Cyprus Beef Up Hacking Defences as Attacks Show EU Vulnerabilities

Last December, a targeted hacking campaign - using tactics reportedly familiar to an elite unit of the Chinese People’s Liberation Army - compromised Cypriot digital networks, resulting in the leak of 1,100 European Union diplomatic cables. The attack exposed the fragility of cybersecurity within European Union networks and gave added weight to those in Cyprus who have warned of the threat of cyber-attacks, and have worked hard to build up the nation’s defences.

Ruairi Kavanagh  Feb 22 2019

The attack was a setback for those involved in Cypriot cyber-security, but the spotlight should more accurately be shone directly on the European Union in general, with the incident exposing the remarkably poor protection of routine exchanges amongst EU officials. The US company that exposed the leaks, Area 1, said in the New York Times that there “was nothing really sophisticated about the incident”, which pierced the EU’s diplomatic network and revealed opinions between all 28 nations, on everything from terrorism to Trump to Trade Tariffs, and much more.

EU Exposure

A spokesperson for the US National Security Agency said, in the same report, that the EU had been repeatedly warned that its almost obsolete communication system, was a prime target for a cyber-attack by states such as China, Russia, Iran, or other countries. The ‘wake-up’ call has seen EU officials grappling with new layers of security and secrecy, that they must now try to standardise across all 28-member states. Further criticism could be directed at Brussels for taking so long to do this, considering it is 12 years since the ‘cyber-war’ took place against an EU country, Estonia, in 2007. The crippling incident compromised Estonian banks, government agencies, businesses, broadcasters, and ministries.

That the 2018 attack happened to target European Diplomats based in Cyprus is unfortunate, considering that few nations have worked as hard as the island nation has, in recent years, to build up a cohesive strategy to deal with cyber-attacks and hacks.

Developing capabilities

In June last year, Cyprus unveiled its own national Computer Security Incident Response Team (CSIRT), dedicated to coordinating the response to cyber-attacks on critical information, infrastructure, and networks, in both the public and private sector. The Minister of Transport and Communication, Vasilliki Anastasiadou, said that the new agency would spearhead efforts to

https://www.southeusummit.com/europe/cyprus/cyprus-beefs-up-hacking-defences-as-attacks-show-eu-vulnerabilities/
deal with any digital intrusions. She added that important steps had been taken since 2013, such as engaging with the EU Agency for Network & Information Security (ENISA), and staging major conferences on the subject. This move to involve both public agencies, private business, and international experts, in coordinating the country’s readiness, culminated in the staging of the 14th annual International Conference on Terrorism and Electronic Mass Media in Limassol, last Winter. It included experts from Belgium, Italy, the UK, Israel, Romania, Saudi Arabia, Serbia, Spain, and France.

Prior to the event, the island’s head of electronic crime prevention, Mr. Andreas Anastasiades, said that Cyprus was adequately prepared to handle a major cyber-attack on its public or private networks, with Cypriot personnel now contributing to the counter cyber-effort, not just in the Republic, but elsewhere in the EU. The Union’s Agency for Law Enforcement Training (Cepol), has asked members of CSIRT to prepare a training programme for use in other countries on counter cyber-attack measures, Mr. Anastasiades explained. “This recognition is not accidental but is due to the constant upgrading of the office in all areas, and the results of its actions, as well as its ongoing cooperation with Europol,” he added.

In terms of digital usage, Cypriots are well-above average users of social media platforms, with Facebook being practically ubiquitous in the country, but they measure below the EU average when it comes to online financial transactions and online retail. Of course, it’s not just an individual’s money that can be targeted in a cyber-attack, it’s their personal data. The main cyber-threats, according to Anastasiades, are identity and password theft, malware, ransomware and encryption, but the threats are forever evolving, as, reassuringly, are the methods to counter them.

**Maritime Threats**

As an island nation with a rich seafaring and shipping tradition, Cyprus also views the threat of maritime cyber-attacks extremely seriously. The massive cyber-attack in June 2017, on one of the world’s largest shipping firms, AP Moller-Maersk, cost the company 300 million dollars, but a more serious attack could be far more damaging, according to Peter Sutcliffe of the CSO Alliance, an online community of shipping company security officers. “A worst-case scenario might involve intrusion that involves a cascade failure of a vessel carrying hazardous or polluting material, or possibly sustained disruption of networked navigational systems that could have an industry wide impact,” he said. Cypriot Deputy Shipping Minister, Natasa Pilides said, last November, that the Ministry was developing seafarer training courses in cyber-security at the country’s maritime training institutions. “We oversee the content and make sure it is approved and taught in the prescribed way,” she said, before adding that companies needed to provide their crews with the right training in this area. “There are a lot of legal issues, such as what constitutes evidence (of cyber-crime), that will be resolved with experience, and the International Maritime Organisation (IMO) will need to get more involved,” she added.

https://www.southeusummit.com/europe/cyprus/cyprus-beefs-up-hacking-defences-as-attacks-show-eu-vulnerabilities/