Nelli Sviili (nekasvii@student.jyu.fi)
13.2.2020

Etätyö 4: Kyberhyökkäyksen torjunta

Decision Document

We are in a situation, where cyber-attackers have targeted several airports in different countries. Office of the High Representative of the Union for Foreign Affair and Security Policy have noticed suspicious cyber-attacks in several airports in Europe. European Centre for Cyber Security in Aviation, ECCSA, confirms in their report that at least 10 different cyber-attacks (in US, France, Italy, UK, Germany, Poland, Turkey and Belgium) have been implemented since January 2020.

The report reveals that the cyber-attacks have been attacks against power grids, DDoS-attacks, hijacking information screens, drones in the airports airspaces, cyber-attacks on flight-planning computers, a networks connectivity issues, cyber-attack against the passport control systems, Eurocontrols critical servers takeover by hackers, and spreading a virus to the air traffic control systems.

Memorandum for the Director of EU Intelligence and situation Centre, EEAS, shows in their report that coordinated cyber-attacks against several airport operations systems have been blocked in London Heathrow, Frankfurt, Munich and Brussels airports. Also, media have been interested in some of these events. Cyber-attacks have caused harm and many threatening situations in the airports. So far, the damage has been only financial.

No-one has claimed for responsibility. EU Intelligence and Situation Centre believes that the group called Al Kala, which supports ISIS ideology, is behind the cyber-attacks. Also, there are rumours, that hacking groups sponsored by Mordor are behind the cyber-attacks.

This all should be investigated to determine their potential involvement in the cyber-attack. We should not exclude other possible cyber-attackers. As the EASA has stated in the latest cyber security review, *they* [cyber-attacks] *can be carried out from virtually anywhere and by anyone with sufficient knowledge, using low-budget methodologies.* If the expert team can find out who is behind the attacks, **the attacker must be held accountable** for their actions, **and the cyber-attacks must be stopped** as soon as possible. These investigations should be concealed from the media, that a potential cyber-attacker group does not find out too early that the investigators are after them. **Responsibility for investigating the cyber-attackers lies on the shoulders of the national security authorities in cooperation with Europol's European Cybercrime Centre, EC3.**

First and foremost, security organizations need to **update their policies** to reflect the current security situation in aviation, how to react for cyber-attacks. These **policies should be provided to all airports and staff should be trained to operate properly during the cyber-attacks**. Staff should be prepared to act correctly in all kind of cyber incidents, and they should be able to minimize disruption to air service and maintain the security for civil passengers and to the staff. **ECCSA would be logical author to contact all airports and update their policies with national aviation authorities.**

Secondly, **airports must be instructed to check their networks, softwires must be updated, firewalls and antivirus protections must be ensured**. **It is also necessary to check the possible network's backup systems. National authors can rely on ECCSA's expertise in maintaining IT systems.**

Air traffic has evolved in an era when flight data could not be accessed via networks. Even today, there are significant gaps in data security at airports and vulnerabilities in data systems. Flight data is particularly sensitive to phishing, manipulation and destruction. There are huge differences how to protect flight data in airports and in countries. It creates challenging environment to create one common and secure system for flight data, which would be available in all airports and all countries. Amount of data is likely to grow in the future.

It is reasonable to assume that one of the main functions of cyber-attacks is to stimulate fear in the deep rows of the nations. Fear-raising has been successfully used, for examples, in Eastern Ukraine during the Russian invasion of the Crimea. Cyber-attacks against air traffic have already caused fear among people. An impact of the fear on economical or national security level should not be underestimated. **The main European authors (included EU, Europol, ECCSA) should put together a press-institution, which would take responsibility for media visibility. Their main task would be to manage truthful communication to the media for supporting public safety and to correct fake news.** In the media all kind of criminal activity should be condemned.

At the national level, the focus must be on securing air passenger transport. **At the level of EU or NATO, the focus is on finding lasting political solution to the situation.** It is desirable but not expected that all states in EU and in NATO will support the work to prevent cyber-attacks on air traffic networks. The importance of bilateral relations between states should not be underestimated as a political tool. Common legislation condemning cybercrime should be developed at both EU and NATO level. The legislative process is challenging, and it will last for years if not decades. Even if the legislation process will not lead until the ratifiable law, it can prevent cybercrime by state actors.

At national, European and international level, research and development efforts should be made to reduce secure networks on aviation. Aviation data requires reliable and secure networks. Firewalls in all aviation related networks need to be strengthened and antivirus protection must be built stronger. Potential security threats to IoT devices, for examples drones, should be addressed, and all unnecessary access of IoT devices should be denied from all aviation networks. All aviation staff who is involved in their works with computers, should be trained to work safety of networks. **These activities will be organized at national level. ECCSA will act as a guiding and supporting body on the process.**