Alerta per ciberatac: un 'hacker' podria fer caure un avió?

Fa anys que els experts informàtics adverteixen que els avions de passatgers són vulnerables als ciberatacs. Les companyies aèries i els fabricants d'avions n'han ignorat en gran part els riscos, però el que ha passat darrerament ha portat les autoritats alemanyes i els pilots a prendre's seriosament les amenaces.

Marcel Rosenbach i Gerald Traufetter
© Der Spiegel

Als funcionaris de l'Agència Europea de Seguretat Aèria (AESA) no els feia gens de gràcia el que sentien. Un espanyol de 32 anys sense afaitar, amb els cabells lligats en una cua, parlava dels ordinadors de cabina i sobre els punts febles i les llacunes de seguretat que tenen. Concretament, explicava als treballadors de l'AESA com havia aconseguit comprar peces originals de proveïdors de la indústria aeronàutica a Ebay per tan sols uns quants centenars de dòlars. El seu objectiu era simular l'intercanvi de dades entre els models actuals d'avió de passatgers i els controladors aeris que hi ha a terra per trobar possibles portes falses. La recerca li va sortir bé. Molt bé.

La presentació d'aquell espanyol va tenir lloc en una sala de conferències del grup empresarial EADS, amb vistes a les teulades de Colònia. L'havien convidat després que, d'acord amb l'ètica dels *hackers*, havia notificat a l'agència que tenia pensat presentar els resultats d'anys d'investigació en un congrés d'experts informàtics. També hi havia enginyers d'aerolínies i fabricants d'avions que seguien la presentació per vídeo. En acabar, recorda l'expert, tots volien saber el mateix: "No deu pas voler fer pública tota aquesta informació, oi?".

La preocupació se centrava en la descoberta principal, que el hacker encara avui repeteix. "Als avions moderns, hi ha una bona colla de portes falses, a través de les quals els pirates informàtics poden accedir a un gran nombre de sistemes de navegació aèria".

Aquell noi es diu Hugo Teso, i ara treballa per a una empresa de seguretat de dades amb seu a Berlín. Durant els últims anys, ha rebut encàrrecs de diverses empreses per intentar-se introduir en els seus ordinadors i xarxes. Però com que Teso també és pilot i encara té una llicència vàlida, en el sector de l'aviació s'ha anat guanyant la reputació que els seus advertiments sobre seguretat s'han de prendre seriosament.

Teso ha demostrat que ni tan sols es necessita un ordinador per segrestar un avió per control remot. N'hi ha prou amb un *smartphone* equipat amb l'aplicació PlaneSploit, que ell mateix ha desenvolupat. Teòricament, els ciberterroristes podrien fer servir una aplicació com aquesta, o alguna de semblant, per prendre el control del sistema de direcció d'un avió i, en el pitjor dels casos, estavellar l'aparell.

A quin perill s'atenen aerolínies i passatgers?

Els atacs als ordinadors de cabina han estat un tema recurrent als congressos d'experts informàtics. Però durant molt de temps les companyies aèries i els fabricants d'avions han intentat treure importància a les advertències, o les han ignorades completament. La setmana passada, però, el debat es va intensificar. L'FBI està analitzant si l'expert informàtic nord-americà Chris Roberts ha implementat realment –si més no parcialment, trobant-se a bord d'una aeronau– el que Teso ha advertit i simulat. Roberts afirma que s'ha introduït unes quantes vegades en el sistema d'entreteniment d'un avió de passatgers corrent i que fins i tot ha manipulat els motors de la nau durant el vol.

Les afirmacions i la consegüent investigació han desencadenat un nou debat entorn del perill potencial a què fan front aerolínies i passatgers. L'Oficina de Comptabilitat Governamental (OCG) dels Estats Units ja havia assenyalat al gener els problemes potencials per al control del trànsit aeri, afirmant que la tecnologia que s'utilitzava per comunicar-se entre pilots i controladors era obsoleta. Mentre no s'abordi el problema, deia l'informe de l'OCG, "els punts fe-

bles que hem identificat és probable que es mantinguin, fet que, com més va, més posa en un risc innecessari l'operació segura i ininterrompuda del sistema de control aeri del país".

En un altre estudi, publicat a l'abril, l'agència analitzava amb més detall els avions en si i advertia explícitament de la creixent connectivitat de components individuals. "Aquesta possibilitat d'interconnexió pot donar potencialment accés remot no autoritzat al sistema de navegació dels avions", explica l'informe. Un dels coautors de l'estudi va dir a la televisió nord-americana que les descobertes són especialment aplicables als avions més nous, com ara el Boeing 787 Dreamliner i els models Airbus de llarg recorregut A350 i A380.

Si les afirmacions que ha fet darrerament Roberts, l'expert informàtic nord-americà, es confirmen, s'esvairien pràcticament tots els dubtes que queden sobre la vulnerabilitat dels avions de passatgers i seria una prova pràctica que els models d'avió comuns poden ser controlats per *hackers*.

Es diu que Roberts va fer aquestes declaracions a un agent especial de l'FBI al febrer i al març. L'agent va incorporar transcripcions d'aquelles converses en una petició judicial en què demanava permís per analitzar maquinari que prèviament s'havia confiscat a Roberts.

Interceptar sistemes sensibles

Segons un document de l'FBI, que va fer públic el portal de notícies canadenc APTN, Roberts va aconseguir accedir il·legalment als sistemes d'entreteniment de bord –fabricats per companyies com Panasonic i Thales– d'avions de passatgers com el Boeing 737, el Boeing 757 i l'Airbus A320. Ho va aconseguir un total de quinze vegades de vint entre el 2011 i el 2014. Per fer-ho, va connectar el portàtil a la caixa d'elements electrònics del seient –que sol estar situada sota cada seient– fent servir un cable Ethernet, cosa que ja és prou desconcertant.

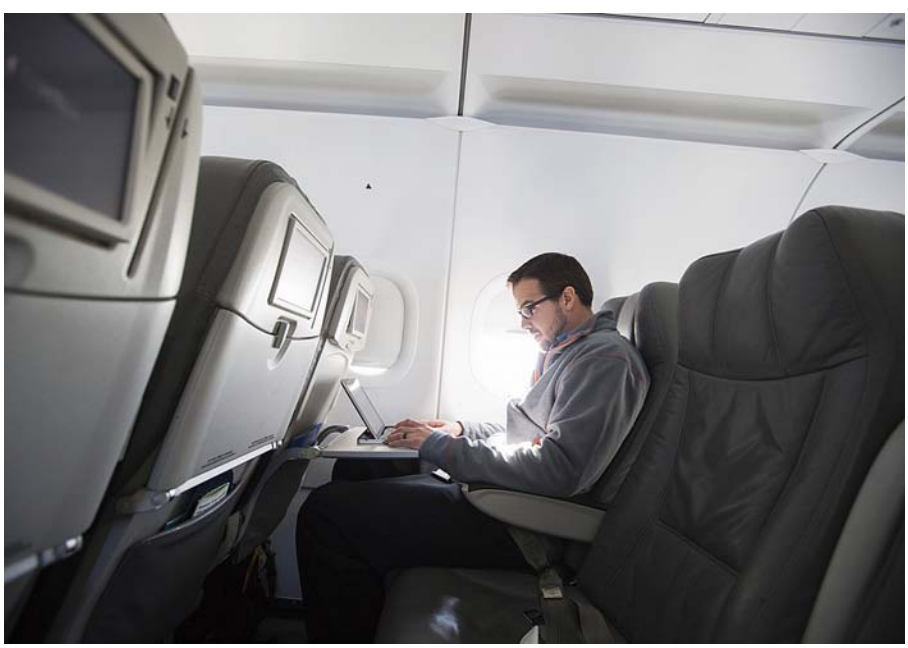
Però Roberts també hauria pogut fer servir aquesta caixa potencialment per infiltrar-se en els sistemes sensibles que controlen els motors. En un cas, fins i tot podria haver manipulat els motors durant el vol. Diu que va aconseguir introduir el comandament "CLB", que en anglès representa "climb" ('ascendir') i els motors van reaccionar degudament, segons el document que recull el que Roberts va afirmar davant de l'FBI.

Actualment, Roberts té poca presència pública, només va dir a Twitter la setmana passada que el seu "equip legal encara està fent consultes, de moment no dic res". Sí que va escriure, però, que "durant els últims cinc anys el meu únic interès ha estat millorar la seguretat dels avions". Diu que l'FBI "va condensar incorrectament" els seus treballs en un únic paràgraf en la seva declaració jurada.

Sembla que l'FBI es pren molt seriosament Roberts i els seus esforços per accedir il·legalment als sistemes de computació dels avions. El document de l'FBI ajuda a explicar un incident de mitjan abril que va fer aparèixer Roberts, originari de Colorado, per primera vegada als titulars. Anava a bord d'un 737 de United Airlines i es va connectar a Twitter mitjançant la xarxa de Wi-Fi per a passatgers. "Comencem a jugar amb els missatges EICAS? "QUE BAIXIN LES MÀSCARES D'OXIGEN" Que hi ha algú?", va escriure. EICAS són les sigles en anglès de "sistema d'indicacions del motor i d'avís a la tripulació", que envien dades en temps reals dels motors de l'avió a la cabina.

Reacció rècord

L'FBI, juntament amb United, va reaccionar a la piulada en un temps rècord. Després que Roberts fes transbord a Chicago, a mig camí del trajecte de Denver a Syracuse, uns agents de l'FBI van en- →



→ trar a l'avió d'on acabava de baixar per examinar la caixa d'elements electrònics de sota el seu seient. Les dues caixes més pròximes, segons apunta l'FBI, presentaven senyals que les havien intentat de manipular. A la revista *Wired*, Roberts va negar que fos responsable de la manipulació.

Quan Roberts va arribar a Syracuse, l'FBI el va fer baixar de l'avió i li va requisar l'equipament electrònic. En aquell moment, semblava que l'FBI només reaccionés davant de la piulada de Roberts. Però el document de l'FBI que ara s'ha difós permet entendre la nerviositat dels agents: el document assenyala que Roberts, en l'interrogatori a què va ser sotmès al febrer, va prometre que mai més no intentaria accedir a xarxes d'avions.

ELS CIBERTERRORISTES PODRIEN FER SERVIR UNA APLICACIÓ, PER PRENDRE EL CONTROL D'UN AVIÓ

Companyies aèries i fabricants han callat durant molt de temps respecte a aquests incidents i a les possibles conseqüències. Un portaveu de Lufthansa, per exemple, va dir: "La nostra política és no comentar aquesta mena d'esdeveniments". Airbus només va insistir que els seus sistemes i procediments són segurs i que estan equipats per resistir ciberatacs potencials. L'empresa no va voler fer comentaris, dient que no parlava públicament sobre els seus sistemes de seguretat.

Entre els pilots, però, la qüestió és tan urgent com inquietant. "La indústria i les companyies aèries no poden continuar de braços plegats", diu Markus Wahl, portaveu de Vereinigung Cockpit, un sindicat de pilots alemany. "Sempre hem suposat que el capità podria defensar-se d'un ciberatac", va dir el portaveu. Tanmateix, va afegir que no es pot descartar el perill sense reflexionar-hi i que no s'hauria de trivialitzar. Wahl, que és pilot, va dir que les aerolínies fins ara no han tractat la qüestió amb el nivell adequat d'urgència.

SEGURETAT. "Als avions moderns, hi ha una bona colla de portes falses, a través de les quals els pirates poden accedir a un gran nombre de sistemes de navegació aèria." A la imatge de baix Hugo Teso.

L'any passat, Vereinigung Cockpit va convidar Hugo Teso a la seva convenció anual. "Després de la presentació, tothom estava força contemplatiu", explica Wahl. La raó era, en part, l'expertesa de Teso. "Aquell home és un gran coneixedor de la cabina de comandament", conclou Wahl.

El perill de les modificacions

Certament, aquestes preocupacions ajuden a explicar la reacció aïrada a una proposta que va tenir acceptació després de l'accident de Germanwings. La proposta era que es dirigissin els avions de passatgers per control remot des de terra. La idea té el suport de Klaus-Dieter Scheurle, cap de la companyia alemanya de control aeri Deutsche Flugsicherung. En canvi, Wahl diu que "això crearia un nou objectiu enorme per a ciberatacs".

Teso comparteix l'opinió de Wahl. Fa poc fins i tot va identificar diversos riscos de seguretat addicionals. Quan un avió surt de fàbrica, diu Teso, és molt menys vulnerable. Els problemes apareixen quan més endavant es modifiquen els aparells, per exemple, instal·lant-hi Wi-Fi i sistemes d'entreteniment o equipant els pilots amb tauletes per a operacions prèvies al vol que després s'enduen a la cabina.

Algunes autoritats alemanyes, com l'Oficina Federal per a la Seguretat Informàtica (OFSI), es prenen seriosament les qüestions que planteja Teso. Les seves investigacions, diu un portaveu, han estat "analitzades detingudament". "La seva visió és realista i ha exposat punts febles que cal eliminar". L'OFSI, però, no està d'acord amb Teso que aquests punts febles puguin ser aprofitats fàcilment. "Nosaltres creiem que un atac, encara que tingués èxit, faria passar una mala estona als pilots, però no n'hi hauria prou per prendre el control de l'aparell".

Als Estats Units, sembla que el cas de Roberts ja ha portat conseqüències. Fins ara, els portàtils es consideraven un perill sobretot pel pes: cas de fortes turbulències durant l'enlairament o l'aterratge podrien caure i fer mal a algun passatger. Però ara als membres de la tripulació no tan sols se'ls demana que s'assegurin que els ordinadors estan guardats durant l'enlairament i l'aterratge; l'FBI i les autoritats del trànsit aeri han emès un avís per a tot el personal de vol que vigilin els passatgers que intentin connectar el portàtil a aparells de l'avió. •

Traducció d'Arnau Figueras