Programme Cyber security Conference (English programme) June 5th 2018

Laura Tjebbes
Laura.tjebbes@heliview.nl
+31 (0)76 548 40 15

Programme committee members:

Phédra Clouner, deputy director, Centre for Cyber security Belgium

Pascal D'Eer, CTO, governmental organisation

Jeroen Hulshof, CISO, Baloise Insurance

Johan Sleeckx, Lead security, Baloise Insurance

Peter Spiegeleer, Enterprise Security Architect, Proximus

Erik R. van Zuuren, founder, Trustcore.EU

heliview
CONFERENCES & TRAINING

heliview
CONFERENCES & TRAINING

Programme

Theme: **Secure your Digital Transformation**
'How to Stay Secure in an Insecure World?'

08.30 Registration possibility participants + Coffee & Tea

09.00 **Opening programme by moderator**
Erik R. van Zuuren, *founder*, **Trustcore.EU**

09.20 **Keynote**
The state of Cyber Security in Belgium & the role of the CCB
For a few decades Cyber Security has become an important concern for enterprises and government agencies handling private and sensitive information. However and as threats evolve for the worse rapidly, they all have to upper their game!
In the specific and rapidly evolving area of Cyber Security and the context whereby parties can be held liable in case of a data breach, it is important that each "owner" constantly identifies its risks and implements security measures and controls.
An update will be given on the current state of affairs with regard to cyber-activity from a Belgian perspective as-well-as a view on what the National Centre for Cyber Security can do to support owners, enterprises and governments.

Miguel de Bruycker, *Managing Director,* **Centre for Cyber security Belgium**

CENTRE FOR CYBER SECURITY BELGIUM

09.45 **Keynote – Organisational security (track)**
Train Like You Fight
Stories from the field about readiness at the inevitable breach
A reaction at a breach causes often more damage to the organisation than the incident itself. The main reason for this is the lack of good preparation. With all focus on 'prevent' and 'detect', the attention for 'respond' is often neglected. According to a casestudy of the Ponemon Institute in 2017, an incident response plan lacks at 75% of all organisations. Erno Doorenspleet tells you with several examples about the importance of an incident response plan and answers the question how to properly react in case a breach happens.

Erno Doorenspleet, *Global Executive security Advisor*, **X-force Command, IBM**

IBM

10.10 **Opinion poll**

10.35 **Morning break with 1-to-1 meetings**

11.15 Break-out sessions

Organisational security track	Threat intelligence / Management track	Threat intelligence / management track
Break-out session 1A **Strengthening your organization's cyber-culture and cyber-resilience** Approximately 80% of all security incidents are caused by human errors. Unfortunately, employees are often not aware of the important role they play within the information security of their organization. Otherwise put, as long as investments are only in technical measures, your organisation will continue to run an increased risk. Hence investments need to be made in "organizational controls". So, how do you ensure that your employees look at things differently? How do you encourage your employees to work "securely"? How do you create a culture where everyone feels (co-)responsible for cyber security? In this session get some insights into how to set up a solid security awareness program which targets to strengthen your "organizational resilience". Philip Verbeeck, *enterprise account manager,* **Kaspersky Lab**	**Break-out session 1B** **New cyber threats entering the online attack surface of organisations.** With the increase in use of digital technologies, driven by the need for businesses to become more visible and agile, there has been a strong increase in the number of endpoints and potential ways for cybercriminals to gain access to the networks of organisations. As a result, the entire cyber battlefield has evolved and become more complex. With this, new cyber risks are evolving. What cyber threats should you expect in the **future** and how can you start to secure your organisation **today**? Pieter Jansen will provide insight into new types of cyber threats: how they work and how you can prevent your organisation from becoming a victim. In addition you will be informed about the online attack surface hackers use and why it is essential to constantly track this in the process to avert cyber attacks and to stay compliant on cyber security. Pieter Jansen, *CEO & Founder,* **Cybersprint**	**Exclusive break-out session 1C** **Cyber Security starts with decent risk analyses, maturity measurement and action plan!** In this session, V-ICT-OR will demonstrate how local governments can use the V-ICT-OR-tool to: • Perform a risk analysis of their information security policies: what are the potential risks of the current policy? Which risks are limited, which are significant? • Analyze the maturity of their information security policies: do they still need work (and if so, in what respect) or are they already quite mature? • Formulate a safety plan with a view to the future: what actions can they link to specific risks? Who ensures the follow-up of said action and what is its deadline? If these actions are effectively performed, the current information security policy is strengthened. Eddy van der Stock**,** *voorzitter,* **V-ICT-OR Vlaamse ICT organisatie**

11.40 Possibility to change halls

11.45 **Break-out sessions**

Threat intelligence / Management Track	Technical security track	Threat Intelligence / Management Track
Break-out session 2A **Modern Day Attacks – Examples and countermeasures** In this session, we will give you an insight into some of the advanced techniques employed by Nation State hackers and e-Criminals, including the countermeasures to prevent these attacks from happening in your environment. While providing these insights, the goal is not to bury you under the bits and bytes but to give you the knowledge and understanding of the key strategies proven to keep the attackers out of your organisation. Ronald Pool**,** *cyber security specialist,* **Crowd strike**  	**Break-out session 2B** **A New Era of Cyber Threats: The Shift to Self Learning, Self Defending Networks** • Leveraging **machine learning and AI algorithms** to defend against advanced, never-seen-before, cyber-threats • How new **immune system** technologies enable you to pre-empt emerging threats and reduce incident response time • How to achieve **100% visibility** of your entire business including cloud, network and IoT environments • Why automation and **autono mous response** is enabling security teams to neutralize in-progress attacks, prioritise resources, and tangibly lower risk • **Real-world examples** of subtle, unknown threats Arthur Vermeire**,** *senior cyber security manager***,** & Elizabeth Entjes**,** *Cyber security account executive***, Darktrace**  	**Break-out session 2C** **Could the CISO play the role of a DPO?"** - Discussion with the audience in relation to the activities of the CISO and DPO - Exchange on various criteria that would allow a CISO and DPo do combine their activities - Legal and practical considerations preventing those activities to be performed by the same entity/person. - Overview with the audience of their own experience Georges Ataya, *Professor and Academic Director (SBS-EM) of IT and Information Security Management Education* **Solvay Brussels School**. 

12.10 **Possibility to change halls**

12.15 **Keynote – Technical security check**
'Change is Simply an Act of Survival'
As organizations make the move to the cloud, they are finding that the network is becoming irrelevant from a security perspective. In this session we will explore developments in malware and the business like approaches threat actors are taking to breach networks. We will look at threats that can affect corporate users and strategies to ensure a more secure architecture in the future.

Bil Harmer, *CISO Americas,* **Zscaler**

12.40 **Lunchbreak with 1-to-1 meetings**

13.50 Break-out sessions

Organisational Security track	Threat Intelligence / Management track
Break-outsession 3A **Is ICT a reflection of our today's society?** ICT is more and more similar to our physical society, more and more ICT is shared and/or publically used and/or public-facing. Today, in many organizations, ICT security measures are still based on a design/ idea that ICT is situated in a closed proprietary environment, with some access gateways to the outside world. Should it help if we use the comparison between our physical society and ICT and look back how it was in the last century and how it is today? Can that improve the understanding of cyber security by Non ICT management? Or should we approach the subject along another approach? What if business objectives are not being achieved, because you have underestimated the cyber security risks? How do you link cyber security risks to business objectives? Do you end up with the same set of information security measures when using both approaches assuming the infra-structure used by an organization is public/shared (not secure)? In other words what type of Information/Data Security measures do you need and should you manage yourself as an organization in a ICT world in which infrastructure is public/shared, legally requirements are raising and the amount of criminal offences, terrorism/hacker-attempts is increasing every day? How can I explain the need for different security measures to my management? It is not about the protection of the ICT infrastructure but about the protection of the data, which is the accountability of the organization itself. Erik IJpelaar, *Manager Security,* **Traxion** TRAXION Partners in Information Security	**Break-out session 3B** **Protection of critical infrastructures - Why and how cloud security can beat on premise** In today's connected world more and more critical infrastructures are monitored and managed by using the internet. The critical question for many companies and subject matter experts is to what extent the internet access is secure, reliable and ideally also fast. To fight the "attack industry" requires a distributed perimeter approach for effective defence. To counter ever evolving threats this perimeter approach must be constantly reviewed and updated. This approach provides more security than on premise. Stefan Mardak**,** *Enterprise Security Architect Senior*, **Akamai** Akamai FASTER FORWARD

14.15 Possibility to change halls

14.20 **Break-out sessions**

Organisational security Track	Technical security Track
Break-outsession 4A **Orchestration in Incident Response: A Game-Changing Strategy** Orchestration allows for security teams to process incidents faster and more accurately. And by automating repetitive and menial tasks and delivering the right information to the right analyst at the right time, orchestration can significantly drive down Mean-Time-To-Response. •How orchestration and automation are defined and how the two strategies relate •How to effectively leverage automation to support an orchestrated incident response function •Best practices for orchestrating your SOC and achieving faster, more efficient, and intelligent incident response Tycho Schmidt, *Incident Response Sales Engineer,* **IBM** 	**Break-out session 4B** ***Identity. Security. Automation. Document Signing*** Document management has evolved from paper and wet ink to automated workflows and electronic signatures. But with involves identity, security and compliance, which are very important aspects in this new era of pervasive digitization. When it comes to signatures, you need to be able to sign documents smoothly but you also want your signature to be compliant with the legal requirements. So, identities and cybersecurity are closely linked. This session will look into the potential threats of digital signatures and correct setup of automating a Document Signing workflow in the world of digitization. Ronald de Temmerman**,** VP Strategic Sales**, GlobalSign** 

14.45 **Possibility to change halls**

14.50 **Break-out sessions**

Technical security Track	Technical security Track
Break-out session 5A **Securing the New App Economy** The focus of digital identity for the New App Economy is to remove silos, minimize redundant effort, enable better collaboration and provide a foundation for regulatory compliance. The challenge is that shared credentials for both commercial and public-sector organizations will require organizations to innovate to address requirements for physical access, protecting PII, delivering cross-agency services and re-thinking how digital consumers interact. In this session, we will discuss best practices across the industry that can be applied to enable interoperable credentials, we will explore architectural practices to manage identity assurance levels, and identity verification for both logical and physical access. Des Powley**,** *EMEA director Security***, CA** 	**Break-out session 5B** **Customers are online, is your company ready to engage with them?** First Jeroen Starrenburg, will explain the true values behind Customer IAM (CIAM). Because of its full potential, CIAM is the fastest growing market within the fintech industry. CIAM is the true value in customer engagement. The great thing about CIAM however is that it provides so many more strong benefits. For instance, GDPR compliance, bank grade security, major savings on input and output, shorter time to market, and strengthening your sales channels like for instance agents. Next Jeroen Hulshof, from Baloise Insurance will explain why CIAM is critical for supporting the Brand Identity and accelerating their digital transformation. Jeroen will share his approach on building the foundations for providing a next-level customer experience to connect to online services from any device in a Simply but Safe way. *Jeroen Hulshof***,** CISO, **Baloise** & Jeroen Starrenburg**,** *CEO***, Onegini**  

15.15 **Afternoon break with 1-to-1 meetings**

15.55 **Break-out sessions**

Technical security Track	Threat Intelligence / Management Track
Break-out session 6A **Better security through virtualization** Don't think on how to secure your virtualisation infrastructure. Instead think of how virtualisation can help you increase your overall security posture. During this session we'll go over the pitfalls of modern security infrastructure implementations and how virtualisation can drastically change an organisations entire security DNA. Frederick Verduyckt, *NSX SE Specialist*, **VMware** vmware	**Break-out session 6B** ***Protecting you most valuable asset - Data*** Shockingly, most companies fail to protect their most valuable data – and can't tell if it's been touched or stolen. Clearly, your data should be the primary focus. So, why do insiders and outside attackers keep hitting our unstructured data systems? Why does this keep happening? It's because data is in the dark. Think about the questions you should be able to answer if your data is secure: Where's my sensitive data, and where is it exposed? Who's got access to what? What's being used, and by whom? What's stale – what can I get rid of? Who owns this data? Maybe most critically… To keep data safe, our brightest light needs to be on the data itself. We are fighting a different battle – so your data is to be protected first. Not last. Jeremy Agenais**,** *sales manager***, Varonis** VARONIS

16.20 **Possibility to change halls**

16.25 **Keynote technical security Track**

Enhancing your security posture with endpoint detection

In a world where the threat landscape constantly changes having just an endpoint protection solution isn't sufficient anymore. During this session we will go over the challenges organizations face and changes that are needed when it comes to detecting and responding to advanced threats. We will also cover a few key do's and don'ts when selecting products / technology.

Patrick van der Veen, *solution sales engineer*, **F-secure**

F-Secure

16.50 **Keynote**

Cyber Threat Intelligence: The persistent relevance of Sun Tzu.

In an era of ever-accelerating change on all fronts security analysts risk suffering from cognitive overload. The pace of change of the business and the rapid innovation of TTPs catalyzed by lawless online markets are central focal points of this conference. Amid all this FUD the temptation to simply resign ourselves to this new normal is almost irresistible. We contend though that a few centuries-old guidelines can help in still confidence and focus to all security practitioners in today's daunting environment. In this keynote we will elaborate on what these guidelines can mean for organization of cyber security at the individual, the enterprise and the industrial level.

Wim Bartsoen, *Head of Cyber Defence, Data Protection & Privacy and Awareness*, **BNP Paribas Fortis**

17.15 **Short wrap up by moderator**

Erik R. van Zuuren, *founder*, **Trustcore.EU**

17.25 **Networking reception at the network area**