**Semester-hackarna kan bli en del av vårt framtida resande**

**Nedstängda bagagehanteringssystem, självkörande bussar som blivit hackade till att blockera trafiken eller boardingkort som är ur funktion. Låter det som en avlägsen och obehaglig dystopi? Men den framtiden kanske är här snabbare än vi tror, menar Erik Henriksson på Akamai i Sverige.**

Så här i slutet av sommaren är det många som fortfarande vårdar sina semesterminnen ömt. Kanske har man redan börjat fundera på någon ny resa och nya spännande resmål, kanske redan till det stundande höstlovet. Vi reser allt mer och framförallt mer under hela året. Resandet blir också allt mer automatiserat med hjälp av den nya teknologin. Men den nya teknologin gör också vårt resande allt mer sårbart och öppet för hackare som på något sätt vill störa ut trafiken. Erik Henriksson på Akamai ser en allt större marknad för hackare breda ut sig.   
  
– Tänk dig att en hackare beslutar sig för att till exempel stänga ner bagagehanteringen på en av världens största flygplatser. Det är lätt att föreställa sig kaoset som snabbt skulle uppstå. Vad händer om hackaren sedan krävde en lösensumma för att låsa upp de digitala nätverk som de hade kapat, säger han.

Enligt en nyligen släppt rapport från Akamai är ett sådant scenario inte någon fantasi i någon avlägsen dystopi. Det ligger precis runt hörnet, menar Erik Henriksson.

– Det kanske låter lite skrämmande. För även om vi inte är helt där än, så finns det flera oroande trender som vi tar upp i rapporten. Och det bygger på att tekniken fortsätter att utvecklas, med stora och snabba framsteg inom artificiell intelligens, automation, biometri – och dessutom en snabbt växande IoT-marknad. Med detta kommer en ökande och potentiellt risk för att illasinnade aktörer utvecklar digital infrastruktur som siktar mot att skada vitala samhällstjänster, säger han.

Erik Henriksson menar att cyberkriminella alltid kommer att söka hitta de svagaste länkarna, som att identifiera personer som aldrig uppdaterar sina lösenord och använder oidentifierade WiFi-nätverk utan granskning. Eller så söker man hitta kommersiella sektorer där man släpar efter i säkerhetsstandarder. Ett sådant segment, som rapporten pekar ut, är den ständigt växande turistmarknaden.   
  
– Bara under 2017 inträffade nästan fyra miljarder skadliga inloggningsförsök mot webbplatser som tillhör flygbolag, kryssningsfartyg, hotell, resebyråer, biluthyrning och transportorganisationer. Det är svindlande siffror, tycker Erik Henriksson.

Att se att problemet växer och från var attackerna har sitt ursprung är lätt, att hitta vem som är ansvarig är svårare. Organiserade cyberkriminella riktar sig mot just turistbranschen för att det är relativt oskyddat. Därför menar Erik Henriksson att det hotell och restauranger kan dra lärdom från både finans- och retail-branschen. Det finns tekniska skydd, men man behöver förstå hur hotbilden ser ut inom sin bransch. Erik Henriksson tycker att man ska polisanmäla alla cyberbrott och se till att polisen får del av data.   
  
– Det hjälper till i arbetet för att kartlägga cyberbrott och förstå de komplexa kriminella nätverk som ligger till grund för det. Annars finns det stor risk för att semester-hackarna kan komma att bli en del av vårt framtida resande, avslutar han.