**מה משמעות מתקפות הסייבר שאירעו על מתקני רשות המים / עמרי וקסלר\***

מדיווח שפורסם בווינט ב-26 באפריל, נודע כי מתכתובת בין רשות המים למערך הסייבר הלאומי כי שורה של מערכות תפעוליות במתקני מים ברחבי הארץ חוו מתקפות סייבר, שלמרבה המזל נכשלו. מתקפות סייבר על מערכות תפעוליות או מערכות לבקרה תעשייתית אינן תופעה חדשה, אולם נדירה ומסוכנת.

**במה מדובר?**

מערכות תפעוליות או מערכות OT משמשות בכל העולם לבקרה ושליטה בתהליכים תעשייתית במפעלים ותשתיות קריטיות, כגון תחנות חשמל, כורים גרעיניים, תשתיות מים וביוב ולוויינים. לאורך העשור האחרון, ועם התפחויות טכנולוגיות, מערכות אלו חוברו בהדרגה לרשת האינטרנט באופן שמקל על התפעול והשליטה בהן, אולם במקביל חושף אותן למתקפות סייבר. מתקפת סייבר על מערכות שכאלו אינה דבר פשוט לביצוע ומחייבת מודיעין מוקדם ועבודת הכנה, אולם עלולה להוביל לנזק פיזי ממשי. אפשרות נוספת, הנראית הרבה יותר סבירה במקרה שנחשף כעת היא ניסיון גניבת הרשאות של מפעילי המערכות במטרה להסתנן אליהן ולאסוף עליהן מידע או על מנת להתקין נוזקות שונות.

מתקפות על מערכות אלו נדירות. המתקפה הראשונה על מערכות תפעוליות נחשפה לראשונה ב-2010, כשתולעת הסטקסנט, שפותחה על פי מקורות זרים על ידי ארה"ב וישראל, שיבשה את מערך הצנטריפוגות במתקן להעשרת אורניום בנתנז שבאיראן. ב-2014, הובילה מתקפת סייבר לפיצוץ במפעל פלדה בגרמניה. ב-2015 וב-2016, השביתו האקרים רוסים את אספקת החשמל לכרבע מיליון תושבים באוקראינה. גם ישראל חוותה ניסיונות כושלים למתקפות על מערכות אלו, כשב-2013 ניסו האקרים סורים לבצע מתקפת סייבר על מערכות המים של חיפה ולמרבה המזל נכשלו.

**מי עלול לעמוד מאחורי המתקפות?**

בעוד שעברייני סייבר קיימו בעבר מתקפות על תשתיות קריטיות, מתקפות על מערכות תפעוליות מצריכות הכנה רבה מראש ויכולות טכניות מורכבות. עד כה, מתקפות על המערכות התפעוליות עצמן יוחסו בעיקר לממשלות זרות. לאחר חשיפתה של סטקסנט, הקביל ראש ה-CIA וה-NSA לשעבר, מייקל היידן את היכולת החדשה לנשק הגרעיני שהוטל על יפן בשלהי מלחמת העולם השנייה. היידן טען שמרגע שהיכולת הזאת נחשפה לעיני העולם, עוד מדינות, בדגש על מעצמות, יפעלו לפתח אותה. מאז 2010, רוב המתקפות שתועדו יוחסו לרוסיה, שמפתחת יכולות סייבר שיאפשרו לה לערער ולהחליש מדינות הנתפסות כיריבות אסטרטגיות. שחקן עולה נוסף בהקשר ורלוונטי מאוד לישראל הוא איראן.

איראן הודתה מספר פעמים מאז 2010, שמתקפת הסטקסנט עליה הסבה את תשומת ליבה לתחום הסייבר וממשלת איראן השקיעה רבות מאז בהגנת סייבר אך בעיקר ביכולות סייבר התקפיות, וכיום איראן מוגדרת אחת המדינות האגרסיביות ביותר בעולם במרחב הסייבר. מאז 2010 תקפו האקרים איראניים עשרות תשתיות קריטיות במזה"ת, בדגש על מפעלים פטרוכימיים וצינורות גז ונפט בערב הסעודית, בכווית ובאיחוד האמירויות. הרסניות ככל שהיו למערכות המחשוב, המתקפות הללו כולן כוונו כלפי הרשתות המנהליות של המתקנים בלבד. עם זאת, איראן חותרת לשיפור יכולות הסייבר ההתקפיות שלה ובנובמבר 2019 הזהירו חוקרי מיקרוסופט כי האקרים איראניים החלו להתמקד בגניבת הרשאות של מפעילי מערכות תפעוליות.

**כיצד מדינות מתמודדות עם האיום?**

מדינות רבות בעולם השמיעו בשנים האחרונות אזהרות מפני מתקפות הסייבר על תשתיות קריטיות ופעלו לאסור עליהן במסגרת תהליך ניסוח נורמות התנהגות בין-לאומיות בחסות האו"ם. חלק מאותן המדינות כגון צרפת ובריטניה איימו להגיב בכוח על מתקפות סייבר על תשתיות קריטיות. ארה"ב רופפה את המגבלות על שימוש ביכולות סייבר התקפיות וב-2018 ניסחה את אסטרטגיית ה-Defend Forward, במסגרתה פועל פיקוד הסייבר האמריקני לשיבוש פעילותם של האקרים ברשתות של מדינות זרות. ביוני 2019 דווח כי ארה"ב פרצה לרשת החשמל של רוסיה כצעד הרתעתי לאחר מספר תקריות בהן פרצו האקרים רוסים לתשתיות קריטיות בארה"ב.

**מה ישראל יכולה לעשות?**

פעילותו המהירה של מערך הסייבר הלאומי, האחראי להגנה על תשתיות חיוניות בישראל מנעה ככל הנראה נזק נרחב. לא מן הנמנע כי התוקפים בדקו את ערנותה של ישראל המצויה, ביחד עם מדינות רבות, בעיצומו של המאבק בנגיף הקורונה וניסו לבחון את האפשרות של גרימת נזק נרחב, כגון עצירת אספקת המים ליישובים או החדרת כלור או מי שפכים למי שתייה. ישראל נמצאת מספר רמות מעל יריבותיה במרחב הסייבר ואל לה להישאר בעמדה מגננתית בלבד לנגד מתקפות סייבר על תשתיות קריטיות. עליה להיערך לניסיונות נוספים ולהיות ערוכה לבצע פעולות לשיבוש פעילותם של ההאקרים מבעוד מועד ולהרתיעם.

\*עמרי וקסלר הוא חוקר בכיר למדיניות סייבר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון באוניברסיטת תל אביב.