מספר פנימי : 2191953

הכנסת העשרים וארבע

יוזמת: חברת הכנסת מירב בן ארי

פ/3792/24

הצעת חוק איסור פרסום זמני של מתקפת סייבר, התשפ"ב–2022

מטרה

1. מטרת חוק זה לקבוע הוראות בעניין איסור פרסום זמני של מתקפת סייבר, וכן לקבוע מנגנוני דיווח על קיום מתקפת סייבר, וכל זאת על מנת לצמצם, ככל ניתן, פרסום אודות מתקפת סייבר כאמצעי לחץ והבכה לארגון הנפגע וכן על מנת לוודא כי ההתמודדות עם האיום נעשית בצורה מיטבית עבור הארגון הנפגע ועבור פרטיות האזרחים.

הגדרות

2. בחוק זה –

"ארגון" – עסק או כל מי שמספק שירות לציבור, למעט המדינה ורשות מקומית;

"הגורם הממונה" – עובד בכיר במערך הסייבר הלאומי שהוסמך על ידי ראש מערך הסייבר הלאומי לבצע את הפעולות לפי חוק זה או לפיו;

"דיווח ראשוני" – הודעת ממונה האבטחה בארגון, או בעל העסק אם אין ממונה אבטחה כאמור, הכוללת פרטים אודות מתקפת הסייבר ואודות הארגון הנפגע, לרבות פרטים אודות מידע אשר ברשותו;

"דיווח שני" – הודעת ממונה האבטחה בארגון, או בעל העסק אם אין ממונה אבטחה כאמור, הכוללת תיאור מפורט ההתמודדות הארגון עם מתקפת סייבר, לרבות מידע אודות הנזק הנגרם, מערך ההגנה שעמד לרשות הארגון ככל שישנו, זהות התוקף אם ידועה, צפי להמשך המתקפה וכל מידע אחר הרלוונטי לתקיפה;

"חוות דעת" – הודעת מומחה הכוללת פרטים אודות מתקפת סייבר לרבות פרטים אודות זיהוי התוקף (לא ניתן בטח לא בקבועי זמן הללו), לנזקים שהתממשו או שיש חשש כי יתממשו, לדרכי ההתמודדות של הארגון ולצעדים שנקט או שצריך היה לנקוט בטרם התקיפה ובמהלכה;

"מומחה" – מי שמופיע ברשימת מומחים שקבע השר לפי סעיף 7;

"מידע" – נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו, וכן פרטי חשבונות בנק, כרטיסי אשראי, תעודת זהות, דרכון, וכל נתון נוסף שיש במסירתו לאחר כדי להשית נזק על אדם וכן סוד מסחרי כהגדרתו בחוק עוולות מסחריות, התשנ"ט–1999[1];

"מתקפת סייבר" – פעילות שנועדה לפגוע בשימוש במחשב או בחומר מחשב השמור בו, שלא על דרך גרימת היזק פיזי כגון שבירה, ובין היתר:

(1) שיבוש פעולתו התקינה של מחשב או שיבוש השימוש בו, לרבות בדרך של מחיקה שינוי או הדלפת מידע, אחסון או הצגת מידע או פלט כוזב, מניעה או שיבוש הגישה לרשת תקשורת, מתן גישה לגורם שאינה מורשה, וכן חדירה שלא כדין כמשמעותה בחוק המחשבים, התשנ"ה–1995[2];

(2) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר;

"רשימת מומחים" – רשימה שקבע השר;

"השר" – השר לביטחון הפנים.

איסור פרסום אודות מתקפת סייבר

3. לא יפרסם אדם אודות מתקפת הסייבר, מעת התרחשותה של המתקפה ועד חלוף 30 ימים מעת שליחת הדיווח הראשוני כאמור בסעיף 4(א) ולא יפרסם כאמור בתוך 14 ימים מיום דיווח שני כאמור בסעיף 4(ג), אלא ברשות בית משפט שלום.

נוהל דיווח על מתקפת סייבר

4. (א) היה לממונה האבטחה בארגון, או בעל העסק חשד כי מתבצעת נגד הארגון מתקפת סייבר, ידווח דיווח ראשוני בהקדם האפשרי, לקצין בכיר שימנה המפקח הכללי של משטרת ישראל.

(ב) הדיווח יתבצע על גבי טופס ייעודי שיישלח בהודעה אלקטרונית לכתובת ייעודית; השר יקבע הוראות לעניין זה בתקנות.

---

[1] ס"ח התשנ"ט, עמ' 146.
[2] ס"ח התשנ"ד, עמ' 366

(ג) היה ובחלוף הזמן 30 ימים מעת שליחת הדיווח הראשוני סבר מומחה כי הטיפול במתקפה לא הסתיים ידווח הארגון, בהקדם האפשרי, לקצין בכיר שימנה המפקח הכללי של משטרת ישראל דיווח שני, אודות מצב ההתמודדות עם המתקפה ועל הפרטים שנתגלו לו בזמן שחלף, על גבי טופס ייעודי. אל הטופס, תצורף חוות דעתו של מומחה, שתכלול מידע אודות המתקפה לרבות פרטים בעניין המניע למתקפת הסייבר על הארגון הנפגע, השלכותיה וכל מידע בדבר פגיעות אפשריות לארגון.

(ד) היה ובחלוף הזמן כאמור בסעיף (ג2) המתקפה לא הסתיימה, ידווח הארגון למערך הסייבר הלאומי דיווח שני, אודות מצב ההתמודדות עם המתקפה ועל הפרטים שנתגלו לו בזמן שחלף, על גבי טופס ייעודי. אל הטופס, תצורף חוות דעת של מומחה, שתכלול מידע אודות המתקפה, השלכותיה וכל מידע בדבר פגיעות אפשריות לארגון.

(ה) הגורם הממונה רשאי להמליץ בפני הארגון כיצד לפעול, ואף לבצע פעולות לשם שמירת פרטיות, בתיאום עם הארגון.

פנייה לבית משפט שלום

5. (א) חלפו 14 ימים מיום דיווח שני, יוכל הגוף לפנות לבית משפט שלום לבקשת צו איסור פרסום.

(ב) בית המשפט ידון בבקשה, תוך מתן דגש לשאלת היות הפרסום מהווה פרסום אודות מתקפת סייבר כאמצעי לחץ והבכה לארגון הנפגע.

(ג) קבע בית המשפט כי צו איסור פרסום מוצדק, יוציא צו שמשכו לא יעלה על 45 ימים.

(ד) חלפו 45 הימים והמתקפה עודנה נמשכת, רשאי הארגון לבקש מבית משפט שלום צו איסור פרסום שמשכו לא יעלה על 30 ימים נוספים, ולא יינתנו צווים נוספים על צו זה.

זכות ערעור

6. החלטות כאמור בסעיף 5 ניתנות לערעור בתוך שבעה ימים, ובית המשפט שלערעור ידון בערעור בדן יחיד.

רשימת המומחים

7. (א) השר יקבע רשימת מומחים בתחום התגובה המהירה (incident response) למתקפת סייבר (בסעיף זה – רשימת מומחים).

(ב) השר יכליל מומחה ברשימת המומחים אם הוא בעל ניסיון, ידע או אמצעים הדרושים לביצוע הפעולות והבדיקות האמורות ולו לפחות חמש שנות עיסוק בתחום התגובה המהירה (incident response) למתקפת סייבר.

(ג) השר רשאי לקבוע בתקנות, תנאים נוספים להכללת מומחה ברשימת מומחים.

(ד) רשימת המומחים כאמור בסעיף קטן (א) תפורסם באתר האינטרנט של משטרת ישראל.

שמירת הוראות 8. אין בהוראות חוק זה כדי לגרוע מחובות בעניין הודעה ודיווח החלות לפי כל דין.

ענישה 9. (א) המפרסם מידע בניגוד לכללי חוק זה – דינו מאסר שישה חודשים.

(ב) היה והמידע כולל חשיפת פרטים שיש בהם כדי לפגוע באינטרס חיוני – דינו מאסר חמש שנים.

דברי הסבר

בשנים האחרונות חלה אינפלציה דרמטית בתקיפות סייבר ברחבי העולם ובישראל בפרט, בין היתר בשל דיגיטציה מואצת בחסות הקורונה, עבודה מרחוק - הגדלת הפגיעות של חברות, הקריפטו כאמצעי תשלום, מתקפות סייבר שונות על ישראל, לרבות התקפות סייבר של גורמים איסלאמיים, וכיוצא באלו.

אירועי סייבר מונעים משתי מוטיבציות עיקריות: אירוע תודעתי שמטרתו לייצר כאוס והד תקשורתי, או אירוע שמטרתו כופר כסף. התוקפים משתמשים בדרך כלל באחד משלושת מנופי הלחץ: הצפנת קבצים של מערכות מידע וסחיטה לשם השבתם, גניבת מידע וסחיטה כנגד איום פרסום המידע ברבים על מנת לגרור צעדים משפטיים אזרחיים או רגולטוריים ופגיעה במוניטין, ופרסום המידע ברבים על מנת ליצור כאוס ותחושת אי בטחון.

כלי האיום המרכזי של יוזמי אירועי הסייבר הוא התקשורת. ללא פרסומים תקשורתיים, התוקפים אינם מצליחים ליצור את אפקט הכאוס ולגרום לאיום ממשי.

על מנת לסכל את האמצעי המרכזי הזה, הצעת החוק מציעה להסדיר את אופן הטיפול במתקפות סייבר כנגד ארגונים ואת מנגנון הדיווח והפרסום אודותיהן. זאת, בין היתר, באמצעות קביעת איסור פרסום זמני אודות מתקפת סייבר. ההצעה קובעת מנגנונים הכוללים פנייה לבית משפט שלום, כאשר ישנו צורך להרחיב את משך הזמן שבו הפרסום אסור. כמו כן, מוצע להטיל עונשי מאסר על הפרת חוק זה.

הוגשה ליו"ר הכנסת והסגנים
והונחה על שולחן הכנסת ביום
ט"ו באייר התשפ"ב (16.05.2022)