Notes on 2 hours EUNIS workshop

‘How to Make Cloud Services Secure’

Organised by: SIG Information Security and GDPR
Date and time: Tuesday 3/11 14.00-16.00 CET
Attendees: 21
Introductory talk: Jeroen Vandeleur - Service line manager Cyber Architecture and Cloud Security, NVISO, Belgium

Introductory talk ’Incident Response in the Cloud: Foggy with a Ray of Sunshine’
Slides: https://www.eunis.org/wp-content/uploads/2020/11/NVISO-IR-in-the-cloud-Foggy-with-a-ray-of-sunshine-v2020.pdf

In his talk, Jeroen Vandeleur firstly addressed a real-life example.
‘Design security for cloud services’ should start with multi factor authentication to not get in the wrong people; filtering network traffic using network security tools to avoid being hacked; use role-based access rather than local accounts and with a centralised authentication platform be able to monitor logins; and turning on all facilities for logging user activity, data flows, server operations. If you don’t you are vulnerable and have a high probability to be attacked.

‘Cloud Security Incident Analysis’. When attacked, check (for Azure: the NSG Flow) logs of incoming and outgoing traffic to identify origin and impact of the incident; do a check on loss of sensitive data, using (SQL Server Audit); check which users are impacted (AD sign ins) via the central authentication platform; check the system logs for suspicious actions. If you have not enabled all these logging functions - and your response to the attack is to shut down all systems, you are in deep trouble. But if you have secured the logs, you can create a timeline of what happened.

‘Main challenges during Incident response’ are: traffic filtering and availability of logs (see above) - in particular long retention of logs is important to be able to spot the first instances of attack preparation; access management (see above); insecure host configurations - sometimes it’s too easy to take over control of servers; identification of the resource owner - you need to know who in your organisation, using a credit card, bought and implemented the cloud service.

‘Security monitoring toolset’ Jeroen briefly went through solutions for Microsoft Azure and Amazon AWS re identity and access policies; centralised access and built-in alerts; firewalls; user activity tracking (Office 365 has Unified Audit Logs, very useful but not enabled by default!) and more.

‘Centralised Cloud logging’ Jeroen demonstrates how agents can do the various monitoring activities into a Log Analytics Repository and combine/analyse these in alerts, dashboards, et cetera (in both Azure and AWS). It is recommended to start at the basics - logging identity and access, network and systems flows. Additional monitoring steps can be taken once the basic logs are ok.

'Automation of incident response' is the next step. Cyber-attacks present a 'Whack-A-Mole' challenge, the moment you beat one attack, another attacker pops-up. This is due to lack of resources to beat them all; a constant increase in the number of tools that do not work together; Security Operation Centers (SOCs) are overwhelmed and their operations are static; detection speed is too low (206 days on average!). Therefore SOCs should be equipped with an OODA loop (Observe, Orient, Decide, Act - the first two can be automated, the last two require human interference). Examples of automated scenarios and actions are presented. An important action is to move infected servers to an Incident Response subnet for investigation. An overview of automation tools is shown, and demonstrated. The example script that we used is downloadable on our github repository: https://github.com/NVISO-BE/cloud-security-automation

'In summary'
The challenges are Resources, Tools, Events, Static and Speed. The responses are Automation, API Calls, Intelligence, Community and Centralised approaches.

'Round of questions'
Thorsten Küfer comments that all should be aware that on premise security still is a little easier to work on than really entering the cloud for secure university services. Asked about the testing and alert settings in the scripts, Jeroen explains that whenever possible this is done in a testing environment but if caught in a real incident you may have to work in the real environment. In many cases you can select 'monitor but do not execute the designed action'-mode.
Denise Dittrich raises the question how central IT can arrange for automation if the resources are not centrally owned. Jeroen promotes the approach to update all security measures prior to letting new services go into production. Central IT should have sufficient access to distributed services to manage the security - distributed service management can still control subscriptions.
Rolf Bjornskau signals that when going to the cloud some years ago, this was seen as an opportunity to bypass central IT, and consequently was not giving priority to security, How in such a situation can we correct this. Jeroen points at ARM (Azure Resource Manager) templates (similar things are available in AWS) where you can define exactly what you want the infrastructure to look like, and have ARM policies that you can apply, to check if you are compliant to what you have set-up with regard to security. So if for instance a new server is planned to be installed, such templates combined with centrally known vulnerabilities that could occur with this particular server, you may discover if sufficient security measures have been taken. For a big part it is an organisational challenge - developers must learn that also outside premises, central security approaches are important.

Interaction and exchange

- The majority (around 75%) of participants is seriously planning to migrate critical services towards cloud environments, so talking about security aspects does matter.
- Almost all attendees see a shared responsibility mode (for instance when you make use of PaaS of SaaS) an absolute requirement when ordering cloud services. Shared means that not only you as a cloud customer but also the cloud service provider is responsible to ensure security, with clarity who is responsible for which parts. Jeroen especially points to examples like HR

departments, or small organisations, buying and using software that often relies on a website of which it is unclear if it is monitored for, and reporting about breaches.

- The majority (70%) indicates to prefer bigger Cloud service providers such as Amazon, Microsoft and Google over smaller ones. However, with the new legislation coming into effect it is no longer a matter of size but of location - the appetite for non-american, European solutions will grow. Bigger companies still tend to have more capacity to act if things go wrong. It is noted that preference for a provider also depends on the type of cloud service - there is a big difference between a large infrastructural service and a more specific service. In the latter case, smaller providers tend to be more flexible, e.g to adapt to legal changes, than the larger ones. Receiving a response to individual cases from larger cloud providers is difficult. There is a need for a European approach, like we managed to do with GALILEO in response to GPS, political and financial support for regional/European companies could help.

Sharing experiences

Asbjorn Thorsen shares possibilities and experiences with security of Microsoft Office365. For protection of O365 mailboxes the Exchange Online Protection (EOP) is used effectively for base layer security measures: configuring filtering and rules for connection, malware and spam. For protection of O365 services the Advanced Threat Protection (ATP) can be used to configure policies for safe links, safe attachments, SPF records, DKIM, DMARC and anti-phishing policies. These safe links option proved to be too complicated, so it is not used. O365's Identity Protection's multi-factor authentication has been rolled out for all users, and no-one complained. Various Information Protection policies are available in O365, such as Data Loss Prevention but these have not yet been tested.

SPF (Sender Policy Framework) allows you to publish authorised mail servers to avoid spam being sent on your organisation's behalf; DKIM (Domain Keys Identified Mail) adds a digital signature to each email you sent, so the recipient's email server can check if it indeed comes from you. On top of SPF and DKIM, DMARC (Domain-based Message Authentication Reporting and Conformance) can be used for email validation. This works well, except for 3rd parties sending emails on behalf of the sender). DMARC's XML-based daily aggregate reports and real time MARF-based Forensic reports can be interpreted and visualised by the Dmarcian DMARC Inspector tool.

Lessons learned on using the O365 tools: they work well, provide almost too much functionality, and if not used exactly right you will remain as vulnerable as before. The amount and complexity of what you need to know, learn and apply is big, and it takes much effort to get things working but given the danger it was worth the initial investment and we are now able to fill in the blanks. Each week three morning meetings take place to monitor if applied policies are working well. Next step is to ensure our O365 and other universities' O365 policies are connected.
Questions and issues left: O365 is not flawless and it changes all the time as do the licences; sending employees to training courses is recommended. As a consequence of the end of the Privacy Shield - can we continue to use O365?
To get to where we are now we used a step-by-step course on configuring and managing O365 security provided by Plural Sight. Other useful links:
https://protection.office.com/
https://securitycenter.windows.com/

https://portal.azure.com/
https://dmarcian.com/

It is noted that SPF and DKIM are not limited to be used with O365. More than half of the audience uses O365. Denise Dittrich explains that at Aachen University students can use nearly all of the functions in O365. Exchange Online is not part of this, as Aachen uses an on-premises exchange system, for employees it's only Teams. Zoom is used for education and teaching. Thorsten informs that Muenster University has a license for O365 but is hardly using it, Exchange is used on premises, not online.

Methods are needed to prevent employees from procuring and start using services that attract users without checking/solving the security risks. Jeroen explains that 'conditional access', so a list of conditions that have to be met, is a possible method. There are also cloud security access brokers (CASB) who can help out, e.g. telling you which users use which cloud services, or checking if files that users upload from Dropbox are indeed safe to share. Another option are trust-based access policies: fully trusted, semi trusted or non-trusted users that each have specific rights/conditions re their access and behaviour. Example is Jeroen's phone, which is a semi-trusted device - he totally owns it, can install and use services as he likes but when he wishes to access the NVISO cloud services he must use a specific piece of software on top of that, so if the phone gets lost it cannot be used for malicious means.

NVISO counts at least one breach of security a week within its O365 customer base, mostly these are compromised accounts - use of two-factor authentication can take out 90% of these.
Asbjorn found that some cases using the legacy protocol ActiveSync makes normal credentials work without the second factor, so you have to disable it, or use conditional access as a workaround. Rolf warns that older versions of O365 install the legacy authentication by default, and when installing modern authentication, you must indeed actively disable the old ones, such as ActiveSync, POP3, etc. You can do that in the admin part, the organisational settings - in fact you need to configure modern authentication for your Outlook client, to work together with enabled two-factor authentication.

Matija Puzar asks if others use DMARC and what policy 'deny' or 'reject' they apply for employees subscribing to newsletters of other institutions. The external newsletters are often a reason not to use DMARC. Asbjorn suggests an approach to use an alias-email address, e.g. myname[at]lists.myuniversity.my country, and use this for all newsletters and then set.up DMARC for that 'lists' domain. Consequences are that these email addresses will receive the spam, and that users must know and remember about this separate email addresses, when subscribing. Also, there will be many lists they have already subscribed to. *Risto Rahu* of Tartu University informs that they work on a solution to add headers to such incoming newsletter messages.

Wrap-up and close

Thorsten concludes that managing cloud security stuff is more complex than it seemed at the start - the logging and managing of these, and trace back back in case of incidents requires a lot of preparation - not only online but also on premises. This takes a lot of staff time. There is a need to know what your users are doing, what cloud services they buy and often you'd want to be quicker, providing a safe solution yourself. It would be preferred to manage these centrally to arrange for safe use.

With regard to the need for European solutions, perhaps on the IaaS (infrastructure) level there are good non-US alternatives, e.g. Deutsche Telekom. For PaaS (platform) level, there are no clear alternatives to Azure/O386 or AWS/Amazon.

Inventorial Menti-poll about the workshop

Q1. Why has this 2 hours workshop been worth attending?

Most answers indicated that hearing about what others are doing is appreciated, as well as getting an overview of basic cloud services, their use and the monitoring which is complex. Also mentioned is that we get into detail on how Azure and O365 work, and share our challenges and tips.

Q2. What can we do to improve the workshop next time?

Suggested is to have (break-out rooms to) discuss topics in even more detail; have more time for questions; set-up a demo account to validate some recommendations; concrete tips on configuring O365 mail protection against phishing and spam; have similar dedicated workshop on Amazon/AWS (as this one was on O365/Azure)

Thorsten shares the idea that the more regular exchange calls will be planned for the SIG, so members can get or stay in touch, discuss whatever they like, address issues, ask questions without agenda, about once every two months. Invitations will be sent to the list.

Q3. Do you prefer a chat-tool like IRC, Mattermost, Signal or DeltaChat for communication between SIG members?

Like in the workshop a week ago, participants in majority would like to give such a chat tool a try.