אסטרטגיות לביטחון סייבר בתחום הבריאות בישראל ובהולנד: סקירה השוואתית

סטפן ווינק

הקצב המהיר של החידושים הטכנולוגיים יצר שורה של הזדמנויות לשינויים בתחום הבריאות. שינויים אלה משפרים את איכות החיים, אך גם יוצרים זירת הזדמנויות לפושעי סייבר. שירותי הבריאות מופקדים על בריאותם של האזרחים, אולם במקביל הם גם אחראים לא פעם לחלק משמעותי מהתפוקה הכלכלית הלאומית. הגברת הסיכונים בתחום ביטחון הסייבר בענף הבריאות המשתייך למערכת התשתיות הקריטיות, מציבה איום על הביטחון הלאומי ומחייבת תגובה ממשלתית. מאמר זה משווה בין האסטרטגיות והתקנות הלאומיות לביטחון סייבר של ישראל ושל הולנד, כחלק מאסטרטגיית ההגנה שלהן על ענף הבריאות מפני איומי סייבר, ומביא המלצות לאסטרטגיות ותקנות עתידיות בתחום זה.

מילות מפתח: ענף שירותי הבריאות, טכנולוגיה, תקנות ואסטרטגיה לאומית לביטחון סייבר, האינטרנט של הדברים הרפואיים (IoMT), תשתיות קריטיות

מבוא

תחום שירותי הבריאות נמנה על המגזרים הנהנים מההתפתחויות הטכנולוגיות המואצות.[1] ייעודו ופעילותו חיוניים לבריאותם של אנשים, ובמקרים מסוימים גם אחראים לחלק ניכר מהתפוקה הכלכלית הלאומית.[2] הטכנולוגיות המתפתחות

סטפן ווינק סיים תואר ראשון בלימודי ניהול אבטחה באוניברסיטת סאקסיון למדעים יישומיים בהולנד, ובעבר התמחה בתוכנית לביטחון סייבר של המכון למחקרי ביטחון לאומי.

1 Sanjay Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients", *Forbes*, April 2, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/04/02/health-care-innovation-harnessing-new-technologies-to-benefit-patients/#4d7afdf45a88.

2 "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities", *KPMG*, September 2015, pp. 1-6; "Critical Infrastructure Sectors", *US Department of Homeland Security (CISA)*, February 2, 2019, https://www.dhs.gov/cisa/critical-

והדיגיטציה ממלאות תפקיד מרכזי בפיתוח מוצרים, שירותים ומחקרים, לטובת החולים והספקים גם יחד. לשילוב של הגנטיקה והביולוגיה עם נתוני עתק (Big Data) ובינה מלאכותית, שזכה לכינוי "מהפכת האוטומציה והמידע הרפואיים", הייתה השפעה רבה על המחקר. שילוב זה חולל מהפכה בייצור תרופות, ברפואה מותאמת אישית ובסביבת העבודה הקלינית, ושינה את אופן האבחון והטיפול בחולים.[3]

בריאות דיגיטלית מגבירה את היעילות והאפקטיביות של מערכות רפואיות ומשפרת את ניהול המרשמים, את שירותי הבריאות מרחוק, את הפיקוח והמעקב ואת הפעולות הקליניות עצמן.[4] לדיגיטציה של מערכת הבריאות יש ערך מוסף, בכך שהיא מאפשרת את הגדלת המרחק הגיאוגרפי לטיפול בחולים. דוגמאות לכך הן המערכת הכירורגית "דה וינצ'י" ומערכות רובוטיות המסייעות למנתחים לבצע פעולות עדינות ממקומות שונים.[5] השילוב של טכנולוגיות מתפתחות, מערכות מידע, רשתות רפואיות ומכשור רפואי, המחוברים ביניהם בְּמה שמכונה "האינטרנט של הדברים הרפואיים" (Internet of Medical Things – IoMT), מתפתח באופן שהוא קריטי למערכות הבריאות ובה בעת עלול לשבש את פעילותן.[6]

סיכוני אבטחת סייבר בענף שירותי הבריאות

תוצר לוואי של ההתקדמות בתחום הבריאות הדיגיטלית הוא הסיכון המשותף למכשור רפואי, ל"אינטרנט של הדברים הרפואיים", ליישומים רפואיים דיגיטליים, לתוכנות, למערכות מידע ולהתקני אבטחה ("חומות אש" ואנטי וירוס).[7] התוצאה של סיכון כזה יכולה להיות פגיעה בנתונים, ובכלל זה בקניין רוחני של הארגון,

---

infrastructure-sectors; "Critical Infrastructure Sectors*", European Cooperation Network on Critical Infrastructure Protection (euconcip)*, March 15 2019, https://www.euconcip.org/; Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs* 3, no. 2 (2011): 61-78.

3 "2018-2019 Innovation in Israel Overview", *Israel Innovation Authority*, January 14, 2019, pp. 60-62; Poonen, "Health Care Innovation Harnessing New Technology to Benefit Patients".

4 "Connected Health, How Digital Technology Is Transforming Health and Social Care", *Deloitte Center for Health Solutions*, London, 2015, pp. 1-40; "2018-2019 Innovation in Israel Overview".

5 ראיון עם אליאב נ., 25 בנובמבר 2018.

6 Safi Oranski, "Obstacles on the Path to Comprehensive IoMT Security", *Cyber MDX*, November 26, 2018, https://www.cybermdx.com/blog/obstacles-on-the-path-to-comprehensive-iomt-security.

7 Aurore Le Bris and Walid El Asri, "State of Cybersecurity & Cyber Threats in Healthcare Organizations", *Journal of Strategic Threat Intelligence,* January 10, 2017,https://blogs.harvard.edu/cybersecurity/2017/01/10/cybersecurity-cyber-threats-in-healthcare-organizations/; Barbara Filkins, "Health Care Cyberthreat Report",

כמו מחקרים רפואיים, ניסויים וממצאים; פגיעה במידע כספי ובחיובים הקשורים להעברות כספים אלקטרוניות (EFT); פגיעה בפרטי מטופלים ובהיסטוריה הרפואית שלהם, הקשורים לרשומות רפואיות ממוחשבות (EHR) או לתיק רפואי ממוחשב (EMR).[8] בסופו של דבר, תהיה בכך פגיעה בפעילות של שירותי הבריאות ובשירות שהם נותנים, דבר שיגרום לעלויות נוספות כתוצאה מנזקים ומתביעות, וכל זאת תוך פגיעה ברווחת המטופלים.[9]

כדי להמחיש את פגיעויות האבטחה בתשתיות הרפואיות, פיתחו חוקרים במרכז לאבטחת סייבר באוניברסיטת בן גוריון תוכנה זדונית המנצלת פגיעויות של מכשירי הדמיה רפואיים, כגון מכונות CT ו־MRI, ושל הרשתות המעבדות את ההדמיות. במחקר נמצא כי סריקות ה־CT שעברו שינוי מכוון (המציג ממצאים סרטניים) הובילו רדיולוגים מנוסים לאבחן את המצב הרפואי בצורה שגויה.[10] ככל הידוע, תרחיש כזה טרם התממש במציאות ולא גרם נזקים או מוות. מרבית התקפות הסייבר על ענף הבריאות עד היום כללו פריצות לנתונים של רשומות רפואיות ממוחשבות, וזאת כתוצאה מנקודות תורפה ברשתות של בתי החולים, של ספקי שירותי בריאות כמו חברות ביטוח, או של גורמים הקשורים בשרשרת האספקה.[11]

רבע מכלל הפריצות למאגרי נתונים בארצות הברית מתרחש, לפי ההערכות, בענף הבריאות.[12] אחד המקרים הבולטים היה חשיפתה של קבוצה חדשה של האקרים, שזכתה לכינוי "תולעת כתומה" ("Orangeworm"). החשיפה נעשתה על ידי חברת Symantec בתחילת 2015, לאחר שההאקרים שתלו תוכנה זדונית מותאמת – Kwampirs – שכוונה נגד מחשבים של ספקי שירותי בריאות וספקים של צדדים שלישיים במספר מגזרים הנותנים שירותים לענף הבריאות. בדרך זו השיגה קבוצת ההאקרים גישה בלתי מורשית לרשומות רפואיות ממוחשבות ולמכשירי הדמיה רפואיים, כגון MRI וציוד רנטגן.[13]

SANS Institute and Norse, March 2014, pp. 1-42; "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities".

8 Ibid.

9 Ibid.

10 Kim Zetter, "Hospital Viruses: Fake Cancerous Nodes in CT Scans, Created by Malware, Trick Radiologists", *The Washington Post*, April 3, 2019, https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/.

11 Filkins, "State of Cybersecurity and Cyber Threats in Healthcare Organizations"; "Health Care Cyberthreat Report".

12 "Health Care Innovation Harnessing New Technology to Benefit Patients".

13 Jessica Davis, "New Hacking Group Targeting Healthcare Infects Mri, X-Ray Machine", *Healthcare IT News,* April 24, 2018, https://www.healthcareitnews.com/news/new-hacking-group-targeting-healthcare-infects-mri-x-ray-machine; Security

מתקפת "דיוג", שהתרחשה בשנת 2018 נגד חשבונות דוא"ל של עובדי חברת UnityPoint Health שבוויסקונסין, גרמה לפריצה לנתונים של 16,000 מטופלים. מתקפה עוקבת על המערכות העיסקיות של החברה הביאה לפריצה לנתונים של 1.4 מיליון מטופלים.[14] בשנת 2018 גם נפרץ מחשב של עובד בחברת Med Associates בניו יורק – ספקית של תביעות בנושאי בריאות – ונחשפו למעלה מ־270,000 רשומות של מטופלים.[15] באותה שנה נפגעו במיזורי Blue Springs Family Care, Cass Regional Medical Center, וכן LabCorp מהתקפות של תוכנות כופר, שמנעו מהמשתמשים גישה למערכות התקשורת שלהם ולרשומותיהם הממוחשבות.[16]

בשנים 2015־2018 פרצו האקרים, ששמו על הכוונת את מאגר הבריאות הממלכתי של סינגפור, לרשומות של 1.5 מיליון מטופלים, ובתוכם לפרטיו של ראש הממשלה לי סיאן לונג.[17] ביוני 2017 דווח על פריצה לרשתות המחשבים של שניים עד שלושה בתי חולים בישראל, אם כי מערך הסייבר הלאומי שלה אישר רק את דבר קיומן של שתי מתקפות. האירוע הביא להחלפת חמישים מחשבים מיושנים וחשופים לפגיעה.[18]

Response Attack Investigation Team, "New Orangeworm Attack Group Targets the Healthcare Sector in the U.S., Europe and Asia", *Symantec*, April 23, 2018, https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia.

14 Jessica Davis, "1.4 Million Patient Records Breached in Unitypoint Health Phishing Attack", *Healthcare IT News*, July 13, 2018, https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack.

15 Jessica Davis, "270,000 Patient Records Breached in Med Associates Hack", *Healthcare IT News,* June 20, 2018, https://www.healthcareitnews.com/news/270000-patient-records-breached-med-associates-hack.

16 Jessica Davis, "Update: Ransomware Attack on Cass Regional Shuts down HER," *Healthcare IT News*, July 11, 2018, https://www.healthcareitnews.com/news/update-ransomware-attack-cass-regional-shuts-down-ehr; Jessica Davis, "Ransomware, Malware Attack Breaches 45,000 Patient Records," *Healthcare IT News,* July 26, 2018, https://www.healthcareitnews.com/news/ransomware-malware-attack-breaches-45000-patient-records.

17 Jessica Davis, "Hackers Breach 1.5 Million Singapore Patient Records, Including the Prime Minister's," *Healthcare IT News*, July 20, 2018, https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers.

18 Globes Correspondent, "Cyber Attack Hits Israeli Hospitals", *Globes*, June 29, 2017, https://en.globes.co.il/en/article-cyber-attack-hits-israeli-hospitals-1001194803 ; Judy Siegel-Itzkovich and Sharon Udasin, "Cyber Attacks Hit Israeli Hospitals as Globe Battles New Computer Virus", *The Jerusalem Post*, June 29, 2017, https://www.jpost.com/Israel-News/Israel-thwarts-hackers-from-cyber-attack-on-hospitals-498256.

הרגולציה בענף הבריאות בישראל ובהולנד

ביטחון הסייבר של מערכות הבריאות בישראל היה אחד הנושאים שנדונו במהלך סמינר ה"סייבר־מד", שהתקיים במסגרת כנס "סייבר־טק" בתל אביב בינואר 2019. מסקנת הדיון הייתה כי ביטחון הסייבר של מערכות הבריאות בישראל נמצא "מתחת לקו הבריאות" וכי אינו מוכן לאיום המתפתח על רשתות התקשורת, המכשור הרפואי והארגונים המספקים שירותים רפואיים. לדברי מנהל בית החולים האוניברסיטאי "הדסה", התשתיות הקריטיות החיוניות מותאמות לתקנים, אולם מרכיבים אחרים, כגון התקנים מרחוק, זוכים לאבטחת סייבר ברמה שהיא פחות חסינה. המעבר לבריאות דיגיטלית, הנובע מהטכנולוגיות החדשות ומהאפשרות ליצור שילוביות, הציב אתגרים חדשים רחבי היקף, המאיימים על המוניטין של ארגוני הבריאות.[19]

לשם השוואה, 56 אחוזים מבתי החולים בהולנד עמדו בשנת 2015 בתקנים לאבטחת מידע בענף הבריאות (NEN–7510120).[20] אמצעי האבטחה הפכו למחייבים מאז מאי 2017, וציות להם הוא תנאי הכרחי לקבלת גישה למספרי השירות של אזרחים בכל ענף הבריאות ההולנדי.

מספרן העולה של מתקפות סייבר נגד רשתות והתקנים בכל תחום התשתיות הקריטיות מסַכן את השירותים גם בתחום הבריאות ואת האמון בספקים של שירותי הבריאות. מתקפות אלו הובילו ליוזמות לשיפור החוסן והעמידות של הארגונים בכל תחומי הבריאות, כולל בארגונים המשרתים את ענף הבריאות, ולגיבושה של אסטרטגיה לאומית לביטחון סייבר.

אסטרטגיות לאומיות לביטחון סייבר

ביטחון סייבר הפך לחלק אינטגרלי מהאבטחה הארגונית ומוגדר על ידי תאגיד הטכנולוגיה CISCO כ"שיטה להגנה על מערכות, רשתות ותוכניות מפני התקפות דיגיטליות".[21] בשנת 2011 הוצג בכנס הבין־לאומי לביטחון תשתיות של מידע קריטי (CRITIS) מחקר השוואתי בין עשר אסטרטגיות לאומיות לביטחון סייבר. לפי המחקר, חסרה הגדרה משותפת לביטחון סייבר ברמה האירופית והבין־לאומית.[22]

19 Ami Rojkes Dombe, "CyberMed: Cyber Threats and Challenges in Healthcare", *Israel Defense*, January 28, 2019, https://www.israeldefense.co.il/en/node/37255.

20 "Cyber Security Risk Assessment (CSRA) for the Economy", *CPB Netherlands Bureau for Economic Policy Analysis*, 2017.

21 "What is Cybersecurity", *CISCO*, December 2, 2018, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

22 H.A.M. Luiijf, Kim Besseling, Maartje Spoelstra and Patrick de Graaf, "Ten National Cyber Security Strategies: A Comparison", in *Critical Information Infrastructure Security,* ed. Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis and Stephen Wolthusen (Berlin: Springer, 2013), pp. 1-17.

גיבוש אסטרטגיות ביטחון לאומי במסגרת האיחוד האירופי הוא תופעה חדשה יחסית, וראשיתה בתחילת שנות האלפיים. קביעת אסטרטגיות לאומיות כאלו מעודדת קובעי מדיניות להגדיר יעדים אסטרטגיים ולנסח הנחיות כיצד להגיע אליהם. אמירה ידועה בעולם האבטחה גורסת כי "חוזק ביטחון הסייבר הוא כחוזק החוליה החלשה ביותר".[23] ארגון יכול להיות בעל מערכת ביטחון סייבר מצוינת, ועדיין לסבול מחוסר יעילות אם אין לו מערכת ניהול סיכונים מקיפה בתחום זה.[24] ההתפתחויות בנושא ביטחון סייבר – שרשרת האירועים שזירזו את קבלת ההחלטות בנושאי הסייבר בהולנד ובישראל – זקוקות להבהרות כדי להבין טוב יותר את מהותן של אסטרטגיות ביטחון הסייבר בשתי המדינות. השוואת שתי האסטרטגיות שתובא להלן תתמקד באופן שבו הולנד וישראל מתמודדות עם אתגרי ביטחון הסייבר ובדרך שבה שתי המדינות מגדירות מהם הנכסים הרלוונטיים למדיניות ביטחון הסייבר שלהן.

הקריטריונים שלהלן מבוססים על הנושאים המרכזיים שמופיעים במדריך NCSS Good Practice Guide[25] ועל המחקר שנערך על ידי Luiijf ואחרים,[26] וישמשו להשוואת האסטרטגיות הלאומיות לביטחון הסייבר של ישראל והולנד. סוגיית המפתח הראשונה היא **משטר סיכונים ברמה האסטרטגית והלאומית,** כאשר אחת האסטרטגיות היא יצירת תוכנית־אב כוללת המפרטת כיצד יושגו המשימה והיעדים. סוגיית המפתח השנייה היא **הסביבה הרגולטורית הלאומית**, שהיא חלק מהאסטרטגיה הלאומית הכוללת של ממשלות. סוגיית המפתח השלישית היא **בעלי העניין העיקריים באסטרטגיות הלאומיות לביטחון סייבר**, וכוללת מידע על סביבת בעלי העניין המייצגים תחומים רבים ומעורבים בתהליך פיתוחה של האסטרטגיה הלאומית לביטחון הסייבר. סוגיית המפתח הרביעית היא **הגדרת תשתיות קריטיות ואובייקטים קריטיים**. סוגיית המפתח החמישית והאחרונה היא **מודיעין סייבר ומודעות לביטחון סייבר**. להלן יתייחס המאמר לפעילויות של סוכנויות ביון וגופים ממשלתיים בתחום הסייבר ולקשר שלהן למשאבים

23 Niels Nagelhus Schia, "'Teach a Person How To Surf': Cyber Security as Development Assistance", *Norwegian Institute of International Affairs,* Report no. 4, 2016, pp. 1-36.

24 Gabi Siboni and Hadas Klein, "Guidelines for the Management of Cyber Risks", *Cyber, Intelligence and Security* 2, no. 2 (2018): 23-38.

25 European Union Agency for Network and Information Security (ENISA), NCSS Good Practice Guide, *Designing and Implementing National Cyber Security Strategies* (Heraklion: ENISA, 2016), pp. 1-59.

26 H.A.M. Luiijf, Kim Beseling, Maartje Spoelstra and Patrick de Graaf, "Ten National Cyber Security Strategies: A Comparison", in: *Critical Information Infrastructure Security*, ed. Sandro Bologna, Bernhard Hammerli, Dimitris Gritzalis and Stephen Wolthusen (Berlin: Springer,2013), pp.1-17.

העומדים לרשותם של מוסדות הבריאות, במטרה להגביר את המודעות לביטחון סייבר ברמה הלאומית.

א. משטר ניהול סיכונים סיכונים ברמה אסטרטגית ולאומית

סוגיית המפתח הראשונה לניתוח אסטרטגיית ביטחון סייבר לאומית היא משטר סיכונים (Risk Governance). משטר ניהול סיכונים מציע לארגונים ולמדינות יתרונות והזדמנויות ומאפשר לארגונים ולסביבתם להשתנות, תוך צמצום התוצאות השליליות של הסיכונים הנלווים.

משטר ניהול סיכונים בישראל

משטר ניהול הסיכונים בישראל עבר במהלך העשור האחרון מהתמקדות ראשונית בהגנה על תשתיות מידע ומאגרי מידע ממוחשבים, כפי שקבעה הרגולציה, לגישה ישירה יותר של הגנה על מרחב הסייבר בעזרת אינטראקציות אסטרטגיות אזרחיות־צבאיות ושיתופי פעולה ציבוריים־פרטיים.[27] ארגונים מתמודדים עם אתגרים רבים במערכות הסייבר, ובמקביל יש תוכניות אקדמיות וממשלתיות שיוזמות ומפתחות פעולות ופתרונות טכניים חדשים לשיפור אמצעי הנגד והתגובה להתקפות סייבר.[28] כך, בשנת 2016 הטמיעו מערך הסייבר הלאומי ומשרד הבריאות את מערכת MedSOC – מרכז לפעולות אבטחה עבור תעשיית הרפואה. MedSOC עוקבת אחרי מתקפות בתחום הבריאות ומפרסמת מידע רלוונטי ברשת שלה. הפורטל של MedSOC נתמך על ידי צוות החירום לטיפול באירועי מחשב (CERT-IL), הכפוף למערך הסייבר הלאומי.[29]

הרגולציה המקומית בישראל מתבססת על תקנים בין־לאומיים, וזאת בהתאם להחלטת הממשלה 2443 "לקדם רגולציה לאומית והובלה ממשלתית בתחום ביטחון הסייבר". ככלל, כל הארגונים בישראל מתבקשים או נדרשים לעמוד בתקנים ISO/IEC 27001 ו־ISO 15408, החלים על "ארגונים ומערכות ניהול אבטחת מידע" ועל "מדדי הערכה לאבטחת טכנולוגיות מידע" בהתאמה.[30] ארגונים

27 Michael Raska, "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy", *S. Rajaratnam School of International Studies, Singapore*, January 2015, https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

28 "Cyber Security Risk Governance", *International Risk Governance Council*, October 2015, pp 1-33.

29 ראיון עם אליאב נ., 25 בנובמבר 2018.

30 Eli Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through", *Yigal Arnon & Co. Law Firm*, February 1, 2018, https://www.arnon.co.il/member/4358/articles; "ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements", *ISO*, October 2013, https://

ייעודיים נדרשים לנקוט אמצעים נוספים, המבוססים על קריטריונים המתייחסים לתשתיות קריטיות ברמה הלאומית ולהנחיות הגוף הרגולטורי. בשנת 2012 פרסם משרד הבריאות חוזר מס' 18/2012, המורה לכל ארגוני הבריאות וספקי השירותים הנלווים לעמוד בתקן ISO 27799. החוזר הציג פרמטרים ביחס ל"סביבת סיכון אבטחת המידע" של הארגון בעת "בחירה, יישום וניהול בקרות" הנוגעים ל"תקני אבטחת מידע ארגוניים ושיטות ניהול אבטחת מידע".[31] משרד הבריאות פיתח, יחד עם מכון התקנים הישראלי, מערכת הסמכה מתקדמת בשירותי הבריאות, המאמצת קריטריונים נוספים של מכון התקנים.[32]

ציוד רפואי מיוצר עם מערכות נעולות, וכך מונע גישה למערכות ההפעלה שלו. מערך הסייבר הלאומי מנהל מעבדת מחקר רפואי, יחד עם בית החולים איכילוב, לבדיקת תקני איכות למכשור רפואי (לפי הנחיות ממשלתיות). המערך מספק את הידע והציוד, ואילו בית החולים איכילוב מספק את סביבת הבדיקות. הפעילות כוללת מבחני חדירה, קישוריות רשת וזיהוי פגיעויות וחולשות.[33]

משטר ניהול סיכונים בהולנד

בשנת 2018 הוקם בהולנד ארגון Z-CERT, כמענה להזדמנויות ולסיכונים שיתפתחו כתוצאה מהדיגיטציה של ענף הבריאות, וכן כמענה לאתגרים אחרים הנוגעים לפרטיות הנתונים ול"אינטרנט של הדברים" (IoT).[34] Z-CERT הוא חלק מיוזמה של איגוד בתי החולים בהולנד (Nederlandse Vereniging van Ziekenhuizen), הפדרציה ההולנדית של המרכזים הרפואיים האוניברסיטאיים (Nederlandse Federatie van Universitair Medische Centra), שירות הבריאות הכללי של הולנד והמרכז הלאומי לביטחון סייבר בהולנד (NCSC). Z-CERT מציע שירותי מומחים למוסדות הבריאות בהולנד ועושה זאת בעזרת אספקת ידע מעמיק על רשתות רפואיות, יישומים רפואיים ומכשירים רפואיים.[35] מכשירים רפואיים חייבים לעבור הערכה לפני הוצאתם לשוק בהולנד, במטרה לקבוע אם יוצרו בהתאם לדרישות

---

www.iso.org/standard/54534.html; "ISO/IEC 15408–1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model", *ISO*, January 2014, https://www.iso.org/standard/50341.html.

31 Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal through"; "ISO 27799:2008 Health informatics – information security management in health using ISO/IEC 27002", *ISO*, July 2008, https://www.iso.org/standard/41298.html; "ISO 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002", *ISO*, July 2016, https://www.iso.org/standard/62777.html.

32 ראיון עם יניב פ., 6 בינואר 2019.

33 ראיון עם אליאב נ., 25 בנובמבר 2018.

34 ראיון עם הסל ב., 17 בדצמבר 2018.

35 שם.

של צו EEG/93/42 וצו EC/2007/47 העוסקים במכשור רפואי. פיתוח של מכשור רפואי מתוכנן ברובו כך שישמור על עקרונות הפרטיות והאבטחה. פירוש הדבר הוא שהחברה המַפתחת את המכשירים הרפואיים וגם הגורמים המשולבים בשרשרת האספקה צריכים להקדיש תשומת לב לאמצעים משפרי פרטיות, המכונים גם "טכנולוגיות משפרות פרטיות" (PET).[36] אבטחת המידע היא באחריות של כל מוסד בריאות. התקנים NEN 7510 ו־NEN 7512, שבתי החולים בהולנד חייבים לעמוד בהם, מבטיחים שיושגו הרמות הדרושות של אבטחת מידע ופרטיות. מלבד הַתקנים הסטטוטוריים, כל בית חולים צריך להחליט איזה תקן מתאים לסביבת הסיכון שלו.[37]

ב. הסביבה הרגולטורית הלאומית

ממשלות קובעות רגולציות שמחייבות את ענף הבריאות ליישם אמצעי ביטחון סייבר הולמים כדי להסדיר ולחזק את אמצעי ביטחון הסייבר בתחום הבריאות. יישום הרגולציות בענף הבריאות על ידי הטלת האחריות על הארגונים – תוצאה של עלייה במספר התביעות והקנסות של סוכנויות ממשלתיות על אי־ציות – מביא לשיתוף פעולה רחב יותר.

הרגולציה בישראל

כדי להבטיח שארגונים ציבוריים ופרטיים יוכלו לפעול לנוכח איומי ביטחון הסייבר, יש צורך להקים סביבה רגולטורית (בין־)לאומית ו/או מסגרת מדיניות מתאימה, שיבצעו לעיתים קרובות הערכות תכופות של אסטרטגיות ויעדים בתחום ביטחון הסייבר ויעדכנו אותם בהתאם. ישראל נקטה מאז 1981 מספר מהלכים וחוקקה חוקים להגנת הפרטיות וביטחון הסייבר, במטרה להתמודד באופן כללי עם בעיית ההגנה על הפרטיות. החוקים והמהלכים העיקריים בתחום זה הם חוק הגנת הפרטיות משנת 1981;[38] התיקון לחוק הגנת הפרטיות משנת 2001;[39] החלטת הממשלה 3611 לקידום יכולות הסייבר הלאומיות משנת 2011;[40] החלטת הממשלה 2444 לקידום המוכנות הלאומית לביטחון הסייבר משנת 2015.[41] בשנת 2018 פרסמה ממשלת ישראל טיוטה לחוק ביטחון סייבר והוציאה "קול קורא" לציבור לבקש

36 שם.

37 שם.

38 Ian Bourne, "A Guide to Data Protection in Israel", *Israeli Law, Information and Technology Authority (ILITA)*, January 2010.

39 Ibid.

40 "Resolution 3611 – Advancing National Cyberspace Capabilities", *Israel's Prime Minister's Office*, August 7, 2011, pp. 1-6.

41 Deborah Couriel-Housen, "Israel: Organization Security Cyber National", *Cyber Defense Center of Excellence NATO* 2. no, 4 (February 2017): 12-1.

את הערותיו לטיוטה. הצעת החוק מסכמת שנים של התייעצויות ודיונים בשאלת הגישה לביטחון סייבר בישראל ומשלבת מספר חידושים בחקיקה ובמדיניות בנושא זה.[42]

חוק הגנת הפרטיות מהווה את החקיקה העיקרית להגנת מידע בישראל. לחוק שני מרכיבים: הראשון הוא ההגנה על הפרטיות באופן כללי, והשני עוסק ספציפית במאגרי מידע וקרוב הרבה יותר לחוקי הגנת נתונים מסוג "מידע".[43] החוק התפתח עם הזמן ועבר, מאז שהתקבל לראשונה ב־1981, תשעה תיקונים. בשנת 2001 התווספו אליו תקנות ברוח המונחים האירופיים להגנת מידע, באופן שמגביר את התאמתו לתקנים האירופיים.

הרשות הישראלית למשפט, טכנולוגיה ומידע (רמו"ט, כיום הרשות להגנת הפרטיות) הוקמה בספטמבר 2006 כחלק ממשרד המשפטים, מכוח החלטת הממשלה 4660. משימת הרשות היא לחזק את ההגנה על מידע אישי, להסדיר את השימוש בחתימות אלקטרוניות ולהגביר את האכיפה בתחומי הגנת הפרטיות ועבירות הקשורות לטכנולוגיות מידע. הרשות להגנת הפרטיות פועלת גם כבסיס ידע מרכזי של הממשלה לחקיקה הקשורה לטכנולוגיה ולפרויקטים גדולים של IT, כמו eGov.[44] כאמור, בשנת 2011 קיבלה הממשלה את החלטה 3611 העוסקת בהקמת מערך הסייבר הלאומי, וזאת במטרה לחזק את ההגנה על תשתיות לאומיות קריטיות ולהסדיר סמכויות ותחומי אחריות בתחום הסייבר.[45]

כאמור, בשנת 2012 גם פרסם משרד הבריאות את חוזר 18/2012. החוזר מחייב את כל מוסדות הבריאות בישראל לקבל הסמכה של תקן ISO 27799, ואת כל ספקי השירות המחזיקים במידע רפואי, או במידע הנוגע לתשתית המוסד הבריאותי, לעמוד באותו תקן.[46]

הרגולציה בהולנד

כדי להבין את החוקים ההולנדיים העוסקים בפשעי סייבר ובאבטחת מידע, יש לסקור את ההיסטוריה של החקיקה ההולנדית שהובילה לסביבה הרגולטורית (הבין־) לאומית ו/או למדיניות הנוכחית של הולנד בנושאים אלה. החוקים המרכזיים הנוגעים לפשעי סייבר שנחקקו בהולנד הם חוק פשעי מחשב (Wet computercriminaliteit)

---

42 Deborah Housen-Couriel, "A Look at Israel's New Draft Cybersecurity Law", *Net Politics*, *Council on Foreign Relations*, August 5, 2018, https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law.

43 Bourne, "A Guide to Data Protection in Israel".

44 Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through".

45 "Resolution 3611 – Advancing National Cyberspace Capabilities".

46 ראיון עם אליאב נ„ 25 בנובמבר 2018; Greenbaum, "Israel Chapter on Cybersecurity – Getting the Deal Through".

משנת 1993[47] וחוק פשעי מחשב II (Wet computercriminaliteit II) משנת 2006, וכן התיקון האחרון לו, שהביא לחקיקת חוק פשעי מחשב III.[48]

לכאורה, ניתן להעמיד לדין בהולנד בגין הפרת פרטיות מידע או הפרת הגנה על מידע על בסיס התערבות בנתונים, לפי סעיף 350a של החוק הפלילי ההולנדי.[49] למעשה, אין בחוק הפלילי ההולנדי פירוט שמתייחס באופן ספציפי להפרות הקשורות להגנת מידע. חוק רלוונטי נוסף הוא חוק הגנת המידע (Wet bescherming persoonsgegevens) משנת 2000,[50] הנאכף בעיקר על ידי אמצעים מינהליים שקבעה הממשלה. החוק עודכן בשנת 2015 כדי להבטיח שארגונים ידווחו על דליפת נתונים, וכן כדרך להרחיב את הסמכות המינהלית של המועצה ההולנדית להגנת המידע (College bescherming persoonsgegevens).[51]

ברמה הבין־לאומית, הולנד, כחברה באיחוד האירופי, מיישמת את "החלטת המסגרת JHA/2005/222 של מועצת אירופה... בנושא התקפות על מערכות מידע", מפברואר 2005. ריבוי ההתקפות על מערכות מידע והתגברות האיומים של פשע מאורגן הביאו את האיחוד האירופי להחליף באוגוסט 2013 את "החלטת המסגרת" ב"דירקטיבה EU/2013/40... בנושא התקפות על מערכות מידע".[52]

החקיקה הראשונה של האיחוד האירופי שהתמקדה באופן ספציפי בביטחון סייבר נקראת "הדירקטיבה בנושא אבטחת מערכות מידע ורשת" (דירקטיבה NIS). היא כוללת אמצעים חוקיים להגברת הרמה הכוללת של ביטחון הסייבר ולסנכרון המדיניות בנושא ביטחון סייבר בין המדינות החברות באיחוד, כשהמטרה הסופית היא לתמוך בחברה ובכלכלה של אותן מדינות על ידי שיפור המוכנות הדיגיטלית וצמצום עד למינימום של אירועי סייבר.

---

47 "Computer Crime Act", *Government of the Netherlands: Ministry of Justice and Security*, October 28, 1993, pp. 1-33 (in Dutch).

48 "Computer Crime Act II", *The Government of the Netherlands: Ministry of Justice,* July 4, 2006, pp. 1-2 (in Dutch); "Computer Crime Act", *The Government of the Netherlands: Ministry of Justice and Security*; October 8, 2018, pp. 1-33 (in Dutch).

49 "Dutch Criminal Code", *Official Publication of the Kingdom of the Netherlands*, April 22, 2015, p. 165 (in Dutch).

50 "The Data Protection Act", *Official Publication of the Kingdom of the Netherlands*, July 6, 2000, pp. 1-25 (in Dutch).

51 "Amendment of the Data Protection Act", *Official Publication of the Kingdom of the Netherlands*, June 4, 2015, pp. 1-8 (in Dutch).

52 "Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems", *Official Journal of the European Union*, March 16, 2005, pp. 67-71; "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA", *Official Journal of the European Union*, August 14, 2013, pp. 8-14.

"הרגולציה הכללית להגנה על מידע" (GDPR) של האיחוד האירופי אושרה סופית בפרלמנט האיחוד ב־14 באפריל 2016, לאחר הכנות שנמשכו ארבע שנים. מטרת הרגולציה היא להגן על כל אזרחי האיחוד האירופי מפני הפרות של פרטיות ופריצות לנתונים. ההבדל העיקרי בין הרגולציה החדשה ובין הדירקטיבה הקודמת הוא בסמכות השיפוט המורחבת שנכללת ברגולציה ומתפרסת על פני כלל מדינות האיחוד האירופי, וכן הקנסות על ארגונים שיפרו אותה.[53]

כל גוף ממשלתי או ארגון ציבורי באיחוד האירופי, שעוסק בבקרה או בפיקוח, נדרש למנות קצין אבטחת מידע (DPO), וזאת במקרים שבהם הפיקוח כולל מעקב קבוע, שיטתי ובקנה מידה גדול אחר אנשים, או כאשר מתקיים פיקוח בהיקף נרחב על מידע אישי רגיש.[54] מינוי קצין אבטחת מידע בהולנד הוא חובה רק אם הארגון ההולנדי עומד בדרישות הרגולציה החדשה.

ג. בעלי עניין עיקריים באסטרטגיה לאומית לביטחון סייבר

יש חשיבות לדעת מיהם בעלי העניין הרלוונטיים בענף הבריאות המעורבים בתהליכים המרכזיים במוסדות הבריאות השונים. אסטרטגיות לאומיות לביטחון סייבר, המשכילות לערב בעלי עניין רלוונטיים, ישיגו מודעות אופטימלית למצב, וכתוצאה מכך יגדילו את התשואות של כל הגורמים המעורבים באותה אסטרטגיה.[55]

בעלי העניין בישראל

ישראל היא מחלוצות שיתופי הפעולה עם בעלי עניין בנושאי ביטחון סייבר. אלה כוללים מוסדות ממשלתיים, את האקדמיה וארגונים במגזר הפרטי. שיתוף פעולה בנושא ביטחון סייבר הוא הרחבה טבעית של דפוס שיתוף פעולה לאומי שכבר קיים בתחומים אחרים,[56] ובא לידי ביטוי באחת מיוזמות הדגל של ישראל – פרויקט "יוזמת החדשנות" (CyberSpark) בבאר שבע. תהליך זה כולל מספר רב של בעלי עניין ומאפשר להפגיש ביחד את השחקנים הרלוונטיים. ההקשר וההיקף של התהליך האסטרטגי, ובפרט הבמה שעליה הוא מתרחש, מסייעים מאוד לקביעת הפרופיל של בעלי העניין.

---

53 "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", *Official Journal of the European Union*, May 4, 2016, pp. 1-88.

54 Global Legal Group, "The International Comparative Legal Guide to: Data Protection 2018", *Global Legal Group*, 2018.

55 Alexander Klimburg, ed. *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE 2012).

56 Housen-Couriel, "A Look at Israel's New Draft Cybersecurity Law".

הארגון האחראי על פיתוח אסטרטגיות לביטחון סייבר בישראל הוא מערך הסייבר הלאומי, הכולל בעלי עניין משלוש קטגוריות: הרמה הלאומית, המרחב האזרחי וארגונים לאומיים ובין־לאומיים. כל אלה רלוונטיים למטרה אותה נועדה לשרת האסטרטגיה. הרמה הלאומית מורכבת ממשרדי ממשלה ומסוכנויות בעלי ידע וקשר לתעשיית הבריאות, לחקיקה ולביטחון הסייבר; בעלי עניין מהמרחב האזרחי כוללים את משטרת ישראל ויחידת הסייבר הלאומי שלה, לצד גורמים מהאקדמיה; המרחב הלאומי והבין־לאומי כולל, בין השאר, מוסדות בריאות, ארגונים לשירותי בריאות (קופות החולים) וארגוני תקינה בין־לאומיים. בעלי העניין "הפנימיים" כוללים מנהלי אבטחת מידע ראשיים (CISO), נציגים מחטיבות ה־IT ואת ההנהלה של מוסדות הבריאות.

ענף הבריאות הישראלי מתמודד עם כמה תקנים בין־לאומיים הקשורים לאבטחת מידע ברשת. משום כך, יש תועלת בעירוב שחקנים מתחומי אחריות וידע אחרים בעת הכנת אסטרטגיה לאומית לביטחון סייבר עבור תחום הבריאות.

בעלי העניין בהולנד

האסטרטגיה הלאומית של הולנד לביטחון סייבר 2 (NCSS2) גובשה על ידי הקבינט ההולנדי ביחד עם מגוון רחב של ארגונים ציבוריים ופרטיים, מוסדות ידע וארגוני חברה אזרחית. אסטרטגיית NCSS2 מאפשרת לממשלת הולנד לגבש גישה משולבת לפשעי סייבר, עליה היא התחייבה בהסכם הקואליציוני. ב־1 בינואר 2012 הוקמה בהולנד "המועצה לביטחון סייבר" (CSR), שהיא גוף מייעץ עצמאי, המורכב מהקבינט ההולנדי ומנציגים בכירים מארגונים ציבוריים ומהמגזר הפרטי.[57]

ממשלת הולנד יכולה כיום לסמוך על מגוון רחב של שותפויות ציבוריות־פרטיות שיגבשו אסטרטגיית ביטחון סייבר מקיפה לתחום שירותי הבריאות בעתיד. שני גופים – "המרכז ההולנדי לשיתוף וניתוח מידע בתחום הבריאות" (ISAC) ו־Z-CERT – מבטיחים כי ענף שירותי הבריאות בהולנד יהיה מוגן טוב יותר, וזאת בזכות שיתוף המידע, בין היתר בתחומים של התקפות סייבר בין־מגזריות ומגמות מתפתחות בתחום יכולות הסייבר.

יעד נוסף באסטרטגיית ביטחון הסייבר הלאומית של הולנד הוא "דיפלומטיית סייבר". מטרתה היא לפתח מרכז של מומחיות בתחום המשפט הבין־לאומי וביטחון הסייבר, שיקדם שימוש חיובי במרחב הדיגיטלי. המרכז יאגד מומחים וקובעי מדיניות בין־לאומיים, דיפלומטים, אנשי צבא וארגונים לא־ממשלתיים,

57 "The National Cyber Security Center (NCSC) bundles knowledge and expertise", *Government of the Netherlands*, January 12, 2012, https://www.government.nl/latest/news/2012/01/12/the-national-cyber-security-center-ncsc-bundles-knowledge-and-expertise.

וזאת במטרה לחלוק ידע עם גופים קיימים. המומחים הבין־לאומיים יכללו גם כאלה החברים ב"מרכז האירופי לפשעי סייבר" (EC3 – Europol) וב"קומפלקס הבין־לאומי לחדשנות של האינטרפול" (Interpol Global Complex for Innovation – IGCI), המשַמש לפיתוח מחקרים בתחום זה.[58]

ד. תשתיות קריטיות ואובייקטים קריטיים

זיהוי נכון של נכסי הארגון חשוב לא רק מנקודת מבט עיסקית אסטרטגית, אלא גם מהיבט של אבטחה, ובכלל זה אבטחה בסייבר. אפשר להגדיר נכסים כמשאבים וכיכולות מוחשיים ובלתי מוחשיים, המאפשרים לארגון להשיג את יעדיו האסטרטגיים.[59]

התשתית הקריטית בישראל

ביוני 2017 גיבשה "הרשות הלאומית להגנת סייבר" במשרד ראש הממשלה את "המתודולוגיה להגנת סייבר בארגונים". הגנה על ארגונים היא מרכיב בתפיסת ההגנה הלאומית של ישראל, המתמקדת בהגנה על הכלכלה הישראלית והמרכיבים החיוניים שלה כנגד כל הפרעה. המסמך של "הרשות הלאומית להגנת סייבר" מנחה ארגונים כיצד להגדיר ולמפות את נכסיהם, לבצע הערכת סיכונים ולבדוק את מערכות ביטחון הסייבר שלהם. האסטרטגיה הלאומית לביטחון סייבר בישראל מתמקדת בצורה ברורה במיפוי הנכסים הקריטיים והמשניים של ארגון והקשר שלהם לספקים. שרשרת האספקה היא אחד הסיכונים הגדולים ביותר עבור ארגון. מכיוון שהתלות בצדדים שלישיים הופכת לקריטית גם בענף הבריאות בישראל, ארגונים הקשורים לתחום זה חייבים לשפר ולהתאים את תהליכי ניהול הסיכונים שלהם.

מהערכת סיכונים של מוסדות הבריאות שערך משרד הבריאות עלה כי מוסדות מסוימים תלויים במערכות רבות, שכולן נתמכות על ידי ספק חיצוני אחד (צד שלישי או ספק). כמו כן מצא משרד הבריאות כי מרבית בתי החולים בישראל משתמשים במערכת של אותו ספק.[60] לפי נציג של "הרשות הלאומית להגנת סייבר", מערך הסייבר הלאומי מכין, ביחד עם מספר בעלי עניין, אסטרטגיית סייבר ספציפית לתחום הבריאות, כדי להתמודד עם האיום הגובר של התקפות סייבר בענף הבריאות".[61]

---

58 Annegret Bendiek, "The European Union's Foreign Policy Toolbox in International Cyber Diplomacy", *Cyber, Intelligence and Security* 2, no. 3 (2018): 57-71.

59 Mark Frigo and James Hurley, "Understanding Your Organization's Genuine Assets", *Strategic Finance*, February 2014.

60 ראיון עם יניב פ., 6 בינואר 2019.

61 ראיון עם אליאב נ., 25 בנובמבר 2018.

התשתית הקריטית בהולנד

אסטרטגיית ביטחון הסייבר הלאומית של הולנד פותחה כדי לגבש מודל משטר מוגדר היטב, שיהיה בו איזון דינמי בין ביטחון, חופש ותועלת חברתית־כלכלית. במקביל, ממשלת הולנד ביקשה להתאים את תחומי האחריות של אבטחה פיזית גם על אבטחת הסייבר, והיא מתכוונת לעשות זאת על ידי דו־שיח עם ארגונים המתמודדים עם איומי סייבר.

נכון להיום, ממשלת הולנד אינה פועלת ליצירת התנאים ולגיבוש האמצעים לביטחון סייבר בתחום של שרשרת האספקה לעסקים או לענף הבריאות. יחד עם זאת, הצעת החקיקה האירופית יוצרת את התנאים והאמצעים שיוכלו לחול על מוצרים ושירותים של טכנולוגיות מידע ותקשורת גם בהולנד.[62] יתרה מכך, נכון להיום אין בהולנד אסטרטגיית ביטחון סייבר ספציפית להגנה על מוסדות המספקים שירותי בריאות מפני מתקפות סייבר. למרות זאת, ניתן לסכם ולומר כי מנקודת מבט לאומית הולנדית, החקיקה, התקנים והרשויות להגנת המידע של הולנד ושל האיחוד האירופי יוצרים את שכבת ההגנה הנדרשת מפני איומי סייבר על ענף הבריאות ההולנדי.

ה. מודיעין סייבר ומודעות לאבטחת סייבר

הן ישראל והן הולנד מתמקדות במודיעין סייבר ובמודעות לביטחון סייבר בתשתיות קריטיות כחלק ממאמציהן להילחם באיומי סייבר ולהגביר את המודעות אליהם בקרב הארגונים. הסיבה לכך היא ששתי המדינות התחילו להפנים את המטרות שמאחורי התקפות סייבר מתוחכמות ומזיקות ואת השפעותיהן על תשתיות קריטיות.

מודיעין סייבר ומודעות לאבטחת סייבר בישראל

ענף הבריאות בישראל בכללותו לא הגיע לרמה המיטבית של מודעות לסכנות אליהן חשופים הרשתות והמכשור הרפואי בתעשיית שירותי הבריאות. למעשה, ההזנחה בטיפול בפגיעויות ובעדכוני תוכנה הופכת את מוסדות הבריאות בישראל למטרה מושלמת.[63] מודיעין הסייבר בתחום הבריאות מועבר בישראל בעיקר דרך מוסדות ממשלתיים: משרד הבריאות אוסף מידע על ביטחון סייבר באמצעות שלל מקורות, כמו גופי ממשל, ארגונים אזרחיים וארגונים בין־לאומיים.[64] המשרד

62 ראיון עם Tom S., 19 בדצמבר 2018.

63 Patricia Williams and Andrew Woodward, "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem", *Dove Press Journal*, no. 8 (2015): 305-316.

64 ראיון עם יניב פ., 6 בינואר 2019.

גם מעודד את מוסדות הבריאות בישראל להתחבר לשירותי מודיעין הסייבר שלו ללא תשלום, כדי להשיג הגנה נוספת.

מערך הסייבר הלאומי של ישראל ומשרד הבריאות הקימו את מערכת MedSOC כדי לספק מידע על מתקפות סייבר בתחום שירותי הבריאות ולשתף מידע דרך רשת MedSOC. נכון להיום, רשת MedSOC מחוברת רק לבתי חולים, והיא צפויה להתחבר לכל מוסדות הבריאות בישראל במהלך חמש השנים הבאות.[65] בנוסף לכך, ממשלת ישראל התחייבה להשקיע משאבים ומאמצים בכל מוסדות החינוך בתחום סיכוני סייבר ולחזק את מאמצי ביטחון הסייבר במגזר הטכנולוגי.

מודיעין סייבר ומודעות לאבטחת סייבר בהולנד

הארגונים הגדולים במגזר הפרטי בהולנד מגלים, ככלל, מודעות מספקת לביטחון הסייבר, ורובם גם מודעים לכך שתקיפות סייבר עלולות לגרום נזק לנכסיהם. הבעיה היא שמתקפות סייבר יכולות לפגוע גם בתדמית הארגון. ממשלת הולנד קיימה מפגשים עם מדינות נוספות באיחוד האירופי כדי לדון בשאלה האם לחייב ארגונים לדאוג לביטחון סייבר בתחום החומרה והתוכנה.[66] למרות שהממשלה השקיעה רבות בהעלאת המודעות לאיומים דיגיטליים, יש צורך בגישה מחודשת, שתתמקד בתמרוץ ארגונים ובסיוע להם לנקוט פעולות לשיפור האבטחה המקוונת.

בסוף 2017 השיקו המשרד לכלכלה ומדיניות האקלים ומשרד המשפטים והביטחון של הולנד תוכנית משותפת שנקראת "מרכז אֵמון דיגיטלי" (DTC). חזון התוכנית הוא להגביר את חוסן העסקים מול איומי סייבר, תוך התמקדות בשתי משימות מפתח: הראשונה היא לספק לעסקים מידע אמין ועצמאי על נקודות תורפה דיגיטליות וייעוץ קונקרטי לגבי הפעולה שעליהם לנקוט; המשימה השנייה היא לטפח בריתות בין עסקים לאבטחת סייבר.[67]

ממצאים השוואתיים

שתי האסטרטגיות הלאומיות לביטחון סייבר של ישראל ושל הולנד הן בעלות מטרות דומות: להגן על מרחב הסייבר מפני אויבים ולהעצים את חוסן הסייבר. עם זאת, קיימים הבדלים בין שתי המדינות במרכיבים, כמו סביבת איומי הסייבר,

65 ראיון עם אליאב נ., 25 בנובמבר 2018.

66 Herna Verhagen, "De economische en maatschappelijke noodzaak van meer cyber security – Nederland digitaal droge voeten", *Nederland digitaal droge voeten, The Hague*, September 2016.

67 "Factsheet Digital Trust Center", *Government of the Netherlands: Ministry of Economic Affairs and Climate Policy*, August 6, 2018, pp. 1-4.

התנאים הסוציו־פוליטיים, מגמות הביטחון, המסורות ורמת המודעות לסייבר. אלה הביאו להבדלים משמעותיים בגישתן של שתי המדינות לביטחון הסייבר.[68]

משטר ניהול סיכונים

יש קווי דמיון וקווי שוני רבים בין הגישות של ישראל והולנד מבחינת משטר ניהול הסיכונים. לשתי המדינות יש גופים ממשלתיים (בהולנד – משרד הבריאות ו"המרכז הלאומי לביטחון סייבר" – NCSC; בישראל – משרדי הבריאות, הרווחה והספורט ומערך הסייבר הלאומי), המארגנים פגישות סדירות עם המוסדות המספקים שירותי בריאות, במטרה לשמור על הידע הנצבר בתעשייה ועל המודעות שלה לאתגרים ולתהליכים הרלוונטיים. עם זאת, עצם ההקמה של רשת MedSoc בישראל, התומכת באופן ספציפי במגזר השירותים הרפואיים, היא הוכחה ברורה לכך שממשלת ישראל מבינה כי איומי הסייבר מהווים כיום איום פוטנציאלי לרציפות העיסקית של ענף שירותי הבריאות. בהולנד פועל "המרכז הלאומי לביטחון סייבר", אך אין גוף המתמקד ספציפית בענף הבריאות.

הסביבה הרגולטורית

בנוסף למשטר ניהול הסיכונים, ממשלות ישראל והולנד חוקקו חוקים דומים בנושא סייבר ומידע, אם כי כל אחת משתי המדינות שומרת על המאפיינים הייחודיים שלה, שהם תוצאה של מיקומה ומצבה. שתי המדינות גם קבעו תקנות למינוי מנהלי אבטחת מידע ראשיים וקציני אבטחת מידע בארגונים. חוק הפרטיות בישראל מחייב את המחזיקים במידע למנות מנהלי מידע, אלא שלמרות החובה, החוק לא תמיד נאכף.

חרף הדמיון בין שתי המדינות, ישנם כמה הבדלים עיקריים ביניהן בתחום הרגולציה: בהולנד יש חוק ביטחון סייבר, שמתעדכן בימים אלה לפי תקנות "הרגולציה הכללית להגנה על מידע", ובכך הוא מציע שיטה טובה יותר להתמודדות עם נתונים אישיים. עדכון החוק גם הביא להקמת "הסוכנות להגנת נתונים" (DPA), כסמכות העיקרית בהולנד לנושא זה. בישראל, נכון להיום, אין חוק ביטחון סייבר (הוא נמצא עדיין בשלבי ניסוח). מצב זה מקשה על גופי הממשל בישראל לאכוף שימוש באמצעים או לקבוע תקנים מסוימים של ביטחון סייבר לענף שירותי הבריאות. עם זאת, שתי הסביבות הרגולטוריות בישראל ובהולנד דומות בכל הנוגע לביטחון סייבר ואבטחת מידע, וזאת מכיוון שישראל העתיקה

68 Martti Lehto, "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies", *International Journal of Cyber Warfare and Terrorism* 3, no. 3 (2013): 1-18.

בצורה נרחבת את "הדירקטיבה האירופית להגנת מידע" כדי להבטיח התאמה רבה יותר עם התקנים האירופיים.[69]

בעלי העניין העיקריים באסטרטגיה

הולנד וישראל הן חלוצות בתחום ביטחון הסייבר, שכן שתיהן תומכות בשיתוף פעולה עם מומחים מכל מוסדות הממשלה, וכן מהמגזר האזרחי והתעשייתי, לצורך השגת ביטחון בסייבר. אמנם, מסמך האסטרטגיה הלאומית לביטחון סייבר של ישראל אינו מתמקד בשיתוף פעולה בין־לאומי כמו במקרה של האסטרטגיה ההולנדית, אך ריבוי השותפויות הפרטיות־ציבוריות הבין־לאומיות מלמד בבירור על האינטרסים של ממשלת ישראל בשיתוף פעולה בין־לאומי בנושא זה.

הגדרת תשתיות קריטיות ואובייקטים קריטיים

היבט משמעותי באסטרטגיה הלאומית לביטחון סייבר של שתי המדינות הוא הסודיות, השלמות והזמינות של המידע. האסטרטגיה של ישראל מדגישה שימוש בבקרות ספציפיות להגנה על מערכות וארגונים מפני פגיעה בסודיות, בשלמות ובזמינות של מידע ומערכות. מסמך האסטרטגיה ההולנדי אמנם מציין את הסודיות, השלמות והזמינות, אך אינו מספק תפיסה להתמודדות עם שאלת ביטחון הסייבר. שתי המדינות מכירות בכך שיש למפות את הנכסים הקריטיים והמשניים של מוסדות הבריאות, כדי להבין את האיומים על התהליכים המתקיימים בהם ואת נקודות התורפה שלהם.

יחד עם זאת, הגישה של ישראל להתמודד עם נקודות התורפה בשרשרת האספקה של ענף הבריאות היא יוצאת דופן בתחום ביטחון הסייבר: מערך הסייבר הלאומי ומשרד הבריאות הקימו מערכת מבוססת ציונים בכדי לבדוק עד כמה המערכות והשירותים של הספקים הם קריטיים לענף הבריאות, וכן כדי לבדוק את אמצעי ביטחון הסייבר אצל הספק, בהתבסס על קריטיות המוצרים ו/או השירותים.

מודיעין סייבר ומודעות לאבטחת סייבר

ישראל והולנד נמנות על המדינות היותר מפותחות מבחינת חדשנות בתחום הסייבר ואמצעי ביטחון הסייבר. מערך הסייבר הלאומי בישראל מגן באופן יזום על ענף הבריאות על ידי סריקת "הרשת האפלה" במטרה לאתר פושעי סייבר ושיטות חדשות של מתקפות סייבר. שירות המודיעין של הולנד הקים את "יחידת הסייבר המאוחדת" (Joint SigInt Cyber Unit – JSCU), המספקת מידע ומיומנות מקצועית לכלל התשתיות הקריטיות.

69 Bourne, "A Guide to Data Protection in Israel".

במקביל, ממשלת הולנד יצאה בתוכנית לשיפור המודעות לביטחון סייבר בחברה ההולנדית באמצעות פרסומות ומדיה. היוזמה הממשלתית מכוונת לכל אזרחי הולנד, תוך שהממשלה משנה בהדרגה את גישתה מגישה מבוססת־ידע לגישה של רכישת מיומנויות בביטחון סייבר.[70] בישראל אין יוזמה דומה להרחבת מיומנויות ביטחון הסייבר של אזרחיה. עם זאת, יחידה 8200 של צה"ל מתמקדת בלוחמת סייבר ופועלת כזרז בתחום ביטחון הסייבר ב"אומת ההיי־טק".

הבדל נוסף בין שתי המדינות הוא מערכת MedSOC הישראלית, המשתפת מידע על איומי סייבר ספציפיים בענף הבריאות. למרות שהמערכת עדיין נמצאת בשלבי פיתוח ראשונים, כל מוסדות שירותי הבריאות בישראל אמורים להיות מחוברים למערכת הפצת המידע בתוך חמש שנים.[71]

מסקנות

השינויים הטכנולוגיים בענף הבריאות והאיום המתמשך של מתקפות סייבר הממוקדות ברשתות ובמכשור רפואי בתחום שירותי הבריאות (שהולך ומתעצם בזכות הקישוריות המתפתחת), יוצרים מטרה מושכת למתקפות. אלו כוללות את "האינטרנט של הדברים הרפואיים", יישומים רפואיים, תוכנות, מערכות מידע והתקני אבטחה בכל מוסדות הבריאות. התגברות האיומים הללו על כל התשתיות הקריטיות גרמה למדינות רבות להתחיל לפתח אסטרטגיות ולגבש תקנות לחיזוק ביטחון הסייבר. האסטרטגיות הלאומיות והתקנות שגיבשו ישראל והולנד לביטחון סייבר הן מקיפות ונותנות מענה לשורה של איומי סייבר. עם זאת, שתי המדינות צריכות לבצע שיפורים מסוימים כדי לתת מענה לשינויים המתחוללים בתחום הסייבר בענף הבריאות.

משטר ניהול הסיכונים בתחום ביטחון הסייבר מאפשר לשתי המדינות לעדכן את יעדיהן האסטרטגיים ולהשיגם, תוך צמצום סיכונים. הן משטר ניהול הסיכונים והן המשרדים האחראים לכך בישראל ובהולנד מתמקדים בגישה של מטָה־מעלה, שבאה לידי ביטוי במפגשים בנושא ביטחון סייבר עם מנהלי IT ומנהלי בתי חולים. לעומת זאת, קיימת שונות ניכרת בין שתי המדינות בגישה שלהן כלפי אמצעי ביטחון הסייבר במכשור הרפואי; בעוד שישראל יצרה סביבה בטוחה לבדיקת המכשור הרפואי החדש טרם הכנסתו לשימוש, הולנד בחרה בדרך של הנחיות וייעוץ בלבד למפעילי שירותי הבריאות בכל מה שנוגע לבדיקת הציוד הרפואי לפני הכנסתו לשימוש.

---

70 "National Cyber Security Agenda, 'A Cyber Security Netherlands'", *Government of the Netherlands: Ministry of Justice and Security*, April 20, 2018.

71 ראיון עם אליאב נ„ 25 בנובמבר 2018.

שתי המדינות קבעו תקנות להגנה על נתונים בארגונים מפני פושעי סייבר, לרבות בתחום הבריאות, וכן על נתונים פרטיים של אזרחים. ישראל והולנד גם קבעו תקנות המחייבות ארגונים המטפלים במידע רגיש להעסיק מנהלי מידע (מנהלי אבטחת מידע ראשיים וקציני אבטחת מידע). חוק חשוב ורלוונטי נוסף בשתי המדינות הוא החוק ליידוע על פריצה לנתונים, המחייב את מנהלי המידע לדווח על אירועים הקשורים להגנת מידע. יש להניח שכמו הולנד, ישראל תחוקק בסופו של דבר גם חוק לביטחון סייבר, אשר ישפר את הטיפול באירועי סייבר.

בעלי עניין משפיעים מאוד על האסטרטגיה הלאומית לביטחון סייבר בכל מדינה, מאחר שלדרג האופרטיבי יש דעה שונה בנושא ביטחון סייבר מאשר לדרג המופקד על האסטרטגיה. איזון סביר בין סוגיות הנוגעות לביטחון סייבר ובין העבודה השוטפת יועיל לשיפור ביטחון הסייבר, ובכלל זה גם לעובדי מערכת הבריאות. ישראל והולנד מקיימות קשר קבוע עם בעלי העניין בענף שירותי הבריאות שלהן, במטרה לגבש אסטרטגיות סייבר אפקטיביות שיעודדו מחויבות פרו־אקטיבית ורב־תחומית מצידם. לצד הגדרת תחום התשתיות הקריטיות, גם מוסדות הבריאות צריכים להגדיר מהם הנכסים הקריטיים והלא קריטיים שלהם, כך שיוכלו ליישם אמצעי ביטחון סייבר מיוחדים על אותם נכסים שזקוקים לכך.

האסטרטגיות הלאומיות של ישראל והולנד בנושא ביטחון סייבר מתמקדות במיפוי נכסי ארגונים באמצעות תהליך של הערכת סיכונים ובדיקת מערכות קיימות להגנת סייבר. שתי המדינות גם מדגישות את חשיבות ביטחון הסייבר למניעת מתקפות ברשת.

ישראל והולנד מעמידות במרכז תשומת הלב של ענף שירותי הבריאות את הסודיות, השלמות והזמינות של המידע. ההבדל הגדול ביניהן בהתייחסותן לענף שירותי הבריאות הוא שממשלת ישראל לקחה על עצמה את האחריות לסייע לענף זה בנקודות התורפה של שרשרת האספקה, בעוד שהולנד בחרה למלא רק תפקיד אינפורמטיבי באבטחת שרשרת זו.

מודיעין סייבר ומודעות לביטחון סייבר הופכים להכרח בענף שירותי הבריאות. שירותי המודיעין של ישראל פועלים יחד עם משרד הבריאות וסורקים את "הרשת האפלה" לאיתור מתקפות סייבר חדשות. הצבא ושירותי המודיעין בהולנד הקימו את "הרשת הלאומית לתגובה למתקפות", במטרה לאתר ולהרתיע מתקפות סייבר באמצעות פתרונות ביטחון סייבר חדשים. יתרה מכך, ממשלת הולנד גיבשה תוכנית למודעות ביטחונית, העושה שימוש בפרסומות כדי ליידע על הסכנות הקיימות באינטרנט ולהגביר את החוסן האזרחי. בישראל אין כיום תוכנית דומה למודעות בנושא ביטחון סייבר, אך הידע בתחום הסייבר מתרחב באמצעות יחידות של צה"ל המתמקדות בלוחמת סייבר ומודיעין. מודיעין הסייבר בישראל מופץ גם באמצעות

מערכת MedSOC החדשה, המאפשרת למשרד הבריאות ולמערך הסייבר הלאומי להעלות אליה מידע על התקפות סייבר או על פגיעויות ברשת.

המלצות

להלן המלצות לשיפור ולהתנהלות בתחום האסטרטגיות הלאומיות לביטחון סייבר, שחלקן מסתמכות על החוזקות הנוכחיות של האסטרטגיות הקיימות בישראל ובהולנד.

ראשית, יעילותן של האסטרטגיות והתקנות בנושאי סייבר הקיימות בשתי המדינות תלויה ביכולת הממשלות להסתגל לעולם הסייבר המתפתח. אסטרטגיות ביטחון סייבר עתידיות יצטרכו, אפוא, להיצמד לבסיס הקיים של תקנות וחוקים, אך תוך עיצוב מחודש וגמיש של הסביבה הרגולטורית ומערכות המידע בארגונים בעלי תשתית קריטית. על הממשלות לעדכן את האסטרטגיות, המדיניות והתקנות שלהן על בסיס שנתי או דו־שנתי, כדי שיישארו רלוונטיות להתפתחויות החדשות בעולם הסייבר.[72]

שנית, בדיקה ופיתוח של אסטרטגיות ביטחון סייבר חדשות מצריכים תהליך מתמיד של הערכת סיכונים. על ישראל והולנד להמשיך ולהחזיק בגישתן לביטחון הסייבר, המגינה על ענף שירותי הבריאות מפני התקפות סייבר, שכן פושעי סייבר לעולם לא יפסיקו לנסות לפרוץ למערכות המידע של מוסדות המספקים שירותי בריאות. למרבה המזל, שתי המדינות נוהגות להעמיד למבחן את אסטרטגיות ביטחון הסייבר שלהן בתרגילים ארציים, ועושות זאת כדי לשפר ולחזק נוהלי אבטחה קיימים. מערך הסייבר הלאומי בישראל ומקבילו ההולנדי (NCSC) צריכים לקבל על עצמם אחריות רבה יותר לענף שירותי הבריאות באמצעות עידוד המוסדות ומנהלי אבטחת המידע שלהם לגבש תוכניות להמשכיות עיסקית ולתרגל מצבים שיכינו את העובדים למקרה של משבר סייבר.[73] בנוסף לכך, כדי להגן על בסיסי הנתונים הרפואיים הלאומיים מפני התקפות סייבר, על מערך הסייבר הלאומי של ישראל ו"מינהלת הבריאות והנוער" של הולנד לתת את הדעת למוסדות קטנים ופחות מאובטחים ולהגדיר עבורם גישה אבטחה נפרדת, מתוך הבנה שמוסדות כאלה נוטים פחות, או מסוגלים פחות, לבצע עדכוני מערכת או לרכוש מכשור רפואי חדש.

שלישית, על ממשלות ישראל והולנד לחקור אסטרטגיות ביטחון סייבר של בעלות ברית נוספות, כדי להבטיח יכולת טובה יותר להתייחס לאיומים המתעוררים בזירה הבין־לאומית. זאת, מתוך הנחה שככל שירבו הגורמים המעורבים בהתמודדות עם איומים כאלה, כך יפחת הנטל על כל אחד מהם. מה שחסר כיום הוא חלוקת נטל

72 ראיון עם יניב פ., 6 בינואר 2019.
73 ראיון עם אליאב נ., 25 בנובמבר 2018.

כזו בין ממשלות. בנוסף, קונצנזוס בין־לאומי סביב הגדרות, חוקים וחלופות בתחום ביטחון הסייבר יקל את האילוצים שבפניהם ניצבת הרגולציה במדינות שונות.

רביעית, יש לקדם מודעות רבה יותר לביטחון סייבר בחברה המקומית בכלל ובמוסדות שירותי הבריאות שלה בפרט. אחדות מההנחיות צריכות להתמקד בהגברת המודעות לביטחון סייבר אצל צוותי שירותי הבריאות, מכיוון שאלה מִטבעם אינם נוטים לעסוק בכך, אלא מתמקדים בבריאות המטופלים. על הארגונים ואנשי הצוות המספקים שירותי בריאות להכיר את הסכנות לביטחון הסייבר ואת שיטות המתקפה במרחב זה.

חמישית, למרות שישראל והולנד מחזיקות בגישה מתקדמת כלפי ביטחון הסייבר, יש לציין כי בשתי המדינות גם נותרו פערים לא מטופלים בתחום זה. יש לקוות שמחקרים עתידיים ומאמצים נוספים להבנת איומי הסייבר בתחום שירותי הבריאות ישפרו את החוסן החברתי בשתי המדינות. בנוסף לכך, שיתוף פעולה נרחב עם מספר רב יותר של מדינות ברחבי העולם יתרום גם הוא להפיכתו של מרחב הסייבר בשתי המדינות לטוב ולבטוח יותר.