IF YOUR TOOTHBRUSH CALLS YOU, IT MIGHT NOT BE FOR DENTAL HYGIENE: THE IMPORTANCE OF SECURING THE INTERNET OF THINGS

25Oct2018

Press Release

Second Europol-ENISA conference tackles security challenges of IoT

INTERNET OF THINGS SECURITY CONFERENCE

Europol - ENISA 24-25 October 2018

Our world is hyper-connected now. Current estimates are that there are around 10 billion electronic devices with access to the internet and that number will have at least doubled by 2020. In addition to the many advantages and opportunities, the emerging ability of connected devices to impact the physical world has also created a new set of vulnerabilities and possibilities of exploitation by criminals. To address these vulnerabilities, tackle them effectively and to fully realise the great potential that it offers, ENISA and Europol have brought together 300 experts from the private sector, security community, law enforcement, the European Computer Security Incident Response Teams (CSIRTs) community and academia for a two-day conference in The Hague.

The Internet of Things (IoT) is a wide and diverse ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context, automate decisions and provide better situation awareness. In simpler words, it makes our televisions, bathroom scales, fridges and even our cars and cities 'smart' and creates new opportunities for the way we work, interact and communicate, and how devices react and adapt to us. IoT has added to our overall convenience, ease of use and even safety but it is important to implement adequate security measures to protect the IoT from cyber threats. What will happen when cheap and unprotected IoT devices allow criminals to watch your every move from your vacuum cleaner's camera, change the settings of your connected medical device or drive your car into a wall?

These challenges – whether technical, legal, policy or regulatory – need to be addressed across different sectors and stakeholders. For the second year in a row, ENISA and Europol joined forces to gather the world's leading experts from the private sector and law enforcement and cybersecurity community to discuss the security challenges around Industry 4.0, IoT application domains and concrete case studies in the automotive, aerospace and smart home industry and emerging IoT trends like artificial intelligence and digital forensics.

The second IoT Security Conference provides a unique platform for experts to provide the audience with insights into the security requirements of IoT, a mapping of relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems and to deliver the many opportunities IoT offers in a safe and privacy-respecting manner.

THE MAIN CONCLUSIONS OF THE CONFERENCE ARE:

- security should not be an afterthought when designing systems and IoT systems are no exception;
- implementing security does not need to be complicated. As ENISA's report shows, baseline security recommendations for IoT were made accessible via an interactive online table. This allows for easy access to specific good practices;
- law enforcement needs to be in a position to go beyond defence and incident response by being able to investigate and prosecute the criminals abusing connected devices;
- there is a need to discuss digital forensics in regard to IoT and the importance of data and privacy protection, considering the amount and different categories of data collected by the IoT;
- this joint conference is an excellent example of much-needed multi-disciplinary dialogues. ENISA and Europol are working closely together to inform key stakeholders of the need to be aware of the cybersecurity and criminal aspects associated with deploying and using these devices;
- the IoT has great potential and provides tremendous opportunities to improve the way we interact, do business and go about our daily lives.
- In 2019 and beyond, holistic, pragmatic, practical and economically viable security solutions need to be promoted and the entire IoT ecosystem needs to be looked into. ENISA will be working on an automotive IoT case study and welcomes the active support of all partners. Cybersecurity is a shared responsibility. Stronger collaborations with industry are planned together with other initiatives to ensure coordinated efforts and explore all possible synergies.

ENISA's Head of Core Operations Department, Steve Purser commented: "It is important and essential to collaborate because cybersecurity is a shared responsibility and that is ever more true in the IoT domain. This joint conference is an excellent example of these much-needed multi-disciplinary dialogues. The benefits and opportunities that IoT brings are numerous and of paramount significance for the entire society. It is our duty to ensure that this is done in a secure, safe and reliable manner. IoT security is a prerequisite for a secure and safe connected digital society. The time to act for Internet of Things security is now. I welcome the collaboration with Europol, and I am confident that such joint efforts contributing to ensuring IoT security for all."

Europol’s Deputy Executive Director of Operations, Wil van Gemert added: "Law enforcement must have the tools, skills and expertise to investigate the criminal abuse of the IoT. We have a leading role, together with our partners, to go beyond increasing cyber security and resilience of the IoT as we can make a specific contribution in terms of deterrence. The complexity of IoT and its resulting cybersecurity challenges call for a holistic, smart and agile approach. As IoT is now a present reality as opposed to a futuristic concept, the necessity to have this multi-stakeholder conference to put cybersecurity at the heart of the IoT ecosystem is self-evident."

Useful tool for law enforcement use

The Internet of Things has many advantages for law enforcement as a new tool to fight crime. Police are already using connected devices like smart cameras for major events and to fight robberies and home burglaries, bodycams to raise situational awareness, sensors in firearms to track when and how often it is used, and so on. It is important that law enforcement also invest in the safety and security of its IoT-connected devices, to protect the privacy of the citizens it works for.

Crime scenes are changing because of the IoT: data from connected doorbells, cameras, thermostats, fridges, etc. can provide useful and crucial evidence. The necessary forensic techniques and training will need to be used to safeguard this data. Big data collected by IoT devices, for example for facial recognition from camera images after a major incident, will become an integral part of a criminal investigation but also require the necessary means to protect the privacy of citizens.

Common understanding of IoT cyber security

ENISA has been working for several years on identifying security threats and risks in the Internet of Things and on providing recommendations to strengthen its security. To address the challenges and lay the foundation for IoT security, ENISA has introduced Baseline Security Recommendations for IoT, to ensure common understanding and interoperability when it comes to IoT cyber security.

Device manufacturers and users of IoT devices and systems can use these recommendations as a checklist against which to assess their IoT security solutions. For this reason, an interactive online tool has also been developed that can be used to define one's own threat model and accordingly identify specific security measures to deter, protect and prevent pertinent threats.

Building on this work, ENISA continues to engage with stakeholders and will publish a new study in 2018 on Good Practices for Security of IoT with a focus on Industry 4.0 and smart manufacturing, while in 2019 relevant efforts concerning smart cars are expected.

CRIME AREAS Cybercrime • High-Tech crime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

Source URL: https://www.europol.europa.eu/newsroom/news/if-your-toothbrush-calls-you-it-might-not-be-for-dental-hygiene-importance-of-securing-internet-of-things