RIK VAN DUIJN - 19 AUG 2021

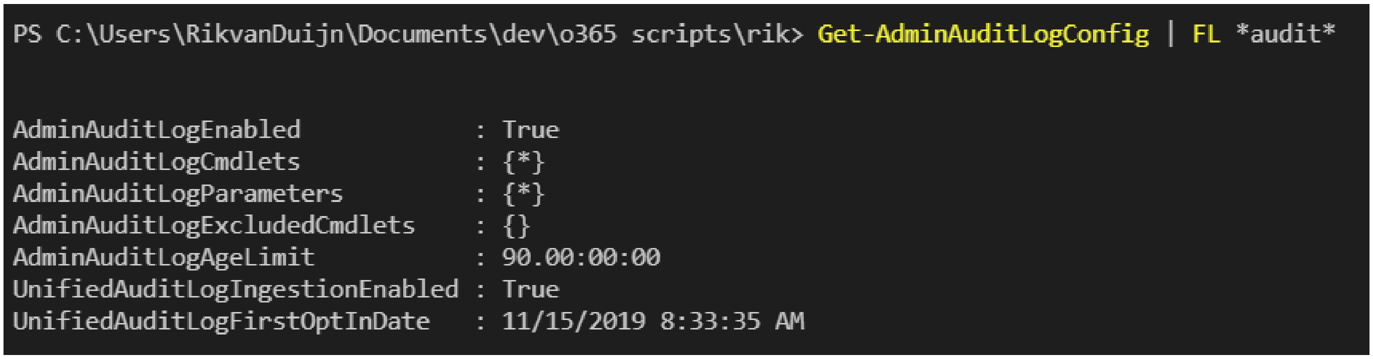
OFFICE 365 AUDIT LOGGING

It's important to enable audit logging for o365 even if you are not monitoring them actively. Atleast if you get hacked there's logging to investigate :). The audit log is not always enabled by default, it seems to rely on license levels. However there are some important things to take into consideration.

You can enable the unified audit log and be done. However there are some things to take into consideration. Especially when it comes to mailbox operations and logging. Office 365 audit logging can be tricky to manage. There's some things you need to be wary of when relying on the o365 logging. Essentially we need to make sure Unified Audit log is enabled and the mailbox audit settings are set correctly.

UNIFIED AUDIT LOG

The unified audit log is a combination of logging from SharePoint, Exchange Online, Teams and more. If you use o365 just make sure to enable it. It can be checked using "Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled". Enabling can be done via: "Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true"



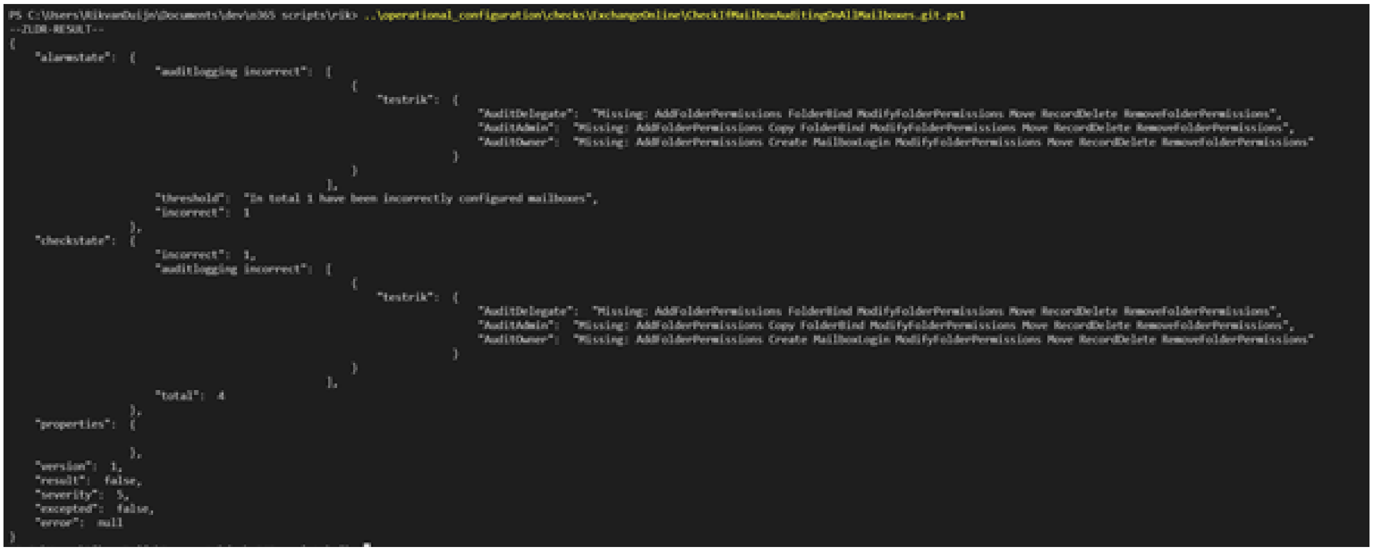
```
PS C:\Users\RikvanDuijn\Documents\dev\o365 scripts\rik> Get-AdminAuditLogConfig | FL *audit*


AdminAuditLogEnabled             : True
AdminAuditLogCmdlets             : {*}
AdminAuditLogParameters          : {*}
AdminAuditLogExcludedCmdlets     : {}
AdminAuditLogAgeLimit            : 90.00:00:00
UnifiedAuditLogIngestionEnabled : True
UnifiedAuditLogFirstOptInDate    : 11/15/2019 8:33:35 AM
```

Make sure you can detect any modifications to the UnifiedAuditLogIngestionEnabled setting.

MAILBOX AUDIT SETTINGS

Mailbox Audit settings describe which operations on the mailbox are logged. Unfortunately we cannot set a standard set of operations that are logged for every mailbox. This forces the administrator to set them per user. After a new mailbox is created we need to set which mailbox operations are logged. Which audit operations are set seems to depend on the license level (business vs e3 vs e5).

Let’s say we create a new user the following auditoptions are set:



```
PS C:\Users\RikvanDuijn\Documents\dev\o365 scripts\rik> ..\operational_configuration\checks\ExchangeOnline\CheckIfMailboxAuditingOnAllMailboxes.git.ps1
--ZLDR-RESULT--
{
    "alarmstate":  {
                       "auditlogging incorrect":  [
                                                      {
                                                          "testrik":  {
                                                                          "AuditDelegate":  "Missing: AddFolderPermissions FolderBind ModifyFolderPermissions Move RecordDelete RemoveFolderPermissions",
                                                                          "AuditAdmin":  "Missing: AddFolderPermissions Copy FolderBind ModifyFolderPermissions Move RecordDelete RemoveFolderPermissions",
                                                                          "AuditOwner":  "Missing: AddFolderPermissions Create MailboxLogin ModifyFolderPermissions Move RecordDelete RemoveFolderPermissions"
                                                                      }
                                                      }
                                                  ],
                       "threshold":  "In total 1 have been incorrectly configured mailboxes",
                       "incorrect":  1
                   },
    "checkstate":  {
                       "incorrect":  1,
                       "auditlogging incorrect":  [
                                                      {
                                                          "testrik":  {
                                                                          "AuditDelegate":  "Missing: AddFolderPermissions FolderBind ModifyFolderPermissions Move RecordDelete RemoveFolderPermissions",
                                                                          "AuditAdmin":  "Missing: AddFolderPermissions Copy FolderBind ModifyFolderPermissions Move RecordDelete RemoveFolderPermissions",
                                                                          "AuditOwner":  "Missing: AddFolderPermissions Create MailboxLogin ModifyFolderPermissions Move RecordDelete RemoveFolderPermissions"
                                                                      }
                                                      }
                                                  ],
                       "total":  4
                   },
    "properties":  {

                   },
    "version":  1,
    "result":  false,
    "severity":  5,
    "excepted":  false,
    "error":  null
}
```

Checking mailbox audit settings

The different operations are documented here:

https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide

There are three different types of operations:

- Owner: The owner of the mailbox.

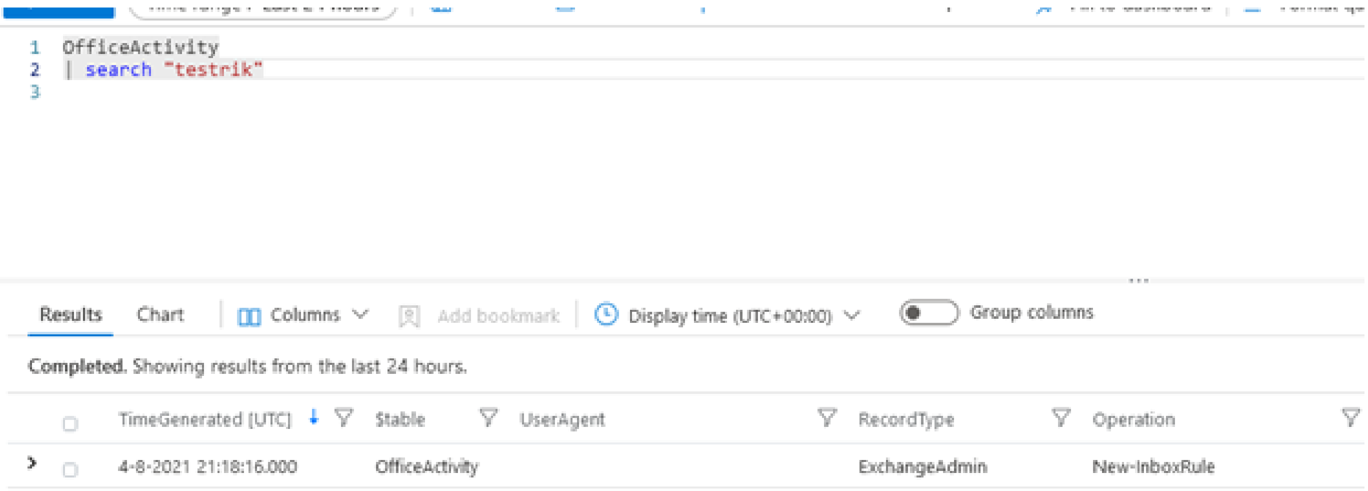
After creation of a new user some operations related to the user’s mailbox will not be logged by default. The following are interesting:

- Owner: MailboxLogin
- Delegate: Folderbind
- Admin: Folderbind

Folderbind: “A mailbox folder was accessed. This action is also logged when the admin or delegate opens the mailbox.”

Mailboxlogin: “The user signed into their mailbox.”

If we dont change anything and log into a mailbox and create a mailbox rule the following logs are created:



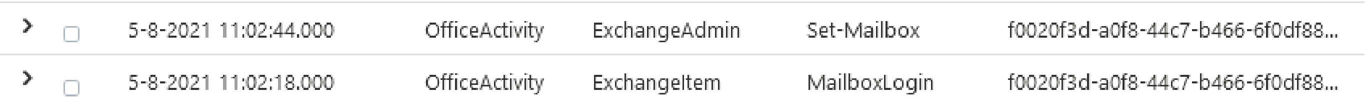
```
OfficeActivity
| search "testrik"
```

Completed. Showing results from the last 24 hours.

□	TimeGenerated [UTC]	$table	UserAgent	RecordType	Operation
□	4-8-2021 21:18:16.000	OfficeActivity		ExchangeAdmin	New-InboxRule

Default logging after account creation.

If we enable the MailboxLogin operations we can see the login operation and perfoming another, unrelated, action:



›	□	5-8-2021 11:02:44.000	OfficeActivity	ExchangeAdmin	Set-Mailbox	f0020f3d-a0f8-44c7-b466-6f0df88...
›	□	5-8-2021 11:02:18.000	OfficeActivity	ExchangeItem	MailboxLogin	f0020f3d-a0f8-44c7-b466-6f0df88...

Logging after we enable audit on all mailbox operations.

Note: *keep in mind that mailboxlogins != azureAD logins. So accessing other resources than mail will not be*

SUBVERTING LOGGING

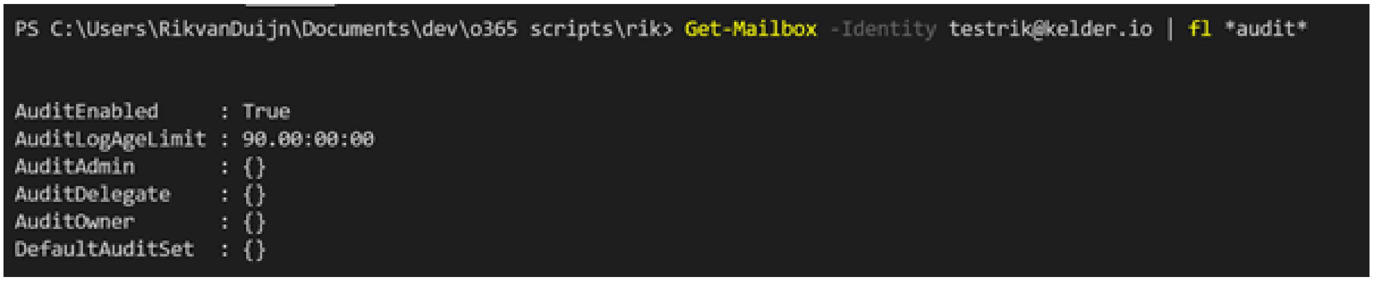
Attackers can try to subvert logging in order to obfuscate their actions.

UNSETTING AUDITOPTIONS TO PREVENT LOGGING

It's possible to unset all audit operations for a specific mailbox. Doing so will result in less logs however not all log operations will be hidden. After setting every audit option to zero we can still see mailbox rules being created and auto forwarding being set.

"Set-Mailbox -Identity testrik@kelder.io -AuditEnabled $true -AuditOwner @() -AuditDelegate @() -AuditAdmin @()"

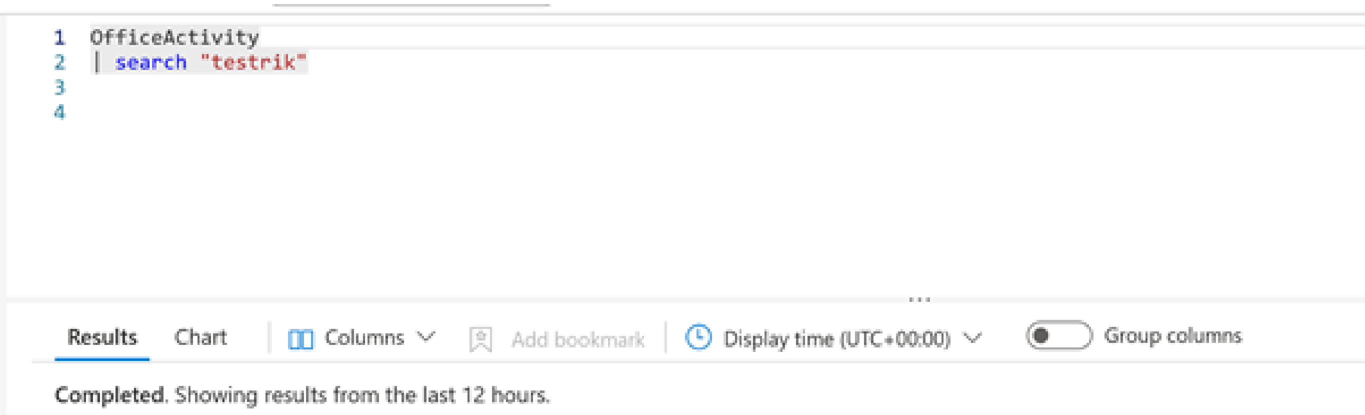
We can verify the audit settings are set to nothing:



```
PS C:\Users\RikvanDuijn\Documents\dev\o365 scripts\rik> Get-Mailbox -Identity testrik@kelder.io | fl *audit*


AuditEnabled     : True
AuditLogAgeLimit : 90.00:00:00
AuditAdmin       : {}
AuditDelegate    : {}
AuditOwner       : {}
DefaultAuditSet  : {}
```

All audit operations set to null.

The mailbox login is not logged, but rule creating and forwarding being set on the mailbox are. It seems there's always a default set of items being logged. It's not quite clear to me from available documentation what is in that default set, but I guess it's based on the type of license the user is assigned.



```
OfficeActivity
| search "testrik"
```

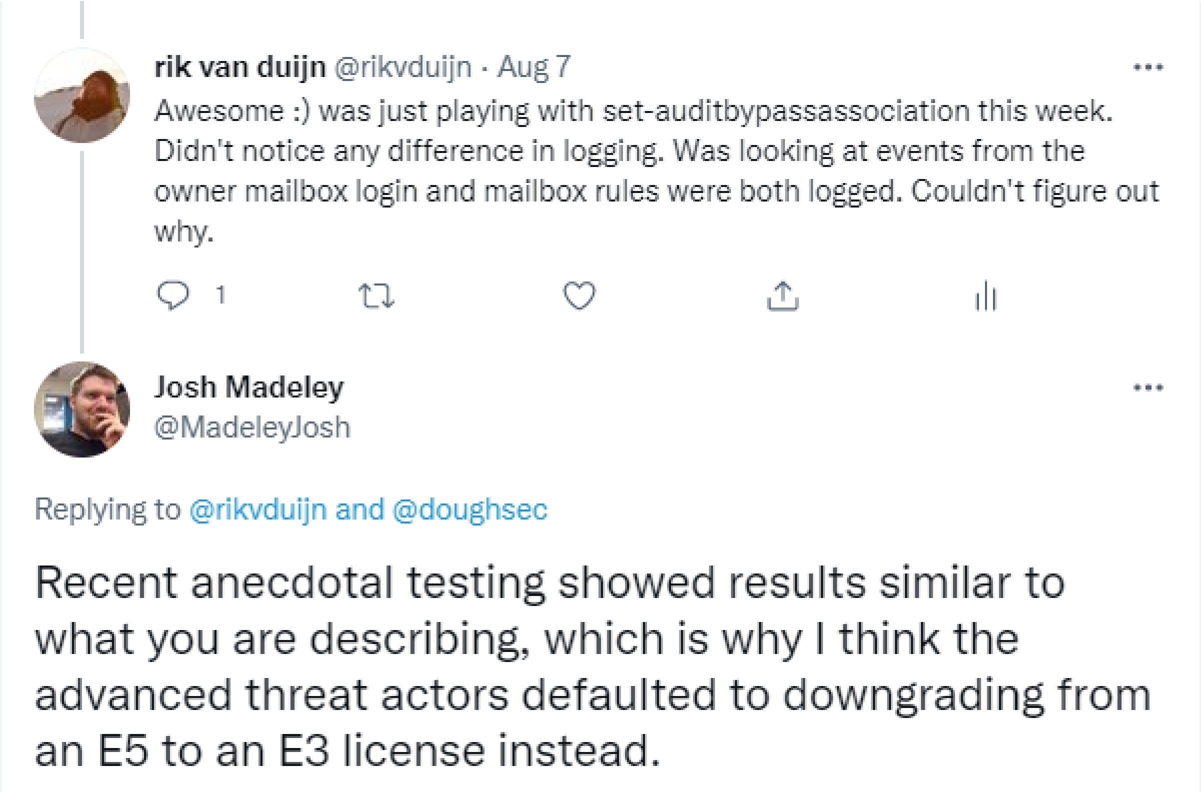
Completed. Showing results from the last 12 hours.

Logs after unsetting audit options.

SET-MAILBOXAUDITBYPASSASSOCIATION

Mailbox Audit Bypass according to the documentation should prevent activities from being logged. It's a technique that has been described in the BlackHat talk: "Cloudy with a chance of APT".

I tried setting the bypass on our test mailbox. Surprisingly, Audit logging kept coming in. I've asked one of the authors of the talk and it seems they've seen similar behavior. Still it's smart to keep track of the bypass association..



rik van duijn @rikvduijn · Aug 7

Awesome :) was just playing with set-auditbypassassociation this week. Didn't notice any difference in logging. Was looking at events from the owner mailbox login and mailbox rules were both logged. Couldn't figure out why.

Josh Madeley
@MadeleyJosh

Replying to @rikvduijn and @doughsec

Recent anecdotal testing showed results similar to what you are describing, which is why I think the advanced threat actors defaulted to downgrading from an E5 to an E3 license instead.

ATTIC AND LOGGING

Within the Microsoft365 module in Attic a tenant is monitored for different logging factors including the capability to automatically fix issues (pending user approval). In relation to audit logging we monitor the following

- Are there mailboxes with Auditbypass enabled

The following fixes exist:

- Enable unified audit log
- Correctly set mailbox audit settings

Want to know what it is we check and fix? Check our checks and fixes here. Or buy a subscription here.

FUTURE WORK

- Detect license downgrade as described in the BlackHat talk “Cloudy with a Chance of APT” By Doug Bienstock and Josh Madeley. https://www.slideshare.net/DouglasBienstock/bhusa-2021-cloud-with-a-chance-of-apt
- Figure out if AdminAuditLogExcludedCmdlets actually works, would be shitty to miss Set-MailboxRule or something like that.
- Create a fix to unset any Auditbypass. Not hard: Get-Mailbox -ResultSize Unlimited | Set-MailboxAuditBypassAssociation -AuditBypassEnabled $false
- currently working on an automated rollout of Sentinel including the OfficeActivity/AzureActivity connectors
- Figure out if setting AdminAuditLogEnabled to false is possible and results in no logging
- Investigate what is logged once a Graph app interacts with mailboxes

BLOGS

OFFICE 365 AUDIT LOGGING

RIK VAN DUIJN - 19 AUG 2021

It’s important to enable audit logging for o365 even if you are not monitoring them

RANSOMWARE, NATIONALE CRISIS?

ERIK REMMELZWAAL - 04 AUG 2021

Als er 1 digitale dreiging is die veel in het nieuws komt, dan is het ransomware. Er wordt zelfs gesproken van een nationale crisis. Lees verder

MIJLPALEN EN HOE HET GAAT

ZOLDER B.V. - 02 JUL 2021

Vandaag gebeurden er op Zolder toch een paar dingen die blogwaardig zijn. Dus prima aanleiding om nog maar eens de laptop open te klappen en te vertellen hoe het gaat. Nieuwe collega's Het is 1 juli 2021 en we zijn ruim een jaartje onderweg als Zolder. De belangrijkste stap die we vandaag zetten, is dat […] Lees verder

ZOLDER WORDT HOOFDSPONSOR HCZ

ZOLDER B.V. - 01 JUL 2021

Vandaag is bekend geworden dat Zolder de nieuwe hoofdsponsor is van HCZ – Hockeyclub Zevenbergen. De komende drie seizoenen zal het logo van Zolder daarom voorop de shirts van alle HCZ leden prijken. We zijn heel erg trots op deze nieuwe stap voor ons jonge bedrijf, en hopen zo de relatie met onze regio te […] Lees verder

BREDA ROBOTICS

ERIK REMMELZWAAL - 10 MEI 2021

Zolder BV is toegetreden tot het netwerk van Breda Robotics. Deze vereniging brengt organisaties bij elkaar die actief zijn rondom robotisering in de regio West-Brabant. Voor Zolder geeft Breda Robotics de mogelijkheid om samen te werken met de robotiseringsindustrie. Te begrijpen hoe die sector precies werk en op welke vlakken

27% .NL DOMEINEN SLECHT BESCHERMD TEGEN SPOOFING

ERIK REMMELZWAAL - 29 APR 2021

TLDR: We scanden de DNS records van 1,6 miljoen .nl domeinen en vonden uit: 9% is rechtstreeks gekoppeld aan Microsoft 365, daarmee is Microsoft veruit de grootste Google is nr2 en heeft 4% van de domeinen aan zich verbonden, nagenoeg gelijk aan een aantal andere spelers. Van alle mail-enabled domeinen heeft 27% geen SPF record […] Lees verder

ZOLDER BIEDT MKB BETAALBARE EN EENVOUDIGE SECURITY-APP

ZOLDER B.V. - 12 APR 2021

“Attic voorkomt dat security een luchtbel wordt” Security is bij mkb-bedrijven vaak het ondergeschoven kindje. Ze hebben er de mensen en het budget niet voor. Dat maakt deze doelgroep een aantrekkelijk doelwit voor cybercriminelen. Voor de vier doorgewinterde cybersecurity-experts van start-up Zolder reden om Attic te introduceren. Deze eenvoudige, goedkope en toekomstbestendige app maakt mkb’ers […] Lees verder

NIEUWE THEMESONG VOOR ZOLDERSESSIONS

ERIK REMMELZWAAL - 13 MRT 2021

Ik vond het tijd worden voor een nieuw liedje voor onze Zoldersessions. Tot nu toe hadden we er een rechtenvrij liedje onder staan, namelijk EVA_失望した, maar wilden toch iets meer 'eigens'. Daar schakelden we Bjørgen van Essen voor in met dit eindresultaat. Dit is hoe dat tot stand kwam. Lees verder

ZOLDER.APP OPEN BETA

receive a free subscription to the Zolder.App Premium Plan for the remainder of the beta phase, which is scheduled to run through April 30th 2021. Zolder.App […] Lees verder

GGD DATA IS TOPJE VAN IJSBERG

ERIK REMMELZWAAL - 26 JAN 2021

Maandag kwam RTL Nieuws, na onderzoek van Daniël Verlaan, naar buiten met het nieuws dat gestolen data van de GGD online wordt verhandeld door criminelen. Het gaat om data die onderdeel uitmaakt van het bron- en contactonderzoek dat de GGD uitvoert als onderdeel van de bestrijding van Corona/COVID-19. De data bevat gevoelige persoonsgegevens en criminelen […] Lees verder

#CES2021 - WE ARE READY!

ERIK REMMELZWAAL - 06 JAN 2021

We are very excited to be part of the #CES2021NL mission! Meet us at CES (Januari 11-14) in our online booth 10609 and see how we solve global challenges with NLTech. Erik Remmelzwaal, Co-Founder & CEO Yes I indeed think we are ready for CES. At this virtual event we will showcase Zolder.App. I am […] Lees verder

ZOLDER.APP BLOG 3 - FEEDBACK

ERIK REMMELZWAAL - 27 NOV 2020

Bij het ontwikkelen van een nieuwe dienst, zeker als dit Software-as-a-Service betreft, is feedback vanuit (potentiële) afnemers cruciaal. In het geval van Zolder.App is de doelgroep het MKB. We zijn al gelijk na lancering van het merk Zolder gestart met het vinden van MKB-ers die als tester wilden helpen. Oproep 19-apr-2020 Dit leidde tot

AZURE APP CONSENT POLICIES

RIK VAN DUIJN - 11 NOV 2020

OAuth consent phishing has been on the rise for a while now. Unsurprisingly, Microsoft has gradually introduced measures to protect from this type of attack. Latest: Risk-Based Step-Up Consent. Lees verder

HONEYTOKENS USING AZURE KEYVAULTS

RIK VAN DUIJN - 15 OKT 2020

In 2017 Wesley and I gave a presentation at SHA2017 about honey/pot/tokens. We actually planned on building a fully fledged platform. But never came further then the POC phase of that project. This week we got a product demo from the guys at Thinkst, i've always loved this way of thinking: let the attacker come […] Lees verder

ZOLDER.APP BLOG 2 – PROBLEEM & OPLOSSING

ZOLDER B.V. - 08 OKT 2020

Het is best een goed idee om voordat je begint met het bouwen van een product of dienst, te weten welk probleem je ermee gaat oplossen. Voor Zolder.App: we lossen het probleem dat MKB-ers slecht beveiligd zijn op door enterprise-niveau security voor hen toegankelijk te maken. In feite zijn er een aantal problemen die we […] Lees verder

RISK OF EXPOSED HOME AUTOMATION SERVICES

WESLEY NEELEN - 24 SEP 2020

At home, I am automating many things for fun. Currently I am using Home Assistant, an incredibly powerful piece of software for automating your home. Regularly I am combining the home automation experiences with security. Home automation is often

ZOLDERSESSIONS STUDIO SETUP

ZOLDER B.V. - 27 AUG 2020

Here is the kitlist which we end up with to record our Zoldersessions 🙂 Audio Input 4x Rode Procaster microphone 4x Triton Audio FetHead Microphone PreAmp 4x YellowTec m!ka Mic Boom Focusrite Scarlett 18i8 3rd gen Audio Output 4x Shure SRH840 Headphone ART HeadAmp 4 headphone amplifier Video Input 2x Sony Handycam main cameras Logitech […] Lees verder

ZOLDER.APP BLOG 1 - HET IDEE

ERIK REMMELZWAAL - 27 AUG 2020

Op Zolder bouwen wij aan een mobiele app die MKB'ers op een baanbrekende manier moet helpen digitaal weerbaar te zijn. We verwachten in het vierde kwartaal van 2020 de app te kunnen lanceren. In deze blogreeks neem ik je mee in de ontwikkeling van Zolder.App. Eigenlijk was er niet 1 idee, maar is Zolder.App het […] Lees verder

HACKING THE TRAFFIC LIGHT OF THE FUTURE

WESLEY NEELEN - 06 AUG 2020

Nowadays we are connecting everything we can think of to the internet. Usually to make our lives easier or more comfortable. Some of the new upcoming innovations are related to making our traffic smart with the goal to improve safety, comfort and the traffic flow. We dived into this technology to analyze the inner workings and identify potential security risks. Lees verder

DETECT LATERAL MOVEMENT WITH AZURE SENTINEL

WESLEY NEELEN - 01 JUL 2020

wanted to add monitoring features into the network. If an attacker is in our network, we would like to get a notification. Lees verder

ZOLDERSESSIONS

#37 - DAVE MAASLAND

#36 - OSCAR KOEROO

#35 - BJØRGEN VAN ESSEN

#34 - STAN HEGT

BREDA ROBOTICS

#33 - CHANTAL VAN SPAENDONCK

#32 - THIJS BOSSCHERT

#31 - CHRIS VAN 'T HOF

#30 - ERIK REMMELZWAAL

#29 - ROOS DIJKXHOORN

#28 - JOHN FOKKER

#27 - CHANTAL STEKELENBURG

ZOLDER

APPLIED
SECURITY
RESEARCH

Zolder biedt digitale bescherming voor de technologie van de toekomst. Voor de ontwikkeling en het onderzoeken van de nieuwe digitale veiligheid werkt Zolder met een team van professionele hackers, ervaren security researchers, softwareontwikkelaars en beveiligingsadviseurs.

Privacy Statement - Responsible disclosure