Editorial

Digitalization and Cyber Crime – "Opportunity Makes the Thief"

Joachim Wuermeling

Professor Joachim Wuermeling
Member of the Executive Board
Deutsche Bundesbank
and Chairman of the Council
of the E-Finance Lab

More Digitalization Means More Data and More Systems

In the age of the Internet of Things, computers deal with more than just abstract data, they are increasingly reaching out into the real world of physical objects. This digitalization trend means that everyday electronic appliances are increasingly being transformed into interlinked IT systems – such as the networked home. More systems, more data – the number of IT systems is increasing at breakneck speed, including at central banks. Of course, this also raises the question of whether they are sufficiently secure.

More Data, More Damage

The increasing digitalization of essential tasks means that even data that was formerly unavailable in an electronic format can now be collected, stored and evaluated. However, more data, possibly of a sensitive nature, also means that the potential for damage is greater in case of loss. Current figures show that the risk of harm has increased substantially. The WannaCry attack in May 2017 confirmed this hypothesis and demonstrated that critical infrastructures such as hospitals, too, are vulnerable.

More Systems, More Weak Points

The greater the number of IT systems in use worldwide and the more interlinked they are, the higher the number of potential victims and possible weak points. Identifying these weak points, assessing their potential harm, and rectifying them in a timely manner represents an immense challenge for manufacturers and users alike.

More Weak Points, More Attacks

Any system with weak points can be targeted by attackers and/or be exploited as a means of attack. Organized crime has established new business models in this field. This is demonstrated by the increasing number of malware attacks, in which malicious software (known as ransomware) encrypts the victim's data and promises to decrypt them again in return for payment. As the number of victims increases, cyber criminals are able to further expand their network of botnets, computers they control, and use to carry out cyber-attacks. In the age of the Internet of Things, where every household – and, in some cases, every household member – has multiple connected devices, it is only a matter of time before everyone has been attacked or weaponized.

More Attacks, More Security

Manufacturers must ensure that their products are more inherently secure, particularly in the Internet of Things. This necessitates a commitment to uniform security standards and the principle of "secure by default". Even today, ensuring heightened security poses an immense challenge. This statement is also valid for central banks as part of the critical infrastructures. In a world of growing numbers of IT systems and ever shorter product cycles, it will become a critical issue. Yet, this is not solely a matter for the manufacturers. Private and business users alike also need to develop a sense of increased responsibility for keeping digital infrastructures and their sensitive data secure.

More Security, More Trust

In my view, efforts to manage the risks stemming from cyber crime are still in their infancy and must be improved, e.g., through mandatory security designs. Forcing "critical" security configurations to be remedied and patches applied as soon as flaws are found would reduce the potential for zero-day exploits such as the WannaCry case. There may also be further ways for governments to promote cyber security as a public good.

Electronic "things" embrace more and more real-world physical objects. We therefore need more secure systems from trustworthy manufacturers plus users who are more security-conscious. This is an absolute must if the challenge of "digitalization" is to be successfully met.