C VISION INTERNATIONAL

AGENDA

The Future of IT & Cybersecurity

CIO & CISO Think Tank

SPEAKERS

Florian Jörgens
CISO
Vorwerk SE & Co. KG

Alexander Zhitenev
Group CISO
IFCO

Klaus-E. Klingner
Information Security Officer
M. Asam GmbH

Matthias Jungkeit
CISO/DPO
Münchener Hypothekenbank eG

Max Imbiel
CISO
Bitpanda

Matthias Orthwein
Lawyer / Partner
SKW Schwarz Rechtsanwälte

Thomas Zeulner
CISO
TDK Electronics

Berthold Panzner
Chief Architect
Nokia

Ilona Simpson
CIO EMEA
Netskope

Roberto Avanzi
Senior Principal Security Architect
Arm

Click Here to Register

November 21, 2023

Central European Time

www.cvisionintl.com

Welcome & Registration

10:30 AM-10:45 AM

Morning Networking

10:45 AM-11:15 AM

Opening Remarks

11:15 AM-11:20 AM

Striking a Balance: AI Information Security in the Organization – Navigating the Landscape Between Complain and Comply

11:20 AM-11:35 AM

The session deals with the typical defensive reactions of a company's business functions to the CISOs request for security measures and proposes ways to counter them creatively. The dialogue becomes even more difficult with obscure topics, such as generative AI. In the second half of the session or so, basic insights of experts such as Andrej Karpathy are summarized: Insights on how the transformer models underlying the large language models work and what implications that has.

PANELISTS

Matthias Jungkeit

CISO/DPO

Münchener Hypothekenbank eG

FIRESIDE CHAT

Bridging the Gap Between IT and the Business

11:40 AM-12:15 PM

Bridging the gap between business and technology is not easy and requires discipline and balance between technology, people, and the business. For so many organizations today, technology is the business. Technology needs to be understood as a critical enabler in every part of the organization from the front line to the back office. It creates new value by crunching data to deliver new insights, it spurs innovation, and it disrupts traditional business models.
For business and technology leaders alike, new actions and behavioral changes can help their organizations make this shift. CIOs must take responsibility for problems, they should convey that when technology fails, many people typically share responsibility.

CHAIR

Florian Jörgens
CISO
Vorwerk SE & Co. KG

PANELISTS

Alexander Zhitenev
Group CISO
IFCO

Berthold Panzner
Chief Architect
Nokia

Is the AI smart enough for EU data protection regulation?

12:20 PM-12:35 PM

While human brains already struggle sometimes with the compliance requirements of EU data privacy regulations (GDPR), the combination with the use of artificial intelligence does not necessarily make it easier. This session explores the practical impacts that GDPR has on the use of generative AI solutions in the daily use of companies. Through the example of practical use cases, it will be demonstrated where the most dangerous pitfalls are and how experienced legal experts recommend to deal with them.

PANELISTS

Matthias Orthwein
Lawyer / Partner
SKW Schwarz Rechtsanwälte

KEYNOTE

12:40 PM-1:00 PM

Digital Transformation: Why IT and Security Have To Join Forces to Succeed

Many drivers such as Digital Transformation, ubiquitous working environments as well as the need to protect organisations in an ever increasing level of sophistication in Cyber attacks have led to unprecedented complexity, high cost and inadequate governance. In her session, Ilona will explore how-not-to and how to deliver value through convergence and modernisation, and how to break out of the cost/risk/value trade off dilemma by joining forces of IT and security teams.

PANELISTS

Ilona Simpson
CIO EMEA
Netskope

Lunch & Networking

1:00 PM-2:00 PM

FIRESIDE CHAT

2:00 PM-2:35 PM

Social Engineering: New in 2023

Social engineering attacks are a growing concern for businesses and individuals alike, as cybercriminals continue to use advanced techniques to trick people into divulging sensitive information or performing actions that can lead to data breaches. In 2023, these attacks are expected to become even more sophisticated, making it increasingly challenging for individuals and businesses to identify and prevent them. To protect themselves, individuals and businesses must be vigilant and aware of these tactics. They must also implement comprehensive security measures, such as security awareness training, anti-phishing software, two-factor authentication, and access controls. Additionally, businesses must establish policies and procedures for responding to social engineering attacks, including incident response plans, data backup and recovery, and regular security assessments. By taking these proactive steps, businesses and individuals can better protect themselves from the risks associated with social engineering attacks in 2023 and beyond.

CHAIR

Florian Jörgens
CISO
Vorwerk SE & Co. KG

PANELISTS

Klaus-E. Klingner
Information Security Officer
M Asam GmbH

Roberto Avanzi
Senior Principal Security Architect
Arm

Poor Cyber Hygiene

2:40 PM-2:55 PM

In the digital age, practicing good cyber hygiene is essential to maintaining the security and integrity of personal and business data. However, in 2023, the lack of basic cyber hygiene practices will continue to be a major cause of cyber incidents. Cybercriminals exploit these vulnerabilities to gain unauthorized access to sensitive information, steal data, and launch damaging cyber attacks. It's crucial for individuals and businesses to prioritize basic cyber hygiene practices, such as using strong passwords, regularly updating software, and backing up data. Additionally, individuals and businesses must educate themselves and their employees on cybersecurity best practices and the latest threats to stay ahead of the evolving threat landscape. By taking these proactive steps, individuals and businesses can protect themselves from cybercriminals who prey on poor cyber hygiene practices.

PANELISTS

Max Imbiel
CISO
Bitpanda

Closing Remarks & Networking

2:55 PM-3:30 PM

TOGETHER WITH

netskope