חומר רקע למפגש מקוון (ינואר 2021):

ניהול סיכוני סייבר בסקטור הפיננסי והשירותי על רקע פרשת שירביט והאירועים האחרונים

רקע

בעשור האחרון כפועל יוצא ממהפכת המידע הדיגיטלי אנו עדים למתקפות סייבר על גופים שונים ובכללם גופים עסקיים, בעיקר בסקטור הפיננסי והשירותי. פעולות תקיפה/חדירה למערכות מידע, תקשורת וטכנולוגיה על ידי האקרים לסוגיהם, בין אם הפועלים ברשות עצמם ו/או בחסות גורם אחר, דוגמת מדינה או גורמים פליליים לשם דוגמת סחיטה כלכלית, נזקים תפעוליים, השגת יתרונות עסקיים-מסחריים בדרכים לא-כשרות (גניבת ידע, קניין רוחני) ו/או ריגול למטרות מודיעיניות-ביטחוניות, הפכו לחלק בלתי נפרד משגרת היום-יום של כל מדינה, חברה עסקית ותשתיות ציבור בכל מגזר ותחום.

מגמה זאת עלתה לאחרונה לכותרות בהקשר של פרשת שירביט ואירועים נוספים אך היא אינה חדשה ומציבה כיום בפני חברות רבות אתגר משמעותי. מקרים בולטים שעלו לסדר היום התקשורתי בישראל בשנים האחרונות הם פריצה למערכות לאומי קארד, תקיפת ספקית התוכנה עמיטל דאטה, טאואר סמיקונדוקטור בע"מ ופריצה לשרת אפליקציית Paybox של בנק דיסקונט שבעקבותיה דלף מידע אישי אודות משתמשי האפליקציה. אירוע זה הוביל להגשת תביעות נגד הבנק בסך של 1,377.5 מיליון ש"ח. במגזר הצבאי, תקיפת IDF על ידי החמאס לצורך השגת מידע בטחוני, תקיפת מתקני תשתיות בישראל על ידי האקרים איראניים ועוד.

ככל שהתלות במערכות המידע והטכנולוגיה הופכת למוחלטת (וקריטית), חלון ההזדמנויות העומד לרשות הגורם התוקף הינו בלתי-מוגבל כך שבמצבים רבים עשוי להתקיים נזק משמעותי לאורך זמן ולעיתים אף נזק בלתי-הפיך. הנזק העיקרי הוא אובדן או זליגת נתונים אך בנוסף יכול הארגון לאבד, באופן זמני, יכולת שירות אשר יכולה להוביל לאובדן לקוחות, פגיעה במוניטין וירידה במחיר המניה (בחברות ציבוריות). כאשר נתוני החברה כוללים מידע אישי של הלקוחות, עלולה להתקיים פגיעה בנכסי-המידע האישיים של הלקוח – קרי קניינו הפרטי של הלקוח. ראו **נספח** - חמי פקר ראש מנהלת הסייבר במשרד ראש הממשלה לשעבר.

בשנת 2018 פורסם תזכיר חוק הגנת הסייבר, לעניין הקמת מערך סייבר לאומי אשר יאפשר להגדיר מדיניות ולקדם את היכולת הלאומית במרחב הקיברנטי[1]. מערך הסייבר הינו תולדה של החלטות ממשלה[2], בהן הוחלט לאחד את כל גופי ההגנה הלאומיים לעשייה משותפת בהגנת הסייבר והקמת הרשות הלאומית להגנת הסייבר. למערך מנדט לקבוע דרישות בתחום הגנת הסייבר אשר יחולו על פעילויות משקיות, ככל שאינן מוסדרות בדין אחר ושהן חשופות לסיכוני סייבר משמעותיים. בהתחשב בעובדה כי האסדרה

[1] תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018.

[2] קידום ההיערכות הלאומית להגנת הסייבר

משפיעה על הפעילות המשקית, יש לציין כי התזכיר מציע מודל רגולטורי המשלב בין ההסמכה לפיתוח שיטות ותפיסות הגנה לבין הפעלת שיקול דעת מנהלי ורגולטורי המתבסס על העקרונות המוצגים בחוק, כל זאת על מנת ליצור מסגרת משפטית שתאפשר את הפעלת הסמכויות הללו. יתר על כן, הסמכה זו נועדה להגן על אינטרסים ציבוריים ושמירה על יציבות כלכלית של הפירמות בהתאם לרמות הסיכון השונות של כל פירמה. קדמה למערך הרשות הממלכתית לאבטחת מידע בשב"כ שהוקמה בשנת 2002.

הדיווח על מקרי סייבר בישראל אינו בהכרח אחיד ורשמי ולעיתים קרובות נסמך על מידע תקשורתי. תופעה נוספת היא תקיפת סייבר על שרשראות אספקה, כלומר המתקפה מתבצעת על חברה אחת שהיא ספקית ללקוחותיה וכתוצאה מתקיפה זו נוצרת שרשרת אירועי סייבר. לדוגמה, בחודש דצמבר 2020, ספקית התוכנה עמיטל דאטה הותקפה באופן רחב ובעקבות כך למעלה מ-40 מלקוחותיה נפגעו. חברת אוריין ש.מ בע"מ (לקוחה של חברת עמיטל דאטה) הותקפה גם כן ובעקבות הידיעה בתקשורת, הודיעה אוריין לבורסה על כך שהיא הותקפה אך שמדובר באירוע סייבר ללא השפעה מהותית על תוצאותיה הכספיות. הציבור לא מודע לרוב תקיפות הסייבר שמתרחשות, זאת בשל העובדה שחובת הגילוי תיעשה על ידי חברות ציבוריות רק במצב שמדובר באירוע מהותי, שאר החברות לא חייבות לדווח, הן פשוט מעדיפות לשלם את הסכום המתבקש כדי לשמור על המוניטין ועל אמון הציבור. חלק מהמקרים אכן מדווחים לרשויות אחרות כגון רשות הגנת הפרטיות, רשות שוק ההון, הפיקוח על הבנקים וכדומה, ככל ומדובר במידע רגיש ופרטי, לרוב הדיווח לא יהיה ציבורי.

בשנת 2019, ביצע המפקח על הבנקים[3] סקר בקרב נושאי המשרה הבכירים במערכת הבנקאות בישראל בדבר הסיכונים מנקודת מבטם של הבנקאים. ממצאי הסקר עולה כי הסיכונים המטרידים ביותר (ואף התעצמו ביחס לשנה הקודמת) המצויים במערכת הבנקאית הם סיכון הסייבר וסיכון הטכנולוגיה וההמשכיות העסקית, הנובעים מהמהפכה הטכנולוגית העוברת על כלל תחומי חיינו. ממצא נוסף ומעניין שעולה מן הסקר , גורס כי דרכי ההתמודדות המובילות של הבנקים לגבי סיכון הסייבר הן הגדלת הוצאות האבטחה בתחום טכנולוגיית המידע (כ-90% הסכמה) והטמעת טכנולוגיות חדשות לניטור והגנה (כ-85% הסכמה).

עד כה התקפות הסייבר התמקדו בזליפת מידע ואין עדויות כי בוצעה מניפולציה בכספי הארגונים כך שהפגיעה הפיננסית העיקרית היא תדמיתית (ואובדן שווי המניה בחברות ציבוריות, בעקבות זאת). למרות זאת, מתוקף היותם "מנהלי כספים של אחרים" (Other people's Money), לגופים הפיננסים צורך במנגנון בטיחות נוסף. מנגנון זה הינו נהלים. מערכת טכנולוגית הגנתית אינה יעילה ללא הגדרה, עמידה ואכיפה של מערכת נהלים.

[3] מערכת הבנקאות

השלכות אירוע סייבר

כאשר מתגלה כי ארגון עבר תקיפת סייבר, ההשלכות עלולות להיות משמעותיות. הנזקים הנלווים יכולים להגיע באופן ישיר או עקיף, ועשויים להיות כבדי משקל, כגון: נזקים כלכליים הנובעים מהפסדים שנגרמו לארגון כתוצאה מהפריצה, השבתת פעילות הארגון, נזק משפטי הנובע מחשיפת הארגון לתביעות ייצוגיות וכן תביעות מצד בעלי המניות כנגד הדירקטוריון וההנהלה, גניבת קניין רוחני ו/או קניין פיזי ופגיעה חמורה במוניטין ובאמון הלקוחות. במחקרם של Ablon, Heaton, Lavery & Romanosky[4] שהתבצע בארצות הברית בשנת 2016 ופורסם על ידי התאגיד RAND, רצו לבחון את ההשפעה של הודעה האומרת כי קיים פוטנציאל חשיפה של מידע אישי אודות הלקוח על הישארותו של אותו לקוח בפירמה. הסקר נערך בקרב 64 מיליון בני אדם. ראשית, כ-44% מהנשאלים ענו כי הם קיבלו הודעה כזו בשנה האחרונה. בקרב הנשאלים שפרטיהם האישיים נחשפו, 89% נשארו בפירמה שממנה פרטיהם נחשפו ואילו 11% בלבד עזבו.

במחקרם של Agarwal, Ghosh, Ruan & Zhang[5] בשנת 2020, רצו לבחון את ההשפעה של אירועי סייבר על התנהגות הלקוחות תוך התמקדות בשני מגזרים – המגזר הפיננסי (בנקים) ומגזר הקמעונאות. לפי הממצאים, ההשפעות של אירועי הסייבר קרו רק בטווח הקצר, כלומר ניכר שינוי בהתנהגות הלקוחות לתקופה קצרה. בטווח הארוך נראה כי לא חל שינוי בהתנהגות הלקוחות והאירוע לא גרם לעזיבתם או גרם לקיטון בהכנסות ו/או כניסת לקוחות חדשים.

מן האמור לעיל, ניתן לומר כי לאירועי הסייבר אין השפעה חזקה אם בכלל על התנהגות הלקוחות. במחקרם של Richardson, Smith & Watson[6] בשנת 2019, בחנו את ההשלכות של פריצה למערכות החברה על החברה במספר היבטים. מן הממצאים עולה כי בממוצע ההשלכות הכלכליות על חברות שנפרצו הינן נמוכות, כ-0.3% בחלון הזמן הקצר שבו התקיפה התגלתה. אחת מהשערות המחקר הייתה כי התקפות סייבר משפיעות לרעה על תשואות שוק המניות לטווח קצר וארוך, מבחינה אינטואיטיבית יש היגיון אך ממצאי המחקר מראים כי כאשר ההודעה יוצאת החוצה, מחיר המניה יורד אך לא באופן משמעותי. המחקר מוסיף ומראה כי גם לאחר תקופת זמן מסוימת של מספר חודשים מהיום שבו הודיעו על ההתקפה לא חלה מגמת ירידה במחיר המניה, כלומר, הירידה במחיר מתרחשת רק בימים הראשונים ולאחר מכן המניה חוזרת לעצמה. המחקר בחן 827 אירועי סייבר שהתרחשו למשך תקופה של 15 שנים (כ-417 חברות), ולמעשה החוקרים רצו לבדוק את סוג המידע שנחשף. ב-53% מהמקרים המידע שנחשף היה מידע אישי אודות לקוחות ו-34% היה מידע כספי אודות לקוחות.

[4] Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information
[5] Privacy versus Convenience: Customer Response to Data Breaches of Their Information
[6] Much Ado about Nothing: The (Lack of) Economic Impact

בנוסף, המחקר בחן גם כן את הקשר בין אירועי סייבר לביצועי החברה העתידיים כגון הכנסות ושיעור צמיחה, ROS ו-ROA, הנבדקות הן חברות שהותקפו וכאלה שלא הותקפו, אשר דומות בפעילותן. מן הממצאים עולה כי אין הבדל כה משמעותי במשתנים שנבדקו בין חברה שהותקפה לחברה שלא הותקפה.

הנחיות הרגולציה הפיננסית בישראל

בשנת 2015, פרסם הפיקוח על הבנקים את הוראת ניהול בנקאי תקין[7] שדנה בנושא ניהול הגנת הסייבר בתאגידים הבנקאיים. בין היתר, ההוראה מציגה את האחראיים הממונים על ניהול סיכוני הסייבר בתאגיד (דירקטוריון והנהלה), אסטרטגיית הגנה ומסגרת לניהול סיכוני הסייבר והדיווח לפיקוח על הבנקים במקרה של אירוע סייבר או התרעה על אירוע סייבר. בפרסום זה לא מופיעים פרטים לגבי הדיווח ובאותה שנה פורסם מכתב[8] שבא להסדיר את הוראת הדיווח – למעשה, התווספה הוראה נוספת בעניין "דיווח על אירוע סייבר".

באוגוסט 2016, פרסמה רשות שוק ההון, ביטוח וחסכון חוזר ניהול סיכוני סייבר בגופים מוסדיים[9], המציג את העקרונות לניהול סיכוני סייבר שעל פיהם ארגונים מחויבים לפעול על מנת להתמודד עם הסיכונים הנלווים. בין היתר, החוזר מציג תפקידים ותחומי אחריות, מסגרת ניהול סיכוני הסייבר, ניהול הערכת הסיכונים, ביצוע סקרים וכדומה. על מנת לקבל תמונת מצב ברורה יותר, ביצעה הרשות בחינה של מספר גופים מוסדיים למשך תקופה של שנתיים. במסגרת הבחינה, נעשו מבדקי חדירה שנועדו לבחון את מערכות ההגנה של הארגון, נקודות חולשה ויישום התהליך והפעולות הנלוות. בחודשים מרץ[10] ויולי[11] 2018, פורסמו חוזרים נוספים המתארים את המסקנות שעולות לאחר ביצוע המבדקים, תוך התייחסות לסוג הסיכון והמלצות לגביו. מן הממצאים עולה כי מרבית הגופים אכן מודעים לחשיבות העניין, אך עדיין טעון שיפור וחיזוק מערך הסייבר בארגון.

בחודש אוקטובר 2020, פרסמה רשות שוק ההון מכתב הפונה למנהלי חברות הביטוח בדבר מיפוי סיכוני סייבר בפעילות הביטוחית[12]. מטרת המכתב היא להדגיש את חשיבות ניהול סיכוני הסייבר בפעילות הביטוחית לצורך שיפור ניהול הסיכונים של החברות בתחום זה. כמו כן, נדרש לבצע סקר בחברות הביטוח לזיהוי וכימות חשיפת החברה לסיכוני הסייבר ולדווח על הממצאים לדירקטוריון.

---

[7] ניהול הגנת הסייבר
[8] הוראות הדיווח לפיקוח
[9] ניהול סיכוני סייבר בגופים מוסדיים
[10] טיוטת עמדת ממונה: סיכום ממצאי ביקורת סייבר
[11] עמדת ממונה: סיכום ממצאי ביקורת סייבר
[12] מיפוי סיכוני סייבר בפעילות הביטוחית - טיוטה

בהתאם לעמדה משפטית מספר 105-33 בעניין גילוי בנושא סייבר[13] שפורסמה על ידי הרשות לניירות ערך, ישות לא חייבת לתת גילוי בדבר סיכוני הסייבר הכלליים הקיימים, זאת מאחר ומטרת הדיווח הכספי היא מתן מידע רלוונטי למשקיעים ובמצבים מסוימים גילוי כללי זה עלול להקשות על הבנת הסיכון. יש לציין כי הגילוי כפוף למבחני המהותיות הרלוונטיים. על מנת לקבל תמונת מצב רלוונטיות בדבר חשיפת החברה לסיכון הסייבר, יש לבחון מספר גורמים ביניהם: התרחשות תקיפות סייבר קודמות לרבות חומרתן ותדירותן, ההסתברות להתרחשות תקיפות סייבר, אפקטיביות יכולות התאגיד למנוע או להקטין את החשיפה לסיכוני סייבר, היבטים עסקיים של התאגיד ופעילותו, היוצרים סיכונים מהותיים בתחום הסייבר, והעלויות וההשלכות הפוטנציאליות של סיכונים אלה, לרבות סיכונים ספציפיים לתחום פעילותו וסיכונים של ספקי שירות וצדדים שלישיים אחרים עימם התאגיד בא במגע, המשאבים הכרוכים בשמירה על הגנות סייבר לרבות קיומו של כיסוי ביטוחי המתייחס לתקיפות סייבר, הפוטנציאל לפגיעה בנכסים ובכללם קניין רוחני ומוניטין, וכן עוצמת הפגיעה האפשרית ביתרונות תחרותיים שיש לתאגיד, חוקים ותקנות קיימים או תלויים ועומדים, אשר עשויים להשפיע על העלויות הנלוות לתאגיד בקשר עם אותה רגולציה. כמו כן, ככל וחשיפת התאגיד לסיכוני סייבר הפכה למהותית יותר להבנת הפעילות או שחל אירוע סייבר בעל השפעה מהותית על סעיפי הדוחות, יש לתת ביטוי לכך בדו"ח הדירקטוריון.

מכוח תקנה 36(א) בדבר אירוע או עניין החורגים מעסקי התאגיד הרגילים, על התאגיד לבחון את מהותיות האירוע לצורך דיווח לציבור וככל ושקלול הנזקים עולה לכדי מהותי, יש לפרסם זאת מכוח התקנה. התקנה מפורטים אירועים בתחום הסייבר, שבמידה והם מתקיימים הדבר עשוי לחייב פרסום דיווח מידי. לדוגמה, פעילותו העסקית של התאגיד הופסקה לפרק זמן, מאגרי מידע חיוניים נפרצו, התאגיד נדרש לשלם כופר בסכום מהותי בעקבות תקיפת סייבר וכך הלאה. יתרה מכך, יש לתת ביטוי לתיאור האירוע והשלכותיו.

[13] עמדה משפטית מספר 105-33 : גילוי בנושא סייבר

שאלות לדיון

1. עד כמה הבעיה היא מהותית כפי שמשתקף מחומר הרקע שלפניכם או שולית כפי שמראים לכאורה מחקרי המימון?
2. האם לאור הקשר ההדוק בין גופים פיננסיים התקפה על אחד היא בעצם רוחבית על כל המערכת?
3. מהי הפגיעה בלקוח להוציא פרטים אישיים? הרי הוא לכאורה מוגן נגד מניפולציות ואולי הדבר מסביר את ההשפעה המתונה? האם יש יתרון לבנקים והאם התגלו נסיונות למניפולציה בחשבונות כגון העברת יתרות?
4. האם סיכון הסייבר יוצר מחסום לדיגיטציה מהירה, שהרי בהיבט זה הסייבר הוא של "נוגדן" דיגיטציה?
5. האם היבטי החקיקה והרגולציה הנוכחיים למול גופים פיננסיים במדינת-ישראל מספקים ומשקפים מענים מקצועיים מספקים למול האיומים/סיכונים?
6. האם הרגולציה לסוגיה ניתנת לבקרה ואכיפה? האם הבקרה רלוונטית לקצב השינויים הארגוניים?
7. מהו מרחב ומידת האחריות של הגופים הרגולטוריים במקרה של נזק כתוצאה מהתממשות האיומים? האם לגופים הרגולטוריים קיים סל כלים מספק לגיבוש ההנחיות?
8. האם אימוץ תקינה וולונטרית על ידי חברות, כדוגמת תקן ISO27001 (תקן שפורסם על ידי ארגון התקינה הבינלאומי ISO והנציבות הבינלאומית לאלקטרוטכניקה IEC בשנת 2005 ושודרג ועודכן לאחר מכן) שלמעשה נועד לשיפור רמת אבטחת המידע של גופים שיבחרו להשתמש בו, מספק?
9. האם קיים ארביטראז' רגולטורי בהיבט הסייבר – למשל, האם הדרישות החלות על גופים בנקאיים נוקשות יותר מאלה החלות על חברות ביטוח, בתי השקעות וגופי אשראי חוץ בנקאי?
10. כיצד יש לתמחר את הסיכון – למשל צורכי חיתום בביטוח?
11. באשר לעניין הגילוי – כיצד נמדדת מהותיות מבחינה איכותית והאם הניסוח הקיים לא מוביל לכך שמרבית אירועי התקיפה אינם מדווחים?
12. שרשרת אספקה – כיצד לנהל את הסיכון הנובע משרשרת אספקה והאם צריכה להיות חובת דיווח לספקים?
13. לאור פוטנציאל הנזק המשמעותי, האם יש להכיל על דירקטוריוני החברות חבות נוספת לממש אחריותם/סמכותם בכל הקשור לעמידת חברה במדיניות האבטחה?
14. האם יש לחייב ברגולציה, הקצאת מסגרת תקציבית קבועה/שנתית (מסך תקציב הארגון) למימוש משאבים לטובת מעני אבטחה? (כ"א מקצועי, בקרה, הסברה, הדרכה, רכש והטמעת אמצעים)
15. מנגנוני פיצוי מובנים לציבור כחלק מהרגולציה – האם יש לקבוע קווים מנחים?
16. האם קיימים מודלים גלובליים מוצלחים לצמצום האיומים שהוטמעו בשוק הפיננסי, שעל מדינת-ישראל לאמץ?
17. האם תפיסת ומערכי האבטחה המוטמעים בגופים/ארגונים כיום, רלוונטית ליכולות התקיפה הגבוהות והתפתחות או שנדרש שינוי תפיסתי מהיסוד? האם ניתן להדביק את הפערים?

18. אחריות לאומית – במצב של תקיפת חברה ו/או גופים משמעותיים במגזר הפיננסי – האם קיים או נדרש גורם בעל אחריות לאומית למעקב ובדיקת התמונה המערכתית לוודא שאין סוגיה פיננסית מתפתחת שיכולה להוות כשל לאומי מתמשך?
19. שאלה משפטית – האם לקוח של גוף שהותקף יכולה לתבוע את הגוף?
20. מידת האחריות של מדינת-ישראל – האם נדרשת הכלה של אחריות ואכוונת המדינה (מערך הסייבר הלאומי), בכל מצב בו קיים פוטנציאל פגיעה למידע אישי של הציבור או לפגיעה כלכלית מתמשכת בנכסי מדינה?
21. כיצד מייצרים הרתעה של תוקפי הסייבר ומגנים על הקורבנות?