Prof. Dr. Michael Backes

Director of the Center for IT-Security, Privacy, and Accountability (CISPA)

Professor, Chair of Information Security & Cryptography, Saarland University

What are the most common types of cybercrimes?

If we leave out all criminal activities that are both online and offline like fraud, the trade of illegal goods and harassment, then the most common type of cybercrime is the creation and spread of malware to steal sensitive information or for financial gain, e.g. ransomware, banking Trojans as well as denial of service attacks. Most of these attacks exploit common vulnerabilities in old systems, software or protocols. This is why it is crucial for companies and consumers to keep their systems updated, keep regular back-ups and to exercise a healthy suspicion of unexpected emails and new websites.

In recent years there has been a dramatic increase in cases of more sophisticated as well as targeted system and network intrusions. These attacks oftentimes specifically target vital infrastructures like energy and financial networks, large corporations, or government agencies. The attackers do this by exploiting new, unknown IT vulnerabilities and getting access to a network through tailored social engineering, which is known as spear-phishing.

What do large organizations need to learn from cyber security research to better protect themselves against cybercrimes?

Although large organizations are now better equipped for IT security in regard to personnel and financial resources, successful hacks and data theft are reported almost on a daily basis. One of the main reasons is that even large organizations consider IT security as an afterthought during product and network design. Security is often considered to be of secondary importance in comparison to convenience, feature-richness, time and budget constraints. In order to be effective, IT security has to be a primary goal of the design process right from the beginning. Systems and products need to follow the security-by-design principle.

Another factor is that several large organizations try to re-invent the wheel by building their own custom security and cryptography solutions instead of relying on well-established paradigms that have been field tested and verified through decades of security research. Organizations tend to deviate from the established

standards in order to have an advantage over their competitors, which instead is far less secure than the state of the art.

It is crucial for both research and commercial organizations to focus more on the usability of security solutions. For many security issues like confidential and authenticated email communication, we already have technical solutions. The only reason these are not widely used is the lack of convenience and usability.

What are some of the steps Germany has taken to increase individual privacy and data protection, and what still needs to be improved?

Germany has one of the most comprehensive legal frameworks for data protection in the world. In Germany and the entire European Union, privacy is a basic human right protected by the constitution and the EU Charter of Fundamental Rights. The German data protection law requires that a Data Protection Officer in every organization reviews and advises on all processing of personal data for compliance. In May 2018, the General Data Protection Regulation (GDPR) for the entire EU will come into force. The GDPR will apply to every international company that targets EU customers and for the first time it enables courts and data protection authorities to impose fines that are perceptible even by large international corporations. Additionally, the GDPR requires companies and their products to adhere to the principles of privacy-by-design and privacy-by-default.

The enforcement of these legal requirements needs to be improved. Most European data protection authorities do not have enough personnel in general and IT experts specifically to exercise their oversight in a meaningful way. For privacy-by-design clear guidelines, standards, and best-practices for companies do not exist.

Please describe your recent research project imPACT and how it will affect the Internet of the Future.

Today's Internet is in a deep crisis of confidence due to the high costs of cybercrime together with the hard-to-quantify costs of privacy loss and loss of trust in content and providers. Users unknowingly reveal sensitive personal information and are tracked and profiled by providers without noticing. In addition, they may trust false or distorted content, and get manipulated by other users.

The imPACT project started in 2015. It addresses the key challenges of providing Privacy, Accountability, Compliance, and Trust (PACT) in tomorrow's Internet. My colleagues, Peter Druschel, Rupak Majumdar, Gerhard Weikum, and I received the Synergy Grant from the European Research Council for our idea to conduct joint synergistic research on privacy and security, distributed systems, formal methods, program analysis, database systems, and knowledge management.

We use a cross-disciplinary approach to understand and master the different roles, interactions, and relationships of users and their joint effect on the four PACT properties. The focus is on creating new and better building blocks to guarantee the four PACT properties in future Internet applications. The foundational work will be accompanied by software prototyping and field-trial experiments for testing new user-centric tools that technically safeguard and enforce the needs of individual Internet users.

What are the primary goals and activities of the joint CISPA-Stanford Center for Cybersecurity?

The CISPA-Stanford Center for Cybersecurity is a joint center for cybersecurity research between CISPA and Stanford University. It is funded by the German Ministry for Education and Research. This collaboration between two of the strongest sites for cybersecurity research worldwide has two goals. The first goal is to establish a joint transatlantic research program through synergistically combining our competencies in various fields of cybersecurity research. The second goal is to establish a joint career program for outstanding young researchers to alleviate the shortage of qualified faculty and scientists in IT security.

The center fosters the professional development of a small number of selected, outstanding individuals. It provides them the opportunity to work independently on their own research ideas at Stanford University as Visiting Assistant Professors in the area of cybersecurity for two years and to then return to Germany to continue their research as a senior researcher at CISPA. The ultimate goal is for them to become a professor at a German university or a research leader in an industrial setting.