THE INTERNET OF THINGS: WHEN YOUR WASHING MACHINE AND BLOOD PRESSURE MONITOR BECOME A TARGET FOR CYBERATTACKS

19 Oct 2017

Press Release

Europol-ENISA conference tackles security challenges of IoT

With at least 20 billion devices expected to be connected to the internet by 2020, the Internet of Things (IoT) is here to stay. While it has many undeniable positive effects, the threats and risks related to the IoT are manifold and they evolve rapidly. For this reason, ENISA and Europol joined forces to tackle these security challenges by organising a dedicated two-day conference on 18 and 19 October 2017, which was attended by more than 250 participants from the private sector, security community, law enforcement, the European Computer Security Incident Response Teams (CSIRT) community and academia.

The Internet of Things is a wide and diverse ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. In simpler words, it makes our cameras, televisions, washing machines and heating systems ‘smart’ and creates new opportunities for the way we work, interact and communicate, and how devices react and adapt to us.

It is important to understand how these connected devices need to be secured and to develop and implement adequate security measures to protect the Internet of Things from cyber threats. Beyond technical measures, the adoption of IoT has raised many new legal, policy and regulatory challenges, broad and complex in scope. In order to address these challenges, cooperation across different sectors and among different stakeholders is essential.

The risk of criminals 'weaponising' insecure IoT devices was already identified in the 2014 and 2015 editions of Europol's Internet Organised Crime Threat Assessments and in ENISA's 2016 Threat Landscape Report. It became a reality at the end of 2016 with several DDoS attacks of unprecedented scale originating from the Mirai botnet. It must be assumed that cybercriminals will develop new variants and enlarge the variety of IoT devices affected by this type of malware.

This joint Europol-ENISA conference, the first one on the topic, provided the opportunity for all the relevant stakeholders to come together, discuss the challenges faced and identify possible solutions, building on existing initiatives and frameworks. A specific focus was on the role of law enforcement in responding to the criminal abuse of the IoT.

The two-day meeting was testimony to the willingness of all the relevant international actors to ensure that the many benefits of the IoT can be fully realised by jointly addressing the security challenges and combating the criminal abuse of such devices, ultimately making cyberspace a safer place for all.

The main conclusions of the conference are:

- The need for more cooperation and multi-stakeholder engagement to address interoperability, as well as security and safety issues especially in light of emerging developments like industry 4.0, autonomous vehicles, and the advent of 5G.
- As securing the end device is often technically difficult and expensive to achieve, the focus should therefore be on securing the architecture and underlying infrastructure, creating trust and security across different networks and domains.
- There is a need to create stronger incentives to address the security issues related to the IoT. This requires achieving an optimal balance between opportunity and risk in a market where high scalability and short time-to-market dominate, positioning security as a distinctive commercial advantage and putting it at the heart of the design and development process.
- To effectively and efficiently investigate the criminal abuse of the IoT, deterrence is another dimension that needs strong cooperation between law enforcement, the CSIRT community, the security community as well as the judiciary.
- This creates an urgent need for law enforcement to develop the technical skills and expertise to fight IoT-related cybercrime successfully.
- These efforts need to be complemented by raising end users' awareness of the security risks of IoT devices.
- Leveraging existing initiatives and frameworks, a multi-pronged approach combining and complementing actions at legislation, regulation and policy, standardisation, certification/labelling and technical level is required to secure the IoT ecosystem.
- One of the key observations of the conference is the importance of baseline good practices in addressing these IoT security challenges. In the coming months ENISA will publish its "Baseline Security Recommendations for IoT" report, bridging the gap in the area.

Europol's Executive Director Rob Wainwright commented: "Cybercriminals are quick to adapt to and exploit new technologies. They come up with new ways to victimise and affect people's lives and invade their privacy, either by collecting or manipulating personal data or by virtually breaking into smart homes. The Internet of Things is not only here to stay but expected to significantly expand as more and more households, cities and industries become connected. Insecure IoT devices are increasingly becoming tools for conducting cyber criminality. We need to act now and work together to solve the security challenges that come with the IoT and to ensure the full potential."

ENISA's Executive Director Professor Dr Udo Helmbrecht also commented: "The IoT revolution is beginning to transform our personal lives and the infrastructures that we use on a regular basis such as smart homes, smart energy and smart health. Manufacturers and operators of these devices need to ensure that security by design has been incorporated into their selection and their deployment. ENISA is pleased to be working closely with Europol to inform key stakeholders of the

important role that the IoT is taking on and the need to be aware of the cybersecurity and criminal aspects associated with deploying and using these devices".

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES	European Cybercrime Center (EC3)
ORGANISATIONS	European Union Agency for Network and Information Security (ENISA)

Source URL: https://www.europol.europa.eu/newsroom/news/internet-of-things-when-your-washing-machine-and-blood-pressure-monitor-become-target-for-cyberattacks