ALISON

V nasledujúcich piatich rokoch si musí automobilový priemysel rezervovať na obranu proti kyber útokom aspoň 24 miliárd dolárov

Automobilový svet sa mení na ekosystém inteligentnej mobility. Do siete sú pripojené vozidlá počas navigácie aj servisu, testujú sa autonómne vozidlá a každým rokom rastú či pribúdajú služby spoločného využívania áut. S rozvojom odvetvia vznikajú zároveň nové formy kybernetickej kriminality.

Zberná doprava a preprava každého druhu zvyšujú zložitosť celého systému a zároveň riziko kybernetického útoku rapídnym tempom. Štúdia Upstream Security za rok 2019 je prvá svojho druhu a poukázala nielen na to, kto čelí riziku, ale aj ako sa hlavní zainteresovaní chránia a aké ohrozenia možno očakávať v roku 2019.

Autori štúdie počas rokov 2010 – 2018 analyzovali 170 bezpečnostných incidentov spôsobených útokmi na jednotlivé značky, spôsobených aplikáciami alebo v systémoch prepravcov a dopravných služieb. Štúdia opisuje v automotive útoky hekerov od fyzických cez diaľkové až po útoky cez bezdrôtovú sieť, ako aj spôsob, akým útočníci obvykle prenikajú do priestoru inteligentnej mobility.

Útoky možno spustiť odkiaľkoľvek a ohroziť vodičov aj cestujúcich. Problémy, ktoré spôsobia, sú rôzneho typu – chyby v kritických systémoch vozidiel, prieniky do dátových centier na podporných serveroch, krádeže totožnosti pri spoločnom využívaní vozidiel a dokonca ohrozenie ochrany osobných údajov. Riziko je vysoké. Len jeden počítačový útok môže stáť výrobcu automobilov 1,1 miliardy dolárov a celé odvetvie môže do roku 2023 čeliť strate až 24 miliárd dolárov.

Kľúčové zistenia

- Výrobcovia automobilov sú zjavným cieľom kybernetickej kriminality, no čoraz väčšiemu riziku čelia aj dodávatelia prvej úrovne, prevádzkovatelia vozových parkov, poskytovatelia telematických služieb, spoločnosti na zdieľanie áut aj súkromní a verejní prepravcovia.

- Počet útokov nepriateľských hekerov (Black hats) v roku 2018 prevýšil počet kontrolovaných útokov a zistení zo strany etických hekerov (White hats). Došlo k tomu v oblasti inteligentnej mobility po prvýkrát v histórii.

- Spoločné využívanie vozidiel a výmeny vodičov sú terčom úplne nového typu počítačových útokov. Majú merateľný dosah na súkromie a sú zdrojom podvodného správania.

- 42 percent incidentov v oblasti automobilovej kybernetickej bezpečnosti zasiahlo podporné aplikačné servery.

- Zabezpečenie treba vybudovať vo viacerých vrstvách. Samotné vozidlo sa musí chrániť proti útokom zblízka, ďalšie úrovne ochrany sa musia týkať automobilového cloudu, do ktorého je pripojených viac vozidiel, služieb a aplikácií, a siete ktorá poskytuje podporu celej architektúre.

„Každá nová služba a pripojený subjekt znamenajú vytvorenie nového vektoru pre útok," uzatvára Oded Yarkoni, vedúci marketingu Upstream Security.