היערכות ל-Post Quantum Cryptography

06/03/2025
ו' אדר תשפ"ה

[תקציר]

- מחשבים קוונטיים מסוגלים לפצח חלק מאלגוריתמי ההצפנה המצויים בשימוש כיום (בעיקר אלגוריתמים המשמשים להצפנה א-סימטרית).
- לאור התחזקותם של מחשבים אלו בשנים האחרונות, ולמרות שטרם זוהתה יכולת פומבית לבצע זאת באופן אפקטיבי, מומלץ להיערך כבר כעת להטמעת פתרונות אבטחה חסינים למחשוב קוונטי בארגון.

[פרטים]

- מחשוב קוונטי הינו בעל יכולת לפיצוח אלגוריתמי הצפנה פופולריים מסוימים, בעיקר אלו העוסקים בהצפנה א-סימטרית באמצעות:
  - Factorization (RSA)
  - Discrete Logarithms (Diffie-Hellman)
  - Elliptic Curve Discrete Logarithms
- אמנם טרם הודגמה יכולת פומבית אפקטיבית לפיצוח אלגוריתמים אלו, אך התשתית התיאורטית קיימת, והמחשוב הקוונטי מתחזק ביכולותיו באופן מובהק לאורך זמן. איש אינו יודע להעריך במדויק מתי יושגו יכולות אלו וייתכנו פריצות דרך שיאיצו התהליך בצורה משמעותית.

פעולות מידיות לביצוע:

- מינוי גורם ניהולי בארגון כאחראי לנושא ניהול סיכונים בהיבטי מחשוב קוונטי ויישום תוכנית לסגירת פערי אבטחה.
- לימוד תחום ה-PQC, ופתרונות/מוצרים אפשריים למימוש חסינות, ויצירת תוכנית עבודה להוספת אלגוריתמים חסינים למערכות הארגוניות.
- בחינת טכנולוגיות אבטחה חלופיות המציעות חוסן בפני מחשוב קוונטי, דוגמת QKD.
- שילוב העיקרון של Crypto Agility בתהליכי פיתוח מאובטח, התקשרויות ורכש.
- תיעדוף הפעילות בהתאם לקריטיות/סיווג המערכות והמידע.

⚠

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.

המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

- תשומת לב שאלגוריתמים אלו משמשים במספר רב של מערכות אבטחה והצפנה, כולל אלגוריתם TLS הפופולרי מאד לגישה מוצפנת לאתרים, SSLVPN, API וכד' (בדגש על השלב בפרוטוקול העוסק בהחלפת מפתחות הצפנה).

- להלן מספר סיכונים הנובעים ממחשוב קוונטי אפקטיבי:
- זיוף חתימות דיגיטליות דוגמת אלו המשמשות לוידוא אותנטיות ומהימנות של רכיבי תוכנה, לרבות Firmware.
- זיוף חתימות דיגיטליות על מסמכים הניתנים להמרה מידית לכסף כגון תעודות בעלות על נכסים פיננסיים נזילים, לרבות מטבעות דיגיטליים.

- בנושא החתימות, הבעיה עלולה להתממש במיוחד בפלטפורמות שבהן לא ניתן להחליף בקלות את האלגוריתמים המשמשים לבדיקת החתימה. לדוגמה – מערכות ICS/SCADA ורכיבי מכשור רפואי (IoMT) שעבורן מבוצע רכש בתדירות נמוכה מאד.
- הקלטת תעבורה כעת ופיצוח שלה בעתיד - אחד הסיכונים הוא יריבים שמקליטים תעבורה המוצפנת בהצפנה שאינה חסינה לפיצוח קוונטי, ויפצחו אותה לאחר השגת יכולת זו - (Harvest Now, Decrypt Later). כמובן שהפגיעות רלוונטית אם הנתונים יהיו עדיין רגישים ו/או מסווגים. קיים שוני מובנה בין נתונים שרגישותם גבוהה לאורך זמן כגון פרטים רפואיים על אנשים ספציפיים, לעומת נתונים שלאחר זמן ממילא הופכים פומביים כגון הנפקה מתוכננת שיוצאת אל הפועל בטווח זמן מוגדר. הקלטת התעבורה ייתכן והינה סיכון אקטואלי כבר כעת.

[דרכי התמודדות]

- מומלץ למנות גורם ארגוני כאחראי ללימוד וקידום הנושא, איתור המערכות הרלוונטיות הכוללות רכיבים שאינם חסינים, והכנת תוכנית להוספת האלגוריתמים החסינים (בשלב ראשון במקביל לאלגוריתמים קיימים) למערכות הרלוונטיות, תוך כדי תיעדוף בהתאם לרמת הרגישות והסיווג של המערכת/המידע.
- מכון התקנים האמריקאי (NIST) יזם תחרות למציאת אלגוריתמי הצפנה חסינים למחשוב קוונטי (Post Quantum Cryptography Algorithms). בשנה שעברה הוכרזו 3 הזוכים הראשונים בתחרות זו, ואושרו כתקנים פדרליים (FIPS). פרטים בקישורים 3 עד 5. מומלץ מאד להשתמש באלגוריתמים אלו ובנוספים שיאושרו בעתיד כבסיס לפתרונות חסינים למחשוב קוונטי.
- יש להדגיש בהיערכות ל-PQC מענה מתאים להצפנה חסינה במערכות ענן ובמערכות ספקים חיצוניים לארגון דוגמת חברות אירוח (Hosting Providers).
- מומלץ לבחון גם טכנולוגיות אבטחה חלופיות המציעות חוסן בפני מחשוב קוונטי, דוגמת QKD.
- מומלץ לשלב את העיקרון של Crypto Agility (יכולת החלפה מהירה בין אלגוריתמים ופרוטוקולים) בתהליך פיתוח מאובטח, בין אם הפיתוח נעשה בחצרות הארגון, במסגרת מיקור חוץ או בעת רכש פתרונות מדף.
- מומלץ לבחון באופן עתי פרסומים אודות יכולות חדשות של מחשוב קוונטי, עבור טיוב תהליך ניהול הסיכונים הארגוני (ERM).
- במערכות בעלות הצפנה סימטרית, מומלץ שימוש באלגוריתם AES256, הנחשב בשלב זה כחסין.
- עבור פרוטוקולים ואלגוריתמים העושים שימוש ב-Hash, אפשר להמשיך ולהשתמש ב-SHA-256 הנחשב בשלב זה כחסין, אך מומלץ לבחון שימוש ב-SHA-384 או SHA-512, אם המערכות הרלוונטיות תומכות בכך.
- מומלץ לבחון את המשמעויות התפעוליות של המעבר לשימוש ב-PQC דוגמת שמירה על רמת ביצועים התואמת לדרישות היישום.

[מקורות]

1. https://www.cisa.gov/quantum
2. https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF
3. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
4. https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based
5. https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

6. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
7. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/
8. https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/ipd