The Hague, 05/02/2018

EDOC# 945887

Cyber security must be approached from a holistic perspective

As the importance of cyber security continues to grow, so does the necessity to identify the steps different societal actors can take to promote a more secure cyberspace. While security is never absolute, we can reduce the probability of a successful attack, as well as reduce the potential for damage. To achieve this, we must approach security from a holistic perspective. This includes efforts focused on prevention and awareness, detection and mitigation, as well as activities ensuring that law enforcement and public safety agencies have the ability to disrupt, attribute, and investigate unlawful activity online. This holistic approach to security includes the essential aspect of cyber resilience, which accepts that attacks can and will take place, but allows individuals and organisations to recover from such incidents. The implementation of the cyber security breach notification as of 1 January 2018 in the Netherlands is a crucial element in this approach, as it provides the National Cyber Security Centre (NCSC) with the ability to carry out a risk assessment to determine the need for assistance, as well as to warn users. At the European Union (EU) level, the introduction of a Blueprint for a coordinated response to large-scale cross-border cybersecurity incidents and crises also bears mentioning, since this Blueprint focuses on how to respond to a cybersecurity crisis. As Europol, we are supporting the implementation of the Blueprint by contributing the law enforcement perspective and expertise in providing emergency response to major cyber incidents of suspected criminal nature, and we are drawing upon our operational hands-on experiences and the needs communicated to us by the EU cyber law enforcement community.

Cyber security requires international coordination and cooperation

The cross-border nature of cybercrime requires an overarching entity which can facilitate in connecting all the dots to investigate and arrest individuals, as well as to take down or otherwise destruct their infrastructure. Within the cybersecurity ecosystem, the European Cybercrime Centre (EC3) fulfils by its very nature a unique role in the fight against cybercrime. Through its ability to act as a coordinating and supporting platform, EC3 brings both people and information together to enable the Member States in cooperation with various partners to carry out critical operations. Many of the EC3 operations demonstrate how our public and private partnerships allow for exchange of information with the intent of identifying threats and perpetrators. With respect to the identification of threats, EC3 brings together the knowledge gathered from law enforcement agencies across the EU as well as private partners, and shares it through its annual Internet Organised Crime Threat Assessment (IOCTA), which also aims to look ahead at future developments influencing the cybersecurity realm.

Governments must enable law enforcement to conduct investigations

As a linking pin, EC3 is also in a position to identify challenges law enforcement officials face with respect to cybercrime investigations. One of these challenges deserves emphasis here, especially as we reflect on the role of governments and legislation in promoting a more secure cyberspace. The ruling by the European Court of Justice (ECJ) with respect to the ability of Member States to retain data has complicated and in some cases made investigations impossible. In the absence of forensic evidence or eye witness testimonies, the electronic data retained is often the only available tool or potential evidence to initiate and conduct an investigation, both at national and cross-border level. If we accept that security also requires the identification and attribution of perpetrators as well as the destruction of their infrastructure, law enforcement must be able to carry out its investigations to enhance the cybersecurity of all users. As discussions on the issue of data retention

continue at the national and European level, we wish to take this opportunity to emphasise the importance of such access for law enforcement and more particularly public safety purposes. If data retention to ensure public security was defined as a specific purpose in suitable legislation – taking into account proportionality and necessity – it could be implemented in a manner living up to the jurisprudence of the ECJ. For this purpose, based on the criteria established by the ECJ, Europol developed a concept of 'restricted data retention and targeted data access.' This would take into account both the necessity on the side of law enforcement to have access to the data and the proportionality aspect of limiting such access to specific data for particular purposes. Hereby, data retention legislation compliant with both the right to privacy and the right to security would be provided.

Private sector participation is essential for a coherent response against cybercrime

While different societal actors play distinct roles in the cybersecurity ecosystem, cooperation between these different groups remains crucial; since each actor may have a different piece of the puzzle. Many of the operations coordinated and supported by Europol demonstrate how the knowledge, experience and information held by a variety of public and private parties are indispensable to engage in the successful disruption of criminal processes. For example, reflecting on the efforts of last year, the European Money Mule Action (EMMA) week – which had its third iteration in 2017 – brought together the information from the financial services sector as well as law enforcement. Europol, along with Eurojust, provided a coordinating role to facilitate the real-time cross-checks against Europol's databases of the data gathered during the actions, and intelligence gathering for further analysis, as well as swift forwarding and facilitation of the execution of European Investigation Orders. Other efforts include No More Ransom (NMR). This public private cooperative project was launched on 25 July 2016 with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals. Through NMR, law enforcement and IT Security companies have joined forces to disrupt cybercriminal businesses with ransomware connections. Therefore, public and private partners must be in a position and willing to share information as a means to enhance security. This requires willingness on the side of the partners and enablement on the side of governments to draft legislation which facilitates fruitful information exchange.

Prevention and awareness can assist citizens in their security efforts

Since Europol recognises that prevention and awareness also play an important role in the overall approach to cybersecurity, we introduce prevention and awareness campaigns whenever we identify an opportunity related to our operations. Examples of such initiatives are the previously described EMMA week. As part of the action week, Europol coordinated a campaign that aims to inform the public about how these criminals operate, how they can protect themselves and what to do if they become a victim. The above described NMR project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. Targeting perpetrators of crime garners media attention which we use as a vehicle to bring about a broader message in the hopes of making individuals aware of how they can take steps to better protect their data and devices.