לבן - TLP

בטחון, חרום וסייבר, משרד התחבורה

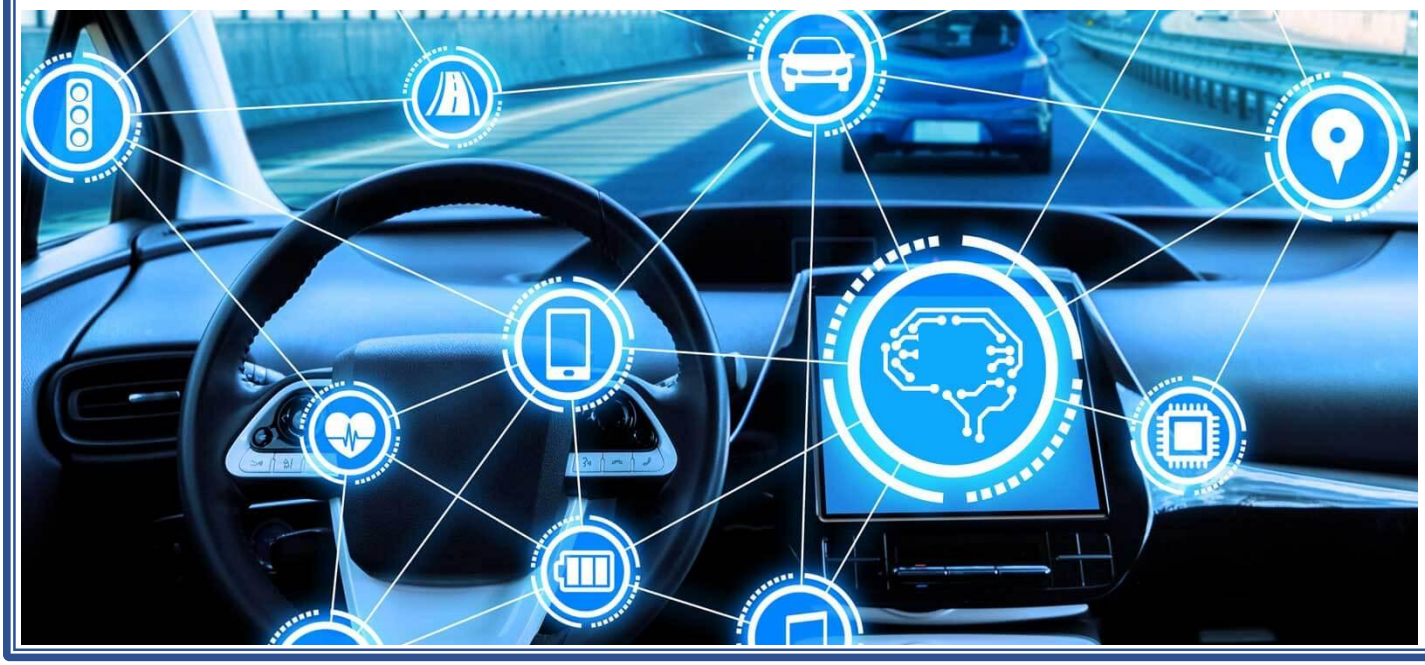
משרד התחבורה והבטיחות בדרכים

מנחה מקצועי - המלצות להגנה בסייבר בתחום הרכב

(עבור יבואנים ומוסכי שירות)

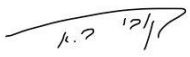
אגף הסייבר המגזרי ומנהל תנועה – משרד התחבורה

4000-0502-2025-000006



כתיבה ועריכה – טבלת עדכון:

גרסה	תאריך	מהות העדכון	כותב	תפקיד
1.0	08/26	גרסה להפצה	שירן אהרוני	רמ"ח סייבר בפרויקטים וחדשנות
			דוד רוזנברג	מנהל תחום בכיר טכנולוגיה וחדשנות

שם המאשר	תפקיד	חתימה	תאריך
קובי בן אהרון	ראש יחידת הסייבר המגזרית		08/26
אדי בן ליש	ראש מנהל תנועה		08/26

תוכן עניינים

1. כללי

1.1. רקע

עם התפתחות הטכנולוגיה והקישוריות, אנו עדים לעלייה חדה בכמות ובחומרה של אירועי סייבר המשבשים את פעילותם התקינה של ארגונים ומערכות. אירועים אלה עלולים לגרום **לפגיעה משמעותית ברציפות התפקודית והעסקית, מניעת שירות לתהליכים מרכזיים במשק ובמקרים מסוימים אף לסיכון חיי אדם.**

מגמה זו הופכת מרכזית גם בתחום התחבורה החכמה ותעשיית כלי הרכב. כלי הרכב של העידן הנוכחי מקושרים, עתירים בטכנולוגיה, ומורכבים מעשרות מערכות ורכיבי מחשוב (לדוגמא - מעבדים, סנסורי איסוף מידע וחיישנים) המתקשרים פנימית ברכב וחיצונית לו, משדרים נתונים, וחושפים את הרכב לחולשות אבטחה. בנוסף, התפתחות ושילוב של טכנולוגיות בינה מלאכותית, ובמיוחד פלטפורמות בינה יוצרת (Generative AI), עתידים להעצים משמעותית את מתקפות הסייבר, שכן, הן כבר אינן נחלתם של מומחים בלבד, אלא מבוצעות על ידי מודלי AI המסוגלים לאתר ולנצל חולשות Zero-day באופן אוטונומי ומהיר. **בהיעדר מנגנוני הגנה, עלולים כלי הרכב להוות יעד אטרקטיבי לתקיפות סייבר המסכנות את פרטיות ובטיחות הנהגים.**

בעוד **שקיימות דרישות רגולציה מחייבות החל מיולי 2024 (רגולציית UNR155[1] ו- UNR156[2]) אודות אבטחת מידע וסייבר עבור ייצרני הרכב,** המתמקדות בתהליכי ומנגנוני הגנה לתהליכי ייצור הרכב ורשתות היצרניות, **תחומי היבוא, התפעול והתחזוקה** של הרכבים אינו **מקבל מענה הולם** במשוואת אבטחת המידע והסייבר.

על כן, **<u>מומלץ ליבואנים ולמוסכים לגבש ולהטמיע תהליכים ואמצעים אשר ישפרו את רמת ההגנה בסייבר בסביבת הארגון וכלי הרכב,</u>** וזאת במטרה לשמר את רמת ההגנה ברכב (עמו הוא מגיע), להפחית את רמת

[1] https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf
[2] https://unece.org/sites/default/files/2024-03/R156e%20%282%29.pdf

הסיכון לאורך כל מחזור חייו **לטובת בטיחות והגנה על משתמשי הדרך ולאפשר מתן שירות סדיר וזמין למקבלי השירות.**

לאור המציאות והאיומים המתפתחים, משרד התחבורה (יחידת הסייבר המגזרית בשיתוף מנהל תנועה) גיבש במסגרת סמכותו **<u>מסמך המלצות זה</u>**.

1.2. **<u>מטרת המסמך</u>**

הגדרת בקרות סייבר ואבטחת מידע המומלצות ליישום עבור יבואני רכב ומוסכי שירות לטובת שמירה על רמת אבטחת הסייבר של כלי הרכב, הגברת החוסן הארגוני, צמצום אירועי הסייבר או לחילופין התמודדות יעילה במידה ויתרחשו.

כלל ההמלצות המובאות במסמך זה נועדו לצורך מתן הכוונה מקצועית**. במידה והארגונים יחליטו ליישם אותן, את חלקן או כולן, הן אינן מחליפות הנחיות או דרישות של יצרני הרכבים עצמם, או דרישות חוק אחרות.**

1.3. **<u>תפיסת ההגנה ועקרונות מנחים</u>**

1.3.1. כ- 96% מהרכבים המיובאים לישראל הינם רכבים העומדים בתקינת הרכב האירופאית (ללא קשר לארץ יצורם), ולכן **כהנחת יסוד היא כי הרכבים המגיעים לישראל (החל מיולי 2024) עומדים בדרישות הגנת הסייבר**:

1.3.1.1. UNR155- רגולציה זו מנחה את יצרני הרכב ליישם תהליכים ומנגנוני ההגנה בסייבר עבור תהליכי ייצור הרכב בהיבט הפלטפורמה, כלומר כלי הרכב עצמו.

1.3.1.2. UNR156 - רגולציה זו מנחה את יצרני הרכב ליישם תהליכים ומנגנוני ההגנה בסייבר עבור תהליכי העברת תוכנה ו/או קושחה אל/מהרכב באופן ידני או אוטומטי דרך האוויר (OVER THE – OTA AIR).

1.3.2. בכדי **לשמר את רמת ההגנה ברכב**, **להפחית את רמת הסיכון לאורך כל מחזור חייו ולאפשר מתן שירות סדיר וזמין למקבלי השירות**, מומלץ ליישם ולהטמיע דרישות הגנה ארגוניות ותפעוליות על פי העקרונות הבאים:

1.3.2.1. הוליסטיות – הגנת הסייבר מהווה נדבך בלתי נפרד מהניהול השוטף של היבואן והמוסך. אין להסתפק בפתרון נקודתי לבעיה מקומית, אלא לשלב שיקולי סייבר ואבטחת מידע בכל שלבי הפעילות העסקית, החל מתכנון מדיניות הארגון ועד לפעולות תפעול ותחזוקה יומיומיים, תוך הגדרה ברורה של סמכות ואחריות בכל רמה.

1.3.2.2. ניהול סיכונים – מיפוי והבנת הסיכונים העיקריים הנובעים מאופן פעילותו. משאבי ההגנה והבקרה יחולקו בהתאם לדרגת הסיכון ולא לפי גישה גורפת.

1.3.2.3. הגנה בשכבות – המבנה הארגוני והתהליכי של היבואן והמוסך יתבסס על שכבות הגנה מרובות, החל מנקודת הקצה (הרכב ומערכות האבחון), דרך מערכות ה-IT הארגוניות, שרשרת אספקה, ועד לרמת המדיניות והפיקוח הניהולי.

1.3.2.4. הפרדה ובידול רשתות – הפרדת הרשת (פיזית/לוגית) הארגונית (מנהלית/משרדית) מזו התפעולית המשמשת את המוסך (במידה וקיימת), בדגש על מכשירי אבחון הרכב ו/או ציוד המתממשק לכלי הרכב בפועל.

1.3.3. להלן טבלה המציגה חלוקה לפי רמות סיכון בהתבסס על התפתחות טכנולוגית של הרכבים והתפתחות הרגולציה בהתאם לתאריכי ייצור הרכב.

קריטריון / תאריך ייצור רכב רגיל	עד 2013	2014 עד יוני 2022	החל מיולי 2022 עד יוני 2027	החל מיולי 2027 ואילך
רמת הסיכון בנגזרת מניתוח תרחישי האיומים והסיכונים	מזערית	נמוכה	בינונית	גבוהה
דרישות רגולציה אירופאית לרכבים	ללא	ללא	עמידה ברגולציות UNR155 ו- UNR156 • החל מיולי 2022 עבור כל אב טיפוס לרכב **מדגם חדש** • החל מיולי 2024 עבור **כל** אב טיפוס **לרכב חדש**	עמידה ברגולציות UNR155 ו- UNR156 עבור **כל** אב טיפוס **לרכב חדש**
דרישות ארגוניות	בהתאם למנחה מקצועי זה			
דרישות תפעוליות	בהתאם למנחה מקצועי זה			

1.4. **<u>תחולה</u>**

המלצה זו רלוונטית ליבואני רכב ומוסכי שירות, ומכילה המלצה לבקרות הגנה בסייבר בחלוקה הבאה:

1.4.1. המלצות לבקרות ארגוניות עבור יבואן.

1.4.2. המלצות לבקרות תפעוליות

1.4.2.1. עבור יבואן לביצוע בדיקות PDI.

1.4.2.2. עבור מוסך שירות לתפעול ותחזוקת הרכב.

נדגיש כי בכל הקשור לפעולות תחזוקה ברכב נדרש להמשיך לפעול על פי הנחיות יצרן הרכב. כלל ההמלצות והדגשים המובאים במסמך זה מטרתם לספק מעטפת הגנה נוספת להפחתת סיכוני סייבר ועל כן ראוי ונכון שכלל הגורמים הרלוונטיים יאמצו ויישמו אותם בהתאם לניהול סיכונים ארגוני.

1.5. **<u>מושגים והגדרות</u>**

אבטחת/הגנת סייבר – כל הפעולות שתכליתן להגן על נכסי הסייבר של ארגון מפני תקיפת סייבר .

אירוע סייבר – התרחשות אשר מעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, שקיים יסוד להניח, כי היא נובעת מפעילות מכוונת במרחב הסייבר.

אירוע סייבר ברמת איום גבוהה – אירוע אבטחת מידע או תקיפת סייבר המהווה איום משמעותי על ארגון או מערכת קריטית, ועשוי לגרום לפגיעה חמורה בתפקוד, במידע או בנכסים אסטרטגיים של הארגון. לדוגמא נזק תפעולי חמור, אובדן או דלף מידע רגיש, איום על בטיחות הציבור, נזק כלכלי גדול, השלכות רגולטוריות ומשפטיות וכו'.

בקרה מפצה – אמצעי אבטחה חלופי המיושם כאשר הבקרה הראשונית או המועדפת אינה ניתנת ליישום, מטעמים תפעוליים, טכניים או כלכליים. הבקרה המפצה מספקת רמת הגנה שוות ערך או מפחיתה את הסיכון לרמה קבילה, ומגשרת על הפער.

התקנים - כל רכיב חומרה בעל יכולת אחסון/ שמירה/ העתקה/ מחיקה/ שכפול של קבצים, אפליקציות, תכנים , תוכנה וקושחה.

ווקטור תקיפה / ווקטור האיום – דרך/שיטה המשמשת תוקף לגישה לא חוקית לרשת, רכיב או מערכת על מנת להשיג אחיזה. ווקטורי תקיפה נפוצים כוללים התקפות הנדסה חברתית, גנבת אישורים, ניצול פגיעויות, והגנה לא מספקת מפני איומים פנימיים.

חולשה – נקודת תורפה במערכת ממוחשבת או ברכיב שלה או בנוהל הקשור אליה אשר ניתן לנצלה כדי לחולל אירוע סייבר.

יבואן – כהגדרתו בחוק "רישוי שירותים ומקצועות בענף הרכב תשע"ו 2016".

כלי רכב מקושרים – כלי רכב עם יכולת לתקשר בצורה דו כיוונית אלחוטית עם מערכות אחרות מחוץ לרכב.

מוסך שירות - כל מוסך כהגדרתו בחוק "רישוי שירותים ומקצועות בענף הרכב תשע"ו 2016".

מוצר תעבורה רגיש – כל מוצר תעבורה כהגדרתו בחוק "רישוי שירותים ומקצועות בענף הרכב תשע"ו 2016", שהוא בעל מעבד או רכיב אלקטרוני ואשר יש לו השפעה בטיחותית לרכב ומערכותיו.

סייבר – ביטוי המתייחס, במובנו הרחב, למערכות מחשוב, רשתות מחשבים והתקשורת ביניהן. במובן צר יותר, הביטוי מתייחס לפעילות ההגנתית וההתקפית המתרחשת בתוך מערכות המחשוב והתקשורת ברחבי העולם.

ציוד תמיכה – כל ציוד המשמש להעלאה/הורדה של תוכנה, קושחה, קבצים, אפליקציות או תכנים, לבדיקות דיאגנוסטיקה, אחזקה ותיקון של מערכות הרכב, ו/או כזה שיש לו ממשק עקיף ו/או ישיר עם מערכות הרכב המשמש לכל מטרה.

קושחה – תוכנה המשובצת בהתקן חומרה ומטפלת בתפקוד הרכיב.

רכב – כל כלי רכב מקטגוריית M ו-N שאינו בעל מערכת נהיגה עצמאית כהגדרתו בסימן ו' לפקודת התעבורה, הנע על 4 גלגלים או יותר, ללא קשר לשיטת ההנעה, כולל רכב פרטי, משאיות, אוטובוסים וסמיטריילרים.

תוכנה – אוסף של הוראות ומידע הניתנות לביצוע על ידי מעבד/מחשב. התוכנה משמשת להפעלת המחשב וחומרות נלוות, לביצוע משימה או אוסף משימות.

תקיפת סייבר – תקיפה במרחב הסייבר שמסכנת נכסי סייבר או מערכות ותשתיות הנתמכות על ידם.

After market - מערכות אשר מותקנות ברכב בהתקנה מקומית.

CANBUS - רשת תקשורת – רשת התקשורת ברכב המשמשת לקישור בין מרכיבים שונים ברכב.

COC (Certificate of Conformity) – מסמך המופק ע"י יצרן הרכב המאשר שהרכב הספציפי (על פי מספר שילדה) תואם לדגם הרכב המאושר ולכן עומד בכל דרישות התקינה האירופית המחייבות ליום הוצאת אישור הדגם.

CSMS – Cyber Security Management System.

PDI – Pre-Delivery Inspection.

RIA – Regulation Impact Analysis.

TARA - Threat Analysis and Risk Assessment.

certificate (Whole Vehicle Type Approval) **WVTA** – מסמך התעדה רשמי מטעם אחת מרשויות האישור האירופאיות (במדינות החברות באיחוד) המאשר שדגם הרכב עומד בכל דרישות התקינה האירופית המחייבת.

2. המלצות לבקרות ארגוניות מיבואן

2.1. **אחריות הנהלה**

2.1.1. אימוץ תקן ISO27001 כאשר התיחום כולל את כל מערכות הליבה והנכסים הקריטיים לארגון. מומלץ לשמר את ההסמכה באמצעות מבדקים/סקרים תקופתיים (אחת לשנתיים). ממצאי המבדקים/הסקרים ותוכנית לטיפולם יוצגו להנהלת הארגון ויאושרו ע"י גורם ניהולי מתאים (מנכ"ל/ועדת ביקורת של הדריקטוריון).

2.1.2. עמידה בחוק הגנת הפרטיות, תשמ"א – 1981 ותקנות שהותקנו מכוחו, לרבות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017.

2.1.3. כתיבת מסמך מדיניות סייבר ארגונית בהתאם לאיומים ורמת הסיכון, אשר תשקף את עקרונות הוראה זו, ותתוקף אחת לשנה. המדיניות תתייחס לכלל המנגנונים ודרכי הפעולה המרכיבים את מערך ההגנה ויוקצו משאבים נדרשים למימושה.

2.1.4. לצורך יישום מדיניות הסייבר הארגונית, הנהלת הארגון תקצה כוח אדם מיומן וייעודי לנושא ההגנה בסייבר אל מול הסיכונים, הצרכים והמערכות הקיימות בארגון, ובין היתר תמנה את בעלי התפקידים הבאים:

2.1.4.1. ממונה הגנה בסייבר אשר אחראי לתכלל את מאמצי ההגנה בסייבר על מערכות התקשוב הארגוניות ולפעול בהתאם להוראות, לנהלים ו- best practice להגנת הסייבר בארגון. הממונה יהיה עובד החברה, חבר הנהלה או כפוף לחבר הנהלה, באופן שבו יימנעו, ככל הניתן, ניגוד עניינים.

2.1.4.2. מנהל הגנה בסייבר אשר מהווה גורם מקצועי ואחראי על הכנה ויישום של תוכניות העבודה למימוש מדיניות הגנת הסייבר בארגון. מנהל הגנה בסייבר יכול להיות גם ממונה הסייבר (בתנאי שעומד בהגדרה לעיל), לחילופין, ניתן להעסיק מנהל הגנת סייבר (שאינו ממונה הסייבר) במיקור חוץ, בהיקף משרה פרופורציונלי לגודל הארגון.

2.1.5. הקמת וועדת היגוי להגנת הסייבר בראשה יעמוד מנהל בכיר מהארגון (בדרגת סמנכ"ל לפחות), ויהיו חברים בה ממונה הגנת הסייבר, מנהל הסייבר ובעלי תפקידים רלוונטיים. מומלץ שהועדה תתכנס לפחות אחת לחצי שנה לעדכונים וקבלת החלטות בנושאי הגנת הסייבר, ובין השאר תאשר את הערכות הסיכונים ואת תוכניות העבודה והמשאבים לטיפול בפערים שנמצאו בביקורות וסקרים תקופתיים. נושאים מרכזיים המומלצים לדיון בוועדה – מעקב משימות תוכנית עבודה, כשירות מערכות ההגנה, תוכנית סקרי סיכונים והצגת ממצאים, תוכנית המשכיות עסקית והתאוששות, אירועי סייבר שהארגון חווה, סטאטוס הגנה לספקים מהותיים (ניהול שרשרת אספקה).

2.1.6. הנהלת הארגון תמסד ערוצי תקשורת וממשקי עבודה שוטפים מול גורמי הסייבר ואבטחת המידע של יצרן הרכב. הממשק יבטיח קבלת עדכונים רציפים אודות חולשות אבטחה ועדכוני תוכנה/קושחה נדרשים, לצד הגדרת נהלי דיווח והסלמה הדדיים בזמן אמת בעת זיהוי אירועי סייבר ברכבים או במערכות השירות.

2.2. **<u>המלצות ליישום והטמעת מערכת ניהול הגנה בסייבר – CSMS</u>**

2.2.1. מערכת (אקוסיסטם) לניהול הגנה בסייבר פירושה גישה שיטתית מבוססת סיכונים המגדירה תהליכים ארגוניים, אחריות ומשילות לטיפול בסיכון הכרוך באיומי סייבר לדוגמא על מרכיבי כלי הרכב, תהליכי העבודה, מערכות ותשתיות, שרשרת האספקה ובאופן רחב על כל הנדרש מבעלי העניין, על מנת להגן מפני מתקפות סייבר ולכן כדאי שתכלול תיעוד של כלל התהליכים, המסמכים, הנהלים והתצורות הרלוונטיות למערכות השונות ומנגנוני בקרה טכניים לטיפול באיומים אלה.

2.2.2. ראוי שהיכולות הנדרשות מסביבה תומכת לניהול הגנה בסייבר (CSMS) יתנו מענה לכל הפחות בתחומים הבאים:

2.2.2.1. <u>טיפול וניהול סיכונים</u>

2.2.2.1.1. הגנת הסייבר בארגון תתבסס על תהליך של ניהול סיכונים, במסגרתו יזוהו האיומים והסיכונים הרלוונטיים לארגון

שעלולים להתממש כתוצאה מפגיעה בנכסי הסייבר (בדגש רב על איומים של סיכון חיי אדם או פגיעה בבריאותו, פגיעה ברציפות מתן השירות, נזק כלכלי משמעותי).

2.2.2.1.1.1. ביצוע תהליך מיפוי עבור הנכסים החיוניים התומכים בתהליכים מרכזיים של הפעילות, ניהול רשימת חומרות, תשתיות, תוכנות, אפליקציות ותרשים ארכיטקטורת רשת עדכנית של הארגון. הנכסים יסווגו לנכסים קריטיים, מהותיים ורגילים.

2.2.2.1.1.2. ביצוע תהליך ניהול סיכונים ויישום הגנת סייבר עבור כלל המערכות והרשתות המשמשות את הארגון בין אם הן מנוהלות על-ידי הארגון ובין אם על ידי צד שלישי. מומלץ לבצע או לתקף את התהליך אחת לשנתיים ו/או בעת שינויים מהותיים, המוקדם מבין השניים. מומלץ לשים דגש על תהליכים תפעוליים והשלכות עסקיות מהפעילות התפעולית.

2.2.2.1.2. בניית תוכנית רב שנתית לביצוע סקר סיכונים ומבדקי חוסן תקופתיים למוצרי אבטחה, מערכות, אתרי האינטרנט ואפליקציות לשירות הציבור, תשתיות ותהליכים מרכזיים שיבוצעו על ידי חברה חיצונית בלתי תלויה המתמחה בתחום אבטחת מידע וסייבר:

2.2.2.1.2.1. סקר סיכונים טכנולוגי רחב – אחת ל-18 חודשים.

2.2.2.1.2.2. מבדק חדירות תשתיתי/אפליקטיבי בהתאם לניהול סיכונים ולכל הפחות אחת ל-18 חודשים או בעת שינוי ארכיטקטוני משמעותי במערכות הליבה.

2.2.2.2. <u>טיפול וניהול המשכיות השירות ותפעולו</u>

בניית תכנית המשכיות עסקית והתאוששות מאסון, הכוללת בין היתר, תכנית להתמודדות עם משבר שמקורו באירוע סייבר ואבטחת מידע ואופן העבודה השוטפת תחת איום קיים. מומלץ

לקחת בחשבון היערכות טכנולוגית בהיבטי מערכות הגנה וניטור, הגדרת צוות היערכות וניהול משבר (ניהולי וטכנולוגי), כתיבת playbooks וביצוע תרגילים ניהוליים וטכניים לזיהוי פערים והפקת לקחים.

2.2.2.3. <u>בניית תכניות עבודה והקצאת משאבים</u>

בניית תוכנית עבודה שנתית ו/או רב-שנתית, אשר תכלול את יישום דרישות מדיניות הגנת הסייבר הארגונית, ומתן מענה לפערים אשר יעלו במסגרת תהליך ניהול הסיכונים, המשכיות השירות ויוקצו משאבים הולמים למימושה.

2.2.2.4. <u>הדרכות ומודעות עובדים</u>

בניית תוכנית הדרכות שנתית מותאמת לאוכלוסיות השונות (עובדים כלליים, בעלי תפקידים רגישים, דרגי הנהלה וכו') להעלאת מודעות אשר תקיף את כלל העובדים והמנהלים בארגון. מומלץ שהתוכנית תכלול לכל הפחות הדרכות ותרגולים בתחום הארגוני והתפעולי (תרגולים ניהוליים ותרגולים טכניים/תפעוליים) לשיפור ושימור הידע ויבוצעו אחת לשנה.

2.2.2.5. <u>טכנולוגיות הגנה</u>

2.2.2.5.1. הקמת והפעלת מערך ההגנה **כמענה לניתוח איומים וניהול סיכונים, עם יכולת עדכון והתאמה**, וזאת לאור האופי המשתנה של איומי הסייבר וחומרתם.

2.2.2.5.2. הטמעת פתרונות וטכנולוגיות הגנה בארגון עבור סוגי האיומים הבאים לכל הפחות:

2.2.2.5.2.1. פגיעה בבטיחות – האיום לפגיעה ברכב ורמת הבטיחות המסופקת למשתמש.

2.2.2.5.2.2. פגיעה בשלמות ואמינות – האיום לשיבוש או פגיעה בשלמות, בדיוק או באמינות המידע כגון הונאה, מידע המועבר בין מערכות היבואן למוסך השירות, מידע אודות כלי הרכב, מידע המסופק לצרכנים, וכד'

2.2.2.5.2.3. פגיעה בזמינות – האיום למניעת יכולת לצרוך ולתת שירותים ו/או שימוש במידע ע"פ הנדרש מהם.

2.2.2.5.2.4. דלף מידע ופגיעה בצנעת הפרט – האיום לחשיפה או גישה לא מורשת למידע רגיש/פרטי ע"י גורמים מורשים ולא מורשים.

2.2.2.6. <u>תשתיות ושירותי ענן</u>

2.2.2.6.1. אימוץ תשתיות ושירותי ענן באופן אחראי, כלומר, יבוצע הליך בחינה והערכה של הסיכונים הרלוונטיים ובניית תוכנית ליישום והטמעה של בקרות לצורך הבטחת רמת הגנה נאותה ובאופן שימזער סיכונים אלה. מומלץ לוודא הקשחת הסביבה ותצורת האבטחה בהתאם להמלצות וסטנדרטים בינלאומיים מקובלים, ועמידה בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.

2.2.2.6.2. מתן עדיפות מקצועית ואבטחתית לשימוש בתשתיות ענן הממוקמות פיזית בשטח הריבוני של מדינת ישראל.

2.2.2.6.3. ביצוע בדיקת נאותות לספק הענן ולדרוש הצגת אסמכתאות תקפות לעמידה בסטנדרטים בינלאומיים כדוגמת תקני ISO27017 ו- ISO27018 (או מקביליו), כאשר התיחום יכלול את כל התשתיות והמערכות אשר הארגון מפעיל. ככל וניתן, חוזה ההתקשרות עם ספק הענן יכיל פרק הגנת סייבר מפורט, רמת השירות הנדרשת לזמינות ואבטחה, הגדרה ברורה של מודל האחריות המשותפת, ואת כלל ההגנות הנדרשות באבטחה ושמירה על הסביבה והמידע.

<u>הערה:</u> בהתקשרות מול ספקי ענן ציבוריים גלובליים, שבהם אין ללקוח יכולת להכתיב סעיפים בחוזה מול ספקי המשנה, ניתן להסתמך על הצגת תעודות תאימות תקפות ורלוונטיות (כגון ISO 27001 הכולל בקרות ניהול ספקים או דוח SOC 2 Type II) כחלופה לדרישה החוזית הישירה.

2.2.2.7. <u>טיפול וניהול פגיעויות</u>

2.2.2.7.1. ביצוע מעקב, ניהול והפצה של עדכוני אבטחת מידע ומערכות הפעלה לכלל המערכות, התחנות, הרכיבים וההתקנים בארגון. מומלץ להגדיר את פרק הזמן לביצוע העדכונים במסגרת המדיניות הארגונית.

2.2.2.7.2. ניהול תצורה ויישום הקשחות ע"פ Best practice המקובלים בשוק ו/או הנחיות יצרן.

2.2.2.7.3. ככלל, הימנעות משימוש במערכות/רכיבים אשר מוגדרים END OF LIFE (EOL) / END OF SUPPORT (EOS).

במקרים חריגים שבהם נדרש שימוש ברכיבים אלו, מומלץ ליישם מענה הגנתי הולם באמצעות בקרות מפצות.

2.2.2.8. <u>ניטור והיערכות לאירועי סייבר</u>

2.2.2.8.1. יישום מנגנוני רישום ואיסוף לוגים לצורך ניטור, זיהוי והתראה על אירועים חריגים. מומלץ שהניטור יופעל לכל הפחות עבור מערכות הגנה, ממשקי ניהול, תשתיות, מערכות תפעוליות מרכזיות, אפליקציות ועמדות הקצה.

2.2.2.8.2. ניטור באמצעות SIEM/SOC פנים-ארגוני או כשירות של חברה חיצונית (MSSP), או לחילופין קיום יכולת לאיסוף לוגים מקומית ולשמירתם למשך חצי שנה לפחות לצורך תחקור אוחר בעת חשד לאירוע/ אירוע סייבר.

2.2.2.8.3. פיתוח יכולת להפעלת צוותי תגובה (IR) לניהול וחקירת אירוע סייבר על כל היבטיו כולל יכולת תחקור, הסקת מסקנות והוצאת המלצות בהתאם.

2.2.2.8.4. דיווח ליחידת הסייבר המגזרית[3] של משרד התחבורה על אירוע סייבר ברמת חומרה גבוהה (דלף, כופרה, השבתת שירות משמעותי, פגיעה ברכבים וכד') יעשה בהקדם האפשרי ולא יאוחר מ-24 שעות. יובהר כי דיווח זה אינו חליף או בא במקום כל דיווח אחר הנדרש על פי חוק.

[3] תיבת מייל לצורך דיווח על אירוע סייבר - agafcybersec@mot.gov.il

2.2.2.9. <u>טיפול וניהול בשרשרת אספקה</u>

2.2.2.9.1. ביצוע מיפוי של הספקים להם קיימת השפעה על נכסי הארגון כמו: בעלי גישה מרחוק למערכות המידע, ספקי תמיכה טכנית, ספקים שמאחסנים או מעבדים מידע של הארגון, נותני שירותים, ספקי ציוד תעבורה רגיש , ספקים בעלי גישה פיזית לחצרות הארגון וכו'.

2.2.2.9.2. ביצוע הערכה ודירוג של הספקים לפי רמת הסיכון הנשקפת לארגון ולתהליכים המרכזיים שלו כתוצאה מפגיעה בספק: ספקים מהותיים, ספקים המהווים סיכון בינוני וסיכון נמוך.

2.2.2.9.3. אחת לשנה מומלץ לבצע תיקוף עבור רמת ההגנה של כלל הספקים המהותיים באמצעות דרישה למענה על שאלון ספקים בהערכה עצמית.

2.2.2.9.4. בהתאם לממצאי השאלונים, ביצוע הערכת סיכונים עם כל אחד מהספקים הרלוונטים, ע"פ מתודת שרשרת האספקה של מערך הסייבר הלאומי[4] ו/או בהתאם ל-BEST PRATICE בתעשייה ולגבש תוכנית לצמצום והפחתת הסיכונים מול הספקים בכלים העומדים לרשות הארגון.

2.2.2.10. <u>טיפול וניהול היבטי חוזים והתקשרויות</u>

2.2.2.10.1. הכנסת דרישות סייבר במכרזים והתקשרויות חדשות, בהתאם לדירוג הסיכון של הספק.

2.2.2.10.2. הטמעת תהליך לבדיקת רמת הגנת סייבר של המוצר בתהליכי רכש של מוצרי מדף.

2.3. **<u>דיווח וביצוע ביקורות</u>**

2.3.1. קיום ביקורות ומבדקים פנימיים לבחינת רמת הגנת הסייבר בארגון, אחת לשנה לכל הפחות.

2.4. **<u>הפצת עלון שירות לצרכן</u>**

[4] https://www.gov.il/he/pages/querysupply

2.4.1. היבואן יספק לצרכן שרוכש רכב חוברת הסבר - "עלון מידע לצרכן להתנהלות בטוחה" על מנת לספק הגנה מקסימלית על מערכות הרכב – ראה נספח א'.

3. המלצה לבקרות תפעוליות - לביצוע בדיקת PDI ומתן שירותי תפעול ותחזוקת הרכב במוסכים.

ההמלצות המובאות בפרק זה מתייחסות לארגונים המבצעים בפועל את הפעילויות התפעוליות, אם במסגרת בדיקות טרום מסירה (PDI) המבוצעות ע"י היבואנים, או במהלך שירותי התחזוקה והתיקון השוטפים במוסכים ובמרכזי השירות.

3.1. אחריות הנהלה

3.1.1. הגדרת מדיניות, תהליכים וכתיבת נהלי סייבר תומכים בהיבטי הגנת סייבר, אשר ישקפו את עקרונות המלצה זו, ויתוקפו אחת לשנתיים לכל היותר. הנהלים יתייחסו לכלל המנגנונים ודרכי הפעולה עבור מתן שירותי תפעול ותחזוקה בדגש למערכות ורכיבים המתממשקים לרכב באופן ישיר/עקיף ובהתאם להקצות את המשאבים הנדרשים למימושם.

3.1.2. לצורך יישום נהלי הסייבר, מומלץ למנות נאמן סייבר שיהיה אחראי על הגדרת, יישום ומימוש פתרונות ההגנה בהתאם להוראות, לנהלים ול-best practice להגנה בסייבר. הנאמן יהיה עובד חברה שהוכשר לכך / יועץ חיצוני.

3.1.3. בניית תוכנית עבודה שנתית/רב שנתית אשר תכלול את יישום דרישות המדיניות, נהלי הסייבר, העלאת מודעות (בדגש על תפקידים רגישים במוסך) ומתן מענה לפערים אשר יעלו במסגרת הליך ניהול הסיכונים (כמוגדר בסעיף 3.2).

3.2. טיפול וניהול סיכונים

3.2.1. הגנת הסייבר במוסך תתבסס על תהליך של ניהול סיכונים, במסגרתו יזוהו האיומים והסיכונים הרלוונטיים למוסך שעלולים להתממש כתוצאה מפגיעה בנכסי הסייבר (בדגש רב על איומים המשפיעים על הבטיחות והשירות לצרכן).

3.2.2. ביצוע תהליך מיפוי וסיווג עבור הנכסים החיוניים התומכים בתהליכי תפעול ותחזוקה של כלי הרכב.

3.2.3. ביצוע הליך ניהול סיכונים ויישום הגנת סייבר עבור כלל המערכות, הרכיבים והציוד המשמשים את המוסך בין אם הם מנוהלים על-ידי

המוסך ובין אם על ידי צד שלישי. מומלץ לבצע או לתקף את התהליך אחת לשנתיים ו/או בעת שינויים מהותיים, המוקדם מבין השניים. מומלץ לשים דגש על תהליכים תפעוליים והשלכות מהפעילות התפעולית.

3.3. **<u>תהליכי תפעול ותחזוקה</u>**

3.3.1. לצורך ביצוע תהליכי תפעול ותחזוקה ברכב, מומלץ להגדיר מי מבעלי התפקידים במוסך מורשים:

3.3.1.1. להשתמש בכלי תוכנה , תוכנה, קושחה, ציוד תמיכה, התקנים, ציוד תעבורה רגיש ונקודות התממשקות / גישה למערכות הרכב.

3.3.1.2. לתקן ולכייל ציוד תמיכה, התקנים וציוד תעבורה רגיש.

3.3.2. ביצוע עדכוני מערכת הפעלה ועדכונים אבטחתיים (PATCHES) לכלי תוכנה, ציוד תמיכה והתקנים, בהתאם להוראות יצרן.

3.3.3. בהינתן שקיים חומר קריפטוגרפי (תעודות הזדהות, מפתחות הצפנה וכיו"ב) הקשור בכלי תוכנה, תוכנה/קושחה, התקנים, ציוד תמיכה וציוד תעבורה רגיש ברכב ומערכותיו, מומלץ לאחסן את החומר בצורה מאובטחת והגדרת נהלים מתאימים לאופן הטיפול בחומרים אלו.

3.3.4. הגדרת תהליכי בקרה וכתיבת נהלים לגבי העברה, אחסון, שימוש, ניהול, או הוצאה מכלל שימוש (גריטה) של תוכנה/קושחה , ציוד תמיכה , התקנים וציוד תעבורה רגיש.

3.4. **<u>טיפול וניהול תוכנה / קושחה והתקנים עבור מערכות הרכב:</u>**

3.4.1. ביצוע התקנה של תוכנה/ קושחה <u>מקורית בלבד</u>, אשר מאושרות על ידי יצרן הרכב ו/או יצרן ציוד תעבורה רגיש ו/או גורמי אבטחת מידע. חל איסור על יצירה, עריכה או עדכון של תוכנה/קושחה על ידי גורמים שאינם מורשים לכך.

3.4.2. העברת תוכנה תבוצע באופן מאובטח ומוצפן וע"פ הנחיות יצרן (לדוגמא שימוש בציוד ייעודי, בערוצי VPN, פרוטוקולים מוצפנים, וכו'). אין לבצע שימוש באמצעים שאינם מאובטחים לדוגמא העברה באמצעות EMAIL, הורדה ממקורות לא מהימנים וכד'.

3.4.3. במידה וקיימים תוכנה/קובץ המותקנים ברכב שלא עברו דרך ערוץ מאובטח וישיר של היצרן, נכון לייצר תהליכי בדיקה, אימות וולידציה

מקדימה לפני העברתם אל מערכות הרכב. תהליך זה יוגדר על ידי גורמי אבטחת המידע של המוסך/יבואן.

3.4.4. הכנסה של תוכנה, קושחה, קובץ או תוכן לרכב ומערכותיו תבוצע באמצעות ציוד ייעודי שהוגדר על ידי היצרן ו/או גורמי אבטחת המידע של המוסך/היבואן בלבד.

3.4.5. מעקב ובקרה אחר התקנים המשתמשים לטובת אחסון תוכנה, קבצים או תכנים עבור מערכות הרכב.

3.4.6. העלאת תוכן, אפליקציות, תוכנה וקבצים לתוך מערכת ה-INFOTAINMENT כולל מערכות הניווט, המאושרות על ידי היצרן ו/או על ידי גורמי אבטחת מידע של המוסך/יבואן.

3.5. **<u>טיפול וניהול ציוד תמיכה המתממשק לרכב</u>**

3.5.1. הגדרת תהליכים ונהלים לבקרת תצורה, רישום, סימון ומעקב עבור כל ציוד תמיכה המתממשק לרכב ומערכותיו לביצוע פעולות הדיאגנוסטיקה, אחזקה, תיקון, כיול וכד' .

3.5.2. ציוד תמיכה ייעודי ישמש לצורך תפעול ותחזוקה בלבד, אל מול רכבי היצרנים אליהם הוגדר, ולא לכל פעילות או מטרה אחרת.

3.5.3. התקנה של כלי הגנה ומימוש בקרות סייבר טכנולוגיות בציוד התמיכה בהתאם לתוכנית התפעולית של המוסך ולכל הפחות הקשחה וסגירת ממשקים (פיזי ולוגי), הגבלת גישה לרשתות חיצוניות בדגש על אינטרנט, בקרת גישה והזדהות לציוד, זאת בהתאם להנחיות היצרן.

3.5.4. ציוד תמיכה ייעודי יכיל חומרות, תוכנות, אפליקציות, קבצים, שירותים או פרוטוקולים המאושרים ומעודכנים על ידי יצרן הרכב ו/או גורמי אבטחת המידע של המוסך/יבואן בלבד.

3.5.5. הגבלת והקשחת חיבור התקנים חיצוניים אל הציוד תמיכה בהתאם לצרכים התפעוליים ועל פי הנחיות גורמי אבטחת מידע של המוסך/יבואן.

3.5.6. ביצוע תהליכי התחזוקה וכיול מערכות הרכב בעזרת ציוד תמיכה באופן מאובטח בהתאם להגדרות יצרן ו/או הנחיות גורמי אבטחת מידע של המוסך/יבואן.

3.5.7. אחסון ציוד התמיכה באזור מאובטח ונעול וביצוע בקרה ותיעוד על הוצאת ציוד התמיכה והחזרתו.

3.5.8. הגדרת תהליכים ונהלים לגבי אופן ההורדה, השמירה וניטור לוגים בכל ציוד תמיכה לצורכי אבטחה והגנת סייבר.

3.6. **<u>טיפול וניהול ממשקי גישה ברכב</u>**

3.6.1. שימוש וחיבור לממשקי הגישה הקיימים ברכב בצורה מאובטחת בהתאם להנחיות היצרן ו/או הנחיות גורמי אבטחת המידע והגנת סייבר של המוסך/היבואן.

<u>הערה</u>: נקודות הגישה ברכב הן כדלהלן, RJ45/ AUX/ WIFI/ BT / USB CELLULAR/ SATCOM/ OBD II וכד'.

3.6.2. ציוד שאושר להתחברות לפלג OBD II יבוצע בהתאם להמלצות המתוארות בסעיף "טיפול וניהול ציוד תמיכה המתממשק לרכב" כך שהציוד לא יהווה פוטנציאל פגיעה למערכות הרכב בעת ההתממשקות דרך פלג זה.

3.6.3. **אין לבצע חיבור מערכות/ רכיבים משדרים לתשתיות הרכב באופן ישיר** שלא על פי הנחיות יצרן, לדוגמא מערכות חברות ביטוח.

3.6.4. התקנת מערכות ברכב ובפרט מערכות After market המצריכות חיבור ל- CANBUS יבוצעו בחיבור השראתי לקריאה בלבד עם הגבלת עוצמת השידור/הרעש למניעת שיבוש והפרעות לתקשורת ו/או בהתאם להנחיות יצרן. בחיבור הקורא ההשראתי אין לבצע הפרדת חוטים שזורים של התקשורת.

3.7. **<u>טיפול וניהול ציוד תעבורה רגיש</u>**

3.7.1. הגדרת תהליכים, בקרות וכתיבת נהלים לשינוע, אחסון ותיקון מוגן ומאובטח של ציוד תעבורה רגיש על מנת למנוע גישה פיזית של גורמים שאינם מורשים לאורך כל שרשרת האספקה של הציוד.

3.7.2. הקשחת כרטיס eSIM/SIM המותקן בציוד תעבורה רגיש (אם מותקן) בהתאם לbest practice.

3.8. **<u>דיווח וביצוע ביקורות</u>**

3.8.1. קיום ביקורות ומבדקים פנימיים לבחינת רמת הגנת הסייבר במוסך, אחת לשנתיים לכל הפחות.

4. נספחים

4.1 נספח א' – עלון מידע לצרכן להתנהלות בטוחה ברכב

עלון מידע לצרכן

משרד התחבורה והבטיחות בדרכים

הגנת סייבר ברכב שלך

מדריך מקוצר להתנהלות בטוחה ברכב מקושר

הרכב של היום הוא הרבה יותר מכלי תחבורה – הוא מחשב על גלגלים.

עשרות מערכות, רכיבי מחשוב וחיישנים מתקשרים בתוך הרכב ומחוצה לו, משדרים נתונים ואוגרים מידע רב על הנסיעות, על הסביבה ועל הנוסעים. החיבוריות הזו נוחה ומתקדמת – אבל היא גם חושפת את הרכב לחולשות אבטחה, ועלולה להפוך אותו ליעד לתקיפות סייבר המסכנות את פרטיותכם ואת פעולתו התקינה של הרכב.

החדשות הטובות: כמה הרגלים פשוטים מצמצמים מאוד את הסיכון. בעלון זה ריכזנו עבורכם את ההמלצות המרכזיות.

נקודות כניסה נפוצות

מערכת המולטימדיה
קבצים ויישומים שמועלים אליה

חיבור הדיאגנוסטיקה (OBD)
שקע השירות של הרכב

השלט / המפתח החכם
האות האלחוטי של המפתח

תקשורת אלחוטית
Bluetooth · Wi-Fi · סלולר

מה עלול לקרות?

פגיעה בפרטיות

- **מעקב אחר מיקום** הרכב ומסלולי הנסיעה שלכם
- **האזנה** לנעשה בתא הנוסעים
- **דליפת מידע אישי** – אנשי קשר, יעדים שמורים, שיחות והודעות

פגיעה ברכב ובנהיגה

- **שיבוש תצוגות**, ניווט ומידע המוצג לנהג
- **השבתת שירותים ויכולות** ברכב – חסימת אפליקציות, נעילת הדלתות, השבתת מיזוג ומערכות עזר
- **גניבת הרכב** – לרבות באמצעים אלקטרוניים

עלון מידע לצרכן · הגנת סייבר ברכב
יחידת הסייבר המגזרית ומנהל תנועה - משרד התחבורה
עמוד 1 מתוך 2

מנחה מקצועי – המלצות להגנה בסייבר בתחום הרכב

(עבור יבואנים ומוסכים)

ההמלצות שלנו: כך תצמצמו את הסיכון

פעולות פשוטות שכל נהג ונהג יכולים ליישם – כבר מהיום

תוכן ויישומים – רק ממקור מהימן

- ✓ אל תעלו למערכת המולטימדיה קבצים ממקור לא ידוע, וודאו שהקבצים והיישומים שבשימוש מהימנים.
- ✓ השתמשו רק ביישומים המאושרים על ידי יצרן הרכב.

אביזרים והתקנים חיצוניים

- ✓ הימנעו מהתקנת אביזרים שלא אושרו על ידי היצרן – מערכות מולטימדיה, מצלמות דרך, מערכות דיאגנוסטיקה וכדומה.
- ✓ צמצמו חיבור של התקנים ומכשירים שאינם שלכם – התקן USB, כונן חיצוני, טלפון או טאבלט – בכבל, ב-Bluetooth או ב-Wi-Fi.
- ✓ בעת התחברות למערכת המולטימדיה בצעו אימות (קוד צימוד) – ואל תבטלו אותו לצורכי נוחות.
- ✓ ברכיבי ניטור נהיגה של חברות ביטוח (למשל לנהג צעיר), העדיפו פתרון המבוסס על אפליקציה בטלפון על פני רכיב המתחבר ישירות לרכב.

צמצום חשיפה שוטף

- ✓ אחת לכמה שבועות עברו על רשימת מכשירי ה-Bluetooth המצומדים למולטימדיה, ומחקו מכשירים לא מוכרים או שאינם בשימוש.
- ✓ שירותים כמו נקודה חמה (Hot Spot) ברכב – השאירו כבויים כברירת מחדל, והפעילו רק בעת הצורך.

שמים לב לסימנים חריגים

- ✓ שימו לב לחיווויים, הודעות, התרעות או התנהגות חריגה של הרכב – למשל מערכת שנדלקת מעצמה או הודעות לא מוכרות.
- ✓ בכל חשד – פנו ליבואן או למשווק הרכב לבדיקה.

סיסמאות ומידע אישי

- ✓ אם ניתן להגדיר סיסמה לממשק הניהול של מערכת המולטימדיה – החליפו את סיסמת ברירת המחדל.
- ✓ בחרו סיסמה שקשה לנחש (לא תאריך לידה או מספר רכב), ועדכנו אותה מעת לעת.
- ✓ הגנו גם על אפליקציית היצרן בטלפון: סיסמה חזקה ואימות דו-שלבי, אם קיים.

לפני מכירת הרכב או החזרת רכב שכור

- ✓ מחקו יעדים שמורים במערכת הניווט.
- ✓ מחקו אנשי קשר, יומן והיסטוריית שיחות.
- ✓ בטלו צימוד של מכשירים (Bluetooth).
- ✓ התנתקו מהחשבונות האישיים ברכב וביישומים.

עדכוני תוכנה

- ✓ התקינו עדכוני תוכנה בהקדם – בדגש על עדכוני אבטחה ובטיחות.
- ✓ עדכנו רק ממקור רשמי ומהימן של היצרן, באמצעות גורם מוסמך ומכשור מאושר.
- ✓ עדכון "דרך האוויר" (OTA) יבוצע רק באמצעות האפליקציה הרשמית של יצרן הרכב.

שימו לב: ברוב כלי הרכב לא ניתן להשתמש ברכב בזמן העדכון, ולא ניתן לעצור עדכון לאחר שהחל – תזמנו אותו בהתאם.

המפתח החכם – הגנה מפני גניבה

- ✓ ברכב עם כניסה והתנעה ללא מפתח: אחסנו את השלט בבית הרחק מדלת הכניסה, או בנרתיק חוסם אותות – כך תקשו על גניבה בשיטת "הגברת אות".
- ✓ אל תשאירו שלט רזרבי או קוד גישה בתוך הרכב.

חושדים באירוע סייבר ברכב?

דווחו ליבואן או למשווק הרכב, וכן למוקד הסייבר הלאומי של מערך הסייבר הלאומי – **חיוג 119**, בכל שעות היממה. דיווח מוקדם מסייע להגן עליכם ועל נהגים נוספים.