"חובה להגן על תשתיות מים נפני התקפות סייבר"

התקפות סייבר על תשתיות מים של מדינה יכולות לגרום לפגיעה ברבבות אנשים, לנזק כספי לחברת המים ולגניבת מידע עסקי על כמויות צריכת המים של אזורים שונים במדינה. ניתוח מיוחד

צילום: Bigstock

מאת דניאל ארנרייך

יכולת של תושבי המדינה לתפקד תלויה בזמינות ואספקה שוטפת של אנרגיה ומים. מרבית מתקני המים בעולם מפוקחים על ידי מערכות בקרה (supervisory control and data acquisition–SCADA) שתפקודן מבוסס על תקשורת, מחשבים, בקרים תעשייתיים וחיישנים חכמים. למרות העובדה כי אספקה רציפה של מים ראויים לשתייה היא חיונית, לעתים אנו עדים לכך שהמערכות לניהול אספקה עירונית לא זוכות למשאבים עבור תחזוקה נאותה. כתוצאה מכך, תשתית המים בערים רבות בארץ (וגם בעולם) סובלות מדליפה מוגברת ומדירדת הצריכה לא מדויקת וגורמת להפסדים כספיים. מעבר לדאגות שפורטו, ישנן כיום חששות חמורות יותר מדליפה והפסדים, כיוון שמערכות הבקרה ובמיוחד אלה שהופעלו לראשונה לפני יותר מעשור, לא נבנו בטכנולוגיה מאובטחת. לכן, הן חשופות לתקיפות קיברנטיות. עד לפני כשני עשורים, אנשים האמינו כי על ידי שמירת בידוד (air gap) בין רשת הבקרה לבין רשת תקשורת ארגונית (IT), מערכות הבקרה מוגנות היטב ותקיפה מחוץ לארגון (externally generated cyber attack) לא יכולה לפגוע בפעולתם. בשנת 2010, כאשר העולם נחשף לתקיפה קיברנטית על הכור האירני (Stuxnet), האחראים על תשתיות קריטיות (critical infrastructure) הבינו כי הגיע הזמן לשדרג את האבטחה הקיברנטית של מערכות הבקרה.

סיכונים למערכות מים

בעשור האחרון הפך החיבור בין רשת הבקרה (OT–operation technology) לרשת הארגונית (IT) לחיוני, על מנת לשדרג את יכולת הפיקוח, לאפשר איסוף נתונים לצורך תכנון תהליכי תחזוקה, לאפשר ביצוע עדכוני תוכנה וגם לקבל ולהפיץ בארגון התראות על תקלות. החיבור בין המערכות גם אפשר התייעלות כוללת, חסכון בכוח אדם, תחזוקה יעילה, זמינות מידע לגבי צריכות מים באזורים שונים וזמינות מידע על צריכת חשמל בתחנות שאיבה.

בשעה שהשינוי המערכתי הנדרש אפשר שדרוג בתפעול הארגוני (productivity), הוא גרם להחלשה של האבטחה הקיברנטית על מתקנים רבים, כגון: תחנות שאיבה, משאבות להגברת הלחץ, בקרת איכות המים, מתקני טיהור מים ועוד. לאור העובדה כי הצורך בנקודות בקרה הולך ומתרחב, מספר החיישנים בכל מתקן גדל ונדרש תחכום בתהליכים (local on-site processes), יישום הגנה קיברנטית יצר אתגר חדש למומחים בתחום המים.

ההרחבה והשדרוג בתפעול הובילו לצורך בתקשורת בפס רחב, הרחבת מערכות הבקרה ושימוש ברשתות ציבוריות. תהליכים אלה מעלים את הסיכון לתקיפה קיברנטית על מחשבי הבקרה שאחראים לתפעול: מתקני שאיבה, מתקני הטפלה, משאבות להגבת הלחצים, מתקנים לבקרת לחצים, מתקני טיהור והשבחת מים, מאגרי מים ועוד.

תקיפה קיברנטית ממוקדת (advanced persistent threat) על בקרים (programmable logic controllers–PLC) מקומיים, עלולה להוביל לנזקים באמצעות: שינוי בתפקוד הבקרים, שינוי בערכים תפעוליים, שינוי בערכים מדווחים למרכז הבקרה, שינוי בערכים המשמשים לחיוב לקוחות ועוד. התערבות חיצונית בתהליכים על ידי תוקף עלולה לגרום לנזק כספי לחברת המים, הפסקת פעולה של מתקנים (supply outage), גניבת מידע עסקי על כמויות אובדן מים (unaccounted for water–UFW), כמויות הצריכה בשעות שיא וגם נזקים חמורים לציוד שיגרמו להשבתה ארוכה ופגיעה בתדמיתה של החברה.

> "התערבות חיצונית בתהליכים על ידי תוקף עלולה לגרום לנזק כספי לחברת המים, הפסקת פעולה של מתקנים, גניבת מידע עסקי על כמויות אובדן מים, כמויות הצריכה בשעות שיא וגם נזקים חמורים לציוד שיגרמו להשבתה ארוכה ופגיעה בתדמיתה של החברה"

הגנה על מתקנים חיוניים

ידוע כי ביטול מוחלט של אפשרויות לתקיפה קיברנטית על מערכת הבקרה היא משימה בלתי אפשרית, אבל יישום מגוון אמצעי הגנה (cyber defense) הוא אפשרי בהחלט. המטרה היא להפחית את הסיכונים (risk mitigation) וכך להפוך את התקיפה למסובכת ויקרה יותר, שדורשת אמצעים חדישים וידע מקצועי. התהליכים לשדרוג ההגנה הקיברנטית ידועים, לא יקרים במיוחד וניתן להוכיח את הכדאיות הכלכלית ביישומם (return on investment- ROI).

אמצעים אלה כוללים החלפת מחשבים ותוכנת הבקרה, שדרוג רשת התקשורת, יישום תשתיות המדמות רשת פרטית (virtual private network – VPN), זיהוי ואישור של המתחברים למערכת (user authentication), הגבלת גישה לתהליכים (role based access control–RBAC), מניעת אפשרויות לחיבור מרחוק, ביצוע עדכוני תוכנה (software patching) ועדכוני לזיהוי וירוסים (antivirus updates) באמצעות תהליכים שמותאמים במיוחד למערכות בקרה, תיעוד נרחב לגבי תפקוד המערכת (auditing) ועוד.

סיכום ומסקנות

אין זה סוד כי התוקפים של היום שדרגו את היכולות והציוד שברשותם, ותפקודם ממומן על ידי ארגונים שמטרתם ליצור נזק ומדינות שמטרתן לגרום לפגיעה חמורה. לכן, כל חברה וארגון שמפעילה מתקנים ותשתיות חיוניים, חייבת להשקיע משאבים משמעותיים כדי לשדרג את אמצעי ההגנה הקיברנטית שלהם. אין כאן שאלה של כדאיות כלכלית או הנחיה מהרשויות, אלא מחויבות לאומית לספק מים באיכות גבוהה, לחץ קבוע וזמינות מרבית, כפי שמקובל במדינות מתקדמות בעולם. ●

דניאל ארנרייך (BSc) הוא יועץ עצמאי במסגרת מומחים לבקרה ותקשורת מאובטחת – (SCCE) בעל ניסיון של מעל 25 שנים בנושא מערכות בקרה על תשתיות קריטיות כגון: חשמל, מים, גז, ומערכות בקרה על תחנות כוח במסגרת פעילותו בחברות מוטורולה, סימנס ווטרפול סקיוריטי.