מבקר המדינה | דוח שנתי 72א - חלק ראשון | התשפ"א-2021

פרק ראשון - נושאים מערכתיים

שימוש משרדי ממשלה בענן ציבורי וההיערכות להקמת ענן מרכזי

שימוש משרדי ממשלה בענן ציבורי וההיערכות להקמת ענן מרכזי

רקע

התפתחות טכנולוגיית מחשוב הענן מאפשרת למגזר הממשלתי להתמודד טוב יותר עם אתגרים רבים הניצבים לפניו, כגון שיפור השירות לאזרח, צמצום השונות בין משרדים והתייעלות תפעולית. אך לצד היתרונות, השימוש בטכנולוגיה זו טומן בחובו גם סיכונים ממשיים בתחומי אבטחת המידע והגנת הסייבר, הגנת הפרטיות ועוד.

בשנים האחרונות הכירה ממשלת ישראל בצורך בתכנון צופה פני עתיד ובהתוויית חזון, מטרות ויעדים שיאפשרו את מיצוי הפוטנציאל הגלום בטכנולוגיית הענן, ויקלו את ההתמודדות עם האתגרים הכרוכים בשימוש בטכנולוגיה זו.

נתוני מפתח

2%
שיעור הניצול השנתי הממוצע של משאבי תשתיות המחשוב המקומיות הקיימים בממשלה בשנת 2018

1%
בשנת 2019 השקיעה הממשלה במחשוב ענן פחות מאחוז אחד מסך השקעתה בתקשוב, לעומת 8% בעולם[1]

102
מספר המערכות אשר הועברו לסביבת ענן[2] מתוך אלפי מערכות מידע ותשתיות מחשוב במגזר הממשלתי

773%
גידול במספר האיומים על שירותי ענן במגזר הממשלתי בעולם בחודשים מרץ ואפריל 2020 לעומת ינואר ופברואר באותה השנה

60%
שיעור המשרדים אשר השיבו לשאלון משרד מבקר המדינה כי לא ביצעו תהליך הפקת לקחים לאחר יישום מערכת בענן

61%
שיעור המשרדים אשר השיבו לשאלון משרד מבקר המדינה כי אין להם תוכנית אב למחשוב או שאין בתוכנית התייחסות למחשוב ענן

99%
רוב מוחלט של המשרדים אשר השיבו לשאלון משרד מבקר המדינה כי לא נתקלו בתקלות מרובות במערכות הענן שלהם

1 על פי רשות התקשוב, מבט על פעילות 2020

2 על פי נתוני יה"ב המעודכנים ליולי 2020.

פעולות הביקורת

בחודשים מרץ עד אוקטובר 2020 בדק משרד מבקר המדינה היבטים בשימוש משרדי ממשלה בענן ציבורי וההיערכות להקמת ענן מרכזי. הביקורת נעשתה ברשות התקשוב הממשלתי שבמשרד הדיגיטל הלאומי, במינהל הרכש שבאגף החשב הכללי שבמשרד האוצר ובמערך הסייבר הלאומי שבמשרד ראש הממשלה. בדיקות השלמה נעשו באגפי מערכות מידע של כמה משרדי ממשלה ויחידות סמך, במרכז השלטון המקומי, ברשות להגנת הפרטיות שבמשרד המשפטים ובמינהלת הטרנספורמציה הדיגיטלית שבאגף התקשוב בצה"ל. במסגרת הביקורת פנה משרד מבקר המדינה ל-72 מנהלי אגפי מערכות מידע ראשיים (להלן - מנמ"רים) במשרדים הממשלתיים וביחידות הסמך שלהם, וביקשם למלא שאלון בנושא השימוש בשירותי ענן ציבורי. על השאלון השיבו 45 (כ-62%) מהמנמ"רים.

תמונת המצב העולה מן הביקורת

תוכנית מעבר ממשלתית מאושרת למחשוב ענן: תוכנית המעבר הממשלתית למחשוב ענן שהוכנה ברשות התקשוב לא הוצגה לוועדת השרים כנדרש בהחלטת הממשלה 2097 משנת 2014, בשל פיזורה של הוועדה בשנת 2015 ואי-הקמתה מחדש. יצוין כי שיעור הניצול השנתי הממוצע בשנת 2018 של משאבי תשתיות המחשוב המקומיות הקיימים בממשלה הינו 2%.

פרויקט נימבוס: פרויקט נימבוס הוא פרויקט רב-שנתי שהחל בשנת 2019 ושנועד לתת מענה מקיף לנושא אספקת שירותי ענן למשרדי הממשלה. הפרויקט מורכב מארבעה רבדים המרכיבים את המכרז המרכזי של מינהל הרכש הממשלתי. במהלך שנת 2020 פורסמו מכרזים לרובד הראשון (אספקת שירותי ענן) והרובד השני (מרכז מצוינות במחשוב ענן) של המכרז, ובמהלך פברואר 2021 פורסם מכרז לרובד השלישי (שירותי מודרניזציה והגירה). טרם פורסם מכרז לרובד הרביעי (שירותי ניטור ומיטוב), ולא נקבע מועד משוער לפרסומו. אי-קיומה של מסגרת זמנים מוגדרת לפרויקט בכללותו עלולה להביא להתארכות יישומו ולעיכוב בתוכנית להעברת משרדי הממשלה לסביבת הענן.

מיפוי מערכות שיושמו בסביבת ענן: נכון למועד הביקורת לא היו בידי רשות התקשוב או בידי גורם ממשלתי אחר מיפוי מלא ועדכני של כל המערכות הממשלתיות שכבר יושמו בענן. מיפוי זה נדרש לשם קבלת תמונת מצב מלאה ומדויקת של הנעשה במשרדי הממשלה ווידוא כי כל משרדי הממשלה פועלים בהתאם להנחיות רשות התקשוב בנושא מחשוב ענן.

אבטחת מידע לעבודה בענן: על אף הנחיה ייעודית של מנהל היחידה להגנת הסייבר בממשלה (להלן - יה"ב)[3] הקובעת כי כל מערכת אשר פועלת בסביבת הענן נדרשת לאישור הוועדה המייעצת לנושא העברת מידע ויישומי מחשוב לסביבת הענן הציבורי, בין אם היא מתוכננת למעבר לענן ובין אם היא כבר פועלת בענן, מתשובותיהם של 42 משרדים על השאלון שהפיץ משרד מבקר המדינה עולה כי במשרדים אלה פועלות בלא שהתבקש אישור הוועדה המייעצת כעשר מערכות בסביבת ענן. הפעלת מערכות כאמור בסביבת ענן בלא שהוועדה בחנה אם יש מקום לאשרן עלולה להביא להתממשות סיכוני אבטחת מידע הכרוכים בהפעלת מערכות אלה.

הנחיות אבטחת מידע בגופים שאינם כפופים ליה"ב: גופים הכפופים להנחיות המגזריות של משרדים ממשלתיים אך אינם כפופים להנחיות יה"ב, כגון חברות תקשורת, תחבורה ואנרגיה, מנהלים באופן עצמאי את תחום הגנת הסייבר במערכות המחשוב שלהם, לרבות בתחום יישום מערכות ענן, ללא גורם מקצועי-אסדרתי מוביל ומפקח - למעט אלו המוגדרים כתשתית מדינה קריטית ומונחים באופן הדוק על ידי מערך הסייבר.

בקרה על יישום הנחיות בתחום אבטחת המידע בסביבת הענן: אין בקרה על יישום הנחיות מערך הסייבר בידי הגופים השונים. כמו כן עלה כי למערך הסייבר אין הסמכות לקיים פיקוח ובקרה על יישום הנחיותיו בנושא הענן.

דרישות הוועדה המייעצת לביצוע בדיקות חדירה למערכת בסביבת הענן: משרד ראש הממשלה (להלן - רה"ם) נדרש לבצע כל 18 חודשים בדיקות חדירה או סקר סיכונים למערכת מעקב החלטות ממשלה שהועלתה לסביבת הענן בדצמבר 2018. בביקורת נמצא כי למערכת בוצעו בדיקות חדירה וסקר סיכונים במועד הקמתה, אולם נכון לפברואר 2021 טרם בוצעו בדיקות חדירה נוספות או סקר סיכונים נוסף.

התקשרות בפטור ממכרז להקמת מערכת בסביבת ענן: בשניים מתוך שלושה פרויקטים להקמת מערכת בסביבת ענן שנבחנו, במשרד הבינוי והשיכון ובמשרד רה"ם, הוחלט להתקשר עם ספק לביצוע הפרויקט ללא ביצוע הליך מכרזי אלא בוצעה התקשרות עם הספק בפטור ממכרז בעילה של ספק יחיד, תוך הסתמכות על הסכם מחירים מרביים שנחתם בין הספק למינהל הרכש הממשלתי. זאת על אף שהסכם המחירים המרביים עם הספק לא חל על שירותי הענן של הספק, וניתן היה לקיים הליך מכרזי.

הליך הפקת לקחים ממשלתי: לא גובש הליך ממשלתי סדור להפקת לקחים מיישום מערכות בסביבת הענן. הליך שכזה יכול לסייע בזיהוי החסמים, הקשיים והליקויים המקשים על משרדי הממשלה בבואם ליישם מערכות בסביבת הענן ולסייע בהתמודדות עימם.

פרסום מדיניות והנחיות: משרד מבקר המדינה רואה בחיוב את העובדה כי פרסומי המדיניות וההנחיות של רשות התקשוב ויה"ב בנושא מחשוב ענן מעודכנים בהתאם להתפתחויות

3 יה"ב היא יחידה הפועלת במסגרת רשות התקשוב הממשלתי במשרד ראש הממשלה. היחידה הוקמה על פי החלטת הממשלה 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר".

הטכנולוגיות. יצוין כי בנובמבר 2020 פרסם מינהל הרכש הוראת תכ"ם "קווים מנחים לאישור ובקרת התקשרויות בענן". בנוסף יצוין כי במהלך הביקורת פרסמה רשות התקשוב בדצמבר 2020 הנחיה בנושא "אישור, תכנון ובקרה לשירותי ענן".

שילוב גופים נוספים בפרויקט נימבוס: משרד מבקר המדינה מציין את שילובם של גופים נוספים, כגון גופים מוסדיים ופיננסיים וכן צה"ל, בפרויקט נימבוס. ריבוי גופים המשתתפים בפרויקט מאפשר איגום משאבים לאומי ויעילות תקציבית.

עיקרי המלצות הביקורת

על מנת להקל את יישומם של פרויקטים בסביבת ענן בעתיד, הן על ידי המשרדים באופן עצמאי והן במסגרת פרויקט נימבוס, מוצע כי רשות התקשוב תבחן את מכלול ממצאיו של דוח זה והמסקנות העולות מהם - תשובות המנמ"רים על השאלון; הצורך בעדכון הנחיותיה; הצורך בביצוע בקרה על הגופים כדי לוודא כי הם מיישמים את ההנחיות; מיסודו של הליך הפקת לקחים, לרבות של גורמים מקצועיים כגון הרשות להגנת הפרטיות; והצורך במדיניות אחידה לכלל הגורמים אשר תוכל לשמש בסיס לאסדרות פרטניות.

מומלץ כי משרד הפנים יגבש תוכנית רב-שנתית לשילוב הרשויות המקומיות במכרז נימבוס. במסגרת הכנת התוכנית ראוי לתת את הדעת לקיומו של מתווה ראשוני אשר ירכז הנחיות של המשרד לרשויות המקומיות, בכלל זה היבטים של הסברה, הדרכה והטמעה, תקצוב וכיו"ב. כמו כן מוצע כי משרד הפנים ומערך הסייבר הלאומי יפעלו בהקדם לקידום הקמת מרכז שליטה ובקרה מרכזי לטיפול באירועי סייבר ברשויות המקומיות, כדי להבטיח רציפות תפקודית של הרשויות המקומיות.

על אגפי מערכות המידע במשרדי הממשלה להעביר ליה"ב מיפוי של כלל מערכות הענן במשרדים ולהביא לשולחנה של הוועדה המייעצת את המערכות שהוקמו בסביבת הענן ללא שאושרו על ידה. על יה"ב להשלים מיפוי של כלל מערכות הענן במשרדי הממשלה. במסגרת זו מומלץ כי הוועדה המייעצת תוודא כי במיזמי ענן שיושמו לפני הקמתה נבחרו ספקים המחזיקים בהסמכות אבטחת מידע מספקות. עוד מומלץ כי יה"ב תנקוט בפעולות בקרה על מנת לוודא כי המשרדים מיישמים את הנחיותיה.

על מנת להבטיח את רמת אבטחת המידע והגנת הסייבר בעת יישום מיזמי מעבר לענן בקרב גופים הכפופים להנחיות המגזריות של משרדי ממשלה, מוצע כי משרדי הממשלה המשמשים כמאסדרים של מגזר פעילות יבחנו את הצורך בהקמת ועדות ענן ייעודיות לגופים הכפופים להנחיות המגזריות, כגון תחבורה, תקשורת ואנרגיה. ועדות אלו יוכלו לוודא כי יישום המערכות בענן עומד בסטנדרטים המקובלים בתחומי אבטחת המידע והגנת הסייבר, וכן לבצע בקרות על יישום מערכות בענן של הגופים. לחילופין, מומלץ כי משרדי הממשלה יבחנו את האפשרות להנחות את הגופים הכפופים והמפוקחים על ידם להקים ועדות ענן פנימיות אשר ידווחו למשרד הממשלתי על יישום מערכות בענן.

מומלץ כי מערך הסייבר יבחן ביצוע עריכת סקר עיתי לבדיקת קריאת ויישום הנחיותיו בנושא יישום מערכות בענן בידי משרדי הממשלה ויחידות הסמך, הן על מנת לצמצם את הסיכון כי לא ניתן מענה ראוי לנושא אבטחת המידע ביישום מערכת בסביבת הענן והן על מנת לבחון את אפקטיביות פעולותיו.

מומלץ כי מבקרי הפנים בכלל משרדי הממשלה וכן האגף לביקורת רשויות מקומיות במשרד הפנים יתנו את דעתם לחשיבות הנושא של מחשוב הענן וישקלו לשלב נושא זה בביקורת בהתאם למתודולוגיות המשמשות גופים אלו לבחירת הנושאים לביקורת.

משרד מבקר המדינה ממליץ כי לאור הגידול הצפוי בהתקשרויות הנוגעות למעבר לסביבת ענן, מינהל הרכש יוודא את העמידה בהנחיותיו בכל הנוגע להתקשרויות בין המשרדים לספקים לקבלת שירותי מחשוב בסביבת ענן, ולצורך כך יבחן את הצורך לבצע אחת לכמה שנים מיפוי כולל של ההתקשרויות - כולל מועדי ההתקשרויות, תוקפן ועלותן.

יתרונות ואתגרים ביישום מחשוב ענן

*כשספק השירות אינו ישראלי, המידע כפוף לדיני המדינה שהספק התאגד אצלה או למדינה שבה מוחזקים השרתים

סיכום

טכנולוגיית הענן מאפשרת גישה נוחה ורחבה למאגר משותף של משאבי מחשוב. בשנים האחרונות פועלת ממשלת ישראל להעברת משרדי הממשלה ויחידות הסמך למודל מחשוב ענן.

תמונת המצב המצטיירת לנוכח ממצאי דוח זה מלמדת על חסמים שונים המעכבים או מונעים יישום של מערכות במחשוב ענן במשרדי ממשלה; על היבטים שונים שהמשרדים אינם מביאים בחשבון במסגרת היישום ועלולים לגרום נזק, החל בנזק כספי וכלה בנזק תדמיתי; על קושי בבקרה על יישום המשרדים את ההנחיות למעבר לסביבת מחשוב ענן, וכן על קושי בבקרה על גופים הכפופים להנחיות המגזריות של המשרדים אך אינם כפופים להנחיות של רשות התקשוב ויה"ב; ועל מחסור במסגרת עבודה כוללת ומאושרת להעברת שירותי המחשוב של הממשלה לסביבת ענן. לשם יישום מיטבי של השימוש במערכות מחשוב ענן קיימות וכאלו שיוקמו בעתיד, ראוי כי החסמים והליקויים שפורטו וההמלצות שניתנו יקבלו מענה כולל, לרבות במסגרת מכרז נימבוס והקמת מרכז המצוינות התפעולית בענן.

שימוש משרדי ממשלה בענן ציבורי וההיערכות להקמת ענן מרכזי

מבוא

ההתפתחויות הטכנולוגיות במהלך השנים הביאו להטמעת מערכות מידע ממוחשבות כחלק בלתי נפרד מפעילותו של כל ארגון עסקי וציבורי. כיום משקיעים ארגונים, ובהם גופים ממשלתיים, חלק ניכר ממשאביהם בפיתוח, הפעלה ותחזוקה של מערכות מידע על מנת למקסם את התועלת העולה מהן, כגון ייעול תהליכי עבודה, שיפור מתן השירות ועוד.

במהלך 15 השנים האחרונות התפתחה בעולם טכנולוגיית הענן. על פי הגדרת מכון התקינה האמריקאי[4] (להלן - NIST) משנת 2011, מודל הענן הוא מודל מחשוב המאפשר גישה נוחה ורחבה למאגר משותף של משאבי מחשוב באמצעות המרשתת (אינטרנט) או קו תקשורת ייעודי. משאבים אלו ניתנים לשימוש על פי הצורך, וניתן להקצות אותם או לבטל את הקצאתם במהירות - תוך השקעה מעטה בלבד של מאמצי ניהול, ואינטראקציה מזערית עם ספק שירותי הענן[5]. היקף התשלום עבור משאבים אלו נקבע בהתאם להיקף השימוש בהם, ורכישתם אינה דורשת התקנה מקומית. כך יכול הארגון להפוך את תשתיות טכנולוגיות המידע למוצר (Commodity) שהוא אינו נדרש לייצר ולתחזק בעצמו, אלא שביכולתו לרכוש מגורם המתמחה בתחום, בדומה לשירותי החשמל והתקשורת. מצב זה מאפשר לארגון להתמקד בליבת העשייה שלו, ובד בבד לספק מענה מהיר לצרכיו המשתנים ולתמוך בחדשנות.

נהוג לחלק את שירותי הענן לשלושה סוגים עיקריים[6]:

1. "תשתית כְּשירות" (Infrastructure as a Service) - במודל זה ניתנים כלל רכיבי התשתית באמצעות המרשתת, ובכך מצטמצם הצורך של הארגון להחזיק בתשתיות פיזיות מקומיות לשם מימוש שכבת התשתית. כך לדוגמה, במקום שארגון יחזיק שרתים לאחסון מאגרי המידע הארגוני, הוא יכול לרכוש שירותי אחסון בענן;

2. "פלטפורמה (מַסֶּדֶת) כְּשירות" (Platform as a Service) - מודל זה מאפשר לספק למשתמשים סביבת פיתוח לשם עיצוב השירותים והיישומים שלהם, בהתאם לכלים ולשפת התכנות שמספקת תשתית הענן הספציפית;

3. "תוכנה כְּשירות" (Software as a Service) - במודל זה התוכנות ניתנות כשירות על בסיס תשתית ענן. כך לדוגמה, במקום שארגון יתקין על כלל מחשבי הארגון תוכנות Office, הוא יכול לרכוש שירותי גישה לתוכנה זו בענן. היתרון הוא האפשרות להשתמש בהתקני קצה, כגון מחשבים, ללא משאבי זיכרון גדולים - מה שמאפשר לרכוש התקני קצה זולים יחסית.

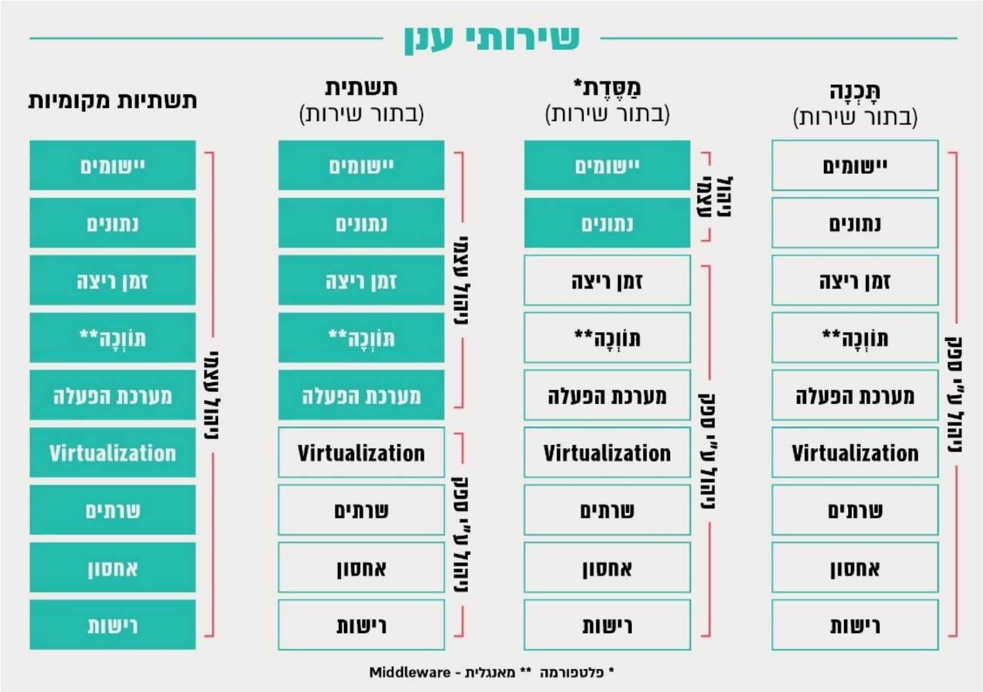
התרשים שלהלן מראה את חלוקת האחריות בין ספק הענן ללקוח, בהתאם לשירות הענן:

4 National Institute of Standards and Technology - NIST

5 להרחבה - מכון התקינה האמריקאי, National Institute of Standards and Technology, The NIST Definition of Cloud Computing, **NIST Special Publication** (2011), pp. 145 - 800.

6 להרחבה - שם.

תרשים 1: **מודל חלוקת האחריות במחשוב ענן**



מקור: NIST, בתרגום משרד מבקר המדינה.

מקובל להתייחס למודלים שונים של פריסת שירותי ענן[7]:

1. ענן ציבורי (Public Cloud) - במסגרת השירות, ספק הענן מספק את כלל השירותים הנדרשים בהתאם לקטלוג השירותים שהוא מציע. אותם שירותים ניתנים למגוון רחב של לקוחות שונים, והספק מציע אותם במגוון אתרים פיזיים על פי שיקול דעתו הבלעדי וללא מעורבות הלקוח. בדרך כלל שירות זה הוא גלובלי ואחיד, ואיננו משתנה בין הלקוחות השונים. הספקים יכולים להציע מחירים אטרקטיביים בזכות יתרון הגודל - שירותיהם ניתנים בהיקפים עצומים, מרחב הגמישות שלהם גדול וביכולתם לבצע שינויים והתאמות מהירים. התשתיות הגלובליות מסופקות על גבי המרשתת ולכן נגישות מכל מקום בעולם, והספקים מדגישים היבטים של אבטחת מידע ושרידות. ללקוח יש השפעה שולית בלבד על קטלוג השירותים.

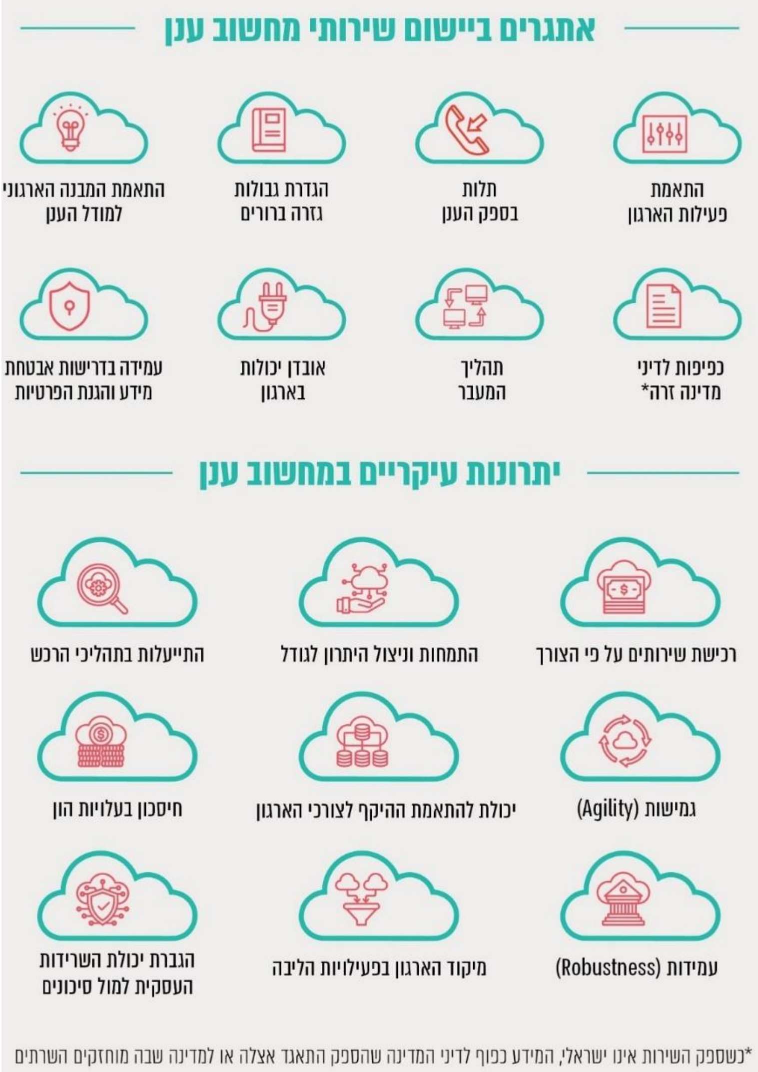
2. ענן פרטי (Private Cloud) - ענן ייעודי למטרותיו של ארגון ספציפי, אשר מוקם ומנוהל באופן עצמאי בידי הארגון או בסיוע ספק שירותים. ההפרדה הפיזית המאפיינת יישום ענן פרטי מבטיחה רמה גבוהה של אבטחת מידע, ומאידך גיסא דורשת היקפי פעילות גדולים ומנטרלת חלק מיתרונות הגודל המאפיינים ענן ציבורי.

7 להרחבה - שם.

3. ענן קהילתי (Community Cloud) - ענן הפועל במתכונת דומה לענן פרטי, אך מיועד לאגד את פעילותם של כמה ארגונים בעלי צרכים משותפים. בניגוד לענן פרטי, הוא מאפשר גם לארגונים עם היקפי פעילות נמוכים יותר לעשות שימוש בענן שאיננו ציבורי לגמרי, אלא מיועד לקבוצת משתמשים סגורה וקבועה מראש.
4. ענן היברידי (Hybrid Cloud) - ענן המשלב חלופות שונות כך שחלק מן המידע מנוהל כענן פרטי וחלקו מנוהל כענן ציבורי, בהתאם לצורכי הנגישות למידע ומידת הרגישות שלו.

לשימוש בשירותי מחשוב ענן יתרונות רבים, אך לצידם אתגרים משמעותיים אשר בהיעדר ניהול נכון עלולים לפגוע בתשתיות הארגון ואף להביא להשבתתו. התרשים שלהלן מדגים את היתרונות לצד האתגרים העיקריים בשימוש בשירותי מחשוב ענן:

תרשים 2: **היתרונות והאתגרים העיקריים בשימוש במחשוב ענן**



על פי נתוני רשות התקשוב הממשלתי, בעיבוד משרד מבקר המדינה.

התפתחות הטכנולוגיה בכלל, ומחשוב ענן בפרט, מאפשרים למגזר הממשלתי להתמודד טוב יותר עם אתגרים רבים הניצבים לפניו, כגון שיפור השירות לאזרח, צמצום שונות בין משרדים, התייעלות תפעולית ועוד. על מנת לייצר מענה מיטבי, המגזר הממשלתי נדרש לתכנון צופה פני עתיד והתוויית חזון, מטרות ויעדים שיאפשרו את מיצוי הפוטנציאל הגלום בטכנולוגיית הענן.

על פי נתוני רשות התקשוב הממשלתי (להלן - רשות התקשוב), נכון למרץ 2020 מערכות המידע במשרדי הממשלה ויחידות הסמך מבוססות על תשתיות מקומיות - שרת, אחסון ורשת תקשורת (On-premises) שמנהל כל משרד בנפרד. תצורת עבודה זו יוצרת איי מידע נפרדים אשר מקשים על שיתוף המידע בין המשרדים[8], וכן מובילה להקצאת משאבים לא יעילה, שכן הקמת כל תשתית מקומית וניהולה דורשים מהארגון להשקיע בהיערכות לצריכה מרבית של משאבי מחשוב בכל נקודת זמן, גם אם ידוע כי הצריכה המרבית תתרחש רק באירועים נקודתיים וחד-פעמיים. על פי נתוני רשות התקשוב, שיעור הניצול השנתי הממוצע של התשתיות המקומיות בממשלה בשנת 2018 היה כ-2%[9].

עוד על פי נתוני רשות התקשוב[10], ההוצאה הכללית על תקשוב בממשלה בשנת 2019 הייתה כ-3.5 מיליארד ש"ח, מתוכם 1.5 מיליארד כפעילות השקעה. ההשקעה במחשוב ענן עמדה בשנת 2019 על פחות מאחוז אחד מסך ההשקעה (כלומר מיליונים בודדים), זאת לעומת 8% של המגזר הממשלתי בעולם. לשם המחשה, על פי נתוני רשות התקשוב, עד יולי 2020 העבירו משרדי הממשלה לסביבת הענן כ-100 מערכות. לפי הערכת רשות התקשוב, לאחר הסרת חסמים הקשורים ברכש מרכזי, סטנדרטיזציה וניהול מרכזי בסביבת הענן, ניתן יהיה להעביר אלפי מערכות ותשתיות לסביבה זו.

פעולות הביקורת

בחודשים מרץ עד אוקטובר 2020 בדק משרד מבקר המדינה היבטים בשימוש משרדי ממשלה בענן ציבורי וההיערכות להקמת ענן מרכזי. הביקורת נעשתה ברשות התקשוב שבמשרד הדיגיטל הלאומי, במנהל הרכש שבאגף החשב הכללי במשרד האוצר (להלן - מינהל הרכש), ובמערך הסייבר הלאומי שבמשרד ראש הממשלה (להלן - מערך הסייבר). בדיקות השלמה נעשו באגפי מערכות מידע של כמה משרדי ממשלה ויחידות סמך, במרכז השלטון המקומי, ברשות להגנת הפרטיות שבמשרד המשפטים, וכן במינהלת הטרנספורמציה הדיגיטלית באגף התקשוב בצה"ל. במסגרת הביקורת פנה משרד מבקר המדינה במאי 2020 ל-72 מנהלי אגפי מערכות מידע ראשיים (להלן - מנמ"רים) במשרדים הממשלתיים וביחידות הסמך שלהם, וביקשם למלא שאלון שנועד בין היתר לאתר חסמים הנוגעים לשימוש בשירותי ענן ציבורי (להלן - שאלון הביקורת). על השאלון השיבו 45 (כ-62%) מהמנמ"רים.

8 הנחיות ראש רשות התקשוב הממשלתי, **מדיניות מימוש חזון הענן במשרדי הממשלה** (מרץ 2020)

9 הנחיות ראש רשות התקשוב הממשלתי, **מדיניות מימוש חזון הענן במשרדי הממשלה** (מרץ 2020).

10 להרחבה ראו:

https://www.gov.il/BlobFolder/news/2020overview/he/מסמך מבט על פעילות תקשוב 2020 - סופי (2).pdf

תמונת המצב הממשלתית של השימוש בענן הציבורי

קביעת מדיניות לאומית בישראל

עם התגברות ההכרה בחשיבות הטכנולוגיות הדיגיטליות בפעילות הממשלה, ולאחר בחינת צורכי הממשלה בתחום טכנולוגיות המידע, החליטה הממשלה במרץ 2011 להקים את יחידת מטה התקשוב הממשלתי[11] במשרד האוצר. היחידה נועדה לקדם ולייעל את מערך התקשוב הממשלתי ואת שיתוף הפעולה בין המגזר הממשלתי לגופים ציבוריים נוספים בתחומי המחשוב, ולשפר את רמת השירות לאזרח. ב-2014 החליטה הממשלה לשנות את שם יחידת מטה התקשוב ל"רשות התקשוב הממשלתי", ולהעביר אותה למשרד ראש הממשלה[12]. בשנת 2019 עמד תקציבה הכולל של רשות התקשוב על כ-236 מיליון ש"ח, והיקף כוח האדם כלל 32 עובדי מדינה, 17 סטודנטים ו-391 נותני שירותים. בשנת 2020 החליטה הממשלה על הקמת משרד הדיגיטל הלאומי, ועל העברת שטח הפעולה של רשות התקשוב למשרד החדש[13].

מטרות רשות התקשוב, כפי שנקבעו בהחלטות הממשלה האמורות, הן, בין היתר, הנחלת ארכיטקטורה וסטנדרטים אחידים ליחידות התקשוב בממשלה; קידום שיתוף מאגרי מידע וידע מקצועי בין גופי הממשלה; ייזום פרויקטי מחשוב רוחביים בממשלה וניהולם; הקמת מערך דיווח ותפעולו, והגברת שקיפות פעילות התקשוב הממשלתית; קידום שיתוף ידע מקצועי בין אגפי מערכות המידע; ליווי ובקרה של פרויקטי תקשוב משרדיים משמעותיים; קידום פלטפורמות רוחביות ויישומים ייעודיים להנגשת מידע ושירותים ממשלתיים לציבור והפעלתם. כן הוחלט להכפיף את כלל משרדי הממשלה להוראותיו המקצועיות של מנהל התקשוב הממשלתי, ולחייבם להיוועץ עימו בכל הקשור לתוכניות העבודה בתחום התקשוב ולתקציב המחשוב המשרדי.

באוקטובר 2014 התקבלה החלטת הממשלה 2097 "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'"[14] (להלן החלטת ממשלה 2097). בין היתר עסקה החלטת הממשלה במעבר למחשוב ענן. בהחלטה נקבע כי "לצורך קידום...תשתיות טכנולוגיות רוחביות על הממונה על התקשוב הממשלתי לפעול להעברת תשתיות התקשוב של משרדי הממשלה למודל 'מחשוב ענן', אשר יאפשר גישה מקוונת לתשתיות, פלטפורמות ויישומים ותשלום על פי השימוש בהם". לשם כך, הוחלט להטיל על התקשוב הממשלתי, בתיאום עם ראש המטה הקיברנטי הלאומי[15] ובהתייעצות עם ראש רמו"ט[16]

11 החלטת הממשלה 3058, "הקמת יחידת מטה ותקשוב ממשלתי במשרד האוצר" (27.3.11).

12 החלטת הממשלה 2099, "העברת שטח הפעולה של התקשוב הממשלתי ממשרד האוצר למשרד ראש הממשלה" (10.10.14).

13 החלטת הממשלה 56, "הקמת משרד הדיגיטל הלאומי ותיקון החלטות ממשלה" (7.6.20).

14 ראו מבקר המדינה, **דוח שנתי 70ב**, "המשרד לשוויון חברתי - המיזם הלאומי 'ישראל דיגיטלית'", עמ' 1589-1511.

15 בהחלטה מס' 2444 (15.2.15) החליטה הממשלה על שינוי שמו של המטה הקיברנטי הלאומי ל-"מטה הסייבר הלאומי". בהחלטה מס' 3270 (17.12.17) החליטה הממשלה לאחד את מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר לכדי יחידה ארגונית אחת - מערך הסייבר הלאומי.

16 רמו"ט - הרשות למשפט, טכנולוגיה ומידע. כיום מכונה הרשות להגנת הפרטיות. יחידה במשרד המשפטים האמונה על הסדרה, פיקוח ואכיפה של החוק להגנת הפרטיות ותקנותיו.

ומנהלי אגפי מערכות המידע במשרדים, להכין תוכנית למעבר למודל "מחשוב ענן" ולהציגה לוועדת השרים[17] עד סוף הרבעון הראשון של שנת 2015.

נמצא כי רשות התקשוב טרם הציגה לוועדת השרים תוכנית למעבר למודל מחשוב ענן כנקבע בהחלטת הממשלה מאוקטובר 2014.

רשות התקשוב מסרה למשרד מבקר המדינה בתשובתה מפברואר 2021 (להלן - תשובת רשות התקשוב) כי ועדת השרים לענייני תקשוב, שיפור השירות הממשלתי לציבור וממשל פתוח שהוקמה באוקטובר 2014, פוזרה עם פיזור הממשלה ה-33 במרץ 2015, טרם סיום הכנת תוכנית המעבר למודל מחשוב ענן. רשות התקשוב הכינה תוכנית מעבר לענן בשנת 2016, אולם ועדת השרים לא הוקמה מחדש בממשלות שבאו לאחר מכן.

יצוין כי במענה רשות התקשוב על ממצאי ביקורת קודמת של משרד מבקר המדינה צוין כי לאחר סיום תהליך התכנון של הקמת הענן הרשות תגיש תוכנית מפורטת לאישור הממשלה[18].

מומלץ כי רשות התקשוב תציג לממשלה תוכנית מעודכנת למעבר למודל מחשוב ענן, אשר תכלול את מתווה המעבר של הממשלה לסביבת הענן, לרבות לוחות זמנים ואבני דרך, במונחי תשומות ההשקעה במעבר ותוצאותיו.

עוד נקבע בהחלטת ממשלה 2097 כי "לצורך תכנון מפורט של העברת תשתיות התקשוב למודל 'מחשוב ענן' ושל הקמת הרשת הפנים ממשלתית, יקצה משרד האוצר לתקשוב הממשלתי תקציב חד פעמי בסך 2.6 מיליון ש"ח לשנת 2015 וכן תקציב בסך 1 מיליון ש"ח לשנת 2016". יצוין כי על פי ההחלטה, "תקצוב ביצוע הפרויקטים 'מחשוב ענן', רשת פנים ממשלתית ודיגיטציה של שירותים ממשלתיים...וכן תקצוב העלות השוטפת (משנת 2018 ואילך) של פרויקט האתר האחוד יותנה במימוש החיסכון הצפוי בתקציבי אגפי מערכות המידע עם המעבר למודל 'מחשוב ענן'...הממונה על התקציבים יוסמך לאסוף עד מחצית מהיקף החיסכון שייקבע מתקציבי אגפי מערכות המידע במשרדים, וזאת שנה לאחר מועד מעבר המשרדים למודל 'מחשוב ענן', כפי שייקבע בתכנון המפורט". בנוסף, בהחלטת ממשלה 326 מיום 16.8.2020 הוקצה תקציב של 250 מיליון ש"ח לעידוד הגירה של מערכות לסביבת הענן.

ביולי ובדצמבר 2020 מסרה רשות התקשוב למשרד מבקר המדינה כי גובש מתווה לתקצוב מעבר מערכות מידע לענן, אשר כולל קיצוץ רוחבי של 3% מתקציבי אגפי מערכות מידע והפניית הכסף לקרן ייעודית אשר מטרתה לסייע למשרדים בהעברת המערכות לסביבת ענן. מתווה זה היה אמור להיות מאושר במסגרת חוק ההסדרים ותקציב המדינה לשנת 2020, אולם נכון למועד הביקורת הוא טרם אושר. רשות התקשוב מסרה במרץ 2021 למשרד מבקר המדינה כי הסכומים המופיעים בהחלטת הממשלה 326 מאוגוסט 2020 נועדו לשמש לעידוד הגירה לשירותי ענן, והם מבוססים על הערכה ראשונית לקצב ההוצאה המשוער המיועד למימוש במסגרת פרויקט נימבוס (ראו הרחבה להלן בפרק "פרויקט נימבוס"). כמו כן מסרה רשות התקשוב כי התקציב

17 על פי חוק יסוד: הממשלה, רשאית הממשלה למנות ועדות שרים קבועות, זמניות או לעניינים מסוימים; מונתה ועדה, רשאית הממשלה לפעול באמצעותה. ועדות השרים פועלות כזרועה הארוכה של הממשלה. במקרה דנן מדובר בוועדת השרים לתקשוב.

18 ראו מבקר המדינה, **דוח שנתי 67ב**, "משרד ראש הממשלה - רשות התקשוב הממשלתי", עמ' 184

טרם הועבר לידיה וטרם סוכם אופן המימוש שלו, וכי במסגרת הרובד השני של פרויקט נימבוס תיבנה תוכנית מפורטת - לרבות שלבי הכנה, הערכות עלות ביצוע לשלבים אלו ועוד.

עולה אפוא כי עד מועד סיום הביקורת, באוקטובר 2020, טרם הושלם יישום תקציב מעבר מערכות המידע במשרדי הממשלה לענן.

מומלץ כי רשות התקשוב ומשרד האוצר יפעלו למימוש הקצאת התקציב למעבר משרדי הממשלה לענן.

בפברואר 2016 פרסמה רשות התקשוב את הנחיית ראש הרשות בנושא ענן ציבורי. על פי ההנחיה, "רשות התקשוב הממשלתי פועלת לקידום העברת מערכות המידע הממשלתיות לתשתית מחשוב ענן (IL-GOV-Cloud)...מטרת המעבר לתשתיות ענן ממשלתי, בין היתר, הינה לייצר סביבת עבודה מודרנית ומתקדמת לתשתיות המחשוב הממשלתיות. הכוונה היא להפעיל תשתית זו החל בשנת 2018, תוך ביצוע הגירה מדורגת אשר תימשך מספר שנים". המסמך מבהיר כי סביבת הענן הציבורי תמשיך לפעול גם כאשר תוקם תשתית הענן הממשלתי. ההנחיה מפרטת את התנאים שבהם רשאים המשרדים להשתמש בתשתית של ענן ציבורי, לרבות הגשת בקשה מפורטות לוועדה המייעצת של היחידה להגנת הסייבר בממשלה.

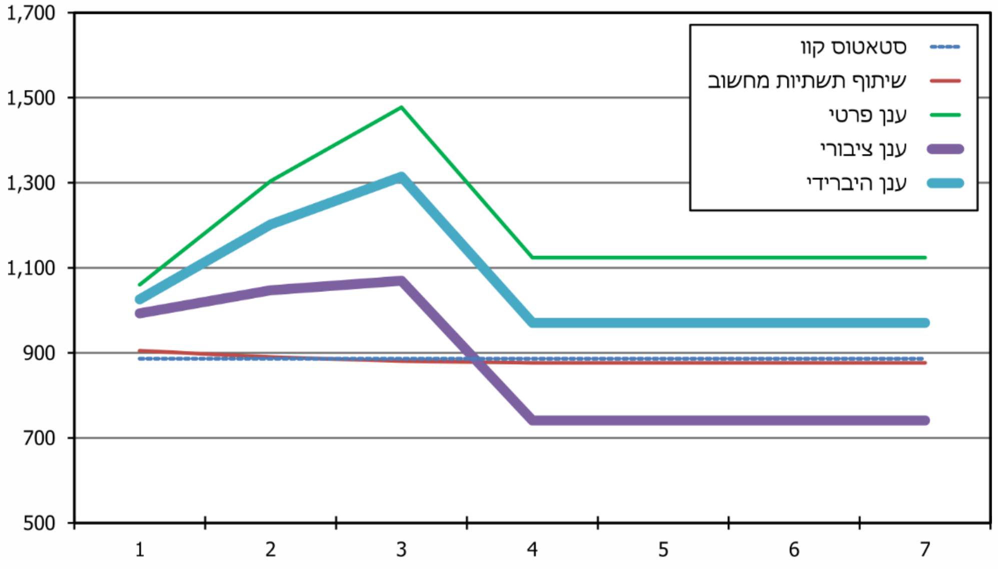
בנובמבר 2016 פרסמה רשות התקשוב את מדיניות מימוש חזון מחשוב הענן במשרדי הממשלה. מסמך זה התווה את המדיניות שעל פיה מחויבים לפעול משרדי הממשלה למימוש חזון מחשוב הענן. על פי המסמך, המעבר לתשתית הענן הממשלתי אמור לסייע בכמה היבטים: שיפור רמת השירות לציבור; יכולת גידול וגמישות תפעולית; הגדרת סטנדרטים אחידים והטמעתם; הגדרת מדיניות אבטחת מידע אחידה; הפחתת עלויות תפעול שוטף; שיפור רמות השירות ותהליכי העבודה; והצבת משרדי הממשלה בחזית הטכנולוגית. המדיניות עוסקת בין היתר בהקמת ענן ממשלתי על גבי תשתיות ייעודיות, אשר הגישה אליו תהיה דרך רשת ייעודית שלא תחובר למרשתת הציבורית.

על מנת לעודד שימוש בשירותי ענן ציבורי, באוקטובר 2017 פרסמה רשות התקשוב את המכרז המרכזי 21/17 ל"רכש שירותי ענן ציבורי". במכרז נכתב כי רשות התקשוב "מקדמת תוכנית לקידום העברת מערכות מידע ממשלתיות לתשתית מחשוב ענן", וכן כי "מימוש התכנית נעשה בשני ערוצים...הקמת תשתית ענן ממשלתית על גבי תשתית ענן פרטית; עידוד השימוש בתשתיות ענן ציבורי - נושא מכרז זה".

בד בבד התקשרה רשות התקשוב עם יועץ חיצוני בין-לאומי לצורך בחינת העברת תשתיות המחשוב מתצורה מקומית לתצורת ענן (מפת דרכים - DCT[19]). במהלך שנת 2018 בחן היועץ כמה חלופות: הקמת ענן פרטי לממשלה בלבד, הקמת ענן קהילתי, הקמת ענן היברידי והקמת ענן ציבורי. להלן פירוט ניתוח העלויות שבוצע:

19 Data Center Transformation - DCT

תרשים 3: **ניתוח עלויות לפי שנים של חלופות המעבר לתצורת ענן, 2018 (במיליוני ש"ח)**



מקור: נתוני רשות התקשוב.

מהתרשים ניתן ללמוד כי חלופת הקמת ענן ממשלתי פרטי היא החלופה היקרה ביותר, וכי לאחר שלוש שנים חלופת הענן הציבורי זולה יותר אף מהשארת המצב כמו שהוא (סטטוס קוו). ניתוח העלויות של החלופות הביא את רשות התקשוב להחליט כי בניגוד לתכנון, המיקוד בשלב הראשון יהיה בהקמת ענן ציבורי ולא בהקמת ענן ממשלתי פרטי. מיקוד זה הביא לייזום פרויקט נימבוס (ראו הרחבה להלן בפרק "פרויקט נימבוס").

במרץ 2020 פרסמה רשות התקשוב עדכון למסמך המדיניות האמור[20]. במסמך החדש נוספה התייחסות לפעילות שנועדה לקדם את פרויקט נימבוס על רבדיו השונים, וכן נכתב שהרשות מעודדת שימוש בשירותי ענן עוד לפני הקמת תשתית ענן בישראל. כמו כן, הצהירה הרשות כי היא מבקשת להוביל תפיסת Cloud Native במשרדי הממשלה - בנייה והפעלה של יישומים בסביבות טכנולוגיות מתקדמות ודינמיות.

בנובמבר 2020 פרסמה רשות התקשוב את מסמך ההנחיה "עקרונות פיתוח מערכות להיערכות לענן". על פי ההנחיה, קיימת תלות בין כל רכיבי הפיתוח של מערכת (כגון: ארכיטקטורת מערכת, תהליך הפיתוח וההפצה, ממשקים ועוד) על מנת לייצר מערכת גומלין[21] ארגונית מוכנה לענן, וכי השאיפה של רשות התקשוב היא שהפיתוח המתקיים בממשלה יותאם לעקרונות פיתוח חדישים ובכך יתאים למעבר לענן.

משרד מבקר המדינה רואה בחיוב את פרסומי המדיניות וההנחיות של רשות התקשוב ואת עדכונן בהתאם להתפתחויות הטכנולוגיות.

20 להרחבה ראו: https://www.gov.il/he/departments/policies/cloud_policy

21 מערכת של גורמים - מוסדות, ארגונים וכדומה - והיחסים ביניהם המשפיעים על דבר מסוים (Ecosystem).

לצד המדיניות הממשלתית שפרסמה רשות התקשוב, בשנים האחרונות פרסמו כמה גופי אסדרה רגולציה פרטנית בנושא מחשוב ענן. להלן דוגמאות אחדות:

1. ביוני 2015 פרסם המפקח על הבנקים שבבנק ישראל (להלן - המפקח) מכתב לתאגידים הבנקאיים בנושא מחשוב ענן. במכתב דרש המפקח מהבנקים קבלת אישור של בנק ישראל מראש לפני שימושם במחשוב ענן, איסור על שימוש במחשוב ענן לצורכי פעילויות הליבה של הבנקים, גיבוש מדיניות פנימית לשימוש במחשוב ענן, עריכת בדיקת נאותות מקדימה לספק שירותי הענן, הכפפת ספק שירותי הענן לביקורות מצד המפקח והגבלות טריטוריאליות על אחסון מידע אישי של לקוחות באמצעות מחשוב ענן. ביולי 2017 פרסם המפקח הוראה שנועדה להחליף את המכתב האמור לעיל, ובחודש נובמבר 2018 פרסם המפקח עדכון להוראה, כך שכיום ניתנת האפשרות לתאגידים הבנקאיים כהגדרתם בהוראה ליישם טכנולוגיית ענן ללא צורך בהיתר מראש מהמפקח. עם זאת האיסור על עשיית שימוש בשירותי מחשוב ענן עבור פעילויות ליבה או מערכות ליבה נותר בעינו. ההוראה מעבירה את האחריות לניהול הסיכונים אל התאגיד הבנקאי ומחזקת את המעורבות של הדירקטוריון ושל ההנהלה הבכירה. בנוסף, התאגידים הבנקאיים יידרשו אחת לשנה להעביר למפקח רשימה מעודכנת של יישומי הענן ורשימה של יישומי ענן עתידיים.
2. בינואר 2021 פרסם משרד התחבורה את מדיניות "הגנת הסייבר למגזר התחבורה". בין היתר המדיניות עוסקת גם בשימוש בשירותי מחשוב ענן, ומנחה את הגוף המגזרי לבצע תהליך של בחינה והערכה של הסיכונים במימוש השירות בענן, ולתכנן את היישום ואת בקרות ההגנה באופן שימזער סיכונים אלה, תוך עמידה בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. במקרים של בחינת העברת שירותים חיוניים לענן, על הגוף המגזרי לפנות לקבלת אישור אגף הסייבר במשרד התחבורה טרם קבלת ההחלטה.
3. באוגוסט 2016 פרסמה רשות שוק ההון, ביטוח וחסכון[22] את חוזר מנכ"ל "ניהול סיכוני סייבר בגופים מוסדיים". החוזר מאפשר לגופים השונים שימוש בשירותי מחשוב ענן בכפוף לכמה פעילויות, לרבות הערכת סיכונים ייעודית, הצפנת מידע, יכולת שליטה ובקרה ועוד.
4. ביולי 2019 העביר משרד הבריאות לגופי הבריאות השונים לקבלת הערותיהם טיוטת חוזר מנכ"ל בנושא השימוש במחשוב ענן. בפברואר 2021 פרסם המשרד את חוזר מנכ"ל 2/2021 בנושא השימוש במחשוב ענן במערכת הבריאות, אשר מטרתו "קביעת אמות מידה להפעלה נאותה של יישומי מחשוב באמצעות מחשוב ענן על ידי ארגוני בריאות כדי לעודד כניסת טכנולוגיות מתקדמות לשימוש". החוזר מפרט את הצורך במדיניות ענן ארגונית ובוועדת ענן ארגונית; את תנאי הסף לשימוש במחשוב ענן; את אופן הפעלת יישום בענן; את תהליך ההתקשרות עם ספק הענן; ואת אופן התיעוד, הדיווח והשמירה של המידע והמסמכים הנוגעים להפעלת יישום בענן.

עלה כי משרד הבריאות השלים, במהלך הביקורת, הפצת חוזר מנכ"ל בנושא השימוש במחשוב ענן במערכת הבריאות.

---

22 אז אגף שוק ההון, ביטוח וחיסכון במשרד האוצר. רשות שוק ההון, ביטוח וחסכון היא רגולטור פיננסי עצמאי בישראל המפקח על גופים פיננסים חוץ-בנקאיים, ובהם חברות ביטוח, קרנות פנסיה, גמל והשתלמות, וכן על מתן שירותים פיננסיים מוסדרים כגון נותני אשראי חוץ-בנקאי.

גופים ממשלתיים וציבוריים שונים שוקדים על גיבוש ופרסום קווים מנחים וחוזרים בנושא מחשוב ענן, מתוך זיהוי הסיכונים הטמונים בהעברת מידע ופעילות לענן.

לצד השמירה על עצמאות גופי האסדרה, מוצע לרשות התקשוב לעקוב אחר האופן שבו מקדמים ומיישמים גופים ממשלתיים את המעבר למחשוב ענן על מנת לוודא כי כל התחומים הרלוונטיים נלקחים בחשבון. מומלץ כי רשות התקשוב תבחן הנחלת מדיניות אחידה לכלל הגורמים אשר תוכל לשמש כבסיס לרגולציות פרטניות. פעולה זו עומדת בהלימה לתפקידי רשות התקשוב כפי שהוגדרו על ידי הממשלה.

עוד מומלץ כי רשות התקשוב תטמיע הסדר לפיו כל גורם מאסדר במערכת הממשלתית אשר מעוניין להוציא חוזר בתחום מחשוב ענן לגופים ממשלתיים הפועלים תחת פיקוחו, יעשה זאת לאחר שטיוטת החוזר תתואם עם רשות התקשוב ותוצג במסגרת ועדת התקשוב העליונה[23]. באופן זה ניתן יהיה לקיים בקרה נוספת על הוצאת החוזרים כאמור, וכן הדבר יתרום לתיאום וסנכרון בין המדיניות הממשלתית הכוללת אל מול פעולותיהם של הגורמים המאסדרים השונים.

רשות התקשוב מסרה בתשובתה כי היא קיימה בשנים האחרונות עבודת מטה יסודית עם כלל גופי האסדרה על מנת לוודא כי הפתרון שפרויקט נימבוס מספק יאומץ על ידם ויבטיח מענה מיטבי לצורכיהם בהיבטים של רכש, סטנדרטיזציה והיבטים תפעוליים ורגולטוריים נוספים. בנוסף, בכוונת רשות התקשוב להקים מרכז מצוינות תפעולי בענן (CCoE) שיעקוב אחר האופן שבו גופים ממשלתיים מקדמים ומיישמים את המעבר למחשוב ענן, ויוודא כי כל התחומים הרלוונטיים נלקחים בחשבון. בתוך כך תפעל הרשות להנחיל מדיניות אחידה לכלל גורמי האסדרה אשר תוכל לשמש בסיס לרגולציות פרטניות, על אף שהנחיה כזאת אינה מתחייבת מתוקף תפקידיה הרשמיים של הרשות.

קביעת מדיניות לאומית - השוואה בין-לאומית

ממשלות שונות בעולם עמדו על הצורך בקידום מדיניות לאומית למעבר לטכנולוגיית ענן. להלן כמה דוגמאות מהעולם שמהן ניתן לעמוד על מעורבות הממשלות בנושא טכנולוגיות ענן:

23 ועדת התקשוב העליונה פועלת כגוף מקצועי המסייע לראש רשות התקשוב לממש את אחריותו וסמכותו, בין היתר בליווי תוכניות עבודה ופיקוח עליהן, בליווי מיזמי תקשוב משמעותיים ופיקוח עליהם, במתן חוות דעת מקצועית ועוד. בראש הוועדה עומד ראש רשות התקשוב וחברים בה נציגים מרשות התקשוב, ממשרד האוצר (מינהל הרכש, אגף תקציבים ולשכה משפטית) ומספר מנמ"רים של משרדי ממשלה.

לוח 1: **דוגמאות מהעולם למעורבות השלטון המרכזי בנושא טכנולוגיות ענן**

המדינה	פירוט מעורבות השלטון המרכזי בנושא טכנולוגיות ענן
אוסטרליה	בשנת 2017 פרסמה ממשלת אוסטרליה את אסטרטגיית הענן שלה[24], שכותרתה "אסטרטגיית ענן מאובטח" (Secure Cloud Strategy), אשר מחליפה אסטרטגיה קודמת בנושא. על פי מסמך האסטרטגיה, למעבר לטכנולוגיית ענן ישנם יתרונות רבים אך גם אתגרים משמעותיים. האסטרטגיה הכללית נועדה לשמש נקודת מוצא, אך על משרדי הממשלה לעצב את אסטרטגיית הענן שלהם בעצמם.
בריטניה	בשנת 2013 הציגה ממשלת בריטניה את מדיניות "ענן תחילה" (Cloud First)[25]. על פי המדיניות, בכל תהליך של רכש של שירות, קיים או חדש, גופי המגזר הציבורי צריכים לבחון ולהעריך ביסודיות חלופות ענן שונות לפני קבלת החלטה, תוך העדפה לענן ציבורי על פני חלופות אחרות. כחלק ממימוש מדיניות הענן מפרסמת ממשלת בריטניה מאז שנת 2013 הסכמי מסגרת לאספקת שירותי ענן. באוקטובר 2019 פרסם השירות הדיגיטלי הממשלתי של בריטניה (GDS) כי המדיניות הממשלתית "ענן תחילה" תישאר בתוקף גם בהמשך ולא תעבור שינוי או עדכון.
ארצות הברית	העיסוק של הממשל הפדרלי בארצות הברית בנושא מחשוב ענן החל כבר בשנת 2010 עם פרסומו של מסמך בנושא "תוכנית יישום לרפורמה בניהול ה-IT הפדרלי". התוכנית התמקדה בהסרת חסמים לניהול אפקטיבי של תוכניות בתחומי טכנולוגיות המידע בממשל הפדרלי. במהלך השנים פורסמו טיוטות ויוזמות שונות, וביוני 2019 הטכנולוג הממשלתי הראשי פרסם את אסטרטגיית "ענן חכם"[26] המושתתת על שלושה עקרונות בסיס: אבטחה, רכש וכוח אדם. על פי האסטרטגיה, שילוב העקרונות מגלם את הגישה הבין-תחומית הנדרשת כדי לספק שירותים בטוחים ואיכותיים יותר לציבור.
אירלנד	בשנת 2012 פרסמה אירלנד[27] את אסטרטגיית מחשוב הענן שלה לסקטור הציבורי. אסטרטגיה זו היא חלק מגישת-העל של הממשל האירי להשתמש בטכנולוגיות מידע ותקשורת (ICT)[28] כדי להביא לרפורמה בשירות הציבורי, תוך מתן דגש מיוחד על מחשוב ענן כמרכיב מרכזי. האסטרטגיה מכוונת להפוך את אירלנד למובילה בתחום מחשוב הענן, והתקווה היא שאימוץ הענן בסקטור הממשלתי יתרום לאימוצו בסקטור הפרטי. באוקטובר 2019 פרסמה אירלנד מזכר המחזק אסטרטגיה זו וקובע כי "הממשלה סבורה כי זהו זמן מתאים לגישה יזומה ומתקדמת לאימוץ מחשוב ענן"[29].
סינגפור	בשנת 2018 ממשלת סינגפור הודיעה על תוכנית חומש להעברת מרבית מערכות המידע שלה מתשתית מקומית לענן ציבורי, כדי לשפר את איכות השירותים הניתנים לעסקים ולאזרחים. נכון ליוני 2020, יותר מ-150 מערכות מידע (עד וכולל רמת סיווג "מוגבל") הועברו לענן הציבורי[30], ועל פי תוכנית החומש המטרה היא להעביר תוך חמש שנים כ-70% ממערכות המידע של הממשלה לענן.
האיחוד האירופי	באוקטובר 2020 חתמו[31] מדינות חברות באיחוד האירופי על הצהרה ל"קידום הדור הבא של טכנולוגית הענן באירופה". על פי המסמך, המדינות יפעלו יחד על מנת לייצר תשתית ושירותי ענן תחרותיים, הן למגזר הפרטי והן למגזר הציבורי.

על פי נתונים שאסף משרד מבקר המדינה

24 להרחבה ראו: https://www.dta.gov.au/our-projects/secure-cloud-strategy

25 להרחבה ראו: www.gov.uk/guidance/government-cloud-first-policy

26 להרחבה ראו: cloud.cio.gov

27 להרחבה ראו: ictstrategy.per.gov.ie/ictstrategy/files/Public%20Service%20ICT%20Strategy.pdf

28 ICT - (Information and Communication Technology)

29 להרחבה ראו: www.gov.ie/en/publication/078d54-cloud-computing-advice-note-october-2019/

30 להרחבה ראו:
https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services

31 להרחבה ראו: ec.europa.eu/newsroom/dae/document.cfm?doc_id=70089

מהאמור עולה כי מדינות רבות מקדמות את השימוש הממשלתי בענן הציבורי, מתוך הבנה כי הנושא הכרחי לקידום מוכנות גבוהה יותר לטכנולוגיה המתפתחת ולאתגרים שיעמדו לפני המדינות בעתיד.

פרויקט נימבוס

רקע

בפברואר 2019 הודיע מינהל הרכש על כוונתו לפרסם מכרז מרכזי לאספקת שירותי ענן המבוססים על מסדת (פלטפורמה) ציבורית (להלן - נימבוס). על פי ההודעה, נימבוס הוא פרויקט רב-שנתי, שנועד לתת מענה מקיף ומעמיק לנושא אספקת שירותי ענן עבור משרדי הממשלה ויחידות הסמך. נימבוס צפוי לכלול כמה רבדים הנוגעים הן ליצירת הערוץ לאספקת שירותי הענן בפועל והן לגיבוש מדיניות ממשלתית בנושא, הגירה לענן וביצוע בקרה ומיטוב (אופטימיזציה) של הפעילות בו. יצוין כי יישומו של מכרז נימבוס אינו כרוך בעלויות, שכן מדובר במעין "זיכיון" שמאפשר לספק הזוכה להקים על חשבונו תשתית, אשר תהיה התשתית המועדפת ליישום שירותי ענן עבור כל המערכת הממשלתית. לצורך קידום הפרויקט הוקם צוות מקצועי ייעודי בהובלת מינהל הרכש ובשיתוף רשות התקשוב ומערך הסייבר, ונערכה עבודת מטה ללימוד התחום ולגיבוש מתווה המכרז. בחודשים אוגוסט וספטמבר 2019 פורסמו פניות לקבלת הערות הציבור על טיוטת עקרונות המכרז המרכזי, שכללו ארבעה רבדים:

1. אספקת שירותי ענן על גבי מַסֶדֶת ציבורית - ברובד זה ייבחרו שני ספקים לאספקת שירותי ענן עבור ממשלת ישראל על גבי מסדת ציבורית. כל אחד מהספקים הזוכים יידרש להקים בשטח מדינת ישראל אתר מקומי (Region) אשר יעמוד בדרישות האבטחה, העמידות והרציפות התפעולית התואמות את צורכי ממשלת ישראל. הענן שיוקם יוכל לספק שירותים לא רק לממשלת ישראל, כי אם לכלל המשק בישראל ואף ללקוחות מחו"ל.

2. גיבוש מדיניות מרכזית והקמת מרכז למצוינות במחשוב ענן (Cloud Center of Excellence או CCoE) - ברובד זה ייבחר ספק אשר ישמש כגוף רוחבי מרכזי למשילות של תהליכי מחשוב הענן הארגוני. הספק יסייע בהנעת תהליכי ההגירה לענן, בהם הגדרת מדיניות ענן, ליווי המשרדים במעבר לענן, הגדרת ארכיטקטורת פתרונות ענן, מתן הנחיות והגנות לגידור הסיכונים ועוד.

3. אספקת שירותי מודרניזציה והגירה (מיגרציה) - ברובד זה תיבחר רשימת ספקים אשר יסייעו למשרדים השונים לבצע את ההתאמות הנדרשות על מנת להקים מערכות חדשות בסביבת הענן וכן להסב אליה מערכות קיימות.

4. אספקת שירותי ניטור ומיטוב (אופטימיזציה) - ברובד זה תיבחר רשימת ספקים אשר יסייעו למשרדים לבצע את הבקרה הנדרשת של צריכת שירותי הענן ואת אפשרות המיטוב של צריכת השירותים ברמה הממשלתית.

התרשים שלהלן מפרט את סטטוס פרויקט נימבוס בפברואר 2021[32]:

תרשים 4: **התקדמות פרויקט נימבוס, פברואר 2021**

על פי נתוני מינהל הרכש הממשלתי, בעיבוד משרד מבקר המדינה.

בנובמבר 2020 מסר מינהל הרכש למשרד מבקר המדינה כי פרסום המכרזים עבור הרובד השלישי והרביעי תלוי בין היתר בתוצאות המכרז של הרובד הראשון, ולכן בשלב זה לא ניתן להעריך מתי יפורסמו המכרזים ומה יהיה משך הזמן מפרסום המכרזים ועד לפרסום הזוכה ברבדים אלו. בתשובת מינהל הרכש למשרד מבקר המדינה מפברואר 2021 (להלן - תשובת מינהל הרכש) נמסר כי הוחלט להקדים את פרסום רובד 3 (אשר כאמור פורסם בפברואר 2021) לפני בחירת ספקים זוכים ברובד 1, וכי הספקים הזוכים ברובד 3 יידרשו להשלים הסמכות בהתאם לספקים שיזכו ברובד 1. מטרת מהלך זה היא קידום המענה למשרדים לצד הרחבת ההזדמנויות לספקים נוספים להצטרף לרשימה. כמו כן מסר מינהל הרכש כי רובד 4 אינו ניתן לפרסום לפני פרסום הזוכים ברובד 1 וברובד 2, עקב התלות התשתיתית שעשויה להתקיים ביניהם.

נמצא כי נכון למרץ 2021, פורסמו מכרזים לרבדים 1-3 וטרם פורסמו זוכים לרבדים אלו[33]. עוד נמצא כי טרם פורסם מכרז לרובד 4 וכי אין לוח זמנים ליישום רובד זה ולסיום המכרז כולו.

לאור העובדה כי הצלחת פרויקט נמדדת בין היתר בעמידה בלוחות הזמנים ביחס לתכנון[34], מומלץ כי מינהל הרכש ורשות התקשוב יקבעו לוח זמנים ליישום הרובד הרביעי ולסיום מכרז נימבוס כולו.

32 יצוין כי בסמוך למועד סיכום דוח הביקורת, באפריל 2021, הודיע אגף החשב הכללי במשרד האוצר כי שתי ספקיות ענן נבחרו כמועמדות לזכייה ברובד הראשון של מכרז נימבוס. לאחר שישלימו את כל התנאים כמועמדות לזכייה, יוכרזו הזוכות ויחלו בהיערכות לאספקת השירותים ובכלל זה, הקמת אתרי ענן מקומיים בישראל בהשקעה ראשונית המוערכת בכ-4 מיליארד שקלים. כמו כן הודיע אגף החשב הכללי כי נבחרה חברת ייעוץ כזוכה ברובד השני של המכרז לייעוץ וליווי הקמת ה-CCoE.

33 ראו ה"ש 32 לעיל.

34 ראו למשל: הנחית ראש רשות התקשוב הממשלתי, "מחזור חיי מערכת תקשוב", סעיף 4.8; מדריך גוף הידע בניהול פרויקטים: (PMBOK Guide) (2018), מהדורה שישית, עמ' 173.

רשות התקשוב מסרה בתשובתה כי מכרז נימבוס הוא דו-שלבי, והוא כלל שלב לימוד ארוך בתחום סבוך ומורכב עם שותפים רבים. למרות המורכבות בתחום המקצועי ובהיקף התיאום הנדרש, נשמרו לוחות הזמנים באופן מוקפד ומדוקדק, תוך גיוס תשומות ניהוליות של כלל הגורמים והגופים הרלוונטיים, וכל זאת בעת משבר עולמי ובתקופה של אי-יציבות ממשלתית.

ביוני 2020 הודיע מינהל הרכש כי משרד הביטחון (בשם צה"ל) עתיד להצטרף למכרז נימבוס כגוף נלווה, ולהיות צרכן של שירותי ענן על גבי מסדת ציבורית מהספק הזוכה. מפגישה שקיים משרד מבקר המדינה בספטמבר 2020 עם מינהלת הטרנספורמציה הדיגיטלית, המשויכת לאגף התקשוב בצה"ל, עלה כי בשנים האחרונות צה"ל משקיע משאבים רבים בהכנת תשתיות המחשוב לעבודה בסביבת ענן כחלק מיישום החזון לטרנספורמציה דיגיטלית. כחלק מההיערכות החליט צה"ל לחבור לפרויקט נימבוס על מנת לאפשר העברה של מערכות לא מסווגות לסביבת הענן הציבורי. כמו כן מסר צה"ל למשרד מבקר המדינה כי הוא נמצא בקשר שוטף עם רשות התקשוב ומינהל הרכש לגבי התקדמות הפרויקט. בתשובתו מסר מינהל הרכש כי משרד הביטחון וצה"ל מהווים חלק מובנה בצוותי העבודה של המכרז, הן בשלב גיבוש הדרישות והן בשלב בדיקת ההצעות.

משרד מבקר המדינה מציין את הרחבת פרויקט נימבוס תוך שילוב גופים נוספים, כגון גופים מוסדיים ופיננסיים, וכן את שילובו של צה"ל בפרויקט. הרחבת הפרויקט מאפשרת איגום משאבים לאומי ויעילות תקציבית.

מכרז המסגרת של רשות התקשוב מול מכרז נימבוס

ביולי 2017 פרסמה רשות התקשוב מכרז מסגרת[35] 21/17 לרכש שירותי ענן ציבורי. בינואר 2018 אישרה ועדת המכרזים המשרדית את בדיקת ההצעות והספקים הזוכים במכרז, 34 במספר.

הוראת תכ"ם 7.3.8.1 קובעת כי "במקרה שבו ערך החשב הכללי מכרז מרכזי עבור הממשלה או פרסם הודעה על כוונתו לפרסם מכרז לפחות שישה חודשים מראש לכל הפחות, לא יערוך משרד מכרז ולא יתקשר בכל דרך אחרת...אלא באמצעות המכרז המרכזי או באישור ועדת הפטור". קביעה זו עולה מהוראת תכ"ם 16.1.0.2 המפרטת את המכרזים המרכזיים שבתוקף, אלו שפורסמו אך טרם נבחר בהם זוכה ואלו שטרם פורסמו. כלומר, פרסום מכרז נימבוס מונע מהמשרדים שימוש במכרז המסגרת 21/17 לרכש שירותי ענן ציבורי.

במהלך הביקורת ביולי 2020, כשנתיים וחצי לאחר ההחלטה על הזוכים במכרז 21/17, ולבקשת רשות התקשוב, מינהל הרכש הממשלתי פרסם את אישורו כי על אף שמכרז המסגרת 21/17 הוא בנושא פרויקט נימבוס - מינהל הרכש יאפשר התקשרויות לטובת רכישת שירותי ענן ציבורי עד לכניסתו של מכרז נימבוס לתוקף בכפוף לתנאים מסוימים. בכך נתן מינהל הרכש את האפשרות לרשות התקשוב ולמשרדים לתת מענה לצרכים המיידיים שלהם, תוך שמירה על מנגנון הגירה מתאים עם כניסתו לתוקף של מכרז נימבוס. בד בבד פרסמה רשות התקשוב ביולי 2020 הנחיה שעניינה "יישום מכרז מסגרת מספר 21/17 למתן שירותי ענן ציבורי". ההנחיה

35 מכרז מסגרת הוא מכרז פומבי שבו נבחר יותר מספק אחד. זהות הספק ממנו תבוצע בפועל כל הזמנה של טובין, שירות או עבודה תיבחר בהתאם להליך תחרותי של פנייה פרטנית לספקים הזוכים.

מדגישה בין היתר כי מכרז המסגרת הוא פתרון זמני בלבד, שנועד לספק מענה לצורכי המשרדים עד לסיום מכרז נימבוס.

כאמור, במהלך הביקורת אישר מינהל הרכש הממשלתי להחריג את מכרז מסגרת 21/17 מהמכרז המרכזי של פרויקט נימבוס עד כניסתו לתוקף, ובכך אפשר לרשות התקשוב לתת מענה לצרכים המיידיים של משרדי הממשלה השונים בכל הקשור למעבר לשירותי ענן.

הסדרת שימוש הרשויות המקומיות בנימבוס

משרד הפנים מופקד על תכנונה וביצועה של המדיניות הלאומית בנושאי השלטון המקומי. המשרד פועל בשתי רמות: ברמה הארצית - מתן הנחיות וקביעת מדיניות; וברמה המחוזית - דרג הביצוע מקיים קשר עם הרשויות המקומיות. בין היתר, המשרד מפקח מטעם הממשלה על הרשויות המקומיות ואחראי להכוונת פעולותיהן בהתאם לחוק ולמדיניות הממשלה.

נכון ל-2019, בישראל יש 257 רשויות מקומיות המאוגדות תחת שתי עמותות. מרכז השלטון המקומי (להלן - מש"ם) הוא עמותה שבה מאוגדות כל העיריות והמועצות המקומיות בישראל, כ-200 במספר. מש"ם מייצג את הרשויות המקומיות כלפי הכנסת והממשלה וכן מספק לרשויות המקומיות הנחיה וייעוץ מקצועי בתחומי הפעילות השונים. בעמותה נפרדת, הנקראת "מרכז השלטון האזורי בישראל", מאוגדות המועצות האזוריות, שכל אחת מהן מאגדת מהבחינה המוניציפלית יישובים כפריים או קהילתיים וקיבוצים.

במסגרת תוכנית העבודה של מש"ם לשנת 2020, הוחלט על "אפיון צרכים וקביעת תנאי סף לטובת יציאה למכרז להקמת ענן מאובטח" במחצית הראשונה של השנה. במרץ 2020, לאחר פרסום מכרז הרובד הראשון בפרויקט נימבוס, התקיימו פגישות בין מינהל הרכש הממשלתי למש"ם לגבי השתתפות מש"ם בפרויקט כגורם מתכלל עבור הרשויות המקומיות. על בסיס פגישות אלו פנה באפריל 2020 מש"ם למשרד הפנים לשם קידום המהלך הרגולטורי הנדרש לצורך הגדרת מש"ם כגורם מתכלל. על פי הפנייה, אם משרד הפנים לא יקדם מהלך רגולטורי זה, מש"ם יפרסם מכרז מקביל לשירותי ענן טכנולוגי. במאי 2020 פרסם מש"ם שתי פניות לקבלת מידע[36], אחת לצורך הקמת ענן עבור הרשויות המקומיות והשנייה לצורך הקמת ענן אבטחת מידע עבורן.

ביוני 2020, שלושה חודשים לאחר פניית מש"ם, השיב משרד הפנים על הפנייה כי "מוצע להקים צוות עבודה משותף אשר יוסמך לקבל החלטות בנושא...הצוות ינוהל על ידי ראש מינהל הפיתוח במשרד הפנים, כמי שימשיך להיות אחראי על הגדרת המדיניות הכוללת בכל הקשור לשלטון המקומי גם בנושא זה, ויכלול נציגים מקצועיים נוספים". באותו חודש השיב מש"ם למשרד הפנים כי הבסיס לשיתוף פעולה בפרויקט נימבוס הוא כי מש"ם "יהיה שותף בהכנת המכרז וילווה את תהליך הטמעתו ברשויות המקומיות...מרכז השלטון המקומי יתכלל ויהווה גוף תווך לרשויות שלא יתקשרו באופן ישיר עם הזוכה במכרז". כמו כן ציין מש"ם כי לטעמו פרויקט נימבוס אינו מספק מענה מלא לנושא הסייבר ברשויות המקומיות.

מפגישות שקיים משרד מבקר המדינה ביוני 2020 עם מש"ם, משרד הפנים ומינהל הרכש, עלה כי הושגה הסכמה לתמיכה ביישום של מחשוב ענן ברשויות המקומיות, לייעול הפעילות שלהן

36 באנגלית RFI - Request For Information.

והשירות שהן נותנות לציבור. משרד מבקר המדינה עמד בעבר על הקשיים שבהם נתקלות הרשויות המקומיות בתחום הדיגיטלי ובשיתוף הפעולה עם השלטון המרכזי בהקשר זה[37].

ביולי 2020 התכנס לראשונה צוות מחשוב ענן בשלטון המקומי, אשר כלל נציגים ממשרד הפנים, רשות התקשוב, מינהל הרכש, מש"ם וישראל דיגיטלית. מסיכום הדיון עולה כי הרשויות המקומיות צורפו למכרז נימבוס ויכולות ליהנות מתנאיו, בדומה למכרזים אחרים של מינהל הרכש. בין היתר נדונו האתגרים שעימם יתמודדו רשויות מקומיות בבואן ליישם מערכות במחשוב ענן. עם זאת, לאחר הדיון העלה מינהל הרכש דרישה כי "על מנת שהמכרז ייתן מעמד מרכזי לרשויות המקומיות...יש לגבש במיידי התחייבות של מסה משמעותית של רשויות מקומיות אשר יתחייבו כי [כ]כל שיבחרו לרכוש שירותי ענן ציבורי, יעשו זאת באמצעות המכרז המרכזי בלבד".

באוקטובר 2020 מסר מש"ם למשרד מבקר המדינה כי למיטב ידיעתם דרישת מינהל הרכש להתחייבות מראש של רשויות מקומיות להצטרף למכרז נימבוס אינה אפשרית מהבחינה המשפטית, וכי מש"ם בוחן עם משרד הפנים דרכים לבטל דרישה זו. בנובמבר 2020 מסר משרד הפנים למשרד מבקר המדינה כי מינהל הרכש החליט לוותר על דרישתו להתחייבות האמורה, ובכך נסללה הדרך לשימוש של הרשויות המקומיות במכרז נימבוס. כמו כן, משרד הפנים עדכן בנובמבר 2020 את גורמי התקצוב הרלוונטיים במשרד האוצר ובמשרד הפנים לגבי חיבור הרשויות המקומיות לפרויקט נימבוס וההשלכות התקציביות האפשריות של החיבור.

מפגישות שקיים משרד מבקר המדינה עם מש"ם בנובמבר 2020 עולה כי לאור ההתקדמות שחלה בנושא, מש"ם החליט שלא להמשיך בתהליך הקמת ענן ציבורי באופן עצמאי לרשויות המקומיות. עם זאת, מש"ם מתכוון להמשיך בתהליך הקמת ענן אבטחת מידע לרשויות המקומיות, בין היתר בשל עיכובים החלים במתן פתרון על ידי משרד הפנים. משרד מבקר המדינה עמד בעבר על המחסור במרכז שליטה ובקרה מרכזי לטיפול ומתן מענה באירועי סייבר ברשויות המקומיות[38]. מפגישות שקיים משרד מבקר המדינה עם משרד הפנים בנובמבר 2020 עלה כי בשל היעדר תקציב עקב מערכות הבחירות לכנסת, לא חלה התקדמות במתן המענה של משרד הפנים ומערך הסייבר הלאומי לרשויות המקומיות.

צירוף הרשויות המקומיות למכרז נימבוס עשוי להביא לחיסכון במשאביהן ולסטנדרטיזציה בתחום מחשוב הענן. מומלץ כי משרד הפנים יגבש תוכנית רב-שנתית לשילוב הרשויות המקומיות במכרז נימבוס, תוך בחינת הפעולות הנדרשות ליישום מהלך זה במערכת מבוזרת הכוללת 257 רשויות מקומיות. בהכנת התוכנית ראוי לתת את הדעת להיבטים של קיום מתווה ראשוני הכולל הנחיות של המשרד לרשויות המקומיות, הסברה, הדרכה והטמעה, תקצוב וכיו"ב.

משרד הפנים מסר למשרד מבקר המדינה בתשובתו מפברואר 2021 (להלן - תשובת משרד הפנים) כי המשרד פעל לצירוף הרשויות המקומיות למכרז נימבוס, מתוך ההבנה של הערך המוסף בצירופן. לדעת המשרד נדרשת תשתית ניהול ברמה הארצית שנותנת מענה רחב בתחום התקשוב והדיגיטל, לרבות בתחום השימוש בענן. לאחרונה הציג אגף פיתוח ארגוני דיגיטציה וחדשנות ברשויות מקומיות תוכנית הוליסטית לניהול ותפעול של תשתיות טכנולוגיית מידע

---

37 מבקר המדינה, **דוח שנתי 70ג** (2019), "ההיערכות הממשלתית ליישום טכנולוגיות מתקדמות ברשויות המקומיות - מיזם ערים חכמות", עמ' 412-430.

38 מבקר המדינה, **דוח שנתי 70ג** (2019), "ההיערכות הממשלתית ליישום טכנולוגיות מתקדמות ברשויות המקומיות - מיזם ערים חכמות", עמ' 412-430.

(Information Technology - IT) ברמה הארצית, האזורית והמקומית, והיא נמצאת בשלבי דיון מול משרד הדיגיטל הלאומי.

בתשובת מש"ם מינואר 2021 למשרד מבקר המדינה (להלן - תשובת מש"ם) הוא מסר כי מש"ם מהווה גוף מייצג, מתכלל ומייעץ עבור כלל הרשויות בארץ, ומשכך הוא רואה עצמו ככזה גם בנושאי הטכנולוגיה השונים, ובהם פרויקט נימבוס. עם זאת, למרות שיתוף מש"ם בצוות יישום מחשוב ענן ברשויות המקומיות, קיימים פערים רבים בין תפקיד מש"ם בעיני הרשויות המקומיות לבין הסמכויות והמידע המינימלי שנחשף בפניו בפרויקט. מש"ם חושש כי חוסר הגדרתו כגורם המתכלל יגרום לכך שרק הרשויות החזקות והמתקדמות יתחברו לענן, ואילו הקטנות והחלשות יישארו במצבן הנוכחי. לדברי מש"ם, המידע אשר נחשף בפניו אינו מאפשר לו לדעת אם המענה יהיה שלם עבור הרשויות, ולא ברור היקף ההתאמה של המכרז לרשויות ולצורכיהן.

מינהל הרכש מסר למשרד מבקר המדינה בפברואר 2021 בהקשר לרשויות המקומיות כי יש לבצע עבודת מיפוי למצב התשתיות ברשויות, כגון פרישתן הנוכחית, הגופים המפעילים תשתיות משותפות ברשויות וכיו"ב. כמו כן, לאחר הקמת CCoE לממשלה, יש לבנות גם CCoE לשלטון המקומי כדי לתמוך במעבר הרשויות לענן בצורה סדורה ומקצועית.

מוצע כי משרד הפנים ומערך הסייבר יפעלו לקידום הקמת מרכז שליטה ובקרה מרכזי לטיפול ומתן מענה לאירועי סייבר ברשויות המקומיות בהקדם, כדי להבטיח רציפות תפקודית של הרשויות המקומיות. יש לתת את הדעת למערכת היחסים בין השלטון המרכזי לשלטון המקומי - הרצון לשמר את עצמאות השלטון המקומי מצד אחד, והצורך להתוות מדיניות וסטנדרטים אחידים בידי השלטון המרכזי מצד שני.

מערך הסייבר מסר למשרד מבקר המדינה בתשובתו מפברואר 2021 כי המערך פועל ברמה הלאומית ומשפיע על מגזרי המשק באמצעות היחידות המגזריות של משרדי הממשלה השונים. הדבר תקף גם לפעילות המערך אל מול היחידה המגזרית במשרד הפנים, שנעשית בצורת הכוונה, ולא ישירות מול הרשויות המקומיות שעליהן אחראי משרד הפנים. עוד מסר המערך כי משרד הפנים העלה קושי משפטי לפיו הסמכויות בתחום אבטחת מידע, ככל שחלות על רשויות מקומיות, נמצאות למעשה בתחום הסמכות והאחריות של משרדים אחרים, ולכן לטענת משרד הפנים אין בידיו הסמכות ואחריות הפיקוח בתחום זה. עם זאת, נוכח חשיבות הנושא, מערך הסייבר פועל לבחינה מעמיקה של נושא הגנת הסייבר ברשויות מקומיות ולקידום הנושא על כלל רבדיו והיבטיו יחד עם שותפים נוספים, לרבות הקמת מרכז ניטור מגזרי לרשויות המקומיות.

משרד הפנים מסר בתשובתו כי הוא אינו רגולטור בתחום הסייבר לרשויות המקומיות, אך הוא פועל כגורם מסייע לרשויות המקומיות במסגרת היערכותן לשעת חירום והבטחת הרציפות התפקודית בה. מינהל החירום שבמשרד הפנים תומך ברעיון להקים מרכז בקרה ושליטה לניטור אירועי אבטחת מידע ברשויות המקומיות. מינהל החירום פעל בשנים האחרונות על מנת לסייע להביא את הרעיון לידי יישום יחד עם מערך הסייבר וישראל דיגיטלית, אולם הרעיון לא הבשיל לכדי יישום אופרטיבי, בעיקר בשל היעדר תקציב. בימים אלו מינהל החירום פועל לבחינת קידום הנושא עם פיקוד העורף.

בתשובתו מסר מש"ם כי לתפיסתו נושא הסייבר הוא נושא בעל חשיבות לאומית מכרעת, ומשום כך עליו להיות מטופל גם ברשויות המקומיות בשיתוף הגורמים הרלוונטיים הכוללים גם את מש"ם, לרבות תקצוב ממשלתי מתאים. מש"ם פועל מיוזמתו בנושא זה מול מערך הסייבר. לדעת מש"ם, הקמת מרכז שליטה ובקרה לרשויות המקומיות היא מבורכת אך אינה יכולה להחליף את הצורך במערך הגנה מלא, הכולל מוצרים, כוח אדם, צוותי התערבות וכדומה, הנדרש עבור

הרשויות. לדברי מש"ם, יש לשמור על עצמאותן של הרשויות ולכן לא נכון שהמאסדרים יבצעו פעולות חד-צדדיות ללא מש"ם, שהוא הגוף המתכלל עבור הרשויות.

נוכח תגובותיהם של מערך הסייבר, משרד הפנים ומש"ם ראוי כי משרד הדיגיטל הלאומי ומשרד הפנים, בשיתוף משרד המשפטים, יבחנו את סוגיית הובלת נושא הגנת הסייבר ברשויות המקומיות ותכלולו.

התמודדות משרדי הממשלה עם המעבר לשירותי ענן ציבורי

במאי 2020 הפיץ משרד מבקר המדינה שאלון רוחבי ל-72 מנמ"רים במשרדי ממשלה ויחידות הסמך (להלן - המשרדים) על מנת לעמוד על החסמים, הקשיים והבעיות בשימוש בשירותי ענן ציבורי (להלן - השאלון). התשובות התקבלו עד יולי 2020. 45 מנמ"רים (כ-62%) השיבו על השאלון במלואו או על חלקים ממנו, בהתאם ליישום מערכות ענן במשרדיהם. להלן עיקרי הממצאים:

קיומה של תוכנית אב הכוללת התייחסות לנושא מחשוב ענן במשרדים

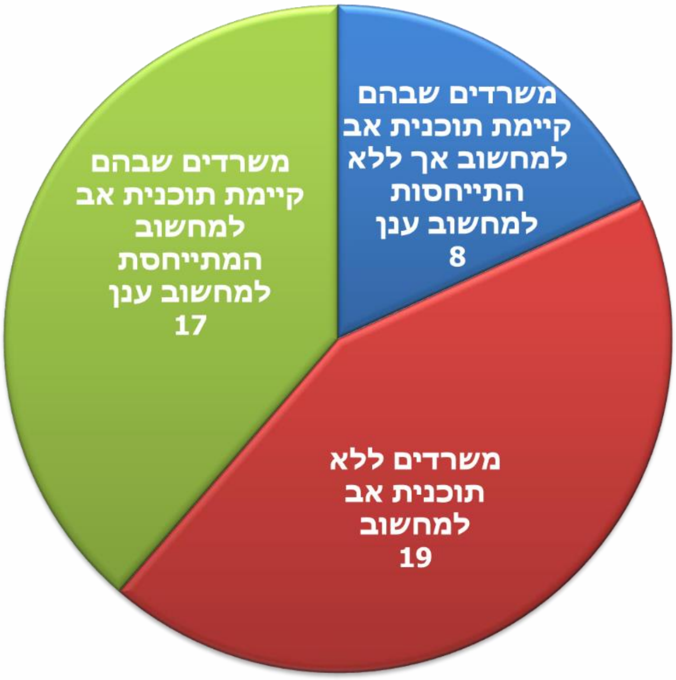
על פי מדריך התכנון הממשלתי[39], תוכנית העבודה השנתית של משרד ממשלתי אמורה לשקף את הפעולות שהמשרד מתכנן לבצע בתקופה נתונה כדי להשיג את מטרותיו. המטרות הן למעשה ההישגים הרחבים שהמשרד מכוון אליהם בפעולתו ואשר מימושם יחולל שינוי מהותי בסביבה החיצונית. המטרות מגדירות את העתיד הרצוי, מצביעות על כיווני הפעולה של המשרד ומהוות אמירה ברורה לגבי חזונו.

תוכנית אב היא תוכנית עבודה רב-שנתית שממנה נגזרות תוכניות העבודה השנתיות. תוכנית אב למחשוב או תוכנית אסטרטגית דיגיטלית מיועדת לתת לארגון מבט כולל וארוך-טווח על צורכי המחשוב שלו. ללא תוכנית אב למחשוב, גובר הסיכון כי תחום מערכות המידע לא יהיה ערוך לאתגרים הצפויים לו בשנים הקרובות[40]. מתוך 44 משרדים אשר השיבו לשאלה זו, ל-19 (43%) לא הייתה תוכנית אב למחשוב או תוכנית אסטרטגית דיגיטלית. מתוך 25 המשרדים שהעידו על קיומה של תוכנית כזו, 8 משרדים (32%) לא כללו בתוכנית התייחסות למעבר לשירותי ענן. להלן פירוט בתרשים:

תרשים 5: **קיום תוכנית אב למחשוב במשרדים והתייחסות למחשוב ענן, יולי 2020**

39 להרחבה ראו מדריך התכנון הממשלתי: https://www.gov.il/he/Departments/General/planning_guide2010

40 להרחבה ראו נוהל מפת"ח - מתודולוגיה לניהול מיזמי תוכנה, הנדסת תוכנה, ניתוח מערכות וניהול איכות תוכנה בישראל אשר פותחה על ידי משרד האוצר. בהחלטת ממשלה 2097 (10.10.2014) בוטלה החובה להשתמש בנוהל מפת"ח.



פרויקט מעבר לענן במשרד ממשלתי הוא פרויקט רב-שנתי ובו נדבכים שונים, כגון הקמת תשתית טכנולוגית, התקשרויות, אבטחת מידע והכשרת ההון האנושי. מהתרשים עולה כי ביולי 2020 בכ-61% ממשרדי הממשלה שהשיבו לשאלון לא הייתה תוכנית אב למחשוב, או שבתוכנית האב שלהם לא הייתה התייחסות למחשוב ענן.

רשות התקשוב מסרה למשרד מבקר המדינה כי היא אינה דורשת ממשרדי הממשלה להכין תוכנית אב למחשוב, אלא מפרסמת תוכנית תקשוב אסטרטגית תלת-שנתית, בהתייחס לכל אגפי מערכות המידע במשרדי הממשלה. תוכנית התקשוב הממשלתי לשנים 2019 - 2021 כוללת התייחסות גם למעבר לענן בממשלה.

משרד מבקר המדינה מציין כי אין בתוכנית התקשוב האסטרטגית של רשות התקשוב כדי להבטיח שכל משרד ממשלתי יקדם את מכלול פעולותיו בהתאם לתוכנית רב-שנתית הכוללת בין היתר פרויקטים של פיתוח, הטמעה ותחזוקה שמיושמים לאורך שנים.

מומלץ כי כלל משרדי הממשלה ישלימו הכנת תוכנית אב למחשוב העוסקת גם במחשוב ענן, נוסף על תוכנית התקשוב האסטרטגית של רשות התקשוב.

שלבי אימוץ של מחשוב ענן במשרדים

להלן שלבי האימוץ של שירותי מחשוב ענן במשרדים, על פי תשובותיהם לשאלון של 44 מנמ"רים:

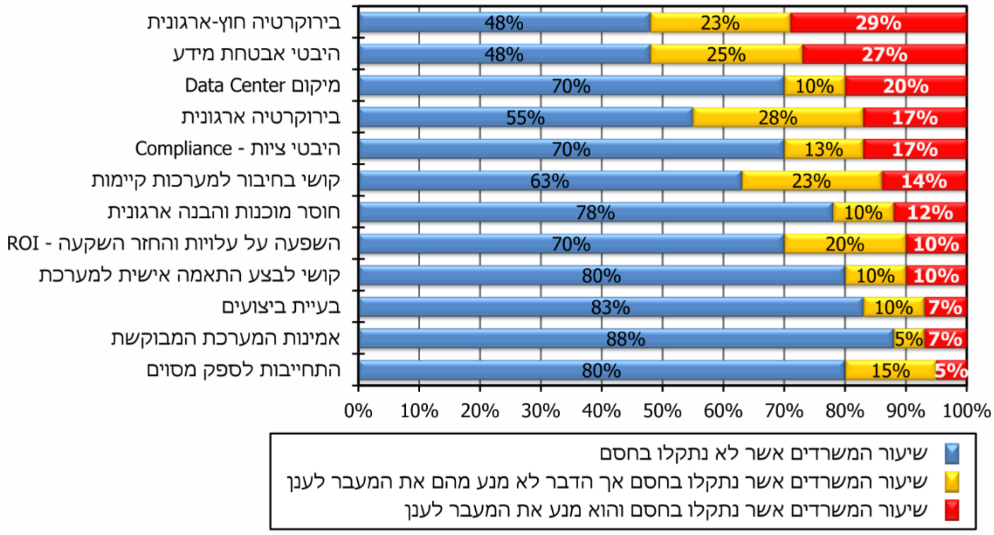
תרשים 6: **השימוש בשירותי מחשוב ענן במשרדים, יולי 2020**

מהתרשים עולה כי רק שלושה מהמשרדים שהשיבו לשאלון (כ-7%) ענו שאין להם כוונה להשתמש בשירותי מחשוב ענן; ב-23 משרדים (52%) נעשה כיום שימוש במחשוב ענן; וב-16 משרדים (כ-36%) מתוכנן שימוש במחשוב ענן בשנים הבאות.

חסמים עיקריים במעבר לשירותי ענן

בתרשים 7 שלהלן מפורטים החסמים המקשים על המעבר לשירותי ענן, על פי תשובותיהם לשאלון של 40 מנמ"רים:

תרשים 7: **חסמים עיקריים במעבר למחשוב ענן במשרדים, יולי 2020 (מתוך סך המשרדים שענו)**



מתרשים 7 עולה כי החסמים העיקריים המעכבים או המונעים מעבר מערכות מידע לענן הם בירוקרטיה פנים-ארגונית וחוץ-ארגונית, היבטי אבטחת מידע, היבטי ציות ומיקום ה-Data Center.

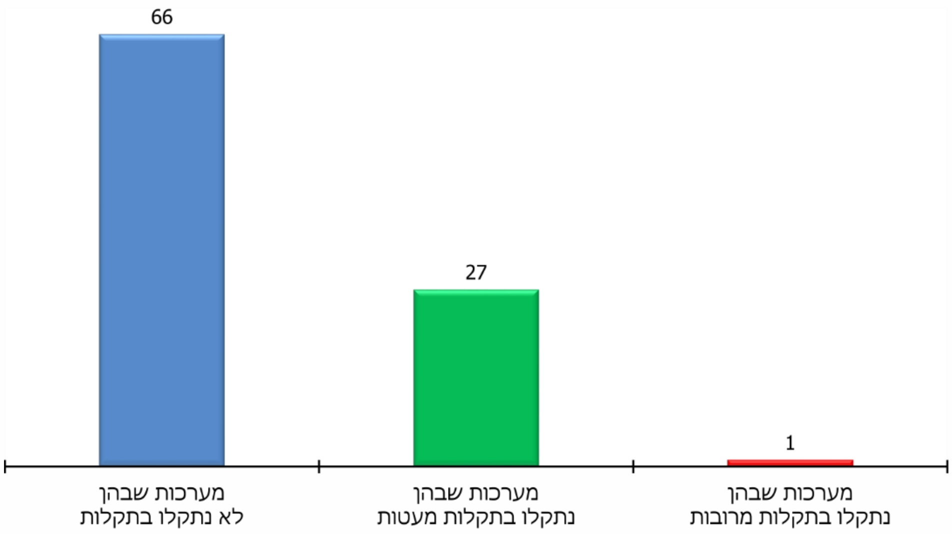
מוצע כי רשות התקשוב תבטיח בהמשך פעולותיה מתן מענה לחסמים שהעלו המשרדים על מנת להקל על יישום הפרויקטים בענן בעתיד, הן על ידי המשרדים באופן עצמאי והן במסגרת פרויקט נימבוס.

בתשובתה מסרה רשות התקשוב כי תמשיך לתת מענה שוטף לחסמים למעבר לתצורת ענן במשרדי הממשלה ובגופים ציבוריים, על מנת להקל על הפרויקטים בענן בעתיד, כחלק מעבודת המטה השוטפת המתבצעת על ידה, ובמסגרת מרכז המצוינות התפעולית בענן (CCoE) שבכוונת הרשות להקים.

תקלות במערכות מחשוב ענן במשרדים

על פי תשובותיהם לשאלון של 42 משרדים, ל-27 מהם יש מערכת אחת או יותר בענן, ולכל המשרדים שענו על השאלון יש ביחד 94 מערכות בענן (כאמור מתוך אלפי מערכות הקיימות בכל המשרדים). בתרשים שלהלן מפורטת התפלגות המערכות לפי מספר התקלות שבהן נתקלו המשרדים:

תרשים 8: **התפלגות המערכות לפי מספר התקלות שבהן נתקלו המשרדים**

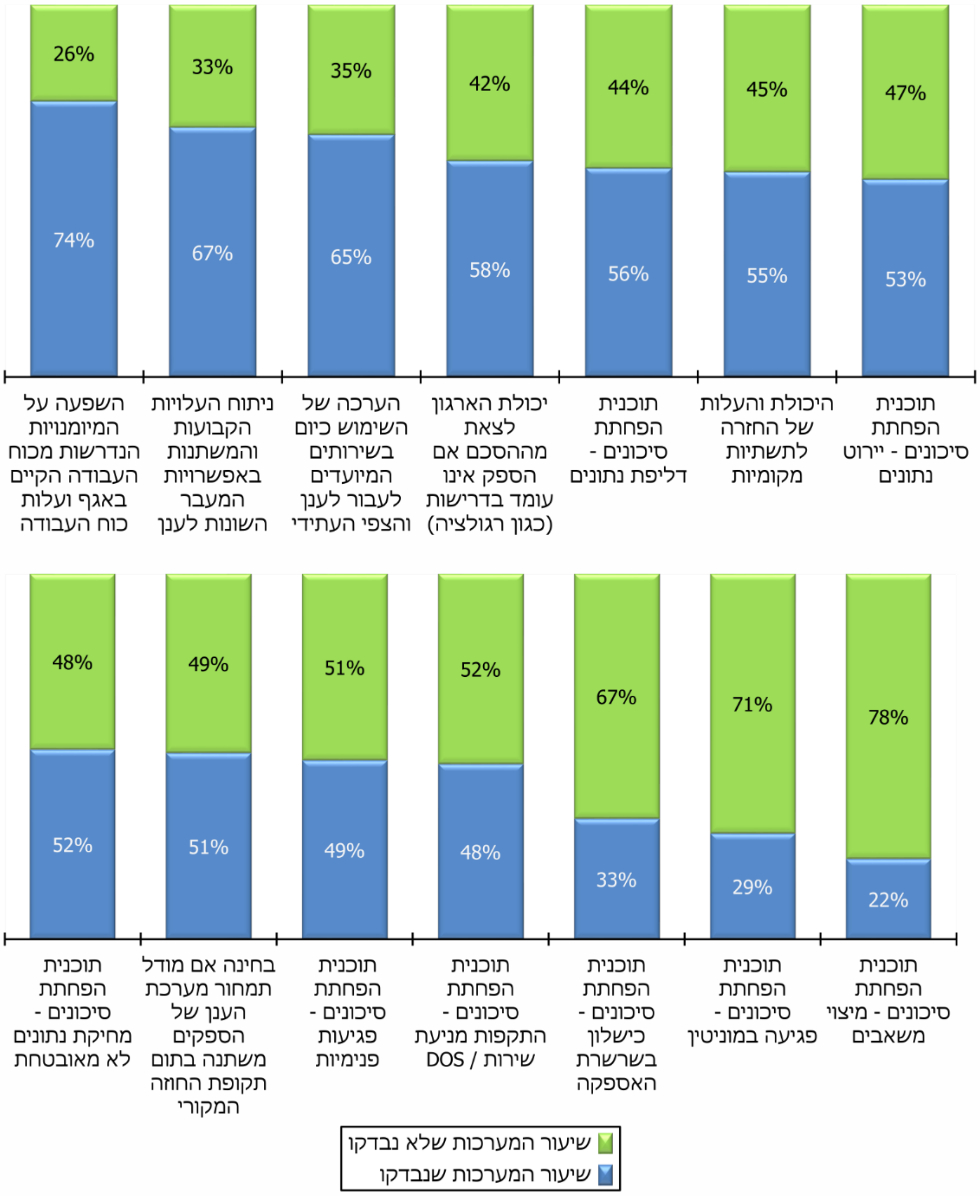


מהתרשים שלעיל עולה כי על פי תשובות המשרדים, ברוב מוחלט (כ-99%) של מערכות המידע בסביבת הענן המשרדים לא נתקלו בתקלות או שהיו להם תקלות מעטות.

ביצוע בדיקות מקדימות לבחינת המוכנות למעבר לענן

טרם ההחלטה על יישום מערכת בסביבת ענן, יש מקום לבצע כמה בדיקות פנימיות מקדימות על מנת לבחון את מוכנות המשרד בכללותו למעבר לענן. הבדיקות יכולות להקיף מגוון נושאים, כגון פגיעה אפשרית במוניטין של המשרד עקב יישום לא נכון של המערכת בענן, ניתוח העלויות במקרה של בקשה לחזור לתשתית המקורית (On premises) ועוד. במסגרת השאלון פורטה רשימה של בדיקות אפשריות. להלן בתרשים 9 פירוט הבדיקות המקדימות עבור מערכות ענן שיושמו במשרדי הממשלה. על שאלה זו ענו 27 משרדים אשר יישמו 84 מערכות בסך הכול:

תרשים 9: **ביצוע בדיקות מקדימות על ידי המשרדים לבחינת המוכנות למעבר למחשוב ענן**



מתרשים 9 עולה כי על פי תשובות המשרדים, במרבית המערכות שתוכננו לעבור למחשוב ענן נושאים רבים לא נבדקו טרם ההחלטה על היישום בענן - למשל דרכים להפחתת סיכונים בתחומים שונים, כגון פגיעה במוניטין וכישלון בשרשרת האספקה; יכולת המשרד להתנתק מהספק ולחזור למערכת בסביבה מקומית. לשם המחשה, רק ל-28 מבין 84 מערכות (33%) בוצעו 10 בדיקות או יותר מתוך ה-14 שצוינו.

במהלך הביקורת, בדצמבר 2020, פרסמה רשות התקשוב הנחיה בנושא "אישור, תכנון ובקרה לשירותי ענן" (להלן - ההנחיה החדשה). ההנחיה החדשה מפרטת דגשים ובקרות אשר על המשרד לבצע בעת יישום פרויקט מחשוב ענן, לרבות בקרות בשלבים הבאים: תכנון; הכנת ההזמנה; יצירת ההתקשרות; אישור ההתקשרות והשימוש השוטף בשירותי הענן.

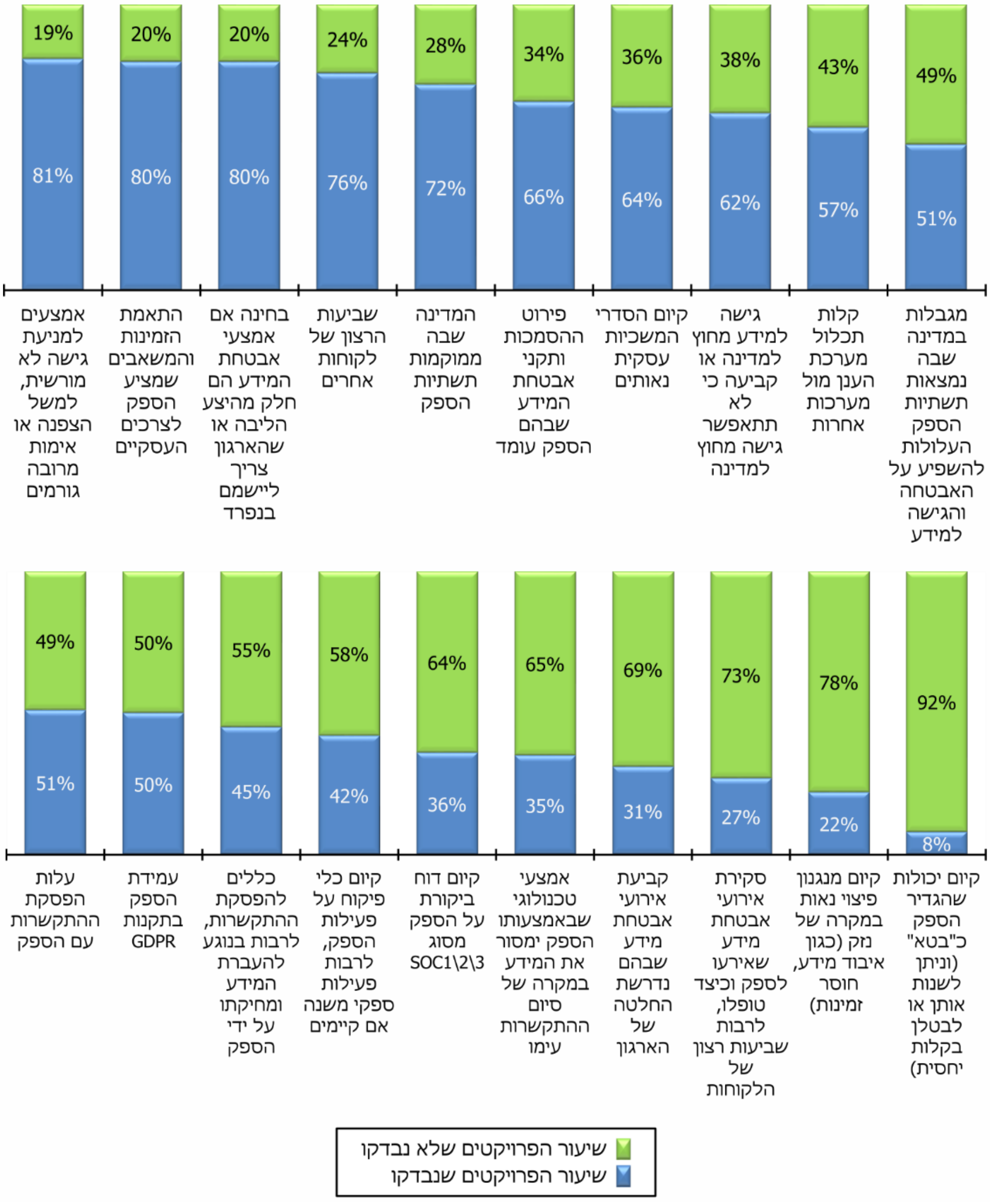
לאור הממצאים שפורטו, מומלץ כי רשות התקשוב תבחן את הצורך בעדכון ההנחיה החדשה כך שתכיל את מכלול הבדיקות אשר על המשרדים לבצע לפני ההחלטה על יישום מערכת בסביבת הענן, וכן תבצע בקרה על ביצוע ההנחיה בידי המשרדים, בהלימה לתפקיד רשות התקשוב כפי שנקבע בהחלטת ממשלה 2097 - לשמש גורם אחראי על קביעת סטנדרטים בתחום טכנולוגיות המידע וסיוע בהטמעתם.

בתשובתה מסרה רשות התקשוב כי בכוונתה להקים במהלך שנת 2021 מרכז מצוינות תפעולית בענן (כחלק מיישום מכרז נימבוס), ובמסגרתו ייבחן הצורך בעדכון ההנחיה החדשה ופירוט מכלול הבדיקות אשר על המשרדים לבצע לפני ההחלטה על יישום מערכת בסביבת הענן. כמו כן תבוצע בקרה שוטפת על ביצוע ההנחיה בידי המשרדים.

בדיקות מקדימות הנוגעות לספק והסכם ההתקשרות

לאחר קבלת ההחלטה על מעבר לענן, יש לבצע כמה בדיקות מקדימות הנוגעות לספק הרלוונטי והסכם ההתקשרות עימו לפני ביצוע ההתקשרות בפועל, במטרה לצמצם את הסיכונים שעלולים לעלות בהתקשרות מסוג זה. בשאלון פורטה רשימה של בדיקות אפשריות. להלן בתרשים 10 פירוט תשובותיהם של המשרדים בעניין הבדיקות עבור מערכות ענן שיושמו במשרדים. על שאלה זו ענו 21 משרדים אשר יישמו 74 מערכות בסך הכול:

תרשים 10: **בדיקות של הספק והסכם ההתקשרות לקראת מעבר למחשוב ענן, יולי 2020**



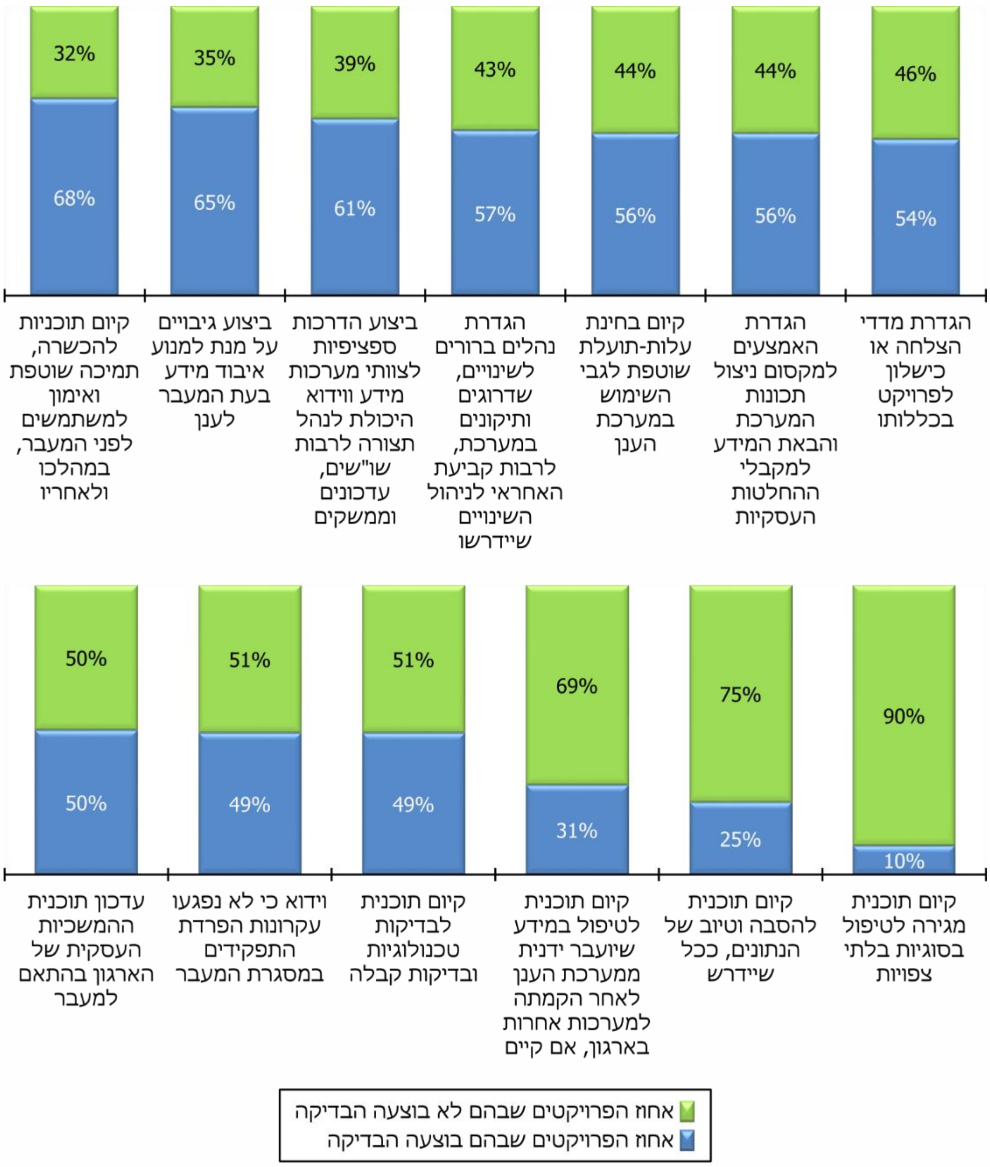
מתרשים 10 עולה כי על פי תשובות המשרדים, הם אינם בודקים באופן אחיד וקבוע גורמים רבים הקשורים לספק ולהסכם ההתקשרות עימו. בין היתר, בהתקשרות עם ספק לא נבדקים פעמים רבות קיומו של מנגנון פיצוי נאות במקרה של נזק, קיומם של כלי פיקוח על פעילות הספק או ספקי משנה וכיו"ב. לשם המחשה, רק ל-18 מבין 74 מערכות (24%) בוצעו 14 בדיקות או יותר מתוך ה-20 שצוינו. בביקורת עלה כי לעיתים לדעת המשרדים בחירה בספק עולמי מוביל מייתרת את הצורך בביצוע הבדיקות המתוארות. עם זאת, משרדים אשר ביצעו את הבדיקות האמורות גילו פערים אשר היה קל יותר לצמצם אותם לפני החתימה על החוזה, כגון קביעת כללים ברורים לסיום ההתקשרות ותכלול מול מערכות אחרות בארגון.

כאמור, במהלך הביקורת, בדצמבר 2020, פרסמה רשות התקשוב את ההנחיה החדשה, הקובעת בין היתר כי עד לסיום מכרז נימבוס יש צורך באישור מרשות התקשוב ולאחר מכן ממינהל הרכש לכל התקשרות חדשה או הארכה של התקשרות קיימת בנושא ענן. הנחיה זו הוגדרה כמסמך מדיניות אשר תוכנו מחייב את קהל היעד - מנהלי אגפי טכנולוגיות מידע, מנהלי טכנולוגיות, מנהלי יישומים ומנהלי פרויקטי ענן ביחידות המונחות על ידי רשות התקשוב.

התייחסות להיבטים שונים בעת יישום מערכת ענן

מעבר לענן יכול להשפיע על הארגון מבחינות שונות - טכנולוגית, עסקית, כספית, היבטי בקרה ועוד. במסגרת השאלון פורטה רשימה של סוגיות כאלו. להלן בתרשים 11 פירוט תשובותיהם של המשרדים על התייחסות לסוגיות אלו בעת יישום מערכות הענן במשרדים. על שאלה זו ענו 19 משרדים אשר יישמו 72 מערכות בסך הכול:

תרשים 11: **היבטים שונים ביישום מערכות מחשוב ענן, יולי 2020**



מהתרשים עולה כי מרבית המשרדים אינם מטפלים בהיבטים רבים הקשורים ליישום מערכות מחשוב ענן, כגון עדכון תוכנית ההמשכיות העסקית של המשרד, הכנת תוכנית להסבת נתונים ולטיובם ובחינת עלות-תועלת שוטפת. היעדר הטיפול בהיבטים אלו בעת יישום המערכת עלול לפגוע בשירות שנותן המשרד, בתכנון התקציבי שלו ועוד.

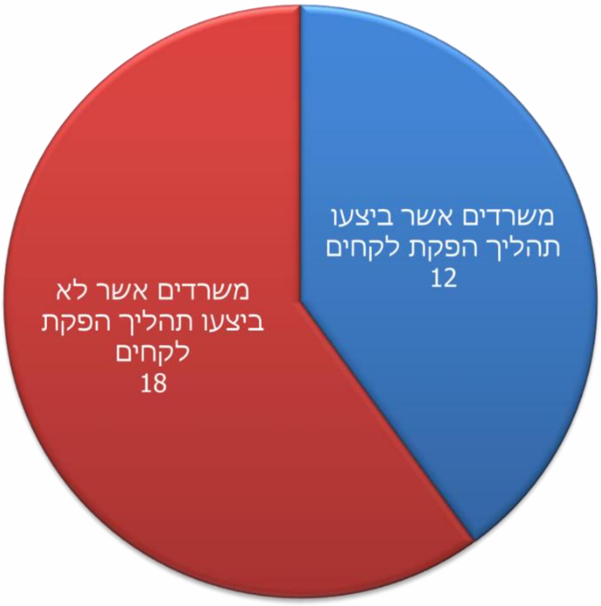
לאור הממצאים שפורטו לעיל, מומלץ כי רשות התקשוב תוודא כי מכלול ההיבטים באים לידי ביטוי בהנחיה החדשה, ותבצע בקרה על יישום ההנחיה בידי המשרדים.

הפקת לקחים מיישום מערכות ענן

מנגנון הפקת לקחים הוא חלק חשוב ובלתי נפרד מכל יישום מערכת מחשוב, לרבות יישום מערכת מחשוב ענן. בסוף שנת 2016 פרסמה רשות התקשוב הנחיה בנושא "תחקור והפקת לקחים", שמטרתה להנחות את המנמ"רים לערוך תחקיר וניהול לקחים ביחידות התקשוב הממשלתי ובאופן יישום הלקחים. על פי ההנחיה, תחקיר הוא בדיקה של אירוע או תופעה חיוביים או שליליים שהארגון מעורב בהם לשם למידה, הפקת לקחים והסקת מסקנות שיאפשרו שכפול של ההצלחה (באירוע חיובי) או מניעת אירועים דומים (באירוע שלילי).

במסגרת השאלון נשאלו המנמ"רים אם בוצע תהליך מסודר של הפקת לקחים לאחר סיום היישום של מערכת מחשוב ענן. להלן תשובותיהם של 30 מנמ"רים אשר השיבו על שאלה זו:

תרשים 12: **הפקת לקחים לאחר יישום מערכת מחשוב ענן, יולי 2020**



מהתרשים עולה כי כ-60% מהמשרדים שהשיבו על השאלון לא ביצעו תהליך הפקת לקחים לגבי יישום מערכת הענן, אף כי תהליך הפקת לקחים הוא חלק משמעותי מיישום של כל מערכת מחשוב.

✩

מחשוב ענן הוא חלק עיקרי בתקשוב הממשלתי בכלל ובתוכניות העבודה העתידיות בפרט. ממצאיו של פרק זה מלמדים כי היבטים שונים הקשורים ליישום מערכות ענן אינם מקבלים מהמשרדים התייחסות מיטבית ובזמן המתאים. בין היבטים אלו ניתן למנות בחינת עלות תועלת, הגדרת מדדי הצלחה וכישלון, בדיקות הקשורות לספק המערכת ולהסכם ההתקשרות לרבות כללים לסיום ההתקשרות, היערכות להסבת נתונים, קיום הליך סדור להפקת לקחים וכיו"ב. היעדר ההתייחסות להיבטים אלו עלול לפגוע בשירותים שנותן המשרד, בתכנון התקציבי שלו, ברציפות הפעילות של המערכת ועוד.

נכון למועד הביקורת לא הוקם הליך סדור להפקת לקחים ממשלתית מיישום מערכות בסביבת הענן. הליך שכזה יכול לסייע בזיהוי החסמים, הקשיים והפערים הקיימים אצל משרדי הממשלה בבואם ליישם מערכות בסביבת הענן ולתת מענה מתאים.

יצוין כי במהלך הביקורת פרסמה כאמור רשות התקשוב בדצמבר 2020 הנחיה בנושא "אישור, תכנון ובקרה לשירותי ענן". עד למימוש מלא של מכרז נימבוס על כל רבדיו מומלץ כי רשות התקשוב תבחן כיצד ניתן לתת מענה לצורך לקיים בקרה עיתית על אופן יישום המעבר לענן.

בנוסף, מומלץ כי רשות התקשוב תבחן מיסוד הליך סדור להפקת לקחים מיישום מערכות בסביבת ענן במשרדים, אשר יוכל לסייע ביצירת סטנדרטיזציה ויקל על יישום מערכות נוספות בסביבת הענן.

בתשובתה ציינה רשות התקשוב כי היא פעלה ופועלת לאיתור מוצרים והתפתחויות טכנולוגיות מתאימות. כמו כן, הרשות מסרה כי מרכז המצוינות התפעולית בענן (CCoE) שבכוונתה להקים אמור, עם הקמתו, למסד הליך סדור להפקת לקחים מיישום מערכות בסביבת ענן במשרדים, במטרה לסייע ביצירת סטנדרטיזציה ולהקל על יישום מערכות נוספות בסביבת ענן.

פעילות גורמי ההסדרה בתחום אבטחת המידע והגנת הסייבר במחשוב ענן

רקע

כפי שתואר לעיל, לשימוש בשירותי ענן יתרונות רבים, כגון נגישות וזמינות מכל מקום בעולם, שירות מקצועי ומוזל בזכות יתרון הגודל של ספקי השירות, אפשרות להרחיב או לצמצם את השירותים בטווח זמן קצר ועוד. אך לצד היתרונות, השימוש בשירותי מחשוב ענן עלול להעלות גם סיכוני אבטחת מידע וסייבר. להלן חלק מגורמי הסיכון בשימוש בשירותי מחשוב ענן:

1. מידע פנימי של הארגון מאוחסן על גבי תשתית ציבורית.
2. קשה לעובדי הארגון להבחין בין המידע שנמצא בתוך הארגון למידע הנמצא מחוץ לו.
3. ספקי הענן הופכים למטרה מועדפת של תוקפים פוטנציאליים.
4. לארגון אין שליטה ישירה על העובדים המטפלים בתשתיות החומרה והתוכנה, שהם הבסיס לשירותים שהוא מספק.

5. גורמי ממשל במדינות זרות עשויים לאלץ ספקי ענן לחשוף מידע של לקוחות השמור אצלם. כך למשל, חוק הענן[41] שחוקק בארצות הברית ביוני 2018 מתיר למדינה לדרוש מידע מספקיות השירות במרשתת, גם אם הוא מאוחסן על שרתים מחוץ לארה"ב.

6. תלות בספק (Vendor Lock-In) עלולה להקשות על הארגון לעבור לספק אחר, גם אם אבטחת המידע של הספק הנוכחי אינה עומדת ברמה הנדרשת. הקושי עלול לנבוע מעלות המעבר, הצורך להכשיר מחדש את כוח האדם לשימוש במערכת החדשה, הסכמים משפטיים כובלים ועוד.

התרשים שלהלן מפרט את התחומים שבהם נדרשת תשומת לב לסיכוני אבטחת מידע וסייבר בענן:

תרשים 13: **תחומים שבהם נדרשת תשומת לב לסיכוני אבטחת מידע וסייבר בענן, יולי 2020**

המקור: מדריך אבטחת המידע בענן של CSA[42], בתרגום משרד מבקר המדינה.

כפי שצוין, אחד מסיכוני הסייבר העיקריים הוא תקיפה של ספק שירותי ענן במטרה להגיע למידע על הלקוחות המשתמשים בשירותיו. במחקר של חברת אבטחה עולמית[43] על השימוש בשירותי ענן מינואר עד אפריל 2020 נמצא כי בחודשים מרץ ואפריל 2020 גדל השימוש בשירותי ענן בעולם, ככל הנראה עקב ההגבלות העולמיות על התכנסויות עקב מגפת הקורונה, ולצידו

41 Clarifying Lawful Overseas Use of Data Act or the CLOUD Act. להרחבה ראו: https://www.congress.gov/bill/115th-congress/house-bill/4943.

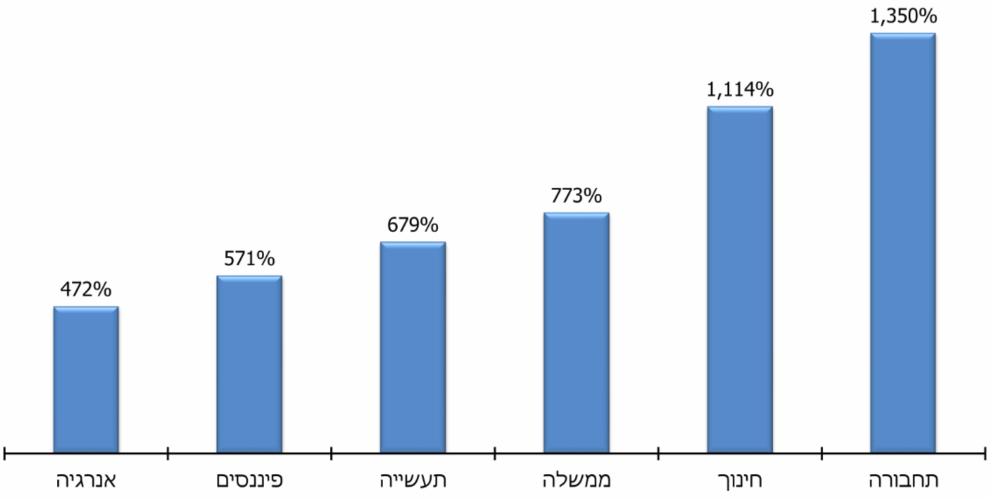
42 Cloud Security Alliance

43 להרחבה ראו: https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk-report-business-growth-edition.html

גדל גם מספר האיומים החיצוניים על שירותי מחשוב ענן ב-630% לעומת ינואר ופברואר באותה שנה. במגזר הממשלתי בפרט גדל מספר האיומים בתקופה זו ב-773%. עוד עלה במחקר כי מרבית התקפות הסייבר הממוקדות מגיעות משלוש מדינות - סין, אירן ורוסיה.

להלן תרשים המתאר את נתוני המחקר בדבר העלייה באיומים על שירותי ענן בעולם בתקופה בין ינואר לאפריל 2020, לפי מגזר פעילות:

תרשים 14: **עלייה באיומים על שירותי ענן בעולם לפי מגזר, ינואר - אפריל 2020 (באחוזים)**



מקור: חברת אבטחה עולמית, בתרגום משרד מבקר המדינה.

לשם המחשה, באוקטובר 2019 דיווחה חברה גלובלית לשירותי מחשוב ענן כי שירות הענן שלה הותקף במתקפת מניעת שירות מבוזרת (DDoS)[44], אשר הביאה להשבתה של כשמונה שעות במתן שירותי הענן ללקוחות החברה. כלומר, במשך יום עבודה שלם נמנעה מלקוחות החברה גישה למערכות אשר נמצאות בסביבת הענן של החברה. בנוסף דיווחה החברה כי בפברואר 2020 היא הצליחה לסכל את מתקפת מניעת השירות המבוזרת הגדולה בהיסטוריה. על פי הדיווח, גודל המתקפה שסוכלה עלה ב-30% על המתקפה הגדולה ביותר על חברה כלשהי דרך המרשתת שתועדה עד אז.

כמו כן, במאי 2020 דיווחה חברת אחסון אתרים הפועלת בסביבת הענן על מתקפת סייבר רחבת-היקף. על פי פרסומים בתקשורת[45], המתקפה הביאה להשחתת אתרי אינטרנט רבים וחשש לגניבת בסיסי נתונים, בין היתר של רשויות מקומיות, רשתות מסחר ועמותות.

44 DDoS - התקפת מניעת שירות מבוזרת (distributed denial-of-service attack), נועדה להשבית מערכת מחשב על ידי יצירת עומס חריג על משאביה.

45 להרחבה ראו: https://www.calcalist.co.il/internet/articles/0,7340,L-3825453,00.html

מחקר[46] אשר פורסם ביולי 2020 וכלל דיווחים של כ-3,500 מנהלי מערכות מידע מ-26 מדינות במגוון מגזרים, העלה כי כ-70% מהנשאלים דיווחו על אירוע אבטחת מידע בענן הציבורי שבו הם משתמשים. כמו כן המחקר העלה כי ארגונים המפעילים סביבות מרובות-עננים הם בעלי סבירות גבוהה ב-50% לחוות אירוע אבטחת מידע בענן בהשוואה לארגונים שמשתמשים בענן בודד.

בדצמבר 2020 דיווחה חברה גלובלית לשירותי מחשוב ענן כי הותקפה במתקפת סייבר. בהקשר למתקפה זו פרסמה[47] סוכנות הביטחון הלאומי האמריקאית "הודעה על מתקפת סייבר" המפרטת כיצד שירותי הענן של החברה נמצאים בסכנה מצד פצחנים (האקרים), ומורה ללקוחות החברה המשתמשים בשירותי הענן לנעול את המערכות שלהם.

פעילות הוועדה המייעצת לנושא אבטחת מידע במחשוב ענן

עם התגברות ההכרה בדבר חשיבות הטכנולוגיות הדיגיטליות בפעילות הממשלה, לאחר בחינת צורכי הממשלה בתחום טכנולוגיות המידע וכחלק מההתמודדות עם סיכוני הסייבר קיבלה הממשלה החלטה בשנת 2015 (החלטה 2443)[48] שקבעה בין היתר הקמה של יחידה להגנת הסייבר בממשלה (להלן - יה"ב[49]), שייעודה הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל המשרדים.

כאמור, באוקטובר 2014 התקבלה החלטת הממשלה 2097. בין היתר ההחלטה קבעה כי על הממונה על התקשוב הממשלתי לפעול להעברת תשתיות התקשוב של משרדי הממשלה למודל מחשוב ענן, אשר יאפשר גישה מקוונת לתשתיות, פלטפורמות ויישומים, ותשלום דיפרנציאלי על פי השימוש בהם. במסגרת יישום ההחלטה פרסמה יה"ב בינואר 2016 את הנחיית "אבטחת מידע במעבר לענן ציבורי" (להלן- ההנחיה). ההנחיה מפרטת את האיומים הקיימים בסביבת הענן, ובהתאם להם את הערכת הסיכונים שהמשרדים נדרשים לבצע והבקרות שעליהם ליישם בעת המעבר לענן. על פי האמור בהנחיה, "משרד ממשלתי המבקש להקים מערכת או להעביר מערכת קיימת לסביבת ענן ציבורי, נדרש לפנות לקבלת אישור ליה"ב, תוך הבהרת הסיכונים הנגזרים למשרד מתהליך המעבר לסביבת ענן...יה"ב, בתיאום עם הגורמים הרלוונטיים, תהיה אמונה על אישור או דחיית הבקשות, בהתאם לניתוח הסיכונים שיוצג על ידי המשרד".

בד בבד עם פרסום ההנחיה, הקים מנהל יה"ב בינואר 2016 "ועדה מייעצת להגנת הסייבר במעבר לענן הציבורי" (להלן הוועדה המייעצת). על פי כתב המינוי של הוועדה, יהיו חברים בה נציגים מרשות התקשוב, יה"ב, מערך הסייבר, רשות הגנת הפרטיות והרשות הממלכתית לאבטחת מידע (רא"מ). הוועדה תעסוק במגוון הנושאים הקשורים להעברת מידע ויישומי

46 להרחבה ראו: https://news.sophos.com/en-us/2020/08/07/the-state-of-cloud-security-2020

47 להרחבה ראו:
https://www.gov.il/he/departments/publications/reports/auto_mach_abuse
https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/

48 החלטה 2443 של הממשלה ה-33, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

49 יה"ב היא יחידה ברשות התקשוב.

מחשוב של המשרדים לענן ציבורי, לרבות התווית יעדים ועקרונות התמודדות; בחינת היבטי הגנת הסייבר למול דרישות הגופים המונחים המבקשים להעביר מידע ויישומי מחשוב לסביבת ענן ציבורי; אישור בקשות המשרדים; מימוש נתונים ומערכות מידע והעברתם לתשתיות ענן מסחריות, בארץ ובחו"ל; קיום תהליכי לימוד והפקת לקחים.

ההנחיה מפרטת את הדרישות ממשרד ממשלתי בעת הגשת הבקשה לוועדה המייעצת, לרבות: הגשת חוות דעת היועץ המשפטי של המשרד בכל הנוגע לחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות) ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017; ניתוח איומים; מידע על הספק; פרטי המידע שמתוכנן לעבור לענן; ניתוח משתמשי המערכת; ניתוח ממשקי המערכת ועוד. בד בבד הנחה מנהל יה"ב את ממוני הגנת הסייבר המשרדיים[50] לעדכן את הוועדה המייעצת אם כבר קיימות מערכות במחשוב ענן, על מנת שזו תוכל לבחון אותן ולאשרן בהתאם להנחיה.

רשומת DNS היא פרוטוקול המתרגם שם מילולי של תחום אתר במרשתת (domain), כגון https://www.gov.il, לכתובת המספרית של האתר (כתובת ה-IP). פרוטוקול זה מקל על משתמשים אנושיים במרשתת משום שהוא מאפשר להם להגיע לאתרים באמצעות כתובת מילולית ולא מספרית.

מפגישות שקיים משרד מבקר המדינה ביולי ובדצמבר 2020 עם יחידת ממשל זמין[51] אשר ברשות התקשוב עלה כי ממשל זמין היא האחראית על מתן רשומת ה-DNS הנדרשת בתחום הממשלתי (gov.il) בעת הקמת מערכת בענן, וכי הרשומה ניתנת על ידי ממשל זמין למשרד הממשלתי רק לאחר קבלת החלטה חיובית בעניין המערכת במסגרת הדיון שמתבצע בוועדה המייעצת ווידוא יישום המלצות הוועדה. עוד ציין ממשל זמין כי מסיבות היסטוריות קיימים מקרים בודדים שבהם משרדים יכולים לייצר לעצמם רשומת DNS, אולם ממשל זמין פועל על מנת לצמצם מקרים אלו.

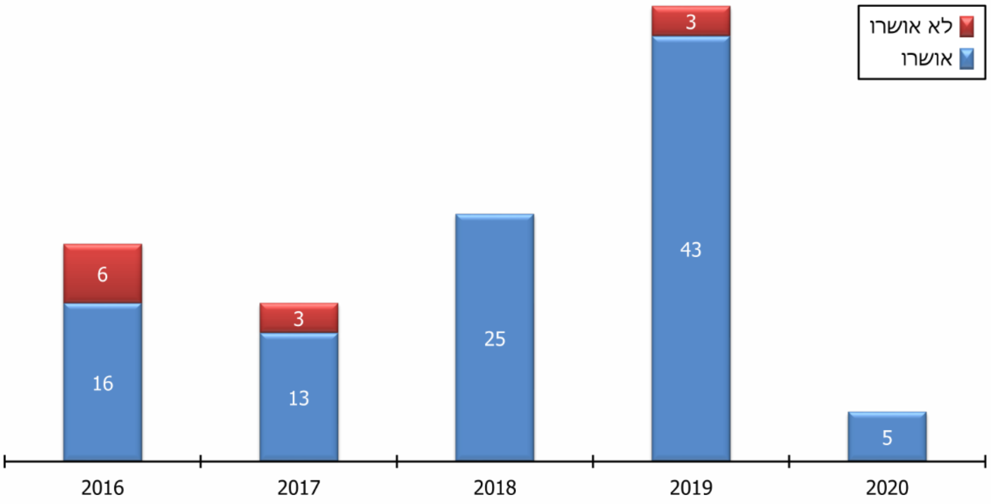
על פי נתוני יה"ב, משנת 2016 ועד יולי 2020 התכנסה הוועדה המייעצת 33 פעמים ודנה ב-114 מערכות של 36 משרדים. תרשים 13 להלן מפרט את פעילות הוועדה המייעצת בשנים 2016 עד יולי 2020:

50 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15), הטילה על מנכ"לי המשרדים לפעול לשיפור רמת הגנת הסייבר, ולשם כך בין היתר למנות ממונה להגנת סייבר.

51 יחידה ממשלתית המפתחת שירותים ואמצעים דיגיטליים עבור ממשלת ישראל. בין היתר אחראית היחידה על אתר השירותים והמידע הממשלתי Gov.il.

תרשים 15: **מספר המערכות שנידונו בוועדה המייעצת לפי שנים וסטטוס אישורן, נכון ליולי 2020**

;



על פי נתוני יה"ב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי מרבית המערכות (102 מתוך 114 מערכות, כ-89%) שלגביהן הגישו המשרדים בקשות לאישור הוועדה המייעצת אכן אושרו.

מתשובותיהם של 42 משרדים על השאלון שהפיץ משרד מבקר המדינה עולה כי על אף ההנחיה של מנהל יה"ב, במשרדים אלה פועלות כ-10 מערכות בסביבת ענן בלא שהתבקש לגביהן אישור הוועדה המייעצת. היעדר בחינה של הוועדה עלול להביא להתממשות סיכוני אבטחת מידע משמעותיים במערכות אלו.

באוגוסט 2020 מסר ממלא מקום ראש רשות התקשוב למשרד מבקר המדינה כי עם הקמת הוועדה המייעצת הוחלט שהיא תייעץ לגבי אופן ההגנה הנדרש של המערכות בסביבת הענן, מתוך הבנה שהנושאים והמערכות שיעלו תחילה לוועדה לא יהיו נושאי ליבה או יכללו מידע רגיש במיוחד, ועל כן יש מקום לשיקול הדעת וניהול הסיכונים של המשרד עצמו. עם זאת, ממלא מקום ראש רשות התקשוב הוסיף כי לאורך השנה וחצי האחרונות ניסו משרדי ממשלה להגיש לוועדה גם בקשות בנוגע למערכות ליבה רגישות, מתוך תפיסה שגויה שהחלטות הוועדה אינן מחייבות ובכל מקרה לא יכולות למנוע מהמשרדים להעלות מערכות אלו לענן. לאור הידע אשר נצבר ברשות התקשוב בנושא הענן במרוצת הזמן, ומתוך מחויבות לבצע את תפקידי הרשות כשומרת הסף בנושא, החליטה רשות התקשוב לשנות את שם הוועדה מ"מייעצת" ל"מאשרת", ועל כן בוצע עדכון במסמכי ההנחיה השונים. לדוגמה, הנחיית רשות התקשוב 4.2.3 שעניינה "יישום מכרז מסגרת מספר 21/17 למתן שירותי ענן ציבורי", אשר פורסמה ביולי 2020, קובעת כי "משרד שיבקש להשתמש במכרז יידרש לקבל אישור מקדים של מינהל הרכש ואישור של ועדת ענן ממשלתית". כמו כן ההנחיה קובעת כי "טרם מימוש השירותים...על המשרד לאשר את הפתרון המוצע בוועדת הענן התקשובית".

מהאמור לעיל עולה כי במועד סיום הביקורת, דצמבר 2020, לא היה בידי רשות התקשוב או בידי גורם ממשלתי אחר מיפוי מלא ועדכני של כל המערכות הממשלתיות שכבר יושמו בענן. כמו כן, משרדים שונים העבירו מערכות לסביבת הענן בלי לקבל את אישורה של יה"ב, הגם שבהתאם להנחית מנהל יה"ב, על אגפי מערכות המידע במשרדי הממשלה להעביר ליה"ב מיפוי של כלל מערכות הענן במשרדים ולהביא לשולחנה של הוועדה המייעצת את המערכות שהוקמו בסביבת הענן ללא אישורה או טרם הקמת הוועדה.

על המשרדים להביא לאישור הוועדה המייעצת את כלל המערכות הממשלתיות שכבר יושמו בענן. עוד מומלץ כי יה"ב תפעל להשלים מיפוי של כלל מערכות הענן במשרדי הממשלה ולוודא עם כל המשרדים כי כל המערכות שהוקמו בסביבת הענן יובאו לאישור הוועדה המייעצת. כמו כן מומלץ כי יה"ב תנקוט בפעולות בקרה על מנת לוודא כי המשרדים מיישמים את הנחיותיה.

פעילות האסדרה של מערך הסייבר הלאומי

בשנת 2015 החליטה הממשלה על הקמת מערך הסייבר[52]. מערך הסייבר מופקד על הגנת מרחב הסייבר הישראלי וקידום מובילות מדינת ישראל כמעצמת סייבר. המערך אחראי על קידום אסדרה לאומית ועל הובלה ממשלתית בתחום הגנת הסייבר; הנחיית גופי תמ"ק מכוח החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998; וכן ניהול, הפעלה וביצוע בהתאם לצורך של כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, ובכלל זה מענה הגנתי שלם ורציף לתקיפות סייבר, לרבות טיפול באיומי סייבר ובאירועי סייבר בזמן אמת.

נוכח הסיכונים בשירותי הענן, פרסם מערך הסייבר כמה מסמכים הקשורים לאבטחת מידע והגנת הסייבר במחשוב ענן. להלן פירוט המסמכים העיקריים שפורסמו:

באפריל 2017 פרסם מערך הסייבר את מסמך "תורת ההגנה בסייבר לארגון"[53] (להלן - מסמך תורת ההגנה), אשר נועד לשפר את החוסן הארגוני והעמידות של כלל הארגונים במשק בפני מתקפות סייבר. המסמך מגדיר שיטה סדורה להכרת הסיכונים הרלוונטיים לארגון, גיבוש מענה הגנתי ומימוש תוכנית להפחתת הסיכונים בהתאם, וכולל המלצות הגנה בנושא מחשוב ענן ציבורי. על פי המסמך, יש להעריך את סיכוני הסייבר ואבטחת המידע הכרוכים בפיתוח וברכש של מערכת חדשה ולנהלם על פי תהליכי ניהול הסיכונים המקובלים בארגון, כדי לוודא כי פתרונות להגנה על המידע שולבו במערכת כבר משלב הייזום והתכנון, דרך הפיתוח ועד לייצור. מסמך זה מופיע כמסמך מחייב במדיניות להגנת הסייבר בממשלה של יה"ב. במאי 2020 מסר מערך הסייבר למשרד מבקר המדינה כי בכוונתו לעדכן את מסמך תורת ההגנה, אשר לדעתו אינו נותן כיום מענה מלא לנושא אבטחת המידע בענן. לאחר סיום הביקורת, בדצמבר 2020, פרסם מערך הסייבר טיוטה להתייחסות הציבור בנושא שיפורים ותוספות למסמך תורת ההגנה.

52 החלטת הממשלה 2444, "קידום היערכות לאומית להגנת הסייבר", והחלטה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", מ-15.2.15. במסגרת ההחלטות הוקמו שני גופים: רשות הסייבר הלאומית והמטה הקיברנטי הלאומי. בדצמבר 2017 אוחדו שני הגופים לגוף אחד - מערך הסייבר הלאומי.

53 להרחבה ראו: https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

משרד מבקר המדינה ממליץ כי מערך הסייבר ישלים עדכון מסמך תורת ההגנה, כך שיכלול מענה מיטבי לנושא אבטחת המידע בשימוש במחשוב ענן עבור המשק בכללותו ומשרדי הממשלה בפרט.

מערך הסייבר מסר בתשובתו כי כפי שצוין לעיל, בשנת 2020 החל פיתוח גרסה 2.0 של מסמך תורת ההגנה אשר זמינה כטיוטה לציבור באתר המערך. הגרסה העדכנית כוללת כיסוי של נושאים מתקדמים דוגמת ענן היברידי, הטמעת מודל "Zero-trust"[54], ניהול אירועים בענן ועוד. כמו כן, לאחר שיסתיים הליך המכרז של נימבוס, יחל המערך בפיתוח המלצות הגנה בהתאם לספק הרלוונטי, שכן הללו תלויות מאוד בספק שייבחר.

במאי 2017 פרסם מערך הסייבר מאמר בנושא "סיכונים בשימוש בשירותי ענן"[55] המפרט את סיכוני האבטחה המרכזיים והמלצות לצמצומם הן מבחינת נוהלי הארגון והן מהבחינה הטכנולוגית.

באוקטובר 2017 פרסם מערך הסייבר את מסמך "שימוש בשירותי ענן - הרחבה לתורת ההגנה בסייבר בארגון"[56], המיועד למנהלי אבטחת המידע בארגונים ומטרתו לשמש כלי עזר להסדרת בנייתה של תוכנית ההגנה הארגונית, תוך התייחסות לשירותי הענן שצורך הארגון.

באפריל 2019 פרסם מערך הסייבר את מסמך "המלצות ליישום הכולל דרישות עקרוניות לעבודה עם ספקים בתצורת ענן (מכל סוג שהוא)". מטרת המסמך, אשר מופנה למנהלי אבטחת המידע והגנת הסייבר בכל גופי המשק הישראלי וכאמור משמש כהמלצה, היא "להוות תשתית למסמך דרישות מלא עבור דרישות הגנת סייבר במכרזים ובהתקשרויות עם ספקי ענן ולרכז כלים ישימים לספקים מטעם מערך הסייבר בנושא". במסמך מצוין כי מתודולוגית ההקשחה שבה בחר מערך הסייבר כברירת מחדל היא מדריכי ההטמעה של הסוכנות להגנת מערכות מידע בארצות הברית (DISA-STIG).

מבדיקה שביצע משרד מבקר המדינה עלה כי נכון למועד הביקורת אין בקרה על יישום הנחיות מערך הסייבר בידי הגופים השונים. כמו כן עלה כי למערך הסייבר אין הסמכות לקיים פיקוח ובקרה על יישום הנחיותיו בנושא הענן בגופים השונים, למעט הגופים המוגדרים תשתית מדינה קריטית.

מערך הסייבר מסר למשרד מבקר המדינה בפברואר 2021 כי המערך רואה חשיבות בהטמעת המסמכים במשק, ולטובת העניין נוקט במספר פעילויות כגון: הקמת קבוצות עבודה עם נציגים מהתעשייה בהן מתעדכנים אודות פרסומים חדשים ומקבלים סקירות מקצועיות; פיתוח מערכת יוב"ל[57] המסייעת למערך לבחון את מידת השימוש של גופים בהמלצות ההגנה של המערך; ביצוע פיילוטים בעת כתיבת המלצות ההגנה למשק וכיו"ב.

54 המודל מתבסס על "אפס אמון" באנשים המנסים להיכנס למערכת הארגון.

55 להרחבה ראו: https://www.gov.il/he/departments/publications/reports/cloud

56 להרחבה ראו: https://www.gov.il/he/departments/policies/cloud_services

57 להרחבה ראו: https://www.gov.il/he/departments/general/yuvalinfo

מוצע כי מערך הסייבר יבחן ביצוע עריכת סקר עתי לבדיקת קריאת ויישום ההנחיות בידי הגופים השונים, הן על מנת לצמצם את הסיכון כי לא ניתן מענה ראוי לנושא אבטחת המידע ביישום מערכת בסביבת הענן והן על מנת לבחון את אפקטיביות פעולותיו. עוד מומלץ כי מערך הסייבר ימשיך לפעול להסדרת סמכויות פיקוח ובקרה על יישום הנחיותיו.

פעולות פיקוח של הרשות להגנת הפרטיות

הרשות להגנת הפרטיות היא הגוף המסדיר, המפקח והאוכף את קיום הוראות חוק הגנת הפרטיות והתקנות מכוחו[58]. פעילות האסדרה של הרשות נעשית בשלושה אפיקים מרכזיים: אסדרה משפטית, רישום ואכיפה מינהלית ופלילית. בשנים האחרונות שונו והורחבו כלי הפיקוח של הרשות להגנת הפרטיות באמצעות הוספת הליך פיקוח רוחב, שבמסגרתו נשלחים שאלונים לגופים רבים שמנהלים או מעבדים מידע אישי, מנותחים ממצאי השאלונים, וכשמתעורר צורך מתבצע גם פיקוח במקום בכמה מהגופים.

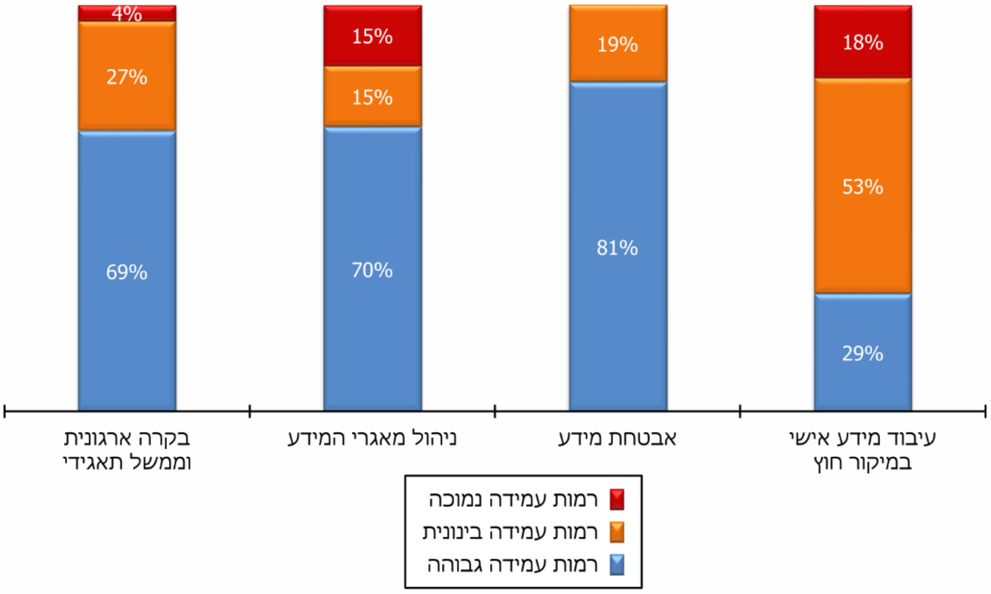
בעבר עמדה הרשות להגנת הפרטיות על כך שמשאבי הפיקוח שלה מצומצמים ביחס למספר הגופים המפוקחים והיקף המידע המנוהל על ידם, ועל כן היא נדרשת למדיניות אכיפה מושכלת המבוססת על סקר סיכונים לקביעת סדרי עדיפות לפעולותיה לגבי תופעות או תחומי סיכון מסוימים שזוהו. לפי מדיניות אכיפה זו, הרשות משקיעה את משאביה בעיקר באסדרת נושאים בעלי השפעה רוחבית על כלל מפוקחיה, באמצעות פיקוחים נושאיים ומגזריים.

בספטמבר 2020 מסרה הרשות להגנת הפרטיות למשרד מבקר המדינה כי היא לוקחת חלק פעיל בוועדת הענן המנוהלת כאמור על ידי יה"ב, על מנת לוודא כי משרדים המתכננים להעביר יישומים לסביבת הענן לוקחים בחשבון גם היבטים של הגנת הפרטיות. כמו כן, באוקטובר 2020 פרסמה הרשות להגנת הפרטיות את "ממצאי הליך פיקוח הרוחב בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל"[59] (להלן - דוח הפיקוח). במסגרת הפרסום, הרשות חילקה את ממצאיה לארבעה תבחינים: בקרה ארגונית וממשל תאגידי; ניהול מאגרי מידע; אבטחת מידע; ועיבוד מידע אישי במיקור חוץ. התרשים שלהלן מראה את רמת העמידה בחוק הגנת הפרטיות והתקנות מכוחו, על פי תשובותיהם של 26 גופים:

58 בהחלטת ממשלה מספר 4660 מ-19.1.06 הוקמה רשות משפטית לטכנולוגיות מידע והגנת הפרטיות במשרד המשפטים. בהחלטת ממשלה מספר 4820 מ-28.6.12 שונה שמה ל"רשות למשפט, טכנולוגיה ומידע". בהחלטת ממשלה מספר 3019 מ-7.9.17 שונה שמה ל"רשות להגנת הפרטיות"

59 להרחבה ראו: www.gov.il/he/departments/publications/reports/audit_report_database_companies

תרשים 16: **רמת העמידה בחוק הגנת הפרטיות והתקנות מכוחו, מגזר שירותי אחסון ועיבוד מאגרי מידע, יולי 2018 - יוני 2019**



מקור: הרשות להגנת הפרטיות

הרשות להגנת הפרטיות ציינה במסקנותיה כי נכון לאוקטובר 2020 "קיימת אי בהירות באשר להיקף תחולת החוק והתקנות על כלל הגופים המשתייכים למגזר זה (שירותי אחסון ועיבוד מאגרי מידע), מתוקף היותם מחזיקים במאגר...הממצאים מצביעים גם על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ". הרשות הצביעה בדוח הפיקוח על הצעדים שעל הגופים לנקוט על מנת לעמוד בדרישות החוק והתקנות מכוחו. בין היתר, הרשות מנחה גופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון עוד לפני ההתקשרות את סיכוני אבטחת המידע הכרוכים בה. כמו כן, על הגופים לוודא כי קיים הסכם התקשרות מול כל גורם חיצוני המחזיק במאגר אשר יכלול את כל הוראות התקנות הרלוונטיות והתייחסות לחובות ולאחריות הספק.

בספטמבר 2020 הרשות להגנת הפרטיות העבירה לידי משרד מבקר המדינה דוגמאות אחדות לאירועי אבטחת מידע אשר על פי החשד מקורם במערכות הפועלות בסביבת הענן - בין היתר מערכות המשרתות רשויות מקומיות, חברות ממשלתיות, עמותות ועוד.

מוצע כי רשות התקשוב תפעל להטמעת המסקנות וההמלצות מהליך הפיקוח ומתחקור האירועים של הרשות להגנת הפרטיות.

רשות התקשוב מסרה בפברואר 2021 כי מכרז נימבוס נותן מענה להיבטי הגנת הפרטיות בשני אופנים: המכרז נבנה כאמור בתצורת Zero Trust אשר אינו מאפשר לספק הענן לגשת למידע. כמו כן, היות ובמסגרת המכרז יוקם אתר מקומי (Region) בישראל, ממילא יחולו עליו חוק הגנת הפרטיות והתקנות מכוחו.

פעילות מגזרית בתחום הגנת הסייבר במחשוב ענן

החלטת הממשלה 2443 ל"קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" כללה בין היתר גם הקמת יחידות להכוונה מקצועית מגזרית[60] בתחום הגנת הסייבר במשרדי הממשלה, בהתאם לסמכויות הרגולציה המופעלות על ידי המשרד הממשלתי או במסגרתו. היחידות פועלות בכפיפות למשרד הממשלתי שאליהן הן שייכות, תחת הנחיה מקצועית של מערך הסייבר.

בנובמבר 2019 הקים משרד הבריאות ועדה ייעודית למגזר הבריאות אשר תרכז את פעילות המעבר לענן בכל הגופים הכפופים לו, לרבות גופים לא ממשלתיים כגון קופות החולים ובתי חולים פרטיים. את הוועדה מרכז מנהל הטכנולוגיות הראשי של משרד הבריאות, המשמש גם כממונה הגנת הסייבר של המשרד, וחברים בה גם נציגי מערך הסייבר, יה"ב והרשות להגנת הפרטיות. נכון ליולי 2020, הוועדה הייעודית קיימה חמש ישיבות ודנה ב-13 מערכות של גופים שונים במגזר הבריאות.

מפגישות שקיים משרד מבקר המדינה בנובמבר 2020 עם מנהל הטכנולוגיות הראשי של משרד הבריאות עולה כי לאור המוכנות ההולכת וגדלה של גופים במגזר הבריאות ליישום מערכות בענן, החליט המשרד על ביצוע תוכנית ניסוי (פיילוט) בבית חולים ממשלתי שבמסגרתה ינהל בית החולים ועדת ענן פנימית וייעזר בכלי לניהול סיכונים אשר פותח על ידי משרד הבריאות, מערך הסייבר והרשות להגנת הפרטיות. אם תצליח תוכנית הניסוי, משרד הבריאות מתכוון להרחיבה לגופי בריאות נוספים בהתאם לרמת המוכנות של הגוף.

בפגישה שקיים משרד מבקר המדינה עם משרד האנרגיה וכן בתשובתו של משרד האנרגיה מפברואר 2021 נמסר כי אגף טכנולוגיות ומידע במשרד האנרגיה אחראי על הרשת הפנים-ארגונית ולא על גופים מפוקחים.

> מפגישות שקיים משרד מבקר המדינה ביולי ואוגוסט 2020 עם מערך הסייבר, יה"ב וכמה משרדי ממשלה עולה כי גופים הכפופים אסדרתית למשרד ממשלתי אך אינם כפופים להנחיות יה"ב מנהלים באופן עצמאי את תחום הגנת הסייבר במערכות המחשוב שלהם, לרבות בתחום יישום מערכות ענן, ללא גורם מוביל ומפקח. כך לדוגמה, לא הייתה הנחיה פרטנית בנושא יישום מערכות בסביבת הענן בגופים שונים בתחומי התחבורה, התקשורת והאנרגיה. לאור הסיכונים הפוטנציאליים במעבר לענן, היעדר הנחיה מתאימה עלול להביא להתממשות סיכונים ואירועי אבטחת מידע משמעותיים אצל הגופים האמורים. יש לציין כי רק חלק מהגופים מוגדרים כתשתית מדינה קריטית[61] וככאלו מונחים באופן הדוק על ידי מערך הסייבר, ואילו היתר לא מונחים בידי אף גורם ממשלתי בנושא ענן.

60 מגזר - כלל הגופים הפועלים במסגרת תחום מקצועי של משרד ממשלתי ובמסגרת אחריותו הרגולטורית (מתוך החלטת הממשלה 2443).

61 האחריות להנחיית גופים אשר להם מערכות ממוחשבות חיוניות (או תמ"ק) הוטלה ראשית על שירות הביטחון הכללי במסגרת החוק להסדר הביטחון בגופים ציבוריים, התשנ"ח-1998. עם הקמת מערך הסייבר הלאומי, נקבע בהחלטת הממשלה 2443 כי המערך יקבל את האחריות להנחיית גופי תמ"ק.

מוצע כי משרדי הממשלה המשמשים כמאסדרים של מגזר פעילות יבחנו את הצורך בהקמת ועדות ענן ייעודיות לגופים הכפופים להנחיות המגזריות וביצוע בקרות על יישום מערכות בענן של הגופים, על מנת להבטיח את רמת אבטחת המידע והגנת הסייבר בעת יישום מיזמי מעבר לענן בקרב גופים אלו. בעת הבחינה יש לקחת בחשבון כי לעיתים הגופים המונחים הם חברות ציבוריות ופרטיות ויש לעדכן בהתאם את מערכת היחסים הרשמית מולם, לדוגמה עדכון תנאי רישיון, הסדרת תנאי פיקוח וכדומה. לחילופין, מומלץ כי משרדי הממשלה יבחנו את האפשרות להנחות את הגופים הכפופים והמפוקחים על ידם להקים ועדות ענן פנימיות אשר ידווחו למשרד הממשלתי על יישום מערכות בענן.

משרד התקשורת מסר למשרד מבקר המדינה בתשובתו מפברואר 2021 כי בהתאם לתוספת הרביעית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, הגורם שמנחה את חברות התקשורת המרכזיות בשוק התקשורת לעניין תחום הגנת הסייבר הוא שירות הביטחון הכללי. עוד מסר המשרד כי הוא ער לסיכונים הפוטנציאליים במעבר של חברות התקשורת לענן, לרבות התממשותם של סיכונים ואירועי אבטחת מידע משמעותיים אצל הגופים האמורים. נוכח האמור, המשרד בוחן בימים אלו, יחד עם גורמים רלוונטיים נוספים, את פעולות האסדרה והפיקוח הנדרשות בנושא זה.

משרד התחבורה מסר למשרד מבקר המדינה בתשובתו מפברואר 2021 כי המשרד פרסם בינואר 2021 את מדיניות "הגנת הסייבר למגזר התחבורה" אשר כוללת בין היתר התייחסות למחשוב ענן. במשרד התחבורה קיים אגף בכיר ביטחון חירום וסייבר אשר מלווה את כלל הגופים במגזר התחבורה, כך שגם גופים שאינם כפופים ליה"ב מקבלים ליווי ממשלתי על ידי היחידה המגזרית. יחד עם זאת, הליווי שהמשרד מספק הינו "טיפה בים ביחס למה שנדרש לקיים בשוטף, היות וקיים מחסור חמור בתקציב ותקנים לנושא". כמו כן, משרד התחבורה מקבל את המלצת משרד מבקר המדינה לעניין הקמת ועדות ענן פנימיות, שיפעלו בדומה לוועדה של יה"ב, וזאת לפני עלייה מסיבית של מערכות חיוניות לענן ללא היכרות או שליטה בנעשה (בדגש על מערכות תפעוליות עם משמעות לחיי אדם). אולם, לשם קיום ועדת ענן נדרש כוח אדם מקצועי עם מומחיות לתחום זה ויכולת לטפל בעשרות פניות, כולל העמקה באופי הנתונים והמערכות. לרשות המשרד לא עומד כוח אדם כזה מפאת מחסור בהקצאת משאבים עבורו.

מומלץ כי מבקרי הפנים בכלל משרדי הממשלה וכן האגף לביקורת רשויות מקומיות במשרד הפנים יתנו את דעתם לחשיבות הנושא של מחשוב הענן וישקלו לשלב נושא זה בביקורת בהתאם למתודולוגיות המשמשות גופים אלו לבחירת הנושאים לביקורת.

משרד הפנים מסר בתשובתו כי האגף לביקורת ברשויות מקומיות ישקול במסגרת הנושאים לביקורת גם את נושא סיכוני הרשויות המקומיות במחשוב ענן. כמו כן מסר משרד הפנים כי במשרד התקיימו בשנת 2020 שתי בדיקות בנושא הגנת הסייבר - האחת במסגרת תיקוף הסמכת ISO27001, והשנייה במסגרת בקרה של יה"ב. שתי בדיקות אלו לא התייחסו לתחום יישום מערכות הענן, ואגף טכנולוגיות המידע מתכנן לבצע בשנת 2022 ביקורת ובדיקה מקיפה אשר תתייחס לתחום יישום מערכות הענן.

תקינה ונוהגים מיטביים של אבטחת מידע במחשוב ענן

על מנת להתמודד עם סיכוני אבטחת מידע במחשוב ענן, הוגדרו בעולם תקינה ונוהגים מיטביים (Best Practices). לוח 2 להלן מרכז את עיקר התקינה והנוהגים המיטביים בתחום אבטחת מידע בענן.

לוח 2: **תקינה ונוהגים מיטביים בתחום אבטחת מידע בענן**

המדינה	שם הגוף	עיקר הפעילות	מהות הפעילות
ישראל	ISO	תקינה בין-לאומית	Iso 27017 (אומץ בישראל)
			Iso 27018 (אומץ בישראל)
האיחוד האירופי	ENISA	סוכנות האיחוד האירופי להגנת סייבר	מסמך בנושא "מבט על שירותי מחשוב ענן מבחינת הגנת על תשתיות מידע קריטיות"
			מסמך בנושא "יתרונות, סיכונים והמלצות לאבטחת מידע עבור מחשוב ענן"
כלל עולמי	CSA	הארגון לביטחון בענן	STAR - תוכנית הסמכה לעמידה בדרישות אבטחת מידע בענן.
ארצות הברית	NIST	מכון התקנים האמריקאי	NIST 800-53
	FedRamp[62]	תוכנית ניהול הסיכונים וההסמכות הפדרלית	הסמכה מחייבת לספקיות ענן אשר מעוניינות למכור שירותים לגופים ממשלתיים בארצות הברית. לשם כך ניתנת הסמכת PATO בידי הסוכנות להגנת מערכות מידע בארה"ב של משרד ההגנה האמריקאי (DISA).

המקור: איסוף נתונים על ידי משרד מבקר המדינה

מהלוח שלעיל ניתן לראות כי נושא התקינה של אבטחת המידע והגנת הסייבר במחשוב ענן מעסיק ארגונים ומוסדות רבים בעולם, על מנת לנסות להגן ככל שניתן על ארגונים המבקשים ליישם מחשוב ענן. בביקורת עלה כי אין תקינה אחת מחייבת למגזר הציבורי בישראל בכל הקשור לאבטחת מידע במחשוב ענן, וכי הגורמים המנחים השונים בוחרים את התקינה שלדעתם רלוונטית.

62 Federal Risk and Authorization Management Program

להלן כמה דוגמאות להתייחסות לנושא התקינה ברשות התקשוב ויה"ב:

1. בהחלטת ממשלה 2443[63] משנת 2015 נכתב כי "ספקים של מערכות מחשוב, המוטמעות או מקושרות למערכות מחשוב ממשלתיות, המבקשים למכור לממשלה שירותים הקשורים בכך, יחויבו לעמוד בתקן אבטחת מידע ארגוני ממשפחת ת"י ISO 27001".

2. במסגרת מכרז המסגרת 21/17 של רשות התקשוב נכתב כי "תשתית הענן תעמוד בתקן אבטחת המידע כדוגמת CSA Star, ISO 27001 או תקן אבטחת מידע דומה אחר. דרישות לעמידה בתקנים נוספים כדוגמת תקן PCI-DSS...תקני FedRAMP, SOC יפורטו ככל הנדרש בתיחורים".

3. במסגרת מכרז נימבוס נכתב כי חלק מתנאי הסף הם: "המציע עומד בכל התקנים הבאים יחדיו: ISO27018; ISO27017; ISO27001".

4. בהנחיית יה"ב בנושא "אבטחת מידע במעבר לענן ציבורי" אשר פורסמה בינואר 2017 ועודכנה בפברואר 2019 נכתב כי במסגרת השיטות המקובלות לבצע הערכת ספק קיימת אפשרות ל"הסתמכות על הערכה / בחינה של צד שלישי...בקטגוריה זו נמצאים גם ספקים אשר יספקו תעודת תאימות לתקנים כגון ISO27001, SSAE16 או CSA STAR. קיום הסמכות לתקנים אלה יכול להקל על מאמצי הבחינה והערכת הסיכונים".

מבחינת הפרוטוקולים של הוועדה המייעצת עולה כי על המשרדים למלא בבקשתם לוועדה את מדיניות אבטחת המידע של הספק המיועד. במסגרת עבודת הוועדה היא בוחנת את ההסמכות הקיימות לספקים המיועדים לבצע את הפרויקטים המבוקשים של המשרדים השונים, ומעירה בהתאם לצורך. אם טרם נבחר ספק, הוועדה הנחתה כי על הספק שייבחר לעמוד בתקן ISO27001.

> מומלץ כי הוועדה המייעצת תבחן קביעת תקינה מחייבת בישראל לספקי מחשוב ענן אשר תשמש את רשות התקשוב ויה"ב. עוד מומלץ כי במסגרת מיפוי המערכות בענן הוועדה המייעצת תוודא כי גם במיזמי ענן שיושמו לפני הקמת הוועדה נבחרו ספקים המחזיקים בהסמכות אבטחת מידע מספקות.

רשות התקשוב מסרה בתשובתה כי היבטי העמידה בתקני אבטחת המידע של ספקי מחשוב ענן מוסדרים בפרויקט נימבוס.

בחינת מיזמי ענן שבוצעו

על מנת לעמוד על אופן יישומם של מיזמי ענן במשרדי הממשלה, משרד מבקר המדינה בחן שלושה פרויקטים אשר כללו מעבר לשימוש בשירותי ענן במשרד ראש הממשלה, במשרד הבינוי והשיכון ובמשרד הבריאות. בפרויקטים נבדקו היבטים של אבטחת מידע ובקרה תקציבית בכל אחד מהפרויקטים. להלן הפרטים:

63 החלטה 2443 של הממשלה ה-33, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

משרד ראש הממשלה:
מערכת מעקב יישום החלטות ממשלה

בשנת 2015 קבעה הממשלה ה-34 בתקנון לעבודת הממשלה[64] כי משרד ראש הממשלה (להלן - משרד רה"ם) אחראי למעקב אחר ביצוע החלטות הממשלה, לריכוז דיווחי המשרדים הממשלתיים השונים ולהצגה תקופתית של ביצוע החלטות הממשלה. בתחילה בוצע המעקב באמצעים ידניים, אולם לאור הסרבול והקושי לקיים ניהול מעקב תקין הוחלט על הקמת מערכת ממוחשבת ייעודית לצורך ביצוע המעקב (להלן - מערכת המעקב).

מערכת המעקב הוקמה על תשתית ענן, ומטרתה הייתה לסייע לכלל המשרדים לדווח על יישום החלטות הממשלה בפועל וכן להנגיש את המידע לציבור. המערכת קולטת את החלטות הממשלה החדשות ומעבירה אותן לאגף ממשל וחברה במשרד רה"ם על מנת שיפרוט את ההחלטות למשימות ויקצה את המשימות הללו לגורמים הרלוונטיים במשרדים. המידע נשמר באתרים שונים במדינות האיחוד האירופי. עלות הקמת המערכת הסתכמה בכ-5 מיליון ש"ח, מתוכם 3.5 מיליון ש"ח להקמה הראשונית של המערכת וכ-1.5 מיליון ש"ח לצורכי ייצוב, תחזוקה והעברת הידע לאגף טכנולוגיות המידע של משרד ראש הממשלה.

אבטחת מידע: בספטמבר 2018 הגיש משרד רה"ם בקשה לוועדה המייעצת להקמה בענן של "מערכת בין משרדית למעקב אחר ביצוע החלטות ממשלה". בנובמבר 2018 דנה הוועדה המייעצת בבקשת משרד רה"ם ליישם את המערכת האמורה בסביבת ענן. לבקשה צורפה חוות דעת משפטית מנובמבר 2018 אשר קבעה כי אין מניעה לשימוש בענן לצורך יישום מערכת זו.

הוועדה המליצה להעלות את המערכת לענן, בכפוף ליישום ההמלצות שניתנו. בין היתר נקבע כי על משרד רה"ם לבצע בדיקות חדירות[65] וליישם את ההמלצות עד ל-2.12.2018, וכן לתאם ביקורת יה"ב עד סוף ינואר 2019. בחודשים נובמבר ודצמבר 2018 בוצעו למערכת בדיקות חדירות וכן סקירות אבטחת מידע על ידי גורמים בלתי תלויים. בסקירות אלה לא נמצאו ליקויים קיימים, ועל כן החליטה יה"ב לא לבצע סקירה נוספת. המערכת עלתה לסביבת הענן בדצמבר 2018.

> על פי פרוטוקול הוועדה, היה על משרד רה"ם לבצע בדיקות חדירה או סקר סיכונים למערכת כל 18 חודשים, החל ממועד הקמתה. בביקורת נמצא כי נכון לפברואר 2021, טרם בוצעו בדיקות חדירה נוספות על אלו שבוצעו בהקמת המערכת, וכן לא בוצע סקר סיכונים נוסף.
>
> על משרד רה"ם לבצע בדיקות חדירה או סקרי סיכונים למערכת, בהתאם להנחיות הוועדה המייעצת של יה"ב. כמו כן, על משרד רה"ם להקפיד לבצע בדיקות אלו בכל 18 חודשים, בהתאם להנחיות הוועדה.

משרד רה"ם מסר למשרד מבקר המדינה בתשובתו מפברואר 2021 כי בדיקות החדירות וסקר הסיכונים למערכת המעקב אחר החלטות הממשלה, בוצעו בעבר בהתקשרויות דרך מכרז מרכזי

---

64 התקנון אושר בהחלטת הממשלה 29 מ-26.5.15. להרחבה ראו: https://www.gov.il/he/departments/policies/2015_dec29.

65 בדיקת חדירות (Penetration test) היא מתקפה מתוכננת ומבוקרת על מערכת ממוחשבת שנועדה למצוא חולשות אבטחה, ולבחון את פוטנציאל הגישה לחולשות אלו ואת הערך שניתן להפיק מהגישה אליהן ואל המידע שהן מאחסנות.

לניהול סיכונים. תוקף המכרז המרכזי לא חודש, ולכן משרד רה"ם ויה"ב בוחנים את האפשרויות לביצוע סקר הסיכונים ובדיקות החדירות. לאחר הסדרת הסוגיות המכרזיות, משרד רה"ם יבצע את בדיקות החדירות וסקר הסיכונים בהתאם ללוחות הזמנים כפי שנקבעו בפרוטוקול הוועדה ובהתאם להנחיות יה"ב.

בקרה תקציבית: מפגישות שקיים ביולי 2020 משרד מבקר המדינה עם משרד רה"ם עלה כי המשרד לא מבצע תהליך מוסדר של בקרה תקציבית שוטפת על הפרויקט בשל עלותו שאינה גבוהה. משרד רה"ם מסר כי עלות השימוש במערכת עומדת על כ-30,000 ש"ח בחודש, מתוכן כ-6,000 ש"ח עבור המערכת עצמה ושאר העלויות (כ-80%) מופנות להיבטי אבטחת מידע והגנת סייבר. משרד רה"ם הוסיף כי אבטחת המידע והגנת הסייבר נערכות ברמה התשתית, ולכן עם העברת מערכות נוספות לסביבת הענן העלויות המדוברות יתחלקו בין כל המערכות.

בתשובה נוספת מאפריל 2021 מסר משרד רה"ם כי על פי סיכום עם אגף התקציבים הוגדרה להקמת המערכת מסגרת תקציבית ברורה לפי שנים, אשר לא חרגו ממנה, וכי לא מבוצעת בקרה תקציבית מעבר לכך.

משרד הבינוי והשיכון: מערכת מחיר למשתכן

מערכת מחיר למשתכן היא יישומון המאפשר לזכאי תוכנית מחיר למשתכן של משרד הבינוי והשיכון להירשם להגרלות לדיור שמבצע המשרד במסגרת תוכנית זו. היישומון המקוון פותח בידי ספק חיצוני והותקן על גבי תשתית ענן מסוג PaaS. עלות הקמת המערכת הסתכמה בכ-2 מיליון ש"ח.

אבטחת מידע: מערכת מחיר למשתכן עלתה לאוויר בשנת 2015, טרם הקמת הוועדה המייעצת. בהליך הקמת המערכת נערכו בדיקות חדירות על ידי חברה חיצונית וסקירת אבטחה של הקוד[66]. לאחר הקמת הוועדה המייעצת, ביקש משרד הבינוי והשיכון חוות דעת בדיעבד על המערכת. בספטמבר 2016 ביצעה יה"ב מבדק אבטחת מידע לתשתית הענן של מערכת זו, וסיפקה המלצות שיושמו על ידי משרד הבינוי והשיכון.

כמו כן, משרד הבינוי והשיכון משתמש בשירותי ספק נוסף על מנת להגן על הגישה למערכת בענן. ספק זה מדווח באופן שוטף למשרד על אירועי תקיפה וכן מבצע ניסיונות תקיפה בעצמו על מנת לוודא כי הגדרות ההגנה מעודכנות ועוצרות את התקיפות. בנוסף, את תהליך ביצוע ההגרלות מלווה משרד רואי חשבון חיצוני. עבור כל הגרלה בנפרד בוחן משרד רואי החשבון היבטים שונים של בקרות בתחום אבטחת מידע המבוצעות על ידי המשרד, לרבות בקרות על בדיקות חדירות, הקשורות בין היתר גם לתשתית הענן של המערכת, ונותן את אישורו. בתשובת משרד הבינוי והשיכון מפברואר 2021 נמסר כי ארכיטקטורת המערכת נבנתה באופן המאפשר את ביצוע ההגרלה ללא התערבות חיצונית. ההגרלה עצמה מבוצעת במחשב שאינו מחובר לרשת המשרד, ואילו בענן נשמרים כל נתוני ההרשמה והמידע המיועד להנגשה לנרשמים להגרלות.

בקרה תקציבית: על פי מידע שמסר משרד הבינוי והשיכון, עלות השימוש במערכת הסתכמה בכ-50,000 דולר בשנת 2018 ובכ-68,000 דולר בשנת 2019. מפגישות שקיים משרד מבקר

66 סקירת אבטחה של הקוד (security code review) נועדה לזהות פגמי אבטחה ביישום הקשורים לתכונות ולעיצוב של הקוד שבו נכתב היישום.

המדינה ביולי 2020 עם משרד הבינוי והשיכון עלה כי נכון למועד הפגישות, בקרת העלויות מבוצעת על ידי אגף מערכות מידע באמצעות הגדרת מסגרת עלויות חודשית שלא ניתן לחרוג ממנה והתראות לאחר ניצול של אחוז מסוים מהמסגרת. לדברי משרד הבינוי והשיכון, חשבות המשרד טרם מתמצאת בבקרה על פרויקטים המבוצעים בסביבת הענן. לדברי המשרד, הציפייה היא כי מכרז נימבוס ייתן מענה לנושא הבקרה החשבונאית על ידי גורמי המקצוע במשרד.

משרד הבריאות: חדרי מחקר

משרד הבריאות הוא הזרוע הממשלתית המופקדת על בריאות הציבור. המשרד אוסף מידע מכוח חיקוקים שונים על מנת לקבל תמונה שלמה ככל שניתן על מערכת הבריאות בישראל, צרכיה, מגבלותיה, מגמותיה, המשאבים שהיא צורכת ושהיא מספקת וכיוצא בזה, על מנת שיוכל להפיק תובנות לתועלת כלל הציבור ולקדם את מערכת הבריאות בישראל.

אחת הדרכים לקידום מערכת הבריאות בישראל היא שימוש במידע הנצבר במשרד הבריאות למטרות מחקר[67], הן בידי משרד הבריאות עצמו והן בידי חוקרים חיצוניים. לשם כך החליט משרד הבריאות על יצירת סביבה ייעודית לכל מחקר, אשר תכיל כלים ונתונים רלוונטיים עבורו לאחר שעברו התממה עמוקה[68]. סביבה זו יכולה להתקיים בענן או בתשתיות המקומיות.

באוקטובר 2015 פרסם משרד הבריאות מכרז בנושא הקמת "מערכת לאיסוף, ניהול ואנליזה של מידע מובנה ומידע בלתי מובנה, בטכנולוגיות Big Data". במכרז נדרשים הספקים לתת מענה לכל אחת מהדרישות הן בסביבת ענן והן ביישום על גבי תשתית מקומית (On Premises), תוך מתן גמישות רבה במעבר בין התצורות. המכרז מסביר כי "המערכת עשויה להשתלב בעתיד ב-'ענן הבריאות' של המשרד, ענן היברידי אשר חלקו ישב בענן ציבורי טהור, וחלקו, משיקולי ביטחון מידע, עשוי לשבת בענן פרטי בתחומי מדינת ישראל".

אבטחת מידע: באוגוסט 2016 הגיש משרד הבריאות לוועדה המייעצת בקשה להקמת "חדרי מחקר וירטואליים מאובטחים בסביבת ענן למחקרי בריאות אגרגטיביים". בדיון שהתקיים סברה הוועדה כי "רמת הסיכון בשימוש בשירותי ענן בחו"ל למערכת זו גבוהה, ועל כן לא סבורה שיש מקום לחריגה מהמדיניות שלא להוציא מידע אישי לענן זה. באם משרד הבריאות סבור כי יש לקיים דיון נוסף של הוועדה בנושא, על מנכ"ל המשרד, יועמ"ש וממונה סייבר להגיע ביחד להסכמה שאין מניעה משפטית/אחרת. כשתוצג הסכמה כאמור, הוועדה תדון שוב".

בעקבות מענה זה קיים משרד הבריאות התייעצויות נוספות עם רשות התקשוב ועם הרשות להגנת הפרטיות, ובעקבותיהן העבירה ביולי 2017 ראש אגף בריאות דיגיטלית ומחשוב דאז בקשה לוועדה המייעצת ל"הסרת התנגדות להעלאת חדרי מחקר וירטואליים לענן ציבורי". הבקשה כללה את אישור היועצת המשפטית של משרד הבריאות והסכמת ממונה הסייבר המשרדי ומנכ"ל המשרד לנושא. בנובמבר 2017 השיבה הוועדה המייעצת למשרד הבריאות כי לאור הפעולות שביצע בתחומי הגנת הפרטיות ואבטחת המידע, היא אינה רואה מניעה בקידום

---

67 להרחבה ראו מיזם תמנ"ע (תשתיות מחקר נתוני עתק):
https://www.health.gov.il/Subjects/DigitalHealth/Activity/Projects/Pages/BigData.aspx

68 התממה היא תהליך להפיכת מידע מזוהה למידע שאינו מזוהה עם האדם שאליו הוא קשור. התממה עמוקה משמעה כי המידע עבר תהליך התממה שני וחד-כיווני.

חדרי מחקר וירטואליים בענן. באוגוסט 2019 ביצע משרד הבריאות באמצעות חברה חיצונית מבדקי חדירה לסביבות המחקר, גם לאלו המותקנות מקומית וגם לאלו בענן.

בקרה תקציבית: מפגישות שקיים ביולי 2020 משרד מבקר המדינה עם משרד הבריאות עלה כי טרם הוסדר תהליך בקרה תקציבית על עלויות השימוש בחדרי המחקר. לתהליך הבקרה התקציבית קיימת חשיבות רבה כיוון שכל עלויות ההקמה והשימוש מושתות על משרד הבריאות. כך למשל, במאי 2020 פנה משרד הבריאות לחוקרים והציע קיום מחקרים על "מאגר קורונה למחקר" אשר הקים המשרד. על פי הפנייה, "השימוש בפלטפורמת המחקר הינו ללא עלות, כל עוד צוות המחקר יסתפק בשירות שיוצע על ידי משרד הבריאות מבחינת תוכנות ונתונים המוצעים בפלטפורמה". עוד נמסר ביולי 2020 מצד משרד הבריאות כי בכוונתו לייצר מודל הפעלה אשר במסגרתו יישא החוקר בחלק מעלויות הפעלת חדר המחקר. בתשובתו מפברואר 2021 מסר משרד הבריאות למשרד מבקר המדינה כי מבוצע שימוש במודולים הקיימים בענן, לצמצום עלויות ותשלום לפי ניצול משאבים. כך לדוגמה מדמימים באופן אוטומטי סביבות פיתוח בענן מחוץ לשעות העבודה, סופי שבוע וחגים.

מבדיקת שלושת הפרויקטים עולה כי היבטי אבטחת המידע והגנת הסייבר הובאו בחשבון בשלב ההקמה של כל אחד מהם. לצד זאת, היבטים הקשורים לבקרה תקציבית על פרויקטים אלו אינם מוסדרים, וכל משרד מנהל את הבקרה התקציבית על פרויקטים אלו כפי שהוא מוצא לנכון. כפי שתואר לעיל, אחד ממאפייני מודל מחשוב הענן הוא צריכת משאבים על פי הצורך, כך שעלות השימוש במחשוב ענן יכולה להשתנות באופן ניכר מדי חודש. האמור מחזק את הצורך בביצוע בקרה תקציבית מסודרת ושוטפת על מערכות מחשוב ענן.

לאחר סיום הביקורת, בנובמבר 2020 פרסם מינהל הרכש הוראת תכ"ם "קווים מנחים לאישור ובקרת התקשרויות בענן". בהתאם להוראה, על המנמ"ר לערוך בקרה על ההתקשרויות בנושא הענן ולדווח על ממצאיה לחשב המשרד, במסגרת אישור החשבונות והרכישות הנוספות. ההוראה מפרטת את הבקרות המקובלות שחשבי המשרד יכולים לבקש תיעוד בגינן מהמנמ"ר.

ביצוע הליך מכרזי לרכישת שירותי ענן

תקנה 3(29) לתקנות חובת מכרזים, התשנ"ג-1993, מאפשרת להתקשר בפטור ממכרז עם ספק שירותים יחיד. המונח "ספק יחיד" משמעו מציע שהוא היחיד שמסוגל לבצע את העבודה, בהיעדר ספקים מתחרים אחרים[69].

69 על פי תקנה 3(29), "התקשרות עם מי שלפי זכויות מכוח דין או בהתאם למצב הדברים בפועל הוא היחיד המסוגל לבצע את נושא ההתקשרות (בתקנות אלה - ספק יחיד), לאחר בחינת קיומם של ספקים לפי תקנה 3א(א)".

מפגישות שקיים משרד מבקר המדינה ביולי 2020 עם שלושת משרדי הממשלה שלעיל, עולה כי בשני פרויקטים לא בוצע תהליך מכרזי אלא התקשרות בפטור ממכרז בעילה של ספק יחיד ועל בסיס הסכם מחירים מרביים[70] שקיים עם ספק התוכנה, על אף שההסכם לא חל על שירותי הענן של הספק. על פי נתוני יה"ב, ספק זה נבחר על ידי משרדי הממשלה ב-43 מתוך 102 פרויקטים שאושרו על ידי הוועדה המייעצת.

בספטמבר 2020 מסר מינהל הרכש למשרד מבקר המדינה כי אכן נמצאו בעבר מקרים שבהם, בניגוד למפורט בהסכם מחירים מרביים, משרדי ממשלה התקשרו עם הספק לקבל שירותי ענן על בסיס ההסכם. על כן פרסם מינהל הרכש הממשלתי הבהרה בנושא לחשבי משרדי הממשלה ולמנהלי מערכות המידע בחודש מרץ 2017. זאת ועוד, בהוראת התכ"ם נוסף סעיף ייעודי הקובע כי ההוראה אינה חלה על שירותי ענן. כמו כן מסר מינהל הרכש כי אין בידיו מיפוי מלא של המשרדים שבהם נעשה שימוש בסביבת הענן של הספק, אולם מעיון בהודעות הפטור של המכרזים עולה כי לא מדובר בהיקף גבוה באופן יחסי להיקפי השימוש הצפויים בענן.

משרד מבקר המדינה ממליץ כי לאור הגידול הצפוי בהתקשרויות הנוגעות למעבר לסביבת ענן, מינהל הרכש יוודא את העמידה בהנחיותיו בכל הנוגע להתקשרויות בין המשרדים לספקים לקבלת שירותי מחשוב בסביבת ענן, ולצורך כך יבחן את הצורך לבצע אחת לכמה שנים מיפוי כולל של ההתקשרויות - כולל מועדי ההתקשרויות, תוקפן ועלותן.

70 הסכם מחירים מרביים - משא ומתן מרכזי שמנוהל על ידי מינהל הרכש לצורך קביעת תנאי רכש מיטביים עבור משרדי הממשלה מול ספק מסוים לרשימה סגורה של מוצרים הכלולים בהסכם.

סיכום

טכנולוגיית הענן מאפשרת גישה נוחה ורחבה, באמצעות המרשתת או קו תקשורת ייעודי, למאגר משותף של משאבי מחשוב. אפשר להשתמש במשאבים אלו על פי הצורך, וניתן להקצותם או לבטל את הקצאתם במהירות ובלא להשקיע משאבי ניהול מרובים. שימוש נכון בטכנולוגיה זו עשוי לייעל את עבודת משרדי הממשלה, לשפר את תהליכי העבודה ולאפשר רמה גבוהה של אבטחת מידע והגנת הפרטיות במידע ממשלתי. לצד זאת, השימוש בטכנולוגיית הענן מעמיד אתגרים ניכרים בתחומים רבים, בהם אבטחת מידע והגנת הפרטיות, בקרה תקציבית, תלות בספק תשתית הענן וכיו"ב.

בשנים האחרונות פועלת ממשלת ישראל להעברת משרדי הממשלה ויחידות הסמך למודל מחשוב ענן, בין היתר באמצעות הגדרת מדיניות והנחיות מתאימים, הקמת ועדה מייעצת בתחומי אבטחת מידע והגנת הפרטיות והכנת מכרז לאספקת שירותי ענן על גבי מסדת מרכזית שתוקם בישראל. עם זאת, על פי המידע הקיים ביה"ב, נכון למועד סיום הביקורת עברו לסביבת הענן רק כ-100 מערכות מתוך אלפי מערכות המידע ותשתיות המחשוב הקיימות בממשלה.

תמונת המצב העולה מדוח זה מלמדת על חסמים שונים המעכבים או מונעים יישום של מערכות במחשוב ענן במשרדי ממשלה; על היבטים שונים שהמשרדים אינם מביאים בחשבון בעת היישום ושעשויים לגרום נזק, החל בנזק כספי וכלה בנזק תדמיתי; על קושי בבקרה על יישום הנחיות למעבר לענן אצל המשרדים, ובבקרה על גופים הכפופים להנחיות המגזריות של המשרדים אך אינם כפופים להנחיות רשות התקשוב ויה"ב; ועל מחסור במסגרת עבודה כוללת ומאושרת להעברת הממשלה לענן.

לשם יישום מיטבי של השימוש במערכות מחשוב ענן קיימות וכאלו שיוקמו בעתיד, ראוי כי החסמים והליקויים שפורטו וההמלצות שניתנו יקבלו מענה כולל, לרבות במסגרת מכרז נימבוס והקמת מרכז המצוינות התפעולית בענן.

יצוין כי במהלך הביקורת פרסמה רשות התקשוב בדצמבר 2020 הנחיה בנושא "אישור, תכנון ובקרה לשירותי ענן". ההנחיה החדשה מפרטת דגשים ובקרות אשר על המשרד לבצע בעת יישום פרויקט מחשוב ענן, לרבות בקרות בשלבים הבאים: תכנון; הכנת ההזמנה; יצירת ההתקשרות; אישור ההתקשרות והשימוש השוטף בשירותי הענן. כן יצוין כי בנובמבר 2020 פרסם מינהל הרכש הוראת תכ"ם "קווים מנחים לאישור ובקרת התקשרויות בענן".