התמודדות עם אירועים סייבר

א. הקדמה

האירוע בו תעסוק העבודה הינו פריצה לנתוני האשראי של לקוחות אקוויפקס, חברת ענק לדירוג אשראי בארה"ב. בחברה זו רשומים מעל 800 מיליון לקוחות פרטיים ומעל 80 מיליון עסקים בארה"ב וגם ברחבי העולם (אוסטרליה, אנגליה ועוד). מדובר בחברה שבידיה יש את מאגר הנתונים השלישי בגודלו בארצות הברית (שירות גלובס, 2017). חברה זו למעשה אוספת נתונים על הלקוחות ופעולותיהם וכך מדרגת את יכולת החזרת ההלוואה שלהם, מסייעת להם לקחת הלוואה, מספקת פיקוח על האשראי ומספקת שירותי מניעת זיוף והונאות באשראי. ברור, כי בידי החברה היה מידע מאד רגיש על הלקוחות שלה: שמות, תעודות זהות, מספרי ביטוח לאומי, טלפונים וכדומה. הלקוחות סמכו על החברה שתגן על פרטיותם אך אליה וקוץ בה – החברה הודיעה בספטמבר 2017 על פריצה למאגרי הנתונים שלה על הלקוחות, שבה נתונים של 145 מיליון לקוחות הועתקו לידי הפורצים. אולם הפריצה לא אירעה בבת אחת וגם לא בספטמבר, אלא בהדרגה ממאי עד יולי. הפורצים הצליחו לחדור עקב רשלנות החברה (לא עדכנה את תוכנת האבטחה של אפאצ'י סטראוט למרות שנתבקשה לעדכן ולא ערכה ניטור של הפריצות למרות שהעברת הנתונים הורגשה במערך אבטחת המידע). כיום, אקוויפקס עדיין מתמודדת עם תביעות, החזרים כספיים ללקוחות ושיקום מערך אבטחת המידע שלה. בסך הכול מעריכים כי הפריצה עלתה לחברה, מ-2017 ועד כה, 1.7 ביליוני דולרים. החשודים העיקריים בפריצה: חיילי צבא סין (Lane, 2020; Symanovich, 2020).

ב. סקירת ספרות

1. **חוסן ארגוני:** ארגונים יכולים לבנות לעצמם שני סוגי חוסן אשר יגנו עליהם מפני מתקפות סייבר. האחד, הוא חוסן אסטרטגי. חוסן זה מתמקד בהגנה של הארגון מפני מתקפות ואיומים בעלי מורכבות גבוהה והתפתחות איטית. מנגד ישנו חוסן שני, מסוג אופרטיבי, שפירושו התכוננות של הארגונים לאירועי סייבר מפתיעים, חריגים, מהירים ועוצמתיים (Goldman, 2010). בהקשר של הפריצה לאקוויפקס, הפריצה לא הייתה "ברבור שחור" (אירוע מפתיע ורב עוצמה) שכן פריצות לנתוני לקוחות רגישים בחברות ענק אמריקאיות כבר מוכרים עוד ממקרי טרגט והום דיפו שחלו בשנים 2013-2014 (Roman, 2014), ואף הפריצה לאקוויפקס התרחשה בתסריט המוכר מהמקרים לעיל – יש פירצה מסוימת באבטחת המידע שקל היה למנוע, הפורצים שואבים את הנתונים הרגישים במשך זמן מה עד שהחברה מאתרת אותם, וגם אז לוקח עוד קצת זמן עד שהחברה פונה אל הציבור ומיידעת על הפריצה. לכן ניתן לומר שמה שהיה חסר לאקוויפקס זה בניית חוסן אסטרטגי ולאו דווקא אופרטיבי. אכן, לחברה לא הייתה מדיניות ברורה לגבי אבטחת המידע, היא לא השתדלה לעדכן את תוכנת החברה חרף בקשות חברת תוכנת האבטחה לעדכן כי יש פירצה, לא הייתה מחלקת אבטחת מידע שכפופה ישירות למנכ"ל ועוד (Newman, 2014). את החוסן האסטרטגי, כמו גם האופרטיבי, ניתן לבנות במגוון דרכים אינטגרטיביות – העסקת מאבטחי מידע מיומנים, קביעת מדיניות ברורה לכל העובדים לגבי אבטחת מידע, מעורבות ההנהלה הבכירה בנושא הסייבר, עריכת ויישום פרוטוקול שיגרתי לניטור, איתור וחשיפת איומים, הענקת סדר עדיפות גבוה לעדכון תוכנות הסייבר ועוד (Goldman, 2010).

2. **מחזור החיים של משבר הסייבר**: לפי סיבוני וקליין (2018א) ישנם מספר שלבים להתמודדות עם משבר סייבר, אשר גם מהווים את מחזור החיים של משבר הסייבר כאשר רמות הלחץ מטפסות עד שלב ההכרעה ולאחריו יורדות לרמת הבסיס. השלבים לפי סדרם הכרונולוגי הם כך: שלב הזיהוי - בירור ראשוני לגבי קיומו של אירוע סייבר; שלב ניתוח - בירור מקיף ומעמיק ככל הניתן, ועל בסיס הניתוח מקבלים החלטה כיצד לפעול לשם בלימת התקיפה; שלב ההכלה - השגת שליטה ראשונית באירוע לשם הכלתו ולשם עצירת החמרתו; הכרעה - נטרול האירוע תוך ניסיון למזער ככל הניתן את הנזק שגרם; שלב ההשבה - חזרת הארגון לפעילות תקינה ומלאה. אם נבחן לפי שלבים אלו את המקרה של אקוויפקס, הרי שהחברה כשלה כבר בשלב הזיהוי: במשך חודשיים (מאי עד יולי 2017) בכלל לא שמה לב שיש לה גניבת נתונים. לפי סיבוני וקליין (2018א) לשם התמודדות עם השלב הראשון נדרשת שגרה של פעולות שוטפות להפחתת היתכנות המשבר ולהגברת המוכנות אליו. אקוויפקס לא רק שלא קיימה שגרה מוצלחת של בקרה על אירועי סייבר אפשריים אלא גם התרשלה בעדכון תוכנת הניהול של הנתונים, חרף כך שהחברה המפתחת של התוכנה ביקשה ממנה בחומרה לעדכן כי יש פירצה מסוימת – ואכן הפורצים פרצו דרך פירצה זו.

3. **המשכיות עסקית:** אחד מהאתגרים בניהול משבר סייבר הינו המשכיות עסקית, שהיא היכולת של הארגון לשמור על פעילות רציפה, שוטפת ושגרתית גם במהלך משבר, או לכל הפחות למזער את הזמן עד לשוב הארגון לעבודה תקינה. אימוץ גישה של ניהול סיכונים בתחום הסייבר יכולה לסייע לשמירת ההמשכיות העסקית שכן כך מתכוננים מראש למשבר דרך גיבוש נייר מדיניות אסטרטגי להתמודדות בעת משבר וכן מבצעים פעילות שגרתית לצמצום סיכוני הסייבר ע"י פיקוח ובקרה (סיבוני וקליין, 2018). במקרה של אקוויפקס, ההמשכיות העסקית נפגעה לזמן מה ונדרש להם זמן להשתקם, וניתן לייחס זאת לכך שלא הייתה מדיניות ניהול סיכונים תקינה, ברורה ומבוקרת.

ג. התפתחות האירוע

במהלך מרץ 2017 חברת אקוויפקס מתבקשת על ידי חברת תוכנת ניהול הנתונים, אפאצ'י סטראט, לעדכן את התוכנה כי נתגלתה בה פירצה שעלולה לסכן את המידע הרגיש המוכל בנתונים. העובדים של אקוויפקס מנסים לעדכן, לא מצליחים, ועוזבים את הנושא (Newman, 2017). באמצע מאי 2017 האקרים מצליחים לפרוץ לנתוני אקוויפקס דרך אותה פירצה שמוזכרת לעיל. הם מושכים את הנתונים הרגישים של הלקוחות של אקוויפקס (שמות, מספרי טלפון, מספרי כרטיס אשראי, תעודה מזהה, מספר ביטוח לאומי, רשיון הנהיגה, תאריכי לידה, כתובות ועוד) מרחבי העולם אל מחשביהם. החברה לא שמה לב לכך שיש פעילות חשודה (שירות גלובס, Symanovich, 2020;2017). רק באמצע יולי 2017 מתעורר חשדה של החברה שמתעסקים בנתוניה. היא בולמת את משיכת הנתונים, אך במידה מסוימת, נותר נזק שנעשה ואין להשיבו: נתונים של כ-148 מיליון לקוחות כבר הודלפו (Lane, 2020; Symanovich, 2020). החברה הצליחה לשמור על סודיות מסוימת בנוגע לדליפה עד לספטמבר 2017 אז יצאה בהודעה לתקשורת ודיווחה על הדליפה. אך ההודעה הייתה עמומה, לקוחות החברה לא הבינו מי נפגע ומי לא, למה החברה לא הודיעה להם במשך חודשיים על הפריצה, איך היא לא גילתה את הפריצה אלא רק ביולי ועוד שאלות. הייתה סערה גדולה בציבור סביב הנושא שלא ניתן להגיד שהיא שככה לחלוטין עד היום. החברה הקימה ללקוחות אתר שבו ניתן לבדוק אם הם נפגעו מהתקיפה ואם כן קיבלו פיצוי מסוים בגובה של 125 דולר או שירותי ניטור אשראי בחינם וגם החזר נוסף של הפסדים בגין הפריצה אם הלקוח הצליח לתעד אותם (שירות גלובס, 2017; Newman, 2019).

היו גם חילופי האשמות בין אקוויפקס לבין אפאצ'י. אקוויפקס טענו שאפאצ'י אשמה כי אצלה הייתה הפירצה, אך נתונים שנתגלו ומעידים כי אפאצ'י פנתה לאוויפקס בבקשה לעדכן בעוד שאקוויפקס התרשלה בנושא זה, מטילים את האשמה על אקוויפקס בלבד ולא על אפאצ'י (Newman, 2017). בכל מקרה, מאז ועד היום, החברה עדיין מתמודדת עם נזקי המשבר, שעלותם כבר הצטברה ל-1.7 ביליון דולר והיא נחלקת בין פיצויים ללקוחות, תביעות ייצוגיות ושיקום מערך