

מאת: בני אביעד

מפגש מקצועי מעניין ושובר שגרה בנושא אבטחת סייבר לרכב, נערך בשני סבבים (7.3.24, 14.3.24) בחברת אניגמטוס ביבנה לחברי איגוד קציני בטיחות בתעבורה. הכנס העניק כלים וידע הנדרשים בעידן של היום כדי להגן בפני התקפות סייבר, וכפי שחווינו בזוועות השבת השחורה בשביעי לאוקטובר אשתקד – מערך טכנולוגי מפואר לא נתן מענה הולם ומשלים ליישובי העוטף ולבסיסי צה"ל. ביום העיון הוצגו בפנינו פתרונות מקוריים שפותחו בחברת אניגמטוס לניטור וניתוח נתונים מעמיקים והתראות בזמן אמת על פעילות סייבר זדונית.

את דברי הפתיחה והברכה, על היוזמה של הנהלת חברת אניגמטוס לקיים אירוע חשוב זה ובלבביות ראויה לציון, נשא שמעון סודאי – יו"ר איגוד קציני בטיחות מקצועיים בתעבורה – שציין את נחיצות מעורבותם הפעילה והמאתגרת של קציני הבטיחות בתעבורה בעידן המשתנה והמתקדם בטכנולוגיות הרכב המודרני ובטיחותו. על המחוקק לתת את דעתו לגבי תוכניות לימודים עדכניות, הכוללות את שילוב כלי הרכב החשמליים, פתרונות טעינה, סייבר ודליפת מידע מהרכב. כדרכו בקודש, כמו בכל הכנסים שהתקיימו עד כה, הזכיר שמעון את שמותיהם של חברי האיגוד ובני משפחותיהם שנפגעו באירועי העוטף והלחימה בעזה.

נטע למפרט, מנכ"ל אניגמטוס, הרצה על תקיפות סייבר בעולם התחבורה והסביר מדוע הורדת זמן התגובה למינימום בצי רכב היא קריטית, ומדוע נדרש פתרון שמסתכל על רשת התקשורת כעל יחידה אחת. לדבריו, השאלה היא לא האם צי הרכב יותקף, אלא מתי ובאיזו עוצמה? הבעיה הופכת לאקוטית יותר כשמדובר בצי רכב כגון משאיות, טנדרים ואוטובוסים, שלהם צרכים תפעוליים רבים. 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 כופר. גם סכנה לתביעות היא סכנה משמעותית.

הרצאה מרתקת במיוחד שמענו מפי חמי פקר, מנהל מרכז הסייבר הלאומי לתחבורה חכמה, על לוחמת הסייבר במימד החמישי. מדינת ישראל היא מאוד חדשנית בחשיבה שלה על עולם הסייבר לתחבורה, ומטרת המרכז שהוקם בבאר שבע נועדה לאפיין את איומי הסייבר, לבדוק מערכות לפני שהן עולות על הכביש ולשמש מוקד ידע לאומי לתחום הסייבר לתחבורה חכמה. חמי עתיר ניסיון ומיומנות, ונבחר לתפקידו הלאומי לאחר שניהל במהלך 26 שנים את מנהלת הסייבר ממלכת-ביטחוני-מודיעיני במשרד רוה"מ, ניהל את חטיבת הסייבר במטה ללוחמה בטרור והמטה לביטחון לאומי ועוד תפקידים מרתקים. על פועלו הייחודי זכה בצל"ש פרס ביטחון ישראל.

מחמי פקר נחשפנו ללוחמה במרחב הדיגיטלי בהיבט המעצמות ועל שדה הקרב העתידי פורץ הגבולות. המעצמות הגדולות, בייחוד ארה"ב, סין ורוסיה, שיכללו את יכולות הסייבר ההתקפיות שלהן, ומסוגלות כיום לשתק מדינות שלמות בלחיצת כפתור. ללוחמת הסייבר מספר תכונות אופייניות: אנונימיות והגנה כמעט מוחלטת לתוקף, ארגז כלים התקפי בר-השגה, יכולת רכישת ידע קלה יחסית, יכולת פגיעה מגוונת בו-זמנית, קושי רב להבחין בתקיפה מוצלחת, בטן רכה במיוחד למותקף, לוחמת מוחות כחמה

המתקדשת בכל רגע ורגע, פוטנציאל נזק הרסני ביותר, ויתרון רב בלוחמה בעצימות נמוכה.

לירן צוויקל, סמנכ"ל סייבר באניגמטוס, הדגים כיצד מערכת לחץ אוויר בצמיגים יכולה לשמש כמשטח תקיפה לרכב. רשת ה-CAN ברכב משולבת בכל המערכות ומהווה מוקד לפריצות סייבר. המידע המתקבל מגוון וכולל הודעות על: לחץ אוויר בצמיגים, לחץ שמן, טמפרטורת מנוע, גובה מפלס נוזלים, לחץ אוויר במערכת הבלמים, עובי רפידות בלם, מהירות, זווית הגה ועוד נתונים רבים. החברה מעסיקה מומחים מתחום הלוחמה האלקטרונית, הסייבר והביג דאטה וכבר רשמה עשרות פטנטים, המהווים בסיס טכנולוגי פורץ דרך לפעילותה הייחודית.

עולם הסייבר והאוטומוטיב שלובים יחדיו וכיום יצרניות הרכב מספקות פתרונות סייבר, אך הבעיה האמיתית מתעוררת כשרכב מסחרי יוצא משערי המפעל ומוסיפים לו אביזרים ומכלולים נוספים - לצרכי ניהול ותפעול, בקרה וניטור, המחברים לרשת התקשורת של הרכב, ומה אם לאחד מהם יש פרצות אבטחה? לצערנו, ידוע שלא כל מוצר עומד בתקן המחמיר של סייבר לאוטומוטיב. הפתרון המוצע מסתכל על רשת התקשורת של הרכב כעל יחידה אחת ללא הבחנה במקור ההודעה.

מערכת אניגמטוס מסתכלת על רשת הנתונים באמצעות חיבור למערכות קיימות כגון הטלמטריה. למעשה מוסיפים שכבה נוספת על המערכות הקיימות המתייחסת להיבטי הסייבר של צי הרכב. אפשרות נוספת המיושמת כבר היום היא הטמעת הטכנולוגיה על חומרה ייעודית שבוצעה ב-1,200 אוטובוסים של חברת דן. המערכת נמצאת במצב קריאה, מאזינה לרשת התקשורת ומנטרת אותה. במקרה של בעיה היא תתריע מיידי, כשהיתרון הבולט שלה הוא מהירות התגובה.

האתגר בניטור סייבר בעולם האוטומוטיב הוא היכולת לזהות אירועים ברשת ה-CAN - שעשויים לרמז על פריצת סייבר. על כן, בשלב ראשון המערכת של אניגמטוס לומדת את המאפיינים הייחודיים של כל רכב בצי ומייצרת עבורו, באמצעות למידת-מכונה, פרופיל ייחודי. לאחר מכן, המערכת מנטרת בזמן אמת את ההודעות ברשת ה-CAN ומשווה אותן לפרופיל. כאשר המערכת מזהה חריגה מההתנהגות האופיינית, היא מפעילה תהליך אימות נוסף, מבוסס AI, כדי להסיק האם מדובר באירוע סייבר אפשרי.

הפלטפורמה של אניגמטוס היא פלטפורמת ענן, ואחד ההיבטים הקריטיים שמאפשרים את פעילותה הרציף היא יכולת דחיסת הנתונים שפיתחה החברה. לדברי אניגמטוס, היא מצליחה לדחוס את הדאטה שמייצר הרכב בשיעור של 99%, דבר שמאפשר את העברת הנתונים מהרכב לענן. אניגמטוס כבר רשמה לזכותה כ-18 פטנטים בטריטוריות שונות. בשנים האחרונות חלה התקדמות משמעותית בכל הנוגע ליישום סטנדרטים של אבטחת סייבר כחלק אינטגרלי מתהליך ייצור כלי רכב חדשים. הרגולטורים באירופה אימצו את תקן ISO/SAE 21434, שמסדיר את נושא אבטחת הסייבר בכלי-רכב, וכיום כל דגם חדש שיוצא לשוק חייב לעמוד בתקן.

דווקא בישראל, משרד התחבורה החיל רגולציה שנותנת מענה ללקונה הזו. לפי נהלי המשרד, כל מכרז בתחום התחבורה הציבורית חייב כיום לכלול דרישה לניטור סייבר של רשת פרוטוקול התקשורת CAN, וזאת כדי לנטר גם אביזרים חיצוניים שהותקנו באוטובוס. המגמה הזו של הרגולציה, להרחיב את התקינה אל עולם - after-market - היא אחד הזרזים העסקיים של חברת אניגמטוס מיבנה, הנמצאת במגעים מול חברות שזכו במכרזים, כדי לספק להן את שירות הסייבר, על מנת שיעמדו בתנאי משרד התחבורה. בנוסף, מבצעים פיילוטים עם ציים של חברות דלק, אנרגיה וחומרים מסוכנים.