פורום שווי הוגן - Fair Value Forum - FVF

סיכום דיון

מסמך זה מהווה את תמצית הדיונים של "פורום שווי הוגן" מתוך מטרה לשתף את הקהל הרחב בעיקרי הדברים. בקריאת המסמך יש להביא בחשבון שמדובר בתמצית הדיון ולא בפרוטוקול מלא. בהתאם למדיניות הפורום, הדברים מובאים שלא בהכרח בציון שמות כל הדוברים. יודגש כי הדברים מייצגים את עמדותיהם האישיות והמקצועיות של חברי הפורום ואינם מייצגים בהכרח את העמדות הרשמיות של הגופים אליהם הם משתייכים.

תאריך המפגש: 04.01.2021

נושא המפגש: "ניהול סיכוני סייבר בסקטור הפיננסי והשירותי על רקע פרשת שירביט והאירועים האחרונים".

חומר רקע למפגש: לחומר הרקע – לחץ כאן

אורחים שנכחו בדיון: לרשימת המשתתפים – לחץ כאן

צוות מקצועי: יואב אטיאס, מיכל ברק, ניב אלמוג, עדן בוכריס

שלומי שוב

בחרנו לעסוק הבוקר בנושא ניהול סיכוני הסייבר – זה לא נושא טריוויאלי לפורום שלנו שהוא פיננסי במהותו – אבל הגענו למסקנה שלמרות שמדובר בסיכון תפעולי – החשיבות שלו וההשלכות הפוטנציאליות רבות הממדים מגיעים לכדי כך שראוי שנדון בו. הטריגר לדיון הוא אמנם המקרים האחרונים לרבות שירביט – אבל חשוב להדגיש כי זהו לא נושא חדש. סיכוני הסייבר התפתחו בזירה העסקית באופן משמעותי מזה לפחות עשור עם המהפכה הדיגיטלית והם ילוו אותנו ביתר שאת ככל שהדיגיטציה תואץ וזה כנראה יקרה. אגב, בעקבות משבר הקורונה חווינו האצה מהירה של הדיגיטציה שניתן להניח שהגבירה את עוצמת הבעיה ואולי גם עוד לא הכל נחשף.

אין ספק שיחד עם שיפור ההגנות גם התוקפים משתכללים ככל שחולף הזמן ולכן זוהי מסוג החשיפות שלא תהיה להן כנראה אף פעם סגירה הרמטית ועל כן הדיון שלנו הוא במישור של ניהול הסיכון. אגב, הקושי המיוחד עם הנושא הזה הוא שלמנהלי הסיכונים באופן טבעי ולהבדיל אולי מסיכונים אחרים, יש פחות מומחיות מקצועית בתחום מאשר למשל במחלקות מערכות המידע ולכן יש קושי מובנה בניהול הסיכון הלא סטאטי הזה שתכופות משנה את פניו. כשמנהל סיכון נמצא בנקודת נחיתות מבחינת מומחיות לגבי סיכון מסוים זה תמיד יותר מאתגר.

אנחנו רגילים לייחס את הסיכון לגופים הפיננסיים – בין היתר לאור האירועים האחרונים, אך זה נובע מהעובדה שהדיגיטציה בגופים אלה שהם נותני שירותים במהותם מפותחת יחסית. אבל סיכון הסייבר הרבה יותר רחב והוא נוגע לכלל הגופים במשק – המשוואה מאד פשוטה: ככל שהדיגיטציה מתגברת - כל ענף כמובן בקצב שלו, הרי שגם הסיכון גדל. תסתכלו למשל כיום על רשתות קמעונאיות, קופות חולים ואפילו האוניברסיטאות שחטפו את ה"כאפה" של המשבר ועברו בבת אחת לדיגיטל – בקיצור בעיקר המגזר השירותי.

גם אם מסתכלים על האירועים האחרונים בסקטור הפיננסי יש כאן מצב מוזר שלכאורה לשלושת הרגולטורים הפיננסיים (ואולי גם נוסיף להם בהקשר של הסייבר גם את הרשות להגנת הפרטיות) יש את הסמכות ופחות את הידע והם מתרכזים בעיקר בדיווחים ודווקא למערך הסייבר הלאומי שיש את הידע והיכולת לעזור אין את הסמכות. גם עצם העובדה שכל רגולטור מוציא את ההוראות שלו בנפרד והן לא בהכרח אחידות היא מוזרה – הסתכלנו למשל לקראת הדיון על הגדרת אירוע סייבר בהוראות של המפקח על הבנקים ובהוראות רשות שוק ההון – שהם שני הרגולטורים הראשיים בתחום - ההגדרה לא זהה כך שיכול להיות מצב דברים שבו אירוע סייבר יוגדר כך למשל במערכת הבנקאית אבל לא בביטוח.

יש לשים לב שלרשות ניע – הרגולטור הפיננסי השלישי יש כאן שני כובעים – אחד כאחראית על הדיווחים של כלל החברות המדווחות והשני כמפקחת על קרנות הנאמנות ועל מנהלי התיקים (אגב, שיכולים להיות מאד קטנים ולכן לסבול מחסרון לגודל שיכול להיות מאד בעייתי בהקשר של הסייבר ולכן להציב אתגר לא פשוט).

עסקנו השנה בפורום בבעייתיות שנובעת מחוסר התאום והחפיפות בין שלושת הרגולטורים הפיננסיים בישראל – תחשבו למשל על בית השקעות שיש לו כמה רגולטורים – ובד"כ המחלקה שאחראית על הסייבר נמצאת למעלה אז היא צריכה לעמוד בכמה רגולציות. אגב, אני חושש מאותם מצבים שבהם לכאורה יש כפל רגולציה – לעיתים קורה בדיוק הפוך ונוצר וואקום כי כל רגולטור סומך על השני. מעבר לכך שיש כאן פוטנציאל לשונות במוכנות לסייבר בין גופים שונים בתוך הסקטור הפיננסי, המצב האידיאלי הוא שיהיה גוף אחד שלפי כללים אחידים יקבע את ההנחיות מצד אחד ויקבל את הדיווחים מהצד השני. מה שכן טוב יהיה אם ניקח את אירוע שירביט – שזה אירוע מתקפה על אמת כאירוע תירגול טוב לצורך תיאום רגולטורי – אני מבין שהיה תיאום בין כלל הרגולטורים במקרה זה וזה חשוב ואולי גם צריך לחשוב על שינוי מבני בנושא כהפקת לקחים.

נושא הדיווח למשקיעים על אירוע סייבר הוא לא טריוויאלי בכלל, במיוחד על רקע סף המהותיות שדורש הפעלת שיקול דעת והאינטרס הברור של המנהלים לא לדווח על מידע רגיש כזה. ההערכות הן ועשיתי לא מעט שיחות עם מומחים לקראת הדיון שהרוב המוחלט של האירועים לא מדווחים למשקיעים – ולפי מיטב הבנתי גם לא לרגולטורים הפיננסיים (אני לא מכליל כאן את הרשות להגנת

פרטיות). וזה גם מעבר לשאלת ההגדרה של אירוע סייבר שגם היא אינה טריוויאלית. המקרים הספורים שאנחנו כן רואים הם בדרך כלל אלה שכבר הגיעו לתקשורת בדרך כזאת או אחרת – בד"כ על ידי לקוחות או צדדים שלישיים ופחות מיישום חובות דיווח. מה שמטריד אותי שאין עקביות בגילוי – יש כמה מקרים ספורדיים שעלו כמו בזמנו לאומי קארד וכעת שירביט. בדוח התקופתי השנתי אנחנו רואים בעיקר דיווח גנרי בסגנון המוכר של לצאת ידי חובה.

מבחינה חשבונאית, מבחן המהותיות הוא אחד ממבחני שיקול הדעת שהם תמיד יותר קשים כאשר יש כל כך הרבה רגישות ואינטרסים סביב המסקנה שלהם. הקביעה של מהותיות כאן צריכה להתבצע לפי גודל הפריצה ופוטנציאל הנזק שהפריצה מעידה עליו. חשוב לי כאיש חשבונאות להדגיש לכם - זה שחברה שילמה כופר בסכום לא מהותי לא מעיד על כך שזהו מידע לא מהותי. תחשבו לדוגמה על תשלום כופר של חצי מיליון שקל של תאגיד גדול – ככל הנראה לא מדובר בסכום מהותי – אבל אי אפשר להגיד שבהכרח זה לא מהותי לאור ההיבט האיכותי. הרי בעצם זה שהחברה היתה חשופה לפגיעה יכולות להיות משמעויות רבות קדימה. אגב, אני נותן את הדוגמה הזאת בד"כ לסטודנטים שלי בקורס תיאוריה חשבונאית כדי להמחיש להם מקרים מהותיים מבחינה איכותית אך לא כמותית. הבעיה היא שבמצב הדברים הנוכחי היכולת של רשות ניע לאכוף ולוודא שמידע שצריך להגיע למשקיעים אכן מגיע אליהם היא מאד מוגבלת, בלשון המעטה.

בשורה התחתונה יש כאן גם סתירה פנימית צורמת - הרי ככל שלא מדובר במידע מהותי למשקיעים אז מדוע אנחנו עוסקים בנושא הזה היום ומדוע כל כך הרבה אנשים רציניים התאספו לדיון הזה? כפי שציינו בחומר הרקע המחקרים מעידים על השפעה לא מהותית על מחיר המניה של דיווח על אירועי סייבר – אבל כנראה שמה עומד מאחורי זה הוא שדווקא האירועים הלא מהותיים הם אלה שמדווחים. פרופ' אלי אמיר, ד"ר שי לוי וצפריר ליבנה מאוני' תל אביב הראו את זה במחקר שלהם דרך הממצא לפיו דווקא כאשר הגילוי נובע מהדלפה ולא מיוזמת החברה ההשלכות שלו על מחיר המניה משמעותיות. המקרה של הסייבר הוא דוגמה חדה שממחישה לדעתי בעיה רחבה יותר בדיווחי חברות בשוק ההון. חברות אוהבות לדווח ארוכות על מה שפחות חשוב ולגבי הדברים החשובים באמת מנסים בדרך כזאת או אחרת לצאת ידי חובה דרך ניסוחים גנריים. דוגמה שממחישה זאת היטב היא המקרה המוכר של יאהו שב- 2016 באיחור של שנתיים-שלוש נאלצה להודות, בעקבות זה שכ- 200 מיליון שמות חשבון, מיילים וסיסמאות הוצעו למכירה בדארק-נט, וזה קרה ערב הקלוזינג של עסקת הרכישה שלה - מה שהוביל להתאמת המחיר מטה בכ- 8%.

בכל הנושא הזה של מרחב הסייבר יש לא מעט היבטי מאקרו לרבות למשל בהקשר של התחרות במגזר הפיננסי וכניסת חברות פינטק חדשות. עולות כאן גם שאלות ברמה הלאומית שהרי יש כאן גם ענייני טרור ועולה שאלה מה תפקיד המדינה בהגנה על המגזר העסקי – כי אם במקרה של שירביט זאת התקפת טרור מה ההבדל בין זה לבין הגנה של המדינה עלינו מהתקפות טילים למשל? כלומר, ראוי

לשאול היום בדיון מדוע המדינה והרגולטורים לא עוברים למודל של הגנה מצרפית? מצד שני צריך גם להגיד שעולות כאן גם שאלות בנגע להגבלים עסקיים ולא פחות מכך שאלות כבדות משקל בנוגע ליכולת של המדינה להתערב בעסקים, כפי שעלה בזמנו בעקבות פרסום המזכר של חוק הסייבר ב-2018 – אגב חקיקה שלא התקדמה מאז.

צריך להבחין בין דיווח למשקיעים לבין דיווח לרגולטור או לא פחות חשוב ואף אולי יותר הוא שיתוף המידע בין הגופים הפיננסים לבין עצמם ובין הגופים לבין הספקים שלהם. ממש לאחרונה ראינו את המקרה של עמיטל שהיא חברת תוכנה המשווקת תוכנות לחברות העוסקות בעמילות מכס שהתמודדה עם מתקפת סייבר ובעקבות כאן נפגעו גם הלקוחות שלה – חברות עמילות מכס כמו אוריין חברה ציבורית שדיווחה גם היא על מתקפה.

כפורום שנקרא שווי הוגן חשוב לנו היום גם לנסות לתרגם את הסיכון התפעולי לערכים כספיים ולכן תהליך החיתום הביטוחי מאד מעניין אותנו. בגדול, הפוליסות נועדות לבטח הן את החברה הנתקפת והן את הלקוחות הנפגעים אבל נשאלת השאלה, כיצד ביטוחי הסייבר מתומחרים? כמובן שבתמחור הביטוח נלקחים בחשבון גורמים רבים הן במישור של מידת החשיפה והן במישור המוכנות של החברה, אבל הכימות הזה לא טריוויאלי בין היתר לאור העובדה שהתחום כל הזמן מתפתח וקשה להסיק לאור נתוני העבר כמו שקורה בד"כ בתחומים אחרים. אנחנו נעסוק בדיון גם בכך ובמתודולוגיות אפשריות. בכל מקרה, ממה שאני מבין הפוליסות משפות לגבי הוצאות יעוץ בעת משבר להגנה על המוניטין ועל אובדן ההכנסות לתקופת השיפוי אבל אינן מכסות נזק פוטנציאלי לשווי המוניטין של החברה הנפגעת - וזאת נקודה חשובה שגם נרצה לדבר עליה היום. שאלת הנזק למוניטין היא לא טריוויאלית.

הסתכלתי קצת לקראת הדיון על הדוחות השנתיים של הסקטור הפיננסי ל- 2019 וראיתי שחמשת הבנקים, למעט דיסקונט מגדירים את רמת החומרה של סיכון הסייבר כבינונית ולא כגבוהה. אגב, גם ישראכרט מגדירה זאת כבינונית. מנגד, חלק מחברות ביטוח מגדירות אותו כגבוה. כך למשל, מגדל מסווגת את סיכון הסייבר כהשפעה גבוהה בעוד כלל ביטוח כהשפעה בינונית. מעניין להשוות בין הביטוח לבנקים עד כמה זה נובע מפערים ברמת המוכנות שהרי התפיסה היא שהבנקים מוכנים יותר אבל יתכן שזה נובע גם מפוטנציאל הנזק ביחס לעוצמת ההון. בבנקים עשו לפני כשנה תרחיש קיצון לאירוע סייבר וממה שאני מבין לא התגלתה השפעה משמעותית על הרווח – עוד מעט נשמע מדני חחיאשווילי סגן המפקח שנמצא איתנו על כך. יהיה מעניין לראות את ההתפתחויות בנושא בקרוב והאם נראה עליה במדרגות הסיכון של הסייבר בדוחות הקרובים.

אין ספק שהמודעות בגופים הפיננסיים לסיכון הסייבר היא גבוהה יותר וכפועל יוצא גם רמת המוגנות שלהם גבוהה יותר, אבל זה כאמור משליך גם על יתר החברות במשק. אגב, שימו לב שחברות הביטוח יכול להיפגע גם בעוד מישור – המחויבות שנגזרת מפוליסות ביטוח שהן מנפיקות דווקא לא בתחום

הסייבר – לא בהכרח שניתן יהיה להחריג את הסייבר מנזקים אחרים שנגרמו – אפילו תקיפות שתוצאתן נזקים פיזיים – ואנחנו היינו עדים לאחרונה לכל מיני התפתחויות בנושא.

זה מתחבר לנושא של אחריות דירקטורים ומנהלים – אין ספק שהתהליך הביטוחי מסייע מאד להגנה, אבל הוא כמובן לא ממצה את הסיכון והאחריות, אבל מהווה נקודת מוצא טובה. התפקיד של הדירקטוריון הוא קודם כל ניהול הסיכון וצמצומו אבל גם כמובן במקרה של תקיפה – כפי שראינו באירועים האחרונים. נמצאים פה נציגים הבכירים בנושא של הרגולטורים הפיננסיים ומנהלי הסיכונים בכל הגופים הפיננסיים המובילים בישראל. זה ברור שלגבי גופים חיוניים/קריטיים גם בסקטור הפיננסי כמו הבורסה לניע המדינה מעורבת אבל אנחנו רוצים דווקא לדבר היום על כלל החברות שאינן גופים קריטיים או ציבוריים - לרבות מהמגזר הפיננסי.

אנחנו נשמע עוד מעט את הרגולטורים השונים. ממה שאני מבין מערך הסייבר אוסף נתונים על האירועים השונים ונשמח לשמוע בהמשך ממיטל אריק ממערך הסייבר על המגמה של האירועים בראיית מאקרו - שאני מניח שנמצאת במגמת עליה בשנים האחרונות. בכל מקרה אני חושב שראוי להסדיר את נושא הסייבר ברמה משקית.

אמיר ברנע

כמה הערות קצרות אחרי הדברים האלה. אין ויכוח לדעתי על פוטנציאל הנזק שיכול להיגרם מפריצות סייבר. במקביל אין חולק שהדיגיטציה או מגמת הדיגיטציה מגבירה את סיכון פריצות סייבר. אפשר גם להוסיף את הרצון לעודד תחרות במגזר הפיננסי כאשר ועדת שטרום ביקשה להרחיב גישה לאינפורמציה, הן של המוסדות הפיננסים והן של הלקוחות שהיא פעולה בעלת השלכות לגבי חשיפת המערכת לפריצות סייבר. מה הם ראשי הנזק? יש ראש נזק ברור של פרסום וגילוי שמות בחשבונות לקוחות שבא לביטוי באירוע שירביט. ראש נזק חמור אחר הוא פוטנציאל של מניפולציה בחשבונות מוסדות פיננסיים ולקוחות כולל מערכות המסחר והסליקה. אגב באופן קצת מוזר לא שמענו על מימוש מניפולציה במסגרת של פריצות סייבר למרות שכל מי שקורא עתון מודע להיקף של פריצה לחשבונות מוגנים (כולל מערכות בחירות, נשק וטרור) קל וחומר למערכת הפיננסית איך זה שלא דווח על עדויות למניפולציה בחשבונות ובסליקה. ראשי נזק נוספים הם העברת מידע כוזב למוסד הפיננסי, פגיעה במוניטין והשבתת פעילות. שימו לב שפריצה לגורם אחד יוצרת נזק רוחבי למערכת הפיננסית עקב גישה לכל המערכת. ככל שאלמנט הדיגיטציה הולך ללוות אותנו בשנים הקרובות, והיתרונות שלו הם כל כך גדולים ומשמעותיים שוודאי לא נרצה לחסום אותו יש להכיר בחשיפות שהוא יוצר למערכת. כמה שאלות: קודם כל יש לי שאלה כללית שלה השלכות לטווח ארוך, אבל האם עצם הפעלת אמצעי הגנה שחלקם מתבצעים על ידי קשר אישי לא קובעת איזושהי תקרה לדיגיטציה? כלומר, האם אפשרי בנק דיגיטלי נטו? בנק דיגיטלי בו כל מערכת התקשורת עם הלקוחות, עם המוסדות הפיננסיים האחרים היא טהורת דיגיטל, כאשר אנו רואים שחלק ניכר מאמצעי ההגנה הם

על ידי קשר ישיר עם הלקוח, או קשר בין מוסדות, או ווידוא בעל פה של אינפורמציה מועברת. השאלה היא האם לא נוצרת פה איזושהי תקרה, איזו חסימה על התפתחות הדיגיטציה שנובעת מפוטנציאל פריצות הסייבר שגם הוא מתפתח במקביל להתפתחות הדיגיטציה. שאלה שניה שקשורה לדברים שהוזכרו, האם הושתקו מקרים של מניפולציה כדי למנוע בהלה? והדבר האחרון הוא נושא ועדת שטרום בהקשר לרפורמת התחרות בסקטור הפיננסי. שם הקוד של הרפורמה הוא , API - Application Programming Interface, שהוא מערך של העברת אינפורמציה בין מוסדות שפועלים במגזר הפיננסי והשאלה אם יש קשר להליך הזה עם כל נושא הגנות הסייבר? נשמע את זה מבנק ישראל, האם הוא לא עיכב את הפעלת ויישום הרפורמה בין היתר בגלל הסיכון הזה, כאשר אינפורמציה מהותית על הלקוח מועברת בין מוסדות שהגנות הסייבר שלהם אינן מאוזנות בהכרח. נניח שהמערכת הבנקאית מוגנת יותר עקב הנחיות הפיקוח שהגדיר סיכוני סייבר כסיכון סיסטמי, מהמערכות בגופים פיננסיים חוץ בנקאיים. המשמעות של העברת אינפורמציה האם משמעותה היא לא בעצם פריצת המערכת כולה כאשר ניתן להגיע לכל מקום מכל מקום ואז השאלה האם באמת העיכוב ביישום מסקנות ועדת התחרות נובע מחשש בנק ישראל לגבי סיכוני סייבר. נשמע על כך מהממונה במשרד מהמפקח על הבנקים.

דני חחיאשווילי

אני אולי אתחיל קצת בהצגה של האגף שאני מנהל. אני סגן המפקח על הבנקים, מנהל אגף טכנולוגיה וחדשנות זה אגף שהקמנו לפני ארבע שנים באמת מתוך מטרה לעודד את הטרנספורמציה הדיגיטלית, לעודד את החדשנות במערכת הבנקאות ומתוך איזו תפיסה שבתוך המבנה המסורתי של הפיקוח על הבנקים של הרגולטור סה קשה לעודד תחרות מעצם זה שיש בו את השמרנות המוטבעת בו ברגולציה ולכן אם אנחנו נקים אגף ייעודי שהתפיסה שלו תהיה לדחוף חדשנות אז נוכל להשיג את היעד בצורה טובה יותר. ואמיר הזכרת את חלק מהדברים את כל הAPI וכל הרפורמה שלנו על בנקאות פתוחה אני עוד שניה אתייחס לזה זה גם כן במסגרת האגף, לצד זה, לצד דחיפת החדשנות והטרנספורמציה הדיגיטלית אנחנו גם באגף עוקבים אחרי סיכוני הטכנולוגיה וסיכוני הסייבר, שזה בא זה לצד זה, ובאמת בודקים שעם הריצה קדימה ועם המעבר לדיגיטציה באמת אנחנו יודעים איך לנהל את הסיכונים האלו, ודרך אגב אנחנו רואים גם בדברים האלה גם במנהל הגנת הסייבר בבנק בסופו של דבר גם כאנאבלייר כמישהו שאמור לאפשר את הדיגיטציה הזאת וככה אנחנו מסתכלים על זה אבל כמובן צריך לדעת לנהל את הסיכונים. דרך אגב התשובה לשאלה האם יכול להיות בנק דגיטלי לחלוטין, אנחנו בהחלט חושבים שכן אנחנו מכוונים לשמה ואנחנו רואים שיותר ויותר פעולות בבנקים המסורתיים וגם בבנק הדיגיטלי שנתנו לו רישיון והתחיל לעבוד בשנה הזאת הם הולכים להיות הרבה יותר דיגיטציה יש עדיין מעורבות אנושית אבל גם המעורבות האנושית היא בסופו של דבר תרד. גם אם אתה תדרוש מעורבות אנושית הרי היום אנחנו יש לנו צ׳אט בוטים ויש לנו כאלה

שיכולים לדבר איתך אפילו וכל מיני דברים שיכולים להחליף גם בקרות אנושיות שאתה חושב שהיום רק בן אדם כול לעשות אותן בסופו של דבר אנחנו נראה גם את המחשב עושה את זה. אז אני רוצה כן להתייחס לשני נושאים ככה בזריזות כי אני יודע שפה אין לנו זמן לנאומים ואפשר לדבר על זה המון. אני רוצה אחד, להגיד למה אנחנו בתוך הפיקוח חושבים שמדובר בסיכון משמעותי, דרך אגב לא רק אנחנו, גם הגופים המפוקחים, אנחנו בפיקוח בשנתיים האחרונות עשינו סקר עושים סקר של נושאי משרה בכירים במערכת הבנקאות וסיכון הסייבר יוצא תמיד יצא בשנתיים האחרונות לפחות במקום הראשון בין הסיכונים המשמעותיים, דרך אגב הסיכון השני שהופיע זה הסיכון הטכנולוגי. זאת אומרת דווקא כל הסיכונים הפיננסיים הם נדחקים ושני הסיכונים האלה הם במקום הראשון. אז אני כן רוצה להסביר למה אנחנו רואים בזה סיכון משמעותי למרות מה שהזכרת שלומי על הדוחות הכספיים, ואחרי זה כן איך אנחנו בתוך הפיקוח מתייחסים לזה לאור ההערכה שלנו שמדובר בסיכון משמעותי, וככל שאחרי זה הזמן יותיר במסגרת הדיון אני אשמח להרחיב אם יהיו שאלות או דברים אחרים. אז אחד, חלק מהדברים הזכרתם, למה זה סיכון משמעותי? אז קודם כל אנחנו חושבים שאנחנו רואים, המערכת הפיננסית היא יעד של תקיפה. רואים את זה דרך אגב לא רק בישראל אלא בכל העולם. וזה נובע משתי סיבות מרכזיות: אחד- המערכת הפיננסית בכל העולם היא הרבה יותר דיגיטלית ממגזרים אחרים ואז ברגע שאתה יותר דיגיטלי אפשר יותר לתקוף אותך באירועי סייבר ובאמת התקיפות כנגד המגזר הפיננסי בכל העולם הן גבוהות יותר. והסיבה השנייה זה כולנו יודעים זה בגלל ששם נמצא הכסף, אוקיי, אז שמה תוקפים אותנו. זה סיבה אחת, אנחנו רואים שמיד, בישראל אפשר להוסיף לזה גם את הסיכון הגיאופוליטי, בישראל יש לנו עוד סיבות נוספות שתוקפים אותנו. הסיבה השניה שזה סיכון משמעותי, ושלומי גם הזכרת את זה, זה סיכון מאוד מאוד דינאמי, אנחנו רואים אותו כל הזמן מתפתח אנחנו רואים שהתוקפים כל הזמן משתפרים, היום כבר מדברים על השתלת קוד בתוכנות, זאת אומרת אפילו פורסם שהגיעו למייקרוסופט והשתילו שמה קוד שבסופו של דבר מאפשר לאיזה גישה ותקיפה, אנחנו רואים שהתוקפים עושים את זה הרבה פעמים לא רק בשביל רווח כספי אלא יש להם גם מטרות אחרות. והקלות שעושים את התקיפות היא הולכת ונהיית יותר קלה, מי שמכיר מהעולם של הטכנולוגיות ענן את כל המושגים של IAS ו Software as a service וכל המונחים האלו, אז עכשיו בעולם של הסייבר יש כברransom as a service , זאת אומרת יש שיתוף פעולה בין תוקפים, אז כמובן זה סיכון משמעותי. אז בסופו של דבר אנחנו כן חושבים שלסיכון סייבר יכול להיות נזק כספי משמעותי אני עוד מעט אזכיר את התרחיש קיצון שעשינו ששמה זה לא עלה, אבל כן אנחנו חושבים שיכול להיות נזק משמעותי. אחד, מחקרים באמת מראים שאין נזק כמו שציינת שלומי, אבל אחד, אין מספיק מידע וזה משהו שצריך לעבוד עליו ואנחנו כן מנסים לשפר את המידע. אני יודע שזו סוגיה שהיא לא רק בישראל אלא בכל העולם מנסים לראות איך אוספים מידע יותר טוב על סיכוני סייבר, אנחנו ממש לא מזמן הוצאנו הוראת דיווח חדשה על אירועי סייבר ואירועי כשל טכנולוגי דרך אגב אנחנו שמנו את זה באותו מקום כי לפעמים יכול להיות גם

אירוע כשל טכנולוגי שהוא לא נובע מסייבר והוא יכול ליצור נזק משמעותי, אז זה בהקשר הזה ואנחנו רואים איך לשפר את זה. גם אם הממוצע של הנזק בעולם שאנחנו רואים הוא עדיין נמוך, המקרה זנב tail risk הוא יכול להיות משמעותי עד כדי פגיעה ביציבות.

שלומי שוב

דני, איך זה מסתדר עם האירוע של התרחיש קיצון מה שאתה אומר עכשיו?

דני חחיאשווילי

תכף אסביר. והסיבה השלישית שזה יכול להיות משמעותי זה באמת אפקט ההדבקה שקיים במערכת הבנקאית. אז כשאתה מסתכל ככה על הסיכון הזה ועל המשמעותיות שלו אז באמת כשאנחנו בתור פיקוח על הבנקים מסתכלים על זה אנחנו מבינים שצריך להסתכל על זה בצורה שונה מהסיכונים האחרים, וזה לא שאנחנו לא עושים את הדברים הרגילים שאנחנו עושים בכל סיכון, את אומרת יש לנו באמת רגולציה שהיא מוכוונת לסיכוני סייבר אנחנו עוקבים אחרי ניהול הסיכונים, עושים הערכה לניהול סיכונים, לרמת הסיכון ולבקרות השונות, אנחנו מסתכלים על כל הדברים הרגילים שאנחנו עושים בקשר לכל סיכון אבל בהיבט של הסייבר יש עוד כל מיני דברים שאנחנו עושים יותר, מה שאנחנו לא עושים בסיכונים האחרים ואני פה אזכיר אותם. הדבר הראשון זה הבנה שיש חשיבות גדולה של שיתוף מידע בין הגופים הפיננסיים בינם לבין עצמם, ואנחנו ממש מעודדים את זה, היינו שותפים להקמת הסרט הפיננסי ביחד עם מערך הסייבר ומשרד האוצר ורגולטורים אחרים, ושמה זה באמת מקום שהוא מאפשר שיתוף מידע, זה אחד. והדבר השני שאנחנו עושים יש לנו פורום של מנהלי הגנת הסייבר שמתכנס באופן קבוע ושמה באמת מביאים מידע על סוגי תקיפות סוגי אירועים, דנים שם בכל מיני סוגיות של מדיניות, ובעצם אנחנו עושים אפסניה לשיתוף מידע בין הגופים הפיננסיים, זה חשיבות מאוד גדולה בשביל להתמודד עם הסיכון הזה.

אמיר ברנע

האם היו מקרים של מניפולציה בחשבונות בארץ כתוצאה מאירועי סייבר?

דני חחיאשווילי

אז הנה בדיוק אני מגיע לזה, והתשובה היא לא, לא היו. ואני בדיוק מגיע לנקודה השניה של מה שאנחנו עושים ואני אולי פה גם אדבר על התרחיש קיצון והתרחיש קיצון שלנו היה בסגנון הזה. אז אנחנו עושים הרבה תרגילים, תרגילים מגזריים כי זו אחת הדרכים להתמודד עם סיכון הסייבר לראות שבאמת אנחנו מוכנים ובאמת ב2019 בסוף 2019 הוצאנו תרחיש קיצון למערכת, זה אנחנו הפיקוח על הבנקים מוציא אחת לשנה תרחיש אחיד בדרך כלל זה היה תרחיש מאקרו כלכלי, סוף 2019 הוצאנו תרחיש קיצון סייבר. התרחיש קיצון סייבר הוא בעצם זה היה משהו שלא ראינו אותו

בכל העולם זה היה משהו די חדשני שניסינו לעשות אני מניח שיותר ויותר אנחנו נראה בנקים מרכזיים אחרים גם עושים את זה, בעצם מה שעשינו התרחיש דימה חדירה דרך צד ג' ,ספק בשרשרת אספקה, אם דיברנו קודם על הבנקאות הפתוחה ועל זה שיש גופים שמתחברים להוריד משהו מהבנק אז משהו בסגנון הזה, שנכנס מצליח לחדור למערכות הבנק ואז מה שהוא עושה הוא משבש את הנתונים של הגיבוי זאת אומרת במשך חודשים הוא יושב במערכות של הבנק והוא משבש את הנתונים של מערכות הגיבוי בלי שאף אחד שם לב כי זה בגיבוי, ואז אחרי תקופה שהוא משבש את הנתונים בגיבוי, הוא נכנס למערכות של הייצור ושמה הוא משבש את הנתונים, זאת אומרת יש שמה שיבוש של הנתונים, מישהו אחד יש לו יותר פיקדונות, משהו אחר יש לו פחות פיקדונות, הלוואות נעלמות או כל מיני דברים כאלו, ואי אפשר לחזור לגיבוי שכן גם הוא משובש. זה היה התרחיש ואת זה הורדנו לבנקים, ובאמת זה היה תרחיש מאתגר זה היה הראשון מסוגו ובעצם הם היו צריכים אחד לראות איך הם מתמודדים ברמה הטכנולוגית, ברמת הסייבר, ברמה מול הלקוחות, היה שמה ממש מובנה מתי זה מתגלה לבנק, מתי זה מתגלה לציבור, כמה זמן לוקח לו לתקן, בסופו של דבר מה שראינו ראינו הנזק הכספי שהיה מהתרחיש הזה והבנקים בתרחישים אצלנו הם בונים דוחות פורפורמה של דוח רווח והפסד ומאזן, אז לא ראינו פגיעה כספית משמעותית אבל כן ראינו סיכון נזילות שעלה בצורה משמעותית. זאת אומרת אנחנו מכירים בספרות את כל המונח הזה של cyber-run, וזה כן ראינו, וכן סיכוני מוניטין שהיו די משמעותיים והיה צריך לדעת איך לנהל את הסיכון הזה מול הציבור. עכשיו המאפיינים של התרחיש סייבר

שלומי שוב

יכול להיות שאם היית לוקח מקרה אחר היית מקבל תוצאה אחרת, לא?

דני חחיאשווילי

נכון. וזה מה שצריך להבין גם בסיכוני סייבר, שהם יכולים הגיע מכל מיני מקומות ותרחישים שונים יכולים להביא לנזקים שונים ולכם אתה צריך להיות מוכן לכמה תרחישים. אנחנו חושבים שגם פה יכול להיות סיכון כספי משמעותי. דרך אגב כשאתה רואה אירועי קצה, מקרים אחרים בעולם שמפורסמים Equifax דוגמה גדולה זה חברת דירוג אשראי בארה"ב שהיה לה שם דלף מידע משמעותי, העלויות שמה היו מטורפות . רואים את זה עד היום הם משלמים על זה המון כספים, אז כן יכול להיות אירוע משמעותי. אז התרגילים והתרחישים זה עוד משהו שאנחנו עושים. הדבר השלישי שהוא חשוב לעשות זה שיתוף פעולה ושלומי הזכרת את השיתוף פעולה עם הרשויות האחרות, זה שיתוף פעולה עם הרגולטורים האחרים, שיתוף פעולה עם רשויות מדינה אחרות, וכמובן עם מערך הסייבר. אנחנו ככלל כשמסתכלים על הגנת הסייבר, אחד האחריות הראשונה היא כמובן של הבנקים עצמם של המערכת הפיננסית עצמה, להגן על עצמה ולהיות הקו האשון אבל אנחנו מבינים

שיש מקרים שנצרכת מעטפת הגנה מדינתית אם זה מערך הסייבר ואם זה גופים אחרים, אנחנו כל הזמן יושבים וחושבים עם הגופים האלה איך לשפר את זה ומה לעשות, זה יכול לנבוע דיברת על זה על האיגום משאבים לפעמים אם צריך, לפעמים יש יכולות שרק למדינה יש והיא יכולה לתת והגופים לא יכולים עד הסוף להיות שמה, אנחנו כל הזמן חושבים איך לשפר את שיתוף הפעולה ואיך לאפשר את הדברים האלה, אנחנו יושבים עם מערך הסייבר, דרך אגב חתמנו על MOU מול מערך הסייבר שמתייחס בדיוק לדברים האלה ומתייחס גם על המעורבות שלהם באירועים ואיך אנחנו מטפלים בדברים האלה, אז זה משהו שצריך כל הזמן לחשוב עליו, ואולי נקודה אחרונה בהקשר הזה אנחנו עוקבים מקרוב אחרי הניהול סיכונים של הבנקים בתחום הזה של הסייבר, אנחנו רואים שהבנקים כן משקיעים הרבה בשביל שתהיה להם הגנת סייבר טובה ואנחנו חושבים שמה שהם עושים, שיש להם יכולות הגנה טובות. מה שכן צריך להבין זה וזאת גם כן אחת מהנחות היסוד שלנו זה שמניעה מוחלטת היא בלתי אפשרית והחודש האחרון שראינו חברות ענק בעולם עם מומחיות אם זה פייראיי וכל מיני שנפגעו מתקיפות סייבר אנחנו מבינים שמניעה מוחלטת בלתי אפשרית ולכן מעבר ליכולות הגנה ויכולות המניעה חשוב שיהיו גם יכולות זיהוי מוקדמות ויכולת להגיב מהר ולהתמודד עם האירועים האלה, ואנחנו באמת אנחנו מכווינים גם לשמה ואנחנו רוצים לראות את היכולות האלו קיימות גם בארגונים שלנו. דרך אגב סקר של פייראיי לימד על זה שבערך 50% מהאירועים הם לא מתגלים ע״י הגופים עצמם. זה נובע מזה שהתוקפים הם בעצם באים מוקדם יותר ומנסים להשיג את הרווח הכספי שלהם, אבל בסופו של דבר זו מלחמה בלתי נגמרת, וצריך לראות איך כל הזמן משתפרים בדבר הזה. אולי מילה אחרונה על הנושא של הבנקאות הפתוחה ומה שאמיר הזכיר, שטרום, אז אנחנו מקדמים את נושא הבנקאות הפתוחה, יש כבר הוראה של המפקח על הבנקים שיצאה שנה שעברה, ועם לוחות זמנים לעלייה לאוויר של בנקאות פתוחה, להעברת מידע לצדדים שלישיים וצריך שתהיה חקיקה בנושא בגלל שהממשלה נפלה אז בינתיים החקיקה לא עוברת. החקיקה הזאת אמורה בעצם לקבוע את הרגולציה על הצדדים השלישיים שבעצם יאספו את המידע הזה, איזה דרישות אבטחת מידע יהיו מהם וכו׳ והיא אמורה בעצם לאבטח את הנושא הזה אבל אין ספק שזה מגביר את סיכון הסייבר וצריך לדעת גם עם הדברים האלה איך להתמודד, אז עד כאן ואם צריך נרחיב בהמשך. תודה.

עמית גל

בוקר טוב. אז אני באמת אנסה להתייחס בקצרה. בטח בזמן שיש לנו אי אפשר למצות את הנושא שזה נושא מאוד משמעותי. אני לא צריך לחזור על מה הסיבות שהנושא הזה חשוב. הרחבתם למה הנושא חשוב אבל אני אגיד שבתור רגולטור פיננסי אני חושב שברור מה עמדתנו אבל בכל זאת אני אחזור על זה, שגם אצלנו נושא הסייבר נמצא גבוה מאוד במפת הסיכונים, ואני חושב שהדיון על זה הוא טוב למרות שכמו שאמרת שלומי זה לא נושא פיננסי מובהק אבל זה הופך להיות כזה דווקא בגלל שהוא

גבוה במפת הסיכונים של מוסדות פיננסיים. אז קצת מהזווית שלנו, הרשות מסדירה את התחום של סיכוני סייבר מעל לעשור אבל אין ספק שבעצימות הרבה יותר גבוהה ב-3-4 שנים האחרונות. לפני כארבע שנים נכנסה לתוקף הוראה הרבה יותר מקיפה בנושא ניהול סיכוני הסייבר והדבר הזה הוא כמובן לא הדבר היחיד, הרשות עושה הרבה פעולות של פיקוח, ביצענו בכמה שנים האחרונות מבדקי חדירה. אני רק רוצה להתעכב קצת במילה אחת גם על מה שאמר אמיר ואני רוצה לחדד גם את זווית המבט שלנו אבל בטח לא נצלול לרמה הפילוסופית של מה זה סיכון סייבר. אין לי ספק שסיכון סייבר זה ספקטרום מאוד מאוד רחב ואפשר לראות את זה גם בהוראות בתחום הזה, סיכון סייבר משיק וחופף ומקביל להרבה סיכונים אחרים, אם זה סיכונים של מעילות והונאות, אם זה סיכונים תפעוליים בעולמות האלה גם יש הרבה נושאים שם, למשל הנדסה חברתית והיבטים של הגנה פיזית אז התשובה היא לנושא הזה של איך מגנים על זה ומה הסיכון הזה אז אני חושב שהתשובה היא מאוד רחבה, אז גם אם אנחנו מסתכלים על תחום שנתסס כנוצץ וזוהר ומתוחכם ואיזשהם עולמות טכנולוגיים וכלים מאוד מאוד מתוחכמים, הדבר הזה לא תמיד רק במחוזות האלה, הרבה פעמים סיכון הסייבר מגיע מהרבה דברים שהם low-tech לפעמים שילוב של הנדסה חברתית, אז זה הדבר הזה. עכשיו אני אגיד לגבי התחום הזה הוא מאוד בכותרות, אבל הפעילות היומיומית גם בטח בהגנת סייבר בתוך הגופים וזה מערך שלם של אנשים שמעורבים בזה בתוך גוף פיננסי – מנהל הגנת סייבר, כמובן מעורבות של ניהול סיכונים, הנהלה, דירקטוריון, ולכל אורך הפעילות הזאת היא לא תמיד נוצצת ואפשר להגיד שאפילו רוב הזמן היא לא נוצצת ואפשר להגיד שגם פעילות הפיקוח שלנו היא לא בהכרח נוצצת. זה עבודה שצריך להבין שהיא דורשת הרבה עקביות, דיוק והרבה מאוד ירידה לפרטים. עכשיו מהכיוון שלנו אני אזכיר משהו שהוא אולי ברור אבל התפקידים של הרשות כמובן בתחום של ראיית סיכונים בכלל היא רחבה היא גם מתייחסת כמובן לשמירה על היציבות של הגוף, להגן על עמיתים ועל המבוטחים, אבל גם נושאים של דיגיטציה, חדשנות טכנולוגית ותחרות וגם בסיכון סייבר במיוחד זה משהו שצריך להבין שנדרש למצוא את האיזון בו. עכשיו דבר שהוא גם ברור אבל בכל זאת אני אזכיר אותו זה שגופים פיננסים הם גופים שבמהות שלהם הם מנהלים סיכונים ולפני הכל ואחרי הכל צריך לזכור שסיכון סייבר הוא עוד סיכון. לא שאני בא להפחית מהסיכון הזה, הוא כמו שאמרתי סיכון מאוד גבוה במפת הסיכונים עם פוטנציאל נזק מאוד משמעותי, אבל בתוך מסגרת ניהול הסיכונים הכוללת של גוף פיננסי גם הדבר הזה נכנס והמסגרת הזאת של ראייה מבוססת סיכונים גם נמצאת ברגולציה.

רקפת שני

בהמשך לדברי דני, האם אתם מבקשים להכניס את זה לתרחישי קיצון? אתם עושים משהו אקטיבי?

עמית גל

תרחישי קיצון זה כלי אחד במסגרת הפעילות הפיקוחית, תרחיש קיצון היה לנו במערכת בזמן האחרון ויש גם תרגולים של המשכיות עסקית, ותיקי חירום, ובפועל יש לקחים מכל פעולות ניהול הסיכון שהגוף עושה.

שלומי שוב

תרחיש של המציאות

עמית גל

אפשר גם לשאול האם התרחיש שהתקיים שראינו אותו בחודש האחרון אגב לא רק בענף הביטוח בכלל אנחנו רואים במדינה, הוא הוא תרחיש הקיצון שאנחנו מתרגלים אז לא בהכרח אבל זה כלי נוסף בהיערכות לסיכוני סייבר, שהם איום שמשתנה כל הזמן.

אמיר ברנע

האם סיכוני סייבר בשירביט מבוטחים בשירביט?

עמית גל

זה ייצא מעגל שקורס בתוך עצמו. אבל כמובן להיבט של סיכון סייבר יש גם השפעה על עמיתים, אנחנו מסתכלים על זה אבל מכל ההיבט הרחב גם של שמירה על אמון הציבור המערכת הפיננסית.

שלומי שוב

עד כמה שיתוף הפעולה בין הרגולטורים משתפר בעקבות האירוע הזה של שירביט?

עמית גל

אז פה אני משתלב עם מה שאמר דני על הרגולטורים הפיננסיים, גם יש הרבה תחומים שהם דומים ויש שיתוף של ידע ועבודה עם מערך הסייבר, תכף נתייחס לזה אבל אין ברירה בתוך הסיכון הזה לשתף פעולה. המערכת הזאת ומעטפת ההגנה שצריכה להיות בניהול סיכון הסייבר מחייבת את הקשר הזה והקשר הזה קיים ועובד. בדבר הזה סיכון הסייבר הוא נהוג להגיד שהוא קצת שונה ברמה הזאת שיש למדינה יש תפקיד בניהול הסיכון. אגב אני לא בטוח שרק בנושא הזה למדינה יש תפקיד אם מסתכלים על זה גם לא בהכרח מייחד אותו, אולי תפקיד טיפה יותר מיוחד, אבל גם לצורך העניין בגניבת מכוניות ובשריפות גם שם למדינה יש תפקיד בהגנה על הציבור והפחתת הסיכון. אבל אין ספק שבתפיסת ההגנה התפקיד של המדינה כולל מעטפת שנותנת המדינה בהגנת סייבר.

שלומי שוב

איזה עוד תובנות למעשה חוץ מהנושא של שיתוף הפעולה בין הרגולטורים שהוא חשוב אתם למעשה מפיקים מתוך אירוע הקיצון שחווינו?

עמית גל

אז אני אגיד, הדבר הזה דורש שהמערכת הזאת של מעגלי ההגנה בסייבר תעבוד בתיאום והרבה הרמוניה, מה הכוונה? הגנת סייבר כמו שאמרנו מגיעה מכל הרבדים החל באיך מתנהג אדם פרטי, מבוטח, איך הוא מגן על המידע שלו מחליף סיסמאות וכולי, גם הגוף המוסדי עצמו אבל גם המדינה בכלים שלה, אני לא אחזור על מה שדני אמר אבל הכלים שיכולה לתת המדינה ברמה מודיעינית ברמה מבצעית וכולי, אבל בדבר הזה מה שחשוב שכל מעגל לא יסתמך על מעגל אחר במובן שכל אחד יודע מה הוא עושה ומה הוא מקבל מהמעגלים האחרים. לא יכול להיות מצב שמבוטח יגיד "מישהו מגן עליי בחברה אני לא צריך לשמור על המידע שלי" ובאותה מידה חברת הביטוח צריכה לדעת שהיא לא צריכה להסתמך על יכולות הגנה שהיא לא אמורה לקבל מהמדינה.

זה חלק עקרוני בבנייה של מבנה הגנה לאומי. רק עוד כמה דברים קטנים שאני רוצה להגיד. ברמת התאוששות מאירוע אני חושב שזה דבר שצריך להבין אותו והוא גם די ברור, יכול להיות שיכולות התאוששות מאירוע מגיעות ברוב המקרים מגוף עצמו. בסופו של דבר אנחנו מדברים על מערכת מדינתית ואנחנו מדברים על תמיכה באירועים אבל בסוף זה המערכות של חברות הביטוח והן מערכות מאוד מורכבות והמפתח להתאוששות הרבה פעמים נמצא שם וביכולות של הגוף והיכרות שלו עם המערכות. ההנחיות שלנו הן הנחיות לדעתי מאוד מתקדמות, מביאות אותנו לרמה של הגנת סייבר טובה בגופים האלו, זה הנחיות מהמתקדמות שיש. אבל אני רוצה להגיד, צריך להבין שמבחינת הפעילות של הרשות, אנחנו לא מגיעים לחברת ביטוח כשיש אירוע ואנחנו לא נעלמים מחברת ביטוח כשנגמר אירוע. הרעיון של פיקוח כמו התהליך של הגנת סייבר זה תהליך מתמשך. זה תהליך שבו אנחנו נמצאים לפני, אנחנו נמצאים בבדיקות, במעקבים, בביקורות, בבדיקה של הרגולציה, וכמובן גם אחרי אירוע. כמו שדני אמר אני רק אסכם בשתי מילים האלה גם אנחנו מסתכלים על זה בצורה שלתפיסתנו בהגנת סייבר אין 100% הגנה. תמיד יהיו אירועים ואנחנו מביאים את הדבר הזה בחשבון אבל השאלה היא מה היא ההתנהלות של החברה. אם קרה אירוע אבל הגוף המוסדי קיים את ההוראות, מתנהל בצורה שקופה, מדווח אלינו כדי שאנחנו נוכל להכיל את האירוע ולתת את התמיכה כמו שאנחנו מצפים, אז ההתייחסות היא אחת. אבל אם אנחנו רואים שהגוף לא מקיים את ההוראות אז אנחנו מתייחסים לזה כמובן בהתאם.

שלומי שוב

בואו נשמע עכשיו את חמי פקר, חמי היה ראש מנהלת הסייבר במשרד ראש הממשלה במשך הרבה מאד שנים.

חמי פקר

תודה שלומי, בוקר טוב חברים. אני חושב שבשלב הזה של הדיון שלומי כדאי שנשמע גם מאנשים יתר לגבי הפערים שהם רואים במצב ההיערכות הנוכחי, לגבי מסגרות האחריות וסמכות. אני חושב שלכולם ברור נושאי תפיסת האיומים/סיכונים. אתה, אמיר ועמית הרחבתם רבות בנושא. העולם המערבי נחשף לראשונה בעשור האחרון (2014), כאשר נודע על תקיפתה של חברה מסחרית בארה״ב, SONY, ע״י יכולות גבוהות של מדינה (עפ״י פרסומים זרים, צפון קוריאה)- בפעם הראשונה הממשל האמריקאי התמודד עם פערים בהיבטי המשפט, רגולציה, היבטים אתיים-מסחריים, זכות הציבור לדעת- האם באחריותו וסמכותו לסייע כן/לא ולהגדיר האם אכן קיים נזק ציבורי, לאומי, כלכלי על החברה והמדינה הנתקפת. רק לאחר כחודש, ממשלה הנשיא אובמה, קיבל החלטה לסייע. באותו זמן הציבור האמריקאי נאלץ להתמודד עם אכיפה של מדינה אחרת עליו, למורת-רוחו הרבה של הממשל האמריקאי. בחינת פערי האחריות וסמכות לגופים הרגולטוריים ומידת יכולתם לעמוד ביכולות הנחייה ואכוונה מותאמת מציאות התקפית מתקדמת- חייבת להבחן מחדש. בהיבט מדינת-ישראל, נושא הטיפול בנכסי מדינה קריטיים החל לפני כעשרים שנה. בעשור האחרון אנו רואים את התרחבות הפער בין יכולות ההגנה על המרחב הדיגיטלי לבין היכולות ההתקפיות המתקדמות בכל יום עוד ועוד. הפער הינו יותר בהיבטים של גורמים פיננסיים, חברות עסקיות-מסחריות וגופים נוספים שמתקשים לייצר משאבי הגנה הולמים ו/או לאור חוסר במודעות להתפתחות האיום/סיכון במרחב המדובר. הקושי להגן נדרש היום לעמוד לדעתי להיבחן ב- 3 שאלות מרכזיות מקצועיות בפורום זה בפני ואולי ההישג המרכזי של הדיון יהיה במיפוי הפערים ולאן הולכים הלאה. שלוש השאלות המשמעותיות לטעמי: האם המדיניות ומקור הידע והתוכן המקצועי שהרגולטור מספק היום לאכוונת הגופים הפיננסיים, אכן מספקת ? האם הרגולטור יכול להחזיק בעתיד צוותים מקצועיים מספיק טובים שעומדים ביכולות הטכנולוגיות ההתקפיות של 2021, לרבות מחלקות שאוספות מודיעין, ממפות סיכונים, מגבשות תורה מקצועית איכותית לעמוד במרבית או לצמצם את הסיכונים במידה רבה ? האם קיים גורם רגולטורי מרכזי שרכן רואה את כל התמונה לאור-זמן ויודע לקשר ו/או להפיק תובנות ומשמעויות מערכתיות למגזר זה ? בנוסף, האם המדינה לוקחת את זה על עצמה לראות את התמונה הפיננסית הלאומית ? ברור לכולנו כי מימד הזמן והקשוי לזהות תקיפת איכותית הינו מורכב במיוחד. על מי האחריות לזהות מי עומד מאחורי המתקפה- מדינה, ארגון טרור, ארגון פשע וכו׳. הגופים הרגולטוריים כאן נדרשים לשאול את עצמם האם באמת מתקיימת תמונה וראיה לאומית

כוללת והשת"פ שדובר כאן עם המדינה, אכן מספק? על הפערים הללו לדעתי עלינו להתרכז בפורום זה.

נקודה נוספת ומהותית במיוחד- האם החברות/גופים הפיננסיים מסוגלים כיום לספק תורת אבטחה יעילה למול המערכות ההתקפיות ? כפי שהוזכר כאן, המשאבים הנדרשים הינם רבים ויקרים מאוד.

שלומי שוב

אז אנחנו יודעים או לא יודעים חמי? אני יודע שאתה מדבר בעדינות, אבל מה אנחנו צריכים להסיק?

חמי פקר

אני חושב שאנחנו צריכים להבין שאולי הגיע הזמן לעבור ולשקול בהיבט המדינה מחדש את כל הנושא של ניהול סיכונים במגזר הפיננסי לטובת ההיבט הלאומי, ואני חושב שלמדינה יש ארגז כלים הרבה יותר משוכלל לסייע בנושא הזה.

אמיר ברנע

מה שאתה אומר אם אני מבין נכון, הוא שברמה של פעילויות ביון של מדינות הגיעו לרמות גבוהות מאוד של יכולות פריצות סייבר ורמה גבוהה של הגנות נגד פריצות סייבר. אתה מעלה את השאלה האם אותה רמה נשמרת ברמה המאקרו פיננסית בתוך המשק, למשל במערכות מסחר, האם יש אפשרות פריצה למערכות מסחר? או למערכות שיתוף אינפורמציה? יש לי הרגשה של פער ככל שאתה מדגיש את הסיכונים, והמגזר הפיננסי נמצא באיזו שלווה כזו ,שזה לא נורא וההשפעה היא מינורית ועוד לא התגלו מקרים של מניפולציות. אני למד שאתה בעד הלאמת הטיפול בסייבר כי הגישה הכללית במשק היא ש"זה יהיה בסדר, לקחנו עוד אנשים והכל יסתדר".

חמי פקר

תרחיש של פגיעה היום במרכז הסליקה של המערכת הבנקאית של מדינת-ישראל לשבוע, יגרום למבוכה לגופים ובציבור ובוודאי לסוגיה מערכתית לאומית רחבה, שהמדינה תידרש לסייע בה.

שלומי שוב

אמיר בדיוק דיבר על זה אתמול.

חמי פקר

לזכות המדינה, יש לומר - המדינה החלה לטפל בנושא לפני למעלה מעשרים שנה. הייתי אומר שבעשור האחרון עם מערך הסייבר הלאומי והקמת המטה, היבטים נוספים הנוגעים יותר להיבטים העסקיים/מסחריים/אזרחיים. השאלה, האם האמור מספק. המדינה קבעה קריטריונים מסוימים לתשתיות קריטיות היום שמטופלות היטב ע"י מערך הסייבר הלאומי. בהחלט נכון וראוי היום לשקול

את מיקומו של המגזר הפיננסי בהשפעה על המשק הלאומי. ייתכן ונדרש היום לייצר מצב שמגזר זה יקבל מעטפת אבטחה הדוקה יותר, חזקה יותר, משמעותית יותר מהמדינה. לדעתי, מתקיים פער משמעותי מאוד בתמונת הסיכונים הכוללת של המגזר הפיננסי, למול המשאבים המוקצים בפועל. פער זה, לדעתי, הולך ומתרחב כל הזמן ולא מצטמצם, לעומת יכולות התקיפה שעולות. ברגע שאין גורם לאומי הרואה את כל התמונה המערכתית, או עשויים להימצא במצב של חשיפה נוראית לאורך זמן, שתתגלה אך ורק בדיעבד, לרבות האפשרות כי יתגלה שמי שעמד מאחורי התקיפה, הינו גורם אחר לחלוטין ממי שסברו.

שלומי שוב

זה בדיוק מוביל אותנו לשמוע גם את הצד של מערך הסייבר.

מיטל אריק

שלום לכולם, שמחה להצטרף לפורום החשוב הזה. ברשותכם אני רוצה רגע לעשות איזשהו זום-אאוט ואז לענות גם על השאלות שעלו. אם אנחנו מסתכלים על התקופה האחרונה אז כולנו מבינים שיש איזושהי מגמה עולמית, אנחנו נמצאים באיזושהי תקופה שהיא יותר כאוטית שמקצינה הרבה מאוד אלמנטים ואנחנו רואים את ההתבטאות של זה כמובן גם במרחב של הסייבר. בתוך זה יש כמובן התגברות של אירועים שגם המערך, למרות היותו פעיל תמיד במרחב ההגנה מבחין בקפיצה בכמות ואיכות האירועים. חשוב שנעשה הבדלה בין מרבית האירועים שמערך הסייבר רואה ומטפל בהם כשגרה, לבין האירוע האחרון שבו מודגמת מתקפה מעצמתית של סולארווינדס שהחלה עם הגילוי של פייראיי. חשוב לי לעשות את ההבדלה הזאת כי זה בעצם גם מאוד ממקד אותנו במאמצי ההגנה שאנחנו צריכים להתפקס עליהם, כולנו. התקיפה של סולארווינדס הינה תקיפה מעצמתית לכל דבר ועניין, תקיפה שכמובן שלא הייתה אמורה להתגלות, תקיפה שהיא שמאופיינת ביכולות מאוד גבוהות של תוקף שבוחר מטרה ולרוב הוא יבקיע אותה. תקיפות מסוג זה הינן איום בראש ובראשונה על התשתיות הקריטיות של המדינה ואינן גורם האיום הראשון אתו צריך להתמודד המגזר הפיננסי. בצד השני יש לנו את כל המתקפות האחרונות, דוגמאתם תקפת pay-to-key, הקבוצה שמוציאה כל יומיים בערך עדכון בטוויטר שלה על מה שהיא עושה, קבוצה שיש לה מטרות של טרור \ הבכה, בשילוב עם רווח כלכלי, שמצליחה להשיג את ההישגים שלה פשוט בגלל שמצב ההגנה הממוצע הוא מאוד מאוד נמוך, וזה משהו שאנחנו חייבים להבין אותו, לפני שרצים לעסוק ולהתמודד עם איום מעצמתי, כדי שנטפל בפערים והחולשות שמביאים למתקפות הרבות שמתבצעות כיום בקלות הבלתי נסבלת.

התוקפים מבינים שיותר פשוט להיכנס לארגונים בדלת האחורית, כי לפעמם הדלת הראשית יותר מאובטחת, ויש איזורים נידחים בכל ארגון גדול שהם פחות תחת תשומת הלב ופחות תחת העין הפקוחה בהיבטי יכולות של גילוי וניטור, בהם קיימת גישה לצד ג' חברות התמיכה והתחזוקה, חברות

שנותנות שירותים למגוון גדול של לקוחות. שרשרת האספקה תמיד על הכוונת כיוון שממנה ניתן להגיע ליעדים רבים. לצד הנ"ל קיימות מתקפות "ריסוס" רבות המנצלות חולשות ומשיגות הצלחות כי כאמור, רמת ההגנה אינה מספקת מה שמוביל למסקנה הבלתי נמנעת שיש לעסוק ביתר שאת גם ובעיקר ברמת הארגון, בהגנת סייבר ובניהול הסיכונים סביב נושא מרכזי זה כיוון שיש לו השלכות מרחיקות לכת על הארגון.

קיימת בעיית מודעות ברמת הנהלות וארגונים בנושא, שלא עוסקים בנושא בעומק הנדרש, שואלים את השאלות ומקצים משאבים לטיפול בנושא. בחלק מהמקרים זה נעשה בצורה רצינית רק לאחר תקיפה משמעותית. לצערנו אין עדיין חיבור תפיסתי בין סייבר ורמת השירותים או המוניטין של חברה או ארגון.

אמיר ברנע

מיטל האם במסגרת הפעולות מאקרו כדוגמה מערכת המסחר בארץ או המסלקה, האם אתם לוקחים אחריות על הגנת סייבר של אלמנטים מאקרו כלכליים שיש להם השפעה רוחבית על כל המערכת ?

מיטל אריק

כמובן. מערכת הסליקה הבנקאית ושירותי הבנקאות האוטומטיים הם גוף תשתית קריטית לכל דבר ועניין, המקבלים ליווי והנחייה ייעודית בהגנת הסייבר. מתחת לרמה הזאת שהיא בעצם ה"קראון ג'ולס" שלנו כמדינה, אנחנו מסתכלים על שכבה נוספת הנקראת "גופי A" שהינם הבאים בתור בחשיבותם גופים חיוניים, בעלי השפעה ישירה על תהליכים לאומיים ויעדי שירות

שלומי שוב

קבוצת A זה לדוגמה הגופים הפיננסיים הבנקים והביטוח?

מיטל אריק

כמובן, גופים פיננסיים והמגזר, הבנקים, חברות הביטוח, הרגולטורים יודעים להצביע על הגופים האלה, העונים על סדרה של תבחינים המצביעים על פוטנציאל הנזק שלהם ממחולל סייבר.

שלומי שוב

זאת אומרת דרך הרגולטורים לכם אין את הסמכות

מיטל אריק

נכון

שלומי שוב

זה מצב תקין? זאת אומרת זה לא היה עדיף אחרת?

מיטל אריק

שת"פ בין מערך הסייבר לרגולטורים הוא הכרח. מערך הסייבר יודע להביא את הידע המקצועי לכל האלמנטים והנדבכים, אבל בהסתכלות המגזרית, מערך הסייבר לא יכול להחליף את הרגולטורים שהינם האוטוריטה בתחומם, בעלי האחריות על הרציפות התפקודית של המגזר, בעלי ההבנה של מארג היחסים וההשפעות בין הארגונים . השיח המשותף קריטי ומוכיח את עצמו, בו כל אחד מהגורמים מביא לשולחן את היתרון היחסי שלו.

אמיר ברנע

אמרת קודם שברמה של הארגונים לדעתך רמת ההגנה היא נמוכה יחסית, עכשיו האם את יכולה להבטיח לנו שלפי שיקול דעתך המקצועי רמת ההגנה על הגופים שאת קוראת להם A או הגופים המאקרו כלכליים שלהם ממשמעויות רוחביות, מסלקה ומסחר דברים כאלה, היא גבוהה יחסית או שאת ביקורתית לגבי רמת ההגנה בפועל?

מיטל אריק

במגזר הפיננסי ניתן לומר את זה בצורה די טובה, גופי הA מקבלים מענה טוב מבחינת רמת ההגנה, אבל זה לגבי גופי A בלבד. בשאר המשק אנחנו יודעים להגיד שלא!

ישנם גופי בחשיבות A ללא גורם מאסדר\רגולטור מולם המערך נכנס כגורם הכוונה מקצועי לאור חשיבותם והשפעתם על המשק על מנת שלא יפלו בין הכיסאות.

שלומי שוב

מיטל אבל ממה שאני מבין, אם אנחנו מדברים על קבוצה A אז יש היום הגנה מספקת נניח מפני תקיפה של ארגוני הפשיעה?

מיטל אריק

חשוב להבין שהגנה בסייבר היא תהליך בלתי נגמר, כל שעתיים בערך יכולה להתפרסם חולשה אחרת שפוגשת את ה"פרימטר" הארגוני, כל המשטח שהוא מנגיש כלפי חוץ, והתוקפים היום משפרים כל הזמן את יכולתם לנצל במהירות גבוהה יותר חולשות אלו, לפני שהארגון מצליח להגיב ולטפל בסגירתן. הם בונים על זה שלארגונים לוקח זמן לעשות את זה. כאמירה כללית אפשר לומר שבמגזר הפיננסי רמת ההגנה של גופי A היא טובה בפני התקיפות האלה, אבל הגופים כל הזמן מאותגרים בנושא הזה, ולכן אנחנו חייבים להמשיך ולתת על זה את הדגש, ולא רק בגופי הA , כיוון שקיימת

קישוריות גבוהה בין הגופים ובגלל שאנחנו מדברים על הנושא של שרשרת ההספקה, ובגלל שאנחנו רואים מתקפות פישינג שמצליחות, אפרופו המתקפה על חברת עמיטל, , ויש לנו בסופו של דבר גם את הגורם האנושי שיעשה טעות וילחץ על קישור, ולכן אי אפשר לנוח על זרי הדפנה ולהמשיך בניהול סיכוני הסייבר ובהגנה באופן בלתי פוסק.

שלומי שוב

אני רוצה לצרף עכשיו לדיון את יעקב מרשות ניירות ערך. יעקב איך אתה באמת רואה בזמנו פרסתם גם הנחייה לגילוי וכו' איך אתה באמת רואה את היישום של ההנחיה הזאת כי אתה יודע אני ככה מרגיש שכולם פה מדברים על החשיבות ועל כמה צריך לשקוד את הנושא הזה אבל השאלה היא האם הוא באמת מקבל תמחור נכון מבחינת החוסר מהותיות לכאורה?

יעקב יודקביץ

בוקר טוב. קודם כל, אני אתייחס לשאלה למה אנחנו פרסמנו את העמדה הזאת, שהרי כמחלקת תאגידים שעוסקת בגילוי ולא בפיקוח על התנהלות אנחנו לא רגילים לפרסם מסמכים שאומרים איך חברה צריכה לנהל את הסיכונים שלה ופה קרה משהו חריג, שבאנו ופרסמנו התייחסות ספציפית לנושא הזה של סיכון סייבר. אני חושב שלאור מה שדיברו פה מקודם זה יכול להיות די מובן כי קודם כל זה סיכון שהוא חדש יחסית - סיכון שהמפעל יישרף או שלקוח מהותי יעזוב, כבר מלפני 50 שנה כל אחד היה יכול להבין שיש כזה סיכון, ואילו זה סיכון שהייתה לנו תחושה שיכול להיות שהחברות שנותנות את הגילוי או דנות בסיכונים לא מספיק מודעות אליו ולכן רצינו לזרקר אותו כסיכון שצריכים להתייחס אליו. אני חושב שעוד סיבה היא גם שזה סיכון שהוא לא כל כך מובן. דיברו פה קודם נניח על הבנקים שבשנים האחרונות מציינים את הסיכון הזה כסיכון המשמעותי ביותר שלהם ; אני מנחש שאם תשאלו אותם למה, הם יענו שזה לאו דווקא בגלל שזה הסיכון עם החשיפה הכספית הכי גבוהה. אנחנו יודעים שסיכון, חלק מהעניין שלו זה היכולת לנהל אותו ; בעוד שסיכון אשראי לדוגמא הוא סיכון שלבנקים יש ניסיון של מאות שנים בלנהל אותו ומכירים אותו, זה סיכון יחסית חדש ומן הסתם משהו שאתה פחות מבין אותו אתה פחות יודע גם להסביר אותו ולנתח אותו בדוחות שלך.

שלומי שוב

אגב יעקב הם מסווגים את זה כבינוני לא כגבוה, לפחות בדוח השנתי האחרון יכול להיות שזה יעלה עכשיו בדוחות הקרובים?

יעקב יודקביץ

כן יכול להיות מאוד שזה גם קשור לדבר הזה. זאת אומרת, ואני לא רוצה לדבר פה בשם הפיקוח על הבנקים, שיכול להיות שיש הבדל למשל מה החשיפה שלך (שמשפיעה על הגילוי בדוחות) ועד כמה אתה חושש מסיכון ואולי פחות מבין אותו (מה שגרם לכך שבסקרים הציגו את הסיכון הזה כזה שממנו חוששים ביותר). בכל אופן, אם אני חוזר אלינו אז זו הסיבה שמצאנו לנכון לפרסם את המסמך. כמו שאמרתי זה מסמך חריג שנועד לזרקר את הנושא ולהפנות את תשומת הלב של החברות לצורך שלהן להתייחס גם לסיכון הזה במסגרת הסיכונים שלהן בדוח השנתי. באופן חריג אנחנו עשינו סקר פנימי שבדק עד כמה העמדה שלנו השפיעה על הגילוי בדוחות שיצאו אחרי הפרסום (בדוחות 2018) וראינו שהייתה לזה השפעה - מבין החברות שראינו שהתייחסו בסיכון הסייבר כגורם סיכון, מעל 20% כללו את הסיכון הזה לראשונה בשנה של פרסום העמדה שלנו ומעל 30% עדכנו את הגילוי, זאת אומרת תיארו אותו יותר בהרחבה או יותר בפירוט לעומת מה שהיה בעבר.

שלומי שוב

לצערי אנחנו טובים בזה כן.

אמיר ברנע

יעקב, אתם נותנים גיבוי להסתרת אינפורמציה על אירועי סייבר מתוך כוונה שיכול ליצור בהלה או ליצור השפעה רוחבית כלשהי? כשאתה מדבר על גילוי דיברת רק באפן כללי על פירוט וגילוי סיכונים? אני שואל על גילוי שהוא במהותו ספציפי וקשור לשיבוש ולאמצעי סייבר מול הגוף הציבורי הזה או מול החברה הזאת

יעקב יודקביץ

זה יותר קשור לדיווחים מיידים העניין הזה שאתה מעלה עכשיו. על זה עוד לא דיברתי. כמו שאמרת- בקשר לדיווחים מיידים, תקנות ניירות ערך מביאות בחשבון את זה שחברות יכולות להימנע בסיטואציות מסוימות מגילוי שיפגע בחברה. השתמשתם פה קודם במונחים שזה יפגע בהנהלה; זה לא בהכרח פוגע בהנהלה אלא פוגע בחברה ובבעלי המניות שלה.

שלומי שוב

אבל הם לא צריכים לבקש את רשותכם לזה?

יעקב יודקביץ

לא צריך לבקש את רשותנו.

שלומי שוב

זאת אומרת אתם בכלל לא מודעים לזה?

יעקב יודקביץ

לא. יש מקרים שאנחנו נהיה מודעים ויש מקרים שלא. תן לי לעשות סדר. קודם כל, חברות יכולות להחליט לא לדווח דיווח מידי בתנאי שהמידע עדיין לא נודע לאף אחד מחוץ לחברה, אם הדיווח המידי ימנע מהם להשלים פעולה שהם עכשיו באמצע לעשות. לכן תאורטית בהחלט יכולה להיות חברה שתגיע למסקנה שעכשיו היא מתמודדת עם איזשהו סיכון, נגיד משא ומתן עם איזה תוקף, ואם היא חושבת שאם עכשיו הנושא הזה יוצא החוצה היא לא תוכל להשלים את התהליך בצורה הטובה ביותר אז התקנות מאפשרות לה לעכב את הדיווח. גם לזה יש הגבלות מסוימות - אם היא רוצה לגייס כספים בזמן הזה או פעולות אחרות היא לא יכולה לעכב, אבל כן יש מסגרת שמאפשרת לעכב מידע וזה גם לא משהו שמצריך פנייה ספציפית לבקש את זה מרשות ניירות ערך.

אמיר ברנע

אבל יעקב, כמו במקרה שהעלית , אז החברה צריכה לדווח על זה בדיעבד. העובדה שלא ידוע לנו על אירועי מניפולציה, זה מכיוון שלא היו מקרים כאלו או שפשוט לא מתייחסים לנושא הגילוי המאוחר?

יעקב יודקביץ

היו דיווחים. ראשית, חלק מהחברות אם הן רואות אירוע שהמהותיות שלו היא מוגבלת הן מדווחות על זה בדוח השנתי ולא בדיווחים מיידים. זה נכון שדיווחים מיידים לא היו הרבה. לגבי חברות שלא מדווחות - דברים כאלה מגיעים לידיעתנו בזמן אמת ויש לנו גם פעילות מודיעינית שאנחנו עושים. אבל גם אם זה לא יבוא לידיעתנו בזמן אמת דרך פעילות מודיעינית, ובסוף במבחן התוצאה החברה תיפגע אז כמובן שהרשות תוכל לבוא ולאכוף על זה שלא היה גילוי בזמן אמת. אמרתם פה שהרשות לא עושה אכיפה, אם יהיו מקרים שיגיעו לידיעתנו וכמו שאמרתי אם ייגרם נזק בוודאי שזה יגיע לידיעתנו, אז תיעשה אכיפה.

שלומי שוב

אני חושב שנכון שאתם תקבלו לפחות דיווח על מצבים כאלו שחברה לא מדווחת בגלל נסיבות כאלו גם לפחות שאחרי שתעבור הבעיה תוכלו באמת לוודא שהגילוי ניתן וגם שזה לא נוצל לרעה, אבל זו דעתי.

יעקב יודקביץ

הפתרון לעניין הזה זה הוא שהתקנות אומרות שחברה ניצלה את הזכות הזאת לא יכולה לבוא סתם ולדווח אלא היא צריכה לדווח מתי זה נודע לה ולהסביר למה היא עיכבה את זה, וגם הרשות במקרים אחרים שאני לא אציין כרגע, התערבה גם בשנה האחרונה בתחומים של חברות שעיכבו דיווח ואחרי זה כשהן דיווחו לא הבהירו בדיוק מה הסיבה לעיכוב וממתי הן עיכבו. אבל בזמן אמת הרשות כמובן לא יכולה להיות מעורבת בכל מקרה שחברות מעכבות דיווח - דבר שהוא גם נפוץ. כן יש שאלה מה יקרה אם בסוף הדבר הזה הסתיים ובסופו של יום זה שום דבר מהותי; יכול להיות באמת שבסיטואציה כזאת החברה תחשוב שהיא לא צריכה לדווח.

אמיר ברנע

אולי זה לא קשור למחלקת תאגידים אלא לגופים אחרים ברשות ניירות ערך , אך שמירה על איכות המסחר ושמירה על הבורסה לניירות ערך בתור גוף.

שלומי שוב

לא לא, הבורסה זה הגוף הקריטי הוא מעליהם. המדינה הגדירה אותו כקריטי.

נמרוד, נשמח לשמוע ממך כמי שמלווה הרבה חברות את הזווית שלך.

נמרוד קוזלובסקי

אני רוצה טיפ-טיפה לתת לכם את נקודת המבט של מי שמלווה באופן רציף חברות בפן המשפטי של אירועי הסייבר. בואו נשים פרספקטיבה, אני חושב ש3 או 4 תובנות שעולות מתוך הדיון עד כה זה איך אפשר להתמודד עם אירועי הסייבר טוב ביותר. אתם אומרים לדווח, כי אנחנו מניחים שהדיווח הזה יאפשר כנראה כתוצאה מהשקיפות הזאת או לנפגעים הפוטנציאליים להתגונן או גם לשוק להגיב נכון לסיכון. שיתוף מידע – אנחנו מניחים ששיתוף מידע בין הגוף הנפגע לגופים אחרים כנראה יציב אותנו במצב טוב יותר כתוצאה משיתוף המידע להתמודדות טובה יותר גם לקולבורציה. וההנחה השלישית הנחה של שיתופי פעולה ההנחה היא שאני אעבוד טוב עם הרגולטורים עם מערך הסייבר עם כולם, תהיה פעולה מענה טובה יותר. לא נעים לי להגיד לכם, אבל חלק גדול ממה שמבקשים מעורכי הדין כל הזמן זה בדיוק לסכל את שלושת אלה. כמעט הפנייה הרגילה לעורך דין תדאג איך אנחנו יכולים לא לדווח, תדאג איך אנחנו יכולים לא לשתף את המידע שלנו, תדאג איך אנחנו יכולים לא לשתף פעולה עם הרשויות בחקירת האירוע. עכשיו יש פה בעיה מבנית שצריך לדבר עלייה, אני כבר 20 שנה חוקר את הנושא באקדמיה ושוב ושוב מסבירים את זה שPublic private partnership קולבורציה זה כי אני מקבל את הכל זה נכון מבחינת Security, בואו זה כי Information sharing נראה את המציאות ואני חושב שלומי הרבה פעמים בשיחות אני למד את זה, את המציאות לגבי

תמריצים שיש לצדדים ואת המציאות לגבי המבנה הארגוני שלהם או התרבות התאגידית שלהם. המבנה האמיתי הוא כזה שאין לאף אחד בארגון תמריץ – לא לדווח, לא לשתף מידע ולא לעבוד עם הרגולטור בשום דרך. למה? מכמה סיבות: א' הדבר הזה עושה אקסלרציה לאירוע שהרבה פעמים הוא אירוע שהיה יכול לסגור אותו בצורה קטנה, ב' יש המון השפעות הדף לאירוע, זה לא רק הדיווח לבורסה, זה שותפים וצדדים שלישיים וטריגר להפעלת ביטוח וטריגר שיש הרבה פעמים לחובות שיש לך מערכות הסכמיות גופים ממש רוצים להגדיר את זה שאין פה אירוע סייבר ולהימנע מלהפעיל את כל המערך הגדול הזה. ולכן אני אספר לכם מאחורי הקלעים מה שקורה ברוב הארגונים זה הדבר הבא – ישנו מערך שיטתי בתוך הארגונים שכל תכליתו למנוע מצב שמה שקורה להם כרגע יוגדר כאירוע סייבר. ישנה פשוט שיטה מבנית מבחינת המבנה הארגוני וגם מבחינת ההתנהגות שיש אירוע סייבר זה כנראה משהו שכולם יודעים עליו – מידע דלף, מידע שובש נפגע integrity של נתונים, אני אעיר לכם את מציאות, הארגונים שאנחנו עובדים איתם לפעמים יש להם כמה עשרות אירועי סייבר, אירוע שירביט לדוגמה זה אירוע שהוא כמעט קשקוש, זה אירוע שהוא קורה על בסיס יום יומי לחברות שמישהו פורץ למייל ומוציא נתונים פרטיים שלהם. אירוע של פגיעה מסוימת בintegrity של עסקאות קורה על בסיס יום יומי בגופים פיננסיים בארץ, אבל מה קורה? הגופים יצרו מנגנון שהוא מנגנון של governance אל תגדירו את הדבר הזה כאירוע. יש הרי את ההתראה יש את מערכת הsecurity יש לך את היכולת אם היית חוקר את האירוע יותר להבין שיש פוטנציאל שהייתה פגיעה אבל יש לי תמריץ גדול לא להפוך את זה לAlert ופה בסופו של דבר המערך שנבנה ברוב הגופים הוא מערך שמי שמקבל את ההחלטה האם יש לי אירוע סייבר או לא הוא האיש הטכני שמופקד בעצם על המערכת והוא גם זה שהרבה פעמים נמשך בזפת ונוצות אם האירוע התממש. אז לו אינטרס מאוד גדול שלא יוגדר אירוע סייבר ואין משהו במבנה הארגוני שייקח ויגיד רגע אתה חווה כרגע אירוע ולכן אני אגיד לכם את המציאות, לא 50% אלא כמעט 95% מהמקרים שמגיעים לתהודה התקשורתית בלית ברירה של הארגון ולא בשליטתו להחליט אם יש פה אירוע או לא, זה מצב שאני מספר לכם מהמציאות, זה טלפון מהכתב מהגארדיין שאומר שהוא עוד 5 שעות הולך לפרסם כתבה שהיה אצלך אירוע ואתה ניצב פתאום אל מול Crisis. זה מצב שבו התוקף אומר לך יש לך 72 שעות לשלם לי ואתה יודע שזה פומבי והדירקטוריון אומר לך חבר יש פה אירוע. זה מצב שבו חברת Security מדווחת לך שנפגעת. רוב הפעמים זו לא החלטה של הארגון להגדיר את הדבר כאירוע, הוא נאלץ להתנהל עם אירוע סייבר.

שלומי שוב

אז מה לדעתך הפתרון?

נמרוד קוזלובסקי

כנראה שהפתרונות נמצאים בכמה דברים. דבר ראשון, תחום שנקרא Corporate governance, בתחום שלך שלומי לדוגמה, בתחום הביקורת בנושא ראיית החשבון בנושא הניהול, יש הבחנה מאוד ברורה בין מי הוא הגוף המבקר לבין מי הוא הגוף המבוקר בשוטף שעושה את הדוחות. בעולם הסייבר אין את ההפרדה הזו, הגוף שמבצע את פעולת הסייבר הוא הרבה פעמים גם הגוף שמזמין את דוחות הביקורת ואת סקרי הסיכונים על עצמו, נותני השירותים תלויים בו ולכן הדבר האחרון שהם רוצים זה להתעמת איתו והוא גם הגורם שמחליט אם יש אירוע או לא. בעולם הראיית חשבון שלומי כמו שאתה יודע רואה החשבון המבקר אומר רגע, יש פה משהו שאני חייב להעיר עליו, בעולם הSecurity אין בעצם corporate governance. הדבר השני, זה בעיות אמיתיות שישנן ברגולציה, כי תבינו את הבעיה שיש לארגון, אם אני מדווח על האירוע אני פתאום חשוף לחקירות של הרשויות, אני חשוף להליכים האדמיניסטרטיביים, יותר מזה, אותו מידע בדיוק שאני אשתף את הרשויות ישמש לאחר מכן לעיתים להליך חקירה כנגדי בכובע השני של הרשות זה גוף אכיפתי. דבר אחרון שרוצה גוף במהלך אירוע זה לבוא כרגע לאחד מהרגולטורים של הרשות להגנת הפרטיות להגיד חברים הנה בואו תעזרו לי בחקירת אירוע מידע שלכם. הוא חושש שאוספים ראיות שלאחר מכן ישמשו כנגדו, ואין את המנגנון שקיים במדינות לאותה חסינות משימוש במידע הזה. הדבר הנוסף שהוא מאוד בעייתי, אני חושב ששלומי רמז על זה היום, הוא שחובות הדיווח מנוסחות באופן שכמעט יש את שיקול הדעת לארגון להגדיר האם יש לי אירוע, האם האירוע הוא מהותי, האם מה שקורה פה הוא כרגע בכלל אירוע, וכתוצאה מכך אנחנו רואים תת דיווח משמעותי או דיווחים חלביים לגמרי, דיווחים כמו "סיכון הסייבר משמעותי בסקטור שלנו ולכן אנחנו כמו גם אחרים מתמודדים איתו", דיווח שאין בו כלום. אם באמת סבורים שהמשמעות בדיווח, צריך לחייב את הדיווח כבר בכמעט ונפגע.

שלומי שוב

נמרוד הנהלים קיימים, זה עניין של יישום ואכיפה.

נמרוד קוזלובסקי

אתה צודק, אבל אני אומר לך בתוך ארגונים שלומי המציאות האמיתית, ארגונים יש להם תמריץ אדיר לא להגדיר דבר כאירוע, לא לדווח עליו. אני עושה סימולציות באופן רציף, התשובה החד משמעית בסימולציות האלה היא שארגונים עושים את הכל כדי שתוצאת האירוע בסופו תהיה שהם לא היו צריכים לדווח לאף אחד החוצה או לשתף פעולה עם הרשויות ושהאירוע הזה נסגר הרבה פעמים בתשלום הכופר או באיזושהי החלטה פנימית. גם ההחלטה אם סיימתי את האירוע, היא החלטה שיש להם תמריץ אדיר להגיד שהאירוע הסתיים, למה? כי אם לא, הם הרבה פעמים נמצאים

בחשיפה אל מול הלקוחות שלהם או מערכות הסכמיות. אם לא נשנה את המבנה של ה Corporate governance ואת מבנה התמריצים, ובוודאי את המבנה הרגולטורי לגבי שיתוף מידע אנחנו נמשיך גם הרבה פעמים להגיד מה חשוב ואיך נמנע להבא ואיך זה לא יקרה.

שלומי שוב

בואו נשמע את הילה קונפורטי שהיתה עד לאחרונה לא מעט שנים מנהלת הסיכונים של כלל ביטוח.

הילה קונפורטי

נאמרו פה הרבה דברים, אני אנסה נקודות שפחות העלו אותן. קודם כל, אתה באמת הזכרת את הנושא הזה שהסוגייה של הסייבר היא פחות באזורי הנוחות של מנהלי הסיכונים מבחינה מקצועית, רובם הם לא אנשי IT מומחים, ובהתאם לזה לא בהכרח הם מומחים מקצועיים לנושא הזה ולכן לדעתי יש פה סוגייה מאוד חשובה של שיתוף הפעולה בין מנהל הסיכונים ובין מנהל אבטחת המידע או הגנת הסייבר. כאשר אני בהחלט חושבת שלמנהלי הסיכונים יש כן תרומה משמעותית בהיבט של ניהול הסיכונים ומתודולוגיית ניהול הסיכונים אל הידע המקצועי הספציפי הטכני של מנהלי הגנת הסייבר. אפשר למשל לחשוב על הסוגייה שהוזכרה כאן של הנדסה חברתית של ההיבט האנושי, הסיכון האנושי שהוא מאוד משמעותי ביישום של מתקפות סייבר , הוא מאוד נושק לעולמות של סיכונים תפעוליים ובדרך כלל זה מקום שמנהלי הסיכונים יודעים להתמודד אתו בצורה טובה יותר מאשר מנהלי הגנת הסייבר ואני חושבת ששיתוף פעולה שלהם יכול מאוד לחזק את הטיפול בנושא הזה למשל. אותו דבר לגבי הנושא של בחינת האיומים והגדרת תאבון הסיכון במובן של לאיזה אירוע אתה מתכונן, וזה מתקשר למה שנאמר פה על אירועים מדינתיים. אני חושבת שספק אם באמת ניתן לחברה להתמודד בעצמה עם אירוע מדינתי וספק אם היא צריכה לקבוע בתאבון הסיכון שלה בכוחות עצמה להתמודד עם אירוע כזה. וזה באמת מכניס את הסוגייה הזו של איפה התפקיד של המדינה באירועים שהם אירועים מדינתיים שהם אירועים שחברה כשלעצמה לא יכולה להתמודד איתם כמו שחברה כשלעצמה לא יכולה לרכוש מערכת כיפת ברזל להגן על המפעל ואף אחד גם לא מצפה שהיא תעשה את זה. יש כאן קושי משמעותי ספציפי כי באמת הרבה פעמים בזמן אירוע לא יודעים אם זה אירוע מדינתי הזה ולכן חשוב להתייחס לכל אירוע משמעותי כאירוע שהוא בעל פוטנציאל להיות אירוע מדינתי וכן לקבל את התמיכה של המדינה והנושאים שהוזכרו כאן של שיתופי פעולה והשתתפות של המדינה בחיזוק הגנה לדעתי סופר חשובים.

אמיר ברנע

הילה, אמרו לנו כאן שיש הסתרה של האירועים האלה, נמרוד היה האחרון שדיבר על זה, אבל דיברו על זה כולם. איך חברת ביטוח מתמחרת ביטוח סיכוני סייבר אם האינפורמציה הזו לא קיימת, לא

יודעים לא את ההסתברויות ולא את הנזקים הפוטנציאליים שיכולים להיות בתרחישים , אז איך מתמחרים ביטוח?

הילה קונפורטי

קודם כל, אתה צודק שיש כאן סוגייה משמעותית של תמחור. לא שהתמחור נסמך על הדיווחים הפומביים בהכרח. הרי מה שקורה בחברות ביטוח זה שהן מקיימות ביטוח מסוים לאורך זמן, מהתביעות הן לומדות ועל בסיס זה הן מתמחרות. אז באמת, אתגר גדול זה שהביטוחים האלה הם ביטוחים חדשים ולכן, המידע שנצבר הוא מוגבל מלכתחילה וכשאתה מוסיף על זה את העובדה שמדובר בסיכון מתפתח ומתפתח בקצב מהיר אז תמיד יש את החשש שהמידע שעליו אתה נסמך גם אם אתה כבר בשנה שנתיים ונצבר לך מידע הוא לא בהכרח בסיס מספיק.

יש פה סוגיות ספציפיות בביטוחי סייבר שהן סוגיות לא פשוטות בכלל. מעבר לחוסר המידע והיכולת להסתמך עליו או מידע פחות רלוונטי בתמחור, יש פה גם סוגייה של סיכון קטסטרופה ששנייה צריך לדבר עליה. בסיכון סייבר יש פוטנציאל לסיכון קטסטרופה שבביטוח הוא מוגדר כהצטברות חריגה של אירועים. אם בדרך כלל חברה מתמחרת ביטוח על בסיס ההתנהגות הסטטיסטית של האירועים וההיקף שלהם, צבר חריג של אירועים נגיד רעידת אדמה בביטוחי רכוש הוא אירוע קטסטרופה מבחינת חברת הביטוח והוא דורש טיפול נפרד. יש פחות מודעות לעובדה שגם בסיכון סייבר יש בהחלט אפשרות לצבר משמעותי של אירועים וזה יכול לנבוע למשל מאירוע מתגלגל, הדבקה, כמו הסיפור של עמיטל שפרצו כנראה לחברה אחת וממנה לחברות נוספות ואז עם כל אלה הם מבוטחים של חברה אחת אז בבת אחת היא ניצבת עם צבר של אירועים ונזקים. זה יכול לנבוע גם ממתקפה רוחבית שראינו מתקפות כאלה בעבר וזה יכול לנבוע מניצול של חולשה במערכת מאוד שכיחה שמנוצלת בו זמנית על פני כמות גדולה של מבוטחים. אלה נושאים לא פשוטים בכלל וצריך לראות איך מתגוננים מפניהם. זה כנראה אומר שבמידה רבה צריך להסתמך על מבטחי משנה וגם להשתמש בכלים אחרים לניהול סיכון ביטוחי.

אמיר ברנע

זו אותה בעיה.

הילה קונפורטי

מבטחי המשנה נכנסו לעולמות האלה קצת קודם ויש להם יכולת טובה יותר לספוג סטייה בתוצאה לעומת התמחור.

שלומי שוב

הילה רצית להגיד עוד משהו מהזווית של מנהלי הסיכונים בחברת ביטוח?

הילה קונפורטי

כידוע לך אני כבר לא מנהלת סיכונים בחברת ביטוח, ולכן אפשר לדבר תאורטית. אני באמת חושבת שהדבר החשוב שצריך להגיד פה זה שמנהלי הסיכונים צריכים לראות את הסיכון הזה כחלק מהסיכונים שצריכים להסתכל עליהם בתוך תמונת הסיכונים הכוללת אחרת היא פשוט חסרה. והם חייבים להיות מעורבים במידה משמעותית יחד עם מנהל הסייבר ובעיקר הם צריכים להבין שהסיכון הזה בהיותו סיכון שמתפתח מאוד מהר, באופן מאוד דינאמי, הוא מחייב חזרה אליו בקבועי זמן קצרים, זה לא משהו שאפשר לעשות אותו אחת לשנתיים, צריך לחזור לזה כל הזמן ולרענן. הסיכון הזה כל הזמן מתפתח ואין ספק שבעקבות הקורונה הוא בעלייה מאוד משמעותית.

שלומי שוב

מיטל שכחתי לשאול אותך שאלה, בתוך קבוצה A, האם יש שונות בין לצורך העניין המוכנות של חברות הביטוח לבין המוכנות של הבנקים, הרי יש תפיסה כזאת שהבנקים יש להם מוכנות גבוהה יותר. יכול להיות שגם אפשר לגזור את זה מדוח הדיווח איפה הם מציבים את הסיכון. יש פערים בתוך קבוצה A?

מיטל אריק

אני חושבת שא' זו שאלה שנכון שהרגולטורים יענו עליה כי הם מגדירים את רמת ההגנה הנדרשת כרגולטורים.

שלומי שוב

כן אבל כל רגולטור את יודעת אין להם הם לא רגולטור אחד על שני הגופים.

מיטל אריק

הרגולטור צריך להגדיר את רף ההגנה מתוך ההיכרות שלו עם התהליכים, ההשפעות ההדדיות, הקשרים בין הגופים יכולת היתירות בכלל, רמת השירות שהוא דורש. בקשר שבין מערך הסייבר ובין הרגולטורים אפשר להסתכל על זה שהרגולטור אומר את ה"מה" צריך לעשות, מה הוא מצפה שיקרה, הוא לא אומר לארגונים איך לעשות את זה. בעניין הזה מערך הסייבר נכנס, הוא נותן את השכבה המקצועית וההכוונה ל"איך" – החל מתורת הגנה לארגון ועד הרזולוציות הנמוכות יותר של התראות הגנה ומענה במוקד 119. בהקשר זה שמחה גם לעדכן כאן שאנחנו נמצאים כרגע לקראת פרסום של תורת ההגנה החדשה שמערך הסייבר מוציא למשק שייחודה בהתאמה לזירה הישראלית, במענה עמוק לכל נושא ניהול סיכונים, באיתור וזיהוי הנכסים והתהליכים החשובים בארגון, מתוך ראייה של תוקף.

שלומי שוב

מיטל את יכולה להיות פוליטיקאית טובה - שאלתי משהו וענית לי על משהו אחר.

מיטל אריק

האחריות הייתה ותישאר של הארגון. על הנהלות ודירקטורים להבין זאת, להיערך בצורה הולמת ובהקדם לפני שיפגוש אותם יום סגריר. הרגולטורים הפיננסיים דאגו להציב דרישות ומצב המגזר ישתפר משמעותית אם תהיה עמידה בהן. למקרים בהם ארגונים לא נותנים מענה ומסכנים בכך ארגונים נוספים מתקיימת פעילות של המערך והרגולטורים על מנת לצמצם ולבלום את הנזקים.

עמית גל

שלומי, התייחסות במילה – אני רק רוצה לשים את הדברים לפחות מזווית המבט שלנו באיזה שהיא פרספקטיבה ובדיון על גופי A, אני רוצה להזכיר שאצלנו יש רגולציה שאני חושב שאפשר להגיד עלייה הרבה דברים אבל היא מתקדמת מאוד. שוב, הרגולציה בישראל היא ברמת פירוט גבוהה וכוללת דרישות משמעותיות. מנקודת המבט שלנו אני רוצה לשים רגע אמירה מאוד מאוד חשובה בפרספקטיבה, הרגולציה חלה על כל הגופים המוסדיים בלי להסתכל על גוף כזה או אחר ולעשות איזה שהוא תיעדוף, היא חלה על כולם במידה שווה ואנחנו מצפים מכל הגופים המוסדיים לעמוד בה. כשאני מסתכל על האכיפה שלנו ואוסף הכלים שיש לנו אנחנו גם מסתכלים על הגופים, אמנם יש גופים שיש להם אולי חשיבות יותר מערכתית ויש גופים יותר קטנים שבהם אנחנו גם נשקיע יותר משאבים. כלומר במסגרת תפקידנו, אנחנו פועלים לעמידה ברמה גבוהה בהנחיות הרגולציה של כל הגופים המפוקחים במסגרת הכלים שעומדים לרשותנו.

שלומי שוב

אני מסכים איתך. ליאה את רוצה להתייחס ממש בקצרה לפערים שהם פוטנציאליים בין הגופים ברמה A?

ליאה צור

שלום לכולם אני רק אגיד שאני הייתי 15 שנים שכירה כמנהלת סיכונים בתחום הבנקאות ומנהלת סיכוני הסייבר בתהליכים העסקיים, היום אני יועצת לכמעט כל הגופים בסקטור הפיננסי במשק אלו שכפופים לבנק ישראל ואלו שלא כפופים לבנק ישראל. ובהקשר הזה אני רוצה להגיד, אני אהיה פחות פוליטיקאית ממיטל ואני אגיד שיש פערים גדולים שלא נאמר גדולים מאוד שלא נאמר גדולים מאוד מאוד מאוד, בזכות זה שבעצם אני חונכתי לבנקאות שזה בעצם המקום עם סטנדרטים מאוד מאוד גבוהים ואני עכשיו מייעצת לעוד גופים אני רואה את הפערים שלפעמים אני אוהבת להקביל את זה

בין סוס ועגלה לבין מרצדס חדישה עד כדי כך בזווית הראייה שלי, צריך להגיד שהמפקח על הבנקים, הרגולטור, הוא רגולטור אחר מאוד שונה, אם זה מבחינת ההנחיות שלו, המפורטות, אם זה מבחינת האכיפה שלו ואם זה מבחינת איך הבנקים מתייחסים אליו כרגולטור, יש שונות מאוד מאוד גדולה ומישהו צריך להגיד את זה אז הנה אמרתי את זה.

שלומי שוב

אוקיי, תודה. זה חשוב שאנחנו מציפים את זה. מיכל שלמה היא סמנכ"לית AIG ישראל ואנחנו נשמח לשמוע את הזווית שאמיר העלה קודם של התמחור, החיתום של ביטוחי הסייבר.

מיכל שלמה

תודה שהזמנתם אותי באמת פורום מרתק.

כמה דברים לעניין ביטוחי הסייבר. אז דבר ראשון אני חושבת שביטוח הסייבר הוא החדשנות האמיתית של עולם הביטוח בשנים האחרונות והחדשנות היא שאנחנו לא רק רושמים את הצ'ק בסוף, בעוד זה שבביטוחים רגילים המבוטח הוא זה שיודע הכי טוב להתמודד עם השריפה והפריצה, בביטוחי סייבר חלק גדול מהמבוטחים CLUELESS כשהם נתקלים באירוע. בעולם הזה הביטוח מכסה לא רק את הנזק שנגרם לצדדים שלישיים, ואת הנזק שנגרם למבוטח, אלא גם עוזר לו להתמודד עם אירוע הסייבר, עומד לצידו ומסייע לו לנהל את המשבר. אנחנו ממנים מומחים מהשורה הראשונה לצד המבוטחים שלנו שנותנים להם ייעוץ משפטי דוגמת נמרוד (ד"ר נמרוד קוזלובסקי), ייעוץ טכנולוגי, ניהול משא ומתן עם התוקף אם נדרש, וייעוץ יחסי ציבור.

אני כל הזמן ממשילה את עולמות הסייבר לעולמות הסטנדרטים. כשאני מנסה לתמחר את פוליסת האש של המבוטח אני שולחת סוקר, סוקר שמסתובב בשטח ובודק את הסיכונים של המבוטחים. בעולמות הסייבר הייתי רוצה לשלוח סוקר טכנולוגי (ואני חושבת שאנחנו נהיה בעולמות שאנחנו נגיע לשם אבל אנחנו עוד לא שם). כרגע חברות הביטוח מסתייעות בכל מיני מודלים, בכל מיני חברות טכנולוגיה שמסייעות לנו להעריך את הסיכון, והסיכון בעצם נובע מכמה דברים:

מסיכונים פנימיים אצל המבוטח, במה הוא עוסק, לאיזה סקטור הוא שייך, בנוסף אנחנו אוספים מודיעין מכל מיני מקורות מידע שאנחנו יכולים למצוא (ברשת וברשת האפלה) וכ'ו.

במרבית הביטוחים היום בעיקר לגופים בינוניים אנחנו מתחילים מהשאלון, שואלים את המבוטח הרבה מאוד שאלות, כשהשאלות הן מתמקדות גם ברמת המערכות בהן הוא משתמש. דיברנו קודם על אירוע קטסטרופה למשל, כאשר אנחנו מעניקים למבוטחים כיסוי לנזק שנובע מספקים שלהם אז אנחנו ממפים את הספקים שלהם ובודקים אצלנו ברמת AIG כמה אנחנו חשופים לאותם ספקים ברמת סיכון קטסטרופה. אנחנו שואלים את המבוטח שאלות ומנסים לקבל מידע לגבי תכנית

המשכיות עסקית שלו ולגבי תכנית התאוששות ממשבר, רמת המודעות של הארגון, חינוך עובדים, הדרכות עובדים. אצל מבוטחים גדולים נעשות פגישות, שיחות עם הארגון, עם מומחים טכנולוגיים כדי להבין את הסיכון לעומק. חשוב לי מאוד להגיד שהביטוח לא בא להחליף את ההיערכות העסקית, את ההתמודדות עם הסיכון ופועל לצידה כצד משלים. חלק עיקרי מתקציב הארגון להתמודדות עם סיכון הסייבר צריך לפעול ברמת ההיערכות והכלים הטכנולוגיים והביטוח הוא רק השלמה לזה. מבוטח שלא יעמוד בתנאי הסף מבחינתנו לא יקבל הצעה לביטוח.

אנחנו נעים לקראת עולם שבו אנחנו נלווה את המבוטח בהתמודדות עם סיכון הסייבר, לא רק עם אירועי הסייבר, נשתף אותו באיך אנחנו רואים את הסיכון הזה, מניסיוננו בעולם בסטטיסטיקות, בחולשות שלו ובמוקדי החשיפה שלו. AIG פעילה בעולמות הסייבר כבר 20 שנה בעולם. אנחנו נשענים לא רק על הניסיון של AIG בישראל (שפועלת 8 שנים בביטוחי סייבר) אבל גם על הניסיון העולמי ובמדינות אחרות בAIG כבר עובדים מודלים כאלה.

כאשר כשאני מבטחת מבוטח בעולמות האש, רעידת אדמה, צד ג' וחבות מעבידים אני פוגשת אותו בעצם פעם בשנה שאני עושה לו ביטוח, בעולמות הסייבר אנחנו מדברים בסיכון דינאמי ולכן מאוד חשוב הקשר עם המבוטח לאורך כל השנה והיכולת לנטר את הסיכון.

אמיר ברנע

מיכל, היו אירועי נזק משמעותי בפועל?

מיכל שלמה

ודאי, בוודאי. גם בישראל וגם בעולם.

שלומי שוב

לפחות שומעים את זה ממישהו. לקח לנו שעתיים להגיע לזה.

מיכל שלמה

היו וקורים כל זמן, אני מוכרחה להגיד שמבחינת הסטטיסטיקה של AIG חומרת האירועים והשכיחות שלהם עלתה משמעותית מאז ה-Covid והעבודה מרחוק, זה אחד הגורמים המסבירים שאנחנו שמים פה אבל גם התוקפים נעשים מתוחכמים כל הזמן, התקיפות נעשות מתוחכמות כל הזמן, יש תקיפות להם יש TARGET ספציפי ולא רק מתקפות ריסוס. מתקפות הכופר הפכו להיות מכופר "רגיל" לDouble extortion זאת אומרת לא רק אנחנו מצפינים את הקבצים שלך אלא אנחנו גם אספנו מידע פרטי ואנחנו נפרסם אותו אם לא תשלם לנו את הכופר.

אמיר ברנע

מיכל, מבחינת הלקוחות הישראלים שלכם במגזר הפיננסי, ישנה פרמיה דיפרנציאלית?

מיכל שלמה

בוודאי, כששואלים אותי כמה עולה ביטוח סייבר אני אומרת שזה כמו לשאול "כמה עולה חליפה ליתום?". הפערים הם דרמטיים.

בעולם הסייבר כל מבוטח בוחר לעצמו איזה גבול אחריות הוא קונה זאת אומרת מה הוא מעריך שהחשיפה שלו תהיה בארוע נזק, וכמה הוא מוכל לשלם (פרמיה). יש לנו מבוטחים שקונים מיליון דולר יש מבוטחים שקונים מאה מיליון דולר גבול אחריות ויש שקונים מליון. אז כמובן יש שינוי בפרמיה שנובע מזה. כמובן הפרמיה מתחשבת בגודל הארגון, ברמת המוגנות שלו, ברמת המערכות שהוא משתמש, במודעות, כל מה שאמרתי קודם שהם פקטורים בשיקול הם פקטורים בתמחור. יש לנו מבוטחים שמשלמים עשרת אלפים דולר ומבוטחים שמשלמים מאות אלפי דולרים.

אמיר ברנע

ומבחינת הסקטור הפיננסי בישראל, יש לכם את הממשק עם הרגולטורים שמטפלים או או אתם עובדים מול החברה וזהו?

מיכל שלמה

אנחנו עובדים מול החברה אין לנו ממשק עם הרגולטור. השתתפנו בשולחנות עגולים של מערך הסייבר גם בתפקידי הקודם בחברת ביטוח אחרת מתוך האינטרס המשותף להעלות את רמת ההגנה. חשוב להגיד שסקר של מערך הסייבר אומר שרק (הסקר נערך ב2019) אבל רק 13% מהארגונים בישראל רוכשים ביטוח סייבר זה נתון מאוד מאוד נמוך, בעולם האחוזים הרבה יותר גבוהים.

אמיר ברנע

נאמר לנו קודם שגם באירוע שירביט הדבר הזה בא לידי ביטוי, כלומר עצם הגילוי של רשימת לקוחות ועל מה הם מבוטחים ואיזה פרמיה הם משלמים.איך את קובעת נזק? איך את מכמתת נזק שלכאורה דורש פיצוי, מצדיק פיצוי למשל בהקשר של גילוי בהבחנה ממניפולציה שבה הנזק יותר ברור.

מיכל שלמה

אני לא בטוחה שהבנתי את השאלה.

אמיר ברנע

אנחנו דיברנו על שני אלמנטים שיוצרים נזק, אחד עצם הגילוי: בא האקר ויכול לפרסם רשימת לקוחות שלך, בדיוק מה כל אחד ומה המאפיינים שלו וכ'ו, ודבר שני אפשרות של מניפולציה בנתונים שאתה צובר לאותו לקוח, העברה מחשבון לחשבון דברים כאלה. אבקש התייחסות לראשון, לעצם הגילוי. אני שואל את עצמי רגע, איך חברת ביטוח מכמתת נזק, נניח שאני לקוח של שירביט ופתאום עולה ההאקר הזה, פרסמו את שמי את העסקים שלי מול שירביט וכ'ו, איך מכמתים את הנזק?

מיכל שלמה

אז כשאנחנו עושים חיתום אנחנו מנסים להבין שני דברים. אמרתי קודם ואמרתי בקצרה- ביטוח מכסה נזק למבוטח עצמו ונזק לצדדי ג'. אנחנו מנסים להבין אחד, מה הנזק הפוטנציאלי למבוטח כתוצאה מהשבתת מערכות, ובעולם הזה שונים מאוד גופים יצרניים שנשענים על הטכנולוגיה בייצור שלהם והמערכות מושבתות. בצד השני אני מנסה להבין נזק פוטנציאלי מדליפת מידע ולהבין איזה מידע הארגון מחזיק ומה הנזק הפוטנציאלי, והנזק הפוטנציאלי יכול להיות כי אני גוף פיננסי שמחזיק הרבה מאוד מידע פיננסי, כי אני גוף רפואי שמחזיק הרבה מאוד מידע רפואי...כי אני גוף יצרני ואני מחזיק הרבה מאוד מידע על הלקוחות שלי ועוד.

שלומי שוב

ירידת ערך של מוניטין את לא עושה, נכון?

מיכל שלמה

דיברנו על זה אני ואתה, לגבי ירידת ערך של מוניטין. כאשר יש אירוע סייבר קבועה בפוליסה תקופת שיפוי בה אנחנו מבטחים, משפים את המבוטח על אובדן רווחים. ככל שבתקופה הזו אובדן הרווחים נובע ממוניטין יש לו כיסוי. אבל יכול להיות שאובדן המוניטין מתגלגל קדימה ובעוד שלוש שנים יש לו מחיר אין לזה כיסוי במסגרת הפוליסה.

שלומי שוב

דיברת על חברות טכנולוגיה שתומכות באמת בתהליך הזה של התמחור אז אנחנו הזמנו את שלום בובליל מחברת סטארט-אפ שמתעסקת רוב הלקוחות שלך שם הם בחו"ל אני מבין, אבל נשמח לשמוע על המתודולוגיה שלך.

שלום בובליל

אני מוביל את המוצר בחברה שקוראים לה קאבר ואנחנו מתעסקים בלסייע לחברות ביטוח וחברות ביטוח משנה בעיקר לכמת ולתמחר סיכוני סייבר. אני כן רוצה בעיקר להתייחס לאיך אפשר בכל זאת

לתמחר סיכוני סייבר אבל שמעתי לא מעט דברים עד עכשיו ואני כן אשמח טיפה להגיב. אז הדבר הכי חשוב שלי חשוב לציין ואני חושב שיש איזשהו פער בין המציאות לבין איך שאנשים רואים אותה זה שיש מידע. אפשר להמשיך לחזור אחר המנטרה שאין מספיק מידע בשביל למדל סיכוני סייבר, יש אינסוף מידע מה שאין זה ידע, וגישה לאנשים שיודעים למדל. אנחנו יודעים את זה כי אנחנו שנים עובדים בלתמחר ולסייע לחברות הביטוח שנושאות את הסיכון ולמבטחי המשנה שיושבים מאחור, להבין מה החשיפה הפוטנציאלית של עסקים ואנחנו מסוגלים לאמת את המודלים שלנו באמצעות אחד, תביעות שרואים זאת אומרת אירועי סייבר שקורים ובהם חברות הביטוח משפות על הנזק אבל מעבר לזה גם אירועים שקורים ולאו דווקא מובילים לתביעות זה עוד משהו שיכול לסייע במידול של הסיכון. דבר שני שאני רוצה לציין זה שאין דבר כזה פשוט מידול של סיכוני סייבר אני כן רואה את הבעיה הזאת כבעיה שמתחלקת לשלושה אלמנטים, הראשון זה באמת מה שנקרא Attritional losses התקיפות האלה שאנחנו רואים יום יום והן מבוססות על שיטות וטכניקות שהן פחות או יותר מוכרות ומובילות לרוב המוחלט של המקרים, החלק השני זה החלק של Large losses זאת אומרת אירועים שהם ייחודיים לא קרו בעבר אבל בפוטנציאל של דברים שניתן לחזות והחלק האחרון זה מה שנקרא אירועים קטסטרופליים, הילה נגעה בזה בצורה מאוד מאוד נכונה, הסיפור הזה של Single point of failure שזה יכול להיות Third party service provider איזשהו נותן שירות חיצוני שלאור איזושהי בעיה כשל אצלו במוצר או שהשירות יורד או שבעקבות תקיפה נוצר דלף של מידע למספר רב של חברות בנקודה אחת בזמן, האלמנט השני שיכול להוביל לקטסטרופת סייבר זה כל מה שקשור לחשיפה של איזושהי טכנולוגיה, חולשה שקיימת בטכנולוגיה שהיא מאוד פופולרית שהיא גם ויראלית אז אפשר לנצל אותה במקביל בהרבה מאוד מקומות במקביל נגיד כמו שקרה לפני מספר שנים בתקיפה של Notpetya מאחוריה עמדה מדינה אבל זה לא משנה מי עומד מאחורה מה שמשנה זה הImpact. הדבר השני שחשוב לי להעלות ולציין הוא שאני שמעתי הרבה מאוד התייחסות לגופים זרים, תקיפה של ממשלות, אני חושב שזה מאוד מאוד סקסי לדבר על התקיפות האלה, אני חושב שזה מאוד מתאים לנו כחברה להימשך לאזורים האלה של חסמבה וסוד מוחלט וכל הסיפורים האלה של איך מדינות וגופי ביון תוקפים, הרוב המוחלט של הנזק שאנחנו רואים הוא נזק שנובע מגופים שהמטרה שלהם הוא אינטרס כלכלי, להרוויח כסף, דיברנו על Covid אנשים נשארים בבית יש להם פחות הכנסות והדרך שלהם להרוויח זה פשוט לתקוף אבל לא רק בבנקים אני חושב שבהרבה מאוד מקומות חברות שיש להן כסף שיש להן הכנסה הן נהנות מכל מיני סיבות מTraction בתקופה של קורונה ויש כאלה שאין להם יושבים בבית ולכן אנחנו רואים יותר תקיפות.

שלומי שוב

תדבר על המתודולוגיה בכמה מילים.

שלום בובליל

אני כן חושב שיש איזושהי אבולוציה כל עולם הסיכון מתחיל בזיהוי ממשיך במניעה ובסוף מגיע לניהול. אבל איך אנחנו מצליחים להגיע למצב שאנחנו ממדלים סיכון סייבר בצורה שתאפשר למנהל בסוף להסתכל על Dollar value כמה כסף הוא הולך לאבד, מתחלק לשניים Frequency וSeverity ברמה הכי פשוטה שיש אנחנו צריכים לאסוף כמה שיותר מידע פירמוגרפי על הארגון, על העסק מה הוא עושה איפה הוא יושב Subsidiaries, את מי הוא משרת, איזה אפליקציות יש לו, אלו אמצעי אבטחה ולאחר מכן אנחנו יכולים בעצם להריץ איזושהי סימולציה שהתפקיד שלה זה לא לחזות מה יקרה בדיוק לארגון אלא לבחון באמצעות הרצה של סימולציית מונטה קרלו מה הם הנזקים שהם יותר שכיחים לעומת נזקים שהם פחות סבירים ולהוציא מזה איזשהו Accident probability care איזשהו גרף שמתאר בעצם את הסיכוי לחוות כל מיני רמות של נזק בהסתמך על אירועים שאנחנו מפיקים מהם האירועים האלה אמרתי ולהוציא מזה איזהשהו Exceedance probability curve אז אנחנו לוקחים מאה אלף אירועים שמייצגים בספקטרום של האירועים השונים שיכולים לקרות עושים תהליך של Reduction לבחור את ה10,000 אירועים שהכי רלוונטיים לעסק ואז רק מריצים את הסימולציה. למה זה מעניין וחשוב? כי זה מאפשר פעם ראשונה להסית את השיח מהדקויות האלה שאנשים מדברים עליהן בסוף סייבר ואבטחת מידע זה נושא לגיקים למיניונים לא למנהלים ומקבלי החלטות אבל מתי שמתחילים לדבר על כסף הכל משתנה. במקום לשרת חברת ביטוח הדבר האחרון שאנחנו עכשיו התחלנו לעשות זה לעבוד עם תאגידים מאוד מאוד גדולים ולאפשר להם לעשות פחות או יותר אותו דבר אבל במקום מנקודת המבט של המבטח אנחנו נותנים להם בעצם גישה למה תהיה החשיפה הפוטנציאלית שלהם, יש כאן איזהשהו בנק שאנחנו עובדים איתו זה בנק גלובלי אני לא אנקוב בשם אבל הוא פעיל בעיקר באירופה עם נוכחות מסוימת בארצות הברית ומה שמעניין בבנק הזה זה שהוא עבר תהליך של טרנספורמציה, אז אנחנו רואים שבעצם זה גוף שאנחנו ממדלים לאורך זמן אז אני יכול לתת לכם כאן את הטרנד ומה שאתם רואים כאן מאוד מעניין זה שבפעם הראשונה בעצם שאנחנו הרצנו ב2019 את הסימולציה שלנו הProbable maximum loss זאת אומרת האירוע עם הנזק הכי גבוה שהוא עדיין אפשרי שזה בעצם לקחת Return אחד ל-250 מתוך הסימולציה של העשר אלף ולשקף את זה, אז אתם יכולים לראות שסך הכל הנזק הפוטנציאלי שסקרנו שחזינו 1.4 מיליארד דולר שזה פשוט ענק אפילו לקבוצה פיננסית כזאת גדולה ואתם יכולים לראות שינואר 2020 אנחנו כבר מדברים על נזק של 360 מיליון דולר בProbable maximum loss

כמובן שאלו התרחישי קיצון שאנחנו באים למדל אם מדברים על הנקודה הזאת של Probable maximum loss של תרחיש קיצון אבל יש יכולת גם להתייחס לתרחישים שהם הרבה יותר שכיחים והנזק שלהם הוא הרבה פחות גבוה.

שלומי שוב

תודה שלום אין ספק שיהיה מעניין ליישם את המודל שלך גם על בנקים בישראל. אנחנו רוצים לסכם היה דיון מרתק, רגע לפני שאנחנו מסכמים דני רוצה להגיב לדברים שנאמרו

דני חחיאשוילי

קודם כל באמת דיון מרתק אתה אמרת את זה בדיוק לפניי, זה אחד, שניים, אני כן רוצה להתייחס לעניין הזה שנמרוד העלה לגבי הדיווחים, אני חושב שאני לא יודע לאיזה מגזרים הוא מתייחס אבל במערכת הבנקאית אנחנו לא רואים בעיה בזה שלא מדווחים או שגופים מנסים להתחמק מדיווח, הפוך, אני אגיד שאנחנו מקבלים די הרבה דיווחים גם במקרים שלא מחויבים דיווח אפילו לפי ההוראות שלנו וגם אם אנחנו לא מקבלים אותם אנחנו רואים את זה בדיעבד כשאנחנו באים לבנקים ואנחנו רואים את הדברים האלה, ולכן אם הם לא מדווחים זה אפילו יותר בעייתי מבחינתנו.

שלומי שוב

אבל אתה כרגולטור מקבל את הדיווח.

דני חחיאשוילי

אני כרגולטור מקבל את הדיווח, אני מקבל ואני אגיד עוד שני דברים בהקשר הזה, אחד כשאנחנו מקבלים את הדיווח אנחנו שני הדברים הראשונים שאנחנו מסתכלים זה ההשפעה של זה על כל המערכת ואם יש לזה השפעה על המערכת אז אנחנו פועלים בשביל שגם הגופים האחרים ידעו על הדבר הזה, ודבר שני אנחנו מסתכלים על ההשפעה על הלקוחות ואם יש השפעה על הלקוחות אז גם אנחנו פועלים שהדיווח יגיע ללקוחות כמה שיותר מהר בשביל שיהיו ערוכים ומוכנים לדבר הזה. אז סך הכל מבחינת הדיווחים זה עובד. אני אגיד אולי עוד משפט אחד בנושא הזה, שאני מסתכל על זה גם מבחינת הגוף, אני חושב שנכון שהוא ידווח על זה מבחינת ניהול הסיכונים שלו, מבחינת ניהול המוניטין שלו, הדברים האלה הם יוצאים בסופו של דבר ולכן חשוב שהגוף ידע איך לנהל את זה ואיך להוציא את זה בצורה נכונה בשביל לא ליצור פאניקה וזה האינטרס של הגוף בסופו של דבר לדווח וזאת התפיסה שלנו באופן כללי בנושא הזה, אני לא אתייחס לדברים האחרים אני מבין שהזמן קצר אז תודה היה באמת מאוד מעניין.

אמיר ברנע

לסיכום במילה, אני קצת מכיר את המערכת הפיננסית ואני שומע את סיפורי עלילות 8200 שמפורסמות בתקשורת, אתה שואל את עצמך רגע , יש איזה שהוא פער בהתייחסות לסייבר יחסית ליכולות הפריצה ולנזק שהן יכולות לגרום. . שמעתי כאן: אל תדאג המערכת בטיפול. יש מי שדואג, המערכת היא בבקרה, והדיווחים איכשהו מגיעים ולכן המוסדות הפיננסיים במיוחד בנקים וגם אחרים יודעים איך להגן על עצמם. עכשיו אני שואל אם זה כל כך מבוקר ושקט ורמת הסיכון כמו שאמרים לנו ירדה מ-1.4 מיליארד ל300- מיליון והכל בסדר. קיימת סתירה בין היכולות והשקט היחסי. אני שואל האם להיות רגוע כי הדוברים כאן מרגיעים שהסיכון בשליטה? להיות אופטימי?

שלומי שוב

אני פחות אופטימי ממך, לפחות ממה שאני הבנתי בין השורות, יש כאן דברים רגישים שלא ממש נאמרים באופן מפורש לדעתי – ובכלל מיטל אמרה שהמצב במשק לא טוב. שמענו גם היום שהמצב בביטוח הוא לא כמו בבנקים. ממה שאנחנו מבינים המצב בבתי השקעות למשל רחוק מלהיות טוב והם גם לא נמצאים בדרגה A יחד עם יתר המגזר הפיננסי שמיטל דיברה עליה, שזה מאד מדאיג.

אם אני צריך לסכם את הדיון על הנושא "הלא מהותי" שאנחנו מדברים עליו אני חושב שחייבים לחשוב על שינוי מבני, על משהו שבאמת יביא לאופטימום את הטיפול בנושא הזה שיחבר למעשה יותר בין סמכות ובין אחריות בלי לגרוע כמו שמיטל אמרה מהמומחיות שכמובן לכל רגולטור יש על הסקטור. אני חושב שאולי גם הסיפור של שירביט צריך להביא אותנו באמת לעשות את השינוי הזה ולייצר משהו שהוא יותר אחוד, תוך ניצול היתרונות. צריך להבין אין כאן יותר מידי זמן כי הדיגיטציה טסה ואנחנו חייבים לעבוד פה מהר. זאת אומרת כן צריך לקחת פה את כל הגורמים ולנסות לפחות בעניין הזה לשפר את המבנה ואתם יודעים שאני חושב שצריך בכלל לשפר את הרגולציה את המבנה של הרגולציה הפיננסית בארץ. מה שכן, חשוב לי להדגיש שהצורך החשיבה על שינוי מבני, לא גורעת מהאחריות של החברות והדירקטוריונים שלהן לנושא. האחריות נמצאת קודם כל על כתפי החברות והן חייבות להשתפר בנושא.

במקביל צריך לשפר את הנושא של זרימת המידע, לא יכול להיות שזרימת המידע תהיה כמו שנמרוד אמר כל כך סלקטיבית כך שלמעשה האינטרס הספציפי של החברה עולה על אינטרס המאקרו של המשק. צריך לראות איפה מוצאים את האיזונים. אני קורא גם לרשות ניירות ערך לקבל את הדיווחים, לפחות לעצמה כדי שתהיה בקרה על המידע למשקיעים מתי זה יוצא, מתי זה לא יוצא, מתי באמת יש רגישות מיוחדת וצריך להמתין - אבל אז זה צריך לצאת בדיעבד כי אנחנו לא רואים שהם גם יוצאים בדיעבד. נראה לי שהיה לנו דיון טוב ומקווה שלא רק אני רואה את זה - תודה רבה.

על הפורום:

מטרת "פורום שווי הוגן" Fair Value Forum (FVF), הפועל במסגרת התכנית בחשבונאות של בית ספר אריסון למנהל עסקים במרכז הבינתחומי הרצליה, היא לתרום לאיכות המידע בשוק ההון, ולייצר שיח מקצועי פורה בנושא. הפורום שמקיים מפגש חודשי, משמש קבוצת חשיבה שמייצרת דיוני עומק בסוגיות שנמצאות על סדר היום ומשמש פלטפורמה לשיתוף ידע, זיהוי בעיות, תהליכים ומגמות וכ- Best Practices למדווחים, לרואי החשבון ולמשקיעים.

הפורום, בייסודם של פרופ' אמיר ברנע, הדיקן המייסד של בית ספר אריסון למנהל עסקים, ורו"ח שלומי שוב, ראש תכנית חשבונאות וסגן דיקן, בית ספר אריסון למנהל עסקים, כולל מומחים מובילים מהאקדמיה ומהפרקטיקה בתחומי החשבונאות הפיננסית, הכלכלה והמימון וכן משתתפים בו נציגים של מדווחים, אנליסטים וגופי הרגולציה הפיננסית בישראל וחיבור בין תחומי הידע השונים.

סיכומי הדיונים שמתפרסמים לציבור הרחב מבוצעים על ידי הצוות המקצועי של הפורום המורכב מבוגרים מצטיינים של התכנית בחשבונאות.

אתר הפורום: www.fvf.org.il