Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

19 בפברואר 2026
ב' בהדר תשפ"ו

לכבוד:
מערך הסייבר הלאומי – משרד ראש הממשלה
(באמצעות אתר התזכירים הממשלתי)

הנדון: התייחסות איגוד האינטרנט הישראלי לתזכיר חוק הגנת הסייבר הלאומית, התשפ"ו-2026

שלום רב,

איגוד האינטרנט הישראלי (ע"ר) ("**איגוד האינטרנט**")[1] מתכבד להגיש את התייחסותו המקצועית וחומרי רקע לקראת הדיון בתזכיר חוק הגנת הסייבר הלאומית, התשפ"ו-2026 שהתפרסם להערות הציבור ביום 22.1.2026 (להלן: "**תזכיר החוק**").

כפי שמציינים דברי ההסבר לתזכיר החוק, מרחב הסייבר מהווה כיום תשתית אסטרטגית בעלת השפעה מכרעת על הביטחון הלאומי, הכלכלה והחברה בישראל, כאשר מאז פרוץ מלחמת "חרבות ברזל" באוקטובר 2023,חלה עלייה חדה ומדאיגה בהיקף ובעוצמת התקיפות המכוונות נגד גופים אזרחיים במשק, מתוך מטרה לפגוע בחוסן הלאומי וברציפות התפקודית של שירותים חיוניים לציבור.

איגוד האינטרנט הישראלי מזהה גם הוא את העליה המתמדת בעוצמת הסיכון הקיברנטי למשק ולמשתמשים בישראל, ואנו סבורים כי אכן בשלה העת לעיגון מסגרת חקיקתית ייעודית ומקיפה בראייה לאומית. חקיקה כזו נדרשת כדי למלא את החלל הקיים כיום, להבטיח סטנדרט הגנה מחייב לארגונים שבלעדיהם המדינה אינה יכולה לתפקד, וליישר קו עם הנורמות המקובלות במדינות המערב, דוגמת דירקטיבת NIS2 של האיחוד האירופי.[2]

עם זאת, לאור ניסיוננו המעשי בניהול תשתיות אינטרנט מרכזיות בישראל, ולאחרונה כגוף הנמצא תחת סמכות האסדרה של מערך הסייבר הלאומי מכוח חוק הסדרת הבטחון בגופים ציבורים, התשנ"ח-1998 וכעמותה שבין

[1] איגוד האינטרנט הישראלי הוא עמותה בלתי תלויה וללא כוונת רווח, המנהלת שתי תשתיות אינטרנט חיוניות בישראל - מרשם שמות המתחם המדינתי (".il" ו-".ישראל") והפצת המידע על אודותיו ל-DNS, ומחלפי האינטרנט הפנים-מדינתי (IIX ו-IL-IX). האיגוד הוכרז בשנת 2018 כמפעיל "מערכת ממוחשבת חיונית" על פי חוק הסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998. במקביל לפעולתו התשתיתית, פועל האיגוד לקידום ושמירה על עקרונות דמוקרטיים בפעולתו של האינטרנט בישראל. בכלל זה, מפרסם איגוד האינטרנט מחקרי מדיניות המיועדים ליידע ולטייב את זירת האינטרנט הישראלית והגלובלית, על בסיס עבודת מחקר מקיפה ומומחיותיו בצמתים מגוונים של משפט וטכנולוגיה. מחקרי מדיניות אלו כוללים ידע מקצועי והמלצות מעשיות עבור גורמי ממשל והקהל הרחב. למידע נוסף, ראו https://www.isoc.org.il.

[2] האיחוד האירופי: כניסה לתוקף של רגולציית הגנת סייבר חדשה בתחום התשתיות החיוניות (NIS2, CER)
https://www.isoc.org.il/regulation-digital-services/global-review/nis2-cer

מטרותיה גם הגנה על זכויות אדם ואזרח במרחב הדיגיטלי,[3] נבקש להציע מספר תיקונים. במסמך זה נפרט דיוקים והבהרות לפרקי החקיקה השונים, אותם נדרש להוסיף ולפתח עם התקדמות תהליך החקיקה, במטרה להבטיח את יעילות רגולטורית תוך שמירה על האיזונים הנדרשים להבטחת האינטרס הציבורי, הוודאות העסקית במשק וזכויות אזרח.

הערות ודגשים לפרק ההגדרות

דברי ההסבר לתזכיר מציינים במפורש כי "מדובר בחקיקה ממוקדת, דיפרנציאלית המבוססת על ניהול סיכונים ואיזון רגולטורי". עם זאת, האיגוד סבור כי קיימת סתירה פנימית בין הצהרה זו לבין חלק מההגדרות שנותרו רחבות ועמומות. יש לשקול להרחיב ולספק הגדרות מדויקות וקביעת מדרג פנימי.

"נכס מידע משמעותי": ההגדרה הקיימת מתמקדת בתוצאה הפונקציונלית של פגיעה בנכס ("שתקיפת סייבר נגדו עלולה..."), אך נעדרת הגדרה מהותית למונחים היסודיים "מידע" ו-"מאגר מידע". מומלץ לשקול או להפנות להגדרות הקבועות בחוק הגנת הפרטיות, התשמ"א-1981 (להלן – **חוק הגנת הפרטיות**) ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן – **תקנות אבטחת מידע**), או לחלופין לקבוע הגדרות מדויקות בגוף החוק. זאת, על מנת למנוע כפילות רגולטורית, סתירות משפטיות ואי-ודאות הן מול סמכויות הרשות להגנת הפרטיות, והן אשר להיקף הסמכות שמוקנות על פי החוק. כמו כן, מוצע כי לצד ההגדרה בחקיקה, יוסמך מערך הסייבר (בתיאום עם הרשות להגנת הפרטיות) לפרסם הנחיות ספציפיות לסיווג, על מנת ליצוק תוכן מעשי למונח "משמעותי" בהתאם לרגישות המידע וסוג המאגר.

"ספק שירותים דיגיטליים ושירותי אחסון": סעיף (1) להגדרה כולל כל שירות המקיים "קשר פיזי או לוגי קבוע או ארעי" עם מחשבי מקבל השירות. ניסוח רחב זה עלול להחיל חובות רגולטוריות כבדות על ספקים שאינם מהווים סיכון מהותי לתשתית הלאומית. יש לשקול הגדרת רף של מהותיות או זיקה קבועה לליבת השירות (למשל, שהקשר עם מחשבי הלקוח הוא מהותי ומרכזי לליבת השירות) וזאת על מנת למנוע החלת חובות רגולטוריות כבדות על ספקים שאינם מהווים סיכון משמעותי.

"פגיעות חמורה": ההגדרה אינה מבהירה מי מוסמך לקבוע כי פגיעות היא "חמורה", ואינה קובעת מתודולוגיה מוכרת לסיווג. יש לקבוע האם מערך הסייבר הוא הגוף היחיד המוסמך להעריך "פגיעות חמורה" או שמא יש להסמיך גופים נוספים בעלי ניסיון וכשירות לזיהוי פגיעות חמורה. כמו כן, ראוי לקבוע בחוק מנגנון סיווג שקוף ע"ב מתודולוגיה מקובלת בתחום (למשל CVSS מעל סף 0.7)[4] וחובת פרסום ציבורי של רשימת פגיעויות חמורות שאושרו, יחד עם מנגנון ערעור.

---

[3] פעילות קו הסיוע לאינטרנט בטוח בשנת 2025 - https://www.isoc.org.il/sts-data/helpline-isoc-2025

[4] דירוג CVSS - Common Vulnerability Scoring System – הוא הסטנדרט המקובל כיום לדירוג פגיעויות (להבדיל מדירוג סיכונים), ומאומץ בין היתר על ידי NIST. ראו: https://nvd.nist.gov/vuln-metrics/cvss

"פעולה להגנת סייבר בחומר מחשב": היעדרה של הגדרה למונחים "רשת" ו"רשת הארגון" פוגעת במידתיות ולגיטימיות סמכות חודרנית זו, התלויה בכך שפעולות מרחוק מוגבלות לרשת הארגון ואינן זולגות לרשתות או חומר מחשר של צדדים שלישיים או לקוחות.

"שירותי אחסון": ההגדרה הנוכחית אינה מבהירה האם נכללה בה גם גם אחסון פיזי של חומרי מחשב (כמו כוננים או קלטות גיבוי) שאינם מחוברים לרשת. לגישת איגוד האינטרנט הישראלי, יש להחריג אחסון פיזי שאינו מקוון מהחובות הטכנולוגיות המפורטות בחוק באופן מפורש, או לצמצם אותן בהתאם לסיכון הספציפי.

"שירותים דיגיטליים": ראו הערות בפרק ייעודי.

"תקיפת סייבר": מומלץ להרחיב את ההגדרה כך שתכלול במפורש את המרכיב של "פרסום מידע שהושג שלא כדין. ההגדרה הנוכחית מתמקדת בפריצה ובשיבוש, אך אינה מתייחסת לפרסום מידע שהושג שלא כדין – שלעתים קרובות מהווה את עיקר הנזק לציבור, כפי שראינו באירועים דוגמת התקיפה על המרכז הרפואי "מעייני הישועה". מוצע להרחיב את ההגדרה כך שתכלול במפורש גם פרסום מידע שהושג שלא כדין כתוצאה ממתקפת סייבר, בין אם על ידי התוקף ובין אם על ידי צד שלישי.

פרק ב' לחוק: מערך הסייבר הלאומי

<u>כשירויות וביקורת על הפעלת הסמכויות החדשות</u>

הגדרת מערך הסייבר הלאומי כגוף "מבצעי-טכנולוגי" בס' 2 אינה מתיישבת עם הסמכויות שהתזכיר מבקש להעניק לו, שהן סמכויות של גוף מאסדר במרחב הקיברנטי, בעל סמכויות אסדרה וענישה בדרך של הטלת עיצומים כספיים. גוף טכנולוגי במהותו מספק כלים, הגנה וייעוץ, בדומה לפעילות ה-CERT וה-SOC הלאומיים המוזכרים בדברי ההסבר. אולם, סמכויות מנהליות ושל מדיניות מצביעות כי מדובר למעשה בגוף מאסדר. בנוסף, התזכיר מבקש "להפריט" את סמכות הטלת עיצומים כספיים לקבוצה גדולה של בעלי תפקידים במערך הסייבר הלאומי, ברגולטורים ענפיים ובגופים נוספים בהסמכתם להטיל עיצומים כספיים, וזאת מבלי לקבוע תנאי כשירות למילוי תפקיד זה ומבלי לקבוע מסגרת מהותית להפעלת סמכויות אלה.

נזכיר כי חלק מהסמכויות שהתזכיר מבקש לתת לראש מערך הסייבר ולממונים ברגולטורים ענפיים דומות, והפעלתן עשויה להיות למקרים דומים, לאלו המוקנות לראש הרשות להגנת הפרטיות. נבקש להפנות למודל הטלת העיצומים הכספיים שנקבעה בחוק הגנת הפרטיות במסגרת תיקון מס' 13, אשר התקבל לאחרונה והוחל ביישומו, כמודל ראוי ומאוזן להפעלת סמכות המאפשרת הטלה של עיצומים כספיים בסכומים גדולים על פרטים ותאגידים במגזר הפרטי.[5] התזכיר מבקש להפקיד סמכות דומה, לא בידי אדם בודד העומד בתנאי כשירות של שופט מחוזי, אלא בידי שורה רחבה של נושאי תפקידים בשירות הציבורי, בדרגת ראש אגף,

[5] ראו סימן ב': הטלת עיצום כספי; סימן ג': לסימן ד': התחייבות להימנע מהפרה; סימן ה': הוראות שונות לעניין עיצום כספי; תוספת שלישית עיצום כספי על הפרת תקנות אבטחת מידע; עיצום כספי על הפרת תקנות העברת מידע מהאזור הכלכלי האירופי; סכומים מופחתים לעניין עיצום כספי בחוק הגנת הפרטיות כמודל להסדרת הפעלת הסמכות להטיל עיצום כספי.

הממונים על ידי מנכ"לים של משרדי ממשלה ויחידות סמך שונות, שאין להם כל ידע, רקע והכשרה בהפעלה של סמכויות כאלה, שהן חלף להליכים פליליים.

ביזור זה של סמכויות הטלת עיצומים כספיים תגרום בין היתר לשונות רבה, בין המוסמכים השונים, בהטלת העיצומים. כלומר, מחד גיסא אין משטר מוגדר היטב ותחום להפעלת הסמכות, ומאידך גיסא יש גורמים רבים המפעילים את הסמכות הזו. נוסיף עוד כי בעוד שבמקרה של ראש הרשות להגנת הפרטיות, אשר לו גם סמכות חקירה פלילית, והוא יכול לבחור בין החלופות השונות (עיצום כספי, התראה מנהלית או חקירה פלילית), בהליכים על פי התזכיר לממונים המוסמכים להטיל עיצום כספי רק כלי אחד, והם עשויים להפעיל אותו מבלי לראות את התמונה הכוללת, שכן יהיה נוח לעשות זאת. נזכיר גם שהרף הראייתי הנדרש להטלת עיצום כספי הוא נמוך בהרבה מהליך פלילי, עניין שעשוי לתמרץ את בעל הסמכות להפעילה.

התוספת הראשונה לחוק הגנת הפרטיות, המעגנת את החלטות הממשלה בהקמת הרשות להגנת הפרטיות, קובעת בין היתר את עצמאות הפעלת הסמכויות של הרשות והעומד בראשה, וכן את תנאי השירות של ראש הרשות, אשר אמור להיות כשיר למינוי כשופט מחוזי והוא נעדר הרשעה פלילית או משמעתית בעבירות רלוונטיות לתחום שבו עוסקת הרשות. במקרה של ראש הרשות להגנת הפרטיות, תנאי הכשירות למינויו לתפקיד קבועים בחוק, ואף מחייבים כי יהא בעל כשירות לכהן כשופט מחוזי.

בנוסף, לא נקבעה בחוק קציבת כהונה לתפקיד ראש מערך הסייבר, ומן הראוי לקבוע, בדומה לקביעה בחוק הגנת הפרטיות ובדומה לכל תפקיד בעל סמכויות אסדרה בישראל, כי תקופת כהונתו של ראש מערך הסייבר תהא קצובה לתקופה אחת, שאינה ניתנת להארכה.

בנוסף, על פי סעיף 6 לתזכיר, לראש מערך הסייבר סמכות להסמיך עובדים של מערך הסייבר לביצוע פעולות שונות, חלקן חודרניות ביותר למערכות מחשבים ומידע בכלל המשק הישראלי, אך החוק אינו קובע תנאי כשירות לאותם עובדים,[6] בניגוד למקובל בחקיקה עדכנית. בהיקף הסמכויות ורוחב היריעה של התזכיר, מתחייב כי הדרישות המהותיות להסמכת העובדים יקבעו בחקיקה, אשר גם תחייב חקיקת משנה מפורטת לתנאי הכשירות הספציפיים למשימה.

מול היקף הסמכויות הנרחב שתזכיר החוק מבקש להעניק למערך, נדרש לקבוע בחוק מנגנוני פיקוח הולמים מעבר לחובת הדיווח השנתי החסוי לוועדת החוץ והביטחון. לכל הפחות, יש להוסיף עיגון מפורש של כפיפות מערך הסייבר למערך ביקורת המדינה (למעט מידע מסווג) וחובת פרסום דוח שנתי פומבי (למעט מידע מסווג). כמו כן, ראוי לקבוע מנגנונים נוספים של פיקוח ציבורי, כגון הקמת ועדת ייעוץ ציבורית בהשתתפות נציגי ענף הטכנולוגיה, האקדמיה והחברה האזרחית.

<u>היבטי תיאום בין גורמי הגנת הסייבר ואחריות לגיבוש תמונת מצב סייבר</u>

תזכיר החוק אינו מסדיר בבירור את שאלת האחריות המקצועית על גיבוש תמונת מצב הסייבר הלאומית או את הממשקים בין המערך לבין גורמים מקבילים רלוונטיים, כגון רשות הגנת הפרטיות, גופי הבטחון

[6] ראו והשוו: סעיפים 23ט' 23נ' לחוק הגנת הפרטיות.

ורגולטורים סקטוריאליים. מוצע לעגן בחוק חובת אחריות מפורשת של ראש המערך לניהול תמונת מצב סייבר לאומית מאוחדת, ולקבוע מנגנון לשיתופה – בצורה מאובטחת ובהגנה על מידע מסווג – עם הרשויות המוסמכות הסקטוריאליות ועם ארגונים חיוניים, לשם חיזוק ההגנה המונעת.

כמו כן, תזכיר החוק מזכיר את ה-CERT ואת ה-NSOC אך אינו מגדיר את מסגרת פעולתם, גבולות סמכותם, ומנגנוני ה-CERT ביחס לדיווחי ארגונים. מומלץ לקבוע בחוק או בתקנות SLA לתגובת ה-CERT לדיווחי ארגונים וכללים לחלוקת אחריות בין ה-CERT לבין היחידות המגזריות.

פרק ד' לחוק: אסדרה לאומית בתחום ההגנת הסייבר

בחירת המחוקק לא לאמץ את קריטריון ה-NIS2 הגורף (כל ארגון מעל 50 עובדים או מחזור כספי העולה על 100 מליון יורו) ובמקומו לקבוע סף סקטוריאלי ממוקד מאפשרת למקד את נטל הרגולציה על ארגונים בעלי פוטנציאל נזק לאומי משמעותי.

עם זאת, התבחינים והספים שנקבעו למגזר השירותים הדיגיטליים נמוכים במיוחד - ספקים עם מחזור מעל 40 מיליון ש"ח או מעל 50 עובדים, או כאלו המספקים שירותים לממשלה או לגוף מונחה - **ועלולים לכלול חלק ניכר מתעשיית ההייטק הישראלית מבלי שפעילותה מהווה סיכון לתשתית לאומית.** מעבר לכך, גם האכיפה כלפי ספקיות טכנולוגיה רב-לאומיות (כמו גוגל, אמזון או מיקרוסופט) תהיה מורכבת ואולי בלתי אפשרית, באופן שייצור אכיפה לא-שוויונית לרעת חברות ישראליות. על כן, מוצע לעדכן את הוראות הפרק על בסיס העקרונות הבאים:

א. הפרדת קריטריון "ספק לממשלה": לקבוע שספק לממשלה ייחשב ארגון חיוני רק אם שווי ההתקשרות עולה על סף מינימלי (לדוגמה: 5 מיליון ש"ח לשנה).

ב. מניעת אפליה בין ספקים מקומיים לבינלאומיים: לעגן מנגנון הכרה בציות שהוכח ביחס לרגולציה בינלאומית (SOC 2, ISO 27001, FedRAMP) כתחליף לחלק מדרישות הדיווח המקומיות.

כמו כן, בהתאם להגדרת התזכיר בדברי ההסבר כ"השלמה" בלבד להסדרת תשתיות מדינה קריטית, יש לעגן במפורש את החרגת ה"גופים המונחים" מחובות רמת ההגנה הבסיסית. צעד זה נועד למנוע סתירות מול משטר ההנחיה המקצועי של גופי הביטחון (מלמ"ב/שב"כ) המעוגן בחוק להסדרת הביטחון.

סימן ב': הגנת סייבר בארגונים והצורך בעיגון חובות דיווח הדדיות ושיתוף מודיעין

תזכיר החוק מתמקד בחובות הדיווח של הארגונים, אך שותק באשר לחובות המערך כלפי המשק והארגונים המונחים על ידי מערך הסייבר. **אנו סבורים כי הצלחת המאמץ הלאומי מבוססת על הדדיות, כך שראוי לעגן בחוק גם חובה של מערך הסייבר לשתף תמונת מצב ומידע מודיעיני רלוונטי עם הארגונים החיוניים, כדי לסייע להם להתגונן מראש מפני איומים מזוהים.**

עיגון החובה המפורשת של מערך הסייבר לשתף מודיעין סייבר מונע (לרבות מידע על טכניקות התקיפה, מערכי תוקפים ידועים וחתימות איומים) עם ארגונים חיוניים או מונחים רלוונטיים, בכפוף להגנות על מידע מסווג, היא מרכיב יסוד של המודלים האסדרתיים ב-NSC הבריטי ו-CISA האמריקני וראוי לעגנה גם בזירה הישראלית.[7]

כמו כן, לשם הגנת הפרטיות בדיווחים המועברים למערך ו/או למאסדר הסייבר הענפי נדרש לקבוע בחקיקה חובה להטמיע מנגנוני "התממה" (Anonymization) על ידי הגוף המדווח, כדי להבטיח שמידע טכני לא יכלול פרטי זיהוי של משתמשי קצה ללא צורך מבצעי מובהק.

בנוגע לסעיף 10 הסוקר את רמת הגנת הסייבר, אנו סבורים כי חזקות הציות בסעיף קטן ב(1) אינן מספקות מענה מספק לטיוב הנטל הרגולטורי, שכן הן מותנות בהלימה לדרישות התוספת הרביעית ובכך יוצרות נטל רגולטורי כפול. בנוסף, סעיף קטן ב(3) פוגע בוודאות העסקית בכך שהוא מאפשר לראש הממשלה לשנות את התוספת ללא הליך חקיקה סדור או היוועצות סטטוטורית עם גורמי מקצוע רלוונטיים.

סימנים ג'-ד': סמכויות פיקוח וחדירה לביצוע פעולות בחומר מחשב

האינטרס הציבורי והמציאות העכשווית מצריכים לספק לרשויות האכיפה המדינתיות כלים אפקטיביים לפעול בעת מתקפת סייבר חמורה. עם זאת, הסמכויות חסרות-התקדים שתזכיר החוק מאפשר להקנות למערך הסייבר – ובפרט הסמכויות לדרוש ידיעות ומסמכים ולביצוע פעולות פעילות בחומר מחשב פרטי – מעוררות חשש חוקתי וביטחוני שיש לטפל בו.

בהינתן כי קיימת תכלית ראויה וצורך ממשי – הבטחת הרציפות התפקודית של שירותים חיוניים ומניעת נזק "רוחבי" למשק – הלגיטימיות החוקתית של סמכויות אלו תלויה בקיומם של מספר עקרונות אותם יש לעגן באופן יותר מפורש בחקיקה:

מדרג פעולה מובנה (Step-by-step escalation): פעולה אקטיבית של המדינה בדרישת ידיעות ומסמכים ולבטח בחדירה לחומר מחשב של גוף פרטי תבוצע אך ורק כמוצא אחרון, לאחר מתן אפשרות זמן סביר לפעולה עצמית ו/או סיוע טכני מרחוק בנוכחות ופיקוח נציג הארגון. רק במקרה של חוסר יכולת או סירוב הארגון, ובתנאי שקיים חשש ממשי לנזק לאומי – תופעל סמכות ביצוע ישירה. יש לעגן בטקסט החוק כי הפעלת סמכות המערך לפי סעיף 17 והוראות סימן ב' תוגבל אך ורק למקרים בהם קיים "צורך להסתייע ביכולות שמצויות בידי מערך הסייבר הלאומי ולא בידי הרשות המוסמכת", ותבוצע ככל הניתן "באמצעות הרשות המוסמכת".

צמידות מטרה – כל המידע שיאסף במסגרת הפעולות להגנת סייבר ישמש למטרה זו בלבד, ולא ישמש למטרות אחרות.

תיעוד ובקרה: כל פעולה אקטיבית חייבת להיות מתועדת באופן מלא ובלתי ניתן לשינוי, אשר יוגש לעיון

[7] ראו למשל: https://www.ncsc.gov.uk/blog-post/introducing-active-cyber-defence-2; https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais

הארגון ולביקורת שיפוטית בדיעבד, כדי להבטיח שהפעולות לא חרגו מהנדרש לבלימת התקיפה.

ביקורת שיפוטית ומדרג סנקציות: מומלץ כי מתן הוראות לביצוע פעולות אקטיביות בחומר מחשב (סריקה, חסימה או ניתוק) יותנה באישור שיפוטי מקדים, בדומה לצווי חיפוש, תפיסה או חדירה לחומר מחשב. כמו כן, מומלץ לשקול את המרת העונשים הפליליים בגין אי-ציות להוראות בעיצומים כספיים מדורגים, ולהותיר את המישור הפלילי למקרים של רשלנות פושעת או סיוע מכוון לגורמי אויב.

אבטחת הגישה מרחוק: אחת הסוגיות המדאיגות ביותר במישור הטכנולוגי-נורמטיבי היא יצירת "דלת אחורית" למערך הסייבר לצורך הגישה מרחוק. הכלי המאפשר למערך הסייבר לחדור לרשתות הארגונים כדי "להגן" עליהן, **הופך בעצמו ליעד אסטרטגי עבור תוקפים**. פריצה למערך הסייבר עלולה להעניק לתוקף מפתחות גישה לכלל המשק הישראלי. לפיכך, יש **לעגן בחוק דרישות מחמירות לאבטחת כלי הגישה מרחוק** של המערך, כולל שימוש באימות רב-שלבי פיזי, הצפנה מקצה לקצה והפרדה מוחלטת בין רשתות הניטור לרשתות הביצוע.

חשיבות היבטים אלו מתחדדת בשים לב לכך שהמודלים הרגולטוריים במדינות דמוקרטיות, כדוגמת NIS2, נמנעים מהענקת סמכויות חדירה פעילה דומות לאלה המוצעות בתזכיר הישראלי, ומסתמכת על חובות דיווח וביקורות תקופתיות. הפער ממחיש את הצורך בריסון מובנה של סמכויות אלו.

לכך מצטרפים גם ההיבטים הפרטניים בנוגע לסעיפי פרק זה:

דרישות ידיעות ומסמכים: הסמכות המוקנית בסעיף 12 רחבה מדי ואינה מבחינה בין פיקוח שוטף לבין אירוע נקודתי. לאור רגישות המידע המצוי בידי הארגונים, יש לצמצם סמכות זו כך שתופעל רק בכפוף לצו בית משפט ותחת עקרונות של מזעור מידע וצמידות מטרה.

"תקיפת סייבר חמורה": ס' 14 המגדיר את המונח נתון לשיקול דעת רחב מדי וכולל גם "חשש ממשי" לפעולה. מדובר בסמכות חסרת תקדים המאפשרת מתן הוראות והליכי אכיפה פולשניים, ולכן היא מחייבת הטמעת מנגנוני איזונים ובלמים וזכות שימוע לארגון.

סמכות הכרזה של צה"ל: אנו מסתייגים מהרחבת מעגל הגורמים המוסמכים להכרזה על אירוע חמור באמצעות הוספת ראש חטיבת ההגנה בסייבר הנמצא בס' 18. בהיעדר מדרג סמכויות או מנגנון תיאום ברור, סמכות זו יוצרת שכבה נוספת של נטל רגולטורי על גופים שאינם כפופים לצבא בשגרה.

פרק ה' לחוק: עיצום כספי

שיקול דעת אכיפתי: מוצע לתקן את נוסח הסעיף כך שייקבע מפורשות כי הסכום הנקוב מהווה תקרת מקסימום (קרי: "עיצום כספי בסכום של **עד** 300,000 ש"ח"). קביעה זו חיונית כדי לאפשר לרשות המוסמכת להפעיל שיקול דעת ומידתיות בקביעת גובה העיצום, תוך התחשבות בחומרת ההפרה, משך ההפרה והתנהלות הארגון. דברי ההסבר מציינים כי "מטרת העיצום המנהלי היא להחזיר את הגורם המפוקח למצב ציות ולא לגרום להפסקת פעילותו" ויש לעגן עיקרון זה בגוף החוק כאמור.

הרתעה יעילה באמצעות עיצום כאחוז מהמחזור הכלכלי של הגוף המפוקח, מעבר לסכום התקרה הנקוב, כדי להבטיח תמריצים המבוססים על היקף הפעילות, הנזק הפוטנציאלי ורמת האחריות. קביעת עיצום המושפע מהיקף ההכנסות נדרשת כדי להבטיח הרתעה אפקטיבית כלפי תאגידים גדולים, עבורם קנס בסכום קבוע עשוי להיחשב כ"עלות עסקית" (Cost of doing business) זניחה שאינה מתמרצת השקעה בהגנה. מנגנון זה יוצר הלימה בין גודל הגוף והנזק הפוטנציאלי לבין רמת האחריות המוטלת עליו.

פרקים ה'-ו' לחוק: איתור פגיעויות והוראות נוספות

סעיף 43 מאפשר למערך לאתר "פגיעויות חמורות ידועות" בארגונים ולהזהיר עליהן. האיגוד תומך בסמכות זו כמנגנון הגנה יזומה, אך מבקש לתחום את גבולותיה.

ראשית, יש להבהיר את המונח "פגיעויות חמורות הידועות" למערך הסייבר, אשר עשוי לכלול גם פגיעויות שלא פורסמו ברשימות ציבוריות כגון CVE/NVD. עמדתנו המקצועית היא שיש לעגן בחקיקה את העיקרון כי סריקה אקטיבית תוגבל לפגיעויות שפורסמו ברשימת CVE/NVD, ואילו מידע על פגיעויות שהמערך מחזיק מסיבות מבצעיות (שלא פורסמו) יועבר לארגון בנפרד בהתרעה ממוקדת – ולא באמצעות סריקה טכנית. שנית, ראוי לחייב את המערך להודיע לארגון על ביצוע סריקת פגיעויות לפני ביצועה (למעט נסיבות חריגות מוסברות) ולאפשר לארגן לתאם את מועד הסריקה.

לעניין זה, מן הראוי היה לעגן בחקיקה ראשית את העקרון שקבעה הנחיית פרקליט המדינה 2.38 "מדיניות העמדה לדין וענישה בעבירה של חדירה לחומר מחשב" משנת 2018 להימנע מלהעמיד לדין מומחי סייבר שאיתרו חולשות בשירותי תוכנה, חומרה, תקשורת. מאחר ופעילות זו, של "האקרים לבנים", קרי מומחי אבטחת מידע והגנת סייבר המאתרים כשלים שונים חשובה ביותר לשמירה על רמת הגנת הסייבר המדינתית, יש לתת וודאות חקיקתית לפעולתם התקינה והחשובה של גורמים אלה.

ס' 48 הסתייעות במומחה: הסעיף מאפשר אצילה כמעט מלאה של סמכויות פיקוח פולשניות למומחים חיצוניים, המהווה הרחבה חסרת תקדים של מעגל המוסמכים. יש לקבוע מנגנונים שיגבילו את כוחם של מומחים אלו מראש ויגדירו תנאי סף למינויים.

סעיף 49 מסדיר את חובת הסודיות החלה על מי שקיבל מידע אישי מכוח החוק, ומחייב מחיקתו בתוך שנתיים לכל היותר. האיגוד מברך על עיקרון זה, אך מדגיש מספר היבטים שיש להוסיף ולפתח בנוסח החוק:

- **תקופת שמירה – קיצור הסף**: שנתיים כתקופת שמירה מרבית עשויות להיות ארוכות מדי לסוגי מידע מסוימים (כגון כתובות IP זמניות). מוצע לקבוע תקופות שמירה דיפרנציאליות לפי סוג המידע: מידע מזהה – 6 חודשים; מידע טכני הקשור לאירוע – עד שנתיים; מידע נדרש להליכי אכיפה – עד סיום ההליך.

פרסום ציבורי של ארגון: דרישת אישור ראש המערך לפרסום ציבורי של שם ארגון מפר היא נכונה. יש להוסיף דרישה שהפרסום יכלול גם פירוט ממצאי ההפרה, כדי שישמש לא רק כסנקציה אלא גם כאמצעי שיפור מידע לשוק.

כתובות IP כמידע אישי: החוק אינו מגדיר מפורשות האם כתובת IP מהווה "מידע אישי", ומפנה לפרשנות חוק הגנת הפרטיות. האיגוד קורא לאמץ בפירוש בחוק גישה פרשנית דינמית: כתובת IP תיחשב "מידע אישי" כאשר ניתן לשייכה ליחיד בקלות סבירה – בהתאם לפסיקת בית הדין האירופי לצדק (CJEU) ולתקנות ה-GDPR.

כמו כן, על מנת להגן על הזכות לפרטיות של אדם שמידע אישי לגביו הגיע לידי אדם אחר לפי חוק זה, מוצע לקבוע בסעיף קטן (א) שככל שאדם קיבל מידע אישי שהתקבל לפי חוק זה, הוא ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא למטרת ביצוע סמכות של האדם להגנת סייבר לפי דין, או לפי צו בית משפט.

ס' 53 שמירת דינים: ההסדר חסר תאימות לחוקים מהותיים שעשויים לעמוד בסתירה לתזכיר. נדרש תיקון שיחיל את שמירת הדינים במפורש גם על חוק הגנת הפרטיות, על מנת להבטיח ודאות משפטית ולמנוע סתירות בין הרגולטורים השונים.

סעיף 58 מרחיב את הפטור מחוק חופש המידע לכלל יחידות המערך העוסקות בהגנת הסייבר על המגזר האזרחי. האיגוד מבין את הצורך בסודיות, אך מזהיר מפני הרחבה גורפת. בשים לב לערכים הראויים של מניעת חשיפה של שיטות ואמצעים מדינתיים להגנת סייבר או מידע רגיש אחר, אנו סבורים כי ראוי לצמצם את הפטור כך שיחול על (א) מידע מסווג ביטחונית; (ב) מידע שחשיפתו עלולה לחשוף שיטות ויכולות של המערך; (ג) מידע שחשיפתו עלולה לפגוע בחקירה פעילה. כלומר, הפטור לא יחול על: מידע מנהלתי-ארגוני; נהלים כלליים שאינם מסווגים; ותקציבים המאושרים על ידי הכנסת. גרסה גורפת של הפטור תפגע בשקיפות ציבורית ותקשה על פיקוח דמוקרטי אפקטיבי על גוף בעל סמכויות נרחבות.

הערות ודגשים בקשר לתוספת השלישית לחקיקה

בעוד שהתוספת הראשונה והשניה לחוק ממפות את הגורם המאסדר הענפי של מגזרי המשק השונים, התוספת השלישית לחוק מבקשת למפות את הנושאים בכל מגזר הנדרשים לאסדרה. לעניין זה נבקש להעיר בסוגיות שבהן יש לאיגוד האינטרנט הישראלי ידע מיוחד.

1. הקביעה כי ספק נקודת חילוף אינטרנט (IXP), הידוע בישראל כמחלף אינטרנט (Internet exchange) שהוא ספק המעמיד לרשות אחרים מתקן רשת המאפשר חיבור גומלין בין יותר משתי רשתות עצמאיות, לשם העברת תעבורת אינטרנט ביניהן שייכת לסעיף 9 בתוספת "שירותים דיגיטליים ושירותי אחסון" היא מוטעית. מחלף אינטרנט (IXP) הוא שירות תקשורת, בדומה לגופים המנויים בסעיף 1

לתוספת ("תקשורת") שהם ISP (ספקי גישה לרשת). מחלף פועל בעיקר באמצעות ציוד תקשורת (נתבים ומתגים), ומקשר בין רשתות מחשבים ועל כן צריך להכלל בסעיף 1. יובהר כי איגוד האינטרנט הישראלי מפעיל היום, בלעדית, שני מחלפים (IIX ו-IL-IX). עד תיקון 76 לחוק התקשורת (בזק ושידורים), התשמ"ב-1982 נדרש רשיון להפעלת שירות זה, אך דרישה זו בוטלה בתיקון 76 וכיום לא נדרש אף רישומו במרשם המתנהל על פי חוק.

2. ההגדרה של רשם שמות מתחם[8] (domain registrar) בסעיף 2 לפרק 9 בתוספת השלישית מוטעה – רשם אינו "מוכר" שמות מתחם, שכן שמות מתחם מוקצים לתקופה קצובה, והינם זכות חוזית אשר עשויה לפוג. הוא גם אינו רק עוסק ברישום מול המרשם, אלא במחזור החיים הכולל של שם המתחם, הכולל את הרישום, החידוש, עדכון הפרטים, מחיקה וכד'. רשמים יכולים להיות גופים קטנים, בינוניים וגדולים, והם יכולים לספק שירותי רישום עבור מרחבי שמות המתחם המדינתיים (אותם הם מבצעים מכוח הסמכה של איגוד האינטרנט הישראלי), או עבור TLD שונים מרחבי העולם (כגון .com, .net, .uk וכד'). אנו מציעים להוסיף להגדרה גם מתן שירותים לגופים חיוניים, כהגדרתם בתזכיר.

3. המונח "ספק DNS" בסעיף 3 לפרק 9 בתוספת השלישית צריך להיות מחולק לשניים: "ספק שירותי DNS סמכותניים (אוטוריטטביים)" ו"ספק שירותי DNS רקורסיביים" – מדובר בשתי משימות שונות לחלוטין, אשר מסופקות בדרך כלל על ידי גופים שונים, ויש להגדירם בנפרד. הראשון משמש כמקור המידע המוסמך על אודות הקישור בין שם המתחם וכתובת ה-IP המשרתת אותו, והוא באחריות המחזיק בשם המתחם (בדרך כלל, הארגון שפועל באותו שם מתחם), אף שבמקרים רבים השירות ניתן על ידי צדדים שלישיים. השני הוא ספק שירותי מידע, אשר אוסף מידע משרתים סמכותניים שונים ברחבי הגלובוס, ומעביר את התוצאה הסופית (כתובת ה-IP המשרתת את שם המתחם הספציפי) למשתמש הסופי (בין אם אדם או מכונה). ברוב המקרים, השרתים הרקורסיביים פועלים בספקי גישה לאינטרנט וממילא נמצאים תחת רגולציית הגנת הסייבר המדינתית. בנוסף, הם יכולים לפעול במסגרת הארגון עצמו, או בשירותים גלובליים כגון google, cloudflare, quad9 וכדומה.

4. מנהל מרשם TLD המוגדר סעיף 4 לפרק 9 בתוספת השלישית – נכון להיום שני ה-TLD הרלוונטיים (IL. ו.ישראל) מנוהלים על ידי איגוד האינטרנט הישראלי המוגדר כמפעיל של "מערכת ממוחשבת חיונית" ונמצא תחת סמכות ההנחיה של מערך הסייבר בנושאי הגנת סייבר ומנוי בתוספת החמישית לחוק הסדרת הבטחון בגופים ציבורים, התשנ"ח-1998. לא ברורה הסיבה להוספת TLD נוספים, שכן מדובר בהחלה אקס-טריטוריאלית שאין לה כל משמעות אפקטיבית, והיא תהא אות מתה. יותר חשוב היה לקבוע שגופים מונחים וגופים חיוניים, יעשו שימוש בשמות מתחם ברמה המדינתית, שפעולת מנהל ה-TLD שלהם כפופה לרגולציית הסייבר המדינתית.

[8] בנוסח התזכיר מצויין בטעות "מתחום" במקום מתחם. אנחנו יוצאים מהנחה שמדובר בטעות כתיב.

5. נבקש להצביע גם על חוסר בהגדרתם של גופי מדיה (תקשורת כתובה ואלקטרונית) ככאלה שהחקיקה חלה עליהם. הסכנה שבתקיפת סייבר על גוף כזה, על החברה והכלכלה הישראליים גדולה ביותר, ולמיטב הבנתנו את התזכיר הם אינם נכללים ברשימת הגופים המוגנים.

סיכום

תזכיר חוק הגנת הסייבר הלאומית, התשפ"ו–2026 מסמן צעד חשוב ומבורך בהתמודדות ישראל עם אחד האתגרים הביטחוניים-כלכליים המשמעותיים של עידן הרשת העכשווי. ניסיון 2018 הוכיח כי הצלחת חקיקה כזו מותנית ביצירת איזון ראוי בין אפקטיביות ביטחונית לבין ביטחון משפטי ושמירה על זכויות המגזר הפרטי.

האיגוד עומד לרשות הגורמים המוסמכים להמשך הידברות מקצועית על הצעות התיקון המפורטות לעיל, ומבקש להיות שותף בתהליך החקיקה השוטף.

בכבוד רב,

ד"ר אסף וינר
סמנכ"ל מחקר ומדיניות

עו"ד יורם הכהן
מנכ"ל

איגוד האינטרנט הישראלי