Workshop 2 ‘How to Make Cloud Services Secure’
Tuesday 3/11 14.00-16.00 CET

Description
This two-hour workshop will address what actions can be taken, and what approaches and tools are available, to increase security in a world where cloud services rule - examples are Microsoft’s 365 and Amazon services. What is the role of, and how to best set up security centers? What can be done to prevent, detect, resolve security breaches? How to set priorities in security policies? How to use offerings by cloud service providers to improve our security? The introductory talk will be delivered by Jeroen Vandeleur. The discussions will address technical and implementation issues. If terms like ‘MISP’, ‘DKIM’ and ‘SPF’ ring a bell, this workshop is for you.

Audience
CIO’s, security officers involved in the technology behind secure cloud service delivery

Preliminary programme:
Walk in from 13.45
Start workshop 14.00

1. Welcome and introductions (10 minutes)
   Thorsten Küfer, Asbjørn Thorsen - EUNIS

2. Introductory talk 'Incident Response in the Cloud: Foggy with a Ray of Sunshine' (30 mins)
   Jeroen Vandeleur, Service line lead Cloud Security, NVISO, Belgium
   “Over the past few years, we have seen organizations move a part of, or even their entire infrastructure, to the cloud. With on-premise infrastructure, it used to be clear that the security needed to be taken care of by the organization itself. With cloud infrastructure, there is quite some confusion about who takes care of which security controls. This confusion has led to several painful incident response cases where we were called in only to discover we hardly had any data to work with.
   Three common problems with incident response in the cloud - lack of knowledge, increased response times, lack of resources - will be highlighted. We will look how we can purposely use what cloud providers offer us to improve our security operations.”
3. **Interaction and exchange** (45 minutes)

   a. **Inventorial Zoom polls** each poll followed by a 5 minute reflection/discussion
      1. Are you looking to migrate critical services in cloud environments?
      2. Is a shared responsibility mode an absolute requirement when ordering cloud services?
      3. Do you prefer bigger Cloud service providers such as Amazon, Microsoft and Google

   b. **Menti meter inventory** - menti.com, then code 61 70 35 2
      each question followed by a 15 minute reflection/discussion
      1. What are the most frequent technology/implementation issues?
      2. Which existing cloud tools/services helped to meet security demands?

   c. **Sharing experiences** What are participants views (35 minutes)
      1) Ordering cloud services is so easy that every department can do this, we see that many of the services running in cloud environments are not managed centrally. How do you approach this problem?
         • Problem of easy ‘credit card’ purchases, central IT too slow.

      2) Discussion about new attack vectors/risks, a new way of security testing when going to the cloud? What are some of the main security risks when you are thinking about cloud solutions?
         • Anti-virus software via the cloud?

      3) What would you prefer?
         a) using as much cloud services as possible and limit your responsibility (SaaS solutions - ‘just eat the pizza’)
         b) remain party in control and deploy virtualized environments (PaaS ‘order the pizza to be delivered and eat’, IaaS ‘bake and produce the pizza’).

      4) A particular good cloud tool/service or policy/approach that helped increase security? e.g., MISP (Malware Information Sharing Platform, [https://www.misp-project.org/](https://www.misp-project.org/)), ATP (Advanced Thread Protection), CASB (Cloud Access Security Broker)
         • How to integrate into Office365
         • Set up SPF, DMARC, DKIM (Mailing list problems, sub domains)
         • ActiveSync not advised

      5) Has a particular Security challenge or incident happened within your institute/region?

      6) **[ONLY IF THERE IS ENOUGH TIME]** What about privileged access management?
a) are you going to rely on cloud security controls (such as conditional access, express route and Privileged access workstations) or
b) do you still want to limit connections (VPN to cloud environment / express route)?

4. **Wrap-up and close** (10 mins)

   a. **Brief check** on possible next steps
      1. conclusions, recommendations?
      2. Possible next steps for participants, the SIG?
      3. Preferred topics for future 2 hour workshops?

   b. **Closing Zoom-polls** on the work of the SIG (5 mins)
      1. This 2 hour workshop has been worth attending?
      2. I’d prefer a chat-tool like Signal or DeltaChat for communication between SIG members?

End of workshop 16.00

Registration

[https://us02web.zoom.us/meeting/register/tZUkf-ysqDssE9MqKsWVaLSq2edx6z70YdqO](https://us02web.zoom.us/meeting/register/tZUkf-ysqDssE9MqKsWVaLSq2edx6z70YdqO)