Digital Whisper
Technologic Papers

על סוגיות מתקדמות בענן

מאת משה פרבר

הקדמה

חברת אמזון עמדה בפני סוגיה עסקית וטכנולוגית באמצע העשור הראשון של שנות האלפיים: העסקים היו מאוד עונתיים וכך גם הדרישה למשאבי מחשוב. כך לדוגמה לקראת בהלת הקניות של חג המולד היה נדרש כוח מחשוב רב עוצמה, אך בשאר ימות השנה משאבי מחשוב אלה נותרו לא מנוצלים. האגדה מספרת כי אז נרקם הרעיון (הרי אמזון היא ענקית הקמעונאות): בואו נמכור לצרכנים שלנו גם משאבי המחשוב ולא רק ספרים וצעצועים. רעיון זה הפך בשנת 2006 ל-Amazon Web Services, פעילות אשר מכניסה לאמזון, על פי ההערכות כמיליארד וחצי דולר בשנה (אמזון לא מפרסת את התוצאות הישירות של AWS). מהלך זה הפך אותה למובילת שוק התשתית כשירות (IaaS) וספקית של שירותי מחשוב למאות אלפי לקוחות.

זו הייתה תחילת דרכו של מחשוב הענן בצורתו הנוכחית כפי שאנו מכירים היום. כמובן שענן היה קיים לפני אמזון וכנראה היה מתפתח גם בלעדיה, אבל לא צריך להרוס סיפור טוב, גם אם אף פעם לא קיבל אישור רשמי של בכירי אמזון.

המטרה במאמר זה היא לסקור את הסוגיות החדשניות כיום בנושא מחשוב הענן מכמה זוויות: סוגיות משפטיות, שאלות העוסקות בממשל ורגולציה, וכמובן אתגרים טכנולוגיים וכל זאת מבלי לגרוע מיכולתה של טכנולוגיית הענן לשנות את הדרך בה אנו צורכים את שירותי המחשוב שלנו.

הערת אזהרה לפני שנתקדם: לא אסקור במאמר זו את אוסף ההגדרות הקלאסי של מחשוב ענן, אלא אעסוק בנושאים מתקדמים בלבד. מטרתי איננה לעשות סקירה נוספת של ההבדלים בין ענן פרטי לציבורי ולהסביר מהי תוכנה כשירות, פלטפורמה כשירות ותשתית כשירות - מושגים אלה מוסברים היטב ברחבי האינטרנט ואני ממליץ למי שאינו בקיא בהם להתעדכן אם ברצונו להפיק את המיטב ממאמר זה. לאורך המאמר אשתדל לציין על נושאים מסוימים לאיזה סוגים של מחשוב ענן הם רלבנטיים אך הבנה של המושגים עצמם הכרחית.

האתגר הראשון - ניהול החוזה

הנושא הראשון שנעסוק בו הוא הנושא המשפטי. יש לזכור כי מחשוב ענן הוא אולי אחד הממשקים היחידים בארגון המחייב את מחלקת המחשוב והמחלקה המשפטית לעבוד יחדיו על מנת לאתר את הסיכונים והמכשולים. לעיתים הדרך היחידה בה יכול הארגון לבצע ניהול סיכונים במעבר לענן הינה דרך בקרות חוזיות ו-SLA, במיוחד בסביבות SaaS.

בעת הקריאה, אנא זכרו כי מעבר להבנת המשמעות המשפטית, ברוב המקרים ללקוח יכולת מועטה לגרום לשינויים מהותיים בחוזה עם ספק ענן. היתרון העסקי של ספקי הענן הינו האחידות בשירותים ללקוחות. לצערי, רבים מהחוזים עם ספקי הענן לוקים בלשון מעורפלת ובחוסר בהירות לגבי תחומי האחריות והמחויבויות שלהם ללקוחות. למרות שישנם מאמצים רבים לשנות מצב זה (ל-HP ול-CSA יש פרויקטים בנושא שמטרתם להגדיר תחומי אחריות בענן), עדיין הדרך ארוכה עד מימוש החזון אשר מתייחס לרכישה של שירותי ענן כמוצר צריכה המעוגן בחוזה ברור דיו.

ניתן לחלק את הסוגיות המשפטיות בהן נתקלים לקוחות בעת מעבר למחשוב ענן לכמה נושאים:
סוגיות פונקציונאליות - מי אחראי על מה? ארגונים צריכים לזכור כי מעבר לענן לא פוטר אותם מאחריות למידע. ברוב הפרשנויות המשפטיות בעולם, לקוח הענן מוגדר כבעל המידע גם אם הוא מאוחסן בענן. אך מעבר לסוגית האחריות הכללית, יש לוודא בתהליך המעבר לענן כי חלוקת האחריות ברורה כגון: בבעלות מי ה-Meta Data אשר נוצר מעיבוד המידע? ומי אחראי לתהליכים מסוימים שאולי יתרחשו - כגון eDiscovery, מענה לצווי בית משפט (למשל לצורך חשיפת מידע), שמירה של המידע ולהבדיל, גריסתו.

שאלות חוזיות - בזמן החוזה יש לוודא כי מהלך החיים של החוזה ברור ומובן וכי מתקיימים בו תנאים לסיום לא צפוי של החוזה. סיכון ידוע במחשוב ענן הינו סיכון החתונה הקתולית עם הספק (vendor lock in). סיכון זה נגרם כתוצאה מבעיות טכנולוגיות או בעיות חוזיות. מטרתנו בחוזה היא לצמצם את החשיפה ע"י הגדרה ברורה של המשאבים אשר יהיו זמינים לצורך ייצוא המידע על ידי הלקוח בצורה שתבטיח לו המשכיות עסקית. מעבר לנושא זה, כל הנושאים החוזיים שהיו רלבנטיים לספק מיקור חוץ הינם רלבנטיים גם כאן עם התאמות שונות לגבי מחשוב ענן.

סוגיות של תחום השיפוט - נושא הגיאוגרפיה הינו נושא משמעותי מאוד בעת מעבר לענן. ולא רק כאשר דנים היכן יתבררו מחלוקות חוזיות. כאשר מידע ארגוני עובר בין מדינות יש לוודא קודם כל האם המידע היה רשאי "לצאת את גבולות המדינה" (האחוד האירופאי לדוגמה אוסר על העברה של נתונים אישיים מגבולות האיחוד למקומות בהם חקיקת הפרטיות מחמירה פחות) והאם חלים עליו תקנות ורגולציות אחרות במיקום החדש. חוקים אמריקאים שונים (כגון FISA ו-Patriot Act) עלולים לאלץ את ספק הענן (האמריקאי) שלכם להעביר את המידע שלכם לשלטונות האמריקאים ללא ידיעתכם.

להלן מספר דוגמאות לסוגיות משפטיות הייחודיות לארה"ב ולאיחוד האירופאי:

ארה"ב - הזכות לפרטיות נגזרת בארה"ב משלל חוקים פדרליים ותקינות ברמת המדינות השונות, אך הבסיס הינו התיקון הרביעי לחוקה הקובע זכות לפרטיות. כך למשל יכול אזרח אמריקאי להיות מוגן מפני חיפוש לא חוקי במחשב הביתי שלו בזכות התיקון הרביעי. אך, התיקון הרביעי, מתוקף הפרשנות שלו, לא חל על מסמכים אשר נשמרים בענן. חשוב להבין נקודה זו כי היא קריטית לכל הפרשנות המשפטית בנושא פרטיות במחשוב ענן ובכלל בארה"ב.

נושא נוסף שרלוונטי בארה"ב, הינו חובת מסירת מסמכים. המשפט האזרחי והפלילי בארה"ב נשען רבות על העיקרון כי הצדדים בבית המשפט מחויבים למסור לצד השני את כלל המסמכים הרלבנטיים לנושא המשפט. לקוחות הענן צריכים לזכור כי העברת המידע לספק ענן (גם אם בתיחום גיאוגרפי אחר) לא פוטרת את אחריות הלקוח למידע והוא עדיין יידרש בעת הליך משפטי לאתר את כל המסמכים הרלבנטיים לנושא. לקוחות ענן צריכים להיערך לאפשרות כזו מראש גם מהבחינה הטכנולוגית (לדוגמה, תהליך איסוף כזה בשרת דואר בענן מורכב הרבה יותר משרת דואר ארגוני) וגם מבחינת ההסכם עם הספק והכלים שהוא מאפשר לצורך תהליך זה. יש להבין כי במקרים מסוימים, במיוחד בעולמות התוכנה כשירות, הספק יכול לקבל זימון לדין כחלק מהתהליך המשפטי נגד לקוח מסוים, אך אותו תהליך משפטי יכול לגרום לחסימת שירות או לחשיפת מסמכי לקוחות אחרים, גם אם אינם צד בתהליך. זאת המשמעות האמיתית של "ריבוי דיירים" בסביבות ענן.

נושא אחרון שיש להבין את חשיבותו כאשר בוחנים סוגיות משפטיות במחשוב ענן בארה"ב, הינה העובדה שחוקים אשר חוקקו אחרי ה-9/11 מאפשרים לממשלה הפדרלית לבצע האזנה כמעט ללא צורך בצווים או הוכחות במיוחד כאשר המידע אינו שייך לאזרחי ארה"ב. חברות המבקשות להעביר מידע לשרתים בבעלות חברות ענן אמריקאיות צריכות לשקול את העובדה כי חברת הענן מחויבת לאפשר לממשלה הפדרלית גישה לשרתים שלהן ללא הודעה ללקוחות.

האיחוד האירופאי - האיחוד האירופאי הינו מוביל עולמי בהקשר של חוקי הגנת פרטיות, והוא משקיע רבות בהגנה על המידע של תושבי האיחוד וגם מידע של תושבים חיצוניים (בניגוד לארה"ב). החוקים באיחוד הם כה נוקשים עד שהם אוסרים כלל הוצאה של מידע פרטי מגבולות האיחוד (ליתר דיוק מחוץ לאזור הכלכלי האירופאי EEA) אלא במידה והוא יזכה לרמת הגנה זהה.

על מנת לאפשר לחברות אירופאיות להעביר מידע לחברות אמריקאיות ללא חשש מהפרה של חוקי הפרטיות, גיבשו לשכת הסחר של ארה"ב והאיחוד הסכם שנקרא Safe Harbor, שבו נקבע כי חברות אמריקאיות יקבלו אישור לאחסון מידע אירופאי לאחר הצהרה כי הן עומדות ב-7 קריטריונים של אבטחת מידע (Notice, Choice, Onward Transfer, Security, Integrity, Enforcement).

הסכם זה, שזכה לביקורות רבות עוד בעבר, קיבל זעזוע נוסף לפני מספר חודשים, כאשר הוועדה המייעצת לאיחוד האירופאי בנושא פרטיות ומחשוב (Article 29 Working Party), יצאה בחוות דעת שלילית לגבי שימוש בעקרונות Safe Harbor עבור מחשוב ענן (WP 196). בשורה התחתונה, הוועדה קבעה כי הסכמי Safe Harbor אינם מתאימים למחשוב ענן והמליצה על שורה של צעדים אשר לקוחות ענן ידרשו לבצע לפני העברה של מידע לספקיות שירותי ענן אמריקאיות. ההמלצות כוללות המלצות חוזיות וביצוע סקר סיכונים מקיף. להמלצות הוועדה אין תוקף מחייב כיום אבל אין ספק שהן מתוות את הדרך שהאיחוד האירופאי הולך לצעוד בה לגבי הגברת האכיפה בנושא הפרטיות. כיוון זה מהווה מכשול אמיתי לספקיות ענן אמריקאיות (וישראליות) ואין ספק כי יעכב את אימוץ טכנולוגיית הענן במישור הארגוני באירופה.

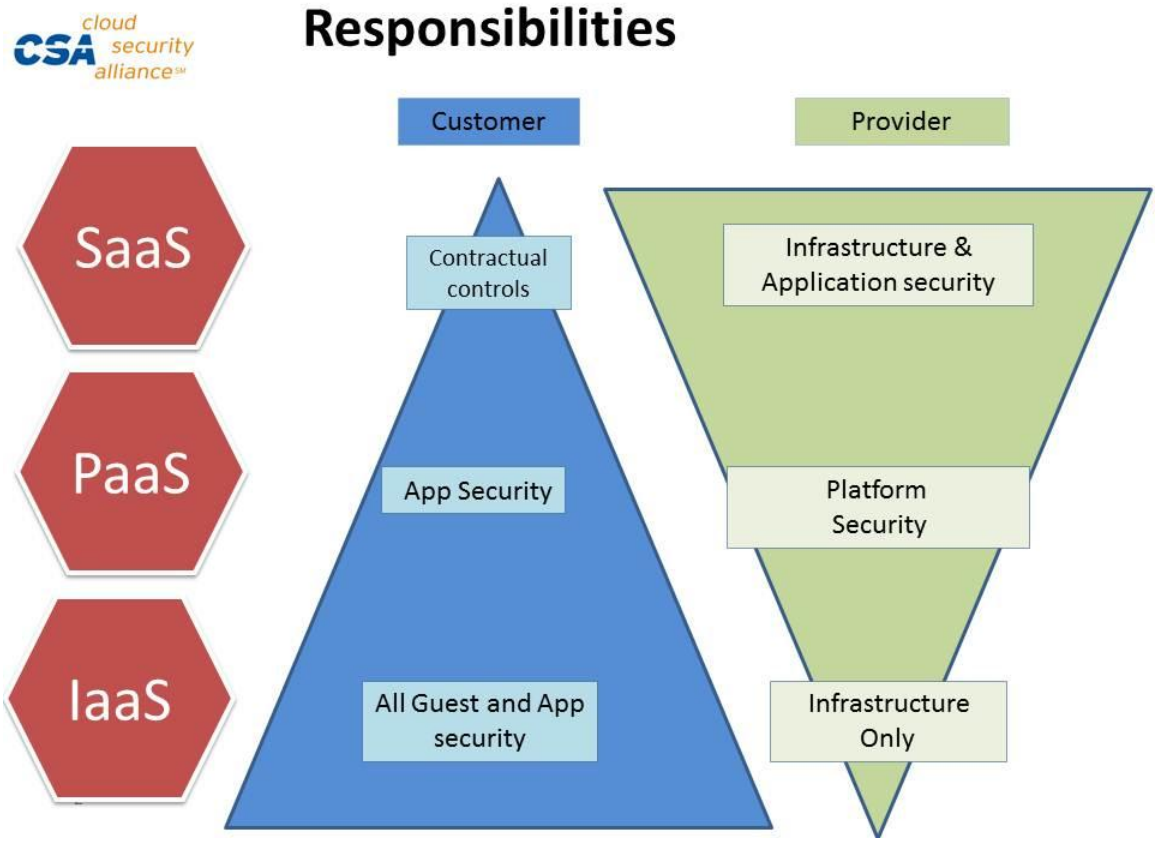
The Responsibility Matrix

כעת נדון בחלוקת האחריות בין ספק הענן ללקוחות הענן. בשביל להבין טוב יותר את נושא חלוקת האחריות, נחדד טוב יותר את שלושה סוגי שירותי הענן העיקריים הקיימים:

תוכנה כשירות (SaaS): תוכנה כשירות היא הסוג הפופולארי ביותר של שירותי ענן, וגם הקל ביותר להבנה. בתוכנה כשירות הספק אחראי על החלק הארי של היבטי אבטחת המידע והלקוח יכול בד"כ להסתמך רק על בקרות חוזיות לגבי השליטה במידע, למעט מספר כלים כגון ניהול משתמשים וביצוע בדיקות וסריקות.

פלטפורמה כשירות (PaaS): בסוג זה של ענן, הלקוח מקבל בנוסף על משאבי המחשוב גם סביבת פיתוח על מנת שיוכל להקים אפליקציות בסביבה זו. הלקוח לרוב יקבל סביבת ריצה, בסיס נתונים ושרתי web. (דוגמאות: Amazon BeansTalk, Force.com, Google Apps). בסביבה זו האחריות לרכיבי הפלטפורמה היא של הספק, ואחריות על האפליקציה עצמה היא של הלקוח.

תשתית כשירות (IaaS): תשתית כשירות הינה שירות הענן הבסיסי ביותר, בה הלקוח מקבל משאבי מחשוב (כגון מעבד, זיכרון, אחסון ורשת) ועל תשתית זו (שבאחריות הספק) הלקוח אחראי להתקין את המכונות הווירטואליות שלו אשר צורכות את המשאבים (דוגמאות: Amazon EC2, Rackspace, Google Compute).

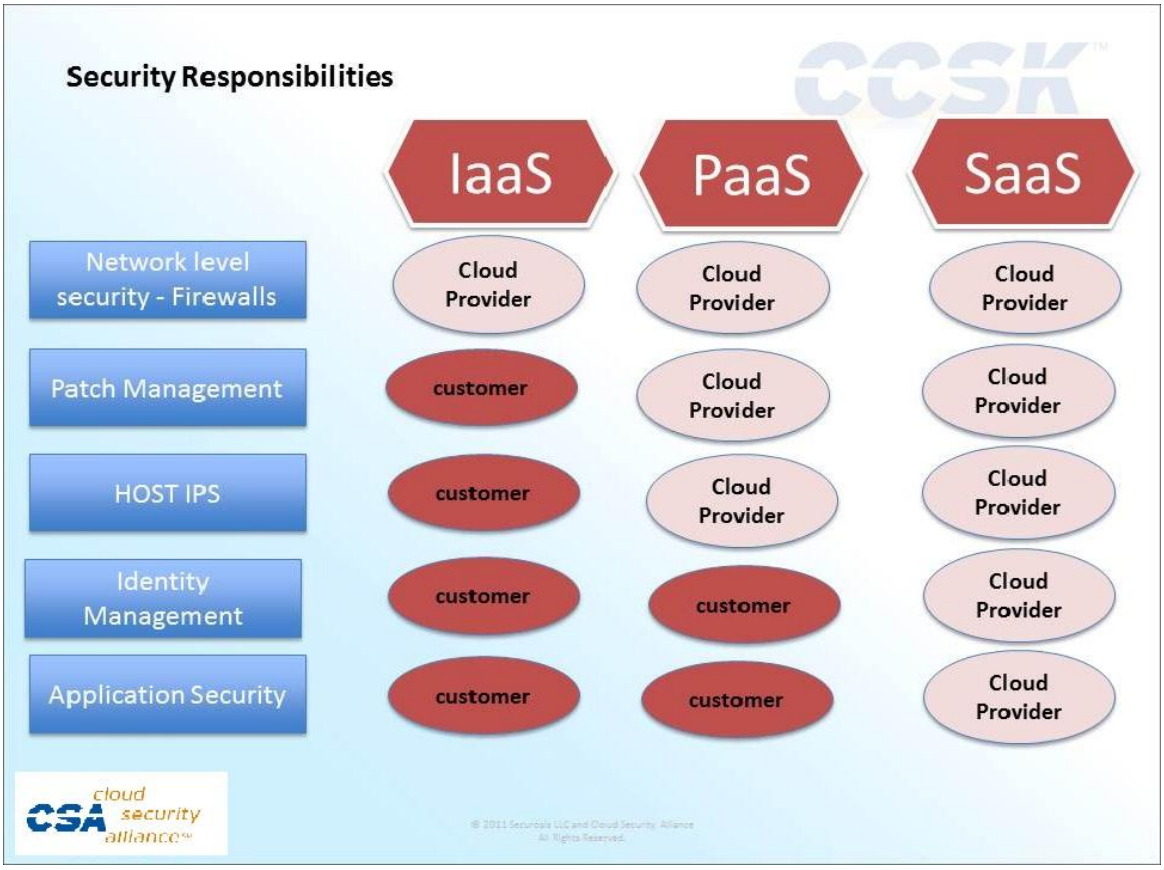


באופן כללי ניתן להגיד כי ככל שעולים ברמת השירות כך קטנים תחומי האחריות של הלקוח, וגדלה האחריות של הספק. השרטוט המצורף מדגיש היטב את השינוי באופי האחריות בהתאם לסוג השירות.

כמה מילים על אחריות

יש להבין כי אחריות (Responsibility) ניתן להעביר לגורמי צד שלישי, בניגוד לחבות (Accountability) - ועל כן, ארגון יכול להעביר חלק מפונקציות אבטחת המידע לארגון חיצוני, אך אינו יכול להעביר את החבות הכללית שלו (Accountability) להגנה על המידע. הבנה של תחומי האחריות קריטית בשלב תכנון העברה לענן. אנו רואים לקוחות של שירותי ענן במודל SaaS אשר אינם מפנימים את העובדה כי עליהם לעבור מעשיה טכנית של אבטחת מידע למצב שבו מנהלים סיכונים בכלים חוזיים ומבצעים הערכה במקום יישום בפועל, ומצד שני אנו רואים לקוחות העושים שימוש בתשתית כשירות ואינם מודעים לכך כי נדרש עליהם ליישם את הכלים המוכרים להגנת השרתים (הקשחות, הצפנות, אנטי וירוס, פיירוול וכו') בעצמם.

השרטוט הבא מתאר מספר כלי אבטחת מידע, ואת חלוקת האחריות בין הספק ללקוח:



לנושאים הבאים יש להקדיש תשומת לב מיוחדת כאשר מתכננים תחומי אחריות בין הספק ללקוח:

- **Penetration Tests & Vulnerability Scan** - הרוב המכריע של הספקים יבקשו כי כל בדיקה מסוג זה תתבצע בתיאום מראש. מדד טוב לבדיקת בשלות אבטחת מידע של ספק הינו מוכנותו לביצוע תהליך זה (באמזון לדוגמה ישנו תהליך מוגדר היטב לנושאים אלה) ויכולתו לספק גם מבדקים קודמים על התשתית שלו. שימו לב כי רוב הספקים הגדולים ישמחו לספק לכם אישורי הסמכה מוכרים ורלוונטיים (כגון הסמכת ISO27001, PCI-PA\DSS ועוד) ולצמצם במידה ניכרת את התיחום של הבדיקות שלכם. לכל סוג של שירות ענן (Paas ,Iaas, SaaS) יש לבצע תהליך נפרד של סריקה וסקירה. זכרו למשל שב-PaaS האפליקציה מפותחת ע"י הלקוח ועל כן הוא נדרש לשקול מימוש תהליך פיתוח מאובטח (SDLC) כמו בכל אפליקציה ארגונית אחרת.

- **Identity & Access Management** - זכרו כי בסביבות IaaS כל נושא ניהול המשתמשים הינו באחריות של הלקוח ועל כן הלקוחות נדרשים לחשוב כיצד תבצעו ניהול בסביבות אלו. ההמלצה הגורפת היא לעשות שימוש בכלים הקיימים בארגון ולעשות להם הרחבה לענן ולא "להמציא את הגלגל" מחדש. בסביבות SaaS מומלץ לבדוק איזה סט של כלים נותן הספק לביצוע זיהוי (SAML הינו תקן מצוין אם

ברצונכם לעשות שימוש בזהות הארגונית הקיימת) ויש לבדוק תמיכה בכלים נוספים לביצוע ניהול, מעקב ו-Provisioning. תקנים כגון OAuth ו-SCIM הופכים, אף הם, להיות סטנדרטים בתחום.

על הצפנות ובקרות אחרות

כעת נסקור את נושא ההצפנה שהוא קריטי למחשוב ענן. פתרונות ההצפנה לענן מתרבים והולכים עם מגוון רב של אפשרויות הטמעה וסוגים שונים של מימוש. לא נוכל לסקור את כולם כאן אבל נעשה סקירה של האפשרויות העיקריות בעולם זה. יש לזכור תמיד כי תכנון הצפנה מעלה מספר שאלות חשובות:

- **היכן נשמרים מפתחות ההצפנה וכיצד ניגשים אליהם?** ישנן מגוון פתרונות לנושא שמירת המפתחות, השאלה העיקרית הינה מפני איזה איום מתגוננים. לדוגמה, רוב ספקי הענן יודעים להציע כיום הצפנה ברמת שרת האחסון (Block storage), הצפנה זו הינה הצפנה סימטרית והמפתח שלה נשמר - אצל ספק האחסון. ברור כי זו הצפנה יעילה ביותר אם אנו חוששים מאובדן של מדיה, דיסקים או קלטות גיבוי, אבל הצפנה זו לא תגן עלינו במידה ואנו חוששים מספק הענן או מפריצה לאפליקציה (הצפנה זו הינה שקופה לשרת האפליקציה).

- **באיזה שלב של מחזור החיים של המידע אנו רוצים להצפין?** בד"כ אנחנו מדברים על:
  1. **Data in motion** - כאשר המידע מועבר אל המשתמש או אל אזורים אחרים.
  2. **Data in Rest** - המידע נמצא באמצעי אחסון נייח (בד"כ בבסיס הנתונים או בשרת האחסון).
  3. **Data in use** - המידע נמצא בשימוש האפליקציה / משתמש.

  בכל אחד מהמצבים המתוארים נדרש סוג שונה של הצפנה. לדוגמא כאשר מידע נמצא בתנועה יש להצפין את התווך בו נעשה השימוש ע"י שימוש בטכנולוגיות כגון SSL / VPN. אנו נתרכז בעיקר ב-Data in Rest מכיוון שהיישום שלו שונה בענן מאשר בסביבות מסורתיות.

- **באיזה טכנולוגיות ענן מדובר?** בתשתית כשירות ניתן לצפות מהספק במקרה הטוב ל- Block level encryption ופתרונות אחרים הינם באחריות הלקוח. במקרה של תוכנה כשירות הלקוח תלוי לרוב בתמיכה של ספק התוכנה בפתרונות הנדרשים.

ככלל, ננסה לחלק את סוגי ההצפנות לקטגוריות:

- **Storage level encryption** - הצפנה ברמת שרת האחסון. הצפנה זו שקופה לתשתיות ולאפליקציות. אך מפתח ההצפנה ברוב המוחלט של המקרים נשמר אצל ספק השירות.

- **Volume level** - הצפנה ברמת המכונה הווירטואלית, שיטה זה קלה ליישום בסביבות של תשתית כשירות משום שהיא נתמכת ברמת מערכת ההפעלה או אפליקציות שונות. אך אינה רלבנטית בסביבות של SaaS. האתגר העיקרי בהצפנה זו היא היכן לשמור את המפתח וכיצד לגשת אליו.

- **DB based encryption** - רוב בסיסי הנתונים מגיעים עם יכולות הצפנה ברמות שונות (שדה, טבלה וכו'), לפעמים בצורה מובנית ולפעמים באמצעות תוכנות צד שלישי. הצפנה זו יעילה מאוד בסביבות תשתית כשירות אך תלויה בספק השירות עבור בסביבות SaaS או PaaS.

- **Proxy based encryption** - שימוש בשירות חיצוני או במוצר צד שלישי אשר בעל יכולת לקלוט את התעבורה בין הלקוח לסביבת הענן, להצפין חלקים מהמידע או את כולו בשיטה זו ניתן למשל להצפין שמות לקוחות, מספרי כרטיסי אשראי ומסמכים עוד לפני שהם מגיעים לענן, בתצורת הצפנה זו המפתחות מחוללים ונשמרים ע"י הלקוח ללא חשיפה לספק הענן. פתרונות אלה קיימים כיום גם עבור סביבות IaaS וגם עבור SaaS ו-PaaS.

- **DRM** - פתרונות הצפנה ומתן הרשאות מסוג Digital Rights Management הינם פתרונות משמעותיים מאוד עבור ארגונים אשר שומרים מסמכי Office ו-PDF בסביבות ענן. במיוחד עבור אפליקציות כגון Google Docs, Dropbox ופתרונות ECM אחרים. מנגנוני DRM מאפשרים לקבוע ברמת הקובץ מי רשאי לעשות בו שימוש ובאיזה הרשאה. עם זאת פתרונות אלו כיום מתאימים למימוש ברמת קבוצות עבודה או תהליכים ספציפיים וקשה ליישמם ברמת ארגונית מלאה.

לסיכום

טכנולוגיית הצפנה היא רכיב קריטי במעבר לענן, הן משום שטכנולוגיות אלו נדרשות על ידי רגולציות ותקינות רבות והן משום שיישום נכון של טכנולוגיות אלו יכול להקטין בצורה משמעותית את הסיכונים בענן. כמו בכל טכנולוגיה, גם כאן נדרש להבין מה הסיכונים שמתמודדים עימם, מהי הרגולציה הרלבנטית ובאיזה מודל שירות של ענן אנו עובדים כדי לבחור את ארכיטקטורת ההצפנה הנכונה.

על המחבר

משה פרבר הינו ממומחי אבטחת המידע הוותיקים בישראל. בעל ניסיון עשיר בתחום אבטחת המידע ומומחה בנושא של ניהול זהויות, ניהול אירועי אבטחת מידע וטכנולוגיות חדישות נוספות.

בין היתר כיהן משה כמנהל תחום אבטחת מידע בקבוצת המוצרים של נס טכנולוגיות שם עסק במכירה והטמעה של טכנולוגיות אבטחת מידע מורכבות כגון IDM, SIM, DLP ו-Security for ERP. בעברו פיתח מספר קורסים עבור המכללות השונות בנושאי אבטחת מידע, ניהול סיכונים ורגולציה.
בשנתיים האחרונות משה מתמקד בהיבטים שונים של טכנולוגיות ענן, כיזם (חברת Cloud7 המספקת שירותי SECaaS) וכשותף בחברות ההזנק FortyCloud ו-Clarisite. כמו כן משמש מדריך מוסמך של ה-Cloud Security Alliance ועוסק בהדרכות של הסמכת CCSK למומחי אבטחת המידע בסביבות ענן בארץ ובעולם.