aut. Bartosz Józefiak 01.07.2016

BRANŻA TRANSPORTOWA SZCZEGÓLNIE PODATNA NA CYBERZAGROŻENIA

Branża transportowa jest szczególnie wrażliwa na ryzyko cyberataku - podkreślają badacze sieci. Systemy sterowania ruchem stają się łatwym celem dla hakerów - także tych powiązanych z grupami terrorystycznymi. Efektem może być np. paraliż lotów lub kradzież danych pasażerów. Takie sytuacje miały już miejsce w Szwecji, Chinach oraz w Polsce.

Raport na temat przemysłu transportowego przygotował zespół ds. cyberbezpieczeństwa firmy IBM. Wynika z niego, że transport to jedna z branż najbardziej narażonych na atak hakerów.

W dokumencie „Prognozy bezpieczeństwa dla przemysłu transportowego" (Security Trends in the Transportation Industry) czytamy, że cyberkryminaliści obrali sobie za cel systemy używane do obsługi ruchu pociągów, samolotów i samochodów.

Transport na celowniku terrorystów

Autorzy raportu tłumaczą, że branża transportowa jest szczególnie narażona na zagrożenia płynące z sieci ze względu na rosnącą rolę cybernetycznych systemów sterowania, nawigacji, wyznaczania trasy i komunikacji. Systemy używane w transporcie zbierają ogromną liczbę informacji, które mogą wpaść w ręce hakerów chcących sprzedać je na czarnym rynku. Taka sytuacja miała już miejsce np. z punktami przyznawanymi przez linie lotnicze dla najwierniejszych pasażerów. Największym zagrożeniem dla systemów są ataki DdoS, a także wirusy przesyłane drogą mailową do firm transportowych. Ataki wirusami ransomware również nie są rzadkością.

Zagrożenie dla transportu płynie jednak nie tylko od strony złodziei. Duże ryzyko wiąże się też z terroryzmem. Nietrudno sobie wyobrazić, jak wielkie szkody mógłby wyrządzić ekstremista, który przejąłby kontrolę nad systemami sterowania ruchem pociągów, ruchem lotniczym czy sygnalizacją świetlną. Co prawda systemy te są zazwyczaj dobrze chronione, zwłaszcza jeśli chodzi o lotniska, co jednak nie oznacza, że ryzyka nie ma. Zwłaszcza programy odpowiedzialne za sterowanie ruchem ulicznym są podatne na ataki. Eksperci od cyberbezpieczeństwa już udowodnili, że w dobie „smart cities" przejęcie kontroli nad sterownikami świateł nie jest niczym niezwykłym. Urządzenia do komunikacji pomiędzy światłami, kamerami a centrum sterowania ruchem znajdują się w ogólnie dostępnych miejscach i wykorzystują technologię bluetooth do komunikacji. To otwiera szerokie pole do działania dla przestępców.

Paraliż lotnisk w Szwecji i w Polsce

Ruch lotniczy również nie jest całkowicie bezpieczny. Doświadczyli tego pasażerowie w Szwecji. W listopadzie zeszłego roku doszło tam do paraliżu lotniczego, a komputery w wieżach kontroli lotów w Arlandzie, Landvetter i Brommie odmówiły posłuszeństwa. Kontrolerzy nie byli w stanie podglądać ruchu samolotów, dlatego odwołano większość lotów krajowych i międzynarodowych. Początkowo jako

powód incydentu podawano burze słoneczne zakłócające prace radarów. Dopiero kilka miesięcy temu władze przyznały, że przyczyną był atak hakerski. Cyberprzestępcy zaatakowali też systemy komputerowe kontroli lotów na Okęciu. Do akcji doszło w czerwcu zeszłego roku. Z powodu operacji hakerów odwołano 10 lotów krajowego przewoźnika.

Inny atak spotkał chińskie linie kolejowe. W 2014 r. z serwerów kolei narodowej wykradziono dane osobowe pasażerów.

Zagrożone są nie tylko firmy transportowe, ale także indywidualni użytkownicy. Rosnące znaczenie internetu rzeczy w samochodach otwiera je na możliwość cyberataku. Na początku czerwca eksperci od cyberzabezpieczeń zdalnie przejęli kontrolę nad aplikacją obsługującą najnowszy model Mitsubishi Outlander. Dzięki temu zdalnie wyłączyli system zabezpieczeń samochodu.

Ekspert cyberbezpieczeństwa Pierluigi Paganini na swoim blogu podkreśla, że odpowiedzialność za zidentyfikowanie zagrożeń spoczywa na operatorach obsługujących branżę transportową. Z kolei rządy państw powinny przygotować rekomendacje niezbędne do ochrony krytycznej infrastruktury, jaką jest przemysł transportowy.

Czytaj też: Szwecja obwinia rosyjskich hakerów o paraliż ruchu lotniczego