الهيئة السعودية للمقيّمين المعتمدين
Saudi Authority for Accredited Valuers
تقييم
TAQEEM

الأمن السيبراني للمركبات

معد الدراسة: م. إبراهيم سمور

الفهرس

المقدمة

تتطرق هذه الدراسة لتعريف بالأمن السيبراني بالمركبات والاخطار المحدقة بالقطاع نتيجة التطور الهائل الحاصل في التقنيات الإلكترونية للمركبات، وضعف تغطيتها من قبل المشرعين والاتحادات الخاصة بمصنعين المركبات عالميا.

تقدم الشركات المصنعة للمركبات لعملائها تقنيات متطورة كنوع من وسائل الرفاهية لمواكبة الثورة التقنية في مجال الأنظمة الإلكترونية ومن ضمنها نظام المفتاح الافتراضي كتطبيق على جهاز الهاتف، ومفاتيح السيارة المادية التقليدية، وخدمات ما بعد البيع الرقمية الأخرى، التي تستند إلى أنظمة الشبكة العالمية كخاصية الاتصال مع أنظمة المركبات الأخرى والقيادة الذاتية. تؤدي التطورات الحالية والمستقبلية في صناعات السيارات إلى خلق نوعية جديدة من الهجمات على شبكات الاتصال بين كيانات هذه الأنظمة المتصلة بالشبكة.

بشكل متزايد مركبات الوقت الحالي مزودة بأنظمة معقدة تتخاطب مع بعضها البعض لمساعدة السائق لمعرفة حالة الطريق وتحليل كيفية التعامل مع مخاطره بشكل فعال، مثل نظام تحذير التصادم الامامي (الرادار)، نظام الفرملة الذكي، ونظام اتصالات السلامة الخاصة بالمركبة. كما أن أنظمة مساعدة السائق المتقدمة خضعت لتطورات كبيرة لربطها بشبكات الانترنت لتخفيف أخطار السلامة على المركبات والتنبؤ بالحوادث قبل حصولها وإعطاء السائق إمكانية القيادة الشبة ذاتية.

ويأخذ تطوير وتكامل المكونات الإلكترونية في صناعة السيارات بعدًا جديدًا، حيث يتم طرح عدد متزايد من الخصائص المبتكرة والمتصلة بالشبكات التي تعتمد على انترنت الأشياء.

كما ساعدت هذه الانظمة بحماية حياة الكثير من الناس كما حدث في إعصار لارما في ولاية فلوريدا حيث اتصلت شركة تسلا بجميع المركبات الخاصة بها وقامت بتغيير برمجيات خاصة لزيادة مدى قطع المركبات ومعدل استهلاك الطاقة الكهربائية المخزنة في بطارية المركبة بالشحنة لتمكن أصحاب هذه المركبات من تجاوز خطر الاعصار الذي ضرب الولاية في عام 2017م.

التهديدات السيبرانية على قطاع المركبات تعد بالوقت الحال مسألة حياة او موت، تهدد خارطة طريق تطوير أنظمة القيادة الذاتية وان أي فشل في حماية المركبة او قائدها يؤثر على بشكل كبير على سمعة مصنع المركبة واستمراريتها بالسوق.

نطاق الدراسة

مصنعين المركبة.

شركات التأمين.

مستخدمين المركبة.

مقيمين الأضرار.

ما هو الأمن السيبراني في المركبات

الأمن السيبراني بالمركبات يعنى بحماية أنظمة المركبة والإلكترونيات الخاصة بها وخوارزميات آليات الاتصال والتطبيقات التي تعمل من خلالها ومستخدميها وبيانتهم من الهجمات والتخريب وتسريب البيانات.

وبترابط هذه الأنظمة يمكن تفادي وقوع الحادث بشكل كبير، لكن العبث بهذه الأجهزة او وجود اختراقات او ضعف بالعملية البرمجية من الممكن ان يزيد الخطر لوقوع حوادث لا يمكن توقع نتائجها.

وبالإمكان أيضا سرقة البيانات الشخصية لصاحب المركبة، وهذه المخاطر بازدياد مع التوجه العالمي للاعتماد على أنظمة النقل الذكية.

وهنا تكمن أهمية وجود منظومة حماية متكاملة للحفاظ على الخصوصية وتقليل الاختراقات للأنظمة التي تعمل بها المركبة.

هل قطاع المركبات في خطر

أنظمة المركبات الحالية تتشابه بشكل كبير بأنظمة الحاسب في تسعينيات القرن الماضي حيث انها غير مجهزة بتقنيات الحماية للاتصال بالأنترنت او بالدفاع عن نفسها في حالات الاختراق.

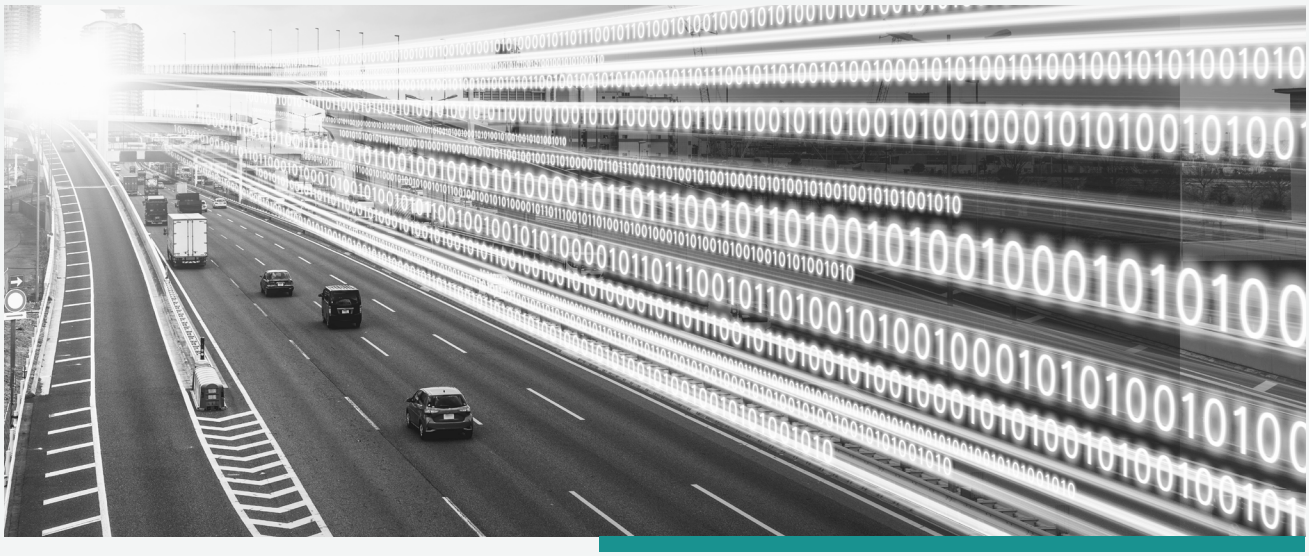
والتطور الثوري الحاصل في المركبات لا يعني زيادة الأمان في المركبات، لكن زاد من تعقيد الأنظمة وضاعف من إمكانية اختراقها او التلاعب بها. مما أدى الى استدعاء 1.4 مليون مركبة في عام 2015م لتحديث الأنظمة الخاصة بها خوفا من إمكانية اختراق أنظمتها.

في 2020م تعرضت معظم مصانع السيارات في أمريكا الشمالية لهجمات ممنهجة أدت لتوقف الإنتاج لأسابيع ومما أدى الى اتحاد مصنعين المركبات لوضع منظومة تحد من هذه الاختراقات في عمليات الإنتاج فقط.

مصنعين المركبات بشكل عام غير مستعدين في الوقت الحالي لهجمات سيبرانية معقدة، حتى مركباتهم غير مزودة بأنظمة تحول دون اختراقها لضعف دور الشركات المبرمجة لأنظمة الحماية في التطرق لهذه التكنولوجيا الخاصة بالمركبات.

ملخص الهجمات من عام 2018م:

- زاد تواتر الهجمات الإلكترونية على السيارات بنسبة 225% من 2018م إلى 2021م.
- ما يقرب من 85% من الهجمات في عام 2021م نُفّذت عن بُعد، مما يفوق عدد الهجمات الفعلية على المركبات من قبل السارقين.
- 40% من الهجمات استهدفت خوادم شركات النقل اللوجيستي.
- شهد عام 2021م تنفيذ 54.1% من الهجمات من قبل جهات تسمى "القبعة السوداء".
- كانت أهم فئات الهجوم هي خرق بيانات الخصوصية (38%)، سرقة واقتحام السيارات (27%)، والتحكم بالمركبات دون علم صاحبها (20%).
- تمثل هجمات الدخول بدون مفتاح 50% من جميع سرقات المركبات. يحتاج اللصوص فقط إلى أن يكونوا قريبين من مفتاح التشغيل حتى يتمكن متسلل القبعة السوداء من التقاط إشاراته وإعادة توجيهها.



الاخطار المتوقعة من المخترقين

معظم المخاطر المتوقعة من المخترقين هي أخطار مالية عن طريق الاستحواذ على المركبات او تعطيل خصائصها للحصول على المال ومن الممكن ان تتعدا هذه المخاطر للقيام بعمليات أخرى او الحصول على المركبة بشكل كامل وتجزئتها وبيعها كقطع غيار، حيث يمثل قطاع قطع الغيار المسروقة حجم سوقي يتجاوز 45 مليار دولار.

يستخدم المخترقين 7 أساليب لاختراق المركبات:

- إرسال رسائل ضارة من خلال نظام الاتصالات والترفيه في السيارة.
- تفعيل نظام حرمان الخدمة وتعطيل خصائص المركبة.
- إرسال رسائل تحتوي على محتوى ضار، يمكن أن تتلقاه المركبة بالإضافة إلى هاتف أو حاسوب منزلي.
- الاستفادة من مكامن الضعف في الحصول على المعلومات الحساسة في بعض المركبات.
- التلاعب مع الشفرات الداخلية للمركبة وبياناتها.
- تضمين الفيروسات في وسائط الاتصال.
- انتحال الرسائل أو البيانات (حيث تظهر الرسالة من شخص تعرفه، ولكنها في الواقع من مخترق تحتوي الرسالة على روابط خبثة تمكن المخترق من الولوج لحواسيب المركبة والعبث بها).

ومنها تأتي الهجمات على المركبات بطرق مختلفة منها:

خدمات المركبات المدفوعة

تعتبر الخدمات المدفوعة من اهم مصادر الدخل للشركات وتم اتاحة هذه الخدمات المدفوعة للمركبات من قبل مصنعين المركبات لإعطاء العميل الخيار لاستخدام خدمات معينة مقابل اشتراك شهري.

2021م شركة جنرال موتورز أعلنت عن أرباح بقيمة 2 مليار دولار عن طريق تقديم خدمات مدفوعة مسبقا لعملائها، وعدد الخدمات المدفوعة بازدياد كما ان المتوقع بحلول 2030م، أن ترتفع أرباح شركات السيارات من الخدمات المدفوعة الى 25-20 مليار دولار.

لم تكن هذه الخدمة بعيدة عن الاختراق عندما أطلقت بي ام دبليو خدمة الكرسي المدفئة المدفوعة مسبقا، واجهة الشركة العديد من الانتقادات ورد فعل غاضب من عملائها. وبعد أسبوع من إطلاق الخدمة تمكن المخترقين من تفعيل الخدمة مجانا لجميع مالكين مركبات بي ام دبليو.

زيادة عدد الخدمات المدفوعة تحتاج الى توثيق هذه العمليات التي تطلب من العميل معلومات شخصية مهمة مثل بصمات الأصابع، وبطاقة الهوية، وبطاقات الدفع. والتي تكون هدفا للمخترقين للحصول على هذه المعلومات واستخدمها بطرق غير مشروعة.

المركبات المتصلة

المركبات المجهزة بتقنية الاتصال مع المركبات الأخرى من أكثر المركبات المعرضة للاختراق. هذه المركبات مجهزه لتخاطب بعضها البعض لضبط المسافة والسرعات فيما بينها لذلك ستكون هدف جيد للمخترقين وتعريضها للخطر عن طريق اختراق الاتصال الخاص بين المركبات وارسال رسائل خبيثة تعطل خدمات المركبة او تعمل على سرقة بياناتها.

اختراق حساب شحن المركبات

كما نعلم ان قطاع المركبات الكهربائية يأخذ بالتطور بشكل سريع في دول العالم وهنالك بعض الدول تتبنى فكرة شحن المركبات أثناء الاصطفاف، وهي خدمة مدفوعة الثمن. هذه إحدى الخدمات التي قد تكون عرضة للاختراق لسرقة بيانات العملاء البنكية او عن طريق العبث بالشواحن لتخريب مركبات العملاء.

للأسف جميع شواحن المركبات في جميع دول العالم غير مجهزه بالوقت الحالي بأنظمة حماية من الاختراق.

سرقة المركبات

المركبات المزودة بأنظمة فتح المركبة وتشغيلها عن طريق البرمجيات، معرضة للسرقة من قبل المخترقين بسهولة دون الحاجة لمفتاح المركبة.

التحكم بالمركبات عن بعد

أمكانية اختطاف المركبة والتحكم بسرعتها وقيادتها عن بعد او إيقاف خصائص القيادة مثل نظام الفرامل او التوجيه مما يؤدي الى وقوع الحوادث.

تعطيل الاساطيل (خدمات الأساطيل والنقل)، حيث تعتمد شركات الاساطيل على نظام تحكم وملاحة مركزيه حيث ان السيطرة على هذه الأنظمة من قبل المخترقين يؤدي الى تعطل خدمات الشركات ويكبدهم خسائر مهولة.

اختراق الخصوصية

المركبات الحديثة مزودة بأنظمة قادرة على تجميع وتحليل البيانات الشخصية لقائدها مما يجعل من هذه المعلومات الحساسة عرضة للسرقة واستخدمها بوجه غير صحيح.

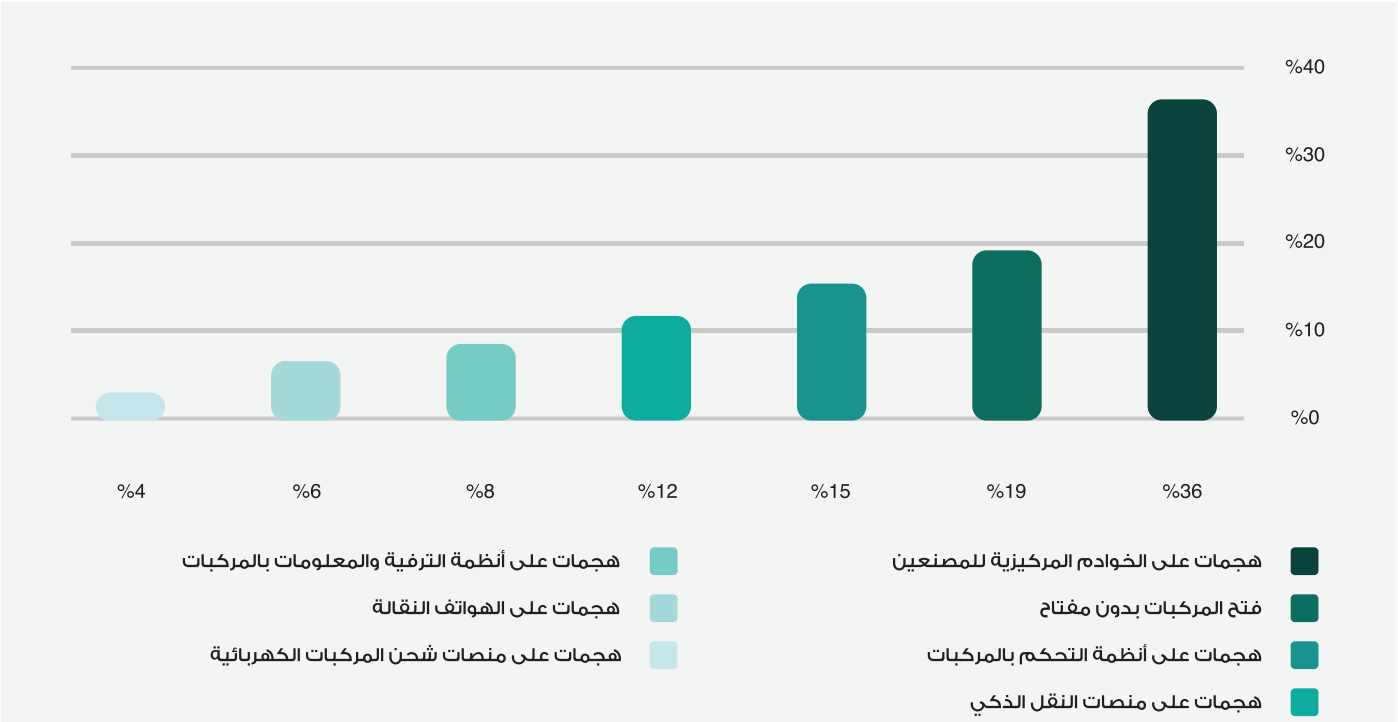
تخريب البيانات التأمينية

مع إطلاق شركات التأمين اليات ذكية لمعرفة كيفية قيادة المركبة وربطها بقيمة التأمين المدفوع في وثيقة التأمين عن طريق الدخول لنظام الاتصالات الخاص بالمركبة وتحليل بياناتها التي تمكن شركات التأمين من وضع سياسة للقيمة التأمينية.

لكن في حال وقوع هجمة من مكان ما على المركبة فأن تواصل شركة التأمين مع المركبة يجعل أنظمة الشركة عرضة للاختراق بما فيها عملائها والأنظمة السحابية المرتبطة بها.

وتتعدى المخاطر السيبرانية في المركبات المتصلة والكهربائية في حالات السرقة، الاختراق او الحوادث عند الحاجة لإصدار تقرير المسؤولية من قبل مباشر الحوادث. هل تكمن المسؤولية على السائق؟ او المخترق او مصنع المركبة؟.

توزيع الهجمات السيبرانية في عام 2022م



كيفية حماية مركبتك من المخترقين

في البداية يجب التعرف على نقاط الاختراق في مركبتك للتمكن من حمياتها من الاختراق الإلكتروني او المادي.

- حساس ضغط الإطارات.
- حساس إشارة المفتاح.
- DSRC مستقبل.
- حساس يد الباب.
- قفل الباب.
- تطبيقات المركبة الذكية.
- USB مأخذ.
- نظام التوجيه والتحكم.
- البلوتوث.
- نظام الوسائد الهوائية.
- نظام الدفع ونقل الحركة.
- نظام مساعدة السائق المتقدم.
- OBDII مأخذ.
- نظام الانارة.
- نظام التحكم بالدخول.
- الكاميرات المحيطية.

1. قم بتحديث نظام التشغيل الخاص بالمركبة بشكل دوري.
2. قم بأبعاد مفتاح مركبتك قدر الإمكان عن مكان اصطفافها لمنع المخترقين من تقوية إشارة المفتاح.
3. استخدم VPN في حال قمت بربط مركبتك بشبكة غير أمنة استخدم برنامج خاص لتغيير عناوين الانترنت الخاصة بك.
4. قم بإيقاف الخدمات التي لا تقوم باستخدامها.
5. ثقف نفسك من خلال الاطلاع على اخر التقنيات الخاصة بحماية المركبة من الاختراق.

الأمن السيبراني وتقييم أضرار المركبات

يعتمد تقييم المركبات المتأثرة بالهجمات الإلكترونية على شدة الهجوم وتأثيره على السيارة. فإذا تسبب هجوم إلكتروني في تلف السيارة، فقد يكون من الصعب تحديد ما إذا كان التقدير دقيقًا أم لا.

في حالة وقوع هجوم إلكتروني، يمكن أن يختلف الضرر الذي يلحق بالمركبة بشكل كبير. سيكون لبعض السيارات ضرر ضئيل أو معدوم، بينما قد يحتاج البعض الآخر إلى أعمال إصلاح كبيرة. من المهم معرفة قيمة المركبة بعد هجوم إلكتروني لأنه قد يؤثر على المبلغ الذي يمكنك استرداده من التغطية التأمينية.

عندما تتعرض مركبة للتلف في هجوم إلكتروني، قد يكون من الصعب تحديد مدى الضرر. وقد لا يعرف صاحب المركبة ما حدث ولا يوجد شهود على الحادث.

من أجل الحصول على تقييم دقيق للأضرار التي لحقت بسيارتك، يحتاج المقيم إلى إجراء بعض التحقيقات وجمع أكبر قدر ممكن من المعلومات.

أولاً: حدد ما إذا كان هناك أي ضرر مادي للمركبة.

ثانياً: ابحث عن أي استدعاءات من الشركة المصنعة للمركبة ومعرفة ما إذا كان قد أصدر أي تحذيرات بشأن تعرض سياراتهم لهجمات إلكترونية مثل هذه. إذا أصدر استدعاءات لهذه الأنواع من المشكلات في العام الماضي أو نحو ذلك، فقد تتمكن من استخدام هذه المعلومات عند محاولة حساب قيمة الأضرار التي لحقت بسيارتك بسبب الهجمات الإلكترونية.

نتائج الهجمات السيبرانية قد تؤدي الى حوادث تحتاج الى مقيم لإصدار تقرير بالأضرار الناجمة عن ذلك الاختراق.

لذلك على المقيم فهم آلية عمل منظومة المركبة الالكترونية والاستفسار الدقيق من العميل عما جرى قبل وقوع الاضرار، وما هي؟ ولإصدار تقرير متكامل يجب اتباع الخطوات التالية وتنبيه العميل وشركة التأمين فحال الاشتباه بوجود اختراق.

1. الاستفسار من العميل عن ما حدث.
2. سؤال العميل عن اي رسائل من قبل نظام المركبة وقت الحادث.
3. سؤال العميل هل قام بتثبيت اي برامج حديثة على نظام المركبة.
4. سؤال العميل هل قام بتركيب اي اجهزة حديثا على المركبة.
5. ربط المعلومات مع الاضرار.
6. البحث عن اي استدعائات من قبل الشركة المصنعة.
7. سحب و تحليل بيانات انظمة المركبة.
8. الكشف عن الأضرار المادية بالمركبة.
9. أصدار تقرير التقييم المفصل.
10. أبلاغ كل من العميل و شكرة التأمين في حال اكتشاف الاختراق.

مجموعه الحلول المقترحة

هناك مجموعة واسعة من حلول الأمن السيبراني على مستوى مصنع المركبة التي تختلف في قابليتها للتطبيق وفعاليتها.

يجب على الشركات المصنعة للمركبات إنشاء ثقافة للأمن السيبراني في دورة حياة تطوير المنتج بأكمله، من المفهوم إلى التحديث المستمر والصيانة. ويجب تحسين كل حل يتعلق بالتكلفة، التسويق، تجربة المستخدم، والابتكار.

الخطوات المقترحة

الخطوة الأولى: تفنيد أولي لملف تعريف المخاطر المقبول.

يجب تحليل نوعية الهجمات للحصول على فهم أولي للتهديدات السيبرانية المحتملة والمخاطر المرتبطة بها.
كما على مصنعي المركبات تحديد مستوى تحمل مجموعات المستهلكين المستهدفة لأنواع المخاطر المختلفة.
وأن يميزوا الأحداث التي قد تتسبب في تخريب هوية العلامة التجارية.

الخطوة الثانية: تقييم التعرض الفعلي للمخاطر الإلكترونية.

يمكن أن يتم ذلك من خلال تقييم شامل لعمليات المنظومة وقدراتها على رد الهجمات دون تأثيرها على تجربة المستخدم. وعن طريق رسم مصفوفة المخاطر المتوقعة وقياس الفجوات الفعلية في أنظمة الحماية مقابل ملف تعريف المخاطر لكل منتج.

الخطوة الثالثة: تحديد مجموعة الحلول بناءً على الفجوات ذات الأولوية الناتجة عن خريطة التعرض للمخاطر.

سيحتاج مصنعي المركبات إلى تقييم الفعالية الإجمالية للتكلفة لحلول الأمن السيبراني فيما يتعلق بتطوير المنتج وتكلفة المنتج نفسها وتكلفة الصيانة.

وبناءً على أخطار الملف الشخصي المختارة للمركبة المحددة، يجب أن يوازن التحسين في أنظمة الأمان بين التكلفة الإجمالية للحل مقابل تكلفة الاسترداد النهائية المتعلقة بمخاطر الفشل السيبراني.

كثرة المشاكل السيبرانية تجعل من المركبة أقل جاذبية للزبائن وعلى النقيض يُنظر إلى تعقيد حلول الأمن السيبراني التي تفرض طلبًا كبيرًا على المستخدمين على أنها مرهقة وقد تكون طاردة للعميل أيضا. كما يجب تقييم كل حل من حيث آثاره على التطور المستقبلي للمنتج.

المراجع

(National Highway Traffic Safety Administration, 2022) (Tribune Content Agency, LLC., 2022) (Berger, 2022) (Intel 471, 2023)

Berger, D. (2022). Auto Industry at Higher Risk of Cyberattacks in 2023. Fortra.

Intel 471. (2023). Cyber Threats Facing the Automotive Industry.

Mackinze. (2022). shifting gears in cyber security for connected cars. New York.

National Highway Traffic Safety Administration. (2022). Automotive Cybersecurity. NHTSA and Vehicle Cybersecurity.

Tribune Content Agency, LLC. (2022). Cyber Attacks on Cars Rise.

Upstream. (2023). Upstream_2023_Global_Automotive_Cybersecurity_Report. Upstream.