Mgr. Marek Rechtik
Masarykova univerzita v Brně
Fakulta sociálních studií
student magisterského studia

Kybernetická bezpečnost v automobilovém sektoru

Úvod

Narůstající konektivita moderních vozidel otevírá řadu příležitostí pro jejich uživatele. Zároveň však otevírá nové příležitosti kybernetickým útočníkům, což může vést k nárůstu kybernetických útoků. Současné trendy vedoucí směrem k digitalizaci, automatizaci a autonomizaci vozidel tyto hrozby ještě více umocňují. Navzdory tomu, že kybernetická bezpečnost autonomních vozidel se stává poměrně značně diskutovaným tématem, kybernetická bezpečnost současných moderních vozů zdá se stojí spíše v pozadí. Cílem tohoto článku tak bude představit kybernetické hrozby a rizika spojených s narůstající automatizací, digitalizací a autonomizací automobilů a nastínit možnosti jejich řešení.

V rámci článku bude nejprve představen současný stav základní přehled kybernetických hrozeb a rizik spojených s moderními automobily. Následující část se zaměří na holistický přístup k zajišťování kybernetické bezpečnosti automobilů v kontextu aktuálního vývoje regulací a standardizace v této oblasti. Závěrečná část se pak bude věnovat implikacím kybernetických hrozeb a rizik v automobilovém sektoru pro Českou republiku.

Kybernetické hrozby a rizika spojená s moderními automobily

Ačkoli do plošného nasazení autonomních vozidel zbývá ještě několik let, současné moderní automobily jsou často tvořeny komplexním digitálním ekosystémem, který je zranitelný vůči kybernetickým útokům. Jedná se o tzv. připojené automobily (*connected cars*), které jsou tvořeny celou řadou digitálních komponentů, včetně připojení WiFi a Bluetooth, mobilních aplikací a cloudu. Služby, které dnes připojení umožňuje, sahají od zasílání cílových adres do vozidla, přes příjem dopravních informací v reálném čase až po parkování na dálku prostřednictvím aplikace pro smartphone.[1] Současné technologie umožňují také možnost komunikace mezi připojenými vozidly navzájem.[2] Jako každé připojené zařízení však mohou být

[1] McKinsey & Company. Cybersecurity in automotive: Mastering the challenge [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Cybersecurity%20in%20automotive%20Mastering%20the%20challenge/Cybersecurity-in-automotive-Mastering-the-challenge.pdf.

[2] KYUSUK, H., WEIMERSKIRCH, A., & SHIN, K. G. Automotive Cybersecurity for In-Vehicle Communication. *IQT QUARTERLY SUMMER* [online]. 2014, 6(1). [cit. 6. 11. 2020]. Dostupné z: https://www.iqpc.com/media/1001748/37529.pdf.

připojená vozidla kompromitována, přičemž v takovém případě může útočník ovládat vše, co je v rámci vozidla možné.[1]

Tyto technologie s sebou tedy přinášejí nejen riziko narušení soukromí řidiče, ale zejména jeho bezpečnosti. Každý rok je po celém světě vyrobeno milion připojených vozidel disponujících zařízeními a mechanismy, které ovládají akceleraci, brzdy i ovládání vozidla. To vše je potenciálně zranitelné kybernetickými útoky, které mohou ohrozit bezpečnost řidiče, a to i bez nutnosti fyzického přístupu k vozidlu.[2]

Ekosystém připojeného automobilu je extrémně složitý s potenciálními miliony koncových bodů či koncových uživatelů. Složitost tohoto ekosystému, s jeho obrovskou velikostí a mnoha funkcemi, vytváří rozsáhlou povrchovou plochu pro potenciální útok, přičemž tato plocha se neustále zvětšuje.[3] V posledních několika letech se moderní automobily staly v podstatě „datovými centry na kolech." Průměrné moderní vozidlo obsahuje zhruba 100 milionů řádků kódu (což je čtyřikrát více než moderní stíhačka), přičemž do roku 2030 se očekává nárůst na 300 milionů.[4]

Vzhledem k neustálému vývoji a rostoucí digitalizaci připojených vozidel, roste potřeba jejich zabezpečení před rozšiřujícím se okruhem hrozeb. [5] Každá nová služba a schopnost totiž vytváří další vstupní body pro hackery. [6] Automobilový průmysl tak čelí zásadním výzvám, protože připojená vozidla se stávají normou a plně autonomní vozidla vstoupí do výroby později v tomto desetiletí. Podle odhadů bude do roku 2023 připojeno k internetu 775 milionů vozidel a v roce 2025 dosáhne počet částečně

[1] PwC. Cyber readiness: are auto companies prepared to counter the risk of an attack? [online]. 2018. Dostupné z: https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-auto-cyber-readiness.pdf.

[2] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

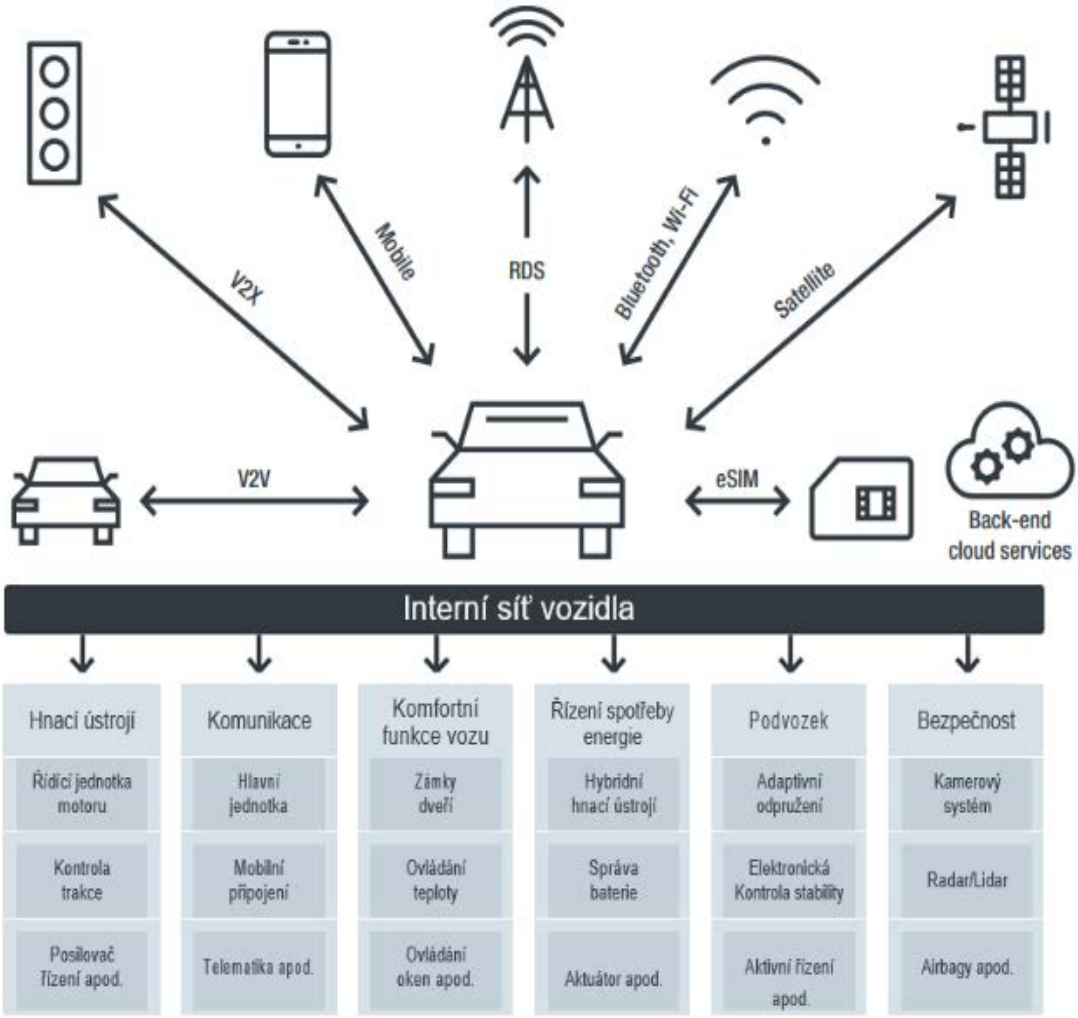
[3] HUQ, N., GIBSON, C., & VOSSELER, R. Driving Security Into Connected Cars: Threat Model and Recommendations. *Trend Micro Research* [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

[4] UNECE. UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: http://www.unece.org/?id=54667&utm_source=UNECE+WP.+29+Final&utm_campaign=bd67d3021f-EMAIL_CAMPAIGN_2020_04_22_03_14_COPY_01&utm_medium=email&utm_term=0_615fc6747a-bd67d3021f-592610470.

[5] HUQ, N., GIBSON, C., & VOSSELER, R. Driving Security Into Connected Cars: Threat Model and Recommendations. *Trend Micro Research* [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

[6] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

automatizovaných či plně autonomních vozidel na silnicích v roce 2025 na více než 14 milionů.[1]



Obr. 1: Vybrané technologie a funkce tvořící vnitřní síť připojeného automobilu[2]

S rostoucím využíváním připojených vozidel roste počet kybernetických incidentů ohrožujících nejen společnosti a spotřebitele, ale také všechny ostatní účastníky silničního provozu.[3] Od roku 2016 do roku 2019 se pak počet kybernetických incidentů

[1] HUQ, N., GIBSON, C., & VOSSELER, R. Driving Security Into Connected Cars: Threat Model and Recommendations. *Trend Micro Research* [online]. 2020. [cit. 6. 11. 2020]. Dostupné z: https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

[2] HUQ, N., GIBSON, C., & VOSSELER, R. Driving Security Into Connected Cars: Threat Model and Recommendations. *Trend Micro Research* [online]. 2020. [cit. 7. 11. 2020]. Dostupné z: https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

[3] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. [cit. 7. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

v automobilovém průmyslu zvýšil více než 7krát.[1] Kybernetické útoky na připojená vozidla přitom mohou mít řadu závažných dopadů na bezpečnost a soukromí jejich uživatelů. Kybernetický útok mířící přímo či nepřímo (skrze výrobce či dodavatele) na připojená vozidla může vést k:

- získání neoprávněného fyzického přístupu k vozidlům;
- manipulaci s ovládáním vozidla;
- využití elektronických řídících jednotek vozidla na podporu škodlivé kybernetické činnosti;
- ukládání citlivých osobních údajů;
- vydírání obětí skrze zavedení ransomwaru.[2]

Jako nejzávažnější lze považovat útoky, jejichž cílem bylo získání kontroly nad ovládáním vozidla, které tvořily za posledních více než 10 let 27 % všech incidentů. Pokud například dojde k útoku načasovanému tak, aby způsobil co největší škody, když je auto v pohybu, důsledky mohou být katastrofické.[3] Miliony automobilů připojených k internetu používajících stejný software mohou vést k tomu, že jediná zranitelnost ovlivní miliony vozidel současně. Útočník by pak mohl zahájit masivní útok proti automobilové infrastruktuře, a potenciálně tak způsobit tisíce úmrtí.[4]

Složitý ekosystém moderních vozidel umožňuje útočníkům využít celé řady vektorů útoků. Podle analýzy společnosti Upstream zahrnují tři nejčastější vektory útoků systémy bezklíčového vstupu, servery a mobilní aplikace. Další vektory pak zahrnují například diagnostickou zásuvku OBD, infotainment, sensory, Wi-Fi, či Bluetooth. Fyzický přístup k vozidlu přitom není k provedení útoku nutný. Již delší dobu převažují vzdálené útoky na vozidla, které lze provést prakticky odkudkoliv.[5]

Útoky často cílí také na samotné výrobce. Prostřednictvím těchto útoků mohou útočníci rovněž kompromitovat připojená vozidla, která jsou často napojena na systémy výrobců a poskytovatelů služeb. Podle průzkumu společnosti Accenture 2/3

[1] AtlasVPN. Automotive cyber incidents doubled in 2019, reaching 188 vulnerabilities [online]. [cit. 7. 11. 2020]. 2020. Dostupné z: https://atlasvpn.com/blog/automotive-cyber-incidents-doubled-in-2019-reaching-188-vulnerabilities.

[2] Fireeye. CONNECTED CARS: THE OPEN ROAD FOR HACKERS [online]. 2016. [cit. 7. 11. 2020]. Dostupné z: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf.

[3] Upstream Security. UPSTREAM SECURITY'S GLOBAL AUTOMOTIVE CYBERSECURITY REPORT: RESEARCH INTO CYBER-ATTACK TRENDS IN THE SMART MOBILITY ECOSYSTEM [online]. [cit. 7. 11. 2020]. 2020. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

[4] ConsumerWatchdog. Kill Switch: Why Connected Cars Can Be Killing Machines And How To Turn Them Off [online]. 2019. [cit. 7. 11. 2020]. Dostupné z: https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf.

[5] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. [cit. 7. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

dotazovaných automobilových společností zaznamenalo bezpečnostní incidenty, které cílily na jejich výrobní průmyslové řídicí systémy.[1] V tomto kontextu nelze podceňovat některé z tradičnějších metod kybernetických útoků jako je phishing. Podle společnosti Hornetsecurity tvoří až 70 % útoků v automobilovém průmyslu emailové zprávy obsahující nebezpečné odkazy či škodlivé přílohy.[2]

Zásadní výzvu pak představují útoky zaměřené na dodavatele automobilových výrobců. Automobily mají složité dodavatelské řetězce a jakákoli zranitelnost v tomto řetězci ohrožuje všechny jeho prvky i celý produkt. Ačkoli v automobilovém průmyslu doposud nebylo objeveno mnoho zranitelností dodavatelského řetězce, každá objevená zranitelnost by mohla ovlivnit miliony vozidel, která již jsou na silnici. Příkladem je nechvalně známý incident Jeep Cherokee, ke kterému došlo v červenci 2015. Hackeři objevili zranitelnost v infotainment systému Harman nasazeném v několika modelech automobilů. Tato zranitelnost jim umožnila získat vzdálený přístup k ovládání motoru Jeepu prostřednictvím mobilní sítě. Společnost byla nucena svolat 1,4 milionu vozidel za účelem provedení softwarové opravy, protože chyba zabezpečení byla v dodavatelském řetězci a nemohla být opravena přes cloud.[3]

Regulace a standardy jako cesta ke komplexnímu zajišťování kybernetické bezpečnosti automobilů

K zajištění kybernetické bezpečnosti na připojených (ale také autonomních) vozidlech je potřeba nastavit komplexní strategii, která bude zohledňovat celý ekosystém připojeného automobilu i celý dodavatelský řetězec a bude schopna čelit novým hrozbám během celého životního cyklu vozidla. Efektivního řešení lze tedy dosáhnout pouze v rámci holistického přístupu.

To znamená, že výrobci automobilů musí již od začátku navrhovat vozidla a související služby s ohledem na jejich kybernetickou bezpečnost, a to proto, že inherentní složitost platforem vozidel, s jejich dlouhými vývojovými cykly a složitými dodavatelskými řetězci, neumožňuje pozdější změny v architektuře vozidel.[4]

---

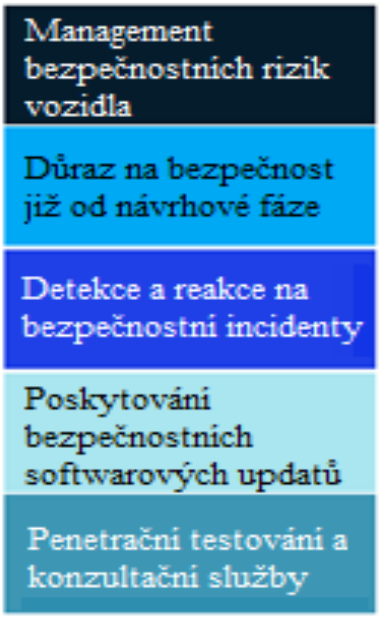
[1] Kissmann, A., & Schmidt, A. Security In The Driver's Seat Achieving Cyber Resilience In The Automotive Industry. *Accenture* [online]. 2018. [cit. 8. 11. 2020]. Dostupné z: https://www.accenture.com/_acnmedia/pdf-92/accenture-security-drivers-seat-automotive-cyber-resilience.pdf

[2] Hornetsecurity. CYBERSECURITY SPECIAL CYBERATTACKS IN THE AUTOMOTIVE SECTOR ON THE RISE [online]. 2020. [cit. 8. 11. 2020]. Dostupné z: https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-automotive-industry-en.pdf.

[3] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. [cit. 8. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

[4] DEICHMANN et al. The race for cybersecurity: Protecting the connected car in the era of new regulation. *McKinsey & Company* [online]. 2019. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/The%20race%20for%20cybersecurity%20Protecting%20the%20connected%20car%20in%20the%20era%20of%20new%20regulation/The-race-for-cybersecurity-Protecting-the-connected-car-in-the-era-of-new-regulation.pdf.

Zpětné opravy na nezabezpečeném produktu nejenže zvyšují náklady a komplexitu celého systému, ale také je lze snáze obejít, protože nemusí strukturálně vyřešit problém zranitelnosti.[1] Automobilky musí navíc zajišťovat kybernetickou bezpečnost po celou dobu životnosti produktu, protože kdykoli se mohou objevit nové technické chyby. Úkol tedy nekončí prodáním automobilu, ale měl by zahrnovat také poskytování softwarových updatů po celý jeho životní cyklus.[2]



Obr. 2: Životní cyklus automobilu z pohledu kybernetické bezpečnosti[3]

Navzdory jistému úsilí některých automobilových společností[4] však většina z nich v oblasti kybernetické bezpečnosti zaostává. Celému automobilovému průmyslu chybí

[1] BORDONALI, C., FERRARESI, S., & RICHTER, W. Shifting gears in cyber security for connected cars. *McKinsey & Company* [online]. 2017. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx.

[2] DEICHMANN et al. The race for cybersecurity: Protecting the connected car in the era of new regulation. *McKinsey & Company* [online]. 2019. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/The%20race%20for%20cybersecurity%20Protecting%20the%20connected%20car%20in%20the%20era%20of%20new%20regulation/The-race-for-cybersecurity-Protecting-the-connected-car-in-the-era-of-new-regulation.pdf.

[3] McKinsey & Company. Cybersecurity in automotive Mastering the challenge [online]. [cit. 10. 11. 2020]. 2020. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Cybersecurity%20in%20automotive%20Mastering%20the%20challenge/Cybersecurity-in-automotive-Mastering-the-challenge.pdf.

[4] IRWIN, B., & MENEGHINI, A. AUTOMOTIVE CYBERSECURITY: SHIFTING INTO OVERDRIVE. *Accenture* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://www.accenture.com/_acnmedia/PDF-130/Accenture-Cybersecurity-Automotive-2020.pdf.

standardizovaný přístup k řešení kybernetické bezpečnosti.[1] Přispěla k tomu mj. také skutečnost, že automobily jsou vyráběny z různých komponentů od různých výrobců či zástupců třetích stran po celém světě. Mnoho automobilových společností pak například nepřijímá odpovědnost za řešení kybernetických rizik, které by se mohly potenciálně objevit dále v rámci dodavatelského řetězce.[2] Efektivní zajištění kybernetické bezpečnosti však vyžaduje úsilí všech zainteresovaných stran.

Velký potenciál k řešení současné situace nabízejí závazné regulace a mezinárodní standardy kybernetické bezpečnosti v automobilovém sektoru. V červnu 2020 došlo v rámci Světového fóra pro harmonizaci předpisů o motorových vozidlech (spadající pod Evropskou hospodářskou komisi OSN) k přijetí dvojice regulací, které stanoví povinné minimální požadavky pro oblast kybernetické bezpečnosti v automobilovém sektoru. Tyto regulace vstoupily v platnost v rámci celé EU v lednu 2021, nicméně vzhledem k širokému používání regulací OSN v automobilovém průmyslu po celém světě se očekává široké přijetí těchto předpisů po celém světě.[3] V rámci EU pak dojde k jejich postupné implementaci v průběhu následujících 4 let (časový rámec zavádění regulací nabízí Příloha 1). Odborníci vnímají tato připravovaná nařízení jako začátek éry jednotných technických pravidel v automobilovém odvětví v oblasti kybernetické bezpečnosti.[4]

Ačkoli výše zmíněné regulace stanoví organizační rámec a minimální požadavky, mají převážně obecný charakter a neposkytují tak žádné podrobné pokyny k provozním postupům. Nezbytnou součástí kybernetické bezpečnosti v automobilovém průmyslu se tak stanou také mezinárodní standardy. Jedním z nejvýznamnějších připravovaných standardů je standard ISO / SAE 21434 (*Road Vehicles – cybersecurity engineering*), který je odborníky v oboru považován za první normu, která stanoví jasné organizační, procedurální a technické požadavky, a to během celého životního cyklu vozidla (od vývoje přes výrobu až po poprodejní služby).[5]

---

[1] DEICHMANN et al. The race for cybersecurity: Protecting the connected car in the era of new regulation. *McKinsey & Company* [online]. 2019. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/The%20race%20for%20cybersecurity%20Protecting%20the%20connected%20car%20in%20the%20era%20of%20new%20regulation/The-race-for-cybersecurity-Protecting-the-connected-car-in-the-era-of-new-regulation.pdf.

[2] MEISEL, A. How automakers can integrate security into connected car design. *Insights* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://intive.com/insights/how-automakers-can-integrate-security-into-connected-car-design/.

[3] UNECE. UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles [online]. 2020.[cit. 10. 11. 2020]. Dostupné z: http://www.unece.org/?id=54667&utm_source=UNECE+WP.+29+Final&utm_campaign=bd67d3021f-EMAIL_CAMPAIGN_2020_04_22_03_14_COPY_01&utm_medium=email&utm_term=0_615fc6747a-bd67d3021f-592610470.

[4] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

[5] McKinsey & Company. Cybersecurity in automotive Mastering the challenge [online]. 2020. [cit. 10. 11. 2020]. Dostupné z:

V současné době dochází k finalizaci tohoto standardu a jeho vydání se očekává v první třetině roku 2021.[1]

Implikace pro Českou republiku

Za posledních 10 let ve světě dramaticky vzrostl počet kybernetických bezpečnostních incidentů v automobilovém průmyslu, přičemž jen za poslední rok se počet zdvojnásobil.[2] Ačkoli v ČR prozatím k žádnému závažnějšímu kybernetickému útoku na automobil nedošlo, s rostoucím prodejem připojených vozidel exponenciálně narůstá jak riziko provedení takového útoku, tak míra škod, kterou takový útok může napáchat. Nelze tedy vyloučit, že během následujících let nedojde k méně či více závažným kybernetickým útokům na připojená vozidla. Kybernetický útok pak může vést k finančním ztrátám, odcizení citlivých nebo osobních údajů a dokonce také k ohrožení bezpečnosti uživatelů vozidel i všech ostatních účastníků provozu, včetně chodců.[3]

Cílem útoků mohou být sekundárně také čeští automobiloví výrobci či jejich dodavatelé, kteří mají rovněž zásadní vliv na bezpečnost automobilů. Podle společnosti Hornetsecurity se automobilový průmysl v roce 2019 stal jedním z nejčastěji zasahovaných odvětví kybernetickými útoky.[4] Na zranitelnost automobilového průmyslu poukázal například letošní útok na společnost Honda.[5] Vzhledem k významu automobilového sektoru pro českou ekonomiku (téměř 10 % HDP) [6] nelze hrozbu kybernetických útoků podceňovat.

Efektivní zajištění kybernetické bezpečnosti automobilů lze dosáhnout pouze prostřednictvím komplexních a dlouhodobě udržitelných opatření mezinárodního charakteru. Řešením současného nedostatečného stavu by se tak měly stát nově přijaté závazné regulace a mezinárodní standardy. Fáze implementace bude nicméně

---

https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Cybersecurity%20in%20automotive%20Mastering%20the%20challenge/Cybersecurity-in-automotive-Mastering-the-challenge.pdf.

[1] Frankfurt Solutions. Automotive Cybersecurity – ISO/SAE 21434 [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://www.frankfurtsolutions.com/en/2020/07/17/automotive-cybersecurity/.

[2] Upstream Security. Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem [online]. 2020. cit. 13. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

[3] ENISA. ENISA good practices for security of Smart Cars [online]. 2019.[cit. 13. 11. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/smart-cars/at_download/fullReport.

[4] Hornetsecurity. CYBERSECURITY SPECIAL CYBERATTACKS IN THE AUTOMOTIVE SECTOR ON THE RISE [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-automotive-industry-en.pdf.

[5] SEALS, T. Snake Ransomware Delivers Double-Strike on Honda, Energy Co*. Threat post* [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://threatpost.com/snake-ransomware-honda-energy/156462/.

[6] KONICAROVÁ, K. *Automobilový průmysl*. *CzechInvest* [online]. 2019. [cit. 13. 11. 2020]. Dostupné: https://www.czechinvest.org/cz/Sluzby-proinvestory/Klicove-sektory/Automobilovy-prumysl.

vyžadovat také aktivní přístup na národní úrovni. Z pohledu ČR je potřeba, aby byl stát připraven poskytnout potřebnou podporu českým automobilovým společnostem při implementaci předpisů a norem kybernetické bezpečnosti.

Očekává se, že regulace Evropské hospodářské komise OSN a standardy ISO zlepší současný nedostatečný stav kybernetické bezpečnosti v automobilovém průmyslu. Blížící se nástup automatizovaných a plně autonomních vozidel však bude vyžadovat novou sadu mezinárodních předpisů a norem. Je tedy potřeba, aby byla ČR připravena podílet se na vytváření jednotných regulací a standardů automobilů s vyšší úrovní autonomie (v rámci EU i EHK OSN), které budou dostatečně reflektovat výzvy v oblasti zajišťování kybernetické bezpečnosti.

Závěr

Čím dál více moderních automobilů v současnosti disponuje celou řadou digitálních komponentů a internetovým připojením, což je činí velice zranitelnými vůči kybernetickým útokům. Ty mohou vést k finančním ztrátám či odcizení osobních údajů uživatelů, ale také mohou ohrozit bezpečnost všech účastníků provozu. Kybernetických útoků na automobily přitom exponenciálně narůstá, přičemž nelze vyloučit možnost více či méně závažného kybernetického útoku v ČR. Sekundárním cílem útoků se mohou stát také automobiloví výrobci či dodavatelé, kteří mají rovněž zásadní vliv na bezpečnost automobilů. Zajištění kybernetické bezpečnosti proto vyžaduje komplexní přístup, který bude zohledňovat celý ekosystém vozu a zajistí bezpečnost po celý životní cyklus vozidla. Zlepšení současného stavu by měly přinést nově přijaté závazné regulace a mezinárodní standardy, nicméně jejich implementace bude do jisté míry závislá také na přístupu státu.

Seznam použitých zdrojů

AtlasVPN. *Automotive cyber incidents doubled in 2019, reaching 188 vulnerabilities* [online]. [cit. 7. 11. 2020]. 2020. Dostupné z: https://atlasvpn.com/blog/automotive-cyber-incidents-doubled-in-2019-reaching-188-vulnerabilities.

BORDONALI, C.; FERRARESI, S. & RICHTER, W. Shifting gears in cyber security for connected cars. *McKinsey & Company* [online]. 2017. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx.

ConsumerWatchdog. *Kill Switch: Why Connected Cars Can Be Killing Machines And How To Turn Them Off* [online]. 2019. [cit. 7. 11. 2020]. Dostupné z: https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf.

DEICHMANN et al. The race for cybersecurity: Protecting the connected car in the era of new regulation. *McKinsey & Company* [online]. 2019. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/The%20race%20for%20cybersecurity%20Protecting%20the%20connected%20car%20in%20the%20era%20of%20new%20regulat

ion/The-race-for-cybersecurity-Protecting-the-connected-car-in-the-era-of-new-regulation.pdf.

ENISA. *ENISA good practices for security of Smart Cars* [online]. 2019.[cit. 13. 11. 2020]. Dostupné z: https://www.enisa.europa.eu/publications/smart-cars/at_download/fullReport.

Fireeye. *CONNECTED CARS: THE OPEN ROAD FOR HACKERS* [online]. 2016. [cit. 7. 11. 2020]. Dostupné z: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf.

Frankfurt Solutions. *Automotive Cybersecurity – ISO/SAE 21434* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://www.frankfurtsolutions.com/en/2020/07/17/automotive-cybersecurity/.

Hornetsecurity. *CYBERSECURITY SPECIAL CYBERATTACKS IN THE AUTOMOTIVE SECTOR ON THE RISE* [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-automotive-industry-en.pdf.

HUQ, N., GIBSON, C., & VOSSELER, R. Driving Security Into Connected Cars: Threat Model and Recommendations. *Trend Micro Research* [online]. 2020. [cit. 7. 11. 2020]. Dostupné z: https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

IRWIN, B., & MENEGHINI, A. AUTOMOTIVE CYBERSECURITY: SHIFTING INTO OVERDRIVE. *Accenture* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://www.accenture.com/_acnmedia/PDF-130/Accenture-Cybersecurity-Automotive-2020.pdf.

KISSMANN, A., & SCHMIDT, A. Security In The Driver's Seat Achieving Cyber Resilience In The Automotive Industry. *Accenture* [online]. 2018. [cit. 8. 11. 2020]. Dostupné z: https://www.accenture.com/_acnmedia/pdf-92/accenture-security-drivers-seat-automotive-cyber-resilience.pdf.

KONICAROVÁ, K. Automobilový průmysl. *CzechInvest* [online]. 2019. [cit. 13. 11. 2020]. Dostupné: https://www.czechinvest.org/cz/Sluzby-proinvestory/Klicove-sektory/Automobilovy-prumysl.

KULDA, T. Kybernetická bezpečnost v automobilovém sektoru: Kdy budeme moct věřit svým autům? *PwC Česká republika* [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://nukib.cz/download/aktuality/Kulda.pdf.

KYUSUK, H., WEIMERSKIRCH, A., & SHIN, K. G. Automotive Cybersecurity for In-Vehicle Communication. *IQT QUARTERLY SUMMER* [online]. 2014, 6(1). [cit. 6. 11. 2020]. Dostupné z: https://www.iqpc.com/media/1001748/37529.pdf.

McKINSEY & Company. *Cybersecurity in automotive Mastering the challenge* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Cybersecurity%20in%20automotive%20Mastering%20the%20challenge/Cybersecurity-in-automotive-Mastering-the-challenge.pdf.

MEISEL, A. How automakers can integrate security into connected car design. *Insights* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: https://intive.com/insights/how-automakers-can-integrate-security-into-connected-car-design/.

PwC. *Cyber readiness: are auto companies prepared to counter the risk of an attack?* [online]. 2018. Dostupné z: https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-auto-cyber-readiness.pdf.

SEALS, T. Snake Ransomware Delivers Double-Strike on Honda, Energy Co. *Threat post* [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://threatpost.com/snake-ransomware-honda-energy/156462/.

UNECE. *UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles* [online]. 2020. [cit. 10. 11. 2020]. Dostupné z: http://www.unece.org/?id=54667&utm_source=UNECE+WP.+29+Final&utm_campaign=bd67d3021f-EMAIL_CAMPAIGN_2020_04_22_03_14_COPY_01&utm_medium=email&utm_term=0_615fc6747a-bd67d3021f-592610470.

Upstream Security. *Upstream Security's Global Automotive Cybersecurity Report: Research Into Cyber-Attack Trends In The Smart Mobility Ecosystem* [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf.

R E S U M É

Tento článek se zabývá problematikou kybernetické bezpečnosti moderních automobilů. Současné trendy digitalizace, automatizace a autonomizace a narůstající konektivita automobilových vozidel s sebou nesou negativní implikace pro zajišťování bezpečnosti v rámci celého automobilového průmyslu. Cílem článku je tedy představit aktuální kybernetické hrozby a rizika spojená s moderními automobily a nabídnout možnost řešení současného nedostatečného stavu v automobilovém sektoru. Komplexní ekosystémy moderních vozidel je činí čím dál zranitelnějšími vůči kybernetickým útokům, kterých exponenciálně narůstá. Řešení současného stavu mohou přinést nově přijaté závazné regulace a mezinárodní standardy, které kladou důraz na komplexní přístup k zajišťování kybernetické bezpečnosti v automobilovém sektoru.

Klíčová slova: kybernetická bezpečnost; automobilový průmysl; autonomní vozidla.

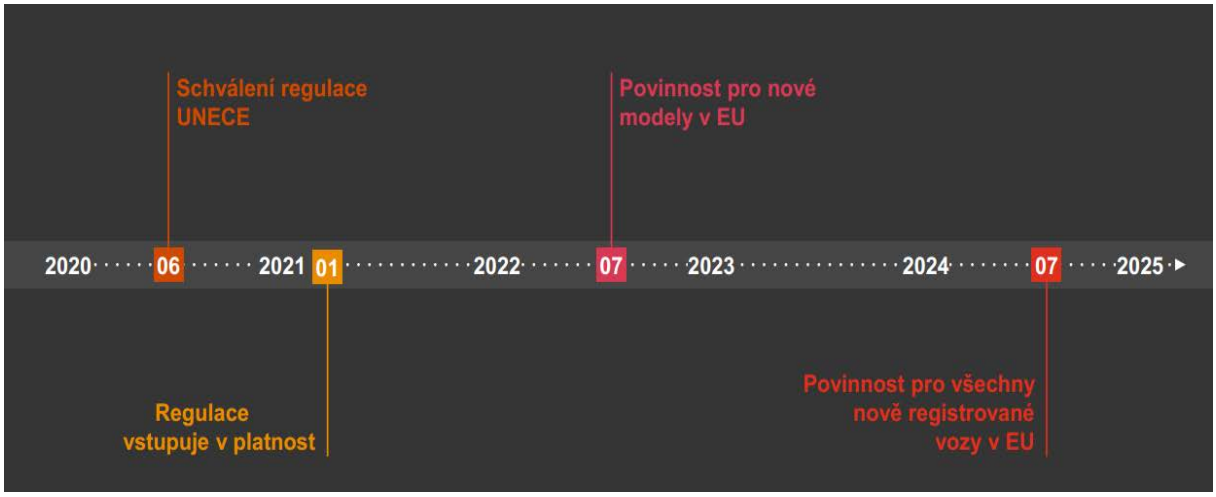
S U M M A R Y

RECHTIK, Marek: CYBERSECURITY IN THE AUTOMOTIVE SECTOR

This article deals with the issue of modern cars cybersecurity. Current trends in digitization, automation and autonomy and the growing connectivity of vehicles bear negative implications for ensuring security and safety throughout the automotive industry. The aim of the article is to present the current cyber threats and risks connected with modern cars and to outline possible solution to the insufficient state of affairs in the automotive sector. The complex ecosystems of modern vehicles make them increasingly vulnerable to cyber-attacks, which are growing exponentially. Newly adopted binding regulations and international standards, which stress the importance of a complex approach to ensuring cybersecurity in the automotive sector, seem to be able to provide a solution to the current situation.

Keywords: cybersecurity; automotive industry; autonomous vehicles.

Příloha 1: Časový rámec přijetí regulací Evropské hospodářské komise OSN (UNECE)[1]



[1] KULDA, T. Kybernetická bezpečnost v automobilovém sektoru: Kdy budeme moct věřit svým autům? *PwC Česká republika* [online]. 2020. [cit. 13. 11. 2020]. Dostupné z: https://nukib.cz/download/aktuality/Kulda.pdf.