الخليج

اقتصاد, سياحة وطيران

10 سبتمبر 2021 19:06 مساء

شركات الطيران تحذر من مخاطر قراصنة المعلومات الجدد



أدت التدابير الأمنية المتخذة في المطارات والطائرات بعد اعتداءات 11 سبتمبر / أيلول إلى الحد بشكل كبير من مخاطر اقتحام إرهابيين قمرة قيادة الطائرات، غير أن مخاوف شركات الطيران تتركز الآن على هجمات قد يشنها قراصنة معلوماتيون.

فبين تحصين أبواب قمرات القيادة، واستخدام أجهزة فائقة التطور لرصد المتفجرات، وإدراج أسماء بعض الركاب على قوائم أمنية، وحظر الأغراض الحادة والدقيقة الرأس، ومراقبة الأجهزة الإلكترونية والأحذية والمواد السائلة داخل الطائرة، يؤكد المدير العام ل «الاتحاد الدولي للنقل الجوي» (إياتا) ويلي والش قائلاً: «إننا أكثر أماناً» داخل الطائرات اليوم.

المخاطر الجديدة

وإن حاول شخص رغم كل ذلك السيطرة على طائرة، فإن «الركاب أنفسهم سيتصدون له على ضوء ما حصل في 11

أيلول / سبتمبر»، برأي دان كاترير الطيار السابق الذي أصبح خبيراً في الأمن الجوي في جامعة «إمبري ريدل» الأمريكية. وأوضح كاترير أن المخاطر الجديدة باتت خفية، ذاكراً من أبرزها فيروس «كورونا» الذي ينعكس على مجمل حركة النقل الجوي منذ نحو سنتين، والهجمات المعلوماتية.

وأكد ويلي والش أن الهجمات الإلكترونية هي من «المخاطر الناشئة» على الأمن الواجب مراقبتها بشكل نشط إلى جانب الطائرات بدون طيار والتهديدات الداخلية.

أبواب جديدة

ومع اعتماد قطاع الطيران تقنيات جديدة وتطويره خدمات عبر الإنترنت وعرضه خدمة الواي فاي على الركاب، تُفتح أبواب جديدة أمام القراصنة. ورأى عدة خبراء، رداً على أسئلة «وكالة فرانس برس»، من غير المرجح أن تتمكن جهة ما من التحكم بطائرة عن بعد، فالنظام المستخدم لقيادة الطائرة منفصل بشكل تام عن نظام التحكم بشاشات الركاب.

وحتى لو عانى هذا النظام خللاً، ترى كاتلين بايلي من شركة «فاير آي» للأمن الإلكتروني أنه «لا يشكل هدفاً جذاباً لمعظم الأطراف بسبب المستوى المطلوب من الخبرة وإمكانية الدخول إلى النظام، فضلاً عن مخاطر سقوط قتلى».

وأوضح بابلو إرناندیز، الباحث في معهد «إيناكسيس» المتخصص في بيانات الطيران، أن الخطر الأكبر قد يأتي من نظام التواصل بين الطيارين والمراقبين الجويين، وهو نظام غير مشفر، ما قد يجعل من السهل على القراصنة الدخول على الخط في حال توافر الجهاز اللاسلكي المناسب. لكنه أكد أنه يتم ضمان أمن الأجهزة الحساسة إذ يبقى أمن الرحلات الأولوية في مجال الطيران.

«الأنظمة «على الأرض

في المقابل، باتت الهجمات على الأنظمة «على الأرض» مثل أنظمة إدارة الحجوزات والأمتعة، أمراً شائعاً كما في 2020، حين تمكن قراصنة من اختراق البيانات الشخصية لحوالي تسعة ملايين راكب من زبائن شركة «إيزي جيت» البريطانية. وأحصت هيئة «يورو كونترول» لمراقبة الملاحة الجوية العام الماضي 1260 هجوماً استهدفت بشكل أساسي شركات الطيران إنما كذلك شركات البناء والمطارات والسلطات وغيرها.

ويقع العاملون في هذا القطاع في العالم الآن ضحية برامج فدية (رانسوموير) بمعدل عملية قرصنة في الأسبوع، فيُستهدفون ببرنامج خبيث يشفّر ملفاتهم فيمنعهم من الوصول إليها إلى أن يدفعوا فدية للقراصنة لإلغاء القفل عن النظام، تحت طائلة نشر البيانات المسروقة، على ما أوضحت الهيئة في مذكرة في مطلع يوليو / تموز.

مال وتجسس

أوضحت دانين ديفيوري رئيسة الأمن المعلوماتي في شركة «يونايتد إيرلاينز» للطيران أن المخاوف تتركز خصوصاً على هجوم إلكتروني «يبلبل العمليات». وأشارت إلى أنه «ليس هناك في الطيران وقت ميت»، فالطائرات تقلع وتهبط بدون توقف في العالم وأي عطل قد تترتب عنه سلسلة من العواقب المتتالية.

وتزداد هذه المخاطر في ظل التخلي تدريجياً عن تذاكر السفر الورقية والتقاسم المتزايد للبيانات مع مقدمي الخدمات، واستخدام المزيد من البرمجيات لإدارة الجداول الزمنية أو استهلاك الوقود بشكل أفضل. ويبدو أن القراصنة

المعلوماتيين يتحركون بغالبيتهم الكبرى بدافع كسب المال سواء من خلال قرصنة البيانات المصرفية أو إعادة بيع بيانات خاصة أو طلب فدية. لكن مع كمية المعلومات المتوافرة حول الركاب، بدءاً بأسمائهم وصولاً إلى سجلهم في السفر، لفتت كاتلين بايلي إلى أن بعض الدول قد تعمد إلى القيام بعمليات قرصنة.

وأوضحت ديفيوري أن مركز تقاسم المعلومات والتحليل الخاص بالأمن المعلوماتي في الطيران الذي أنشأ منذ 2014، يقدم مساعدة كبرى للشركات. ورأت أن الهجمات الإلكترونية تشكل واقعاً جديداً يتحتم على جميع الأطراف، من مسؤولي الأمن الجوي إلى فرق الصيانة، أخذه بالاعتبار. (أ ف ب)

"حقوق النشر محفوظة "لصحيفة الخليج .2024 ©