Stjórnarráð Íslands
Samgöngu- og sveitarstjórnarráðuneytið

EVRÓPSKI NET-ÖRYGGIS-MÁNUÐURINN

Átak til eflingar netöryggis

með því að fylgja opnum fundum og námskeiðum ITU eftir hérlendis með fjarfundum til eftirfylgni hvers viðburðar

Hluti af átaki samgöngu – og sveitarstjórnarráðuneytisins í netöryggismánuðinum 2020 til eflingar netöryggis er að vísa á erlendar ráðstefnur og námskeið um netöryggi sem eru öllum opin og haldin án endurgjalds og gangast fyrir að haldnir séu fjarfundir hérlendis eftir hvern slíkan viðburð, þar sem viðeigandi aðilar geti tengt viðburðinn íslenskum aðstæðum, átt samtal og ákveðið næstu skref til eftirfylgni eftir því sem við á. Kjörorð ráðuneytisins í þessum mánuði er að **netöryggi sé okkar allra**, við verðum öll að vera virkir þátttakendur í þessu starfi. Þess vegna leitast ráðuneytið við að fá fleiri til liðs við sig til að sjá um fjarfundi til eftirfylgni hvers viðburðar og taka virkan þátt í þeim. Markmiðið er ekki að kryfja mál til mergjar á þeim stutta tíma sem er til umráða, heldur að vekja umræðu sem vonandi heldur áfram eftir því sem við á.

Fyrsti viðburðurinn í þessari syrpu er fjarráðstefna um eflingu kvenna innan netöryggis, *Empowering Women in Cybersecurity,* þriðjudaginn 6. október nk. Þeirri ráðstefnu verður fylgt eftir, samdægurs, með íslenskum fjarfundi í umsjón Ástu Láru Magnúsdóttur og Kristjönu Bjarkar Barðdal, *Tækifæri kvenna tengd netöryggi*, sjá nánar:
https://www.stjornarradid.is/raduneyti/samgongu-og-sveitarstjornarraduneytid/radstefnur-og-fundir/taekifaeri-kvenna-tengd-netoryggi/

Nánari upplýsingar um dagskrá netöryggismánaðar í heild má fá á eftirfarandi netsíðu (sem er uppfærð reglulega):
https://www.stjornarradid.is/verkefni/samgongur-og-fjarskipti/netoryggi/#Tab4
Þar er einnig að finna upplýsingar um hvernig eigi að skrá sig inn á viðburði ITU til að geta fylgst með þeim. Þátttöku í íslenskum eftirfylgnifundum þarf að skrá sérstaklega og upplýsingar um skráningu eru veittar á vefsíðunni fyrir hvern fund.

Upplýsingum er einnig miðlað með tístum á Twitter undir merkingu **#netöryggi**

Í eftirfarandi samantektum er notað efni um viðburði ITU, fengið af eftirfarandi yfirlitssíðu og viðeigandi undirsíðum (enskur texti):
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020GCD_Calendar.aspx

A. Vefráðstefnur ITU

Vefráðstefna #1: *Empowering Women in Cybersecurity*

Þriðjudagur 6. október, kl. 12 - 13:30

Dagskrá:

Keynote by Doreen Bogdan-Martin, BDT Director, ITU

Setting the Context and Moderation

Ms. Natalia Mochu, Regional Director, ITU Regional Office for CIS

Speakers

Ms. Natalia Spinu, Chief of Cyber Security Center CERT-GOV-MD, Moldova
Ms. Diana Waithanji, Cybersecurity engineer and Founder of STEM Wahandisi La Femme, Kenya
Ms Abeer Khedr, Chief Information Security Officer, National Bank of Egypt
Ms. Louise Marie Hurel, Cybersecurity and Internet governance Researcher, Igarapé Institute, Brazil
Ms. Min Livanidis, Advisory Board Chair of the Oceania Cyber Security Centre , Australia
Ms. Prity Khastgir, IP Attorney, India

Vefráðstefna #2: *Cyber crisis management planning: How to reduce risk and increase national cyber resilience*

Fimmtudagur 8. október kl. 12:00 – 13:30

Dagskrá:

Setting the Context and Moderation:

Prof. Dr. Marco Gercke, Director, Cybercrime Research Institute

Speakers:

Ms. Lara Pace, CyberSecurity Consultant
Mr. Luc Dandurand, Head of Cyber Operations Guardtime
Dr. Jamie Saunders, Oxford Martin Fellow, Global Cyber Security Capacity Centre (GCSCC), University of Oxford
Mr. Adnan Baykal, Technical Advisor, Global Cyber Alliance
Ms. Indrani Chandrasegaran Kermorvant, Managing Director, Accenture Security
Mr. Adli Wahid, Senior Internet Security Specialist, APNIC

Vefráðstefna #3: *National CIRT, Measuring and Improving Maturity*

Þriðjudagur 24. nóvember, væntanlega 13:00 – 14:30 (uppgefinn tími 12:00 – 13:30 er væntalega rangur, því ekki virðist hafa verið tekið tillit til breytingar yfir á vetrartíma á meginlandi Evrópu)

Dagskrá:

(ITU mun kynna dagskrá síðar)

B. Námskeið ITU

Námskeið #1: *How to conduct effective Open Source Investigations Online*

Efni námskeiðs:

Open Source Intelligence (OSINT) is the collection of publicly available information to be analyzed and transformed into actionable intelligence. The Internet contains large amounts of open source information which, if adequately collected and analyzed following structured methodologies, may be of support as part of the cyber incident response actions by CERTs/CSIRTs. The session will stress the importance of CSIRT-law enforcement cooperation during the response to cyber incidents.
This session is provided by the United Nations Counter Terrorism Centre (UNCCT) of the UN Office of Counter Terrorism (UNOCT), under its Global Counter-Terrorism Programme on Cybersecurity and New Technologies. The Programme assists Member States in raising awareness of the terrorist cyber-threat and in enhancing their technical capacities to prevent and respond to the new threats.

Um leiðbeinanda:

Mr. Vytenis Benetis is a consultant working for UNOCT/UNCCT, and the Director of i-intelligence in Asia. Vytenis has worked as an intelligence analyst for almost a decade. His professional experience covers a wide range of missions and organisations including the Lithuanian Ministry of Defence, NATO, and the European Union on both the operational and strategic level. While working as an analyst, and later as a team leader, Vytenis developed practical solutions to tackling large information flows and delivering actionable intelligence to senior decision makers. Vytenis has an extensive engineering academic background: he holds B.Sc. degree in Systems Engineering from the U.S. Naval Academy and PhD in Mechanical Engineering from the University of Maryland.

Námskeið #2: *Incident Response with TheHive and Cortex*

Efni námskeiðs:

1. Introduction
- HIVE – Central Case Management Platform
- Cortex – Analyzer and Responders for automation
- Case template – SOP steps analyst takes when attack happen
- Collaborate
- Elaborate
- Analysers & Responders – Create SOAR

2. Architecture
- Explain Hive and Cortex Architect
- Workflow for Case Templates

3. Demonstration
- Creating workflows and case Templates for task automation
- SOC-Analyst working on task/case
- Identification
- Ticketing
- Incident Response
- Reports

Um leiðbeinendur:

Navin Kaul is Director with EY and has more than 13 years of experience large projects for various Government clients in the area of Security Governance and crisis management, SIEM and CERT. He has supported multiple government organizations across multiple countries in implementation & administration of Information Security ,Network Security, new cyber security initiative.

Santhosh Kumar R is Consultant with EY and has hands on experience in Red Teaming/Incident Response and Security operation centre. He has led multiple incident response engagement and Red teaming with Open Source tools. He has performed various Incident Response and Forensic for multiple Global organizations and helped them contain and mitigate critical breaches, while he has also helped in early detection of advance threats. He is Offensive Security Certified Professional(OSCP), Offensive Security Certified Expert(OSCE), CREST Registered Tester(CRT), Crest Security Analyst (CPSA) and, Certified Red Team Expert(CRTE).

Námskeið #3: *Communication in Crisis Management*

20. október kl. 12:30 – 15:00

Efni námskeiðs:

Building on experience from a large number of real events, this workshop will give the participants practical hints on how to prepare for and communicate in the event of a cyber crisis.

The workshop will be grouped around three lectures:

- Why crisis communication is increasingly important; defining the standard we need to aim for in our response
- How you can prepare for crisis communication; sharing best practice processes
- What you should do in terms of communication practice in a crisis situation; explaining the best practice actions and behaviours.

Um leiðbeinanda:

Both as a consultant and as a client-side executive, **Roll Olsen** has been involved in high-profile complex crises events. He lectures crises management regularly at the Graduate Institute in Geneva, and advice clients on crises related matters on a daily basis.
Rolf Olsen launched the communication consultancy Leidar in 2010 and continues to lead the company with a clear focus on clients. Leidar has offices in Geneva, London, Brussels, Dubai and Oslo.
Before setting up Leidar, he was CEO Continental Europe of Weber Shandwick, on the world´s largest PR agencies. Prior to this he held executive positions at both European and global level for two American Fortune 50 technology companies; firstly 13 years with Digital Equipment Corporation and then five years with Motorola. Before he moved to Geneva in 1989, he was the Marketing Communications Manager for Digital Equipment Corporation in Norway, night editor in the daily newspaper Nationen, Public Relations Manager at the Norwegian Association of Disabled Persons and information officer in one of the political parties working the Norwegian Parliament.

Námskeið #4: *Industrial cybersecurity and incident response*

Fimmtudagur, 22. október, kl. 12-14:30

Efni námskeiðs:

In recent years the number of cyber incidents involving a variety of digital industrial systems in the energy, oil and gas sectors, transportation, production, government, and other critical sectors has dramatically raised.
The digitalization and global interconnection make it difficult to operate security measures in an old fashioned manner and based only on preventive security controls without considering incident response strategies and plans.
Moreover, existing incident response models for the classical IT environment are not ideal and optimal for complex industrial environments, thus they should be adjusted considering the operational technologies features.
This training will touch critical points on discussion about the difference of IT and OT, roles and responsibilities within the incident response process as well as cover all necessary phases of incident response according to existing standards.

Outline:
Section 1: Industrial cybersecurity challenges
Section 2: Incident Response overview
Section 3: Preparedness and prevention
Section 4: Detection
Section 5: Analysis
Section 6: Containment
Section 7: Investigation
Section 8: Eradication
Section 9: Recovery
Section 10: Post-Incident Activity

Um leiðbeinanda:

Dmytro CHERKASHYN holds a M.Sc. degree in nuclear energy from the Sevastopol National University of Nuclear Energy and Industry, Ukraine, with specialization in physical protection of nuclear facilities, nuclear materials, radioactive wastes and other radioactive sources.
Dmytro has more than 10 years extensive practical experience on securing the critical infrastructure facilities against malicious acts as well as delivering university lectures and specialized trainings in cyber security.
Being security scientist in the Institute for Securtity and Safety at the Brandnburg University of Applied Sciences, Dmytro involved in many international activities, real-life technical assessments and reasearch projects within the cyber security topic.

Námskeið #5: *Cyberthreats and Social Media*

Þriðjudagur 17. nóvember kl. 13:30 – 16:00

Efni námskeiðs:

(ITU birtir lýsingu á námskeiði síðar)

Um leiðbeinendur:

Navin Kaul is Director with EY and has more than 13 years of experience large projects for various Government clients in the area of Security Governance and crisis management, SIEM and CERT. He has supported multiple government organizations across multiple countries in implementation & administration of Information Security ,Network Security, new cyber security initiative.

Mittal Mehta is Sr. Manager with EY and has more than 12 years of experience in Security Consulting. She manages Cyber Threat Intelligence Service at EY India. She has extensive experience in designing and building Threat Intelligence Program and platform, Evaluation of technologies needed for tactical threat intelligence integration/analysis. She also has hands on experience in Cyber Footprint Assessment- Crawling publicly available information as well as information available from deep/dark web that could be leveraged by cyber adversaries. She has led multiple projects for Identifying security threats and business risks and reputation based attacks on social media and digital channels. She is certified in Cyber Threat Intelligence by GIAC, and also Certified for SANS-GWAPT.

Námskeið #6: *Practical Cyberthreats Intelligence and Information Sharing using MISP*

Fimmtudagur 19. nóvember kl. 13:30 – 16:00

Efni námskeiðs:

(ITU birtir lýsingu á námskeiði síðar)

Um leiðbeinanda:

(ITU birtir lýsingu á leiðbeinanda síðar)