TechXplore

Personal data, fodder for cyberwarfare? New models for stepping up cybersecurity

February 8 2021

Credit: CC0 Public Domain

In today's increasingly digital world, cybersecurity is paramount. The upsurge in cyberattacks has far-reaching effects, from jeopardizing users' private data to sparking all out cyberwar, not to mention threatening private businesses' intellectual property. In such volatile times, the only approach is to adopt new models and applications that can address these problems efficiently.

More awake to this issue than most, Regner Sabillon, a doctoral student at the Universitat Oberta de Catalunya (UOC), dissects these models in his thesis, Digital Forensics Assessment, Cyberlaw Review and Cybercrime Analysis to Enforce Cybersecurity. The Importance of Cybersecurity Audits, Assurance, Awareness and Training, which benefited from co-supervision by professors and researchers Jordi Serra from the Faculty of Computer Science, Multimedia and Telecommunications and Víctor Cavaller from the Faculty of Information and Communication Sciences. The research breaks down multiple case studies and highlights the importance of taking appropriate measures to shield data against cyberattacks. Sabillon's academic undertaking has now been reworked into a book titled Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM, which has been named the best new cybersecurity book to read in 2021 by United States website BookAuthority.

The book underscores the need to upgrade security models to ward off the increasingly sophisticated cyberattacks waged against anyone from top-tier institutions to ordinary citizens, with businesses and government agencies also caught in the crossfire. Cavaller explained that the research involved an "extensive review of cybersecurity systems that are being implemented worldwide in different organizations" and that the book "proposes Audit and Awareness Training models that are extremely useful and that have been successfully applied in several institutions with results that have radically improved the capacity of computer protection." "This research provides an opportunity to get to know the levels of maturity of cybersecurity at companies and institutions. It is a great starting point for improving these levels, as shown by the ongoing work that has been published in research articles," said Serra.

Sabillon, a professor at the School of Computing and Information Systems and the Faculty of Business at Canada's Athabasca University, and an ICT and cybersecurity consultant, uses his book as a platform to shed light on prevailing issues in this domain. According to the academic, who is currently working towards his doctoral degree in Network and Information Technologies at the UOC, current issues include "stealing individuals' personal or sensitive data, and even tampering with companies' intellectual property. Cybercriminals are continuously modernizing and sophisticating their attacks."

Cyberwarfare, a very real problem

As our day-to-day lives spill further into the digital world, the risk of cyberattacks grows. Although this trend comes as no surprise, the world has not necessarily readied itself for battle. Indeed, according to ISACA's State of Cybersecurity 2020 report, 32% of respondents agreed that attacks had risen considerably in 2020. Our expert said: "The most common [attacks] are those based on social engineering, advanced persistent threats and ransomware attacks, where systems are ransomed using software that encrypts data, thus blocking their use, in order to extort the owner."

Private companies are not the only ones left scathed. Weak cybersecurity puts government organizations, associations, other types of entity and individuals at risk. Among the most worrying are large-scale attacks waged against countries and major administrative interests. According to the doctoral student, "This is what we're seeing today between world powers such as the United States, China and Russia." He added: "There are many such cases, but there is still no consensus regarding what we might call cyberwarfare, even though the 'cyber' domain has been recognized as the most novel part of otherwise conventional warfare."

To illustrate his point, the expert brought up the cyberattacks allegedly launched by Russia as a deterrent against countries such as Georgia and Ukraine, which have sometimes triggered military action. The digital environment is all around us and advancing at a rapid pace. As a result, cybercriminals are able to switch up their attacks daily, exploiting the vulnerabilities they detect between program updates. Faced with this, said Sabillon, we need new models and measures that effectively tackle the problem.

Innovative solutions and awareness training

In his research, Sabillon explored a number of case studies where the cybersecurity audit model (CSAM) and the cybersecurity awareness training model (CATRAM) were developed and validated. The doctoral student analysed their deployment and ability to bolster and audit national cybersecurity strategies, extensively covering a wide range of issues such as forensic analysis, digital evidence and incident management and thus offering in-depth insight into the latest research on models in cybersecurity management and awareness training.

Sabillon said: "The cybersecurity audit, or CSAM, is an innovative and comprehensive model that offers optimal assessment of cybersecurity in any organization, and can verify specific guidelines for countries planning to launch a new cybersecurity strategy or policy, or wishing to test the effectiveness of those already in place." The CSAM, he said, enables the performance of both internal and external cybersecurity audits: "Any entity has the option of performing a full audit of all cybersecurity domains or of simply selecting specific ones in order to audit certain areas that need oversight verification and reinforcement."

Meanwhile, the cybersecurity awareness training model, or CATRAM, was designed to offer initial training in any organization. According to Sabillon, "It also serves to roll out better approaches to existing cybersecurity awareness training or specific data security training programmes."

Today, there are countries that have thorough, elaborate national cybersecurity strategies in place. However, as Sabillon lamented, many others, especially developing countries, continue to downplay the importance of the matter. He said: "Leading countries generally allocate many resources to their national strategies. These include the United States, the Netherlands, the United Kingdom, Australia, Canada, Singapore, Malaysia, and the European Union, through ENISA." Implementing models such as CSAM and CATRAM, said the UOC doctoral student, is a good starting point for both mending deficient strategies and improving those already in place.

More information: Regner Sabillon. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM, (2020). DOI: 10.4018/978-1-7998-4162-3

Provided by Universitat Oberta de Catalunya

Citation: Personal data, fodder for cyberwarfare? New models for stepping up cybersecurity (2021, February 8) retrieved 7 May 2024 from https://techxplore.com/news/2021-02-personal-fodder-cyberwarfare-cybersecurity.html