מחשוב ענן

פרק א': רקע

מבוא

1. בשנים האחרונות מתפתחת מגמה של מעבר הולך וגובר לתצורות שונות של מחשוב ענן (Cloud Computing). טכנולוגיות אלו מאפשרות ניצול יעיל ונוח של משאבי מחשוב תוך אפשרות לשיתוף משאבים ולשימוש בהם לפי הצורך. זאת, בד בבד עם חיסכון בעלויות ציוד, שטחי ה- Data Center, חשמל וכד'. השימוש בשירותי מחשוב ענן על ידי בנקים בעולם ובישראל עשוי לשמש כמענה לצרכים עסקיים דוגמת שדרוג מערכות מהותיות. מגמה זו צפויה להתגבר, בין השאר על רקע התפתחות ושדרוג טכנולוגיית מחשוב הענן והגברת התחרות בין הבנקים.
2. בצד היתרונות הגלומים בשימוש בטכנולוגיות ענן, שימוש בטכנולוגיות אלו עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מהותיים הקשורים לאבטחת מידע והגנת הסייבר, המשכיות עסקית, שליטה ובקרה על נכסי ה- IT, וכד'. סיכונים אלו נגזרים, בין היתר, מתלות בנותני שירותים או טכנולוגיות ספציפיים; כלי ניהול, אבטחה, שליטה ובקרה שמיושמים בצורה שאינה מיטבית; קשיים בהגנה על המידע וביישום בקרות נאותות; העצמת הנזק הפוטנציאלי במקרה של כשל, במיוחד כאשר נוצרות נקודות כשל יחידות (Single Points of Failure); ועוד. נציין כי סיכונים אלו בחלקם אמנם מוכרים, אך נוכח המאפיינים הספציפיים של טכנולוגיות אלו גלומים בהן סיכונים ייחודיים.
3. הגישה הפיקוחית בהיבטי טכנולוגיה ואבטחת מידע והגנת הסייבר היא מאפשרת (Business enabler) ורואה במעבר מערכות התאגידים הבנקאיים למחשוב ענן, לרבות מערכות מהותיות, חלק מהחדשנות וההתפתחות הטכנולוגית. כל זאת בכפוף לניהול סיכונים מושכל, זהיר וקפדני.

3א. ניהול הסיכונים הכרוכים במחשוב ענן מהווה חלק מהמערך הכולל של ניהול סיכונים תפעוליים בכלל, וסיכוני טכנולוגיית המידע, אבטחת מידע והגנת הסייבר בפרט. משכך, הוראה זו תואמת את הוראת ניהול בנקאי תקין מס' 310 בנושא: "ניהול סיכונים" הקובעת עקרונות יסוד לניהול ולבקרת הסיכונים בראייה משולבת וכלל תאגידית (Firm Wide Risk Management), את הוראת ניהול בנקאי תקין מס' 350 בנושא: ניהול סיכונים תפעוליים" (להלן: "הוראה 350") הקובעת עקרונות כאמור בדגש על הסיכון התפעולי, ומשלימה בדגשים הייחודיים לעניין מחשוב ענן את הוראת ניהול בנקאי תקין מס' 364 בנושא: "ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר" (להלן: "הוראה 364") המהווה את התשתית להוראות הפיקוח על הבנקים בנושאים ייעודיים בתחום טכנולוגיית המידע.

תחולה

4. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א-1981 (להלן בהוראה זו – "תאגיד בנקאי"):
   1) תאגיד בנקאי;
   2) תאגיד כאמור בסעיפים 11(א) (3א) ו-(3ב);
   3) תאגיד כאמור בסעיף 11 (ב);

4) בעל רישיון נותן שירותי תשלום בעל חשיבות יציבותית כהגדרתו בסעיף 36ט וחברות בשליטתו.

(ב) בטל

5. הוראה זו אינה חלה על "ענן פרטי" כהגדרתו בסעיף 6 להוראה זו.

פרק ב': כללי

הגדרות

6. להלן הגדרות ההוראה:

"אירוע"	אירוע כשל טכנולוגי או אירוע אבטחת מידע.
"אירוע אבטחת מידע" ו"אירוע כשל טכנולוגי"	כהגדרתם בהוראה 364.
"דלף מידע"	כהגדרתו בהוראה 364.
הוראה 359	הוראת ניהול בנקאי תקין מס' 359A בנושא "מיקור חוץ".
"מחשוב ענן"	מודל המאפשר גישה נוחה מכל מקום, לפי דרישה, למאגר משותף של משאבי מחשוב הניתנים להגדרה (למשל: רשתות, שרתים, אחסון, יישומים ושירותים), שניתן להתאימו במהירות.
"מידע רגיש"	כהגדרתו בהוראה 364.
"מתקפת סייבר"	כהגדרתה בהוראה 364.
"ענן פרטי"	תשתית מחשוב ענן המוקצית לשימושו הבלעדי של תאגיד בנקאי אחד. התשתית יכולה להיות בבעלותו, בניהולו ובתפעולו של התאגיד הבנקאי או צד שלישי או בכל שילוב ביניהם והיא יכולה להתקיים בחצרי התאגיד הבנקאי או מחוצה להם.
"מחשוב ענן מהותי"	שימוש בשירותי מחשוב ענן במיקור חוץ כהגדרתו בסעיף 8 להוראה 359A, כאשר לעניין זה מהותיות פעילות מחשוב הענן תקבע על פי השיקולים המפורטים בסעיף 27 להוראה 359A ובנוסף גם על פי השיקולים הבאים: (א) סוג הענן. (ב) סוג שירות מחשוב הענן. (ג) שירות מחשוב הענן כולל מידע רגיש. (ד) המידע אינו מידע רגיש, אך כתוצאה מחשיפתו, ניתן להסיק פרטים שיאפשרו לתקוף או לפגוע בתאגיד הבנקאי או בלקוחותיו. (ה) שירות מחשוב הענן מספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד, ולא קיימים אמצעים דומים מסוגיהם גם בחצרי התאגיד הבנקאי.

הוראות כלליות

7. תאגיד בנקאי לא יאחסן, יעביר או יעבד מידע רגיש (כגון: נתוני לקוחות, מידע עסקי חסוי וכד') בענן מחוץ לגבולות מדינת ישראל, אלא אם כן, וידא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לרגולציית הגנת המידע של האיחוד האירופי (GDPR - General Data Protection Regulation).
8. שירותי מחשוב ענן מהותי ייחשבו פעילות מהותית במיקור חוץ וככאלה הינם כפופים להוראה 359A (למעט חובת הדיווח בסעיף 33 להוראה 359A) כמו גם להוראה זו, אשר מפרטת ומרחיבה את ההנחיות הייחודיות להם. בהתאם, ההגדרות המופיעות בהוראה 359A רלוונטיות גם להוראה זו.
9. אין בהוראה זו כדי לגרוע מהחובות החלות על התאגיד הבנקאי לפי כל החוקים והתקנות הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, ובכלל זאת, חוק הגנת הפרטיות ותקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.
10. התאגיד הבנקאי יוודא כי נותן שירות מחשוב הענן יישא באחריות כלפי התאגיד הבנקאי, לרבות קיום החובות הכלולות בחוזה ההתקשרות בין נותן שירות מחשוב הענן לתאגיד הבנקאי, גם במקרה בו נותן שירות מחשוב הענן עושה שימוש בנותן שירות משני.

פרק ג': ממשל תאגידי

11. פרק ב' בהוראה 359A בנושא ממשל תאגידי יחול גם על מחשוב ענן שאינו מחשוב ענן מהותי. זאת, למעט סעיפים 13(ג) ו- 16 בהוראה 359A.

דירקטוריון

12. על הדירקטוריון לדון במסמך "מדיניות לשימוש בשירותי מחשוב ענן", כאמור בסעיף 16 להלן, ולאשר אותו.
13. על הדירקטוריון לאשר את תכנית העבודה הרב שנתית למחשוב ענן, כאמור בסעיף 20 להלן, לרבות יישום של כל שירות מחשוב ענן מהותי.
14. על הדירקטוריון לוודא שהשימוש בשירותי מחשוב ענן יהיה על פי המדיניות שנקבעה כאמור.

הנהלה בכירה

15. על ההנהלה הבכירה לגבש מדיניות לשימוש בשירותי מחשוב ענן אשר תקבע, בין היתר, את מאפייני השירותים המוגדרים כמחשוב ענן מהותי ובהם נדרש אישור של הדירקטוריון, את מאפייני שירותי מחשוב הענן בהם נדרש אישור הנהלה בכירה וכן את מאפייני שירותי מחשוב הענן בהם נדרש אישור אחר.
16. מסמך "מדיניות לשימוש בשירותי מחשוב ענן" יתייחס לקביעת רמת מהותיות שירותי מחשוב הענן בהסתמך על הגדרת מחשוב ענן מהותי בהוראה זו; סמכויות, אחריות ופעולות גורמי ניהול שירותי מחשוב ענן לרבות ניהול נותן שירות מחשוב הענן, גורמי הבקרה והבקרות; מאפייני השירותים והיקפם, תהליכי אישור ודרגי אישור; אחריות הגורמים השונים בתאגיד הבנקאי לטיפול בהיבטים משפטיים, תחזוקה, ניטור, אבטחת מידע והגנת

הסייבר, טיפול באירוע, המשכיות עסקית ורציפות תפקודית וכד'. המדיניות תיתן מענה גם לנדרש בהוראה זו ובהוראות רלוונטיות נוספות.

17. ההנהלה הבכירה תעקוב באופן שוטף אחר יישום מדיניות מסמך "מדיניות לשימוש בשירותי מחשוב ענן", כפי שאושר על ידי הדירקטוריון.
18. התאגיד הבנקאי יגדיר גורם הכפוף למנהל חטיבת טכנולוגיית המידע שיכיר באופן מעמיק את הסיכונים ואת השירותים הטכנולוגיים של כל נותן שירותי מחשוב ענן עמו התקשר התאגיד הבנקאי. התאגיד הבנקאי יבחן את הצורך להגדיר גורם אחראי לכל נותן שירותי מחשוב ענן שעמו התקשר.
19. התאגיד הבנקאי יגדיר גורם הכפוף למנהל הסיכונים, שיכיר באופן מעמיק את סיכוני כלל הפעילות במחשוב ענן.
20. על ההנהלה הבכירה להכין תכנית עבודה רב שנתית למחשוב ענן. התכנית תתן מענה, בין היתר, לסיכונים הגלומים בשירותי מחשוב הענן והבקרות המיושמות או המתוכננות להפחתתם.

פרק ד': יישומי מחשוב ענן המחייבים קבלת היתר - בטל

פרק ה': ניהול סיכונים

21. סעיפים 24 עד 26 בהוראה 359A יחולו גם על מחשוב ענן שאינו מחשוב ענן מהותי.

22. בטל.

23. מבלי לגרוע מהאמור בהוראה 364 (לדוגמא, סעיפים 46 ו – 109), לעניין מחשוב ענן תאגיד בנקאי יבצע הערכת סיכונים וסקר סיכונים באופן הבא:

(א) מיפוי והערכת סיכונים לכל יישום של שירות מחשוב ענן. הערכת הסיכונים תעשה קודם להתקשרות עם נותן שירותי מחשוב הענן ותעודכן באופן שוטף במהלך תקופת ההתקשרות, בין היתר, בהתאם לשינויים, כגון: טכנולוגיים, משפטיים, רגולטוריים, עסקיים וארגוניים אצלו ואצל נותן שירותי מחשוב הענן. אמנם שירות מחשוב ענן מהווה מקרה פרטי של מיקור חוץ, אך הערכת הסיכונים במקרה זה צריכה לכלול גם סיכונים ייחודיים (טכנולוגיים ואחרים) הקשורים לשימוש במחשוב ענן. היבטים עיקריים שיש לקחת בחשבון מובאים בנספח ב' להוראה זו – "היבטים עיקריים להערכת סיכונים במחשוב ענן".

(ב) בשירותי מחשוב ענן מהותי ביצוע סקר סיכונים, כאמור בהוראה 350, יהיה לכל הפחות אחת לשנתיים.

(ג) ווידוא קיום בקרות מפצות מתאימות בהתאם להערכת הסיכונים.

24. הדוחות הסדירים המוגשים להנהלה הבכירה ולדירקטוריון בנושאי סיכונים תפעוליים, כאמור בהוראה 350, יכללו התייחסות פרטנית לסיכוני מחשוב ענן.

25. התאגיד הבנקאי יגדיר:

(א) תחומי אחריות לניהול, שליטה, אישור ותיעוד של שירותי מחשוב הענן בתאגיד הבנקאי.

(ב) מודל חלוקת אחריות בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן, ובכלל זה בהיבטי אבטחת מידע והגנת הסייבר. חלוקת אחריות זו אינה גורעת מאחריות התאגיד הבנקאי לקיום מכלול הדינים וההוראות החלים עליו.

26. עבור כל שירות מחשוב ענן התאגיד הבנקאי יתעד, לכל הפחות, את ההיבטים הבאים:

(א) ההחלטות והשיקולים במימוש שירותי מחשוב הענן, כגון: רמת מהותיות, שיקולים לשימוש בשירותי ענן, סיכונים, אישורים וכו'.

(ב) מאפייני נותן שירותי מחשוב הענן והחוזה עימו, כגון: תאריכי חתימת החוזה, חידושו, ואופציות להארכתו, מיקום מתקני הענן ואחסון הנתונים, סוג השירות ועלותו, סמכויות שיפוט וכו'.

(ג) מאפייני שירותי מחשוב הענן, כגון: מיפוי ותיאור הארכיטקטורה, הממשקים ודרישות אבטחת המידע והגנת הסייבר וכו'.

27. התאגיד הבנקאי יעדכן את התיעוד, כאמור בסעיף 26 לעיל, בכל מקרה של שינוי באחד המאפיינים המפורטים בסעיף האמור. כמו כן, אחת לתקופה שיקבע, יוודא התאגיד הבנקאי את עדכניות התיעוד האמור.

פרק ו': התקשרות עם נותן שירותי מחשוב הענן

28. פרק זה אינו חל על מחשוב ענן שאינו מחשוב ענן מהותי.

בדיקת נאותות

29. במחשוב ענן מהותי, התאגיד הבנקאי יבצע בדיקת נאותות (Due Diligence) לנותן שירותי מחשוב הענן, לרבות זיהוי והערכת הסיכונים הפוטנציאליים בהתקשרות עמו והשימוש בשירותיו, כאמור בסעיף 23, ולכל הפחות לפי הסיכונים המפורטים בנספח ב' להוראה זו – "היבטים עיקריים להערכת סיכונים במחשוב ענן". בנוסף התאגיד הבנקאי יבדוק:

(א) עמידה של נותן שירותי מחשוב הענן בכל דין ורגולציה הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, לרבות דיני הגנת הפרטיות החלים באותה המדינה בה הוא פועל.

(ב) עמידה של נותן שירותי מחשוב הענן ברמת הגנת סייבר נאותה, בין היתר כפי שיוגדר במסמך "מדיניות לשימוש בשירותי מחשוב ענן".

חוזה מחשוב ענן

30. מבלי לגרוע מהחובות החלות על התאגיד הבנקאי לפי הוראה 359A והוראה 364, במחשוב ענן מהותי חוזה ההתקשרות עם נותן שירותי מחשוב הענן יכלול, בין היתר, התייחסות לנושאים הבאים:

(א) מחיקת המידע של התאגיד הבנקאי, או פעולה דומה, ממערכות נותן שירותי מחשוב הענן והתחייבותו כי לא ניתן יהיה לאחזר מידע זה במערכותיו.

(ב) בטל.

(ג) בטל.

(ד) הבטחת יכולתו של התאגיד הבנקאי לקבל מידע הרלוונטי לפעילויות שהועברו למיקור חוץ המוחזק אצל נותן השירות, לרבות ביקורות שבוצעו אצל נותן השירות, ולבחון אותו או להעביר אותו למפקח על הבנקים על פי בקשתו.

(ה) יישום הנחיות המודל שנקבע לעניין חלוקת האחריות כנדרש בסעיף 25.

(ו) מיקום מתקן הענן ממנו יינתן השירות ומיקום אחסון הנתונים, לרבות התחייבות נותן שירות מחשוב הענן להודיע לתאגיד הבנקאי מראש על כל שינוי באמור.

(ז) אופן אחסון המידע הרגיש והנגישות אליו תוך כדי תקופת השירות ולאחריה.

(ח) גיבוי המידע והאפשרות לאחזורו.

(ט) הגדרת יכולת התאגיד הבנקאי להפעיל או להפסיק שירותי מחשוב ענן מהותיים או רכיבים מתוך שירותים אלה לרבות חסימות גישה, ככל שרלוונטי ובעת חירום כדוגמת מתקפת סייבר, מתוך הצורך לצמצם סיכונים. זאת, בין באופן עצמאי ובין על ידי נותן שירות מחשוב הענן בהתאם לבקשת התאגיד הבנקאי. הגדרת התהליכים התומכים ביכולות אלה, תוך התייחסות למשאבים של נותן שירותי מחשוב הענן בהם נעשה שימוש משותף על ידי התאגיד הבנקאי וגורמים אחרים המקבלים שירות מאותו נותן שירות מחשוב ענן.

(י) בחינת שילוב התחייבות נותן שירות מחשוב הענן להשתתפות בתרגילי סייבר שיקיים מולו התאגיד הבנקאי אחת לתקופה, בהתאם לאופי היישום.

(יא) יישום בקרות מפצות הנדרשות מנותן שירות מחשוב הענן בהתאם להערכת סיכונים כמפורט בסעיף 23 להוראה זו.

ניהול ההתקשרות עם נותן שירותי מחשוב ענן מהותי

31. התאגיד הבנקאי ינהל את ההתקשרות עם נותן שירותי מחשוב ענן מהותי על פי העקרונות הבאים:

(א) מעקב אחר ביצועי השירות, הבטחון ואבטחת המידע ועמידה ביעדי השירות המוסכמים עם נותן שירותי מחשוב הענן, כל זאת באמצעי ניטור התואמים את תיאבון הסיכון של התאגיד הבנקאי.

(ב) הערכה של ההסדרים עם נותן שירותי מחשוב הענן, בהתייחס למצבי סיכון, אירועים ושינויים שהתחוללו במהלך התקופה ולתפעול קריטי של מערכות המחשוב של התאגיד הבנקאי בענן. הערכה זו תכלול גם הערכת סיכונים ותביא בחשבון את יכולותיו של נותן שירותי מחשוב הענן, תוך עמידה בדרישות בהיבטי טכנולוגיה, המשכיות עסקית, אבטחת מידע והגנת הסייבר.

(ג) מעקב אחר יישום מודל חלוקת האחריות כנדרש בסעיף 25.

(ד) ניהול ממשקים קבועים ושוטפים של מנהל ההמשכיות העסקית ומנהל הגנת הסייבר של התאגיד הבנקאי עם הגורמים בתאגיד הבנקאי אשר ממונים על הקשר השוטף עם נותן שירותי מחשוב הענן, לרבות הגדרה ברורה של סמכויותיהם ותפקידיהם במסגרת ממשקים אלה.

(ה) קיום תכנית יציאה או סיום התקשרות. התכנית תיבדק ותתעדכן אחת לשלוש שנים.

(ו) בחינת הצורך בעדכון החוזה עם נותן שירותי מחשוב הענן לכל הפחות אחת לשלוש שנים או בעת התרחשות אירוע או שינוי מהותי בשירותי מחשוב הענן או שינוי בכל דין ורגולציה הרלבנטיים לשימוש בטכנולוגיות או בשירותי מחשוב ענן.

(ז) בכל שינוי בשליטה על נותן שירותי מחשוב הענן, נדרשת בחינה מחדש של ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם על ידי בעלי השליטה החדשים.

פרק ז': מכתב ההיתר - בטל

פרק ז'1: אבטחת מידע והגנת הסייבר

32. על התאגיד הבנקאי לנהל את סיכוני אבטחת המידע והגנת הסייבר במחשוב ענן (מהותי ושאינו מהותי), תוך התייחסות בין היתר להיבטים של סיווג המידע, מיקום מפתחות ההצפנה, מעורבות התאגיד הבנקאי בניהול מפתחות ההצפנה ורמת ההצפנה, שיטת ההצפנה ועוד.
33. על המידע של התאגיד הבנקאי להיות מוצפן בעת העברתו בתקשורת וכן בעת אחסונו. במקרים בהם יש קושי לתאגיד הבנקאי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידו כמידע רגיש או שיש בחשיפתם כדי לפגוע בתאגיד הבנקאי ובלקוחותיו.
34. על התאגיד הבנקאי לוודא שביכולתו לבצע ניטור רציף, מלא ובזמן אמת באופן שיאפשר לזהות מתקפת סייבר מוקדם ככל הניתן ובאופן הרלוונטי לסוג שירות מחשוב הענן, וזאת לגבי מתקפות סייבר הקשורות לשירותי מחשוב ענן בין היתר כמפורט בנספח ג' להוראה זו - "ניטור מתקפות סייבר במחשוב ענן".
35. על התאגיד הבנקאי להיערך להתמודדות עם אירועי אבטחת מידע בשירותי מחשוב ענן. היערכות זו תבוצע, בין היתר, בכלים הבאים:
    (א) קיום תרגילי סייבר;
    (ב) ביצוע תרחישים של מתקפות סייבר, שיכללו, לכל הפחות:
        1. מצב בו שירות המחשוב בענן עשוי להישאר פעיל ונגיש אך בפועל לא ניתן להסתמך על אמינות הנתונים המוצגים בו;
        2. תקיפות מערך הגיבויים של שירות המחשוב בענן;
        3. תקיפות שכחלק מהטיפול בהן יידרש ניתוק גישה מיעדים ספציפיים.
    (ג) ביצוע, לכל הפחות, של תרחיש קיצון אחד מייצג בפעילות אחת או יותר משירותי מחשוב הענן המהותיים שלו.
36. על התאגיד הבנקאי לוודא כי עבור כלל ערוצי הגישה אל שירות מחשוב הענן וממנו, קיימים אמצעים לאבטחת מידע ולהגנת הסייבר שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפת התאגיד הבנקאי.

פרק ז'2: המשכיות עסקית

37. ככל שמחשוב הענן מהווה שירות חיוני לתאגיד הבנקאי יחולו עליו הדרישות הרלוונטיות בהוראת ניהול בנקאי תקין מס' 355 בנושא "ניהול המשכיות עסקית" ובפרק י"ד "ניהול המשכיות עסקית (BCM)" שבהוראה 364.
38. ככל שמחשוב הענן הינו מחוץ לישראל, על התאגיד הבנקאי לבחון תכניות מענה לתרחיש של אי זמינות השירות כתוצאה מנתק תקשורתי לחו"ל או מאירועים גיאופוליטיים מול המדינה הזרה. זאת ועוד, התאגיד הבנקאי יעריך את יכולת ההמשכיות העסקית של נותן השירות אל מול איומי הייחוס המקומיים של המדינה המארחת.
39. באתר מחשוב בענן ראשי או חלופי - התאגיד הבנקאי נדרש לוודא עמידתו של האתר בדרישות Tier3 בהתאם לסטנדרטים שנקבעו בתקן UpTime Institute (UTI) על ידי קבלת תעודה מ-UTI או חוות דעת חיצונית מגורם מומחה בלתי תלוי.

פרק ח': דיווח לפיקוח

40. אחת לשנה בגין סיום שנה קלנדרית, על תאגיד בנקאי להעביר דיווח בכתב לידי הפיקוח על הבנקים. הדיווח יתבצע על פי הוראת דיווח לפיקוח מס' 881 בנושא "דיווח על מחשוב ענן (שנתי)".

עדכונים

חוזר מס'	גרסה	פרטים	תאריך
2536	1	מכתב מפקח מקורי	05/07/2017
2579	2	עדכון	13/11/2018
2669	3	עדכון	30/09/2021
2715	4	עדכון	13/06/2022
2849	5	עדכון	17/06/2026

נספח א' – דוגמאות למחשוב ענן מהותי - בטל

נספח ב' – היבטים עיקריים להערכת סיכונים במחשוב ענן

(א) סיכון רגולטורי הנובע משימוש בענן הממוקם מחוץ לגבולות מדינת ישראל - קושי בעמידה בחוקים, תקנות ורגולציות של מדינת ישראל ושל המדינה שבה פועל או מאוחסן השירות או הנתונים. מאחר וקיימים הבדלים בחקיקה בין המדינות יש חשיבות, בין היתר, להתייחס לסוגיות כגון חובת נותן שירותי מחשוב הענן למסור מידע לגורמי חוק ואכיפה גם ללא ידיעת התאגיד הבנקאי והיבטים של הגנת הפרטיות.

(ב) סיכון הנובע משימוש או מאי שימוש בתצורת ענן מרובה (תשתיות ענן המבוססות על שילוב של מספר פתרונות שונים של מחשוב ענן).

(ג) מחזור חיי הנתונים, לרבות מיקום, ריבוי העתקים וחשיפת נתונים.

(ד) ניידות נתונים, רכיבים ומערכות - למשל, האם השימוש ברכיבי מחשוב ענן של נותן שירותי מחשוב ענן מסוים מגביל את התאגיד הבנקאי ועלול למנוע ממנו את האפשרות לעבור לנותן שירותי מחשוב ענן אחר או להעביר את המידע או המערכות חזרה לחצרי הבנק.

(ה) סיכוני אבטחת מידע והגנת הסייבר לרבות דלף מידע, שימוש בכלי אבטחה ייעודיים, אופן ניהול מפתחות ההצפנה, שירות מחשוב ענן המספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד.

(ו) הרשאות גישה, תוך הפעלת כלים המתאימים לסביבת מחשוב ענן.

(ז) ניהול שינויים וניהול נכסי טכנולוגית המידע, לרבות התייחסות לצורך בשינויים הנדרשים מנותן שירותי מחשוב הענן כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים, לשליטה של התאגיד הבנקאי על שינויים במערכות ותאימות תהליכי השינויים למדיניות התאגיד הבנקאי ונהליו.

(ח) סיכונים הקשורים להמשכיות עסקית ו - BCP/DRP, לרבות שינויים בתצורת רשת התאגיד הבנקאי, ומיקומם הגאוגרפי של שרתי הענן ובכללם שרתי הגיבוי.

(ט) סיכונים הקשורים לסביבות העבודה וכלי הניהול העלולים להוסיף מורכבות לתפעול המערכות.

(י) סיכונים משפטיים וביניהם היבטי סודיות, שמירת נתונים ואחזורם, הבעלות על המידע ורישוי תוכנות.

(יא) סיכוני תפעול שוטף (כולל אנשי תמיכה, תהליכי עבודה, ניהול אירועים ועוד), טיפול באירועים חריגים, והקטנתם בין היתר באמצעות הסדרי דיווח וטיפול, הסדרת תחומי האחריות בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן.

(יב) סיכונים הנוגעים למעטפת התקיפה כגון: שילוב מכשירים ניידים (טלפונים ניידים, טאבלטים וכל אמצעי נייד אחר) בשירות מחשוב הענן.

(יג) סיכונים הכרוכים בשרשרת אספקה של שירות מחשוב ענן.

(יד) קיום הפרדה לוגית ומנהלתית בין המערכות של הלקוחות השונים בענן.

נספח ג' – ניטור מתקפות סייבר במחשוב ענן

(א) ניטור הפעילות בענן ישתלב במערך הניטור השוטף של התאגיד הבנקאי. ניהול הניטור והגדרתו יהיו בידי התאגיד הבנקאי, כך שניהול הניטור יהיה לכל הפחות בהתאמה לאופן היישום בענן.

(ב) בהתאם לאמור בסעיף (א), הניטור יכלול בין היתר חריגות מפעילות לגיטימית בתשתיות התאגיד הבנקאי הקשורות בשירות מחשוב הענן, כך לדוגמא שינויי ארכיטקטורת הרשת (סגמנטציה), הקמת שרת חדש, גישה לבסיסי נתונים, שינוי במנגנוני הצפנה, תעבורת רשת חריגה מסביבת הענן.

(ג) אם ניטור זה מבוצע באמצעות כלים המסופקים ע"י נותן שירותי מחשוב הענן, יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של התאגיד הבנקאי.

(ד) במידה והתאגיד הבנקאי ישתמש במערכת ניטור המצויה בסביבות הענן באותה סביבת תשתיתית בה מצוי שירות מחשוב ענן מהותי של התאגיד הבנקאי, התאגיד הבנקאי יגדיר פעולות בקרה להמשך רציפות ניטור שירות מחשוב הענן המהותי בעת ניתוק תקשורת בין התאגיד הבנקאי למערכת הניטור של סביבת הענן.