20.83x25.29	1/2	עמוד 36	new-tech magazine	31/05/2021	77547285-5
טי - חברת סייבריניב ורדי - מנכ"ל קלרוטימנכ"ל קלרוט - 21452					

איום הסייבר על IoT תעשייתי הולך וגובר: כיצד מפחיתים את הסיכון?

יניב ורדי, מנכ"ל קלארוטי - חברת אבטחת הסייבר התעשייתי

עם האצת הטרנספורמציה הדיגיטלית ומיזוג רשתות ה-IT (טכנולוגיות מידע) ורשתות הטכנולוגיה תפעולית (OT), מכשירים מבוססי אינטרנט של הדברים (IoT) ו-IoT תעשייתי (IIoT) הופכים לכלים חיוניים עבור חברות במגזרים כמו נפט וגז, אנרגיה, שירותים, ייצור, תרופות, מזון ומשקאות. בין אם הם ממטבים תהליכים בודדים או מפעלים שלמים ומערכות אקולוגיות קריטיות אחרות של תשתיות, מכשירים אלה מסייעים להגביר את יעילות הייצור ולשפר את המהימנות, התגובתיות, האיכות ותהליכי האספקה של הארגון.

עם זאת, ככל שחברות עושות יותר שימוש במכשירי IIoT שבדרך כלל אינם מתוכננים תוך התחשבות באבטחת סייבר, הן גם מעלות את הסיכון הנשקף לסביבות העבודה שלהן. לפני כמעט ארבע שנים, NotPetya השפיעה על מגוון רחב של תאגידים רב-לאומיים במגזרי הבריאות, האנרגיה והתחבורה, וגרמה לקיפאון בפעילות של חברות רבות, תוך גרימת נזקים המוערכים בעשרה מיליארד דולר. במהלך השנים, ראינו דוגמאות לאופן שבו האקרים יכולים לסכן מכוניות מחוברות לרשת על ידי כך שחדרו למערכות קריטיות כמו המנוע והבלמים. זיוף GPS למשל, מאפשר לתוקפים להפריע למערכות ניווט ולגרום למפעילי כלי תחבורה שונים לרדת מהמסלול. לאחרונה, פלורידה בקושי הצליחה להתמודד עם מתקפה שמטרתה לזהם את אספקת המים במדינה. איום על תשתיות קריטיות קרה לאחרונה בחברת seigeware, כאשר האקר אחד הצליח לאיים בהשבתת המערכות שכל עסק מסתמך עליהן כדי להפעיל את התשתית המשרדית שלו – אורות, מעליות, מיזוג אוויר וחימום, ומערכות אבטחה פיזיות.

ישנן דרכים רבות שבהן גורמים זדוניים יכולים להשתמש במכשירים מחוברים כדי לנקוט בפעולות קיצוניות, או לפעול בשקט ברקע ולשבש את רווחתנו הכלכלית, וגרוע מכך, לגרום נזק פיזי - והסיכון הוא אמיתי. זו לא תהיה הגזמה גדולה לדמיין תרחיש של שיבוש פס הייצור של חברות תרופות מובילות כדי ליצור מחסור בשוק, או תרחיש אחר של פגיעה באיכות המוצרים של חברות מזון ומשקאות, שיכולה לסכן את בריאותנו.

חברת המחקר גרטנר מתייחסת לשילוב של רשתות ונכסים אלה כמערכות סייבר-פיזיות, או CPSs (ר"ת - cyber-physical systems) וצופה כי ההשפעה הפיננסית של התקפות על CPSs אשר תתבטאנה בפגיעות קטלניות, תגיע ליותר מחמישים מיליארד דולר עד 2023. על פי גרטנר, גם ללא הכללת הערך הממשי של חיי אדם במשוואה, העלויות לארגונים במונחים של פיצויים, ליטיגציה, ביטוח, קנסות רגולטוריים ואובדן מוניטין יהיו משמעותיות ביותר. גרטנר צופה כי עד שנת 2024, 75% מהמנכ"לים יהיו אחראים באופן אישי לתקריות CPS.

כדי לטפל בסיכון הגובר הקשור במכשירי IoT, נחתם בארה"ב חוק שיפור אבטחת הסייבר של IoT ב-4 בדצמבר 2020. מתוך הכרה בחוסר האחידות בזיהוי נקודות תורפה וסיכון בשרשרת האספקה על ידי מכשירי IoT, החוק מבקש להחליף את גישת האד-הוק של ימינו בתקנים ובהנחיות עקביות. השורה התחתונה היא שכל מכשיר IoT שנרכש במימון ממשלתי-פדרלי יהיה חייב לעמוד בתקני אבטחה מינימליים חדשים, והדדליין למימושם מתקרב במהירות.

יפעת מידע תקשורתי דרך מנחם בגין 96-98 (לשעבר דרך פ"ת) תל אביב 67138 טל. 03-5635050 פקס. 03-5617166

18.57x11.93	2/2	עמוד 37	new-tech magazine	31/05/2021	77547286-6
טי - חברת סייברינייב ורדי - מנכ"ל קלרוטימנכ"ל קלרוט - 21452					

בעוד שהחוק החדש מיועד בעיקר לסוכנויות ממשלתיות ולספקים ונותני השירות איתם הן עובדות, הרי שיהיה זה נבון מצד חברות ומפעילי תשתיות קריטיות בכל המגזרים לקרוא את המפה, ולהתחיל בהקדם האפשרי לשפר ולאמץ את שיטות העבודה הטובות ביותר שבנמצא לאבטחת IoT ו-IIoT.

נשאלת השאלה איפה להתחיל? חברות תשתית קריטיות צריכות להיות מסוגלות לזהות ולעקוב אחר איומים ממכשירי IoT/IIoT החוצים את גבולות רשתות ה-IT וה-OT. אבל המציאות היא כי רשתות OT היוו "נקודה עיוורת" עבור מומחי אבטחת IT במשך עשרות שנים. ככל שיותר נכסי OT מדור קודם מקבלים ממשק לאינטרנט, וחברות תעשייתיות מוסיפות יותר מכשירים המחוברים לאינטרנט לסביבות שלהם כדי להניע אוטומציה ומודרניזציה, האתגר של צמצום הסיכון רק הולך וגדל. בשל חוסר ניראות וטלמטריה, צוותי אבטחת OT ו-IT לעתים קרובות מגששים באפלה, ואינם מודעים לכל נכסי ה-CPSs שכבר פרוסים בסביבתם ונמצאים תחת אחריותם.

ניהול סיכונים פרואקטיבי דורש יכולת לבחון ולטפל בסיכון מנקודות מבט שונות אך משלימות, כדי ליצור הקשר לאבטחה הכוללת של סביבת OT. תנאי קריטי לכך הוא להגיע להבנה ברורה של מיקום הנכסים שעליהם יש להגן ומיפוי של תעבורת הרשת בארגון. לפני הכל, יש להשיג נראות (Visibility) לרשתות ונקודות קצה של מערכות בקרה תעשייתית (ICS) ולרכז מידע אודות נכסי IT, OT, IoT ו-IIoT ללא צורך בקישוריות נוספת. בדרך זו, ממשקי אדם-מכונה (HMIs) ותחנות עבודה הנדסיות (EWS) יכולים לקבל מידע על איומי IT וחולשות, ולשפר את האבטחה של נכסים אלה מבלי להשפיע על הפרודוקטיביות של הארגון או להאריך את זמני ההשבתה.

מידע אבטחה המקושר לתעבורת רשת הוא גם המפתח לזיהוי ומעקב אחר איומים החוצים את גבול ה- IT/OT. התקפות רבות המשפיעות על סביבות OT מתחילות ברשת ה- IT, כך שגורמי ההגנה דורשים חתימות איום גם עבור התקני ICS ורשתות OT, בנוסף לאלה שנבנו עבור מערכות IT. טכנולוגיה המאבטחת CPSs, ללא צורך בתצורה מחדש של חתימות או עדכונים ידניים, מאיצה את הזיהוי והתגובה.

כלי IIoT הופכים במהירות לסימן ההיכר של סביבות OT מודרניות ולגורם המעניק יתרון תחרותי. בהתאם לכך, חשוב ליישם את התובנות הקיימות לגבי סיכונים ועלויות, ולאמץ את ההנחיות שהוצגו בתקנות החדשות, כדי להקדים את הסיכונים שמכשירי IIoT עשויים להביא עמם לסביבות תעשייתיות.

יניב ורדי, מנכ"ל קלארוטי - חברת אבטחת הסייבר התעשייתי

קרדיט צילום: קרן מזור