אבטחה של שרשראות אספקה קריטיות: הזדמנויות אסטרטגיות לקידום היוזמה להסמכה בין־לאומית של מוצרי סייבר

פול סטוקטון

סין, רוסיה ויריבים פוטנציאליים אחרים של ארצות הברית מגבירים את מאמציהם לפגוע בשרשראות האספקה עליהן מסתמכים רשתות חשמל וענפי תשתית אחרים. כבר כיום מתקיימות יוזמות חשובות לחיזוק ניהול הסיכונים בשרשרת האספקה, אולם למרות האמצעים שננקטו, קהילת המודיעין האמריקאית סבורה שההיקף והתחכום ההולכים וגדלים של ההתקפות על שרשרת האספקה "מציבים חלקים שלמים של הממשל והכלכלה שלנו בסיכון".[1] אתגרים דומים עומדים בפני ישראל, בריטניה ושותפות ביטחוניות אחרות של ארצות הברית. אין כיום תהליך מקיף, המקודם על ידי בעלי עניין, שיבטיח לבעלי תשתיות ולמפעיליהן שמוצרי חומרה ותוכנה חיוניים לא ייחשפו לתוכנות זדוניות או לאמצעי ניצול עוינים אחרים, ולו ברמה הבסיסית ביותר. תהליך הסמכה יתרום רבות לחוסנו של מרחב הסייבר, במיוחד אם גופים ממשלתיים יוכלו לספק מידע על איומים או לתמוך ביוזמה כזאת בדרכים אחרות.

היוזמה להסמכה בין־לאומית של מוצרי סייבר (Cyber Product International Certification – CPIC), שהעלתה המועצה לביטחון תשתיות החשמל (EIS Council) תסייע במתן מענה לאתגרים אלה. היוזמה תוכל לתרום עוד יותר לחוסן התשתיות, אם היא תכלול אמצעים להסמכת מוצרים כבטוחים מפני הפרעה אלקטרומגנטית מכֻוונת (IEMI).

מילות מפתח: סייבר, איומים, שרשרת אספקה, IT, OT, אנרגיה, CPIC

ד"ר פול סטוקטון הוא מנכ"ל Sonecon ולשעבר עוזר שר ההגנה של ארצות הברית לענייני ביטחון המולדת ונושאי הביטחון ביבשת אמריקה. רוברט דנאבורג, אנליסט בכיר ב"סונקון", ערך את המחקר לצורך מאמר זה. הממצאים וההמלצות הם על דעת המחבר בלבד ואינם משקפים בהכרח את עמדות משרד ההגנה האמריקאי או כל גוף ממשלתי אחר.

1 "Supply Chain Risk Management: Intelligence.Gov Background Paper", *National Counterintelligence and Security Center*, March 2017, p. 2, https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf.

היקף האיום וחומרתו

הסיכונים הנשקפים מתוכנות ומחומרות רוסיות וסיניות לחוסן התשתיות (ולביטחון הלאומי בכללותו) זכו בחודשים האחרונים לבחינה קפדנית על ידי הממשל האמריקאי.[2] חלק מהמוצרים הנמכרים על ידי חברות כמו ZTE, Huawei או Kaspersky Labs מהווים רק את "קצה הקרחון" של מאמצים עוינים לחדור לשרשראות אספקה ולהשחית אותן כדי לאפשר ליריבים פוטנציאליים לבסס נוכחות מתמשכת ברשתות בארצות הברית ואצל שותפותיה לדרך.

המסמך "מדיניות אבטחת הסייבר" של המשרד לביטחון המולדת, ממאי 2018, מזהיר כי הקישוריות ההולכת וגוברת בין ענפי התשתית והשירותים המודרניים חושפת אותם לפגיעויות חדשות ו"פותחת פתח לתוצאות הרות אסון כתוצאה מאירועי סייבר".[3] אחת הסיבות לכך היא ההסתמכות הגוברת על שרשראות אספקה שהופכות גלובליות, והמספר ההולך וגדל במהירות של מכשירים המתחברים לרשת האינטרנט. מגמות אלו עתידות להעצים את האתגרים הכרוכים בניהול סיכונים בשרשרת האספקה, וזאת מבלי להמעיט בערכם של מאמצי החדשנות השמים דגש על שיפור האבטחה והחוסן של תחומים אלה.[4] זאת ועוד, למרות המערך הנוכחי של תוכניות במגזר הציבורי והפרטי, שנועדו לצמצם ולמנוע איומים על שרשרת האספקה, "ההתפתחות של איומים מכַוונים, מתוחכמים ומרובי פנים מאיימת לגבור על אמצעי המנע שאנו נוקטים".[5] בהתחשב בסביבת האיומים הנוכחית ובמגמות בשרשרת האספקה הגלובלית, "ניהול סיכונים בשרשרת האספקה בסייבר אינו שאלה של בחירה",[6] אלא חובה.

גורמים עוינים אמנם אינם יכולים להחדיר מרחוק פגיעויות אלקטרומגנטיות, או לנצל באותה דרך פגיעויות קיימות, כפי שהם יכולים לעשות באמצעות נשק הסייבר, ואף על פי כן, קיימים כמה סיכונים גם בדרך פעולה זאת. לדוגמה, גורמים

2 ראו, לדוגמה: Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats", *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats; Joseph Marks, "Chinese Telecoms Could Join Kaspersky on Government Wide Banned List", *Nextgov*, February 13, 2018, http://www.nextgov.com/cybersecurity/2018/02/chinese-telecoms-could-join-kaspersky-governmentwide-banned-list/145960.

3 "Cybersecurity Strategy", *Department of Homeland Security*, May 15, 2018, p. 1, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

4 שם, עמ' 22־23.

5 "Supply Chain Risk Management: Intelligence.Gov Background Paper", p. 2.

6 "Best Practices in Cyber Supply Chain Risk Management", *National Institute of Standards and Technology*, n. d., p. 1, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Business-Case.pdf.

עוינים יכולים להחדיר לשרשרת האספקה של התשתיות רכיבים מזויפים או רגישים במיוחד לאיומים אלקטרומגנטיים. גורמים כאלה גם יכולים לנסות לנצל פגיעויות אלקטרומגנטיות ידועות בתוך רכיבים המצויים בפריסה רחבה, ובכך להגדיל את הנזק הפוטנציאלי שייגרם ממתקפה אלקטרומגנטית.

האיומים על שרשראות אספקה עולמיות הם מרובי ממדים, ויש מספר גורמים ומגמות המעצימים אותם. התגברות האיומים על שרשראות האספקה מחייבת התמודדות איתם, אך גם מציבה מספר אתגרים בפני אלה המנסים לצמצמם.

מספר הולך וגובר של כיווני איום

גורמים עוינים ממשיכים לחפש בהתמדה אחר דרכים חדשות לפגוע, לשבש ולנצל שרשראות אספקה. ואכן, המורכבות הגלובלית הגוברת של שרשראות אלו והתעצמות האיומים מצד גורמים עוינים הכפילו את הסיכון שספקים יכניסו למערכת או לרשת, במתכוון או שלא במתכוון, חומרה, תוכנה או קושחה ששובשו.[7] יוזמות חדשות בתחום מערכות מידע (IT), כמו מחשוב בענן או "התקנים מחוברים" (IoT), תרמו גם הן להרחבת תחומי החשיפה למתקפות סייבר על שרשראות האספקה,[8] הגדילו את מספר נקודות החדירה העשויות לשמש מטרה לגורמים עוינים ויצרו אתגרים נוספים עבור בעלי התשתיות ומפעיליהן, המבקשים לאבטח את שרשראות האספקה שלהם.

גורמים עוינים תרים אחר הזדמנויות לשבש כל נקודה אפשרית בשרשראות האספקה הגלובליות התומכות בתשתיות בארצות הברית. סיכונים קיימים בכל שלב – בתכנון, בייצור, באינטגרציה, בפריסה ובתחזוקה[9] – וגורמים עוינים עלולים להחדיר פגיעויות בשרשרת האספקה עצמה, או לנצל את הפוטנציאל של פגיעויות קיימות שעדיין לא טופלו על ידי מומחי האבטחה.[10]

גם אם פגיעויות אינן קיימות בפיתוח הראשוני, גורמים עוינים יכולים להחדירן בכל שלב במחזור החיים של המערכת.[11] אפשרויות אלו כוללות עדכוני תוכנה או

7 שם, עמ' 1.

8 Jon Oltsik, "Protecting the Cyber Supply Chain", *Cipher Brief*, December 6, 2015, https://www.thecipherbrief.com/article/protecting-cyber-supply-chain.

9 "Supply Chain Risk Management: A Framework for Assessing Risk", *National Counterintelligence and Security Center*, February 2013, p. 2, https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf.

10 "Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks", *Public-Private Analytic Exchange Program*, 2016, p. 4, https://www.dni.gov/files/PE/Documents/Electricity-Infrastructure-Summary.pdf.

11 "Task Force on Cyber Supply Chain", *Defense Science Board*, February 2017, p. 1, https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

"טלאים" שנועדו לטפל בפגיעות של מערכות מחשוב (IT) ומערכות בקרה (OT). בתרחיש כזה מחדירים למערכת קוד זדוני או קושחה ממאירה שנועדה להפעלה במועד מאוחר יותר.[12] התדירות שבה מפעילי מערכות מיישמים עדכוני תוכנה יוצרת הזדמנויות רבות לגורמים עוינים לחבל באותן מערכות, גם זמן רב לאחר שלב התכנון.

גורמים עוינים גם עלולים לחבל בחומרה שחברות תשתית מתקינות במערכת ההפעלה שלהן. לדוגמה, דוח של המועצה למדע הביטחון (Defense Science Board) ציין מספר רב של פגיעויות פוטנציאליות ברכיבי מיקרואלקטרוניקה שבשרשרת האספקה. הדוח התמקד אמנם במערכות נשק, אך רכיבי מיקרואלקטרוניקה דומים נמצאים בשכיחות גוברת בכל ענף תשתית. רכיבי מיקרואלקטרוניקה כאלה "כוללים באופן בלתי נמנע פגיעויות בלתי נראות לעין", שניתן יהיה לגלותן, אם בכלל, רק שנים לאחר שהמוצר נכנס לשירות. ההשפעות האפשריות שלהן נעות בין פגיעה בפעולת המערכת ובין כשל מלא שלה.[13]

עדכוני תוכנה מועדים במיוחד לפגיעות עוינות, שמטרתן היא להשיג גישה ארוכת טווח לרשתות המודיעין הנגדי, מתוכן יוכלו אותם גורמים עוינים לשגר בשלב מאוחר יותר מתקפות לשיבוש פעולות בתחום התשתיות. כך, למשל, מבצע Dragonfly הרוסי התמקד תחילה "בארגונים פריפריאליים, כגון ספקי צד שלישי, שהרשתות שלהם היו פחות מאובטחות", כשהוא משתמש בהם כנקודות מוצא לפגיעה בקורבנות המיועדים.[14] חברת Dragos – חברת אבטחת סייבר במערכות בקרה תעשייתיות (ICS) – שרטטה לאחרונה פרופיל של גורם מאיים ששם על הכוונת שלו רשתות ICS, בין היתר באמצעות מתקפות מסוג watering hole.[15] מתקפות אלו נועדו לגנוב מיומנויות ולהשיג גישה לרשתות ולמכונות של הקורבנות.[16]

---

12 "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions", *The Public-Private Analytic Exchange Program*, 2017, p. 12.

13 "Task Force on Cyber Supply Chain", pp. 1-2.

14 "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", *Department of Homeland Security*, *United States Computer Emergency Readiness Team*, last updated March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

15 תקיפת אתרים לגיטימיים הרלוונטיים למושאי התקיפה, בדרך כלל אתרים טכניים וחדשותיים בתחום המקצועי, באופן שגישה אליהם תגרום לתקיפת מערכות המשתמשים.

16 "CHRYSENE", *Dragos Inc*., May 17, 2018, https://dragos.com/blog/20180517Chrysene.html.

בעלות נסתרת וגלובליזציה של ספקים בשרשרת האספקה

שרשראות האספקה הופכות לגלובליות. ככל שהן נעשות יותר מורכבות ובין־לאומיות, כך עולה היכולת של גורמים עוינים "לחדור לשרשרת האספקה בנקודות מרובות ולבסס בהן מראש פעולות חתרניות מתמשכות ורחבות ממדים".[17]

שליטה, השפעה ואפילו בעלות של ממשלות חורשות רע או תאגידים המזוהים עם ממשלות כאלו על נקודות לאורך שרשרת אספקה גלובלית הן תופעות מטרידות במיוחד. קודים של תוכנות וקושחות מפותחים על ידי ספקים במספר רב של מדינות, ומצב זה "פותח פתח לשפע של הזדמנויות עבור אויביה של ארצות הברית, כמו רוסיה וסין, להחדיר פגיעויות לתוך מערכות שונות, באופן שיאפשר לשירותי המודיעין של אותן מדינות לנצל אותן בשלב מאוחר יותר".[18] חששות דומים קיימים גם לגבי הפוטנציאל שיש לגורמים עוינים להחדיר לשרשראות האספקה רכיבים הפגיעים במיוחד לאיומים אלקטרומגנטיים.

סין גם שולטת ברמה גלובלית ביכולת הייצור וההרכבה של כל הקשור בתחום מערכות מידע.[19] רבים ממוצרי החומרה הנמצאים ברשתות המשרתות תשתיות מכילים רכיבים המיוצרים בסין, דבר שעלול לחשוף אותם לסיכון של הדבקה וזיהום. עדות לאיום פוטנציאלי זה ניתן לראות בדאגה שהביעו לאחרונה גורמי מודיעין ומחוקקים אמריקאיים במהלך דיון שנערך בקונגרס בנוגע לחדירה הסינית לתחום הטלקום, ובמיוחד לחוזי הצטיידות פוטנציאליים עם הממשל והתעשייה האמריקאיים.[20] ארצות הברית גם אסרה על שימוש במוצרים של החברה הרוסית AO Kaspersky Lab בכל מערכות המידע הפדרליות, כשהיא מנמקת זאת בשיקולי ביטחון.[21]

ואכן, גורמים עוינים יכולים למנף את הגישה למערכות כאלו להתקפות זדוניות. יתר על כן, יריבים פוטנציאליים כבר מנסים לחתור תחת יוזמות לניהול סיכונים בשרשרת האספקה, וסביר להניח שאף יצליחו בכך בשנים הקרובות. דוגמה בולטת לכך היא חברת Huawei Technologies – חברת טכנולוגיה סינית החבֵרה במספר

17 "Supply Chain Risk Management: Intelligence.Gov Background Paper", p. 1.

18 Joseph Marks, "DHS to Scrutinize Government Supply Chain for Cyber Risks", *Nextgov*, February 14, 2018, http://www.nextgov.com/cybersecurity/2018/02/dhs-scrutinize-government-supply-chain-cyber-risks/145998/.

19 Lam and Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats".

20 Marks, "Chinese Telecoms Could Join Kaspersky On Government Wide Banned List".

21 "Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses", *Department of Homeland Security, Federal Register*, 82, no. 180, September 19, 2017, p. 43782, https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational.

ארגוני אבטחת סייבר המקדמים יוזמות לניהול סיכונים בשרשרת האספקה, ובהם Open Group (עם תוכנית הסמכה המבוססת על תקן שפיתחה: Open Trusted Technology Provider – O-TTPS)[22] ו־SAFECode (שגיבשה נהלים בסיסיים לפיתוח תוכנה מאובטחת).[23] בנוסף לאיומים ישירים על שרשרת האספקה, הצפי הוא שניהול הסיכונים עצמו יהפוך גם הוא למטרה פוטנציאלית למאמצי חדירה של גורמים עוינים.

העמימות והמורכבות של שרשראות האספקה

ככל ששרשראות האספקה הופכות לבין־לאומיות, כך הן גם הופכות למורכבות יותר. תהליך הגלובליזציה מאופיין ב"רשת מורכבת של ספקים וקבלני משנה של חלקי רכיבים, שירותים וייצור, המתפרסים בכל רחבי המדינה וגם ברחבי העולם", כאשר ריבוי השכבות והרשתות של הספקים יוצר לעיתים בלבול.[24] מכון התקנים הלאומי של ארצות הברית (NIST), שהוא בעל עניין עיקרי בנושא ניהול סיכונים בשרשרת האספקה, מזהיר מפני הקושי הגובר לסנן ספקים ומוכרים. ואכן, חברות רבות מתקשות לסנן שותפים לשרשרת האספקה מעבר לשכבה הראשונה שלהם.[25] עם זאת, רבים מבעלי התשתיות ומפעיליהן תלויים ב"מערכת מורכבת של שרשראות אספקה, שיש ביניהן קישורים הדדיים ושיטת הפצה גלובלית", המשרתת מוצרים ושירותים, ובהם שכבות מרובות של מיקור חוץ וערוצי הפצה מגוונים.[26] גורמים עוינים מסוגלים לפעול באמצעות חברות קש, ארגונים ויחידים כדי להסתיר את נוכחותם, כשהם פועלים לפגוע במאמצים לחשוף אותם ולפעול נגד מהלכיהם.[27]

המספר ההולך וגדל של מוכרים וספקים חיצוניים לחברות חשמל גורם לכך ש"לעיתים מתקשים נותני השירות להבטיח את שלמות שרשרת האספקה".[28] ואמנם, קיימת אפשרות כי מוצרים שעלולים להיות מסוכנים ימצאו את דרכם לתוך מערכות תשתית ללא ידיעת הבעלים.

---

22 "Standard Open Group Membership", *The Open Group*, last updated June 5, 2018, http://reports.opengroup.org/membership_report_all.pdf.

23 "Members", *SAFECode*, https://safecode.org/members/.

24 "Supply Chain Risk Management: Intelligence.Gov Background Paper", p. 1.

25 "Best Practices in Cyber Supply Chain Risk Management: Vendor Selection and Management", p. 1.

26 "Cyber Supply Chain Risk Management".

27 שם, עמ' 2.

28 "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector", *Mission Support Center, Idaho National Laboratory*, August 2016, p. 15, https://bit.ly/2G4OQrH.

החיבור הגובר בין מערכות מחשוב למערכות בקרה

החיבור ההולך ומתחזק בין מערכות מחשוב (IT) ובין מערכות בקרה (OT) מגביר את הסיכונים של מתקפות סייבר ואת השלכותיהן. מערכות OT, כגון מערכות שליטה, פיקוח ורכישת נתונים (SCADA), או מערכות בקרה תעשייתיות (ICS), הופכות לנפוצות בתוך מערכות התשתית. למרות שמערכות OT כאלו פעלו בעבר ברשת נפרדת ומנותקת מרשתות IT, כיום השתיים הולכות ויוצרות בהדרגה חיבור ביניהן.[29] תהליך זה גורם לפגיעויות ומגדיל את פני השטח החשופים למתקפות סייבר, אך יותר מכך מטרידה העובדה שבמקרה של פגיעה במערכות OT, במיוחד אם מדובר בפגיעה בקנה מידה גדול, עלולות להיות לכך השלכות פיזיות ישירות, ואולי אף הרות אסון, על התשתיות.

ההתקדמות בניהול סיכונים בשרשראות האספקה בתעשייה ובממשל

יוזמות חשובות לניהול סיכונים בשרשרת האספקה הולכות ומתרבות ונמצאות כיום בעיצומן. למעשה, יוזמות כאלו צומחות במהירות כה רבה, עד שאין אפשרות להציג סקירה מקיפה ועדכנית שלהן. להלן ייעשה ניסיון ראשוני להציג סקירה כזו. מדובר ברשימה שאינה ממצה את כל ההתפתחויות, ואין ספק שכמה מהיוזמות לניהול סיכונים בשרשרת האספקה הוחמצו בה, אך עם זאת, היא תכלול רבות מהיוזמות החשובות.

המאמצים לקידום ניהול סיכונים בשרשרת האספקה יכולים להתממש בדרך של קביעת תקנים, אימוץ שיטות עבודה מומלצות או נקיטת אמצעים רגולטוריים אחרים, וכולם מתמקדים באותה מטרה: "זיהוי, הערכה ומניעה של הסיכונים למוצרים ושירותים של IT/OT, הנובעים מטבען המבוזר והמקושר של שרשראות האספקה".[30] על היוזמות לניהול הסיכונים לתת מענה "למחזור החיים המלא של המערכת (לרבות תכנון, פיתוח, הפצה, פריסה, רכישה, תחזוקה והרס), שכן איומים ופגיעויות בשרשרת האספקה עלולים, במתכוון או שלא במתכוון, לחבל בכל מוצר או שירות IT/OT בכל שלב שלו".[31]

רבות מהיוזמות שיפורטו להלן עוסקות בהערכת סיכונים בשרשרת האספקה ומנסות לצמצם אותם, לעיתים עבור תחום או ענף תשתיות מסוים. תחילה ייבחנו יוזמות לניהול סיכונים בענף החשמל, ובהמשך יתוארו יוזמות לניהול סיכונים

29 "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector", p. 4.

30 "Cyber Supply Chain Risk Management".

31 שם.

בשרשראות אספקה מרובות תחומים. לצידם יובא פירוט של יוזמה חדשה בתחום זה, המסתמנת כמבטיחה מאוד, אותה מובילה חברת "סימנס".

יוזמות בתחום האנרגיה

תחום האנרגיה, ובעיקר ענף החשמל, ממלאים תפקיד קריטי בהפעלת כל ענפי התשתית במשק. האיומים על תחום זה הם חמורים במיוחד ומהווים גורם מניע, הן למאמצי התעשייה והן למאמצי הממשל, להתמודדות עם ריבוי האתגרים הכרוכים בכך. למרות זאת, המאמצים להגדיר את הדרישות ואת תחומי המחקר והפיתוח לאבטחת שרשראות האספקה עבור טכנולוגיות רשת החשמל אינם מצליחים להדביק את הצרכים, למרות כל הידוע על איומים מצד גורמים עוינים ועל הסיכונים הגוברים הנובעים מהאופי הגלובלי של שרשראות האספקה.[32] יחד עם זאת, כמה יוזמות חשובות נמצאות בתכנון ועשויות להוות את הבסיס להמשך המאמצים בעתיד.

משרד האנרגיה של ארצות הברית

משרד האנרגיה האמריקאי, כגוף העוסק ספציפית בתחום האנרגיה בארצות הברית, פועל לתת מענה לפגיעויות סייבר בשרשרת האספקה בתחום זה. המדריך שהוציא המשרד, שכותרתו "הנחיות לרכש מוצרים לאבטחת סייבר עבור מערכות לאספקת אנרגיה", שגובש בשיתוף עם התעשייה, מצייד את נותני השירותים ב"אסטרטגיות והנחיות מומלצות שיסייעו לתחום האנרגיה בארצות הברית ולספקי הטכנולוגיה לבנות הגנות סייבר, תוך כדי התכנון והייצור של המוצר".[33]

משרד האנרגיה האמריקאי גם פרסם במארס 2018 את "התוכנית הרב־שנתית לאבטחת סייבר בתחום האנרגיה". בין המטרות והיעדים של התוכנית מצוינת החובה "לצמצם את הפגיעויות והסיכונים הקריטיים באבטחת סייבר של שרשרת אספקה".[34] כדי לעשות זאת, מתכנן משרד האנרגיה לנקוט את הצעדים הבאים:

- **זיהוי הפעולות שעל הממשלה הפדרלית לנקוט כדי לצמצם את הסיכונים בשרשרת האספקה**: משרד האנרגיה ישתף פעולה עם גורמים פדרליים אחרים כדי לזהות ולנקוט את הפעולות המתאימות לצמצום סיכוני אבטחת סייבר

32 "Identifying and Mitigating Supply Chain Risks", p. 2.

33 "Energy Department Releases New Guidance for Strengthening Cybersecurity of the Grid's Supply Chain", *Department of Energy*, April 28, 2014, https://www.energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain.

34 "Multiyear Plan for Energy Sector Cybersecurity", *Department of Energy*, March 2018, p. 6.

בשרשרת האספקה, ויסייע לבניית אמון בין בעלים ומפעילים ובין יצרני מערכות בקרה תעשייתיות (ICS) בתחום האנרגיה.

- **פיתוח מעבדת בדיקה וניתוח של מערכות אספקת אנרגיה**: לנוכח האיומים המתפתחים ופגיעויות חדשות המתגלות ומנוצלות על ידי גורמים עוינים, נדרשות יכולות לאומיות שיעריכו את סיכוניהם, יגבשו שיטות חלופיות וישתפו פעולה עם יכולות סייבר נוספות של הממשל ושל המגזר הפרטי, כדי לחלוק מידע מעשי בדרך המהירה ביותר. משרד האנרגיה ייצור בתוך מעבדות לאומיות יכולת בדיקה פיזית של הסייבר, כדי לנתח פגיעויות במערכות וברכיבים שונים, איומים מצד תוכנות זדוניות והשלכות של איומים מסוג "מתקפת אפס ימים" על תשתיות אנרגיה. כמו כן, יתמוך המשרד ביוזמות להקשיח את שרשרת האספקה. צעדים אלה יושגו על ידי פיתוח דרישות ושיתוף פעולה בין המעבדות הלאומיות ובין המגזר הפרטי.[35]

תוכנית אבטחת הסייבר של משרד האנרגיה האמריקאי לשנת 2018 גם מדגישה את חשיבות המחקר, הפיתוח והצגת כלים וטכנולוגיות לסיוע במניעת אירועי סייבר. כשמדובר ספציפית בניהול סיכונים בשרשראות האספקה, על כלים אלה לשאוף "להקטין את הסיכון הנשקף ממערכת זדונית, שעשויה להיות מוחדרת באמצעות רכיבים ומערכות העוברים בשרשרת האספקה".[36] משרד האנרגיה והגורמים השותפים לו כבר השיגו התקדמות מסוימת לקראת יעד זה. התוכנית של המשרד מציינת כי "שיתוף הפעולה המחקרי של משרד האנרגיה מקדם כלים וטכנולוגיות שיסייעו בזיהוי גורמים בלתי רצויים ובעלי פוטנציאל זדוני, שאולי הוכנסו לחומרה, לקושחה או לתוכנה של רכיבי מערכת אספקת האנרגיה דרך שרשרת האספקה". התוכנית כוללת גם "הנחיות לנוסח הדברים שבו ישתמשו רוכשים וספקים של מערכות אספקת אנרגיה, כבסיס לדיון באמצעי אבטחת הסייבר הדרושים למערכות אספקה אלו". כן מסייעת התוכנית "להבטיח את תקינות כל העדכונים והשדרוגים".[37]

האסטרטגיה של משרד האנרגיה האמריקאי קוראת ל"פיתוח קוד מאובטח והבטחת איכות התוכנה (1.2 ו־1.3): ניתן ליישם שיטות קידוד מאובטחות ובטוחות על מוצרים חדשים, אך עלותן הגבוהה, התנגשות עם מוצרים מדור קודם וחוסר ביקוש ממשיכים להיות חסמים מרכזיים בתחום זה. נדרשת השקעה משמעותית בהעלאת המודעות ובהכשרת כוח אדם. סיכוני שרשרת האספקה ממשיכים להיות סוגיה מרכזית".[38]

---

35 שם, עמ' 25.
36 שם, עמ' 34.
37 שם, שם.
38 שם, עמ' 45.

התייחסות משרד האנרגיה להוראה הנשיאותית מספר 13800 – "חיזוק אבטחת הסייבר של רשתות פדרליות ותשתיות קריטיות", שפורסמה במאי 2017, מהווה התקדמות מעודדת, אם כי עדיין לא הגיעה לשלב מימוש. דוח של משרד האנרגיה מכיר בחומרת האיומים בשרשרת האספקה על רכיבי רשת החשמל, ומדרבן את המשרד "לפתח תוכנית לבדיקות של מרכיבי הרשת על ידי מעבדות לאומיות, כדי להעריך את מצב אבטחת הסייבר של שרשרת האספקה ולבחון בסימולציות את ההשפעות של תוכנות זדוניות במרחב הסייבר על רכיבים [ברשת החשמל]".[39] לא ברור כמה התקדמות חלה בנושא זה, אם בכלל, שכן משרד האנרגיה המליץ על הדברים רק באוגוסט 2017.

משרד האנרגיה פועל, יחד עם המעבדות הלאומיות הכפופות לו, כדי לבצע גם בעצמו בדיקות של מוצרים בתחום האנרגיה החשמלית. מתחם הניסויים של תשתיות קריטיות של המעבדה הלאומית של איידהו (INL), הכולל "מתקני ניסוי" לרשת החשמל ולרכיבי סייבר אחרים, "מאפשר ניסויים מדורגים, הן פיזיים והן במרחב הסייבר, על מערכות תשתית בקנה מידה תעשייתי".[40] המשרד משתף פעולה גם עם מעבדות לאומיות אחרות במגוון רחב של פרויקטים בתחום האנרגיה הקשורים לאבטחת סייבר, ועושה זאת דרך מתקן הניסוי הלאומי של מערכות שליטה, פיקוח ורכישת נתונים (SCADA).[41] בנוסף, משתף משרד האנרגיה פעולה עם מספר מעבדות לאומיות (ובראשן INL), ועם בעלי עניין אחרים בממשל ובתעשייה, סביב תוכנית לבדיקת חוסן הסייבר של מערכות בקרה תעשייתיות (CyTRICS), הנמצאת כרגע בשלב הפיילוט. תוכנית CyTRICS משמשת את משרד האנרגיה כדי לבחון רכיבים קריטיים בשרשרת האספקה ולמנף את נתוני הבדיקה לצורך זיהוי סיכונים שיטתיים בה.

הוועדה הפדרלית לפיקוח על שוק האנרגיה והתאגיד הצפון־אמריקאי לאמינות החשמל

הוועדה הפדרלית לפיקוח על שוק האנרגיה (FERC) הניחה את היסודות לדרישות מהמגזר הפרטי בתחום ניהול הסיכונים במערכת החשמל. ביולי 2016 הורתה הוועדה לתאגיד הצפון־אמריקאי לאמינות החשמל (NERC) לפתח תקני אמינות לניהול

39 "Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities", *Department of Energy*, August 9, 2017, p. 29.

40 "Securing the Electrical Grid from Cyber and Physical Threats", *Idaho National Laboratory*, https://www.inl.gov/research-programs/grid-resilience/.

41 "National SCADA Test Bed", *Department of Energy*, https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

סיכונים בשרשרת האספקה,[42] או ליתר דיוק, הפקידה בידי התאגיד את המשימה לגבש תקנים שיחייבו גופים לפתח תוכנית לניהול סיכונים, שתתמקד בארבעה יעדים: "(1) מקוריות ושלמות התוכנה; (2) גישה מרחוק של ספקים; (3) תכנון מערכות מידע; (4) ניהול סיכוני ספקים ובקרות רכש".[43] הוועדה אישרה בינואר 2018 את התקנים הבאים: תקן CIP–013–1 (אבטחת סייבר – ניהול סיכונים בשרשרת האספקה); תקן CIP–005–6 (אבטחת סייבר – פרמטרים לאבטחה אלקטרונית); תקן CIP–010–3 (אבטחת סייבר – ניהול שינויי תצורה והערכת פגיעויות).[44] להערכת הוועדה, השילוב בין תקנים אלה נותן מענה ליעדים שצוינו לעיל. כך, למשל, תקן CIP–013–1 נועד "לצמצם סיכוני סייבר לפעולה אמינה של מתקני אנרגיה מרכזיים, על ידי יישום בקרות אבטחה לניהול סיכונים בשרשרת האספקה של מערכות הסייבר במתקנים אלה".[45]

תקני האמינות של שרשרת האספקה של התאגיד לאמינות החשמל הינם חשובים ביותר לצורך מתן מענה לסיכונים בשרשרת האספקה של ענף החשמל. יתרה מכך, חברות חשמל שונות יזמו בניית יכולות עמידה מול איומי סייבר ואיומים אלקטרומגנטיים, ורבות מהן נקטו צעדים מעל ומעֵבר לדרישות של תקני האמינות ויישמו מרצונן אמצעים נוספים. באותה מידה, סביר להניח שהן ינקטו גישה דומה גם לצורך אבטחת שרשרת האספקה.

התקנים החדשים אמנם מעניקים בסיס חשוב לחיזוק שרשראות האספקה של ענף החשמל, אך הם כרוכים גם במספר מגבלות. לדוגמה, המגבלות הקיימות על הוועדה הפדרלית לפיקוח על שוק האנרגיה והתאגיד לאמינות החשמל, מתוקף סעיף 215 לחוק החשמל הפדרלי של ארצות הברית, גורמות לכך שרק גופים מסוימים בתעשיית החשמל האמריקאית נדרשים לעמוד בתקנים אלה. הוועדה הפדרלית מציינת במפורש שהתקנים אינם חלים על "ספקים, מוֹכרים או גופים אחרים שאינם כפופים לסמכות השיפוט שלה ומספקים מוצרים או שירותים לגורמים הנושאים באחריות".[46] למעשה, התקנים אינם חלים (למעט חריגה קטנה אחת) על מערכות ניטור ובקרה אלקטרוניות (EACMS), על מערכות בקרה פיזיות (PACS) ועל נכסי סייבר מוגנים (PCA) של גופים הכפופים לסמכות השיפוט של הוועדה הפדרלית

42 "FERC Directs Development of Standards for Supply Chain Cyber Controls", *Federal Energy Regulatory Commission*, July 21, 2016, https://www.ferc.gov/media/news-releases/2016/2016-3/07-21-16-E-8.asp#.WQC2DGnysuU.

43 "Supply Chain Risk Management Reliability Standards (Docket No. RM17-13-000)", *Federal Energy Regulatory Commission,* 162 FERC ¶ 61,044, January 18, 2018, p. 5.

44 שם, עמ' 1.

45 "CIP-013-1–Cyber Security–Supply Chain Risk Management", *North American Electric Reliability Corporation*, July 2017, p. 3, https://bit.ly/2A1rWyE.

46 "Supply Chain Risk Management Reliability Standards", p. 7.

ושל התאגיד לאמינות החשמל, וכן של גופים הנחשבים כ"בעלי השפעה נמוכה". הוועדה מציינת כי כתוצאה מכך, "נותר סיכון משמעותי בתחום אבטחת הסייבר, הקשור לשרשרת האספקה למערכות הסייבר של מתקני אנרגיה מרכזיים".[47]

המועצה לתיאום בענף החשמל

המועצה לתיאום בענף החשמל (Electricity Sub-sector Coordination Council – ESCC) היא חוליה קריטית המקשרת בין גורמי הממשל האחראים על ענף החשמל ובין שותפיו בתעשייה. המועצה ובכיריה ממלאים תפקיד חשוב ביוזמות לקידום חוסנו של מערך החשמל ותורמים באופן משמעותי לאבטחה הכוללת של רשת החשמל. בין יוזמות אלו של המועצה נכלל גם נושא אבטחת שרשרת האספקה. ספציפית, המועצה פועלת בשיתוף עם הממשל כדי לכנס בעלי עניין מהמגזר הציבורי והפרטי, וכן ספקי אבטחה וטכנולוגיה, "כדי לזהות ולחלוק שיטות עבודה מומלצות שיתנו מענה לאיומים על שרשרת האספקה".[48] המועצה ומשרד האנרגיה האמריקאי גם פועלים לגיבוש תוכנית מבוססת נתונים לזיהוי שיטתי של פגיעויות וסיכונים בשרשרת האספקה.

הוועדה לרגולציה גרעינית

גופים העוסקים באנרגיה גרעינית אינם כפופים לוועדה הפדרלית לפיקוח על שוק האנרגיה ולתאגיד לאמינות החשמל, אלא פועלים על פי הנחיות אבטחת סייבר משלהם. הנחיות הוועדה לרגולציה גרעינית (Nuclear Regulatory Commission – NRC) בדבר "הגנה על רשתות ומערכות מחשב ותקשורת דיגיטלית" מפרטות את דרישות אבטחת הסייבר עבור הגופים הכפופים לה,[49] אם כי דרישות אלו מחייבות רק באופן כללי את הגופים להבטיח את הגנת המערכות שלהם, ואינן כוללות הוראות ספציפיות לניהול סיכונים בשרשרת האספקה שלהם. אף על פי כן, סעיף (3)(d) בהנחיות הוועדה קובע כי על גופים אלה "להבטיח כי שינויים בנכסים ... יעברו הערכה לפני מימושם", וכי הערכה זו תוכל לטפל בפגיעויות שהוחדרו אליהם באמצעות עדכוני תוכנה וחומרה.

ההנחיות של הוועדה לרגולציה גרעינית מ־2010 מציינות במפורש את הצורך בניהול סיכונים בשרשרת האספקה, כחלק מבקרות האבטחה הניהוליות והתפעוליות. הוועדה ממליצה באותן הנחיות להגן על מתקנים מפני איומים על שרשרת האספקה

47 שם, עמ' 3, 8.

48 "ESCC", *Electricity Subsector Coordinating Council*, January 2018, http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8.

49 "§ 73.54 Protection of Digital Computer and Communication Systems and Networks", *U.S. Nuclear Regulatory Commission*, 2009, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

באמצעות הקמת ערוצי הפצה מהימנים ואימות ספקים, ודורשת שמוצרים שיירכשו יכללו יכולת זיהוי של ניסיונות פריצה או חבלה (או ישאו חותם המוכיח כי קיימת בהם הגנה כזאת).[50] הוועדה לרגולציה גרעינית מתעתדת לבחון מחדש את תקנות אבטחת הסייבר שלה בשנת 2019, ולעדכנן על פי הצורך.[51]

יוזמות רב־מגזריות

המשרד לביטחון המולדת

המשרד לביטחון המולדת מרחיב את מאמציו בתחום ניהול הסיכונים בשרשרת האספקה. בינואר 2018 גיבש המשרד תוכנית משלו לניהול סיכונים בשרשרת האספקה בסייבר (C-SCRM), שנועדה לשמש כ"גורם מוביל וכנקודת התיאום המרכזית עבור כלל הממשל בנושאי ניהול הסיכונים בשרשרת האספקה בסייבר".[52] יוזמת המשרד לביטחון המולדת נושאת בחובה חזון שאפתני, המאפשר קיומה של "סביבה מבצעית ושוק לאומי וגלובלי של טכנולוגיות מידע ותקשורת, שבמסגרתם ניתן יהיה לזהות בקלות ובמהירות קיומם של חומרה, תוכנה או רכיבים מזויפים, לקויים או פגומים, אם בזדון ואם כתוצאה מרשלנות, ותתאפשר נקיטת פעולה לצמצומם או למניעתם ולהפיכתם לנדירים".[53] המשרד לביטחון המולדת מפרט את פעולותיה העיקריות של התוכנית כדלקמן:

- הקמת יכולת להערכת סיכונים בשרשרת האספקה לטובת בעלי העניין.
- הקמת יכולת לתקשורת, יידוע ושיתוף מידע בקרב בעלי העניין.
- גיבוש רשימת יצרנים וספקים מורשים באמצעות יישום תהליך אמין לאימות ואישור נוהלי אבטחה של חברות ומאפייני האבטחה של מוצרים ושירותים בתחום טכנולוגיות מידע ותקשורת.
- סיוע לבעלי עניין בפיתוח ויישום יכולות לניהול סיכונים בשרשרת האספקה.[54]

היוזמה לניהול סיכונים בשרשרת האספקה בסייבר, הכוללת את המינהל לשירותים כלליים (GSA), את משרד ההגנה, את קהילת המודיעין וכן בעלי עניין במגזר הפרטי

---

50 "Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities", *U.S. Nuclear Regulatory Commission*, January 2010, pp. C-29–C-30, https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

51 Sean Lyngaas, "Nuclear Power Plants Have a 'Blind Spot' for Hackers. Here's How to Fix That", *Motherboard*, April 27, 2018, https://motherboard.vice.com/en_us/article/mbxy33/cyberattacks-nuclear-supply-chain.

52 "Cyber Supply Chain Risk Management: Becoming a Smarter Consumer of ICT in a Connected World", *Department of Homeland Security*, June 2018, p. 15.

53 שם.

54 שם, עמ' 16.

בארצות הברית, נועדה לתרום לקבלת החלטות מושכלת בתחום הרכש הממשלתי.[55] לדברי גורם רשמי במשרד לביטחון המולדת, היוזמה "תספק למשתמשים, לקונים, ליצרנים ולמוכרים, העוסקים במוצרים טכנולוגיים, מידע מעשי על סיכונים בשרשרת האספקה ועל הדרכים לצמצומם. היא גם תזהה סיכונים לרשתות פדרליות ולבעלי עניין אחרים ברמה הלאומית או הגלובלית".[56] ג'נט מנפרה (Manfra), עוזרת השר לביטחון המולדת לענייני סייבר ותקשורת במינהלת התוכניות להגנה לאומית (NPPD), הוסיפה על כך שהיוזמה "תזהה ותצמצם איומים ופגיעויות בשרשרת האספקה" של נכסים בעלי ערך רב.[57]

היוזמה לניהול סיכונים בשרשרת האספקה בסייבר מתבססת על כלים קיימים של המשרד לביטחון המולדת, המיועדים לטיפול בסיכונים בשרשרת האספקה. לדוגמה, התוכנית לאבחון ולניטרול סיכונים כוללת אסטרטגיה שנועדה לצמצם איומי סייבר המבוססים על שרשרת האספקה. האסטרטגיה כוללת "רשימת מוצרים מאושרים", שהיא "קטלוג של מוצרים שאושרו כעומדים בדרישות הטכניות של התוכנית לאבחון ולניטרול סיכונים".[58] למשרד לביטחון המולדת יש גם תוכנית ניהול סיכונים ספציפית, שמטרתה "לספק מידע לסוכנויות השונות ולהורות על פעילויות הקשורות לדרך שבה מציעי עיסקאות מזהים, מעריכים ומנטרלים סיכונים בשרשרת האספקה, באופן שיקל על קבלת החלטות ומתן הוראות מושכלות יותר בקרב סוכנויות ממשלתיות".[59]

מכון התקנים הלאומי

מכון התקנים הלאומי (NIST) הוא מקור מרכזי להנחיות בתחום ניהול סיכונים בשרשרת האספקה. למרכז המשאבים לאבטחת מחשבים של המכון (CSRC)

---

55 Jory Heckman, "DHS, Lawmakers Doubling Down on Supply Chain Risk Management", *Federal News Radio*, February 15, 2018, https://federalnewsradio.com/cybersecurity/2018/02/dhs-lawmakers-doubling-down-on-supply-chain-risk-management/.

56 Lauren C. Williams, "DHS Developing Supply Chain Security Initiative", *FCW*, February 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx.

57 "Statement of Jeannette Manfra, Assistant Secretary for Cybersecurity and Communications, NPPD, U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology (2018)", *Department of Homeland Security*, p. 8.

58 "Continuous Diagnostics and Mitigation (CDM) ", *Department of Homeland Security*, last updated February 22, 2018,https://www.dhs.gov/cdm.

59 "Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Supply Chain Risk Management (SCRM) Plan", *Government Services Agency*, August 2017, p. 1.

יש תוכנית מקיפה לניהול סיכונים בשרשרת האספקה בסייבר, המתבססת על היכרותו עם שרשרת האספקה של רשתות IT ו־OT.[60]

פרסומי מכון התקנים ב־2015 בנושא ניהול סיכונים בשרשרת האספקה מספקים הדרכה מקיפה איך לנהל סיכונים בשרשרת האספקה בסייבר. ההנחיות מספקות למשרדי הממשל ולסוכנויות פדרליות מסגרת עבודה, הניתנת לשינוי או להרחבה על פי הדרישות, המדיניות, ההנחיות ושאר המסמכים הספציפיים של כל ארגון.[61] המסמך מציג מערך של תהליכים ואמצעים להערכה וניהול של סיכונים בשרשרת האספקה, ומציע תבנית לפיתוח תוכניות לניהול סיכונים. מכון התקנים גם מספק מערך של שיטות עבודה מומלצות בנושא ניהול סיכונים, הרלוונטיות לכל ענפי התשתית במשק האמריקאי.[62] זאת ועוד, העדכונים שערך המכון בשנת 2017, במסמך שכותרתו "מסגרת עבודה לשיפור אבטחת הסייבר בתשתיות קריטיות", כללו "פרטים חדשים על ניהול סיכונים בשרשרת האספקה בסייבר".[63] עדכון נוסף, מאפריל 2018, כלל עוד שינויים בתחום "ניהול אבטחת סייבר בתוך שרשרת האספקה".[64]

בנוסף ליוזמות ולהנחיות אלו, נוהג מכון התקנים האמריקאי לכנס ראשי ממשל, מנהלים מהמגזר הפרטי ואנשי אקדמיה כדי לדון בסיכונים בשרשרת האספקה. הפורום לאבטחת התוכנה ושרשרת האספקה, הפועל בהובלה משותפת של המשרד לביטחון המולדת, המינהל לשירותים כלליים ומשרד ההגנה, מאפשר למשתתפים "לשתף את הידע והמומחיות שלהם בנוגע לסיכונים בשרשרת האספקה והתוכנה, לשיטות עבודה יעילות ולאסטרטגיות, לכלים וטכנולוגיות לניטרול סיכונים, לגישור על פערים בין אנשים, תהליכים או טכנולוגיות בתחום זה".[65]

---

60. "Cyber Supply Chain Risk Management".
61. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161) ", *National Institute of Standards and Technology*, April 2015, p. 2.
62. "Utility Sector Best Practices for Cyber Security Supply Chain Risk Management", *National Institute of Standards and Technology*, October 2015, https://www.nist.gov/sites/default/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf.
63. "NIST Releases Update to Cybersecurity Framework", *National Institute of Standards and Technology*, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.
64. "NIST Releases Version 1.1 of its Popular Cybersecurity Framework", *National Institute of Standards and Technology*, April 16, 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.
65. "Software and Supply Chain Assurance Forum", *National Institute of Standards and Technology*, last updated March 29, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/SSCA.

כלי יעיל זה לשיתוף ותיאום אכן תורם לניהול הסיכונים, אולם יכולתו מוגבלת ביותר. יהיה זה יקר מאוד ולא מעשי להניח שהמשתתפים השונים בתהליך זה יצליחו לפתח מנגנונים עצמאיים משלהם להסמכת מוצרים, או לחלוק את מסקנותיהם עם עמיתיהם וליצור את "מאגר הביקוש" המאוחד הנדרש כדי להגביר את ההיצע של המוצרים שעברו הסמכה.

משרד הניהול והתקציב

משרד הניהול והתקציב (OMB) הינו מקור מרכזי למדיניות הממשל הפדרלי בנושא אבטחת סייבר. החוק הפדרלי למודרניזציה של אבטחת מידע (FISMA) קובע כי משרד הניהול והתקציב יפקח על המדיניות והנהלים של אבטחת המידע בגופים ממשלתיים. חוזר A–130 של משרד הניהול והתקציב, שפורסם בשנת 2016 ונושא את הכותרת "ניהול מידע כמשאב אסטרטגי", מגדיר את "המדיניות הכללית לתכנון, תקצוב, פיקוח, רכישה וניהול של מידע פדרלי, כוח אדם, ציוד, כספים, משאבי IT ותשתית ושירותים תומכים" עבור הרשות המבצעת של הממשל הפדרלי.[66] המסמך גם כולל הנחיה לגופים אלה כיצד ליישם את החוק למודרניזציה של אבטחת מידע, לצורך ניהול סיכונים בשרשרת האספקה ברמה הפדרלית. ספציפית, המסמך קובע כי גופים ממשלתיים:

- "ישקלו ... סוגיות הקשורות לאבטחת שרשרת האספקה עבור כל פעילות של ניהול ותכנון משאבים, לכל אורך מחזור חיי הפיתוח של המערכת, באופן שיבטיח כי הסיכונים ינוהלו כהלכה".
- "ינתחו סיכונים (לרבות סיכונים בשרשרת האספקה) הקשורים לקבלנים פוטנציאליים ולמוצרים ולשירותים שהם מספקים".[67]

נספח למסמך A–130, ה"מגדיר דרישות סף לתוכניות לאבטחת מידע פדרלי", מחייב גופים ממשלתיים:

- "ליישם עקרונות לניהול סיכונים בשרשרת האספקה באופן שיגן מפני החדרת זיופים, מוצרים בלתי מורשים, חבלה, גניבה או הכנסה של תוכנה זדונית, וכן מפני שיטות ייצור או פיתוח לקויות, וזאת בכלל מחזור חיי הפיתוח של המוצר".
- "לפתח תוכניות לניהול סיכונים בשרשרת האספקה, כמפורט במסמך SP 800–161 של מכון התקנים הלאומי, כדי להבטיח את שלמות אבטחתן, חוסנן ואיכותן של מערכת המידע".[68]

---

66 "Circular No. A-130: Managing Information as a Strategic Resource", *Office of Management and Budget*, July 2017, p. 6, https://bit.ly/2rAjz7Q.

67 שם, עמ' 6, 11.

68 שם, עמ' 40, 42.

בהנחה שמסמך A–130 ייושם בצורה קפדנית, יהיה באפשרותו לתרום לאבטחת שרשרת האספקה שבאחריות הרשות המבצעת. עם זאת, המדיניות שנקבעה לוקה בחסר בפירוט הדרישות הספציפיות, למעֵט הפְניה להנחיות מכון התקנים הלאומי, כפי שצוינו לעיל. גם ההנחייה שכל סוכנות תגבש תוכנית משלה לניהול סיכונים אינה ישימה מבחינה כלכלית, בוודאי לא ברמה הנדרשת. יתרה מכך, למרות שהמדיניות שגובשה חלה על רוב הגופים העוסקים ספציפית בנושא (למעט על הסוכנות להגנת הסביבה, בהיותה גוף העוסק ספציפית בענף המים והשפכים), היא מוגבלת לקבוצה קטנה בלבד של גופים ממשלתיים ואינה חלה על התעשייה או על בעלי עניין אחרים.

מינהל השירותים הכלליים

מינהל השירותים הכלליים (GSA) ממלא תפקיד מפתח ברכישות שמבצעת הממשלה הפדרלית, ובהתאם לכך – באחריות על אבטחת שרשראות האספקה הפדרליות. ספציפית, המינהל "מגבש יכולת מקיפה לניהול סיכונים בשרשרת האספקה, שתבטיח כי גופים ממשלתיים ירכשו חומרה ותוכנה של מערכות מידע מיצרני ציוד מקור, ובכלל זה ממפיצים מורשים וממקורות מהימנים אחרים".[69] מינהל השירותים הכלליים גם אחראי לגיבוש תוכנית להערכת סיכונים מצד הסַפָּק, שנועדה "להעריך סיכונים מוכרים או פוטנציאליים הקשורים לספקים של מוצרים ושירותים".[70]

משרד מנָהל המודיעין הלאומי והמרכז הלאומי לריגול נגדי וביטחון

מנהל המודיעין הלאומי (DNI) גיבש מדיניות לניהול סיכונים בשרשרת האספקה עבור קהילת המודיעין האמריקאית. הנחיה 731 של קהילת המודיעין של ארצות הברית קובעת מדיניות שנועדה "להגן על שרשרת האספקה בהתייחס למחזור החיים של מוצרים, חומרים ושירותים קריטיים המשמשים את קהילת המודיעין, וזאת באמצעות זיהוי, הערכה וניטרול האיומים".[71] להנחיה זו מתלוות הנחיות ספציפיות נוספות שנועדו לקבוע את מידת הקריטיוּת של רכיבים, וכן פרטים הנוגעים לביצוע הערכת האיומים, ולהביא לשיפור בשיתוף המידע.

---

69 Shon Lyublanovits, "Reducing Cybersecurity Risks in Supply Chain Risk Management", *General Services Administration*, September 18, 2017, https://gsablogs.gsa.gov/technology/2017/09/18/reducing-cybersecurity-risks-in-supply-chain-risk-management/.

70 שם.

71 "Intelligence Community Directive 731 – Supply Chain Risk Management", *Office of the Director of National Intelligence*, December 2013, p. 1.

בנוסף להנחיות אלו, גם המרכז הלאומי לריגול נגדי וביטחון עוסק באיומים על ניהול סיכונים בשרשרת האספקה. נייר עמדה של המרכז משנת 2013, וחומרי רקע שלו משנת 2017, מספקים מידע תמציתי אך בעל ערך לגבי איומים בשרשרת האספקה בסייבר וניהול סיכונים.[72] המרכז הלאומי לריגול נגדי גם יזם, בשיתוף עם המשרד לביטחון המולדת, שיתוף פעולה עם התעשייה, התורם למאמצים לקדם את ניהול הסיכונים בשרשרת האספקה. התוכנית לחילופי מידע בין המגזר הפרטי למגזר הציבורי[73] זיהתה את הסיכונים בשרשרת האספקה בסייבר כסוגיה מרכזית של ענף החשמל כבר במסמך עמדה שלה משנת 2016. המסמך מציג ממצאים והמלצות מרכזיים בנושא ניהול הסיכונים עבור התעשייה והממשל גם יחד.[74] דוח מפורט יותר של התוכנית לחילופי מידע בין המגזר הפרטי והמגזר הציבורי, משנת 2017, מסתמך על אותו נייר עמדה ומספק המלצות מקיפות יותר, במיוחד לגבי איומים בתחום מערכות בקרה. הדוח הופק כדי "להדגיש סיכוני אבטחה פוטנציאליים בשרשרת האספקה של מערכות שליטה, פיקוח ובקרת נתונים בשלב ההתחלתי הנוכחי שלהן, במטרה למנוע את הצורך להכניס בעתיד תיקונים יקרים בענפי תעשייה קיימים".[75]

למרות שהדוח כולל בעיקר מידע והמלצות, ואינו מדריך מפורט לפעולה קונקרטית, בכל זאת הוא בעל חשיבות, בהדגישו את התפקיד של המרכז הלאומי לריגול נגדי וביטחון, ובמיוחד של התוכנית לחילופי מידע בין המגזר הפרטי למגזר הציבורי כשותפים מרכזיים ליוזמה להסמכה בין־לאומית של מוצרי סייבר. הדבר נכון במיוחד לאור העובדה שיישום המלצות הדוח של התוכנית לחילופי מידע בין המגזרים, לפיהן על חברות לבנות מנגנוני הסמכה משלהן וליצור את כוחות השוק הדרושים כדי להגדיל את ההיצע של תוכנות וחומרות מוסמכות, הוא בגדר שאיפה לא מעשית.

משרד ההגנה האמריקאי

גם למשרד ההגנה של ארצות הברית יש מדיניות של ניהול סיכונים בשרשרת האספקה, שמטרתה היא להבטיח מערכות ורשתות אמינות. הוראה 5200.44 של משרד ההגנה, שעודכנה בפעם האחרונה ביולי 2017, ועניינה "הגנה על פונקציות קריטיות למילוי משימות, לשם הבטחת מערכות ורשתות אמינות", קובעת כללי מדיניות שמטרתם למזער את הסיכונים הקשורים ל"פגיעויות בתכנון המערכת, או לחבלה או פגיעה בפונקציות או ברכיבים קריטיים של המערכת ... על ידי מודיעין

72. "Supply Chain Risk Management: Framework for Assessing Risk".
73. *The Public-Private Analytic Exchange Program*.
74. "Identifying and Mitigating Supply Chain Risks".
75. שם, עמ' iii.

זר, טרוריסטים או גורמים עוינים אחרים".[76] ההוראה מדגישה את החשיבות של ניהול סיכונים בשרשרת האספקה לכל אורך מחזור החיים של המוצר. זוהי מדיניות המכוונת ספציפית לפונקציות במשרד ההגנה, המוגדרות כקריטיות למילוי משימות, אם כי ניתן להחיל עקרונות וגישות דומים גם על המאמצים והגישה הכללית הכרוכים ביוזמה להסמכה של מוצרי סייבר.

הבית הלבן

הבית הלבן מדגיש את חשיבות האבטחה של שרשראות אספקה גלובליות בשתי יוזמות נפרדות. כדי לנהל את סיכוני שרשרת האספקה פורסמה בינואר 2012 "האסטרטגיה הלאומית לאבטחת שרשרת האספקה הגלובלית", הקוראת לפעול להרחבת ההבנה לגבי האיומים על שרשראות האספקה, הנובעים מ"ניצול המערכת על ידי המבקשים להחדיר אליה מוצרים או חומרים הגורמים נזק".[77] גם "היוזמה הלאומית המקיפה לאבטחת סייבר" של הבית הלבן מדגישה את איומי שרשרת האספקה. יוזמה זאת, שמספרה 11, נועדה "לפתח גישה מרובת מוקדים לניהול סיכונים בשרשרת האספקה העולמית", שניהול הסיכונים במסגרתה יכלול "פיתוח ויישום של כלים ומשאבים להפחתת הסיכון הטכנולוגי והתפעולי לאורך מחזור החיים של המוצרים (החל מתכנון ועד יציאה משימוש) ... ושיתוף פעולה עם התעשייה במטרה לפתח ולאמץ תקנים ושיטות עבודה מומלצות לניהול סיכונים בשרשרת האספקה".[78]

יוזמות במגזר הפרטי

אחת היוזמות במגזר הפרטי נראית מבטיחה במיוחד וראויה לתשומת לב: יוזמת "אמנת האמון" (Charter of Trust). חברת "סימנס" חברה לאחרונה ל"ועידת מינכן לביטחון" ולגורמים ממשלתיים ועיסקיים אחרים (כולל IBM ו־AES) במטרה להשיק את יוזמת האמנה, שנועדה "לפתח וליישם כללים שיבטיחו את אבטחת הסייבר בכל רחבי סביבת הרשת".[79] עיקרון מספר שבע של האמנה מציע בסיס אפשרי לדו־שיח עם חברת "סימנס" ושותפיה לאמנה. לפי עיקרון זה, "חברות, ובמידת הצורך גם ממשלות, יגבשו יכולות הסמכה עצמאיות של צדדים שלישיים

76 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) ", *Department of Defense*, Instruction No. 5200.44, 2017, p. 1.

77 "National Strategy for Global Supply Chain Security", *The White House*, January 2012, p. 4.

78 "The Comprehensive National Cybersecurity Initiative", *The White House*, March 2010, https://obamawhitehouse.archives.gov/node/233086.

79 "Time for Action: Building a Consensus for Cybersecurity", *Siemens*, May 17, 2018, https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

(בהתבסס על הגדרות מותאמות לעתיד, במיוחד כאשר יש סכנת חיים על הפרק), לצורך מתן פתרונות חיוניים עבור תשתיות קריטיות ו'התקנים מחוברים'".[80] יש בכך הזדמנות של היוזמה להסמכה של מוצרי סייבר לחבור למשתתפי "אמנת האמון", כדי למצוא פתרונות משותפים לניהול סיכונים בשרשרת האספקה, שימנפו את היתרונות והמשאבים של כל יוזמה בנפרד.

הסמכת מוצרים

ארגונים ויוזמות הממוקדים בנושא הסמכת מוצרים, בעיקר במגזר הפרטי, מבקשים להעריך סיכונים פוטנציאליים במוצרים, בתהליכים ובמערכות ספציפיים. יש מספר לא מבוטל של ארגונים ותוכניות הסמכה כאלה ברחבי העולם, ואנו נסקור כאן רק כמה מהם. רבים מגופי הסמכה אלה נותנים את הדעת לאבטחת הסייבר, אך רק מעטים מהם כוללים הסמכות לתקנים אלקטרומגנטיים.

מעבדות החיתום

מעבדות החיתום (Underwriters Laboratories – UL) מספקות מגוון רחב של הסמכות, החל ממוצרים, דרך מִתקנים, תהליכים או מערכות ספציפיים, ועד לדרישות ותקנים של התעשייה.[81] מעבדות החיתום, כגורם מוביל בתחומו בארצות הברית, פועלות יחד עם יצרנים, מומחי תעשייה, מעבדות בדיקה אחרות וממשלות, ותקני הבדיקה שלהן נחשבים למעשה ל"תקנים בפועל של ממשלת ארצות הברית".[82] המעבדות יכולות לשמש גם גורמי צד שלישי עצמאיים, לצורך הסמכת שרשראות אספקה ותהליכים הקשורים בהן.[83] מינהל הבריאות והבטיחות בעבודה של משרד העבודה האמריקאי מכיר במעבדות החיתום כאחת ממעבדות הבדיקה המוכרות רשמית ברמה כלל־ארצית.[84]

---

80 "Charter of Trust: For a Secure Digital World", *Charter of Trust,* February 2018, https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

81 "Certification", *Underwriters Laboratories*, https://services.ul.com/categories/certification/.

82 Mike Murphy, "Inside the 122-Year-Old Company that Makes Sure our Electronics Don't Blow Up our Homes", *Quartz*, April 5, 2016, https://qz.com/643007/inside-the-122-year-old-company-that-makes-sure-our-electronics-dont-blow-up-our-homes/.

83 "Supply Chain Certification", *Underwriters Laboratories*, https://services.ul.com/service/supply-chain-certification/.

84 "Current List of NTRLs", *Occupational Safety and Health Administration*, https://www.osha.gov/dts/otpca/nrtl/nrtllist.html.

ארגון התקינה הבין־לאומי והנציבות הבין־לאומית לאלקטרוטכניקה

ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) הם שתי ישויות נפרדות המשתפות פעולה ביניהן כדי לגבש תקנים ולתת הסמכות למוצרים ולתעשייה. הוועדה הטכנית המשותפת של שני הגופים מתמקדת בפיתוח תקנים בתחום מערכות מידע.[85] תקן ISO/IEC 27036, הכולל ארבעה חלקים, מספק הנחיות שנועדות "לסייע לארגונים באבטחת המידע ומערכות המידע שלהם בהקשר של קשרים עם הספקים".[86] בנוסף לפעילות משותפת זו, הנציבות הבין־לאומית לאלקטרוטכניקה מפתחת תקינה אלקטרומגנטית, ובכלל זה תקנים עבור "מוצרים מורכבים, או כאלה הפועלים בסביבה מיוחדת".[87]

סדרת התקנים 62443 של הנציבות הבין־לאומית לאלקטרוטכניקה מציעה מודל שימושי במיוחד. תקנים אלה מתייחסים לצורך לגבש עמידות וחוסן של אבטחת הסייבר בתוך מערכות בקרה ואוטומציה תעשייתיות (IACS). תקן 1–4–62443 מתאר את הדרישות החלות על פיתוח מוצרים של מערכת הבקרה.[88] תקני ISO/IEC יכולים לסייע בקביעת הקריטריונים לתוכניות הסמכה עתידיות, אם כי יש צורך במאמצים נוספים כדי לקבוע באיזו מידה (וכיצד) יספק תקן ISO/IEC בדיקה ואימות מתמשכים של מוצרים וספקים.

חוק SAFETY (המשרד לביטחון המולדת)

המשרד לביטחון המולדת מחזיק בתוכנית להסמכת טכנולוגיות למאבק בטרור. לאחר התקפות ה־11 בספטמבר 2001 בארצות הברית, המגזר הפרטי "הסתייג מאוד מהטמעת טכנולוגיות ושירותים ביטחוניים בסביבה אזרחית, בשל סיכוני האחריות העצומים שהיו כרוכים בכך".[89] החשש של החברות היה כי הן ישאו באחריות, אם המוצר שלהן לא ימנע את המתקפה שהוא נועד למנוע, או לא ינטרל אותה. בתגובה לכך חוקק הקונגרס בשנת 2002 את חוק "התמיכה במאבק בטרור באמצעות אימוץ טכנולוגיות יעילות" (חוק SAFETY), אשר נועד "להבטיח כי איום החבות לא ירתיע יצרנים או מוכרים פוטנציאליים של טכנולוגיות נגד טרור

---

85 "ISO/IEC JTC 1 — Information Technology", *International Organization for Standardization*, https://www.iso.org/isoiec-jtc-1.html.

86 "ISO/IEC 27036-1:2014", *International Organization for Standardization*, April 2014, https://www.iso.org/standard/59648.html.

87 "EMC Product Standards", *International Electrotechnical Commission*, 2018, http://www.iec.ch/emc/emc_prod/.

88 "Overview – The 62443 Series of Standards", *ISA*, 2015, https://fr.scribd.com/document/358894928/ISA-62443-Series-Overview.

89 "Research and Development Partnerships – SAFETY Act for Liability Protection", *Department of Homeland Security*, January 14, 2014, https://bit.ly/2JPIolm.

מלפַתח ולשווק טכנולוגיות מצילות חיים".[90] חוק SAFETY מכיל מנגנון להסמכת מגוון רחב של מוצרים, שירותים וטכנולוגיות כ"טכנולוגיות מאושרות נגד טרור" (QATT), ובכך הוא מאפשר להכניס אותם לרשימת המוצרים המאושרים לצורכי הגנה על ביטחון המולדת מכוח אותו חוק.[91] המשרד לביטחון המולדת מגביל את אחריות המוכרים והמשתמשים של מוצרי הטכנולוגיות המאושרות נגד הטרור.[92] בין המוצרים הזכאים לפטור מאחריות מכוח חוק SAFETY ניתן למצוא גם טכנולוגיות לאבטחת סייבר.[93]

תוכניות בין־לאומיות להסמכת אבטחת סייבר

ישנם כמה מנגנוני הסמכה וגופים שנועדו להבטיח את אבטחת הסייבר של מוצרים. למעשה, סמכות לאבטחה שכבתית של מוצרי מערכות מידע מסחריות קיימת מזה למעלה משלושים שנה.[94] הקריטריונים שעל פיהם פועלות תוכניות הסמכה כאלו מעוגנים בתקנים, כגון "הקריטריונים השכיחים". תקינת "הקריטריונים השכיחים" גם יצרה מערכת הסמכה רחבה הכוללת תוכנית הסמכה למוצרים. המערכת כוללת הבטחת הערכה איכותית של מוצרי מערכות מידע, שיפור הזמינות של מוצרים בטוחים בעלי הסמכה, מניעת הצורך בהערכות כפולות ושיפור מתמיד של "האפקטיביות והיעילות הכלכלית של תהליך ההערכה וההסמכה".[95] עד 5 ביוני 2018 הוסמכו 2,351 מוצרים במסגרת "הקריטריונים השכיחים", ביניהם הֶתקנים ומערכות לבקרת גישה, מערכות הפעלה, התקנים ומערכות לגילוי, והֶתקנים ומערכות להגנת גבולות.[96]

בדומה ליוזמות רבות הממוקדות באבטחת סייבר (בניגוד להתמקדות בתשתיות ספציפיות), אחד החסרונות הפוטנציאליים של "הקריטריונים השכיחים" הוא ההתמקדות במערכות מידע ולא במערכות בקרה. בנוסף לכך, החברות המשתתפות ביוזמת הקריטריונים אינן כוללות את סין, רוסיה או יריבים אחרים של ארצות

90 "The Office of SAFETY Act Implementation", *Department of Homeland Security*, https://www.dhs.gov/science-and-technology/safety-act.

91 "Research and Development Partnerships – SAFETY Act for Liability Protection".

92 שם.

93 שם.

94 Steven B. Lipner, "SAFECode Perspective on Cybersecurity Certification", January 2018, p. 1, https://safecode.org/wp-content/uploads/2018/02/SAFECode_Perspective_on_Cybersecurity_Certification.pdf.

95 "About the Common Criteria", *Common Criteria*, https://www.commoncriteriaportal.org/ccra/index.cfm.

96 "Certified Products", *Common Criteria*, https://www.commoncriteriaportal.org/products/.

הברית במרחב הסייבר.[97] היוזמה כוללת ועדת ניהול, שבה נציגים בכירים מכל מדינה חברה, וזאת "כדי ליישם את ההסדר וכדי לספק אכוונה לכל מדינה בבואה לבצע פעילויות הערכה ואימות בתוכנית הלאומית שלה".[98]

קיים מגוון של תוכניות הסמכה נוספות במגזרים הציבורי והפרטי. כאמור, חלק מיוזמות ניהול הסיכונים בשרשרת האספקה עשוי להיפגע על ידי המדינות החברות בארגון המייסד את היוזמה. כך, למשל, ארגון Open Group מתגאה שחברים בו יותר מ־500 משתתפים בין־לאומיים, כולל נוכחות אמריקאית גדולה במיוחד, אך פריסה זאת של הארגון גם מאפשרת לכלול בתוכו יריבים פוטנציאליים. לעומתו, ארגון SAFECode הוא הרבה יותר קטן, אם כי גם בו עשויים להיות חברים יריבים פוטנציאליים של ארצות הברית.

SAFECode

SAFECode הוא ארגון הפועל במסגרת האיחוד האירופי ומתמקד באבטחת תוכנה. לתוכנית של הארגון יש חזון הדומה ליוזמה להסמכה בין־לאומית של מוצרי סייבר. SAFECode מבקש לסייע למשתמשים "לזהות מוצרים ושירותים מקוונים המספקים אבטחה יעילה, לתמרץ את הספקים להשקיע באבטחה יעילה ולהבטיח להם שיתוגמלו על השקעה זאת".[99] ראוי לציין כי SAFECode מסייע לגופים קטנים ובינוניים, הנאבקים לעמוד בתחרות עם ארגונים גדולים שממנים תוכניות ניהול סיכונים משלהם ברחבי העולם.[100] היוזמה להסמכה בין־לאומית של מוצרי סייבר נותנת מענה לאתגר זה באמצעות ריכוז המשאבים הדרושים לאבטחת שרשראות האספקה, וכן על ידי יצירת "איתות ביקושים" חזק ועקבי למוצרים מאובטחים.

מסמכי רקע של SAFECode העוסקים בהסמכת אבטחת סייבר מספקים כמה נקודות מבט מעניינות: SAFECode מדגיש את חשיבות הסמכת המוצר כבר בשלב הפיתוח שלו, ולא לאחר יציאתו לשוק, וזאת כדי להבטיח שחברות לא ימצאו את עצמן משתמשות במוצר שיש בו פגיעויות פוטנציאליות, בשעה שהוא ממתין לקבלת ההסמכה כמוצר מאובטח.[101] יותר מכך, SAFECode מדגיש את התועלת שבמערכת הסמכה שכבתית, ומציין בהקשר זה כי "תוכניות המספקות רמות משתנות של הסמכה ימריצו מפתחים לחפש את הרמה הגבוהה ביותר של

97. "Members of the CCRA", *Common Criteria*, https://www.commoncriteriaportal.org/ccra/members/.
98. "About the Common Criteria".
99. Lipner, "SAFECode Perspective on Cybersecurity Certification", p. 2.
100. שם, עמ' 3.
101. שם, עמ' 2.

הסמכה".[102] בנוסף, SAFECode מדגיש את טביעת הרגל הבין־לאומית הבלתי נמנעת שנמצאת בשרשראות האספקה כיום, ודוחק ל"הכרה הדדית רחבה, שתביא תועלת מרבית למשתמשים ולמפתחים בכל רחבי העולם".[103]

תשתית ניהול הסיכונים של SAFECode הינה מוגבלת, שכן ההתמקדות היחידה של הארגון היא במערכות מידע (ולא במערכות בקרה). כמו כן, SAFECode מטיל את חובת הציות, הבדיקות והאימות על הארגונים עצמם, דבר שמוביל לכפילות משמעותית במשאבים ולחוסר יעילות. עם זאת, "השיטות הבסיסיות לפיתוח תוכנה מאובטחת" של SAFECode יכולות להוות מקור נוסף לתובנות עבור תוכניות הסמכה עתידיות.[104]

תוכנית ההסמכה O-TTPS

תוכנית Open Trusted Technology Provider Standard (O-TTPS) של Open Group כוללת הנחיות, המלצות, דרישות ושיטות עבודה מומלצות, שמטרתן היא "לשפר את שלמות המידע של המוצרים [מוצרי המדף המסחריים ומוצרי טכנולוגיית תקשורת] ואת אבטחת שרשראות האספקה הגלובליות שלהם".[105] הארגון מסמיך ארגונים שלדעתו עומדים בדרישות התוכנית ומסוגלים להיות "ספקי טכנולוגיה מהימנים".[106]

גם מסמכי המדיניות וההנחיות של תוכנית O-TTPS מספקים חומר בסיסי חשוב ליוזמות עתידיות בתחום אבטחת הסייבר. לדוגמה, מסמך מדיניות ההסמכה משנת 2017 כולל תרשימי זרימת עבודה מפורטים להסמכת צדדים שלישיים, עם פירוט נוסף עבור כל שלב בתהליך.[107] המסמך כולל, בנוסף לכך, גם מדיניות ספציפית הנוגעת לדרישות התאמה והסתגלות, לדרכים בהן ניתן לשמור על ההסמכה ולבצע הסמכה מחדש ולתהליך הערעור על החלטות בנושא הסמכה.

---

102 שם, שם.

103 שם.

104 "Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program (Third Edition) ", *SAFECode*, March 2018, https://safecode.org/wp- content/ uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

105 "The Open Trusted Technology Provider Standard (O-TTPS) Certification Program", *The Open Group*, http://www.opengroup.org/certifications/o-ttps.

106 שם.

107 ראו: "Open Trusted Technology Provider Standard (O-TTPS) Certification Policy (Version 1.1)," *The Open Group*, January 2017, pp. 14-18, https://ottps-cert.opengroup.org/sites/ottps-cert.opengroup.org/files/doc/O-TTPS_Certification_Policy.pdf.

היוזמה להסמכה בין־לאומית למוצרי סייבר

היוזמה להסמכה בין־לאומית למוצרי סייבר (Cyber Product International Certification – CPIC) של המועצה לביטחון תשתיות החשמל (EIS) מסוגלת לתת מענה לרבים מהאתגרים שתוארו לעיל. נכון להיום, בעלים ומפעילים של תשתיות חסרים תהליך מרוכז, המונע על ידי בעלי עניין, שיאשר כי מוצרי חומרה ותוכנה חיוניים עמידים בפני תוכנות זדוניות או סוגי פגיעות אחרים מצד גורמים עוינים, ולו באופן מינימלי. קביעת תהליך הסמכה, כמוצע על ידי המועצה, תתרום תרומה עצומה לחוסן הסייבר, במיוחד אם סוכנויות ממשלתיות יוכלו לספק מידע על האיומים ויתמכו בצורות נוספות ביוזמה. הסמכה בין־לאומית למוצרי סייבר גם יכולה לתרום משמעותית לחוסנן של תשתיות, בזכות הכללתם בה של אמצעים להסמכת מוצרים מפני הפרעות אלקטרומגנטיות מכוונות. להלן יפורטו הנושאים המרכזיים שיש לתת עליהם את הדעת כחלק מקידום היוזמה להסמכה בין־לאומית למוצרי סייבר.

מינוף יכולות ותוכניות קיימות לניהול סיכונים בשרשרת האספקה בארגונים

לישויות רבות במגזר הפרטי יש כבר היום הנחיות רכש המשמשות שיטות עבודה מומלצות. המידה שבה שיטות אלו מיושמות עשויה להשתנות, אך בכל מקרה הן יכולות ליצור בסיס חשוב לפיתוח היוזמה להסמכה בין־לאומית למוצרי סייבר. לא פחות חשובה מכך היא העובדה שישויות אלו כבר פיתחו תרחישים עיסקיים לחיזוק האבטחה של שרשרת האספקה שלהן, ובמקרים רבים הן גם משלמות יותר מתוך רצון לקבל מוצרים בטוחים יותר. יש ערך רב לאימוץ שיטות עבודה מומלצות כאלו.

תיאום ממורכז

מודלים פנימיים לניהול סיכונים בשרשרת האספקה דורשים שכל ארגון יפַתח ויַישם בנפרד תהליכי הסמכה משלו עבור מוצרים וספקים שמשמשים אותו. העלות הנדרשת לשם כך, במיוחד כאשר לוקחים בחשבון את המשאבים הדרושים ליישום ואימות, עשויה להיות גבוהה משמעותית לכל ארגון. אולם אימוץ יוזמת ההסמכה הבין־לאומית יאפשר לחלק עלויות אלו באופן יחסי בין כלל המשתתפים בה, ובכך לצמצם משמעותית את הכפילות במאמצים ובהשקעת משאבים. במקביל הוא יאפשר לתמרץ ולאפשר תהליכי הסמכה ואימות מקיפים הרבה יותר מאשר אלה המקובלים כיום.

הימנעות מאימוץ תקנים "מינימליסטיים"

תקנים שכוללים רק את אמצעי ניהול הסיכונים המינימליים, למרות היותם מועילים, אינם מספיקים כדי להשיג את האבטחה הנדרשת של שרשראות האספקה הגלובליות. חבר הקונגרס האמריקאי לאנגווין (Langevin) הדגיש כי "במקום לאמץ דפוס חשיבה המבוסס על ציות, המעודד את עשיית המינימום הדרוש", עלינו "לתמרץ כראוי את הארגונים לנקוט גישה מבוססת סיכונים לאבטחת הסייבר", כולל כלפי ניהול סיכונים בשרשרת האספקה.[108] באופן דומה, תוכנית AEP קוראת לממשלה ולתעשייה "לתמרץ את הפיתוח העיסקי והכלכלי בתגובה לחוסרים באבטחת שרשרת האספקה" ומתרחקת ממודל תגובתי לאבטחת סייבר לטובת מודל פרואקטיבי יותר, אשר "מכיר בקיום סיכונים מובנים ופוטנציאליים בשרשרת האספקה ומבקש לצמצמם".[109]

כדי להתמודד עם האיומים המתרבים בשרשרת האספקה, על יוזמת ההסמכה ליישם גישה לא רגולטורית, שתתמקד בהסמכה של שיטות עבודה מומלצות ולא בתקינה מינימלית וכללית. למען הסר ספק, האמצעים הרגולטוריים שנסקרו במאמר זה מספקים כולם בסיס חיוני ליכולותיו ולצורתו של חזון ההסמכה. עם זאת, היוזמה להסמכה בין־לאומית למוצרי סייבר אינה אמורה להחליף את התקנים כאמצעי לאבטחת שרשראות אספקה, אלא לספק לחברות השונות חלופות מהימנות, הטובות מסוגן, להבטחת שלמותה של שרשרת האספקה.

אי־אימוץ מודל המבוסס על תקנים יסייע ליוזמה המדוברת להימנע מליצור מבנה רגולטורי קשיח שיקשה על השגת המטרה. הדרישות של הרגולציה מתפתחות בהכרח הרבה יותר לאט מאשר האיומים שבהם הן נועדו לטפל, ונדיר שהן כוללות שיטות עבודה מומלצות. היוזמה להסמכה בין־לאומית למוצרי סייבר צריכה אמנם להיות תואמת לתוכניות ולדרישות הרגולציה, אך רצוי שהיא לא תהיה מוגבלת בגללן. הרעיון הוא שכל תהליכי ההסמכה במסגרת היוזמה יכללו סעיפים שיחייבו הערכה תקופתית ועדכונים, במטרה לתת מענה להערכות העדכניות ביותר ולאיומים המתפתחים.

בינאום היוזמה להסמכה בין־לאומית של מוצרי סייבר מתחילתה

לרוב המכריע של שרשראות האספקה בימינו יש טביעת רגל בין־לאומית. עם זאת, רוב התקנים והנחיות הרגולציה הם ספציפיים למדינה שהתקינה אותם. לדוגמה, כל היוזמות והמודלים שנסקרו במאמר זה, למעט "אמנת האמון" ותוכניות הסמכה ספציפיות לאבטחת סייבר, מתמקדים באופן בלעדי בארצות הברית (אם כי תקני

108 Williams, "DHS Developing Supply Chain Security Initiative".

109 "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector", p. 2.

התאגיד הצפון־אמריקאי לאמינות החשמל חלים גם על גופים העוסקים במתקני חשמל הרשומים בקנדה ומקסיקו). עם זאת, יוזמות חדשניות בנושא ניהול סיכונים בשרשרת האספקה מתפתחות גם בבריטניה, בישראל ובמדינות נוספות, וכדאי יהיה לשלב אותן ביוזמות האמריקאיות.

בינאום היוזמה של הסמכה של מוצרי סייבר יסייע בגיבוש הבסיס הנחוץ של משתמשים במוצר ושל לקוחותיו, ולהרחבתו. ניסיונות מצד רוסיה, סין ומדינות אחרות לנצל את הפגיעויות של שרשראות האספקה נושאים אופי רב־תחומי וגלובלי. גם היוזמה להסמכת מוצרי סייבר צריכה, לפיכך, לקבל אופי דומה.

מערכת רב־שכבתית

היוזמה להסמכה בין־לאומית של מוצרי סייבר תצטרך לשקול פיתוחה של מערכת הסמכת מוצר רב־שכבתית. מבנה רב־שכבתי כזה יכלול: (1) רמה בסיסית, שתהיה גבוהה מתְקני הרגולציה הקיימים, אך לא תגיע עד כדי הרמה "הטובה בקטגוריה"; (2) רמה גבוהה, שתקבע את התקן לדרישות הגבוהות ביותר בקטגוריה. למעשה, באמצעות מינוף תמריצי השוק והגעה לאלפי לקוחות מאובטחים במגוון תחומים, יש סיכוי שרמת "ההסמכה הגבוהה" תהיה טובה אף יותר מאשר "הטוב ביותר בקטגוריה".

תפקיד הממשלה

היוזמה להסמכה של מוצרי סייבר היא בבסיסה יוזמה של התעשייה, אך השתתפות ממשלתית בה תוכל להבטיח כי היא: (1) תפיק תועלת מניסיונם של מנהיגים בכירים; (2) תהיה תואמת באופן מרבי לצרכים של בעלי העניין; (3) תיהנה מאמינות אוטומטית בעיני אותם בעלי עניין; (4) תוכל להיות משולבת ביוזמות ממשלתיות קיימות; (5) תשלב בתוכה סדרי עדיפויות ממשלתיים כדי להפחית עלויות. שילוב פקידי ממשלה של המדינות המשתתפות ביוזמה יספק יתרון נוסף – גיוון בגישות ובפרספקטיבות – אם כי עשוי גם ליצור אתגרים, לאור רמות ההשפעה שהממשלות השונות מסוגלות להפעיל על חברות הפועלות במגזר הפרטי המקומי שלהן.

מסקנות

דיווחים של קהילת המודיעין, משרד ההגנה, המשרד לביטחון המולדת וגופים אחרים בממשל האמריקאי מצביעים על התפתחות רבה של הניסיונות לנצל את שרשראות האספקה ועל המרחקים אליהם הם שולחים את זרועותיהם, באופן שמקשה יותר ויותר על זיהום וחשיפתם. התעשייה והממשל האמריקאיים משלבים כוחות במאמץ משותף ואגרסיבי, כנדרש, כדי לנהל את הסיכונים בשרשרת האספקה בענף החשמל בפרט ובתחום האנרגיה בכלל.

היוזמה להסמכה בין־לאומית של מוצרי סייבר אינה אמורה "להמציא את הגלגל מחדש", או לשכפל מאמצים שכבר מתקיימים. במקום זאת, עליה להיבנות כך שהיא תספק תמיכה לתוכניות קיימות ותגשר על פערים הקיימים ביניהן, וזאת בדרכים ייחודיות שנובעות מהמבנה שהיא מציעה. באופן זה תתרום היוזמה באופן מרבי לחוסנן של תשתיות.

מאמר זה הציג סקירה קצרה של המאמצים הנמשכים בנושא ההתגוננות בסייבר, מתוך מטרה לסייע בדיונים עתידיים ולזהות תחומים חדשים שבהם תוכל היוזמה להסמכת מוצרי סייבר לתרום את התרומה המשמעותית ביותר. בעלים ומפעילים של תשתיות מתמקדים יותר ויותר ברכישת מוצרים נקיים מתוכנות זדוניות. יצירת תהליך של הסמכת מוצרי סייבר, שייעשה במימון ובפיקוח המגזר הפרטי, תוך תיאום עם גופים ממשלתיים, וכן רכישת מוצרים שיענו על התקנים שייקבעו, יאפשרו לבעלי תשתיות ולמפעיליהן לתרום בכך לשיפור התקנים המתהווים ולעודד את כוחות השוק, שהם חיוניים לשיפור ניהול הסיכונים בשרשראות האספקה.