9th annual information security forum

Nordic IT Security

Stockholmsmässan October 26th 2016, Stockholm, Sweden

Partners 2016

RES · PHISHME · GlobalSign GMO INTERNET GROUP · resilient SYSTEMS · Outpost24 Vulnerability Management made easy · radware Every second counts

algosec · CYBERARK · eset ENJOY SAFER TECHNOLOGY · zscaler · SKYBOX SECURITY · expandtalk

tufin · SUPERMICRO · AvePoint · BOMGAR · BT · ERMA · virus BULLETIN

SecuritySolutionsWatch.com Solutions • News • Events · TeleTrusT Pioneers in IT security · iisp The Institute of Information Security Professionals · Global Security Mag · DIGITAL FORENSICS / MAGAZINE · SIG Security · ISACA Denmark Chapter

#nordicitsec

www.nordicitsecurity.com

EDITOR'S FUTURE OUTLOOK

As 2015 came to an end it was time to look back at last year's Nordic IT Security Forum and use the information to gain perspective on the future. 64 speakers covered a wide range of topics during the 3rd of November at Stöckholmsmässan. What are we looking at in 2016?

Online Extortion

Using fear as a major component of the online extortion will increase. Besides solving the technical aspects of each operation it becomes crucial to master the psychology behind online threats. Cyber extortionists will devise new ways to target its victim's psyche to make each attack "personal" - either for an end user or an enterprise.

Data Protection Regulation

The EU Data Protection directive will mandate a high standard of protection on data. DPOs and CISOs must be experts in data protection and data security regulations and must how these should be effectively implemented.
However, not all enterprises will be up to the task. Awareness around data protection will pave the way to a significant shift in the enterprise mindset and strategy against cyber-attacks. We will see more enterprises taking on the role of the 'hunter' instead of the 'hunted', in that they will begin to make use of threat intelligence and next-generation security solutions with custom defense to detect intrusions earlier.

Global Cybercrime Legislation Movement

We need an enhanced international collaboration and partnerships to fight cybercrime - fast legislation, successful takedowns, convictions and arrests. Cybersecurity standards are outdated. Governments and regulators will play a more active role in protecting the Internet and safeguarding users.

Mobility

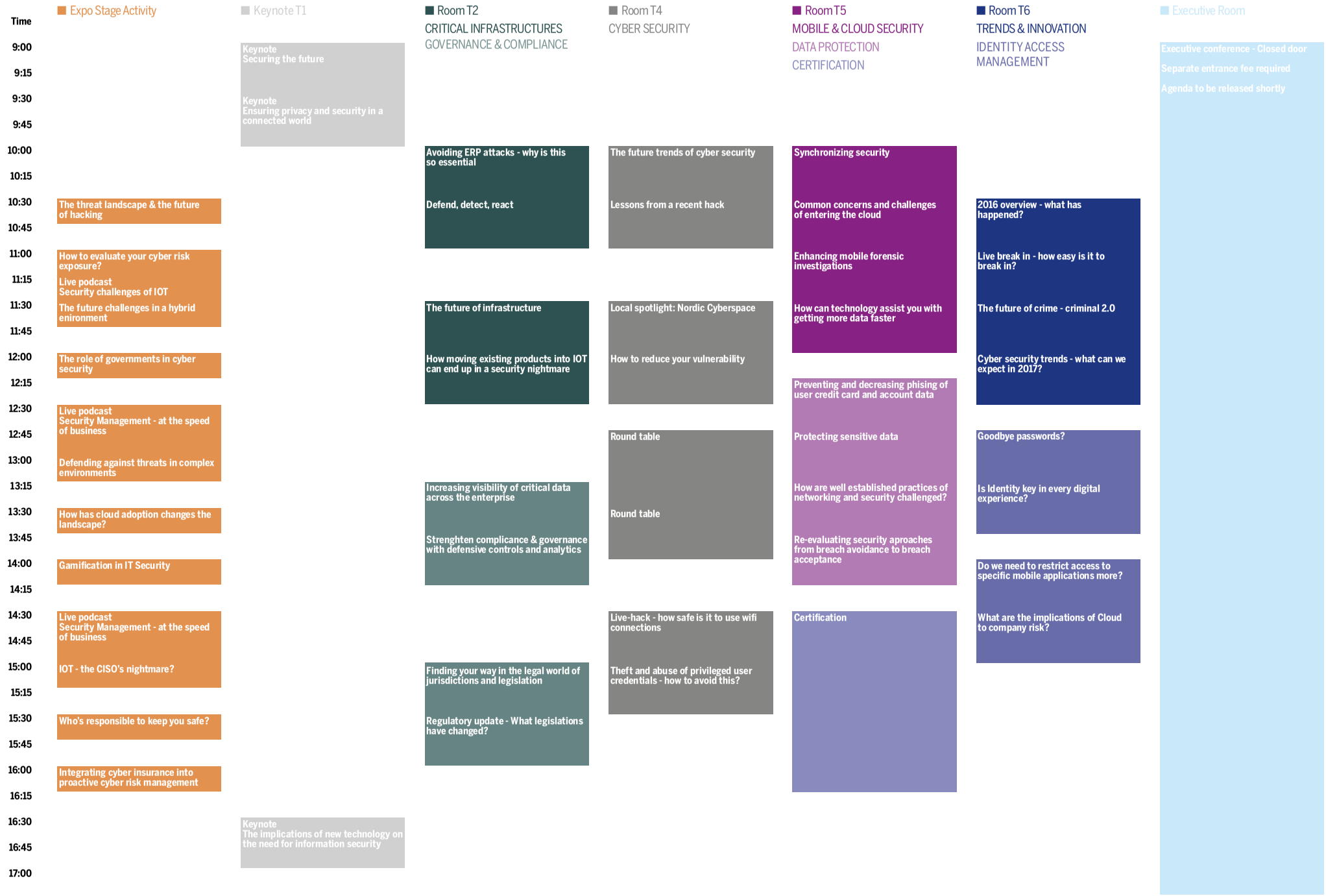
The mobile workforce is increasing, meaning employees who have access to company or other sensitive data through their personal laptop, tablets or smartphones are becoming an increasing risk for organizations. Mobility is now also significantly adopted in commerce. Online sales via mobile devices are growing at three times the rate of traditional online sales and according to PWC's Global Information Security Survey, 57% of the respondents have adopted mobile payment systems. How can we stay secure in a 24/7 connected world?

Cloud Security

Cloud computing has emerged as a sophisticated tool for cybersecurity safeguards in recent years as cloud providers steadily invested in advanced technologies for data protection, privacy, network security and identity and access management. Forward-thinking companies are already shifting away from traditional perimeter defenses in favor of cloud-enabled cybersecurity that is based on real-time analysis of data and user-behavior patterns.

Maaike Gerritse
Producer of Nordic IT Security 2016

Conference at a Glance



MEET THE NORDIC IT SECURITY ADVISORY BOARD 2016

Anne-Marie Eklund Löwinder, Chief Security Officer, IIS

Anne-Marie is Chief Security Officer at IIS. She has been ranked as one of Sweden's foremost experts on IT security by the magazine Computer Sweden. She is a member of the board of CENTR, of IRI (The Swedish Law and Informatics Research Institute), the foundation for Development of Telematiques (TU-stiftelsen) and SNUS (the Swedish Network Users' Society). She is furthermore a member of the information security council of the Swedish Civil Contingencies Agency (MSB) and is one of the handful of individuals assigned as Trusted Community Representative and participates in the DNSSEC key generation for the internet root zone as Crypto Officer, appointed by ICANN (the internet Corporation for Assigned Names and Numbers). She is also a member of the swedish Digitalization Commissions expert group. Ms. Eklund Löwinder was also a member of the very first groups that helped the Swedish Standards Institute (SIS) and Swedac to develop what now is known as the ISO 27000-standard for information security management.

Paolo Balboni, Founding Partner of ICT Legal Consulting & Scientific Director of the European Privacy Association

Paolo Balboni (Ph.D.) is a top tier European ICT, Privacy & Data Protection lawyer and serves as Data Protection Officer (DPO) for multinational companies. Dr. Balboni is a Founding Partner of ICT Legal Consulting (ICTLC), a law firm with offices around the world. He provides legal counsel across Europe to multinational companies specializing in the fields of Personal Data Protection, Data Security, Information and Communication Technology (ICT), and Intellectual Property Law. Dr. Balboni has considerable experience in Information Technologies including Cloud Computing, Big Data, Analytics, and the Internet of Things, Healthcare, Insurance, Banking, Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT). Dr. Balboni is the Scientific Director of the European Privacy Association based in Brussels, the Cloud Computing Sector Director and Responsible for Foreign Affairs at the Italian Institute for Privacy based in Rome.

David Jacoby, Senior Security Researcher, Kaspersky Lab

David is a security evangelist who is currently working as Senior Security Researcher for Kaspersky Lab. He is responsible for not only research but also technical PR activities in the Nordic and Benelux region where his tasks often include vulnerability research and management, penetration tests, security research and public speaking engagements. His day to day job is about improving awareness of the current and future threats and vulnerabilities to which Internet users are exposed and fight cybercrime. David has about 15 years of experience working in the IT security field. This have given him the opportunity to work in many interesting fields such as: Vulnerability and Threat Management, Customer Experience, Penetration Testing, Development and Fighting Cybercrime.

Per Thorsheim, Security Adviser, God Praksis AS

Per Thorsheim works as an independent security adviser, based in Bergen, Norway. He is the founder and main organizer of PasswordsCon.org, the worlds first and only conference about passwords. He has a personal project on convincing the world to implement RFC3207 STARTTLS support for opportunistic email encryption. Per was a finalist for the annual Rosing IT security award in 2012, and was awarded the Commanding General of the Norwegian Armed Forces Cyber Defence Coin in spring 2014 for his contributions to information security. He also claims to know your next password. He currently holds the CISA and CISM certifications from ISACA, and CISSP-ISSAP from (ISC)2.

Mika Kataikko, Director, Cyber Security

Mika Kataikko is director for Cyber Security both in the Jyväskylä Regional Development Company Jykes Ltd. and in the national Cyber Security business development program driven by the Finnish Funding Agency for Innovation (Tekes). Mika has a long and diverse background in the Telecom, ICT and Security businesses, in the positions from supervisory role to product and product area life cycle management, including also quality and security related management and development responsibilities. His versatile job history gives him a wide experience and viewpoint in the different areas of businesses and business making, especially in the areas of ICT and Cyber Security.

Ulf Berglund, M.Sc, CISM, President, Cloud Security Alliance Sweden

Ulf Berglund is the president of the Swedish chapter of CSA, Cloud Security Alliance, a worldwide organization. He is also co-author of the book Guide to the Cloud. Ulf has a long experience from leading positions in the field of information security. He has a background as an officer, his last active years he was principal officer, IT security and information security expert at the Military Intelligence and Security Service (MUST). He has held positions as CTO, senior consultant and senior consultant for companies such Pointsec, Ernst & Young and Technology Nexus. Ulf's consultant and the experience derived from companies like Scania, Swedish Match, the Stockholm Stock Exchange (OMX), the Swedish Central Bank, Apoteket AB (pharmacy) and Hennes&Mauritz AB. He has his own company, U&I Security Group AB.

Karen Lawrence Öqvist, CEO Privasee AB, Privacy Advocate & Expert

Privacy Advocate & Expert – Cannot be Controlled – Cannot be Manipulated – Let the Voice of the Citizen be heard!" is her personal tagline. Karen cares passionately about the right to personal privacy and the right of ownership of our digital identities, Personal Identifying Information (PII), and our digital footprint. She is an author, speaker and entrepreneur, earned two masters degrees and privacy certifications with IAPP (www.iapp.org). With 20+ years experience in information security and compliance; her career has taken her from UK to: Cern in Geneva, Novell in Zurich, Stockholm, and Hewlett-Packard. Today Karen is CEO of Privasee AB, a start-up focused on Data Protection and Privacy.

As partner managers with the Nordic IT Security Forum, Camilla and Simon have been developing and managing sponsorship programs for this leading IT Security Forum with great success. With their dedication and creativity, they ensure the best business value to the partners and unforgettable events for the audience.

Book your participation, influence the content and benefit from extended marketing campaigns.

Contact Camilla Nilsson, Partner Manager
Tel. + 46 723 87 27 70
Email: camilla.nilsson@copperberg.com

Contact Simon Wisniewski, Partner Manager
Tel. +46 8 12 201 585
Email: simon.wisniewski@copperberg.com

Call for papers

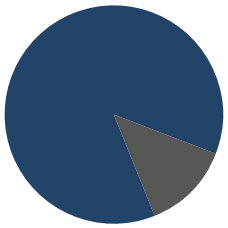
Are you interested in being on stage? You have the opportunity to host demo's, penetration tests, present research, end user cases and more at Nordic IT Security 2016, in November 2016.

I'm looking forward to your inquiry in form of a short abstract (max. 400 words).

Maaike Gerritse, Content Director
Tel. +46(0)735768087
Email: maaike.gerritse@copperberg.com

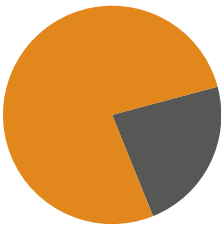
2015 OVERVIEW

CONTENT



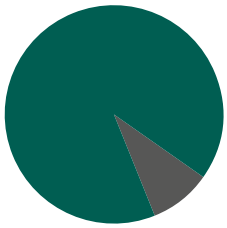
87% of our delegates rated the conference content with 4.6 out of 6.

NETWORKING

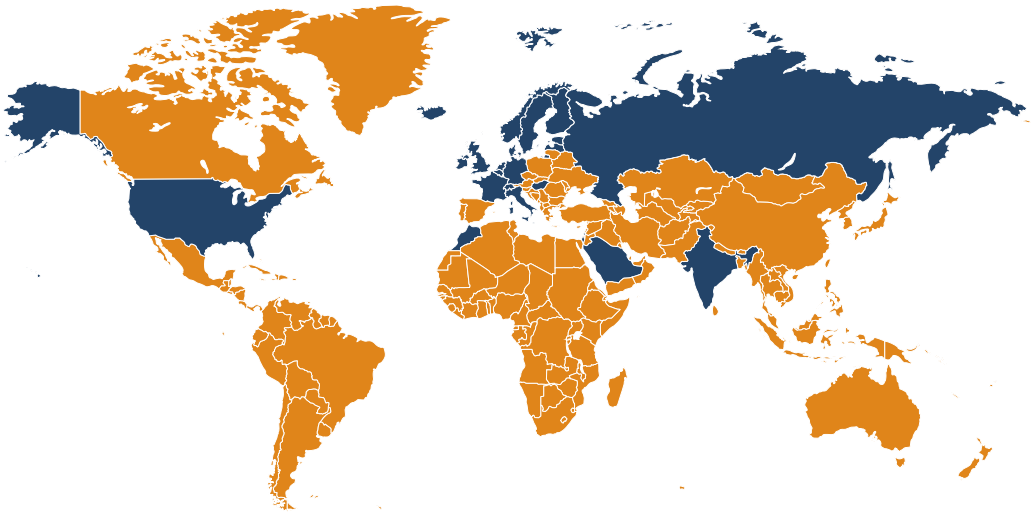


77% of our delegates say that the networking opportunities were very helpful.

SPEAKING



91 % of the speakers want to be back on stage for our 2016 edition!



OUR ATTENDEES TRAVELLED FROM…

Belgium	Hungary	Latvia	Switzerland
Denmark	Iceland	Malta	The Netherlands
Estonia	India	Norway	UK
Finland	Ireland	Russia	USA
France	Israel	Saudi Arabia	
Germany	Italy	Sweden	

600+
attendees

60+
speakers

50+
sessions

45+
exhibitors

600+
minutes structured networking

5
conference rooms

1000
Sqm exhibition

TESTIMONIALS

Very well organized with high quality speakers!

IT Advisor Sweden AB

A really good place to meet both the industry and the potential clients. Many interesting seminars and lots of discussion with interesting people. A place to be!

Outpost24

A great knowledge exchange forum with security thought leaders. The event was well organized and resulted in productive discussions and exchanges.

Vice President, BT Security Europe, BT Group

Nothing could have been improved to make this better.

Bomgar

Great and knowledgeable speakers. Have learned a lot from this event.

Internal Audit & Investigations Department

Met lots of interesting people, listened to several great presentations, and learned some new things about network security.

Royal Institute of Technology, Stockholm

Great conference. Got many good leads out of it.

AlgoSec

ARTICLE

BOMGAR
Scott Walker,
Enterprise Client Manager, EMEA,
Bomgar

Connect fearlessly

We can all agree that over the years we have seen a huge change in security and the challenges it brings. But what has remained consistent throughout are the potential rewards available to cyber criminals, be it credibility within the Cybercrime network, or financial gain.

We ask ourselves the same question every time we read or hear about Cyber breaches in the media; how did it happen? Typically, we look to statistics to identify where these vulnerabilities reside and we can see third party vendors have been identified as one of the biggest targets. With the increase in IT outsourcing and relying on third parties to manage our networks and infrastructure, we need to ensure we can control the layer of defense which protects our sensitive data from potentially less security minded suppliers and partners.

So how can we do that? The best option is to give our vendors a VPN, right?

Cyber criminals have seen this as an opportunity.

Let's take a step back. A VPN has been (and still very much is) a way to manage network access for trusted employees who are working remotely. The main reason for this is because you, as the administrator, have control of their security posture, and the resources being accessed. But when the scope of the VPN is extended to manage connections from less trusted sources, we can begin to see a potential threat.

A common misconception when it comes to developing secure access is to provide your third parties with a VPN, securing their access, but this also opens up a foothold into the network at the same time. The problem is Cyber criminals have seen this as an opportunity. Allowing vendors access to your network via a VPN creates vulnerabilities a cybercriminal can leverage. It gives them the ability to compromise your network and potentially get their hands on your sensitive data. By simply compromising a third party machine, and potentially gaining access to a privileged account whilst using a valid VPN connection, it is likely they have an open tunnel into your network.

Once on the network they have nothing but time moving virtually undetected throughout your network until the keys to the kingdom are found, unlocking sensitive data, source code, IP or whatever is valuable to your organization.

Outsourcing IT to specialists in the form of a third party to achieve benefits such as cost savings doesn't have to be vulnerable and it doesn't have to be frightening. Utilising alternative solutions to VPNs to securely manage and control your third party access can allow your IT teams to remain productive whilst improving security.

David Lacey
Managing Director,
David Lacey Consulting Ltd.

Whither the Nordics in Cyberspace?

As an international consultant, and a former Shell International adviser, I have had plenty of opportunity to note the capabilities and interests of cyber security communities across the world. We all share common standards, but each region adopts a slightly different focus.

American companies prefer technical solutions. The British like bureaucracy (we gave the world ISO 27000). Continental Europe has more focus on the human factor. Some regions lead, others follow. Some communities obey, others challenge. The same directive issued to different communities can be received and interpreted quite differently.

Cyber security also goes through distinct phases, with each one favouring a particular breed of security professional. In the 1980s the focus was on creative local solutions. In the 1990s the challenge was standardised enterprise controls. In the 2000s it was about securing e-Business. Since then the focus has been regulatory compliance.

Compliance steps in when companies don't do enough. But it's a poor driver, encouraging a tick-box approach based on old, established standards. Compliance doesn't recognize imaginative new solutions. It is backward looking, driven by audits rather than forecasts.

To survive in an increasingly dangerous threat environment we need real security, not paperwork. Unfortunately real security is career limiting. Security managers who shut down insecure connections and send projects back to the drawing board are not welcome in today's business. Yet compliance officers and auditors can wield increasing power, and are growing in numbers. In banks they may outnumber security professionals by an order of magnitude. The tail is wagging the dog.

Will this change? Yes. But only after a massive incident with the impact of a 9/11 attack. Then we will witness a sea change in society's perception of cyber security. And the outcome will be increased power to the Chief Information Security Officer, and the onset of a new age of real security, with security professionals empowered to make and enforce decisions based on realistic assessments of risk.

This new age will demand a new attitude and a fresh set of skills: a longer term outlook; the ability to build innovative solutions; outstanding team work across national and organizational boundaries; a capability to manage highly complex systems; and to respond quickly and bravely to attacks. Most importantly it demands a sound understanding of the socio-political landscape, and the ability to strike a balance between the security fears of society and the privacy concerns of citizens.

This new age will demand a new attitude and a fresh set of skills

The Nordics should welcome this change because it better fits the Nordic mind set and capabilities. In an age when technology is largely a commodity, it will be the human, ethical and political skills that shape our cyber security leadership. The Nordic response to cyber security should be to bring these skills to the fore, rather than promulgate the outdated rituals of an earlier age.

Top 10
of 64 speakers.
Congratulations, David!

ARTICLE

Graham Murphy
Manager of Research & Assessment,
Black Berry

IoT and security– the future?

In one of the sessions during Nordic IT Security Forum 2015, Professor Jarno Limnéll highlighted the drive to make digital everything that can be digital. The Internet of Things (IoT) is one of the consequences of this digitisation of everything, whether we recognise it explicitly or not.

Top 10
of 64 speakers.
Congratulations, Graham!

We have already seen examples from the automotive, medical and consumer sectors where security and privacy appear to have been an afterthought rather than a designed-in attribute. I touched on this during the IoT – The CISO's nightmare panel, highlighting BMW's fix for a vulnerability in their Connected Drive functionality – a switch from plain text to HTTPS encryption. In a world where applications and systems need to be resistant to attack, the lack of basic provisions to protect data seems to be a throwback.

During the presentation "The evolution of IoT – What you don't know can kill you", I used a number of failures in a medical device as a springboard to illustrate how hardware and software can work together to build a more resilient platform that can monitor itself. I started with the hardware, with the concept of a hardware root of trust. This uses ROM in conjunction with pre-provisioned certificates to ensure that the first code executed has been signed by the manufacturer. By utilising this trust relationship from the very moment the hardware is powered up, we can ensure that each stage of the boot process is trusted and that we will end up with a platform operating in a known safe state. If you want to know more on root of trust, my colleague Alex Manea has written a short article [1] that will be of interest.

> The Internet of Things (IoT) is one of the consequences of this digitisation of everything

Another failure I highlighted was the presence of debug ports. By connecting to these debug ports, I had the ability to control execution on the device, even to the extent I could alter the contents of RAM and flash memory. For a development device, access to these ports make good sense – how else are the developers meant to debug their code? On the other hand, a production device should not have debug ports and the connections within the circuit that provide such functionality should not be accessible.

Some silicon vendors are highlighting their designs as ideal for IoT usage, but on closer inspection some functionality that is required for anything other than basic security simply isn't present. Admittedly, not every IoT case needs a fully featured security model, but feature creep can take a product in a new direction that requires more security. In other cases, the vendor provides a hardware implementation, but provides little in the way of examples or documentation of how to make security features actually work. In such a case, it becomes difficult to implement a secure IoT solution. In the case of consumer products such as games consoles, much work has been done to defend against an attacker who has physical access to the device. Conversely, little work appears to have been done for IoT solutions. While you can add network security at the software layer to a chip that has no support for physical security, it isn't possible to add physical security to a chip that doesn't support it. The good news is that there are silicon vendors who have recognised the requirements, enabling OEMs to manufacture IoT design with layers of security built in.

On the IoT software side, we have failed to learn from the early days of computer (in)security. Default credentials that don't require changing are commonplace. Cryptographic material such as WiFi keys, private keys, certificates, usernames and passwords are typically stored in plain text. These are issues that many in information security have spent decades to try to prevent, only to see a resurgence in IoT devices. Just as concerning was the university student who came up to me after my presentation and explained that the IoT module on their course was all about the opportunities of IoT, without any of the security training that should go alongside.

IoT should be an enabling technology and vendors shouldn't be repeating the mistakes that were being made 10-20 years ago. The benefits are huge, but there are still challenges on how we deal with security, data gathering and privacy.

[1] How BlackBerry Security Begins At The Endpoints
http://bizblog.blackberry.com/2015/02/blackberry-security-starts-at-endpoints/

Jarno Limnéll,
Professor of Cybersecurity, Aalto University, Finland
Vice President, Cybersecurity, Insta Group Ltd.

We Need European Cybersecurity!

The Nordic IT Security Forum was a success! It was great to meet cybersecurity experts from so many countries, discussions were both topical and interesting, and arrangements worked perfectly. Thank you!

Top 10
of 64 speakers.
Congratulations, Jarmo!

Cyber security has entered the domain of foreign and security policy due to the ever-globalizing world. In this digital domain, strategic advantage can be either lost or won. It is very significant to encourage us Europeans to think together cyber security issues especially from the strategic point of view. We are no longer securing computers – we are securing societies, our businesses and our way of life. We are also protecting our values. As it says in the EU Cyber Security Strategy, "The EU's core values apply as much in the digital as in the physical world."

Most European countries have cyber strategies on paper, but public discussion at policy and doctrinal levels and practical measures are not as mature as they are for example in the United States. Without serious efforts the gap is only likely to widen in Europe. This would increase the potential to become the focal point for more serious cybercrime, espionage and even debilitating attacks.

But it is not easy to deal with 28 countries and despite these steps at EU level, European cyber security remains almost exclusively a national prerogative. This must change. The most important driving force for a new "Cyber Europe" could be the European industry. Companies outside of Europe are currently dominating the rapidly growing cyber security market. For example, in the latest list of "cybersecurity companies to watch in 2015" there are only a few European companies in the Top 100.

At the moment there is a special opportunity for European companies because there is a lot of suspicion in the market towards cyber security products from the US, China, and Russia. European companies would be able to enter the market as a more trustworthy partner.

Europeans are very dependent on foreign internet services, especially GAFA, which stands for Google-Apple-Facebook-Amazon. Nine out of 10 Internet searches in Europe use Google. Where are European alternatives, many people ask? Very relevant question. This dominance should worry Europe, even if the current situation works fairly well.

In the US, Google, Apple, Facebook, and Amazon are generally praised as examples of innovation and the same kind of innovativeness must be encouraged and supported in Europe. The question is not only how much Google, Apple, Facebook, and Amazon dominate every facet of our lives, but also how important and precious the data is they possess in today's world. This data should be understood as a part of cyber power - and Europeans are letting it go abroad.

> We are no longer securing computers – we are securing societies, our businesses and our way of life.

European cyber security companies and digital platform industries must transform themselves and become more competitive. This development has to supported strongly. It is also the job of politicians and lawmakers to protect both European industries and European digital rights. Cyber security issues should be brought more actively into the political discussions in European governments and Europe must clearly outline its own policy – and practical activities – on topical cyber security questions. We have to understand that without an European cybersecurity industry there will not be a credible European cyber security. This is the only way to securing the European cyber future.

ARTICLE

Karen Lawrence Ökvist,
CEO,
PrivaSee

Welcome to the World of Data Protection

PrivaSee is launching an online data protection learning portal. One part of it is the EU Data Protection Digital Fact Card, which is a quick reference source on privacy and data protection fundamentals. Have a sneak peak at the OECD principles:

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate with the knowledge or consent of the data subject.

Collect only the personal data which is necessary for the specified purpose (see the Purpose Specification Principle) and you need to get consent from the data-subject! In practice this could be the insertion of a tick box in a mobile app you've built which the user should select in order to agree that you can collect, store and use their personal data for the purposes specified in the privacy notice. This privacy notice should be clearly marked and hyperlinked from where the user gives consent.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Now this should not be confused with the integrity part of the CIA (confidentiality, integrity, availability) information security triad. In this context data quality is about the quality of the contents of the personal data not about protecting its integrity which is covered in the Security Safeguards Principle. Personal data often changes with time. The easiest way to keep personal data updated is to give the user direct access with rights to update.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as not incompatible with those purposes, and as are specified on each occasion of change of purpose.

This is a useful principle you can use to scope your data protection project. What is the purpose for the collection of personal data? Using this as your flashlight, you can keep focus. There could be more than a single purpose, and each needs to be carefully identified and scoped so that your purpose falls in a natural alignment with the Use Limitation Principle. If after the original assessment personal data collected is to be used for another purpose outside of the original purpose, e.g. marketing, you must get additional consent from the data subject.A clear and defined purpose(s) will reflect in your Privacy Notice (Openness Principle) which is where your purpose(s) for personal data collection are communicated with your customers.

Using this as your flashlight, you can keep focus.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except (a) with the consent of the data subject; or (b) by the authority of law.

Top 10
of 64 speakers.
Congratulations, Karen!

Use Limitation may feel like the same as the Purpose Specification, but it is not. As stated the Purpose specifies what you are using personal data for, and the use is basically how you do this. For example an individual orders a book on amazon.com. The Purpose is that personal data collected is used purely for the purpose of fulfilling the order. This means that the department responsible for the delivery of the order receive only personal data needed to get the book to the customer, i.e. name, address, book ordered delivery choices. There may be additional personal data collected for the purpose of giving a harmonious user experience, and involves placing of cookies to store the customer's buying habits. This is not needed for delivery, this is used by marketing, and so on...Hence each use needs to be stay within the boundaries of each specified purpose.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure.

Without information security there is no privacy. What you should be looking for is evidence of an ISO27x audit and/or certification, a technical security report on the cloud service, including details on how personal data is protected on a cryptographic level. Additionally you would want to see evidence that security SLAs are in-place for outsourced and cloud services, and compliance with local laws and regulations and relevant industry specific standards such as PCI-DSS.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

This is where the privacy policy/notice comes into play. It is the communication channel for the Data Controller/ Processor to communicate with customers on privacy practices followed. It is an opportunity to present the ethics of your organisation on personal privacy. The new Data Protection Regulation makes it a requirement that your Privacy Notice should be clear, understandable and easy to read, even when the target audience is children. By the way as a side -bar there is a provision for the requirement of parental consent for minors (under 13 years) in the new Regulation.

Without information security there is no privacy.

Individual Participation Principle

An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him, within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

You need to have the processes and security in place to be able to fulfil the rights of the data subject: There must be complete transparency between you and the data subject concerning personal data that and what you are storing; You must have the security mechanisms in place to enable transparency to ensure that the individual making the request is actually who they say they are; and The data subject should know who and where to contact in order to fulfil the request.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

You as the Data Controller must have the documented processes and procedures, i.e. evidence that you are following the principles. A Privacy Impact Assessment (PIA) is good practice, which includes privacy risk evaluation, personal data flows and compliance with national data protection laws.

COPPERBERG

Copperberg
Sveavägen 159
113 46, Stockholm, Sweden

Phone: +46 8 650 02 70
Fax: +46 8 441 07 93
Email: info@copperberg.com
www.copperberg.com