digital whisper
Technologic Papers

תקני אבטחת מידע במחשוב ענן

מאת שחר גייגר מאור

רקע - מהו "מחשוב ענן"?

מערכות המידע בסוף המאה ה-20 ותחילת המאה ה-21 מבוססות ברובן על מערכים ממוחשבים. ארגון ממוצע מוציא כל שנה כ-5% מסך ההוצאות התפעוליות שלו על מערכות מידע[1].

בתחילת שנות השמונים של המאה ה-20, כשהצורך במחשוב הארגוני נעשה נפוץ יחסית אך מחיר המחשבים היה גבוה ושכיחותם נמוכה, רוכזו חלק גדול משירותי המחשוב במרכזי שירות מיוחדים שבהם בוצעו רוב החישובים. בשנות התשעים חל מפנה במגמת המחשוב הארגוני ורוב הארגונים הגדולים החלו לרכוש בעצמם את רוב תשתית טכנולוגיית המידע ולהפעילה בתוך הארגון במרכזים מיוחדים (חוות מחשבים או datacenters באנגלית).

שיפור בהיצע פתרונות המחשוב לצד שיפור משמעותי בתשתית התקשורת ועליה בהוצאות על מחשוב הביאו בסוף העשור הראשון של המאה ה-21 לשינוי כיוון נוסף במגמת המחשוב הארגוני. על פי מגמה זו מוצעים רבים משירותי המחשוב כשירות. לפי מודל זה נמצאים המחשבים והתוכנות עצמן מחוץ לשליטת הארגון אצל ספק\י שירותים והארגון קונה את השירותים שבהם הוא מעוניין ומשלם על פי היקף הצריכה שלהם. חברת המחקר גרטנר הגדירה בשנת 2009 "מחשוב ענן" בצורה הבאה: "סוג של מחשוב, שבו טכנולוגיית מידע בעלת יכולת גידול וגמישות, ניתנת כשירות לפי דרישה להרבה לקוחות על בסיס תשתית האינטרנט"[2].

ציטוט זה מסתיר מאחוריו את אחד הקשיים הגדולים שאיתם מתמודדים אנשי מקצוע: העדר הגדרה רשמית ומדויקת למחשוב ענן. למרות שמדובר באופנה טכנולוגית שמלווה אותנו כבר כמה שנים, עדיין ניטשים ויכוחים לגבי המאפיינים וההגדרות שצריכים לחול על מחשוב ענן. מתי באמת מדובר במחשוב "ענן" ומתי מדובר בשירותי מחשוב הניתנים במיקור-חוץ? לא תמיד זה ברור. אולי מדובר באותה הגברת בשינוי אדרת?

---

1 - Computer Economics 2010

2 - Gartner, Experts Define Cloud Computing: Can we get a Little Definition in our definitions?, http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/

הביטוי "מחשוב ענן" - מקורו, ככל הנראה, מהצורה שבאמצעותה נהוג במקרים רבים לתאר את רשת האינטרנט בתרשימים טכניים כמעין ענן סכמתי[3]. עם זאת, אין מדובר במודל אחיד. מחשוב ענן מגיע במגוון "טעמים" והוא בנוי ממספר רבדים:

מודל "קובית הענן[4]" פותח על ידי פורום "יריחו" של ה-Open Group, קונסורציום גלובאלי אשר מקדם תקנים טכנולוגיים, כדי לאפיין ארבעה פורמטים של מחשוב ענן. על פי מודל זה לכל סוג ענן המאפיינים שלו, אפשרויות שיתוף המידע שלו, דרגת הגמישות שלו והסיכונים שלו. מודל קוביית הענן מחלק את המרחב לענן "פנימי" - אם אמצעי המחשוב נמצאים פיסית בתוך חצר הלקוח או ענן "חיצוני" - אם אמצעי המחשוב נמצאים מחוץ לגבולות הפיסיים של הלקוח. דוגמא: מערך אחסון וירטואלי בתוך רשת הארגון הוא ענן פנימי, בעוד שתשתית אחסון שנרכשה בשירותי הענן של חברת Amazon תהיה חיצונית.

חלוקה נוספת של הקובייה היא בממד הקנייני של טכנולוגיית הענן אשר בשימוש: טכנולוגיה "קניינית" היא טכנולוגיה ייחודית לספק מסוים וקשה עד בלתי אפשרי לצרוך אותה מספק אחר. טכנולוגיה "פתוחה" היא טכנולוגיה תקנית אשר ניתן לצרוך אותה ממספר ספקים תוך הקטנת התלות בספק מסוים. הממד האחרון מדבר על טכנולוגיות שמצויות בתוך ההיקף הלוגי של הארגון (Perimeterised Technologies), כלומר בתוך מעטפת של תקשורת מאובטחת. כך ניתן ליישם שירותים חדשים מבוססי ענן באמצעות פתרונות תקשורת מאובטחת (למשל VPN[5]) ולהאריך את גבולות יחידת מערכות המידע בארגון לשירותים נוספים מבוססי ענן. הכיוון השני הוא טכנולוגיות שנמצאות מחוץ להיקף הלוגי של הארגון (de-perimeterised technologies). שירותי הענן נמצאים מחוץ לגבול הלוגי של הארגון ולכן לא חלים עליהם אותם חוקי אבטחת מידע שחלים בתוך הארגון. המידע שיועבר לספק הענן ייעטף או שיורשה לעבור רק כ-Meta-Data כדי למנוע שימוש לא מוגן בו.

חלוקה אחרת של מחשוב מבוסס ענן מתארת את סוגי השירותים שניתן לספק על פי שכבות שירות[6]:

SaaS - תוכנה כשירות (Software as a Service) - היכולת הניתנת בידי הלקוח להשתמש ביישום אשר מופעל על גבי תשתית של ספק שירות ענן. הגישה ליישומים מתאפשרת ממגוון תחנות קצה באמצעות דפדפן אינטרנט או רכיב תוכנה המותקן על העמדה. המשתמש אינו שולט במאפייני התוכנה, בתשתית התקשורת, בשרתים ובמערכות הקשורות אליה, למעט תכונות מסוימות אשר הוגדרו כניתנות לשינוי.

PaaS - פלטפורמה כשירות (Platform as a Service) - היכולת הניתנת בידי לקוח להתקין על תשתית הענן מערכות. הלקוח אינו שולט בתשתית המתפעלת מערכות אלה, לרבות השרתים, האחסון והתקשורת שקשורים אליהן, אך הוא שולט ביישומים המופעלים על גבי תשתיות אלה.

3 - TechTarget, Cloud Computing, http://searchcloudcomputing.techtarget.com/definition/cloud-computing
4 - The Open Group, **Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration,** https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf
5 - Virtual Private Network - רשת תקשורת מוצפנת ומאובטחת
6 - Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing (National Institute of Standards and Technology Special Publication 800-145 7 pages (September 2011): http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

IaaS - תשתית כשירות (Infrastructure as a Service) - היכולת הניתנת בידי הלקוח להקצות, לעבד, לאחסן ולהשתמש במשאבים מחשוביים בסיסיים אחרים עליהם הלקוח רשאי להריץ תוכנות כרצונו. ללקוח אין שליטה על התשתית עצמה, לרבות שרתים, אחסון והתקני תקשורת, אך יש לו שליטה על כל מה שמותקן על תשתית זו.

חלוקה זו רווחת מאוד בקרב רוב אנשי המקצוע ומשמשת כשפה משותפת בדיונים, בכנסים ובפרסומים שונים בתחום. עם הזמן נוספו קיצורים נוספים אשר מתארים שירותים ספציפיים הניתנים כשירות כמו אחסון כשירות, אבטחת מידע כשירות ועוד[7].

הזדמנויות ואיומים הקשורים למחשוב ענן

מחשוב ענן הוא קונספט חדש ואינו מוכר יחסית אשר מגלם בתוכו הזדמנויות ואיומים. ניתוח ההזדמנויות והאיומים מאפשרים למי שמעוניין להעמיק את הידע שלו בתחום, לקבל סט כלים לביצוע ניתוח סיכונים ובחינת דרכי פעולה אפשריות לניצול קונספט זה לצרכיו.

הזדמנויות

שימוש בטכנולוגיות מבוססות מחשוב ענן מאפשרות למשתמש לעשות פעולות חישוביות מסובכות מבלי להתחשב בטכנולוגיה "מתחת". מחשוב ענן "תופס" את עולם מערכות המידע בנקודת זמן קריטית: ישנה הבנה בקרב אנשי המקצוע, כי התשתית ואמצעי המחשוב מגיעים לנקודת פיצוץ. כמות המידע הזמין, החיישנים הקיימים על כל התקן ומכשירים חכמים למיניהם מעמיסים על התשתית הקיימת. כמו כן, נפח השימוש בתקשורת ואחסון גדלים בהתמדה. במציאות זו מחשוב ענן מהווה גישה רעננה, גמישה ומשתלמת מבחינה כלכלית לחלק גדול מהאתגרים לעיל[8]. היתרונות הטכנולוגיים הטמונים בשימוש במחשוב ענן ניתנים לאפיון על ידי מספר קבוצות עיקריות[9]:

<u>שימוש בשירות עצמי ולפי דרישה</u> - מודל השימוש במחשוב ענן מאפשר לארגונים לבנות סביבות מחשוב גמישות ולהרחיבן בהתאם לחוזה ולהיקף העבודה הנדרשת. היכולת לשלם לפי השימוש מאפשרת לנצל בצורה טובה יותר את התקציב ולשנות את מודל הרכישה של מוצרים ושירותים למודל ליסינג, אשר נתמך על ידי ספקי הענן. מודל הענן מכיל יכולות וירטואליזציה מתקדמות אשר תומכות בשימוש לפי דרישה.

7 - Wikipedia, **Cloud Computing**, http://en.wikipedia.org/wiki/Cloud_computing#cite_note-1
8 - Elisabeth, Stahi et.al: Performance Implications of Cloud Computing (**IBM Corp. 2012**): http://www.redbooks.ibm.com/redpapers/pdfs/redp4875.pdf
9 - Marc Vael, **Cloud Computing Advantages -Why you should go for it** (A presentation by ISACA -Cloud Computing Task Force): http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/ISACA_Cloud%20Computing%20Advantages%20%28April%202011%29%20handout.pdf

יכולת השכפול של שרתים וירטואליים[10] ועקרון שיתוף המשאבים (אשר יוזכר בהמשך) מקלים מאוד על ספק הענן לתמוך בצריכה של לקוחות רבים משאבים דומים[11].

<u>גישה רחבה וזמינה מכל מקום</u> - אחד המאפיינים החשובים של מחשוב ענן הוא היכולת "להתחבר לענן" מכל מקום באמצעות האינטרנט. הכוונה היא לחיבורים סטנדרטים שנתמכים על ידי כל מערכות המחשב האישי ומכשירי הטלפון החכמים. אלה הופכים את שירותי הענן לזמינים ואטרקטיביים מאוד [12]. משאבי תקשורת רחבת פס הופכים בסביבת מחשוב ענן לתשתית קריטית עד כדי כך שכלל התפתחות התחום עשויה להיות מושפעת מקצב פריסת תשתיות התקשורת ברחבי העולם. נקודה זו אף עולה לא פעם כצוואר בקבוק אשר דורש טיפול והתאמה במקומות מסוימים בעולם[13].

<u>שיתוף משאבים</u> - כלומר, יכולתו של ספק הענן לשרת מספר רב של לקוחות באמצעות מנגנונים הנתמכים על ידי משאבים פיסיים ולוגיים אשר נפרסים ונסגרים על פי הדרישה[14]. בבסיס שיתוף המשאבים עומדות כמה מתודולוגיות וטכנולוגיות, כשהעיקריות שבהן הן: וירטואליזציה שהוזכרה למעלה וגם multi-tenancy[15]. שיתוף משאבים מעלה מאוד את יעילות השימוש במערכות ומאפשר לספק הענן ליהנות מיתרון לגודל (economy of scale) ושימוש חוזר בטכנולוגיה. תכונה חשובה זו מאפשרת הורדת עלות השימוש עבור הלקוח ומהווה יתרון גדול עבורו[16].

<u>הקצאה מהירה וגמישה של משאבים חדשים</u> - רשימת השירותים שניתנים להקצאה מהירה ללקוחות כוללת שירותי אחסון, יחידות עיבוד (CPUs), ממשקים ועוד. ספק ענן יכול, לדוגמא, לשנות את הקצאת אמצעי האבטחה שלו עבור לקוח מסוים לפי הצורך. הספק מגביל בצורה כזו התקפות על לקוחותיו במהירות וביעילות שאינן נחלתו של ספק שירותי אירוח לאתרים. היכולת להרחיב ולצמצם את המשאבים בצורה דינאמית ופשוטה מהווה יתרון מובהק לשימוש בטכנולוגיות ענן[17].

<u>יכולות אוטומציה מדידות, מבוקרות ואופטימליות</u> - תהליך של אוטומציה בענן עשוי להביא להורדת עלויות. את תהליך האוטומציה ניתן להשוות לייצור מכוניות בפס ייצור. בעבר היה נהוג לייצר מכוניות בפס ייצור אחד, כך שייוצרו הרבה מכוניות דומות יחסית. כך היה גם בענן: השירותים אופיינו בשונות נמוכה ובכמות

---

10 - שרתים אשר חלק ממערכות העיבוד, האחסון והחומרה שלהם משותפים, אך הם פועלים כישויות לוגיות נפרדות. על מכונה פיסית יחידה וייעודית לנושא ניתן להתקין כמה עשרות שרתים וירטואליים.

11 - SUN Microsystems, Introduction to Cloud Computing architecture (Whitepaper, SUN Microsystems June 2009): http://java.net/jira/secure/attachment/29265/CloudComputing.pdf

12 - IDC , Defining "Cloud Services" and "Cloud Computing" , http://blogs.idc.com/ie/?p=190

13 - U.S. House Of Representatives - Subcommittee On Technology And Innovation Committee On Science, Space, And Technology - Hearing Charter: *The Next IT Revolution?: Cloud Computing Opportunities and Challenges (*September 2011*):* http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/092111_charter.pdf

14 - Forbes, **The Economic Benefit of Cloud Computing**,http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/

15 - עיקרון ה-multi-tenancy מייצג שיטה לשיתוף שירותים בין מספר צרכנים שונים. עיקרון זה ניתן להדגמה כמעין "בניין משותף" שיש בו אזורים משותפים לכלל הדיירים ואזורים פרטיים לכל דייר לפי צרכיו. במחשוב ענן מקובל לראות בעיקרון זה הגשמה של חזון שירותי הענן הציבורי.

16 - Expert Group Report, **The Future Of Cloud Computing**, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

17 - Daniele Catteddu and Giles Hogben (editors): Benefits, risks and recommendations for information security (ENISA, 2009): http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

גדולה. כיום אין זה מספיק לחלק גדול מהצרכנים. הם דורשים התאמה אישית של השירותים שאותם הם צורכים מספק שירותי הענן. אוטומציה בעידן של מחשוב ענן צריכה לתת מענה לשני פרמטרים מרכזיים: יכולת שכפול גבוהה של שירותים ושמירה על מספר וריאציות גדול יחסית[18].

העקרונות שנימנו לעיל מאפשרים לצרכנים ליהנות מטכנולוגיות מתקדמות, ניצול משאבים ומחיר נמוך יחסית. מיצוי היתרון לגודל והעלות השולית הנמוכה עבור ספקי הענן מנגישים את אותן טכנולוגיות מתקדמות לכל דורש ומביאים במקרים רבים להורדת עלויות מחשוב עבור יחידים וארגונים כאחד.

איומים

לא קשה למצוא חששות הקשורים למחשוב ענן. מדובר בקונספט חדש ומורכב שהתפרסם אך לפני מספר שנים. כמו כן מדובר בתפיסה טכנולוגית מורכבת ומאתגרת ששונה מאוד מהתפיסה הרווחת בתחום המחשוב.

כיאה לאימוץ טכנולוגיה חדשה, צפוי כי האתגרים יהיו מגוונים מאוד וכדי למפות את החששות של אנשי המקצוע מהאתגרים שצופן מחשוב הענן, מתפרסמים מדי פעם סקרים אשר מפלחים את החששות על פי השיוך הטכנולוגי שלהן. במחקר שפורסם על ידי חברת IDC[19] בספטמבר 2009 התבקשו כמה מאות אנשי מקצוע מתחום טכנולוגיות המידע לדרג את האתגרים המרכזיים במחשוב ענן על פי רמת החשש. האתגר שממנו חוששים 87.5% מהמשיבים הוא נושא אבטחת המידע. אחריו הגיעו נושאים אחרים כמו זמינות הנתונים בענן וחשש מבעיות ביצועים של מערכות הענן[20].

החששות מסוגיות אבטחת מידע בענן המשיכו להטריד את אנשי המקצוע ובסקר שפרסם מגזין הטכנולוגיה InformationWeek בתחילת 2011 הוצגה תמונה דומה: בשלושת המקומות הגבוהים ברשימת החששות של 607 הנסקרים דורגו נושאים הקשורים לאבטחת מידע. נושאים אחרים כמו זמינות וביצועי המערכות, קריסה של ספק הענן, העדר בשלות טכנולוגית של תחום הענן ועוד נדחקו למקומות נמוכים יותר[21]. סקר נוסף של מגזין זה הצביע על המשך המגמה גם באוגוסט 2012[22].

מספר גופים בינלאומיים ניסו בשנים האחרונות לנתח את מתאר האיומים והסיכונים הקשורים לאבטחת מידע במחשוב ענן. בסוף 2009 פרסמה הסוכנות האירופית לתקשורת ואבטחת מידע (ENISA) ניתוח סיכונים למחשוב ענן ובו ניתנו ציוני סיכון למגוון איומים אפשריים[23]. מן הניתוח עולה, כי אכן, רוב האיומים

18 - Cloud Computing Journal, **Automating The Cloud,** http://cloudcomputing.sys-con.com/node/2025961

19 - http://www.idc.com/home.jsp?t=1354283013719

20 - IDC Research, **Cloud Computing 2010 -An IDC Update**, http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update

21 - Michael Healey: InformationWeek Analytics 2011 State of Cloud Computing Survey (InformationWeek, January 2011, Report ID: R1610111)

22 - Michael A. Davis: InformationWeek 2012 Cloud Security and Risk Survey (InformationWeek, August 2012, Report ID: R5080812)

23 - ENISA, **Cloud Computing Risk Assessment,** http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/

שקיבלו ציוני סיכון חמורים קשורים קשר ישיר להיבטי אבטחת מידע. בין שאר האיומים ניתן למנות את הגורמים הבאים:

בעיות זמינות ותקלות בממשקי המערכת - איומים שעשויים לנבוע מחשיפות הקשורות לתשתית הענן או לתווך התקשורת בין ספק הענן לצרכן. סיכונים אלה מקורם בכשל טכני בתשתית הענן, בכשל תהליכי בניהול התשתית או בנזק מכוון למערכות בידי גורם עוין.

ניצול לרעה של הענן - סיכון זה מתאר את החשש של הצרכן מניצול לרעה של תשתית הענן לגניבת מידע רגיש או לפגיעה אחרת. מקורות הסיכון יכולים לנבוע מאנשי תמיכה אצל ספק הענן ובמיוחד אנשי תמיכה בעלי הרשאות גישה חזקות למערכות המידע.

כשל בחציצה בין לקוחות - הזכרנו למעלה שיתוף במשאבי מחשוב. כמו שכבר צוין, היכולת הטכנולוגית לשתף משאבים מביאה להעלאת היעילות התפעולית במערכת ולהוזלת השירותים הניתנים לצרכן. למטבע זו צד פחות זוהר: תכנון לקוי של מערכות מחשוב ציבוריות עשוי להביא לתופעה של זליגת מידע בין שני "דיירים" על אותו רכיב ענני. כשל מהסוג הזה נגרם בסוף שנת 2010 ללקוחות שירותי הענן של מיקרוסופט (Microsoft BPOS\365). עקב תקלה בהגדרות המערכת יכלו חלק מלקוחות השירות לצפות בספר הכתובות של לקוחות אחרים. למרות שהתקלה תוקנה לאחר מספר שעות ולא נגרם נזק ממשי, האירוע הביא לגל פרסומים שלילי בתקשורת[24].

אי מחיקה של מידע - התקני האחסון אשר אוצרים היום את המידע שלי עשויים לשמש לקוח אחר מחר. מחיקה לא יסודית של הנתונים עשויה להשאיר שאריות מידע רגיש על התקני האחסון ולחשוף את המידע הרגיש לעיניים לא מורשות. אחת הסכנות הגדולות בנושא היא העובדה, כי אין כיום חוקים או רגולציות אשר מסדירים את נושא מחיקת המידע בענן. יתרה מזאת, גם אם כבר ניתנה הפקודה למחוק נתונים, ספק הענן יבצע בפועל את המחיקה בהשהיה מסוימת שיכולה לקחת ימים ואפילו חודשים וזאת בשל מתודולוגיית מחיקת המידע הנהוגה אצל רוב הספקים. העברה של מידע באופן ישיר בין ספקי אחסון בענן אינה אפשרית כיום. לקוח שמעוניין להעביר את המידע שלו מספק אחד למשנהו, עליו להעביר תחילה את המידע אליו ולאחר מכן להטעינו לספק הענן השני[25].

במרץ 2010 פרסם גוף בשם Cloud Security Alliance[26] עבודת מחקר מקיפה אשר מתארת את האיומים הבולטים במחשוב ענן. בדומה לניתוח הסיכונים שנערך ב-ENISA, גם במקרה הזה זוהו איומים הקשורים לניצול לרעה של מידע הקשור ללקוחות על ידי עובדים של ספק הענן, נושאים הקשורים לסוגיות אבטחה

24 - GNT, **BPOS: a data leak in Microsoft's cloud**, http://us.generation-nt.com/cloud-computing-data-leak-bpos-microsoft-news-2656841.html

25 - Computer World, **What happens to data when your cloud provider evaporates?,** http://www.computerworld.com/s/article/9216159/What_happens_to_data_when_your_cloud_provider_evaporates

26 ראו הרחבה על גוף זה בהמשך.

בממשקים בין הלקוח למערכות המחשוב בענן ואיומים הנובעים מטכנולוגיות שיתוף המידע אצל ספק הענן. עם זאת, מחקר זה זיהה מספר איומים חדשים אשר יש לתת עליהם את הדעת[27]:

ניצול לרעה של תשתיות מבוססות ענן על ידי גורמים פשיעה אינטרנטיים - בניגוד לכל האיומים האחרים אשר מסכנים מידע של צרכני שירותי הענן. איום זה מתייחס בפעם הראשונה לזהות צרכני הענן עצמם. על פי המחקר, הראשונים לאמץ את טכנולוגיות הענן הינם ארגוני הפשע הקיברנטי. אותם גורמים עלומים אשר אחראים לפריצות למחשבים, הפצת דואר זבל (spam), הפצת וירוסים וגניבת פרטי משתמשים למטרות כלכליות. דוגמא לכך אפשר לראות בשימוש שתוכנת פשיעה בשם Zeus עושה בשירותי הענן של חברת Amazon כתשתית גיבוי לניהול ושליטה ביישומי הפריצה שלה[28]. החשש הגדול במקרה הזה הוא שאותם גורמים עוינים ינצלו את תשתית המחשוב המתקדמת ועתירת המשאבים של ספקי הענן כדי לשכלל את ההתקפות שלהם. איום זה בא לידי ביטוי במספר מישורים:

- על ידי שימוש בטכנולוגיות מבוססות ענן, אותם גורמים עוינים נהנים מיתרון טכנולוגי יחסי על פני הקורבנות שלהם.
- הפעילות העוינת מוסתרת בצורה טובה מאוד בתוך התעבורה הכללית של ספקי השירות ומקשה עוד יותר על איתורה ומיגורה.
- שימוש בתשתית ענן על ידי גורמים עוינים עשוי להביא לירידה באמון לו זוכים ספקי שירות הענן. לקוח שמגלה מי "הדיירים" האחרים בענן שלו עשוי לחשוש עוד יותר מהעברת מידע רגיש לענן.

גורם הסיכון הלא ידוע - שימוש בתשתית ענן מביא, כמו שכבר הוזכר למעלה, לירידה בשליטת הארגון על מערכות המחשוב שלו. כתוצאה מכך עשויים להתווסף גורמי סיכון ואיומים שלא נלקחו בחשבון או שלא היו ידועים לארגון מבעוד מועד. גורמי סיכון שאינם ידועים מקשים מאוד על ניהול הסיכונים במערכות מחשוב מבוססות ענן ומורידים את רמת הביטחון שיש לצרכנים בשירותים אלה.

גורמי סיכון נוספים, אשר הוגדרו על ידי שני המחקרים לעיל כחמורים, מתייחסים להיבטי ציות לרגולציה. דוגמא לכך ניתן למצוא בסיכון העוסק בפערים בין הסביבה הרגולטורית שבה נתון צרכן משאבי המחשוב לבין הסביבה הרגולטורית שלה כפוף ספק שירותי הענן. פערים אלה יכולים לנבוע ממיקומו הגיאוגרפי של ספק שירותי הענן מול מיקומו של הצרכן והבדל במערכת החוקים בין שתי המדינות. סיכון אחר מתייחס לאובדן השליטה שעשוי לחוש הצרכן בעת העברת שירותי מחשוב לספק ענן חיצוני. על פי ניתוח סיכון זה עשויים להיווצר פערים בין נהלים פנים-ארגוניים במערכות המידע לבין התקנים הנהוגים אצל ספק הענן.

27 - Cloud Security Alliance, **Top Threats to Cloud Computing**, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
28 - ZDNET, **Zeus crimeware using Amazon's EC2 as command and control server,** http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110

ניהול סיכונים - מי לוקח אחריות על המידע שלי?

על פי ISO 31000, תקן בינלאומי המגדיר עקרונות והנחיות לניהול סיכונים, קיימות ארבע שיטות לטפל בסיכון במערכות עסקיות וטכנולוגיות לאחר שזה זוהה[29]:

- **הימנעות מסיכון** - אי נטילת הסיכון על ידי ביטול או מניעה של הפעילות העסקית.
- **צמצום הסיכון** - המתקת הסיכון על ידי בקרות ואמצעים שונים.
- **קבלת הסיכון** - ספיגת הסיכון והכלה שלו בפעילות השוטפת.
- **העברת הסיכון** - שיתוף הסיכון עם גורמים נוספים.

ניתן להסיק ממה שאנו כבר יודעים, כי מחשוב ענן מסייע לארגונים ופרטים רבים להתמודד עם סיכונים תפעוליים במערכות המידע שלהם על ידי צמצומם והעברתם לגורם חיצוני. במקרה הזה, לספק שירותי הענן.

כדי שהלקוח ירצה להעביר משאבי מחשוב לספק שירותי ענן, עליו להשתכנע שיש כדאיות במעבר זה, לרבות הורדת הסיכון הכרוך בהפעלת מערכות המחשוב. ספקי ענן מוכרים וגדולים משקיעים מאמצים ניכרים כדי לשכנע את ציבור הלקוחות שתשתיות ומערכות המחשב אצלם בטוחות, זמינות וזולות יותר בהשוואה לאלו אשר נמצאות אצל רוב הארגונים בעולם. כך, הן מקוות, יגיעו עוד ועוד לקוחות פוטנציאלים למסקנה שכדאי להם להעביר את הסיכון שבהפעלת מערכי מחשוב לענן[30]. תחזיות הצמיחה לתחום מחשוב הענן בהחלט תומכות בגישה זו ומראות צמיחה דו ספרתית נאה בשנים הקרובות[31]. עם זאת, לא הכל "ורוד" בענן, אך לפני שיוסבר מדוע, כמה מושגי ייסוד:

אחד המדדים החשובים שהוזכרו כחלק מסקירת ההזדמנויות בענן היה זמינות השירותים. ספקי מחשוב ענן מובילים בעולם מתגאים במתקני המחשוב המתקדמים שלהם אשר נהנים משרידות ויתירות חסרי תחרות אשר מגדילים את היתרון שלהם על פני השארת תשתית המחשוב בחצר הלקוח[32]. הדרך המקובלת כיום בתחום המחשוב לבדוק רמת **שירות** היא על ידי הגדרת חוזה רמת שירות בין הלקוח לספק (SLA - service level agreement[33]).

הדרך שבה ניתן להגדיר את רמת הזמינות של תשתית מחשוב היא על ידי מדידת זמן פעולת התשתית ללא כשל על פני יחידת זמן קבועה (uptime בעגה המקצועית). את ה-Uptime של מערכת מסוימת

---

29 - International Organization for Standardization, **ISO 31000:2009 Risk management -- Principles and guidelines**, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170 (Limited access)

30 - מספר דוגמאות למשיכת לקוחות לענן: http://www.rackspace.co.uk/cloud-computing/ , http://aws.amazon.com/tco-calculator/ , https://www.youtube.com/watch?v=C4Vn6cicdSA, https://www.youtube.com/watch?v=CjYNEjviRCY, https://www.youtube.com/watch?v=I-jmkkYiQac

31 - Seeking Alpha, **Cloud Computing Technology - Investment Strategy: IBM, Microsoft, Intel, Oracle, Amazon**, http://seekingalpha.com/article/889941-cloud-computing-technology-investment-strategy-ibm-microsoft-intel-oracle-amazon

32 - Google, **The Story Of Send**, http://www.google.com/green/storyofsend/desktop/#/hard-working-machines

33 - SLA Information Zone, **The Service Level Agreement** , http://www.sla-zone.co.uk/

מקובל לבטא כאחוז מהזמן שבו המערכת צריכה להיות זמינה. לדוגמא: uptime של 99.95% בחודש מבטא זמינות מערכת שיכולה **לא** לפעול עד 175 דקות בחודש עבודה נתון[34].

ספקי הענן המובילים מבליטים בפרסומים את נתוני ה-SLA וה-uptime שלהם כדי למשוך לקוחות ומשקיעים, כאמור, כסף רב בתשתיות שיעמדו ברמת שרידות וזמינות גבוהות ביותר, תוך זיהום מינימאלי של הסביבה ושמירה על סטנדרטים גבוהים של אחריות סביבתית[35]. עם זאת, בשנים האחרונות פורסמו מספר ידיעות על קריסות מקומיות של שירותי ענן מובילים כמו Gmail[36], שירות התמונות Instegram, שירות Netflix[37], שירותי הענן של חברת Amazon ואחרים. מקרים אלה עשויים להרתיע חלק מהלקוחות הפוטנציאלים מלנסות שירותי ענן[38].

סוגיה חשובה אחרת היא השמירה על פרטיות בענן. זליגה של מידע בין לקוחות שונים בענן הוזכרה כבר במאמר זה בהקשר של חולשה או כשל טכנולוגי במערכת מחשוב מבוססת ענן. מה לגבי אי שמירה על פרטיות כחלק ממדיניות או חוסר תשומת לב ספקיות שירותי הענן? בעבודה שערכה אלכסנדרה קורולובה (Korolova) היא הצליחה ביחד עם עמיתיה להציג ולהדגים פרצות במדיניות הפרטיות של Facebook שאפשרו ניצול לרעה של הפלטפורמה החברתית וממשק המפרסמים על מנת להשיג מידע פרטי על לקוחות הרשת. קורולובה גילתה במחקר שעשתה כי מתקיף יכול להתחזות למפרסם, להיכנס לממשק הפרסום של Facebook ולהגיע למידע פרטי רב, לרבות מידע שהוגדר על ידי המשתמשים כ-"שלי בלבד" (Only Me) ומידע עבור "חברים בלבד" (Friends Only)[39]. דוגמא זו, אף שהיא מתייחסת לרשת חברתית באינטרנט, מתארת בצורה טובה חשש קמאי שקיים בקרב רבים: מי באמת ערב למידע שלנו, כשאנחנו מפקידים אותו בידי גוף זר ודומיננטי כמו ספק שירותי ענן? מי מפקח על אותו ספק ויוכל להשקיט את החששות שלנו כלקוחות?

לקוח שירותי ענן, בין אם הוא פרטי ובין אם הוא מייצג ארגון, עשוי להגיע למצב שבו הוא נדרש לספק מידע פרטי כחלק מדרישות ספק הענן[40]. יש להדגיש כי חשש זה נוגע לכל פיסת מידע פרטית שאנו כלקוחות מעבירים לגורמים חיצוניים כמו מוסדות שלטון ורשויות החוק ולכן הוא מועצם כשאנו בוחנים טכנולוגיה חדשנית כדוגמת מחשוב ענן. לספקיות שירותי הענן, במיוחד לאלה אשר אינן גובות תשלום עבור השירות שהן מספקות, יש מעט מאוד מוטיבציה לשמור על הנתונים של הלקוחות שלהן באמצעות

34 - The Monitoring Guy, **Service Availability Reporting**, http://themonitoringguy.com/articles/service-availability-reporting/
35 - Microsoft News Center, **Microsoft's Quest for Greater Efficiency in the Cloud**, http://www.microsoft.com/en-us/news/features/2011/apr11/04-19greendatacenters.aspx
36 - BostInno, **Gmail Outage: First GoDaddy, Now Gmail is Down for Some Users Today,** http://bostinno.com/2012/09/10/gmail-outage-first-godaddy-now-gmail-is-down-for-some-users-today-report/
37 - CNN, **Instagram down in mass power outage**, http://news.blogs.cnn.com/2012/06/30/instagram-down-in-mass-power-outage/
38 - Computreworld, **Amazon outage sparks frustration, doubts about cloud,** http://www.computerworld.com/s/article/9216098/Amazon_outage_sparks_frustration_doubts_about_cloud
39 - Aleksandra Korolova: Privacy Violations Using Microtargeted Ads: A Case Study (Journal of Privacy and Condentiality Volume 3, Issue 1, 2011 , Pages 27-49)
40 - Siani Pearson: Taking Account of Privacy when Designing Cloud Computing Services (HP Laboratories, HPL-2009-54: http://www.gtsi.com/eblast/corporate/cn/09_09_2009/PDFs/HP%20Lab.pdf)

הצפנת התקשורת למשל או באמצעי הגנה אחרים. בניגוד למוסדות פיננסים, אשר מחויבים לתת דין וחשבון לרגולטור ולחוק ועל כן משקיעים מאמצים גדולים באבטחת המידע של לקוחותיהם, ספקיות שירותי ענן אינן מחויבות, ברוב המקרים, ברגולציות דומות[41]. יתר על כן, חלק מספקיות השירותים באינטרנט, לרבות שירותי מחשוב בענן, מפרסמות הצהרות שונות לגבי המשמעות החוזית של התקשרות הלקוחות עם השירותים שהן מציגות, אך עושות כן בצורה שעלולה להשתמע ככוחנית ובעייתית מאוד מבחינה משפטית. מחקר שנעשה בפקולטה למשפטים באוניברסיטת בונד (Bond) באוסטרליה על שירות Google Docs הראה כי Google רואה בלקוחות שעושים שימוש בשירות שלה "כמסכימים מעצם השימוש בשירות לתנאי הפרטיות של החברה" ושהם "בגיל אשר מתיר להם לפי חוק להקשר בחוזה מסוג זה עם Google". עוד עולה, כי מקריאה של מסמכי הפרטיות ניתן ללמוד כי החברה "יכולה לשנות את התנאים ללא הודעה" ללקוחותיה ואף "להפסיק את השירות או לשנות אותו ללא הודעה" ללקוחות. כמו כן מצוין במסמכי הפרטיות והסכמי השימוש של החברה כי היא רשאית לעשות שימוש במידע אשר "אצור במערכות השירות" לצורך מיקוד והכוונת פרסומות מותאמות ללקוחות. מחקר זה מצביע על סיכונים מהותיים שיש ללקוחות שירותי מחשוב ענן בנושא פרטיות המידע, שמירה עליו ואיזה שימוש **באמת** נעשה בו על ידי ספקיות השירות. החוק הלוקאלי בכל מדינה אינו ערוך לתת מענה גלובאלי לסוגיות פרטיות בשירותים כדוגמת מחשוב ענן. מצד שני, ספקיות הענן עצמן אינן מודעות לבעייתיות הגדולה שבחשיפת שירותיהן על פני הגלובוס והאתגר הגדול של עמידה בהוראות חוקים ורגולציות של מדינות שונות באמצעות מדיניות פרטיות והסכמי שימוש אחידים[42].

תקנים ומוסדות משמעותיים בתחום אבטחת המידע בענן

בעמודים הקרובים תינתן סקירה על חלק מהגופים וההסמכות המשמעותיים ביותר בקידום תחום מחשוב הענן והסדרתו[43]. למחשוב ענן יש היבטים מחשוביים מגוונים ועל כן יש הכרח בהסדרת התחום על רבדיו הטכנולוגיים השונים. בסקירה זו לא ניתן משקל לקבוצות עבודה בתחומים טכנולוגים נוספים כמו התקשורת, הבינה העסקית (BI), האחסון וקבוצות אשר מרכזות את מאמציהן בקידום ממשקים שונים בין הצרכנים לספקי השירות ובין ספקי השירות לעמיתיהם. עיקר המיקוד, אם כן, הינו בתקנים והסמכות הקשורות לאבטחת מידע , שכן מדובר בתחום אשר מרכז עניין רב לאור המחקרים שצוטטו במסמך זה וכן ברוב רובם של המחקרים וניירות העמדה בתחום. קידום כלל הטכנולוגיות מבוססות הענן חייב להתבצע בד-בבד עם קידום התקנים הקשורים לאבטחת מידע.

41 - Christopher Soghoian: Caught In The Cloud: Privacy, Encryption, And Government Back Doors In The Web 2.0 Era, (Indiana University Bloomington - Center for Applied Cybersecurity Research, August 17, 2009): http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553

42 - Dan Svantesson and Roger Clarke. (2010) "Privacy and consumer risks in cloud computing" Computer law and security review, 26 (4), 391-397, http://epublications.bond.edu.au/law_pubs/347/

43 - מטבע הדברים לא יסקרו כל הגופים הנוגעים לנושא הענן. בסקירה זו הושמטו מספר ארגונים משמעותיים מאוד בתחום התקינה והמחשוב, ביניהם: IEEE, ISACA ואחרים.

ISO 27000

משפחת תקני 27000 של ארגון התקינה הבינלאומי (International Standard Organization) מכילה מספר תקנים הקשורים לניהול אבטחת מידע וסיכונים. התקן המוביל במשפחה זו הוא ISO 27001 אשר פורסם ב-2005. מטרת התקן היא: "לספק מודל לביסוס, הטמעה, תפעול, ניטור, סקירה, שמירה ושיפור מערכת לניהול אבטחת מידע"[44]. אימוץ התקן הוא עניין אסטרטגי בארגון. יתרה מזאת, עיצוב אבטחת המידע בכל ארגון הוא עניין שצריך להיגזר מצרכי הארגון, מדרישות האבטחה, מהתהליכים הארגוניים וכן מסדר הגודל של הארגון[45].

על אף שמחשוב ענן אינו מוזכר בתקן ואין התייחסות ספציפית לנושא, קיימים מספר סעיפים בתקן אשר מתייחסים להיבטי אבטחת מידע אשר רלוונטיים למחשוב ענן[46], ביניהם:

- Identification of risks related to external parties - (A.6.2.1) - סעיף זה מתייחס לסיכונים הקשורים לגופים אחרים מלבד הגוף אשר נדרש לתקן בעצמו (סיכוני צד ג').
- Addressing security in third party agreements - (A.6.2.3) - בסעיף זה, כמו בסעיף הקודם, מוזכרים היבטי אבטחת מידע בהסכמים עם גורמים מחוץ לארגון.
- Information back-up - (A.10.5.1) - התייחסות בתקן לנושאי גיבוי נתונים.
- Access control - (A.11) - התייחסות בתקן לנושאי בקרת גישה והרשאות גישה למערכות.
- Classification - (A.7.2.1) - נושאי סיווג מידע על פי רגישות וקריטריונים נוספים.

תקן זה אומץ בקרב כל ספקיות שירותי הענן הגדולות[47] והוא הופך, אט אט, לתקן הכרחי בקרב ספקים חדשים. לקוח שרואה באתר הספק שהוא עומד בתקן מבין את התהליכים שספק זה התחייב לעמוד בהם. התקן מכיל מספר רב של פרמטרים לשמירה על רמה נאותה על בקרות אבטחת מידע ושמירה על נתונים. ולכן, הסיבה המרכזית לאימוץ התקן היא העובדה שהוא מסייע בהורדת הסיכון עבור לקוחות שירות הענן.

FIPS140-2

תקן זה הינו תקן אמריקאי משנת (Federal Information Processing Standards Publication 140-2) 2001 מטעם משרד המסחר והמוסד הלאומי (האמריקאי) לתקנים וטכנולוגיה[48] אשר מסדיר את תחום הצפנת המידע הדיגיטלי עבור רשויות פדראליות אמריקאיות. על פי התקן, ישנן ארבע רמות הצפנה

44 - 27000, **27000 -Toolkit**, http://www.27000-toolkit.com/ (ISO 27001 Citation)
45 - The ISO 27000 Directory, **An Introduction To ISO 27001 (ISO27001),** http://www.27000.org/iso-27001.htm
46 - 27000, **27000 -Toolkit**, http://www.27000-toolkit.com/ (ISO 27001 Citation)
47 - http://aws.amazon.com/security/iso-27001-certification-faqs/ , http://googleenterprise.blogspot.co.il/2012/05/google-apps-receives-iso-27001.html , http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm
48 - Department of Commerce, National Institute of Standards and Technology

למידע[49]. ספקים, מוצרים ושירותים בתחום המחשוב באופן כללי ובענן באופן פרטי מקפידים לעמוד בתקן מתוך הבנה כי מדובר בתקן משמעותי מאוד. מעיון קצר ברשימת החברות המסחריות אשר עומדות בתקן, ניתן ללמוד כי מדובר ברוב רובם של הגורמים המשפיעים בעולם הטכנולוגי[50]. עיקר החשיבות של תקן זה למחשוב ענן הוא אחסון הנתונים אצל ספק הענן והצפנה שלהם בתוך אמצעי האחסון. ככל שההצפנה תתמוך בתקן FIPS ברמה גבוהה יותר, כך רמת האמינות של שירות הענן תעלה.

PCI -SSC

או בשמה המלא: Payment Card Industry - Security Standards Council, הינה משפחה של תקני אבטחת מידע שיזמו חמש חברות האשראי הגדולות בעולם כדי להתמודד עם מכת גניבות כרטיסי האשראי בעידן האינטרנט. תקנים אלה, ובמיוחד PCI-DSS, אשר עוסק באבטחת נתונים, נועדו להגדיר פרמטרים ובקרות אשר יחייבו כל ארגון, מוסד וחברה שמעוניינים לסלוק, לאחסן או להעביר במערכות המידע שלהם פרטי כרטיסי אשראי של לקוחות. את התקן מפעילה מטעם חברות האשראי מועצה מיוחדת ואין מאחוריו כל גוף מדינתי או ציבורי[51]. לכאורה, אין לתקנים אלה קשר ישיר למחשוב ענן. עם זאת, ספקי שירותי ענן מטפלים ומאחסנים נתוני כרטיסי אשראי של לקוחותיהם ולכן סביר שהם יחויבו לעמוד בתקן. התקן נחשב לפרטני יחסית מבחינת דרישות האבטחה שלו. דרישות אלה זמינות באתר המועצה לכל דורש ומאפשרות לכל לקוח של ספק שירותי ענן אשר עומד בתקן לסקור את אמצעי ההגנה והבקרות שספק זה נדרש לעמוד בהם ולהתאים אותם לצרכיו ולצרכי ארגונו[52]. חשוב לציין, כי עמידה של ספק בתקן אינה אומרת בהכרח שמערכות הלקוח עומדות בתקן. מומחים שונים מציינים כי על הלקוח לשים לב בדיוק לסוג ההסמכה לתקן בצד הספק ולסוג השירות כדי לגזור את המשמעות עבורו[53]. גם מועצת ה PCI מנסה להסדיר את הנושא. במסמך הנחיות שפרסמה ב 2011 בעניינים הקשורים לסביבות וירטואליות ולמחשוב ענן, המליצה המועצה כי: ברכישת שירותי IAAS, על הלקוחות לראות במידע, בתוכנה, ביישומים, במערכות ההפעלה, בבסיסי הנתונים ובתשתיות הווירטואליות כאחריות שלהם (של הלקוחות) לעניין עמידה בתקן[54].

49 - Federal Information Processing Standards PUB 140-2: Security Requirements For Cryptographic Modules (Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900): http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

50 - NIST, Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

51 - PCI Security Standards, **About Us**, https://www.pcisecuritystandards.org/organization_info/index.php

52 - PCI Security Standards, **PCI Standards Documents,** https://www.pcisecuritystandards.org/security_standards/documents.php

53 - Wired, **PCI DSS Compliance in the Cloud: Challenges and Tactics**, http://www.wired.com/insights/2012/05/pci-dss-compliance-cloud/

54 - Virtualization Special Interest Group: PCI DSS Virtualization Guidelines (PCI Security Standards Council, June 2011): https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

SSAE-16

Statement on Standards for Attestation Engagements הינו תקן של ארגון רואי החשבון האמריקאי (AICPA) אשר תוקנן בשנת 2010 והוא אבולוציה של תקן ותיק יותר בשם SAS 70. התקן מסדיר את הדרך שבה ארגון פלוני מחויב לדווח על אמצעי הבקרה הקיימים אצלו. הדיווח מאושר אצל רואה החשבון החיצוני של הארגון וניתן לו תוקף. התקן מאמת עבור גורמים חיצוניים שאותם תקנים שהארגון התחייב עליהם אכן קיימים. על פי SSAE 16 נבדקת ומאומת מערכת מידע של הארגון המבוקר, במקרה שלנו -ספק הענן, על כל ההיבטים הקשורים למערכת זו, כלומר: תהליכים, מדיניות ונהלים רלוונטיים[55]. חלק מספקי הענן משתמשים בהסמכת SSAE 16 כאמצעי להעלאת הביטחון של הלקוחות בשירותים שהם מציעים. במקרים מסוימים הספקים אף מציעים ללקוחות להחליף בדיקות ישירות של הבקרות אצל ספק הענן עבור רגולציות כמו SOX[56], בשימוש בדו"ח ה SSAE 16 של הספק[57].

ניהול זהויות והרשאות בענן

ניהול זהויות והרשאות (IAM) הינו תחום העוסק בכל הקשור לזיהוי הגורמים אשר ניגשים למערכת מידע ולהרשאות שיש לאותם גורמים במערכת. IAM משתלב במחשוב ענן במספר צורות: ראשית, הוא מרחיב את התשתית הקיימת בארגון גם לשירותים בענן. בנוסף, הוא מאפשר מעבר בין מספר שירותי ענן על בסיס הזדהות אחת אצל ספק מסוים ונדידה לספק השני עם אותה הזהות. ניהול זהויות והרשאות מאפשר ייעול תהליכי רכישה אצל ספקי הענן וכן הגברת אבטחת המידע[58]. תקנים בתחום ה-IAM בענן הם אינטרס משותף של ספקי השירות ושל הלקוחות. בתחום מתהווים מספר תקנים מעניינים. ביניהם ניתן לסקור את התקנים הבאים[59]:

OAuth (Open Authorization) הינו תקן שמקודם על ידי ה-IETF. התקן מאפשר גישה למערכת באמצעות אפליקציה אשר מזהה את המשתמש שמפעיל אותה באופן חד ערכי. כך קל יותר לגשת ולהזדהות מול מערכות שונות בענן. התקן פועל גם "בכיוון השני" ומאפשר גישה של מערכת לשרתים של משתמש מסוים מבלי שהמשתמש יצטרך לשתף את הפרטים האישיים שלו, אלא על ידי זיהוי של אפליקציה בתווך. מנגנון זה מזכיר במקצת שימוש ברשות מוסמכת אשר מנפיקה תעודות דיגיטליות לישויות באינטרנט (Certificate Authority).

---

55 - NSK Inc., **Become SAS 70 Type II, SSAE 16 Compliant in the Cloud**, http://blog.nskinc.com/IT-Services-Boston/bid/103314/Become-SAS-70-Type-II-SSAE-16-Compliant-in-the-Cloud

56 - http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

57 - Layered Tech, **Certifications and Tech Partners**, http://www.layeredtech.com/why-layeredtech/certifications-and-tech-partners/

58 - TechTarget, **Identity management in cloud computing courts enterprise trust**, http://searchcio.techtarget.com/news/1509770/Identity-management-in-cloud-computing-courts-enterprise-trust

59 - Forrester Blog, **A New Venn Of Access Control For The API Economy**, http://blogs.forrester.com/eve_maler/12-03-12-a_new_venn_of_access_control_for_the_api_economy

OpenID Connect הינו תקן משלים ל-OAuth אשר עוסק במתן פתרון להזדהות חד פעמית על פני מספר שירותי ענן שונים ובלתי תלויים (הזדהות זו מכונה single-sign-on).

UMA - User Managed Access הינו התקן האחרון בסדרה זו. מדובר בתקן אשר נועד להסדיר את השליטה של משתמש פלוני בשיתוף מידע הקשור אליו בין מספר שירותי אינטרנט וענן ולהגדיר אילו פריטי מידע הוא מעוניין לשתף ואילו לא[60].

NIST

National Istitute for Standards and Technology הינו הגוף המשמעותי ביותר כיום בארה"ב לתקינה טכנולוגית. NIST פועל תחת המשרד למסחר והוא מאגד בתוכו מספר גופי משנה וועדות לתקינה והסדרת השימוש בטכנולוגיות ומדע. פעילות NIST בתחום מחשוב הענן מתחילה בהגדרה שגוף זה פרסם[61], דרך פרסומים שונים הקשורים לאימוץ טכנולוגיות ענן והשיקולים והעקרונות הרלוונטיים לגופים פדראליים[62] ועד פעילות דרך צוות עבודה ייעודים לנושא הענן. NIST שואב חלק מההנחיות והסמכויות שלו מחוק בשם Federal Information Security Management Act 2002 או בקיצור FISMA, אשר ממונה על קידום נושאי ניהול אבטחת מידע במוסדות פדראליים והגנה על מידע פדראלי רגיש. בין שאר הנושאים בהם החוק נוגע, FISMA מגדיר פרמטרים הקשורים לקבלת רישיון הפעלה (Authorization To Operate) עבור כל גוף ששומר או מתחזק מידע פדראלי רגיש. מתן ATO לספקיות שירותי ענן מקנה למי שמחזיק אותו יכולת עבודה מול משרדי ממשלה וגופים פדראליים אחרים ומהווה עוד אסמכתא לאיכות השירות. חלק מספקיות שירותי הענן אף התכתשו ביניהן לגבי אישור שניתן (או לא) לאחת מהן[63].

Cloud Security Alliance

ה-CSA הינו גוף ציבורי ללא מטרות רווח אשר הגדיר לעצמו לקדם את השימוש בשיטות אופטימאליות (best practice) כדי להבטיח המצאות אמצעי אבטחת מידע מיטביים במחשוב ענן וכן לקדם חינוך וידע לגבי השימוש במחשוב ענן על מנת לסייע בשיפור השימוש במחשוב באופן כללי[64].

---

60 - Kantara Initiative, **Case Study: Subscribing to a Friend's Cloud,** http://kantarainitiative.org/confluence/display/uma/Case+Study%3A+Subscribing+to+a+Friend's+Cloud

61 - Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing (National Institute of Standards and Technology Special Publication 800-145 7 pages (September 2011): http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

62 - Some of NIST's publications: Guidelines on Security and Privacy (800-144), CC Synopsis & Recommendations (800-146), CC Standards Roadmap (500-291), CC Reference Architecture (500-292), USG CC Technology Roadmap Draft (500-293)

63 - CRN, **Microsoft Admits Lacking Full FISMA Certification For Federal Cloud**, http://www.crn.com/news/cloud/229401710/microsoft-admits-lacking-full-fisma-certification-for-federal-cloud.htm;jsessionid=VL8dEvVU+98uiUAaYpEH+Q**.ecappj03?cid=rssFeed

64 - CSA, About, https://cloudsecurityalliance.org/about/

ה-CSA חוקרים את תחום מחשוב הענן עם דגש על נושא אבטחת המידע וניהול הסיכונים בענן. כחלק מפעילות זו, התגבשו להן מספר קבוצות עבודה ומסמכים חשובים[65]:

- מסמך הנחיות לנושאי חשובים הקשורים לאבטחת מידע במחשוב ענן[66]. מסמך זה מפרט את האיומים המרכזיים הקשורים לשימוש בטכנולוגיות מבוססות ענן. מדובר באחד המסמכים המוכרים של ה-CSA אשר נכתב בראשית דרכו של הארגון ועבר רביזיה בסוף 2011.
- קבוצת עבודה לתחום החדשנות בפתרונות אבטחת מידע בענן.
- קבוצת עבודה לקידום נושא ההסמכות לספקי הענן השונים.
- קבוצת עבודה שתפקידה לבדוק היבטי מחשוב ענן ואבטחת מידע לתחום הניידות (mobile).
- קבוצת עבודה שתפקידה לבדוק היבטי פרטיות ואבטחת מידע בפתרונות Big Data[67] מבוססי ענן.
- קבוצת עבודה שתפקידה להעמיק את הידע לגבי מתן פתרונות אבטחת מידע באמצעות מודל הענן.

מספר יוזמות מאוד מעניינות של ה-CSA מתייחסות לנושא הסדרת והשוואת ספקי הענן בינם לבין עצמם וכן מול תקנים והסמכות חיצוניות. על פי פרויקט של ה-CSA בשם Security, Trust & Assurance Registry או בקיצור STAR, מוזמנים ספקי הענן השונים למלא שאלון מיוחד וטבלת הערכה[68] ולציין בהם את כלל ההסמכות והבקרות החיצוניות שהם מבצעים. מילוי השאלונים מאפשרת שקיפות מול לקוחות פוטנציאלים שמעוניינים במידע לגבי אמצעי אבטחת המידע שספק הענן מצהיר עליהם.

פרוייקט נוסף של ה-CSA מנסה לקדם מנגנוני אמון בין ספקי הענן ללקוחות שלהם על ידי יוזמה בשם Cloud Trust Protocol. מנגנון האמון הזה (CTP) נועד לספק בצורה שקופה מידע ללקוח על אמצעי ותהליכי אבטחת המידע אצל ספק הענן כדי שהלקוח יוכל לקבל החלטות מושכלות לגבי השימוש הנבון מבחינתו בשירותי הענן[69].

פרוייקט אחר ראוי לציון של ה-CSA הוא הסמכה בשם Certified Cloud Security Knowledge[70] שהארגון מנפיק לאנשי מקצוע המעוניינים להרחיב את הידע התיאורטי שלהם בנושאי אבטחת מידע בענן בהתבסס על מסמכי הארגון והנחיות שפורסמו על ידי ENISA, הסוכנות האירופית לתקשורת ואבטחת מידע.

Federal Risk and Authorization Management Program

FedRAMP הינה תקן חדש מתחילת 2012 פרי יוזמה של מספר[71] רשויות פדראליות בארה"ב אשר התאגדו כדי להגדיר בקרות שימוש בשירותי ענן עבור גופים ורשויות פדראליות. בקרות FedRAMP

65 - CSA, **Research**, https://cloudsecurityalliance.org/research/
66 - CSA, **Security Guidance for Critical Areas of Focus in Cloud Computing V3.0**, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
67 - http://en.wikipedia.org/wiki/Big_data
68 - CSA, **CSA Security, Trust & Assurance Resources**, https://cloudsecurityalliance.org/star/
69 - CSA, **Cloud Trust Protocol**, https://cloudsecurityalliance.org/research/ctp/#_downloads
70 - CSA, **Certificate of Cloud Security Knowledge**, https://cloudsecurityalliance.org/education/ccsk/

מתבססות על פרסום NIST מספר 800-53 גרסה 3[72] והם מחייבות כל ספק שירותי ענן אשר מעוניין לענות על מכרזים של רשויות פדראליות. על מנת לעמוד בדרישות התקן, על ספקיות שירותי הענן לקבל אישור FISMA להפעיל שירותי ענן (Authorization To Operate) וכן לשכור חברה חיצונית בעלת אישור מתאים[73] שתבצע סקירה של הספק בהתאם להוראות המסמך של NIST לעיל. עד מועד כתיבת שורות אלה הוסמכו רק שני[74] ספקי שירותי ענן מתוך כמה עשרות שהחלו את התהליך.

הרשות למשפט, טכנולוגיה ומידע

רמו"ט היא רשות ישראלית הפועלת במסגרת משרד המשפטים. היעדים של רמו"ט הם לחזק את ההגנה על מידע אישי, להסדיר ולפקח על השימוש בחתימות אלקטרוניות ולהגביר את האכיפה על עבירות פגיעה בפרטיות. רמו"ט גם משמשת כמרכז ידע בממשלה לחקיקה ופרויקטים בעלי היבטים טכנולוגיים, כגון ממשל זמין[75].

התייחסות רמו"ט למחשוב ענן ולאתגרי אבטחת המידע בו באה לידי ביטוי בהנחייה אשר מפרטת את העקרונות להגנת הפרטיות במידע אישי במסגרת הוצאת עבודות ושירותי מידע אישי למיקור חוץ, כלומר רמו"ט רואה במיקור חוץ של מידע את המאפיין העיקרי של שירותי ענן.
ההנחיה קובעת מספר עקרונות בסיסיים הדורשים הסדרה בטרם הוצאת פעולות עיבוד מידע למיקור חוץ, לרבות[76]:

- בחינה מקדימה של הלגיטימיות להוצאת הפעילות למיקור חוץ.
- הגדרה ברורה של אופי השירות שיבוצע במיקור חוץ וקביעה מדויקת של מטרת השימוש במידע, כך שלא יתבצע שימוש שלא למטרה לשמה נתקבל המידע.
- הגדרת דרישות אבטחת מידע ושמירה על סודיות כדי למנוע זליגה של המידע.
- הבטחת מתן זכות עיון ותיקון לאזרח אליו המידע נוגע.
- עקרונות לאופן בחירת הקבלן, כגון ניסיון קודם ובירור חשש לניגוד עניינים.
- הדרכה והטמעה של דיני הפרטיות בקרב עובדי הקבלן נותן השירות.
- אופן קיום בקרה של המזמין על עמידת נותן השירות בדיני הפרטיות.
- משך שמירת המידע הנמסר לקבלן לצורך ביצוע השירות ומחיקתו עם גמר ההתקשרות.

---

71 - GSA, **FedRAMP Governance**, http://www.gsa.gov/portal/category/103271
72 - NIST, Recommended Security Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Revision 3), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
73 - GSA, Third Party Assessment Organizations (3PAOs), http://www.gsa.gov/portal/category/102387
74 - GSA, Authorized Cloud Service Providers, http://www.gsa.gov/portal/content/131931
75 - משרד המשפטים, אודות הרשות למשפט, טכנולוגיה ומידע , http://www.justice.gov.il/NR/exeres/DC0807D5-F376-4262-8689-DE14A72A0909,frameless.htm?NRMODE=Published
76 - משרד המשפטים, הרשות למשפט טכנולוגיה ומידע (רמו"ט): כך תגנו על הפרטיות במידע בשימוש בשירותי מיקור חוץ , http://www.justice.gov.il/MOJHeb/ILITA/News/mikurhuts.htm

ההנחייה נכנסה לתוקף במאי 2012 ומהווה התייחסות פומבית יחידה (עד עתה) של הרגולטור בישראל לאתגרים הקשורים למחשוב ענן.

סיכום

טכנולוגיות מידע ידועות באופנתיות מתחלפת. חברות שעוסקות במחקר בתחום נוהגות להשתמש ב-Buzzwords (ביטויים אופנתיים בתרגום חופשי) כדי לתאר את המגמות החשובות בכל תקופה. "מחשוב הענן" החל לככב בין הביטויים האופנתיים בשנת 2008 ונמצא מאז בתודעה העולמית והמקומית בתחום המחשוב. השנתיים הראשונות להופעת המושג הן שנות ההתרגשות (hype) והן ייוחדו על ידי כלל הגורמים העוסקים במחשוב להבנת המושג ולמציאת פרשנות שתתאים לאג'נדה, איש איש לפי העמדה שלו: החוקרים דאגו להבליט את המהפכה הגדולה שמחשוב הענן מבשר עבור כולנו, אנשי המכירות בקרב יצרני פתרונות המחשוב היטיבו לתאר איך כל קוויי הפתרונות של מוצריהם מגלמים בדיוק את מה שמחשוב הענן נועד להביע ואילו הצרכנים התחלקו לשתי קבוצות עיקריות: בקבוצה הראשונה התרכזו כל אותם אנשים אשר נסחפו אחר קולות המהפכה ואילו מולם - הספקנים. אלה שמתארים עד היום את מחשוב הענן כ"חזרה לימי ה-Main Frame (המחשב המרכזי) וללשכת השירות של שנות השמונים".

השנים 2010-2011 אופיינו, לדעתי, בהתפכחות רבתי של כלל הגורמים הנוגעים בדבר. אם היו כאלה שראו בחזונם ארגוני ענק רבים אשר מקיימים שגרת מחשוב, כשכל התשתיות ומערכות הליבה שלהם מופעלות באחד ממודלי הצריכה לפי שימוש בענן, אזי הם התבדו כמעט תמיד. מצד שני ניתן לראות כי בשנים אלה החלה הגירה של צרכנים פרטיים וארגונים קטנים ובינוניים בהמוניהם לכיוון אחד או יותר ממודלי הענן. בראיה לאחור ברור, כי עבור סקטורים מסוימים וארגונים בסדר גודל מסוים מודל הענן פתר הרבה מאוד בעיות כספיות ותפעוליות. מצד שני, בארגונים רבים התברר עד מהרה כי בעיות תאימות בין מערכות הענן למערכות הארגון וכן אתגרי אבטחת מידע גדולים מקשים מאוד על ההגירה לענן.

האם ניתן להגיד שהקונספט הצליח או לא? גם כיום קשה להגיד בצורה חד משמעית האם מדובר בהצלחה או בכישלון. נכון לסוף שנת 2012 אין ביכולתנו לקבוע שום קביעה לגבי רמת ההצלחה של מחשוב ענן. יתרה מזאת, מהי היא הצלחה? ובעיני מי? יתכן מאוד שקצב הצמיחה של תחום מחשוב הענן עונה על הציפיות של ספק ענן מסוים ומאכזב ספק אחר.

לאן הולכים מכאן?

מחשוב הענן משתלב בשנים האחרונות במגמה אחרת, חשובה לא פחות, בתחום המחשוב: מובייל (mobile). מאז שנת 2007, עת הפציע מכשיר ה-iPhone הראשון בידיו של סטיב ג'ובס, מייסדה המנוח של חברת אפל, עבר העולם הטכנולוגי טלטלה שנוגעת לכל אחד ואחת מאתנו. המכשיר הנייד, שעד לפני שנים בודדות הוציא וקיבל שיחות טלפון, הפך לעמדת קצה חכמה ומגוונת מעין כמוה. באמצעות מכשיר נייד אחד ניתן לגלוש באינטרנט, לשלוח מייל, לצלם תמונות, לסחור בבורסה, להשתמש כפלס או פנס, לנווט, להפעיל מכונית, להפיג שעמום עם אלפי משחקים ועוד. שם המשחק הפך להיות: אפליקציות. לא עוד גלישה מהמכשיר הנייד לאתר באינטרנט, כי אם יישום שמותקן על המכשיר ומותאם בצורה אופטימאליות לצרכי המשתמש. המכשיר הנייד החכם הביא לשינוי בדרך שבה הצרכן רוצה לצרוך את שירותי המידע שלו. עובדים בארגונים לא נותרו אדישים והחלו לדרוש חוויה דומה גם במקומות העבודה שלהם. כך החלה מגמה של הבאת מכשירים פרטיים לארגונים[77]. מודל צריכת המידע השתנה כך שחלק גדל והולך מהמידע הפרטי נשמר במכשיר הטלפון החכם ואצל ספק האפליקציה, בענן. גם כיום, חלק משמעותי מהמידע הפרטי של שלנו מאוחסן ומופעל באמצעות מערכות מבוססות ענן. מחשוב הענן, כמו שהוזכר כבר במסמך זה, מסוגל לספק ללקוח זמינות גבוהה בכל מקום בו יש תקשורת לאינטרנט. עולם המובייל הוסיף לכך חיבוריות סלולרית אשר מגבירה את הזמינות ואת הגמישות של שירותי התוכן בענן.

לסיכום, ככל ששירותי הענן ימשכו אליהם נתח גדל והולך מהמידע הפרטי וככל שיותר ויותר ארגונים יסתמכו על תשתיות ומערכות מבוססות ענן, כך יגבר הצורך בהסדרת השימוש בשירותים אלה. המשפט יהיה נכון גם מהכיוון השני: קידום תקני שימוש, תקני זמינות, פרטיות ותקני אבטחת מידע יעלה מאוד את אמון ציבור הלקוחות בקונספט שנקרא מחשוב ענן ויאפשר פריחה שלו לאורך זמן.
עם זאת, העדר תקנים מספקים או ריבוי תקנים מקבילים עלול להגביל את הצמיחה של מודל מחשוב הענן עבור לקוחות שמרניים וכן עבור ארגונים אשר כפופים לרגולציות נוקשות בלאו הכי (כמו למשל ארגונים פיננסיים, מוסדות ציבור וממשלה וכיו"ב). אין זה מפתיע שבחלק גדול מהגופים שעוסקים בקידום תקנים בענן ניתן למצוא חברות מסחריות שיש להן נגיעה ישירה לשירותי מחשוב בענן. להן זהו אינטרס ראשון במעלה, שכן הוא שווה הרבה כסף. כמו כן, אין זה מפתיע שהרשויות בארה"ב, אירופה ואפילו ישראל עוסקות בקידום תקנים ורגולציות בתחום מחשוב הענן. תפקידה של המדינה והרגולטור שפועל בשמה לסייע בקידום האינטרסים העסקיים של הגורמים המבוקרים, תוך שמירה על רווחת הצרכנים. גם הרשויות מבינות, כמונו, שמחשוב ענן עשוי לתרום רבות לטכנולוגיה, לפעילות העסקית ולרווחת הציבור. על כן יש לאפשר תמיכה בו על ידי פיתוח מסגרת נאותה של תקנים ורגולציות.

77 - BYOD -Bring Your Own Device