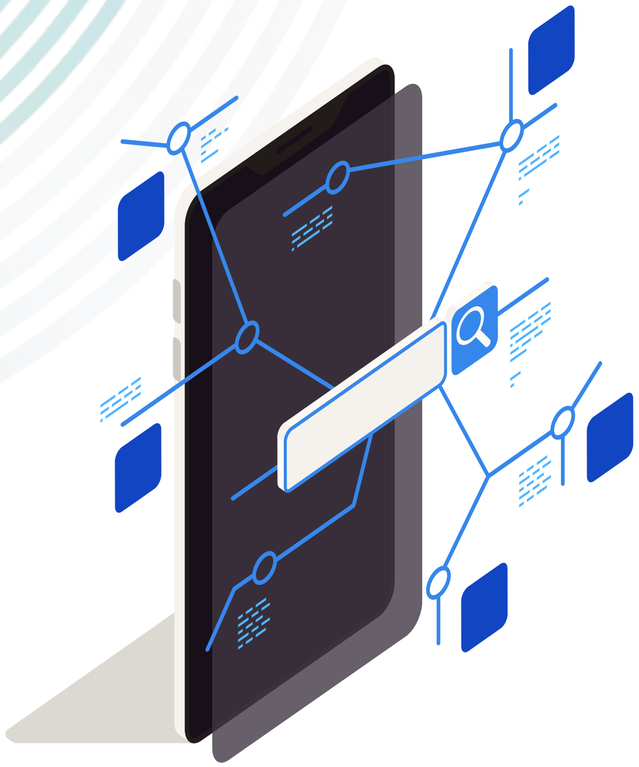
במהלך המלחמה שם המערך כמטרה את נושא העלאת החוסן במשק, בניסיון להגיע לכמה שיותר גופים ומגזרים.

מיזמים טכנולוגים לאומיים להעלאת חוסן

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).

בשנת 2024, החלה המערכת להיות מבצעית ונכון להיום מחוברים אליה קרוב ל-**60** ארגונים ממגזרים חיוניים שונים.



97 ניסיונות למתקפות בארגונים חיוניים שזוהו ונבלמו בעזרת המערכת.

30 אירועי סייבר משמעותיים שנבלמו.

מיזמים טכנולוגים לאומיים להעלאת חוסן

מיזם TITAN - מכפילים את היקף ההגנה על ארגונים

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, העוסקות באיתור, ניטור ומניעת אירועי סייבר במשק הישראלי, מעניקות שירות הגנה לאלפי גופים במשק הישראלי וכך דרך שיתוף במידע הגנתי עימם, מתחזק באופן מרוכז ורחב החוסן במשק.

המערך משתף מידע טכני באופן מהיר עם החברות בפורום אשר משתמשות בו כדי להגן על לקוחותיהן באופן מיטבי. המיזם מביא לידי מימוש מקסימלי את היכולת המצרפית של תעשיית וקהילת הסייבר בישראל במטרה לזהות ולמנוע מתקפות סייבר.

16
חברות MSSP במיזם

1,532
גופים במשק הישראלי שמשתמשים בשירות של החברות

186
שיתופי התרעות, דוחות ומידע הגנתי

הגנה על תשתיות מדינה קריטיות

החוק מגדיר כ-50 גופים בישראל על פי חוק כתשתיות מדינה קריטיות - תשתיות אשר הפגיעה בה באמצעות מתקפת סייבר עלולה להסב נזק לאומי מיוחד.

בתקופת מלחמה, עלו הנסיונות מצד אויבינו לפגוע בתשתיות אלו כדי להפריע למהלך החיים בישראל.

תשתיות אלו זוכות להנחיה ולבקרה לאומית צמודה של המערך בתחום הסייבר, כדי לוודא את עמידתן ברמת הגנה מרבית.

הגנה על תשתיות מדינה קריטיות

הגופים המוגדרים תשתית מדינה קריטית נמדדים על ידי המערך על פי סט של יותר מ-**900** בקרות בשם "רימון", המחולק לחמש דרגות מ-1 עד 5.

בשנת 2024 חלה עלייה של **4.5%** ברמת ההסמכה בדירוג "רימון" בהשוואה לשנת 2023.
גופים בעלי הסמכה של 3 ומעלה הם בעלי יכולת התמודדות עם רוב המתקפות השכיחות.
רוב הגופים שמתחת לדירוג זה, הם גופים שתהליך חיזוק ההגנה אצלם הוא יחסית חדש והם נמצאים בתהליך מדורג ומתמשך.

3.82 ממוצע "רימון" של כלל הגופים ב-2024

62% מהגופים הם בעלי **ציון בטוח (3.5 ומעלה)**

37 מערכות אושרו לעלייה לענן (בקרב גופי התשתיות הממשלתיים)

התפלגות רמת ההגנה בגופי תשתית מדינה קריטית*:

* בתהליך לקראת קבלת הרימון או הוסמכו.

הזדהות בטוחה וביומטריה

הפעילות בתחום ההזדהות והיישומים הביומטריים במערך מתבצעת בשלושה מישורים מרכזיים:

1. פיקוח, הכוונה וגיבוש מדיניות בתחום הביומטרי
2. הכוונה ובניית יכולות בהזדהות בטוחה
3. ניהול המעבדה הלאומית לביומטריה

במלחמה, היה עיסוק מוגבר בנושא סיוע המאגר הביומטרי לזיהוי באירוע רב נפגעים

הזדהות בטוחה וביומטריה

הישגים מרכזיים בשנת הפעילות:

פרסום **דו"ח הממונה #14**
המספק תמונת מצב מקיפה על הפיקוח בפרויקט התיעוד והמאגר הביומטרי.

פעילות **"הגבהת חומות"**
מול **2** משרדי ממשלה להגברת ההגנה על מאגרים ביומטריים.

ביצוע **מבדק eKYC**
לזיהוי הונאות וזיופי מסמכים עבור **7** ספקים.

מימון 12 מחקרים
בתחום הביומטריה והסייבר בשיתוף אוניברסיטת חיפה.

גיבוש **9 חוות דעת מקצועיות**
בנושא הזדהות דיגיטלית בטוחה במגזר הממשלתי והציבורי.

בדיקות לאיומי Deep Fake
במערכות הזדהות אונליין עבור **3** ספקים.

ליווי והכוונה ל-55 משרדי ממשלה,
בהתאמה למדיניות הזדהות דיגיטלית בטוחה.

מבדק חוסן מקיף
למערכת ההזדהות המרכזית בממשלה.

פרסום **2 דוחות פיקוח מיוחדים**
בהקשר להוראת השעה "חרבות ברזל", שעסקו בזיהוי נעדרים וחללים.

דו"ח המלצות לשר הפנים ולכנסת
אודות תפקיד המאגר הביומטרי הלאומי בזיהוי חללים באירוע רב-נפגעים.

מגמות בחקיקה, מדיניות ואסטרטגיה

בעוד שמתקפות הסייבר הולכות ומשתכללות, המסגרת החקיקתית בישראל המסדירה את הגנות הסייבר על מגזרים שונים, נשארה במקום. מנגד, בעולם בולטת המגמה לחיזוק ולהרחבה של רגולציית הגנת הסייבר ועיגונה בחקיקה ראשית.

מערך הסייבר הלאומי מקדם חקיקה לאומית בהתאם לסטנדרטים המקובלים בעולם במטרה לחזק את החוסן של ארגונים החיוניים לרציפות התפקודית.

מגמות בחקיקה, מדיניות ואסטרטגיה

התמודדות עם איומי סייבר במגזר השירותים הדיגיטליים

בעקבות העלייה במתקפות סייבר במהלך מלחמת "חרבות ברזל", אושרה בכנסת הוראת שעה שמטרתה להתמודד עם מתקפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון.

קידום חוק הגנת הסייבר הלאומי

במהלך השנה האחרונה, מוביל מערך הסייבר הלאומי חקיקה לאומית המבוססת על סטנדרטים בין-לאומיים שמטרתה לחזק את רמת החוסן של ארגונים חיוניים במשק ולהבטיח את רציפות פעילותם.
היוזמה תואמת את המגמות העולמיות לחיזוק ולהרחבת אסדרת הגנת הסייבר באמצעות עיגון הנושא בחקיקה ראשית.

החוק נועד לשפר את רמת ההגנה על ארגונים החיוניים לתפקוד המשק, בין היתר באמצעות:

- **חובת דיווח** על אירועי סייבר משמעותיים.
- **דרישה ליישום הגנה בסיסית בסייבר** בארגונים חיוניים.

מדיניות לצמצום סיכוני IoT

על רקע העלייה באיומי הסייבר ממוצרי "האינטרנט של הדברים" (IoT), מקדם המערך מדיניות לצמצום סיכונים ממוצרים אלו. המדיניות תואמת את ההתפתחויות הבין-לאומיות, ובפרט את "חוק חוסן הסייבר האירופי" (Cyber Resilience Act) שהועבר השנה, ובו דגש על אבטחת מוצרים דיגיטליים.

עקרונות פיתוח מאובטח

בהתאם למגמות הגלובליות, מקדם המערך את עקרונות הפיתוח המאובטח (Security by Design & Default) בתעשיית התוכנה הישראלית.
מהלכים אלו כוללים שיח יזום ומפגשים עם התעשייה, האקדמיה ומומחים בתחום, במטרה לשלב תשתית אבטחה חזקה כבר בשלבי הפיתוח הראשוניים.

האסטרטגיה הלאומית להגנת סייבר של ישראל

היערכות אסטרטגית מחודשת בעקבות מלחמת "חרבות ברזל"

בשנת 2023, הוביל המערך תהליך מקיף לגיבוש אסטרטגיה לאומית להגנת סייבר. מתקפות הסייבר שהתעצמו במהלך מלחמת "חרבות ברזל", הדגישו את הצורך בבחינה מחודשת של האסטרטגיה הלאומית, תפיסותיה והיעדים שהוגדרו קודם למלחמה.

התובנות שהופקו יעוגנו במסמך האסטרטגיה החדש הצפוי להתפרסם בתחילת 2025.

אסטרטגיה זו תתווה יעדים לאומיים לשלוש השנים הקרובות (2025-2028) ותכלול תוכנית יישום לאומית מפורטת.

מערך
הסייבר
הלאומי

העלאת מודעות לאיומי הסייבר לציבור הרחב

כחלק מפעילות המערך להעלאת מודעות הציבור לחשיבות הגנת הסייבר, הושקו בשנת 2024 שישה קמפיינים ייחודיים, שנועדו להנגיש מידע וכלים להתמודדות עם איומי סייבר רלוונטיים.

האיומים כלפי אזרחים התעצמו במלחמה והצורך בהעלאת מודעות לסכנות, לדרכי הגנה, והשראת ביטחון בקרב הציבור התעצם.

בין הקמפיינים:

- העלאת מודעות בקרב צעירים לסכנות הדיוג (פישינג)
- הגנה מפריצה לרשתות חברתיות
- הסברה על הגנה על מצלמות אבטחה
- קמפיין ייעודי לאוכלוסייה הערבית
- ועוד

סיכום שנה 2024

העלאת מודעות לאיומי הסייבר לציבור הרחב

6
קמפיינים

כ-26M
חשיפות להמלצות ולאזהרות של המערך

42
אזהרות לציבור

שיתופי פעולה בין-לאומיים

שיתופי פעולה בין-לאומיים

מערכת Crystal Ball

מערכת לשיתוף פעולה בין-לאומי במאבק במתקפות כופרה. המערכת מספקת מעטפת הגנה לארגונים חיוניים במטרה לצמצם את פוטנציאל הנזק מאירועי סייבר.

המערכת פותחה בשיתוף פעולה של המערך, איחוד האמירויות ומיקרוסופט ישראל. המערכת משמשת את מדינות ה-CRI (Counter Ransomware Initiative) אשר לוקחות חלק בשיתוף המידע בה.

70
מדינות חברות ב-CRI

33
מדינות הצטרפו לפלטפורמה או בתהליך הצטרפות

Microsoft

71
שיתופי מידע מהמדינות:

- ישראל
- ארצות הברית
- איחוד האמירויות
- סינגפור
- ספרד
- קניה
- אלבניה

פרסומים משותפים עם גופי הגנת הסייבר בעולם

Engaging with Artificial Intelligence
עדכון והרחבה

שיוך לפעילות Cyber Avengers נגד מגזר המים בארה"ב וניסיונות תקיפה בישראל

התרעה והנחיה על פעילות קבוצת התקיפה Emennet Pasargad

כופרה בשם Phobos

מעבדת חדשנות לאנרגיה, בקרה וסייבר

מעבדת חדשנות

לאנרגיה, בקרה וסייבר

בשנים האחרונות התחזקה פעילות החדשנות שמייצר האקו-סיסטם בתחום הסייבר בבאר שבע. בין המיזמים של המערך גם המעבדה הלאומית לאנרגיה, בקרה וסייבר (ICNL) שהחלה לפעול במלואה השנה.

בשנת 2024 ביצעה המעבדה מבדקים טכנולוגיים לטכנולוגיות מתקדמות בתחום האנרגיה של חברות הזנק וחברות בין-לאומיות, ערכה מחקרים דואליים בשיתוף מפאת, וכן משימות פיתוח יכולות בתחום פורנזיקה לעולמות ICS/OT.

בנוסף, המעבדה השיקה תוכנית לסטודנטים בליווי מנחים שבמסגרתה הוגשו עבודות הגמר המבוססת על מחקר במעבדה.

המעבדה הלאומית
למערכות בקרה וסייבר

27 ניסויים ומחקרים

32 הדרכות ואימונים

1,100 משתתפים ומבקרים

תעשיית הסייבר

מדינת ישראל היא אחת מהמדינות המובילות בעולם בתחום הסייבר, בזכות שיתוף הפעולה של תעשיית הסייבר כולה באקו-סיסטם הישראלי המייצרים יחד פתרונות הגנתיים חדשניים.

היקף ההשקעות הפרטיות בחברות הסייבר בשנת 2024 עמד על **3.8 מיליארד $**, המהווים **36%** מסך ההשקעות בענף ההייטק לשנה זו.

תעשיית הסייבר

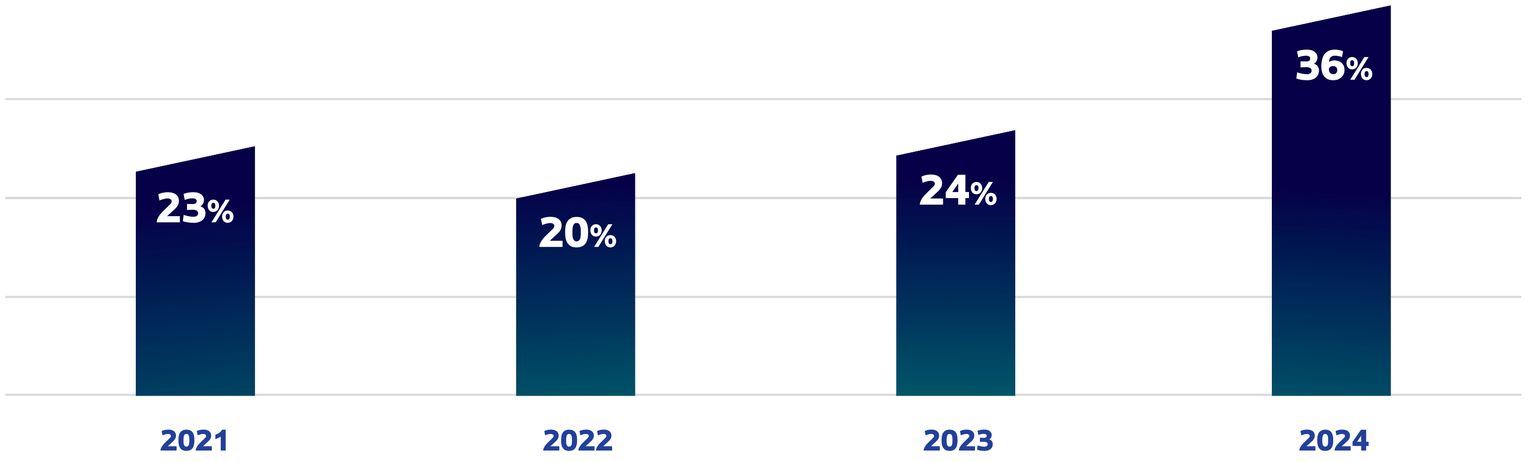
ההשקעות בחברות סייבר ישראליות לאורך השנים[1]:

הנתונים המעודדים של תעשיית הסייבר הישראלית, גם בשנה מאתגרת, מעידים על הצורך בהמשך חיזוק התעשייה ותרומתה לכלכלה. המפתח להמשך קידום התעשייה ועידוד החדשנות והיזמות הטכנולוגיות טמון בהשקעה בפיתוח ובהכשרת ההון האנושי.

עלייה של
90%
בהיקף ההשקעות בסייבר בהשוואה לשנת 2023

5 מתוך 10
סבבי הגיוס הגדולים ביותר בהייטק בשנת 2024 היו בתחום הסייבר.

אחוז ההשקעות בתחום הסייבר מתוך כלל ההשקעות במגזר ההייטק הישראלי:



[1] עיבודי מערך הסייבר הלאומי לנתוני הדו"ח השנתי לשנת 2024 על האקוסיסטם הישראלי בהייטק של Startup Nation Central

הון אנושי

בשנת 2024, לצד האתגרים המשמעותיים שנבעו משנה של מלחמה, חוסר ודאות ותנאים מבצעיים מורכבים, נמשכה ההשקעה בהכשרת אוכלוסיות מגוונות לתחומי סייבר ובינה מלאכותית.

התוכניות שאפו לשמר רצף לימודי והזדמנויות שוות עבור תלמידים ובוגרים מכלל המגזרים, ובכלל זה תוכניות ייעודיות לנערות ותוכניות לחברה הערבית. עיקר הפעילות התמקדה בפריפריה הגאוגרפית, אך בשל המציאות הביטחונית והצורך בפינוי אוכלוסיות רבות, חלה ירידה בהיקף המשתתפים בהשוואה לשנים קודמות, מה שהוביל להתאמות ושינויים בתוכניות ההכשרה והנגשה.

הון אנושי בסייבר בישראל

תוכניות לבני ובנות נוער מהפריפריה הגאוגרפית - חברתית

תוכנית גשרים

8,000
תלמידים

54
בתי ספר

20
רשויות

תוכנית מגשימים

173
כיתות

תוכנית ממריאות

55
כיתות

סך הכל בשתי התוכניות

3,420
תלמידים

228
כיתות

תוכניות לאוכלוסייה בוגרת

סייברספייס

287,000
רשומים

16,020
סיימו את הקורסים בהצלחה

שותפים לפרויקטים

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

כתיבה ועריכה:
אגף דוברות פרסום והסברה

מערך
הסייבר
הלאומי