הפיקוח על הבנקים

תל-אביב, ז׳ טבת תשפ״ה

07 ינואר 2025

לכבוד התאגידים הבנקאיים ובעלי רישיון נותן שירותי תשלום יציבותי

יו״ר דירקטוריון ומנכ״ל

הנדון: היערכות המערכת הבנקאית לסיכוני סייבר הנובעים מיכולות מחשוב קוונטי

מחשוב קוונטי

1. מחשוב קוונטי הינו טכנולוגיה חדשנית בעלת פוטנציאל לספק יכולות מחשוב שיאפשרו פתרון בעיות מתמטיות מורכבות, שעד כה היו בלתי ניתנות לפתרון בהינתן יכולות המחשוב הקיימות. טכנולוגיה זו צפויה להביא לשינוי מהותי במגוון רחב של תחומים ותעשיות.
2. לצד היתרונות הגלומים בהתפתחות זו, מחשב קוונטי בעוצמות גדולות דיין, יוכל לשמש לפיצוח של אלגוריתם ההצפנה האסימטרית, שנמצא בשימוש נרחב, ולהחליש הצפנות אחרות (להלן: פריצת הצפנה בעידן המחשוב הקוונטי). שיטות הצפנה אלו מהוות, בין היתר, את הבסיס לחתימה דיגיטלית ולתקשורת מוצפנת ברשת האינטרנט. כתוצאה מכך, רמת האבטחה והחיסיון של עסקאות פיננסיות ונתונים רגישים שמוסדות פיננסיים מעבדים עלולה להיות בסיכון עם הופעתם של מחשבים קוונטיים חזקים מספיק. הסיכון הוא בחשיפה של מידע מוצפן וכן בפגיעה באמינות החתימות ואמינות המידע החתום.
3. עד לאחרונה, הערכות של מומחים ואנליסטים בתחום מערכות המידע היו כי ההיתכנות של מחשב קוונטי בעוצמה הנדרשת רחוקה עשרות שנים. אולם, משנת 2022, לאור התקדמות ביכולות הבניה של מחשבים קוונטיים חזקים ויציבים יותר, לוחות הזמנים מתקצרים. כיום, גורמי המקצוע המובילים, כולל אנליסטים וגופים בינלאומיים[1] מעריכים כי סיכוני פריצת ההצפנה בעידן המחשוב הקוונטי יתממשו בעשור הקרוב, או אף לפני.
4. מכון התקנים האמריקאי (NIST) התחיל בתהליך תקינה עולמי להצפנה פוסט-קוונטית ("Post Quantum Cryptography", PQC) תהליך זה כולל בחירת אלגוריתמים קריפטוגרפים אשר יוכלו לפעול עם פרוטוקולי רשת ותקשורת קיימים ולהגן על מידע רגיש מפני פריצת הצפנה בעידן המחשוב הקוונטי. במקביל, נמצאות בתהליך ניסוי יוזמות מחקר הכוללות טכנולוגיה קוונטית להפצת מפתחות ("Quantum Key Distribution", QKD) להקמת ערוצי תקשורת מאובטחים להפצת מפתחות הצפנה.

---

[1] *World Economic Forum* - WEF (2022) - Transitioning to a Quantum Secure Economy (pp. 9)
Monetary Authority of Singapore - MAS (2024) - Advisory on Addressing the Cybersecurity Risks Associated with Quantum
National Institute of Standards and Technology - NIST (2016) – Report on Post Quantum Cryptography (pp. 6)

5. הסיכון הקרוב ביותר הקשור לפיצוח הצפנה בעידן המחשוב הקוונטי הוא הפוטנציאל בהפיכתם המיידית של נתונים ומידע בעלי ערך לטווח זמן ארוך, שיש ערך בשמירתם מוצפנים למשך שנים קדימה, למידע שניתן לפענח אותו בצורה מהירה, ברגע שיהיו קיימות יכולות פריצת הצפנה בעידן המחשוב הקוונטי. סיכון זה, אשר מכונה גם "Harvest now, Decrypt later", מתייחס לאפשרות של גניבת מידע מוצפן שנאסף באירועי סייבר שונים כבר עתה ושמירתו על ידי התוקפים למועד בו תהייה קיימת אפשרות קלה לפענוח ההצפנה.

<u>היערכות המערכת הבנקאית לעידן המחשוב הקוונטי</u>

לאור האמור לעיל, ישנה חשיבות בהיערכות המערכת הבנקאית להתמודדות עם סיכוני אבטחת המידע והסייבר הקשורים למחשוב קוונטי, ובפרט סיכוני פריצת הצפנה בעידן המחשוב הקוונטי, וזאת בהתאמה להתפתחויות הכוללות בתחום זה. בהתאם לקבוע בהוראת ניהול בנקאי תקין 364 "ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר" – (להלן הוראה 364) ובהוראות ניהול בנקאי תקין הרלבנטיות לתחום טכנולוגיית המידע, אבטחת מידע והגנת סייבר שבתוקף למועד זה, הנכם נדרשים לפעול, לכל הפחות, כדלקמן:

6. **העלאת מודעות לנושא בתאגיד הבנקאי, מעקב שוטף אחר התפתחויות בתחום המחשוב הקוואנטי והערכת סיכוני הסייבר הנלווים**

להגדיר וליישם מנגנונים להתעדכנות שוטפת ומתמשכת בהתפתחויות במחשוב הקוונטי, תוך העלאת הידע והמודעות לסיכוני אבטחת המידע והסייבר הרלוונטיים, בקרב כלל הגורמים הרלוונטיים בתאגיד הבנקאי:

6.1. הבאת הנושא לידיעת כלל הגורמים הרלוונטיים בתאגיד הבנקאי, לרבות הדירקטוריון וההנהלה הבכירה, כדי לוודא הכרה של האיומים הפוטנציאליים של טכנולוגיית המחשוב הקוונטי, ושל חשיבות תמיכתם במאמצים למעבר לפתרונות אבטחה של העידן הפוסט קוונטי. הנושא יידון באופן תקופתי, בהתאם להתפתחויות הטכנולוגיות בנושא, אך לפחות אחת לשנתיים, ויכלול סקירה של התפתחויות כלליות בעולם המחשוב הקוונטי בכלל וכאלו המשפיעות על המגזר הבנקאי, וכן, סטאטוס ההיערכות הארגונית לטיפול בסיכוני המחשוב הקוונטי.

6.2. מעקב אחר התפתחויות מתמשכות בתחום המחשוב הקוונטי העלולות להשפיע בהיבטי הגנת סייבר ואבטחת מידע על שירותים פיננסיים, והאפשרות למזער אותם באמצעות התפתחויות בתחום פתרונות אבטחה קוונטיים כגון PQC ו-QKD בהתאם להתפתחויותיהם, לרבות תוך קיום שיח עם גורמי תעשייה רלוונטיים, גופי מחקר, או מרכזי שיתוף ידע.

6.3. שילוב הנושא כחלק מתהליך ניהול סיכוני סייבר מול שרשרת אספקה, תוך קשר שוטף עם צדדי ג' להערכת השפעת ההתפתחות המחשוב הקוואנטי על סיכוני שרשרת האספקה של התאגיד הבנקאי, ודרישה מצדדי ג' רלוונטיים לאמץ פתרונות עמידים כאשר הם יהיו זמינים מסחרית. דגש מיוחד על הקשר עם ספקים של תוכנה וחומרה מהותיים והימנעות מהישענות על ספקים ויצרנים שאינם נערכים לעידן הקוואנטי או שעשויים להוות סיכון טכנולוגי בעידן הזה.

7. **מיפוי וניהול נכסי מידע מוצפנים**

לבצע מיפוי של נכסי מידע מוצפנים[2]. מיפוי זה יאפשר לתאגיד הבנקאי, בין היתר, להבין את מידת חשיפתו לסיכוני אבטחת מידע וסייבר הרלוונטיים לעידן המחשוב הקוואנטי וכן תאפשר לייצר תכנית מעבר לפתרונות הצפנה מותאמים לעידן המחשוב הקוואנטי, כשאלו יהיו זמינים.

המיפוי יכלול, בין היתר:

7.1. מיפוי נכסי מידע מוצפנים במנוחה (Data at rest). תוך התייחסות למאפיינים הבאים:

i. סוג אלגוריתם ההצפנה ואורך המפתח.

ii. פרטי בעל המידע.

iii. מערכות ויישומים אשר עושים שימוש באלגוריתם.

iv. משך הזמן בו המידע המוצפן תקף ונדרש להיות מוצפן, ובפרט תוך התייחסות לסיכון של "Harvest now, decrypt later".

v. רמת רגישות וקריטיות המידע (אישי, רפואי, בטחוני, סודי-עסקי וכדומה).

7.2. מיפוי תהליכים ומערכות אשר עושים שימוש בהצפנה אסימטרית בתנועה (Data in motion) מול גורמים מחוץ לארגון.

7.3. מיפוי מידע מוצפן בהצפנה אסימטרית הנמצא מחוץ לארגון מכל סיבה שהיא (כגון: סביבת ענן אשר הארגון עושה בה שימוש, העברה יזומה, גיבוי, מידע אשר דלף כתוצאה מאירוע סייבר בעבר) עם אותם מאפייני מיפוי שהוגדרו בסעיף 7.1.

8. **היערכות לפיתוח מיומנויות ויכולות להתמודדות עם סיכוני סייבר הקשורים למחשוב קוונטי (בהתאם להתפתחויות בנושא)**

לאור ההערכות בדבר מועד התממשות יכולות פריצת ההצפנה בעידן המחשוב הקוונטי, כמפורט בסעיף 3 לעיל, יש להתחיל בהיערכות לבניית תשתית שתאפשר לתאגיד הבנקאי מוכנות נאותה, המותאמת להתפתחות הנושא (הן בצד התממשות הסיכון והן בצד התפתחויות בתחום המוכנות ההגנתית לקראתו). בנוסף, יש לבחון בצורה מתמשכת את התזמון הנאות לקידום המיומנויות הנדרשות, בהתאם להתפתחויות. היערכות זו צריכה לכלול, בין היתר, התייחסות ובחינת הצורך לפעולה בתחומים הבאים:

8.1. הכשרת עובדים לתהליכי המעבר לפתרונות האבטחה הנדרשים.

8.2. הגדרת המשאבים הנדרשים להקמת סביבת מעבדה וניסוי עבור הפתרונות.

8.3. בחינת תשתית המחשוב הקיימת ותאימותה להפעלה של הצפנה פוסט קוונטית (מהיבטים של כח מחשוב, תמיכת יצרן, גרסאות תוכנה וכדומה).

8.4. היערכות למעבר משימוש באלגוריתמים פגיעים לאלגוריתמים חדשים עמידים, לכשיהיו זמינים, באופן שייצר השפעה מינימלית על מערכות המידע והתשתיות.

8.5. זיהוי מסמכי מדיניות ונהלים שצפויים להיות מושפעים וגיבוש תכנית לעדכונם ותיקופם כדי להבטיח את תאימותם לעידן הפוסט קוונטי ולמעבר לפתרונות אבטחה קוואנטים.

---

[2] יצוין כי מיפוי כאמור הינו חלק מתהליך זיהוי וסיווג של פעילויות, תהליכים ונכסי מידע הנדרש במסגרת הוראת ניהול בנקאי תקין 364 בנושא "ניהול סיכוני טכנולוגיית המידע, אבטחת המידע והגנת הסייבר"

8.6. הגדרת פתרונות חלופיים למקרים בהם לא ניתן להסב מערכות לשימוש בהצפנה פוסט קוונטית או במקרה שהסיכון יתממש מוקדם מהצפוי.

הנכם נדרשים לבנות תכנית היערכות ראשונית, הנותנת מענה לנושאים שפורטו לעיל. תכנית זו תדון בדירקטוריון ובהנהלה.

תכנית היערכות זו תועבר למנהלת אגף טכנולוגיה, חדשנות וסייבר בפיקוח על הבנקים בתוך שנה מיום מכתבי זה. את המיפוי הנדרש בסעיף 7 לעיל, יש להשלים במסגרת היערכות התאגיד הבנקאי לעמידה בדרישות הוראת ניהול בנקאי תקין מס' 364.

בכבוד רב,

דניאל חחיאשוילי

המפקח על הבנקים

העתק:

גב' טל הראל מתתיהו – סגנית המפקח על הבנקים, מנהלת אגף טכנולוגיה, חדשנות וסייבר

גב' איה גל-עד – מנהלת יחידת הסייבר הפיקוחית

גב' ליאורה נבון – מנהלת יחידת טכנולוגיה בבנקאות

סמנכ"ל טכנולוגיות

מנהל סיכונים ראשי

מנהל הגנת הסייבר