Post event report

The 13th e-Crime & Cybersecurity Germany

18th June 2019 | Munich, Germany

Strategic Sponsors

BITSIGHT
The Standard in SECURITY RATINGS

CROWDSTRIKE

DIGITAL GUARDIAN

FLASHPOINT

LastPass ••• | by LogMeIn

LexisNexis RISK SOLUTIONS

ThreatMetrix

onelogin

Synack

VENAFI

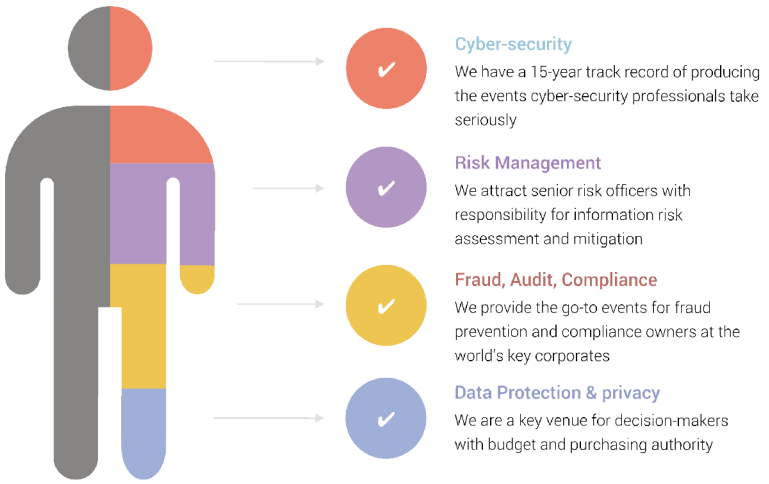
zscaler

Inside this report:

Key themes

- Getting the basics right
- The nature of nation state actors
- Cyber risk identification, measurement and management
- Cost-effective compliance
- Securing specialised systems
- AI: separating the hype from the reality

Who attended?



Speakers

David Anumudu, CISSP, CSSLP, CISM, Solution Architect, **Flashpoint**

Henrik Becker, Director Compliance & Risk Management, **Unitymedia Kabel**

Frank Borchard, Head of IT, **Otto Group**

Stefan Bosnjakovic, IAM & GRC Architect, **Deutsche Kredit Bank**

Ruben Caris, Anti Financial Crime, **HypoVereinsbank – UniCredit Bank AG**

Jake Curtis, Information Security Officer, **BurdaForward**

Wolfgang Fricker, IT Compliance Manager, **Lotto24**

Georg Gann, Regional Sales Director DACH & Eastern Europe, **Venafi**

Nathan Howe, Principal Solution Architect, **Zscaler**

Jirko Kaeding, Account Executive – DACH Region, **BitSight**

Christoph Kumpa, Director DACH & EE Region, **Digital Guardian**

Heiko Löhr, Head of Section Cybercrime Unit, **German Federal Criminal Police Office**

Georg Mattern, Information Security Officer, **Siemens**

Marcus Mueller, VP of Enterprise Sales EMEA, **OneLogin**

Jakob Oberascher, Senior Sales Engineer DACH and Eastern Europe, **Digital Guardian**

Ron Peeters, Managing Director EMEA, **Synack**

Marek Pietrzyk, Director and Program Manager, **UBS Switzerland**

Andy Renshaw, Senior Director – Market Planning – Fraud and Identity, **ThreatMetrix**

Dr. Christoph Ritzer, Partner, **Norton Rose Fulbright**

Daniel Sandmann, Attorney at Law, Senior Lecturer at **University of Augsburg and ICN Business School Nancy/Berlin**

Tobias Schubert, Enterprise Sales Engineer DACH, **CrowdStrike**

Peter van Zeist, Sr. Solutions Consultant, **LogMeIn**

Agenda

08:00	Breakfast networking and registration
08:50	Chairman's welcome
09:00	**How to manage the evolution of regulatory risk** **Felix Czwikla,** DPO, GlaxoSmithKline Consumer Healthcare • Adaptations since GDPR and lessons learnt • How does GSK manage regulatory risks and resulting incident response models? • How has the prioritisation of data privacy shifted and what does this mean for future security roles?
09:20	**Harnessing the power of a digital identity network: reducing e-crime, building trust** **Andy Renshaw,** Senior Director – Market Planning – Fraud and Identity, ThreatMetrix • How harnessing a global view of trust, and risk, helps detect and block advanced fraud • Building trust using digital identity intelligence can help better distinguish between good customers and fraudsters in near real time • An analysis of recent attack patterns and fraud typologies from the ThreatMetrix Digital Identity Network, which analyses 110 million transactions a day
09:40	**Implementing a compliance and governance control framework within the business** **Stefan Bosnjakovic,** IAM & GRC Architect, Deutsche Kredit Bank • Affording the appropriate members of the business the correct level and scope of access • How to manage intertwined business processes and IT while conforming to ever increasing compliance standards • Shedding light on the compliant implementation of segregation of duties
10:00	**Machine Identity Protection – the next hot category in IT security** **Georg Gann,** Regional Sales Director DACH & Eastern Europe, Venafi • What are machines? • What are Machine Identities? • Day-to-day challenges to overcome around Machine Identities • How to gain Visibility, Intelligence and Automation to protect your Machine Identities
10:20	Networking and refreshments break
10:50	**EXECUTIVE PANEL DISCUSSION** **Demystifying cyber-threats with law enforcement** **Heiko Löhr,** Head of Cybercrime from the German Federal Police (BKA) **Ruben Caris,** Anti Financial Crime, HypoVereinsbank – UniCredit Bank AG **Patricia Andre,** Business Continuity Manager, Allianz
11:10	**Your users don't care about the network, so why try and push them there?** **Nathan Howe,** Principal Solution Architect, Zscaler • Secure application access for your users regardless the location of the app or the user • Decoupling your users from your applications and networks • Your apps exist everywhere, on prep and the cloud, etc. therefore the internet has already become part of the company • Elimination of the need for network-centric solutions such as remote access VPN
11:30	**How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal)** **Jirko Kaeding,** Account Executive – DACH Region, BitSight Participants will see a live view into the BitSight Portal. We will demonstrate how continuous cyber-risk monitoring works for your company and the affiliates, your suppliers and peers. • How the cyber-risk rating can be improved in the easiest way. All risk vectors and the results will be demonstrated • How cyber-risk for your own company and its affiliates, suppliers and peers can be managed based on qualified events and ratings
11:50	**Enterprise password management and reporting – best practice** **Peter van Zeist,** Sr. Solutions Consultant, LogMeIn Besides multi-factor authentication, single sign-on and biometric data, passwords are still the most common form of authentication. In our session we will talk about how: • Organisations are better able to reconcile the needs of IT departments and users • Companies can counteract bad password habits • LastPass makes companies more secure in an unconventional way • You enable your employees to do the same without much effort • You'll be safer in five steps
12:10	Networking and refreshments break
12:30	**Protecting yourself inside out** **Jake Curtis,** Information Security Officer, BurdaForward • The human risk factor: are your employees aware they are being targetted? • How do you adequately sensitise employees to these risks? • Password management and multi-factor authentication for overall safety

Agenda

12:50	**Cyber investigations in fast mode**
	Tobias Schubert, Enterprise Sales Engineer DACH, CrowdStrike • How to achieve automated investigation TODAY • How to apply intelligence and cutting-edge technology to incident response • How to turn attacks into an opportunity to improve defence – automatically
13:10	**OneLogin Access Management: leading cloud transformation**
	Marcus Mueller, VP of Enterprise Sales EMEA, OneLogin • The dynamic future: 2025 • Evolution across three domains of business • The rise of the dynamic marketplace • Unifying access across the enterprise
13:30	Lunch and networking
14:20	**How AI can improve cyber-defence – building security analytics platform at UBS**
	Marek Pietrzyk, Director and Program Manager, UBS Switzerland • The evolution of critical persisting cyber-threats – impacting the growing attack surface of modern digital business environments • Leveraging AI, big data analytics and machine learning technologies to automate detection of abnormal behaviours of devices, users or networks • Lessons learnt from the successful global implementation from technological, operational and managerial perspectives
14:50	**3 steps to establish a data-centric security framework**
	Christoph Kumpa, Director DACH & EE Region, Digital Guardian, and **Jakob Oberascher,** Senior Sales Engineer DACH and Eastern Europe, Digital Guardian Forrester has created a framework to help security and privacy leaders implement a security strategy focused on the data. Their data security & control framework breaks down the problem into three areas: • Defining the data • Dissecting and analysing the data • Defending and protecting the data During this session, Christoph and Jakob will quickly drill into this framework and suggest how to derive tangible results from its three core disciplines.
15:10	**How risk intelligence derived from threat actors can inform software vulnerability management**
	David Anumudu, CISSP, CSSLP, CISM, Solution Architect, Flashpoint • Why managing vulnerabilities represents a huge challenge for enterprises • Triage troubles – what makes prioritisation so difficult? • Techniques your organisation can use to ensure that the most important emerging vulnerabilities are addressed
15:30	**Privacy and cybersecurity – legal framework and case study**
	Dr. Christoph Ritzer, Partner, Norton Rose Fulbright • Legal implications in case of a cyber-incident – how to deal with the incident and comply with the law • Overview on legal and regulatory risk landscape • GDPR aspects and NIS Directive • Cyber-incident response – case study: Legal and regulatory best practices
15:50	**Offensive security testing with a hacker mindset**
	Ron Peeters, Managing Director EMEA, Synack • There is exponential growth in cyber-attacks and attacks are increasingly sophisticated with greater break-in success • Traditional vulnerability scanning and compliance-based penetration testing prove ineffective to detect many serious vulnerabilities in live systems • Hear about a revolutionary new security testing approach using large teams of highly vetted international, top-class security researchers who can find serious vulnerabilities in any live system often within a matter of hours • Several supporting case studies are discussed including how Synack was able to break in the Pentagon within just four hours
16:10	Networking and refreshments break
16:30	**EXECUTIVE PANEL DISCUSSION** **Security and business synergy – aligning cybersecurity with organisational goals**
	Henrik Becker, Director Compliance & Risk Management, Unitymedia Kabel **Frank Borchard,** Head of IT, Otto Group **Georg Mattern,** Information Security Officer, Siemens **Wolfgang Fricker,** IT Compliance Manager, Lotto24
16:50	**Compliance and competitivity; balancing regulation and innovation**
	Daniel Sandmann, Attorney at Law, Senior Lecturer at University of Augsburg and ICN Business School Nancy/Berlin • Enforcing GDPR and beyond • The race for xtech and IT due diligence • The future of regulation
17:10	**Staying one step ahead: insights into cybercrime and the importance of collaboration**
	Heiko Löhr, Head of Section Cybercrime Unit, German Federal Criminal Police Office • If co-operation between the private industry and the police in case of a cyber-attack is to yield success it should preferably begin ahead of the incident: mutual trust and short information channels reduce and prevent damage in a crisis • The identification of reasons for and originators of cyber-attacks and data leaks is also in the interest of the affected enterprises and their customers • The confiscation of attacking IP infrastructures and the arrest of those involved in cybercrime are unique features of the law enforcement agencies
17:30	Conference close