בין טכנולוגיה לרגולציה

בעוד הטכנולוגיה שועטת קדימה ומאפשרת קיומם של מודלים יצירתיים לשמירה וניהול המידע הארגוני, הרגולציה בנוגע לאבטחת מידע בענן מתבשלת על אש קטנה. כיצד מתגוננים עד שהרגולציה תבשיל? | **יונית טל**

שירותי הענן, הפורחים בשנים האחרונות, מביאים מזור לבעיות עימן מתמודדים ארגונים שונים במשק, ובעיקר תורמים להתייעלות תפעולית וכלכלית. יחד עם זה, אחד החששות הגדולים המלווים ארגונים במעבר לענן הוא אובדן השליטה, המתבטא בעיקר באופן ההגנה על המידע ועל פרטיותו. המענה לחששות ולהתלבטויות אלה נע, כמו תמיד, בטווח שבין הטכנולוגיה לרגולציה.

"הגישה בעבר הייתה להחזיק את המידע ולנהל אותו בתוך הארגון, בהנחה שכך המידע מאובטח באופן מלא, על-ידי גורמים נאמנים לארגון", אומר **תומר בקשי**, מומחה אבטחת מידע ואחראי על תחום הענן בחברת **2Bsecure**, חברת הסייבר ואבטחת המידע של מטריקס. "לאורך השנים הגישה השתנתה וכיום ארגונים מבינים, כי התשומות הנדרשות מצידם להחזיק את כל המידע בארגון גבוהות מאוד, וכי שירותי ענן מקלים עליהם מקצועית, תפעולית וכלכלית. כחברה שמעניקה שירותי אבטחת מידע לארגונים, גם באמצעות מודל ענן, אני יכול להעיד, כי אנו מספקים מודלים עסקיים מגוונים, החל משירות ענן מלא ועד לפתרונות משולבים, אשר מאפשרים ללקוח לקנות פתרון תוכנה מסויים ולקבל את ניהול המוצר, את תפעולו השוטף ואת תחזוקתו כשירות ממחלקת הענן שלנו. מגוון המודלים להתקשרות שאנו מספקים רחב כך שאין חברה שלא יכולה למצוא אצלינו פתרון ההולם את צרכיה ואת תפיסת העולם שלה".

הדוגמא הטרייה ביותר העומדת לרשותינו היא מתקפות הסייבר החוזרות ונשנות שהתקיימו במהלך מבצע "צוק איתן" ואשר איימו על המידע של ארגונים רבים ומגוונים במשק. "במסגרת המבצע זיהינו וחסמנו באמצעות שירותי אבטחת המידע בענן אלפי מתקפות סייבר, על בסיס יומי. חלקן נועדו להשתלט על האתרים ועל מידע פרטי אודות הלקוחות של הלקוחות שלנו, וחלקן ביקשו לפגוע בזמינות האתר", מספר בקשי, "העוצמות הטמונות בשירות שלנו אפשרו לנו לשלוט בכל המתקפות ולהדוף אותן".

האם יש מגזרים להם מתאים יותר להשתמש בשירותי ענן?

"קל יותר להתייחס למגזרים להם פחות מתאים להשתמש בענן, ובראשם גופים ביטחוניים. אנו רואים כי גם החדירה של שירותי ענן לגופים פיננסים גדולים מתעכבת, אם כי לאחרונה יותר ויותר גופים פיננסים, ובהם בנקים בעולם, מתחילים להעביר מערכות מידע תומכות לענן. מוכן כי את מערכות הליבה שלהם הם עדין שומרים בבית".

מיחשוב ענן כמיקור-חוץ

הגוף האחראי על אבטחת המידע בישראל היא הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים (רמו"ט), האחראית, בין היתר, לאכיפת נושא הגנת הפרטיות והחקיקה הקשורה למערכות מידע בישראל. אך בעוד הטכנולוגיה שועטת קדימה ומאפשרת קיומם של מודלים יצירתיים לשמירה וניהול המידע הארגוני, הרגולציה, כך נראה, טרם הבשילה.

אז למה מחכים? שאלתי את נעמי אסיא, עורכת דין, מייסדת ושותפה בכירה במשרד עורכי דין ועורכי פטנטים נעמי אסיא ושות'. "נכון להיום החקיקה הישראלית בעניין זה מושתתת על חוק הגנת הפרטיות, שורה של תקנות והנחיות הנוגעות, בין היתר, להעברת מידע לחו"ל, החלפת מידע בין גופים ציבוריים ושימוש במיקור-חוץ לעיבוד נתונים הכוללים מידע אישי. אחד המסמכים החשובים לענין זה הינו הנחיות רשם מאגרי המידע 2/2011 לענין מיקור-חוץ לעיבוד מידע, מ- 2012", מונה אסיא את המסמכים המשפטיים הרלוונטים ומודה, כי "מאז ומעולם המשפט מפגר אחרי הטכנולוגיה. שירותי ענן היום נכנסים תחת המטריה הרחבה והמוכרת יותר של שירותי מיקור-חוץ. כך שכל מי שמתקשר עם ספק שירותי ענן צריך לקחת תקנות אלה לתשומת ליבו".

> במקרה בו המידע של הלקוח מאוחסן מחוץ לישראל, חלות מערכות החוקים של שתי המדינות, לצד החוק להוצאת ידע מגבולות ישראל וחוק פרטיות המידע. אך לא מן הנמנע, כי מערכות החוקים של שתי המדינות עלולות לסתור זו את זו

זה המצב היום, אך וודאי שזה לא המצב האופטימלי. למיחשוב ענן מאפיינים ייחודיים המבדלים אותו ממיקור-חוץ ואלה מעלים שאלות משפטיות מורכבות. למשל, אחד היתרונות הטמונים בשירותי ענן קשור לגמישות בשרתי האירוח וההתאמה המהירה לצורכי המשתמש. אך יתרון זה יכול להפוך לחיסרון כאשר הלקוח לא יודע באופן ודאי היכן מאוחסן המידע שלו בכל רגע נתון.

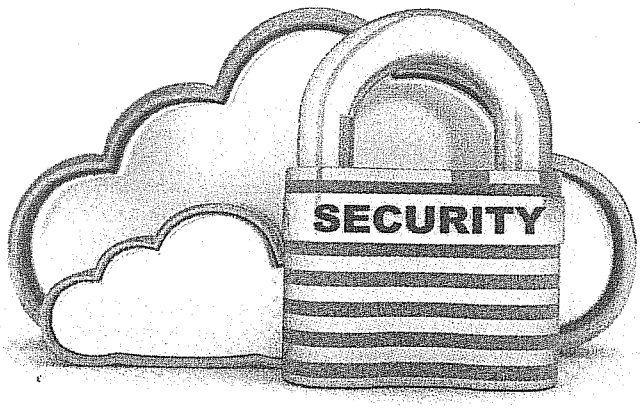
נשאלת השאלה, על-פי איזו מערכת חוקים יש לפעול כאשר הלקוח נמצא בישראל, אך המידע שלו מאוחסן בשרתים שונים ברחבי העולם? "המיקום הגיאוגרפי של הענן מעורר שאלות בעניין המשפט הבין-לאומי", מסבירה אסיא, "במקרה בו המידע של הלקוח מאוחסן מחוץ לישראל, חלות מערכות החוקים של שתי המדינות, זאת לצד החוק להוצאת ידע מגבולות ישראל וחוק פרטיות המידע. ואגב, לא מן הנמנע כי מערכות החוקים של שתי המדינות עלולות לסתור זו את זו".

החוק האמריקני מרתיע

ההבדלים בין מערכות החוק הנוגעות לשמירה על פרטיות המידע מתחדדים כאשר אנו מתבוננים במערכת החוקים של ארה"ב. "כאשר נפרץ שרת, או אתר אינטרנט, בארה"ב, ויש בו מידע על לקוחות, החוק מחייב את הארגון להודיע לכל לקוח ולקוח כי האתר נפרץ", מצביעה אסיא על אחד החוקים התומכים בפרט. "חוק זה אינו חל בישראל, אך כאשר מידע של חברה ישראלית מאוחסן בארה"ב החוק חל גם לגביה", היא מוסיפה.

חוק אחר מפורסם, וקצת פחות תומך, הוא חוק הפטריוט השנוי במחלוקת, אשר נחקק בתגובה לפיגועי ה-11 בספטמבר, ומעניק יד חופשית לרשויות אכיפת החוק, לאיסוף מודיעין בתחומי ארצות הברית. על-פי החוק, שנכנס לתוקפו ב-2002, רשאי ה- FBI לבצע חיפוש בדוחות כספיים, תכתובות דואר אלקטרוני ושיחות טלפון, כמו גם לקבל גישה לתיעוד פיננסי, ללא קבלת צו משפטי. "המשמעות של זה ברורה", אומרת אסיא, "חוק זה חל לא רק על חברות אמריקאיות, אלא על כל חברה ישראלית אשר המידע שלה מאוחסן בחוות שרתים ברחבי ארה"ב".

על רקע זה, יש כבר לא מעט דוגמאות בשוק של חברות שנמנעות מלהתקשר עם ספקי ענן המאחסנים מידע בארה"ב. לדוגמא, כבר ב- 2011 חברת BAE סיסטמס הבריטית, החליטה לוותר על שירותי תוכנת האופיס של מיקרוסופט הזמינה בענן, ה - Office 365 , משום שמיקרוסופט לא יכולה הייתה להבטיח, כי נתוני החברה לא ישונעו מאירופה לארה"ב וכך יהיו נתונים לביקורת תמידית תחת "חוק הפטריוט" האמריקני. מיותר לציין, כי ספקיות ענן אירופאיות משתמשות בחוק הפטריוט כגורם מאיים כנגד לקוחות הפוזלים לעבר המתחרות האמריקניות.



נעמי סיגר 14.9.14

בדצמבר 2009 הכיר האיחוד האירופי בחוק
נת המידע הישראלי ואיפשר לארגונים המ־
יקים במידע באזור האיחוד, להעביר
ונים הכוללים מידע אישי לישראל, מבלי שהדבר
ווה הפרה של הדירקטיבה של האיחוד האירופי
ניין הגנת מידע. בד בבד, ממש לאחרונה פירסם
מפקח על הבנקים טיוטא בנושא "ניהול סיכונים
זביבת מיחשוב ענן". על־פי הטיוטה יש היתר
נקים להוציא מידע מחוץ לגבולות מדינת ישראל,

להצביע על פתרונות טכנולוגים חדשים שנמצאים בפיתוח מואץ, ויש מקום להניח כי יכבשו את השוק בשנים הקרובות. אחד הפתרונות האלה הוא פתרון של הצפנת מידע והצפנת דרכי הגישה למידע. "יש היום פתרונות לשימור מידע באופן מוצפן כך שספק הענן, או כל גורם אחר בדרך, לא יוכלו לגשת למידע. יש לזה מחיר כלכלי, כמובן, שכן השירות הזה מאד יקר בינתיים, כמו גם, מחיר ברמת הביצועים, היות וההצפנה של המידע מאטה את תהליכי השליפה

דאי לחייב את ספק שירותי הענן לדווח ללקוח
כל מקרה בו שירותי הביטחון, או הרשויות
במדינה בה המידע מאוחסן, דורשים מספק הענן
לראות את המידע של הלקוח. כן רצוי לדרוש
מהספק להודיע ללקוחותיו על כל שינוי מהותי
בתנאי ההתקשרות בין הצדדים

ל ספקי ענן העומדים בדירקטיבות על הגנת מידע
במדינות האיחוד האירופי.

בינתיים, ותצפינו

בעוד הרגולציה מתגבשת ומתהווה לאיטה, ניתן

והעיבוד של המידע ברמת השימוש השוטף" מסביר בקשי. "הצפנת דרכי הגישה למידע פירושה הצפנה של התווך שבין הארגון לבין ספק הענן. הגישה למידע אינה מתאפשרת דרך האינטרנט, אלא דרך מערכת ביניים בדומה ל- VPN".

לעגן בהסכם

בעקבות החוק הישראלי הנוגע לשירותי ענן, המתאפיין באי־בשלות, ממליץ **ד"ר נועם וינבלט**, מנהל מחלקת ניהול סיכונים ורגולציה ב- 2Bsecure, חברת אבטחת המידע והסייבר של מטריקס, לעגן בהסכם ההתקשרות עם ספק הענן, כל נושא שיש לגביו אי־וודאות מבחינת החוק.

"למשל, כדאי לחייב את ספק שירותי הענן לדווח ללקוח בכל מקרה בו שירותי הביטחון, או הרשויות במדינה בה המידע מאוחסן, דורשים מספק הענן לראות את המידע של הלקוח (לדוגמה בארה"ב, בהתאם לחוק הפטריוט). עוד רצוי לדרוש מהספק להודיע ללקוחותיו על כל שינוי מהותי בתנאי ההתקשרות בין הצדדים. לדוגמא, לחייב את הספק לדווח ללקוח על שינוע המידע שלו לשרתים אזורים, במדינות אחרות. במקרה כזה, ניתן לאפשר ללקוח את הזכות לבטל ההתקשרות עם ספק הענן.

"כדאי לעגן מראש בהסכם ההתקשרות עם הספק גם עקרונות לסיום הקשר בין הצדדים", מוסיף ומציע ד"ר וינבלט. "כן מומלץ לקבוע עקרונות למחיקה, או העברה, של נתוני הלקוח מאתרי המיחשוב של הספק, מסגרת הזמן לביצוע העברת הנתונים, השיטה בה זה יבוצע והעלויות.

"חשוב גם להבין היכן נמצא המידע ומי הם השחקנים השונים בשרשרת האספקה. לפעמים ההתקשרות איננה בין לקוח לספק שירותי ענן בלבד, אלא בדרך מעורבים שחקנים נוספים העשויים להיחשף למידע של הלקוח", מרחיב ד"ר וינבלט, "לכן חשוב לנהל מראש את כל מערכת הסיכונים הכרוכה בהתקשרות כזאת, להבין לאילו תקנים, רגולציות ומערכות חוקים מציית כל הגופים בשרשרת האספקה, ואילו סעיפים צריך להכניס בהסכם ההתקשרות כך שהמידע של הלקוח יהיה מוגן מכל כיוון.

"עוד רצוי להתייחס בחוזה למיקום ולחוק השיפוט שיחול על החוזה, גם במקרה של סיום ההתקשרות ו/או במקרה של סכסוך בין שני הצדדים. מומלץ לקבוע מראש שורה של כלים והליכים, שיאפשרו ללקוח לעקוב אחר ההתנהלות של ספק שירותי הענן, כמו קבלת דוחות תקופתיים, שיפורי גירסאות תוכנה, עמידה בנהלי התאוששות מאסון וכו'", מוסיפה עו"ד אסיא. בסופו של דבר, הלקוח נותר אחראי לאבטחת המידע שברשותו גם כאשר המידע מאוחסן בענן ואינו מוחזק במערכות המידע בארגון. על־פי חוק ההגנה על הפרטיות מ- 1981 על הארגון לנקוט, מצידו, באמצעים הטכנולוגים להבטחת המידע ולוודא שהאמצעים הפיזיים עליהם מוחזקים הנתונים מוגנים כראוי. "היות והאחריות למידע חלה על ספק שירותי הענן כמו גם על הלקוח, במיוחד כאשר מדובר בתקיפות סייבר, אני ממליצה לשני הצדדים לרכוש פוליסת ביטוח", אומרת עו"ד אסיא.