גלובס
זירת העסקים של ישראל

כשאין 100% אבטחה, עדיף לעודד חברות לחשוף פריצות

לפני שרגולטורים רצים להעניש חברות שנפגעו מפריצה - שינסו לשתף איתן פעולה

עו"ד נתנאלה טרייסטמן 23/5/19

נדמה שאפליקציית המסרים המיידיים וואטסאפ תמיד היתה איתנו. מאז שפרצה לחיינו בסערה בשנת 2011 היא סחפה אחריה עוד ועוד משתמשים עד שהחליפה כמעט לגמרי את הודעות ה- SMS הוותיקות.

אחת הסיבות לפופולריות של וואטסאפ, היא שעל פי הצהרת החברה היא מיישמת ומטמיעה אמצעי הגנת מידע כברירת מחדל ומספקת הצפנה מלאה, מקצה לקצה, בזמן השימוש בשירות על ידי המשתמשים ואף משתמשת באמצעי הגנה נוספים. כלומר, מי ששולח הודעה בוואטסאפ יכול להיות סמוך ובטוח שאת המסר קיבל הנמען בלבד. בהתאם, אנו מתכתבים באפליקציה על הנושאים הכי אישיים ורגישים שלנו. אם רוב האנשים מתחלחלים מהרעיון שמישהו אחר יתעסק להם בטלפון הנייד, כניסה לוואטסאפ שלהם היא כבר טאבו של ממש.

אבל מה אם למרות הבטחת החברה ההודעות שלנו הגיעו לעיניים זרות? ואכן, הצהרות לחוד ומציאות לחוד, וכך הודיעה לאחרונה פייסבוק, הבעלים של וואטסאפ, כי התגלתה פרצת אבטחה באפליקציה וקראה לכל המשתמשים לעדכן לגרסה חדשה ומאובטחת יותר.

מעבר לתחושת אי הנעימות, האירוע מעלה שאלות מהותיות בדבר אחריותה של וואטסאפ לכך שההגנה מפני פריצה של תוכנת ריגול למערכת שלה כשלה. האם ומתי הרגולטור יקום ויקבע מהם גבולות האחריות של חברה כלפי משתמשיה? ומתי כישלון בהגנה על פרטיות המשתמשים יגרור סנקציות או קנסות?

הרגולטור האירופי, למשל, שחוקק את ה-GDPR שקובע קנסות גבוהים ביותר, הבין כי בשימוש באינטרנט ובטכנולוגיות שונות לא ניתן להגיע ל-100% ביטחון. בהתאם לכך הוא אינו יכול לדרוש מהארגונים להציע שירות שהוא בטוח לחלוטין בהיבט של אבטחת המידע, שכן הקנס שנקבע על הפרת חובות אבטחת המידע, נמוך יותר מאשר ביחס לחובות ההגנה על הפרטיות.

בשורה התחתונה, נראה כי גם אם החברות יבצעו את פעולות האבטחה האופטימליות, עדיין לא ניתן להבטיח כי יגיעו למצב בו יצליחו למנוע באופן מוחלט מהאקרים או חברות ריגול לפרוץ אליהן. המציאות הזו הזה הופכת את המשימה של הרגולטור לכמעט בלתי אפשרית, הרי אי-אפשר לאכוף הגנה שבאופן מובנה אינה יכולה להיות מובטחת ב-100%. מדוע חברה שעשתה כמיטב יכולתה צריכה להיענש?

צריך לחשוב מחוץ לקופסה - ולשנות את מאזן הכוחות הקיים: במקום שהרגולטור יעמוד מול החברות ויטיל עליהן קנסות וסנקציות, הוא צריך לשלב איתן ידיים.

מובן שבמקרה שחברה לא פעלה כדי להגן על הנתונים של המשתמשים באופן מקסימלי, היא צריכה להיקנס. אבל, מה קורה אם חברה פעלה כשורה והשקיעה באבטחת מידע ברמה המקסימלית ולמרות זאת נפרצה? הדבר המתבקש הוא שבמקום שהרגולטור 'יגלה' על הפריצה ויעניש את החברה, שהחברה תעדכן בעצמה את הרגולטור במה שקרה ותשתף אותו בפתרונות שננקטו וכמובן - לא תיקנס.

היתרון במצב כזה הוא שהרגולטורים, שלעתים קרובות עומדים חסרי אונים מול עולם הסייבר המתפתח בקצב מסחרר, יוכלו להיות יותר חכמים בזכות המידע שיקבלו מהחברות, והחברות אשר עד עכשיו פעלו מתוך אינטרס שהרגולטור לא יגלה על הכשלים שלהן, ישתפו אותו מרצונן.

ניתן לראות בארצות הברית שהרגולטור מתחיל להבין את זה. על פי החוק, אם חברה פנתה מיוזמתה ופעלה בשקיפות ובכנות מול הרגולטור והציבור - היא לא תיקנס, אלא אם נמצאו כשלים באבטחה שלה.

הכותבת היא שותפה במשרד יגאל ארנון ושות'. מתמחה בתחומי המשפט המסחרי, פרטיות והייטק.