SHARE:

Join Our Email List

The KIT

Knowledge & Information Technology

cébé
IT & Knowledge Management

No. 294 - 16 August 2021

In this Issue

Our Consulting Services

IT Strategy and Roadmap
Enterprise Architecture
Business Process Modeling
Enterprise Software Selection
IT Innovation Briefings
IT Due Diligence for M&A
Cloud Computing Adoption
Enterprise Security Maturity
Knowledge Management
Communities of Practice
Taxonomy Development
Enterprise Social Media Adoption

European Union Security Landscape News

European Union institutions make up an alphabet soup of commissions, centers, regulations and projects. A recent document on 5G security is an opportunity to describe some of this landscape.

ENISA is the European Network and Information Security Agency. It supports member states and other institutions as they implement the Network and Information Systems (NIS) Directive.

In June 2021, the European Cybersecurity Competence Center (ECCC) was established. It will be based in Bucharest, Romania.

To make things more confusing, there is a thing called the European Electronic Communications Code (EECC). A recently published supplement to the EECC technology-neutral Guideline on Security Measures specifically concerns 5G

For more information

Visit us: www.cebe-itkm.com
E-mail us: info@cebe-itkm.com
Phone: +1 415 870 4856
+33 970 444 992
Twitter: @cbaudoin
See: Previous KIT issues

Forward this issue to colleagues and friends!

network security. The goal is to guide "competent national authorities" on how to ensure that mobile operators implement or strengthen security measures for 5G networks.

Both industrial and consumer-oriented IoT plan to rely on 5G networks to expand coverage and increase bandwidth to the Internet.

Digital Twins of Buildings

Environmental concerns are creating a demand for modeling the energy consumption of buildings (see KIT No. 285, for example, or articles in the CABA Newsbrief). The U.S. Department of Energy is following this direction on a grand scale: its Oak Ridge National Lab (ORNL) is planning to create, over the next five years, digital twins showing the energy use of all 129 million buildings in the country. Their software, AutoBEM (BEM = Building Energy Modeling) uses publicly available data such as satellite imagery, street views, number of windows, wall and roof materials, number of floors, and types of HVAC systems. The project uses supercomputing resources from the Argonne National Laboratory in Illinois.

LinkedIn Profiles for Sale

A month ago, 600 million profiles scraped from LinkedIn were offered for sale on a hacker forum. According to this ambiguously worded article from TechRepublic, this leak only contains publicly available information that may be in violation of LinkedIn's terms of service, but does not constitute an illegal breach. However, the article says that the scraped data contains e-mail addresses, which by default are not visible to people who are not direct connections of a member. If the hackers found a way to circumvent this setting, then the leak would certainly amount to a privacy violation.

This is the third time in four months, according to CyberNews, that millions of LinkedIn profiles are collected and published. LinkedIn is toeing a fine line in the first place: they monetize access to profiles and the ability to contact other members through their paid premium subscriptions, while making it difficult to collect information if you are not a premium member. And various services (such as PhantomBuster) allow you to run scripts to scrape the public content of profiles, while flying under LinkedIn's radar by limiting the number of results -- something that can fairly easily be circumvented by adding search filters (give me all the As, then give me all the Bs, etc.).

Universal Vulnerability Identifier

The Cloud Security Alliance (CSA) has stood up a new Universal Vulnerabiilty Identifier Working Group, whose purpose is to organize the "discovery, reporting, publication, tracking and classification" of technology vulnerabilities, because "the number of vulnerabilities is growing faster than we are currently able to track them."

New Toolkit to Help Organizations Using AI

The United Kingdom's Information Commissioner Office (ICO) has published a beta version of a new AI and Data Protection Risk Toolkit. Its goal is to help organizations comply with data protection regulations when they use AI to process personal data.

Seen Recently...

"The large army of the good guys is led by hapless, incompetent, unmotivated bureaucrats with meaningless certifications in this or that, consumed by building an audit trail showing that they've followed the ever-growing body of useless regulations so that when the nearly-inevitable security disaster happens, they can prove it wasn't their fault."

-- David Black, "recovering programmer," in a Forbes Magazine article entitled "Cyber-Security: Here's Why the Bad Guys Are Winning"

"I figured out how to articulate why I think that telework is not the future... When we stop using all of our senses to communicate with each other, we stop being living beings.."

-- Jenny Fristrup (in personal correspondence)