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

כ' בחשוון התשפ"ב
26 בספטמבר, 2021

לכבוד:
הגב' אתי שמואלי, מנהלת אגף הנדסת תקשורת
משרד התקשורת

באמצעות דוא"ל: etis@moc.gov.il

שלום וברכה,

הנדון: התייחסות לשימוע משרד התקשורת בעניין היערכות לניהול ההגנה בסייבר

איגוד האינטרנט הישראלי (ע"ר) ("**איגוד האינטרנט**")[1], מתכבד להגיש את התייחסותו לשימוע שפרסם משרד התקשורת בנושא היערכות לניהול ההגנה בסייבר ביום 11.8.2021 ("**השימוע**" או "**התיקון המוצע**").

איגוד האינטרנט שותף להנחת המוצא העומדת בבסיס התיקון המוצע, לפיה רשתות התקשורת בישראל מהוות תשתית לאומית חיונית אשר יש להבטיח את היערכותה הראויה להגנה מפני תקיפות סייבר. כמו כן, אנו סבורים כי ההסדרים המגוונים הכלולים בתיקון המוצע מכסים באופן ראוי תחומי היערכות רלוונטיים, אשר יש לוודא כי חברות התקשרות אכן מיישמות. כמו כן, אנו מברכים על אימוץ של מדרג חובות רגולטוריות, כתלות בהיקף פעילותו של המפוקח, המביא בחשבון את השונות הגדולה בין היקפם של השחקנים השונים בשוק תשתיות התקשורת והאינטרנט בישראל.

עם זאת, נבקש להציע מספר הערות מבניות באשר ל-"חלוקת העבודה" הרגולטורית בזירה זו, אליהן נדרש משרד התקשורת להתייחס בטרם ייקבעו תיקוני הרישיונות נושא השימוע.

א. החובה למנוע כפילות רגולטורית: מעמדה של רגולציית הסייבר מטעם שירות הבטחון הכללי

ההכרה בחשיבותה של הגנת מערכות ממוחשבות בקרב חברות התקשורת המרכזיות בישראל הובילה עוד בשנת 2011 לעדכון התוספת הרביעית לחוק הסדרת הבטחון בגופים ציבוריים, תשנ"ח-1998 ("**חוק הסדרת הבטחון**"), כך שתכלול את רוב ספקיות התשתית והגישה לאינטרנט בישראל: בזק, פלאפון, סלקום, פרטנר, הוט טלקום, 012 סמייל טלקום, 013 נטוויזיון, בזק בינלאומי, מירס תקשורת וחברת net 4 phi (מיזם התשתית הסלולרית המשותף של פרטנר והוט).

[1] איגוד האינטרנט הישראלי הוא עמותה בלתי תלויה וללא כוונת רווח, המנהלת שתי תשתיות אינטרנט חיוניות בישראל - מרשם שמות המתחם המדינתי (.il) והפצת המידע על אודותיו ל-DNS, ומחלף האינטרנט הפנים-מדינתי (IIX). האיגוד הוכרז בשנת 2018 כמפעיל "מערכת ממוחשבת חיונית" על פי חוק הסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 והוא מונחה על ידי מערך הסייבר הלאומי לענייני הגנת הסייבר של מערכת זו. במקביל לפעולתו התשתיתית, פועל האיגוד לקידום ושמירה על עקרונות דמוקרטיים בפעולתו של האינטרנט כתשתית טכנולוגית, מחקרית, חינוכית, תרבותית ועסקית בישראל. למידע נוסף, ראו https://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

משמעות המצאותן של חברות אלו בתוספת הרביעית לחוק הסדרת הבטחון היא הכפפתן ל-"רגולציה" מטעם שירות הבטחון הכללי בכל הנוגע לשמירת אינטרסים של בטחון לאומי בפעילותם ; ובפרט בכל הנוגע לאבטחות מערכות ממוחשבות חיוניות והפיקוח עליהן. בכלל זה, מוסמך שירות הבטחון הכללי לתת הנחיות מקצועיות לחברות התקשורת הנ"ל בכל הנוגע לאבטחת מערכות ממוחשבות חיוניות ולרבות לעניין דיווח עליהן.[2]

על רקע זה, אנו קוראים למשרד התקשורת להבהיר מדוע נדרש להכפיף את בעלי הרשיונות לרגולציית סייבר מקבילה מטעמו (להבדיל מעדכון התוספת הרביעית לחוק הסדרת הבטחון); ולהבהיר מה מתכונת "חלוקת העבודה" המתוכננת בינו לבין שירות הבטחון הכללי והרציונלים העומדים בבסיסה.

ב. כשירותו המוסדית של משרד התקשורת כרגולטור להגנת סייבר

רגולציה מדינתית על היערכות והתמודדות של ארגונים כנגד סיכוני סייבר היא התפתחות הכרחית של תפקידי הממשל בשנים האחרונות. בישראל, כמו גם במדינות מערביות אחרות, רגולציה זו מתבצעת על ידי סוכנות מינהלית ייעודית לתחום הגנת הסייבר, מתוך הבנה כי מדובר בתחום אשר דורש מומחיות מקצועית ייחודית. כך, בישראל, הרגולטור שהופקד על תחום הגנת הסייבר הוא מערך הסייבר הלאומי, כגורם המקצועי להנחיה ופיקוח על היערכות של גופים ציבוריים ופרטיים.

עם זאת, על פי מסמכי השימוע עולה כי תחום רגולציית הגנת הסייבר של חברות התקשורת בישראל מתוכנן להתבצע על ידי משרד התקשורת, אשר עד כה לא עסק בתחום מקצועי זה, **כאשר מסמכי השימוע לא מתייחסים מספקים מידע הכרחי באשר לכשירות המוסדות של משרד התקשורת לפעול כרגולטור בתחום הגנת הסייבר, בהשוואה למערך הסייבר הלאומי.**

אמנם, בשנים האחרונות התפתחה "חלוקת עבודה" רגולטורית בין מערך הסייבר הלאומי לבין רגולטורים ענפיים של סקטורים קריטיים אחרים, כגון משרד הבריאות כרגולטור הענפי של שירותי הבריאות או המפקח על הבנקים כרגולטור הענפי של מערכת הבנקאות, לפיה ההנחיות להיערכות הגנת סייבר ניתנות ונאכפות על ידי הרגולטור הענפי (תוך הנחיה מקצועית באשר לנורמות האבטחה שיש לקבוע מטעם מערך הסייבר הלאומי). על כן, ניתן להניח כי הרציונליים של חלוקת עבודה זו עומדים גם בבסיס היוזמה הנוכחית של משרד התקשורת להפוך לרגולטור הסייבר של סקטור התקשורת ותשתיות האינטרנט.

עם זאת, למיטב ידיעתנו, משרד התקשורת הוא הגוף הממשלתי היחיד שלא פועלת במסגרתו יחידה ייעודית לסייבר, כך שכשירותו המוסדית לפעול כרגולטור אפקטיבי של תחום הגנת הסייבר בסקטור התשתיות התקשורת והאינטרנט נופלת מזו של מערך הסייבר הלאומי או של שרות הבטחון הכללי. זאת, הן מבחינת הידע המקצועי הייחודי הנדרש לשם קביעת החובות הרגולטוריות שראוי להחיל על מנת להתמודד עם איומי הסייבר והן מבחינת היקף כוח האדם הנדרש לשם פיקוח אחר עמידת המפוקחים בשלל החובות הקבועות בתיקון המוצע.

[2] סעיף 10 לחוק הסדרת הבטחון.

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

בכלל זה, יש להדגיש הפיכתו של משרד התקשורת לרגולטור אבטחת הסייבר של חברות התקשורת בישראל מהווה חריג ביחס לחלוקת העבודה הרגולטורית הנוהגת במדינות מערביות אחרות, בהן הרגולטורים האמונים על הגנת הסייבר של רשתות תקשורת הם סוכנויות ייעודיות לאבטחת סייבר, או לכל הפחות רגולטור ייעודי לתקשורת אלקטרונית.[3]

על כן, אנו קוראים למשרד התקשורת שלא לקדם את תיקון הרשיונות נושא שימוע זה ללא הצגת מידע שיאפשר לבחון את כשירותו המוסדית לפעול כרגולטור הסייבר של סקטור התקשורת (ועדיפותו על פני מערך הסייבר הלאומי או שירות הבטחון הכללי), לרבות בכל הנוגע להיבטי לכוח אדם ותקצוב הנדרשים לעדכון ואכיפה שלל החובות הרגולטוריות המוצעות בשימוע זה.

***

נשמח לעמוד לרשותכם בכל הבהרה שתידרש. ניתן לפנות אלינו באמצעות הדוא"ל: policy@isoc.org.il

בברכה ובכבוד רב,

ד"ר אסף וינר
ראש תחום רגולציה ומדיניות
איגוד האינטרנט הישראלי (ע"ר)

עו"ד יורם הכהן
מנכ"ל
איגוד האינטרנט הישראלי (ע"ר)

העתקים:

הוועד המנהל, איגוד האינטרנט הישראלי (ע"ר).

לירן אבישר בן חורין, המנהלת הכללית, משרד התקשורת.

[3] באיחוד האירופי, הגופים הרגולטוריים האמונים על הגנת סייבר ברשתות תקשורת הם הסוכנות האירופית לאבטחת סייבר (ENISA) ורגולטור לתקשורת אלקטרונית של האיחוד האירופי (BEREC). באנגליה, הרגולציה על היערכות הסייבר נעשית באמצעות שילוב של המרכז הלאומי לביטחון סייבר (NCSC), נציבות המידע (ICO) ומשרד התקשורת הבריטי (OFCOM).