حفاظت از خودروها در برابر حملات سایبری

امروزه کسی نیست که با حمله‌های سایبری آشنایی نداشته باشد و چنین حمله‌هایی تأثیرات منفی زیادی بر زندگی بسیاری از افراد گذاشته است. تاکنون این حمله‌ها به‌طور مستقیم آسیب جسمی به کابران وارد نکرده است (البته نرم‌افزارهای مخربی وجود داشته‌اند که قادر به ایجاد خسارت‌های فیزیکی نظیر انفجار نمایش‌گر پیش روی کاربر بوده‌اند). روند اتصال خودروها به شبکه‌هایی نظیر اینترنت اجتناب‌ناپذیر خواهد بود و همین امر سبب خواهد شد بخش مهمی از حمله‌های سایبری بر خودروها و وسایل نقلیه متمرکز شود.

در حال حاضر، روز به روز بر شمار خودروهایی با قابلیت اتصال به اینترنت افزوده می‌شود و این خودروها طعمه‌های بسیار خوبی برای مهاجمان سایبری خواهند بود. آن‌ها می‌توانند با نفوذ به چنین خودروهایی، به‌سادگی آسیب‌های فیزیکی قابل توجهی به طعمه‌های خود بزنند. چندی قبل بود که گروهی از محققان موفق شدند از راه دور به یک خودروی جیپ نفوذ و آن را در بزرگ‌راه کنترل کنند.

□□□□ □□□□□□□□□□: □□ □□ □□□ □□□ □□ □□□ □□□ □□ □□□ □□□□□□□□

فیات کرایسلر بعد از مشخص شدن نفوذپذیری محصولاتش، بیش از یک میلیون دستگاه از خودروهای خود را فراخواند تا آن‌ها را مورد بازبینی امنیتی قرار دهد. وقتی قادر باشیم با یک خودرو در گوگل جست‌وجو کنیم، توییت بفرستیم و توسط یک تلفن همراه از راه دور به آن دسترسی داشته باشیم، عملاً آن خودرو به یک ابزار همراه تبدیل شده است و در نتیجه لازم است مشابه بسیاری از تمهیدات امنیتی مرسوم در حوزه ابزارهای همراه را در صنعت خودروسازی هم پیاده کنیم. در آینده‌ای نزدیک، میزان سطح امنیت سایبری یک خودرو را نیز باید به‌عنوان یک پارامتر مهم در تعیین استاندارد خودرو در نظر بگیریم. خودرویی که به‌راحتی قابل هک و نفوذ باشد، قطعاً نباید راهی به جاده‌ها بیابد. کافی است یک خودرو مورد حمله سایبری قرار بگیرد و فردی شرور از راه دور کنترل خودرو را در دست بگیرد. دیگر هیچ چیزی قابل برگشت نخواهد بود و عواقبی به مراتب بدتر از سوانح رانندگی فعلی رخ خواهد داد. هر چند تاکنون اتفاقات فاجعه باری در این حوزه رخ نداده، اما لازم است صنعت خودروسازی از سال‌ها تجربه‌ای که در حوزه نرم‌افزارهای متصل به اینترنت کسب شده است، برای بالا بردن ایمنی سایبری خودروهای آینده استفاده کند.
به‌منظور بالا بردن سطح ایمنی سایبری در خودروها می‌توان سه رویکرد مهم را در پیش گرفت. نخست این‌که خودروها باید به سیستم به‌روزرسانی از راه دور مجهز شوند تا نیازی نباشد برطرف کردن یک نقص امنیتی همه

خودروها فراخوانده شوند و نقص برطرف شود؛ زیرا فراخوانی فیزیکی خودروهای آسیب‌پذیر کاری بسیار پرهزینه و زمان‌بر است. نکته دومی که خودروسازان باید مورد توجه قرار دهند، جدا کردن سیستم‌های اطلاعات سرگرمی (Infotainment) خودرو از سیستم‌های حیاتی و حساس خودرو است، به گونه‌ای که ارتباط بین این دو سیستم به‌طور دقیق تحت کنترل باشد.
مشابه همان رویکردی که در خطوط هوایی شاهدیم و شبکه‌های وای‌فای درون هواپیما از سیستم‌های ناوبری هواپیما مجزا هستند. سومین مورد این است که خودروسازان همواره باید این طور فرض کنند که برخی حمله‌های سایبری قطعاً موفق خواهند شد و در نتیجه لازم است هر جزء از نرم‌افزاری را که طراحی کرده‌اند، ایمن‌سازی کنند. به طوری که اگر یک مهاجم موفق شد به بخشی از سیستم نرم‌افزاری نفوذ کند، موفق به کنترل کل سیستم نشود. در هر صورت، حتی اگر یک شرکت خودروساز در گروه امنیتی خود از زبده‌ترین افراد استفاده کند، باز هم سال‌ها طول خواهد کشید تا یک سیستم ایمن در برابر حمله‌های سایبری در خودروها ایجاد شود. به‌ویژه این‌که چنین حمله‌هایی بر خلاف نفوذهایی که به‌طور مثال به کامپیوترهای رومیزی صورت می‌گیرد، بسیار زیان‌بارتر خواهد بود؛ زیرا به‌طور مستقیم با جان انسان‌ها و سلامت آن‌ها سروکار دارد.

شرح شکل: این دو نفر از جمله کسانی بودند که موفق شدند با حداقل تجهیزات، از راه دور خودرویی را در یک بزرگ‌راه هک کنند.

منبع:

تک کرانچ
تاریخ انتشار:
16 آبان 1394

نشانی منبع: https://www.shabakeh-mag.com/information-feature/2147