SECAUDIT
IT & CYBER AUDIT EXPERTS

אבטחת רשתות OT

מאת: יוענה נחום, ראש תחום רגולציה ותחקור נתונים ב"סקאודיט"

מהי אבטחת Operation Technology - OT ומדוע היא חשובה כל כך?

סביבות OT מריצות מערכות מחשוב השולטות בתהליכים פיזיים, כגון מכונות תעשייתיות המפעל ייצורי, תחנות כוח, גז, מים, ציוד רפואי או תחבורה. בסביבות אלה קיימים רכיבי בקרה, מחשוב לטובת ניהול הסביבה ורכיבי תקשורת. מערכות אלו יכולות לכלול מערכות פיקוח, שליטה ואיסוף נתונים (SCADA) , מערכות בקרה מבוזרות (DCS) ובקרים מתוכנתים (PLC) השולטים בתהליכים השונים (למשל תהליך חימום של דוד או הפעלת ציוד MRI בבית חולים).

נציין עם זאת כי כל Data Center עושה שימוש בסביבת OT לניהול מערכות המיזוג, החשמל וכו' (HVAC[1]), כך שגם אם סביבת המחשוב העיקרית של הארגון הינה IT, ברוב המקרים הארגון יעשה שימוש ב OT.

אבטחת טכנולוגיה תפעולית (OT- Operational Technology Security) מתייחסת למרכיבי אבטחת סייבר המסייעים להבטחת המשכיות, שלמות ובטיחות הפעילות ברשתות תעשייתיות.

כלומר, אם נפשט-

IT - מתמקד בסודיות, שלמות וזמינות של מערכות ונתונים, למשל ברשת בנקאית.

OT- מתמקד בהמשכיות, שלמות ובטיחות הציוד, תהליכים פיזיים והתשתיות, למשל ברשת מפעל ייצור.

למתקפות סייבר על רשתות תעשייתיות ותשתיות קריטיות יכולות להיות מגוון רחב של השפעות מרחיקות לכת על ארגון, לקוחותיו והציבור כולו. ההשלכות כוללות שיבושים בפעילות (שעשויים לגרום להפסקת ייצור כמו גם הפסדי הכנסות), נזק למתקנים, פציעות עובדים, אסונות סביבתיים, אי עמידה ברגולציה וחבות אזרחית או פלילית.

דוח בנושא, שנכתב ע"י חברת Fortinet[2] מעלה שכמעט 74% מארגוני ה-OT דיווחו כי חוו פריצת תוכנה זדונית ב-12 החודשים האחרונים, שגרמו נזקים לפרודוקטיביות, להכנסות, למוניטין, לקניין הרוחני ולבטיחות הפיזית של הארגון ולעיתים באופן מסכן חיים.

אתגרים באבטחת סביבות OT

1. מערכות ישנות - מערכות OT רבות תוכננו והוטמעו לפני עליית המודעות לסיכוני הסייבר. מערכות אלו עושות שימוש ברכיבים, בתוכנות ובפרוטוקולי תקשורת שיש בהם חולשות הגנת סייבר מובנות והן חסרות לרוב את תכונות האבטחה המובנות הקיימות במערכות IT מודרניות. פעמים רבות, עדכון של רכיבי המחשוב מצריכים עדכון של רכיבי הייצור כולו, דבר המייצר עלויות כבדות.

2. קושי בהתקנת עדכוני אבטחה- התקנת עדכוני אבטחה (באם קיימים למערכות אלו) אינה פשוטה. מערכות אלו הן חלק מתהליכים/תשתיות קריטיים אשר לעיתים רחוקות, אם בכלל, ניתן לעצור אותם או לסכן את רציפותן. בנוסף, היצרנים עצמם נמנעים מעידוד לקוחותיהם לבצע התקנה של עדכונים לאור תקלות אפשריות.

3. הרחבת משטחי התקיפה- לצורך דיגיטציה של פעולות וחדשנות דיגיטלית חוברו סביבות ה- OT לרשת האינטרנט ולמערכות ה-IT של הארגון, כמו גם הורחבה הגישה מרחוק לסביבות לו, היבטים אשר הרחיבו את משטחי התקיפה בארגון וחשפו אותן לאיומי סייבר חמורים.

4. מיפוי חסר של סביבות ה-OT ופילוח הרשתות- ברוב הארגונים לא קיים מיפוי תהליכי עבודה ונכסים מקיף ועדכני לסביבת ה-OT ופילוח הרשתות הקיימות, באופן המקשה על הארגון להעריך סיכונים כמו פגיעויות קריטיות, חשיפה לתעבורת אינטרנט ותצורות שגויות שעלולות לחשוף את הארגון.

5.הגורם האנושי- בבסיס הסיכונים והחשיפות לאיומי סייבר ואבטחת מידע קיים הסיכון הנובע מהגורם האנושי. גם באבטחת רשתות וסביבות OT, הסיכון הנובע מהגורם האנושי מהווה אתגר משמעותי. תוכניות הכשרה ומודעות חיוניות בהפחתת סיכונים אלו.

6.העדר ידע של אנשי אבטחת המידע בארגון- בארגונים רבים, אנשי אבטחת המידע והעומד בראשם (CISO) חסרים את הידע והמומחיות הנדרשים בתחום טכנולוגיות תפעול ובקרת תהליכים.

אז מה בכל זאת ניתן לעשות?

1.הפרדת רשתות (סגמנטציה)- רשתות תעשייתיות רבות במהלך השנים הפכו לרשתות גדולות ושטוחות. הטמעת סגמנטציית רשת עוזרת לבודד נכסים קריטיים ולהגביל גישה לא מורשית. ע"י חלוקת הרשת לאזורים מבודדים, ניתן להכיל את ההשפעה של פרצת אבטחה, ולמנוע כניסה של תוקפים . במידת הצורך קיימים מוצרים כגון דיודה חד כיוונית המשמשת להעברת מידע בערוץ חד כיווני ומניעה מוחלטת של כל תעבורה בכיוון המנוגד.

2.ניטור רציף- ניטור בזמן אמת אחר פעילויות הרשת חיוני לאיתור ותגובה לאירועי אבטחה באופן מידי. שימוש במערכות לזיהוי חדירה (IDS) , מערכות לזיהוי אנומליות והטמעת מערכת לניהול אבטחת מידע ואירועים (SIEM) יכולים לשפר את הנראות, זיהוי וניתוח התנהגות ברשת.

3.אכיפת גישה מרחוק מבוססת 'אפס אמון' (Zero Trust) - בארגונים רבים קבלני אחזקה או צוותי התפעול עצמם מתקינים יכולות גישה מרחוק לנכסי ה-OT. פתרונות גישה לרשת 'אפס אמון' (ZTNA) מסייעים לארגונים להפחית סיכוני סייבר באמצעות שירות גישה מרחוק מאובטח המאמת משתמשים ומעניק גישה רק למשאבים ספציפיים בהתאם למדיניות.

4.בקרות גישה ואימות- הוספת שכבת אבטחה נוספת ע"י הגבלת גישה לצוות מורשה בלבד ויישום אמצעי אימות חזקים, כגון אימות רב-גורמי – MFA -Multi Factor Authentication.

5.עדכונים שוטפים- תכנית עבודה מקיפה להטמעת עדכוני אבטחה שוטפים של תשתיות ומערכות חיוניות בתאום ובאישור היצרנים.

6.תכנית תגובה לאירועים והתאוששות- פיתוח תכנית תגובה לאירועים ועדכונה חיוניים למזעור ההשפעה של אירועי אבטחה. על התכנית לכלול נהלים מוגדרים לזיהוי, הכלה, מיגור, שחזור והפקת לקחים מאירועים. חשוב לבצע תרגולים שוטפים של התכנית ע"מ לוודא יכולת יישומה בפועל בעת אירוע אמת.

7.הכשרות והדרכות מגובות בנהלים – הכשרת גורמי ה IT הפועלים בסביבות OT להכרת הסיכונים ושיטות ההימנעות וצמצום הסיכון.

תקנים רלוונטיים וחקיקה באבטחת רשתות OT

קיימים כיום מספר תקנים שונים העוסקים באבטחת OT (OT Security Standards), בין היתר:

1.NIST SP 800-82 - מספק סקירה מעמיקה של היבטי OT ומפרט טופולוגיות טיפוסיות, איומים ופגיעויות נפוצות וכן אמצעי אבטחה נגד סיכונים נלווים.

2.ISA99/IEC 62443- מגדירים מתודולוגיות להערכת סיכונים, פיתוח רכיבים מאובטחים, תכנון ארכיטקטורת רשת תעשייתית מאובטחת ואופן מדידת רמת הבשלות עבור כל דרישת אבטחה.

3.EU NIS/NIS2 Directive- חקיקת אבטחת סייבר הנאכפת במדינות האיחוד האירופי. מטרתה להגביר את האבטחה והחוסן של תשתיות קריטיות ע"י דרישות אבטחה, חובות דיווח ואמצעי פיקוח מחמירים.

4.המשרד לאיכות הסביבה פרסם בינואר 2020 מדריך סייבר בנושא "עמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה", הכולל דרישה לניהול נאות של סיכוני הסייבר בסביבת ה- OT.

5.למשרד האנרגיה ולרשות הממשלתית למים ולביוב קיימים נהלים מחייבים הקובעים סטנדרט הגנה נדרש בנוגע לרשתות הבקרה של יצרני החשמל וספקי המים והביוב.

לסיכום, אבטחת רשתות וסביבות OT הוא אתגר משמעותי הדורש גישה הוליסטית ומסתגלת. מתקפות הסייבר הולכות ומתפתחות גם לטכנולוגיות תפעוליות שמשמשות לניטור ובקרה על תהליכים תפעוליים, תעשייתיים, יצרניים ופיזיים בארגון.

ככל שתשתיות קריטיות ממשיכות להתפתח, על הארגון לתעדף היבטי אבטחת סביבות OT וכן להכיר, לזהות ולנהל את השוני וההשפעות של איומי סייבר על הסביבה הפיזית לעומת סביבות אחרות כדי להגן מפני הסיכון ההולך וגדל של איומי הסייבר.

על ידי הטמעת שיטות עבודה מומלצות והישארות מעודכנת במגמות מתפתחות, ארגונים יכולים לחזק את סביבות ה- OT שלהם ולצמצם את החשיפות והסיכונים הקיימים.