מבט על

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

"מוכנות קוונטית" בתשתיות הלאומיות: מהצהרות ספקים להוכחות ברמת השירות

אופיר יוסף ונדב כהן[1] | גיליון 2219 | 15 בנובמבר 2026

יריבים מדינתיים יכולים כבר היום ליירט תקשורת מוצפנת ולשמור אותה עד שיעמוד לרשותם מחשב קוונטי שיאפשר לפענח אותה. משום כך, ההיערכות לעידן הפוסט־קוונטי היא סוגיה של ביטחון לאומי כבר בהווה. תקני הקריפטוגרפיה הפוסט־קוונטית הראשונים פורסמו בשנת 2024, ובעלות בריתה של ישראל הציבו יעדים וקבעו אבני דרך למעבר לתקנים אלה בשנים 2030 עד 2035. ואולם רכישת מוצר "עמיד קוונטית" אינה מבטיחה שהשירות החיוני שבו הוא משולב יעבור את השינוי בבטחה. האתגר המרכזי של המדינה אינו רק החלפת אלגוריתמים, אלא הוכחה שהשירותים החיוניים, ובהם תקשורת, בקרה ועדכוני תוכנה, ימשיכו לפעול בבטחה גם לאחר השינוי, תוך שמירה על אבטחה ורציפות תפקודית. מאמר זה מציע למדוד מוכנות ברמת השירות באמצעות ראיות מבדיקות שילוב, ולהגדיר מראש את אופן ההתאוששות מתקלות ואת הסמכות לאישור סיכונים לאורך המעבר. ההמלצות שלהלן מיועדות לקובעי מדיניות ולרגולטורים, שביכולתם לקבוע דרישות אחידות ולתעדף את השירותים החיוניים ביותר.

האיום כבר כאן: "אסוף עכשיו, פענח אחר כך"

מנגנונים נפוצים להחלפת מפתחות ולחתימות דיגיטליות נשענים כיום על בעיות מתמטיות שמחשב קוונטי חזק דיו צפוי לפתור ביעילות. אמנם מועד הופעתו של מחשב כזה אינו ידוע, אך הסיכון מתחיל מוקדם יותר: יריב יכול לאסוף כיום תעבורה מוצפנת ולפענח אותה בעתיד. גישה זו מכונה "אסוף עכשיו, פענח אחר כך" (Harvest Now, Decrypt Later), והיא רלוונטית במיוחד למידע מודיעיני, לתקשורת מדינית, לסודות מסחריים ולמידע אישי שחייב להישאר חסוי לאורך שנים. ישראל היא יעד מתמשך לריגול סייבר של גורמים מדינתיים, ותעבורה שנאספה בעבר ובהווה עלולה להפוך בעתיד לנכס מודיעיני בידי יריביה. לכן משך חיי המידע מחייב היערכות מוקדמת ומדורגת. המשמעות היא שקביעת סדרי העדיפויות צריכה להתחשב בתקופת הסודיות הנדרשת גם לאחר סיום השימוש השוטף במידע.

סיכון עתידי שני נוגע גם לחתימות דיגיטליות, המשמשות לאימות זהותן של מערכות ולאישור עדכוני תוכנה וקושחה לפני התקנתם. יריב שיוכל לזייף חתימות יוכל להחדיר עדכון זדוני לרכיב בקרה בתשתית קריטית או להתחזות למערכת לגיטימית, ולכן יש חשיבות מיוחדת להגנה על שרשראות עדכון של מערכות בקרה ופלטפורמות שצפויות לפעול שנים רבות.

שני הסיכונים שונים בלוח הזמנים שלהם. חשיפת מידע היא סיכון של ההווה, שכן מה שנאסף היום לא יוגן בדיעבד. זיוף חתימות יתאפשר רק כאשר יעמוד לרשות היריב מחשב קוונטי, אך ציוד שמאמת עדכונים באמצעות מפתח קלאסי שאי אפשר להחליף יישאר פגיע לאורך כל חייו. לכן, בהגנה על מידע נקבעת הדחיפות לפי משך הסודיות שלו, ובחתימות לפי משך החיים של הציוד שנרכש היום.

---

[1] אופיר יוסף עומד בראש התוכנית לאבטחת סייבר במכללה האקדמית תל אביב־יפו ותלמיד לתואר דוקטור בתקשורת קוונטית באוניברסיטת חיפה. ד"ר נדב כהן הוא חוקר בכיר אורח במכון למחקרי ביטחון לאומי.

המכון האמריקאי לתקנים וטכנולוגיה (NIST) פרסם באוגוסט 2024 שלושה תקנים ראשונים לקריפטוגרפיה פוסט־קוונטית (PQC), הכוללים מנגנוני ביסוס מפתחות וחתימות דיגיטליות, וקרא לארגונים להתחיל במעבר מיד (יצוין כי מאמר זה מתמקד במעבר ל-PQC בנפרד מהפצת מפתחות קוונטית – QKD, המחייבת תשתית פיזיקלית ייעודית). ארצות הברית, בריטניה והאיחוד האירופי פרסמו יעדים, המלצות והנחיות הכוללים גם אבני דרך מדורגות עד 2035. חלק מהדרישות שפורסמו מוקדמות יותר, ואף מחייבות: לפי הנחיות הסוכנות לביטחון לאומי האמריקאית (NSA), רכש חדש של מערכות ביטחון לאומי יידרש לעמוד באלגוריתמים העמידים החל מינואר 2027, ומפת הדרכים האירופית ממליצה על סוף 2030 כמועד להשלמת המעבר בשימושים בסיכון גבוה. ללוחות זמנים אלה עשויה להיות השפעה על שיתוף הפעולה הביטחוני, על התאימות הבין־מערכתית ועל דרישות המופנות ליצואנים ישראלים. לפיכך, בעת גיבוש יעדים בישראל ראוי להבחין בין דרישות מחייבות של שותפים לבין אבני דרך המשמשות לתכנון ולהיערכות.

בישראל כבר ננקטו צעדים ראשוניים, ובהם מכתב הפיקוח על הבנקים מינואר 2025, הדורש מהבנקים להיערך ולמפות נכסים מוצפנים, והנחיית מערך הדיגיטל הלאומי מ-2025 למיפוי נכסים מוצפנים במשרדי הממשלה. מיפוי כזה מספק תמונת מצב של רכיבים, אלגוריתמים וספקים, והוא מאפשר לקבוע את היקף המעבר הנדרש, אך אינו מלמד אם השירות שנשען על הרכיבים יכול לעבור את השינוי. השלב הבא של מדיניות לאומית צריך להתמקד בהוכחת המוכנות של השירותים הנשענים על אותם רכיבים. מעבר הדרגתי ממיפוי לבדיקות שילוב יאפשר להשתמש בתוצרי המיפוי לצורך הגדרת תחומי אחריות ויצירת בסיס השוואתי בין מגזרים.

אתגר השילוב בין המערכות

ספק יכול ליישם במוצר שלו את אלגוריתם התוכנה הנכון, אך הראיות שהוא מספק נעצרות לרוב בגבולות המוצר. נדרשת בדיקה שתראה כיצד המוצר פועל כחלק מהשירות החיוני כולו. מערכות בקרה, ציוד תקשורת ותיק ושירותים חיצוניים עשויים להגיב באופן שונה למפתחות, לחתימות ולהודעות תקשורת גדולות יותר. מסיבה זו, ראיות לביצועי מוצר מסוים צריכות להשתלב בבדיקות של השירות מקצה לקצה, בתצורה ובעומס המייצגים את פעילותו. יש לתת תשומת לב לממשקים בין ציוד של יצרנים שונים, לתהליכי אימות ולהשפעות האפשריות על זמני תגובה וזמינות.

חברת Cloudflare תיארה בשנת 2025 מקרים שבהם הודעות גדולות יותר במהלך הקמת חיבור מאובטח חשפו הנחות מוקדמות של ציוד ותוכנות בדרך התקשורת. חלק מהחיבורים נותקו אף שהאלגוריתם הקריפטוגרפי עצמו פעל כמתוכנן, והמקרה המחיש את חשיבותן של בדיקות תאימות בין רכיבים. עבור תשתיות לאומיות יש לבדוק גם מערכות בקרה תעשייתיות, ציוד משובץ, קישורים בעלי רוחב פס מוגבל ושרשראות אספקה מורכבות. במערכות אלה השפעה קטנה על זמני ההקמה או על גודל ההודעות עשויה לשנות את אופן הפעולה של השירות כולו.

בישראל התלות בספקי תקשורת ומחשוב בינלאומיים מחייבת גם תיאום בין מדיניות הרכש לבין מועדי הזמינות של פתרונות משודרגים. מסגרת בדיקות משותפת תאפשר למדינה לזהות תלויות חוצות מגזרים (קשרים והשפעות הדדיות בין מערכות, רכיבים וספקים), ולקבוע סדרי עדיפויות על בסיס נתונים אחידים. תשתית ידע משותפת תוכל גם לסייע למפעילים להבין אילו שילובים טכנולוגיים כבר נבחנו ומהן ההגבלות שנצפו בבדיקות.

מוכנות נמדדת ברמת השירות

נבחן לדוגמא שירות גישה מרחוק ובקרה של מפעיל תשתית קריטית, כגון חברת חשמל המתפעלת תחנות משנה. שער תקשורת חדש עשוי להגן על חיבור אחד באמצעות הצפנה פוסט־קוונטית, בעוד חיבורים אחרים או מנגנוני חתימה עדיין נשענים על פתרונות קיימים. בדיקה מוצלחת של השער היא ראיה מועילה, אך אין בה הצדקה להגדיר את השירות כולו כ"מוכן קוונטית". לכן הוכחת מוכנות השירות מחייבת בחינה של מכלול החיבורים, אמצעי האימות ומנגנוני ההתאוששות שעליהם נשענת אספקת השירות.

דוגמא נוספת היא שרשרת העדכונים של פלטפורמות ומערכות נשק, שבה חתימות דיגיטליות מאמתות תוכנה וקושחה לפני התקנתן ברכיבים קריטיים. אם המעבר יכלול רק את ערוצי ההצפנה ולא את מנגנון החתימה, הפלטפורמה תיוותר פגיעה לזיוף עדכונים לאורך כל שנות שירותה, ומשום כך ההנחיות האמריקאיות מקדימות את המעבר בחתימות על קושחה. בדיקה ברמת השירות תבחן את מסלול העדכון כולו, ממקור התוכנה ועד אימותה והתקנתה ברכיב הקצה. גישה זו מאפשרת לקובעי המדיניות להגדיר מוכנות ביחס לשירות ולמחזור החיים שלו, ולא ביחס לרכיב בודד.

משתי הדוגמאות עולה מהי ראיה למוכנות ברמת השירות. ראיה כזו מתחילה בהגדרת גבולות השירות ותלויותיו, ומפרטת את גרסאות הרכיבים ואת התצורות שנבדקו בפועל. היא כוללת מדידה של תאימות, זמינות, שיהוי ורציפות, לצד רמת ההגנה הקריפטוגרפית, בעומסים המייצגים את אופי השירות. תוקפה מוגבל: עדכון מהותי או החלפת ספק מחייבים בדיקה מחודשת. תמונת מוכנות הבנויה מראיות כאלה מבחינה בין מוכנות שכבר הוכחה לבין התחייבות של ספק לשדרוג עתידי, ומאפשרת לעקוב אחר שירותים שנבדקו, תלויות שנותרו פתוחות ואבני הדרך הבאות. על בסיס זה אפשר לייחס לכל שירות רמת מוכנות, בהתאם להיקף הבדיקות שהושלמו ולתלויות שעוד דורשות טיפול. ספירת מוצרים ששודרגו, לעומת זאת, עלולה להסתיר תלות קריטית שלא טופלה.

התאוששות היא החלטה ביטחונית

מעבר מדורג לקריפטוגרפיה פוסט־קוונטית מחייב לתכנן מראש גם את תנאי ההתאוששות במקרה של תקלה בשלב הפריסה. חזרה זמנית לתצורה קודמת עשויה לשקם את זמינות השירות, אך היא מסירה את ההגנה הפוסט־קוונטית: תעבורה שתיורט בחלון הזמן הזה תישאר חשופה לפענוח עתידי גם לאחר שההגנה תוחזר, כך שחזרה זמנית עלולה להפוך לחשיפה קבועה. נוסף על כך, תוקף עשוי לנסות לגרום לכשל מכוון המעודד מעבר לתצורת הגנה חלשה יותר, תרחיש המכונה מתקפת שנמוך (downgrade attack). **מנגנוני החזרה לאחור הופכים בכך לחלק ממשטח התקיפה של המערכת.**

התאוששות מתקלה כרוכה אפוא בהכרעה בין סודיות המידע, זמינות השירות ובטיחות התשתית, ומשקלם היחסי משתנה ממגזר למגזר. חזרה זמנית לתצורה קודמת היא חריגה ביטחונית, ואת מאפייניה אפשר להגדיר: מי אישר אותה, לכמה זמן, באיזה ניטור, וכיצד תועדה. חריגה שאין לה אחד מאלה הופכת בפועל למצב קבע. הסיכון החמור ביותר טמון דווקא בצעדים שנועדו להחזיר את הקישוריות: נטרול שקט של מנגנוני האימות חושף את השירות לזיוף ולהתחזות, ולא רק לחשיפת מידע. גם ההכרעה בין המשך פעולה בהגנה מופחתת לבין השבתת השירות היא בחירה בין שני סיכונים ביטחוניים שונים. לספק אין את התמונה המלאה הנדרשת לו, ובמערכות ביטחון לאומי היא נוגעת לדרג פיקודי או ניהולי. כאשר כללי ההכרעה נקבעים מראש, ההחלטה בשעת תקלה נשענת על אחריות ברורה ועל מסלול ידוע לחזרה להגנה המתוכננת. כאשר הם נקבעים בזמן אמת, היא נשענת על לחץ הרגע.

השלכות על חברות ומפעילי תשתיות

ליישום מדיניות כזו יש השפעה ישירה על תכנון ההשקעות של חברות, על רציפות אספקת השירות ועל חוזי ההתקשרות עם ספקים. הגדרת דרישות מדורגות וידועות מראש תאפשר למפעילי התשתיות לתאם מועדי החלפת ציוד, להיערך לעלויות שדרוג ולהציג חלופות לטיפול בתלויות מרכזיות. מסגרת רגולטורית המבוססת על בדיקות משותפות ועל דרישות ראיה אחידות יכולה לצמצם כפילויות וליצור ודאות בתכנון לטווח ארוך. עבור חברות הפועלות במספר מגזרים, עקביות בדרישות ובאופן הצגת התוצאות עשויה לייעל את ההיערכות ואת חלוקת ההשקעות.

משמעויות והמלצות למדיניות בישראל

הדרישה לראיות אינה טיעון בעד המתנה. מיפוי תשתיות ובדיקות שילוב הם תהליכים ממושכים, ולכן התחלה מוקדמת מאפשרת למדינה לתכנן השקעות ולצמצם תלויות בהדרגה. ההמלצות שלהלן מתחלקות לשני מעגלים. המעגל הראשון נמצא בשליטת המדינה: הגדרת מוכנות, תיעדוף וכללים לחזרה לאחור. המעגל השני תלוי בספקים בינלאומיים, ובו טמונה המשמעות הייחודית לישראל: קצב המעבר של מערכות ישראליות ייקבע במידה רבה לפי מפות הדרכים של ספקים זרים, שסביר שיתעדפו את דרישות השווקים הגדולים, ובראשן דרישות הרכש של ממשלת ארצות הברית ומפת הדרכים האירופית. ארגון ישראלי בודד יתקשה להשפיע על סדרי עדיפויות אלה, אך המדינה יכולה להגדיל את השפעתה באמצעות רכש מתואם, דרישות התואמות את תקני בעלות הברית ובדיקות משותפות.

• **אמות מידה למוכנות פוסט־קוונטית:** מומלץ כי מערך הסייבר הלאומי והרגולטורים המגזריים, כל גוף בהתאם לסמכויותיו, יגבשו אמות מידה לבחינת מוכנות פוסט־קוונטית ברמת השירות. אמות המידה יגדירו ראיות נדרשות, בדיקות תאימות, תוקף האישור וחובת הערכה מחודשת לאחר שינוי מהותי בשירות. יש להתאים את עומק הבדיקות ואת מחזורי הדיווח לרמת החשיבות של השירות ולמאפייני ההפעלה שלו. במסגרת זו יש לבחון את הכיסוי שנותנות ההנחיות הקיימות בכל המגזרים החיוניים, ובהם התשתיות הקריטיות ומערכת הביטחון, ולוודא שהן כוללות בחינת מוכנות ברמת השירות, ולא רק מיפוי. לצד זאת, מומלץ לקבוע מתכונת דיווח מדידה הכוללת שיעור שירותים קריטיים שנבדקו, תלויות מהותיות

ותוכניות התאוששות מאושרות. ריכוז הנתונים במסגרת מדידה משותפת יאפשר לגורמי הפיקוח לזהות חסמים שחוזרים במספר ארגונים ולקדם מענה רוחבי.

• **תיעדוף לאומי:** מומלץ לקבוע תיעדוף לאומי המבחין בין שני סוגי סיכון: בהגנה על סודיות, לפי משך הסודיות הנדרש למידע; בהגנה על אימות ועדכונים, לפי משך החיים הצפוי של הציוד והיכולת להחליף בו מפתחות אמון. בשני המקרים יש להביא בחשבון את חיוניות השירות. תיעדוף כזה יאפשר להפנות משאבים לשירותים שבהם שילוב של מידע רגיש, ציוד ותיק ותלות בספקים מצדיק התחלה מוקדמת. מפת הדרכים האירופית, למשל, מגדירה כשימוש בסיכון גבוה כל שימוש שבו חשיפת המידע גם בעוד עשר שנים ויותר תגרום נזק משמעותי.

• **מנגנוני חזרה לאחור:** מומלץ שהרגולטורים המוסמכים יקבעו כללים להפעלה זמנית בתצורה קודמת, שיכללו גורם מאשר, משך חריגה וניטור מתאים, וכן חובה לשמר את מנגנוני האימות בכל תרחיש. במערכות ביטחון לאומי יש להגדיר מראש את הדרג הפיקודי או הניהולי המוסמך להכריע בין המשך פעולה בהגנה מופחתת לבין השבתת השירות.

• **רכש מתואם ודרישות לשדרוג:** מומלץ שמשרד הביטחון וגופי הרכש הממשלתיים, בתיאום עם הרגולטורים של התשתיות הקריטיות, יגבשו דרישות קבלה אחידות התואמות את דרישות בעלות הברית, כך שהספקים יפגשו דרישה ישראלית אחת ומוכרת. דרישות הקבלה יכללו ראיות מוכחות לפעולה הדדית, לביצועים ולתוכנית התאוששות. במסמכי ההתקשרות יש להבחין בין יכולת זמינה שכבר נבדקה לבין יכולת עתידית, ולקבוע מועד מחייב לאספקת שדרוג פוסט־קוונטי, המותאם לאבני הדרך של בעלות הברית. ניתן גם להגדיר מראש אחריות ספק למסירת תוצאות בדיקה ולתיאום עדכונים נדרשים עם יצרנים נוספים בסביבת השירות.

• **סביבת בדיקות משותפת:** מומלץ לקדם סביבת בדיקות משותפת למגזרים חיוניים, שתאפשר לבחון תאימות בין פתרונות חדשים, ציוד ותיק ומערכות בקרה. הסביבה תשמש גם ערוץ משותף מול ספקים להעברת ממצאים ודרישות תיקון, ותאפשר לזהות מוקדם מערכות שספקיהן לא יספקו שדרוג בזמן, כדי להחליט אם להחליף אותן, לבודד אותן או לפתח חלופה מקומית. במסגרת זו ראוי לשלב גופי תקינה, גופי רכש ומפעילי תשתיות, ולשתף בין המגזרים ממצאים שניתן לפרסמם.

סיכום

הסיכון הקוונטי מחייב כבר היום החלטות על שירותים ומידע שימשיכו להיות חיוניים ורגישים לאורך שנים. נקודת המבחן למדיניות בישראל היא היכולת להציג ראיות לכך שהשירות כולו מוכן לשינוי, לרבות התלויות, הביצועים ודרכי ההתאוששות. מכאן נגזרת השאלה שכל דיון על התקדמות המעבר צריך להעמיד: אילו שירותים חיוניים כבר הוכיחו מוכנות, אילו פערים נותרו, ומי אחראי לסגירתם ולסיכון שנותר עד אז. תשובה מגובה בראיות לשאלה זו משמעותית יותר מכל רשימת מוצרים הנושאים את התווית "מוכן קוונטית".

עורכי הסדרה: ענת קורץ, רינת חרש ואלדד שביט.