SHARE:

Join Our Email List

The KIT

Knowledge & Information Technology

cébé
IT & Knowledge Management

No. 293 - 2 August 2021

In this Issue

- Data Protection News
- Top 100 Cybersecurity Companies
- AI and IoT in Healthcare
- Vulnerability Found in PLCs
- Non-News of the Week

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

For more information

ERRATUM: The title of issue no. 292 showed a date of July 1 instead of July 16. Apologies!

Data Protection News

The POPI Act (Protection Of Personal Information) came into effect in South Africa on July 1st. Ironically, we were informed of this by a South African company, AMC International, which had spammed a non-existent address in the cebe-itkm domain and was sending us a notice of our right to unsubscribe. POPIA was signed into law in 2013 but did not take effect until July 1, 2020, with a one-year grace period to achieve full compliance. POPIA and similar acts have been called "children of GDPR" because they generally follow the principles of the European Union's General Data Protection Regulation.

Speaking of which, the Luxembourg National Commission for Data Protection has determined that Amazon's processing of personal data did not comply with GDPR; it has issued a fine of €746 million (about $880 million) and a demand that the company revise certain business practices. Amazon intends to appeal (source: CNBC). Under GDPR, enforcement is the responsibility of the individual EU countries' data protection agencies and fines can be as much as 4% of revenue.

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!

Top 100 Cybersecurity Companies

ASD has published one of its famously comprehensive -- and super-expensive -- marketing reports, this one about the cybersecurity industry. If you are the CISO of a large company looking for a strategic provider, or a company in this domain trying to learn about your competitors or potential partners, you may want to pay the $5,400 for a single-user copy or $9,450 for an enterprise-wide copy. The report includes 100 company profiles as well market and revenue projections up to 2031.

AI and IoT in Healthcare

The Industrial Internet Consortium (IIC) recently approved a new "test drive" for gait analysis. IIC test drives are "short-term rapid-engagement pilots for technology end users to employ and adopt IoT technologies" and stimulate IoT adoption in industry.
This test drive, led by Shinshu University and Toyo Company of Japan uses sensors and cameras to collect data on how an elderly person walks, allowing the pre-symptomatic diagnosis of certain geriatric diseases and improving the prevention of falls.
It is not clear how the project will leverage work done years ago on gait analysis, in particular at the MIT Media Lab under Prof. Hugh Herr, where a project called "Wearable Wireless Sensors for Gait Analysis" was active from 2000 to 2003. Let's hope that the new test drive does not reinvent the wheel.

Vulnerability Found in Programmable Logic Controllers

We (and others) often point out that industrial IoT systems, which use general-purpose operating systems and communication protocols and are connected to the Internet, are therefore more prone to attacks than older, proprietary, isolated SCADA (Supervisory Control and Data Acquisition) systems. But older technology is not immune to cybersecurity problems. This was famously demonstrated when Iranian enrichment centrifuges were apparently damaged in 2009-2010 by the StuxNet worm, designed specifically to target programmable logic controllers (PLCs) and allegedly developed jointly by US and Israeli intelligence services.
History can repeat itself, and a July 12 article in TechRepublic is headlined "Vulnerability in Schneider Electric PLCs allows for undetectable remote takeover." The vulnerability, discovered by security research firm Armis, "affects a wide variety of Modicon [PLCs] used in manufacturing, utilities, automation and other roles."
It should be noted that vulnerability does not always imply exploit. Certain steps taken when integrating a device or a piece of software into a system may make it impossible to exploit the weakness. The article lists some recommendations by Armis, with which Schneider is cooperating to mitigate the issue.

Non-News of the Week

The KIT occasionally pokes fun at people who, as the French say, "break down an unlocked door" by painstakingly making an obvious point. This week's medal in this category goes to Accenture, cited by TechRepublic under the title *"Thinking of the cloud as a cost-saving tool puts businesses at a disadvantage, Accenture finds."* Somewhat more usefully, but still short on originality, the article continues: *"The most successful companies consider cloud technology a continuum of tools for strategizing and transforming business practices, a study of leaders suggests."*

Seen Recently...

"If software engineers built bridges, 50% of them would fall down, 20% of them would explode because they managed to work C4 into the design, 20% would explore despite having no combustible material in them whatsoever, and the remaining 10% would actually work well."

-- Arstechnica, cited by Lou Mazzucchelli in a Facebook post

"Part of the problem is that 'engineering' is to software as 'fish' is to bicycle."

-- The same Lou Mazzucchelli, at the end of a series of comments on that post