

"השאלה היא לא האם צי הרכב יותקף, אלא מתי ובאיזו עוצמה?"

חברת אניגמטוס, המתמחה באבטחת סייבר לצי רכב, פיתחה פתרון הגנת סייבר המספק ניטור וניתוח נתונים מעמיק והתראות בזמן אמת על פעילות סייבר זדונית. נטע למפרט, מנכ"ל החברה, מסביר מדוע הורדת זמן התגובה למינימום בצי היא קריטית ומדוע נדרש פתרון שמסתכל על רשת התקשורת של הרכב כעל יחידה אחת

נסף לבנון, בשיתוף אניגמטוס



נטע למפרט | צילום: מיה אפיס דבורין

בכבישי העולם נעים כ-1.5 מיליארד כלי רכב. המשמעות היא שעל הכביש נעים, למעשה, 1.5 מיליארד מחשבים על גלגלים. כ-90% מכלי הרכב המנוהלים במסגרת ציים מקושרים ומחוברים למערכות חכמות, למערכות דיאגנוסטיקה, לרכבים אחרים, לחניונים, לבניינים ולשלל אפליקציות. חיבורים וממשקים אלה יוצרים משטחי כניסה נרחבים לרכב, ובכך גדלה החשיפה לתקיפות סייבר - בדיוק כמו למחשב ולסמארטפון.

הבעיה הופכת לאקוטית יותר כשמדובר בצי רכב כגון משאיות, טנדרים ואוטובוסים, שלהם צריכים תפעוליים רבים. בעולם ישנם כ-100 מיליון כלי כאלה המנוהלים במסגרת ציי רכב. ניהול הצי מחייב את המנכ"ל, הדירקטוריון ומנהל הצי לקחת אחריות בנושא הסייבר ולערוך לביטחונם של הנהגים, הנוסעים והסביבה. כבר כיום נרשמות מדי שנה אלפי תקיפות סייבר נגד רכבים, תקיפות העלולות להוביל לאובדן חיי אדם, להשבתה תפעולית של צי הרכב ולפגיעה אנושה במוניטין, בהכנסות ובקניין של החברות המתפעלות וכן לדרישות כופה. גם חשיפה לתביעות היא סכנה משמעותית.

"השאלה היא לא האם צי הרכב יותקף, אלא מתי ובאיזו עוצמה", אומר נטע למפרט, מנכ"ל חברת אניגמטוס, המתמחה באבטחת סייבר לצי רכב. פתרון הגנת הסייבר שלה מספק ניטור וניתוח נתונים מעמיק והתראות בזמן אמת על פעילות סייבר זדונית. החברה מעסיקה מומחים מתחום הלוחמה האלקטרונית, הסייבר והביג דאטה וכבר רשמה עשרות פטנטים, המהווים בסיס טכנולוגי פורץ דרך לפעילותה הייחודית.

"עולם הסייבר והאוטומוטיב התחברו לפני לא מעט שנים וישנן כיום לא מעט יצרניות רכב המספקות פתרונות סייבר, אך הבעיה האמיתית מתחילה כשרכב מסחרי - ולא פרטי - יוצא משער המפעל", מוסיף למפרט. "בעוד שבמצב הרגיל ניתן לסמוך על אבטחת הסייבר של מכונית מן

השורה, כמעט בכל רכב מסחרי מותקנים אביזרי צד ג' נוספים, לצרכי ניהול ותפעול, בקרה ונייטור, המחברים לרשת התקשורת של הרכב. ומה אם לאחד מהם יש פרצות אבטחה? לצערנו, ידוע שלא כל מוצר עומד בתקן המחמיר של סייבר לאוטומוטיב."

אז מה הפתרון שלכם?

"פתרון שמסתכל על רשת התקשורת של הרכב כעל יחידה אחת ולא מבחין במקור ההודעה - בין אם מדובר במחשב מקורי של הרכב (ויש בין 80 ל-150 כאלה) ובין אם מדובר באחד מאביזרי צד ג', שהותקנו בו מיד כשיצא מהמפעל. כשבוחנים את כל הרכב, כולל האביזרים הללו, מתקבל ניטור סייבר אמיתי, מלא ושלם. מערכת אניגמטוס מסתכלת על רשת הנתונים באמצעות חיבור למערכות קיימות, כגון מערכות הטלמטריה המותקנות במעל ל-100 מיליון רכבים בעולם. הפתרון הוא למעשה הוספת 'שכבה נוספת' על המערכות הקיימות - שכבה המתייחסת להיבטי הסייבר על הצי. לאחרונה התחלנו ביישום הזה מול חברת 'פוינטר', איתה יש לנו שיתוף פעולה (ראה מסגרת).

"אפשרות נוספת המיושמת על ידינו כבר היום היא הטמעת הטכנולוגיה על חומרה ייעודית כפי

שבצענו ב-1,200 אוטובוסים של חברת התחבורה הציבורית דן. חשוב לציין כי המערכת שלנו נמצאת במצב של קריאה בלבד, מאזינה לרשת התקשורת ומנטרת אותה. במקרה של בעיה היא תתריע מייד, כשהיתרון הבולט שלה הוא מהירות התגובה. ידוע שבכל אירוע סייבר אחד מהפרמטרים החשובים להצלחה בהתגוננות הוא מהירות התגובה, וזכורים לא מעט מקרים, חלקם בישראל, שבגלל תגובה מאוחרת של צוות ה-IT - הנוק הפך לחמור הרבה יותר יכולת הניטור והניתוח בזמן אמת מורידה את זמן התגובה למינימום האפשרי. בעת אירוע סייבר אניגמטוס יודעת לתת תמונה מפורטת של האירוע, המסייעת לאנשי ה-IT בארגון לטפל בו במהירות וביעילות המקסימלית - ולמזער את הנוק. זהו חידוש משמעותי בשוק הזה, שרבים מהשחקנים בו יודעים להתריע על אירוע סייבר בדיעבד, להודיע שהוא התרחש. זה לא מספיק טוב."

מהיכן מגיעה היכולת הזאת?

"בדרך כלל, לפני שקורית התקפת סייבר מתקיימים עוד שני שלבים מקדימים: הראשון הוא בדיקת השטח, שבמהלכה ההאקר מחפש מהיכן הכי נכון יהיה להיכנס לרכב. מערכת אניגמטוס יודעת לזהות ניסיונות כאלה ולהודיע עליהם. השלב השני הוא ביסוס יכולת. ההאקר כבר מצא דרך להיכנס, מבסס יכולת שליטה באחד המחשבים ועושה תכנות מחדש. ברגע שלתוקף יש יכולת שליטה, הוא יבחר את המועד והזמן לבצע את התקיפה. גם על כך אניגמטוס יודעת להתריע. אם הלקוח התעלם מהאזהרות - המערכת גם תדע להתריע על תקיפה של ממש, בזמן אמת. בסיוע אנשי סייבר בכירים (לשעבר מכוחות הביטחון) יצרנו פרוטוקול תגובה לאירוע, המסדיר כיצד יש לנהוג בזמן ניסיון חדירה, ביסוס יכולת או אירוע סייבר אמיתי."

אחריות מנהלית על אירועי סייבר
תעשיית הרכב נמצאת במקום השלישי ברשימת נפגעי אירועי סייבר. חברות מחקר מעריכות שהנוק מכך בחמש השנים הקרובות יגיע ל-505 מיליארד דולר, לא מאוד רחוק מה-700 מיליארד שישפוג העולם התאגידי. צי רכב שהותקף עלול להיות מושבת מעבודתו ולהפסיד לחברה כסף רב. השבתה תימנע מתן שירות, תויק כך למוניטין ואולי אף תקלקל מוצרים - למשל, אם מדובר במשאית קירור הנמצאת בדרכה לספק בשר או חלב לרשתות שיווק. כמובן שהסיכון הגדול ביותר הוא של הנוסעים ברכב. ואם מדובר בתחבורה ציבורית, בה עשרות רבות של אנשים נוסעים באוטובוס אחד, זהו סיכון בלתי נתפס.

מעבר לסכנות עצמן, קיימת גם חובת האחריות. התקפת סייבר שמה את המנהלים במקום בו הם נדרשים לתת תשובות על הכשלים שאפשרו אותה, על חוסר עמידה ברגולציות אבטחת סייבר ואף עלולה להסתיים בתביעות בגין הנוקים שנגרמו. "אם חלילה קורה משהו - לא ילכו רק למנהל צי הרכב, אלא גם למנכ"ל ולמועצת המנהלים", מדגיש למפרט. "יש להם אחריות מנהלית על אירועי סייבר. לכן כשאנחנו מדברים עם ארגונים - זה לרוב קורה ישירות מול המנכ"לים. הם מבינים שהם לא יכולים להתעלם מהסכנה."

מי הם הלקוחות הבולטים שלכם?

"ציי הרכב של החברות דן, פיליפ מוריס ופוינטר. אנו נמצאים בתהליכי פיילוט עם גופים נוספים, כמו חברת האוטובוסים מטרופולין ונמל אשדוד. במקביל, אנו נמצאים בשלבים של יציאה לשווקים בין-לאומיים ומתקיים מו"מ עם ציי רכב מרכזיים מאוד בארה"ב ובאירופה."

בשיתוף חברת אניגמטוס