 # Draft version 0.1b

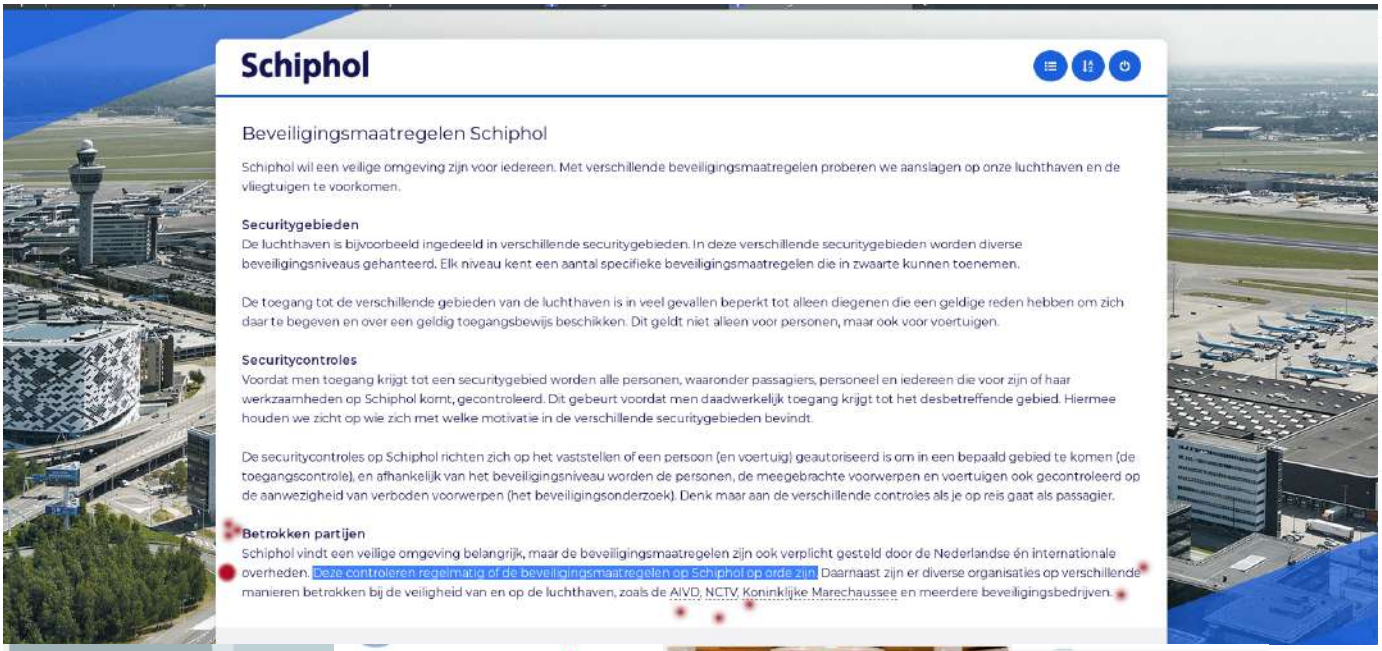
Schiphol Group; Security Catch-22 structure versus "***Safeguard***" method
Just a few example observations, focused on **3** telltale subjects.

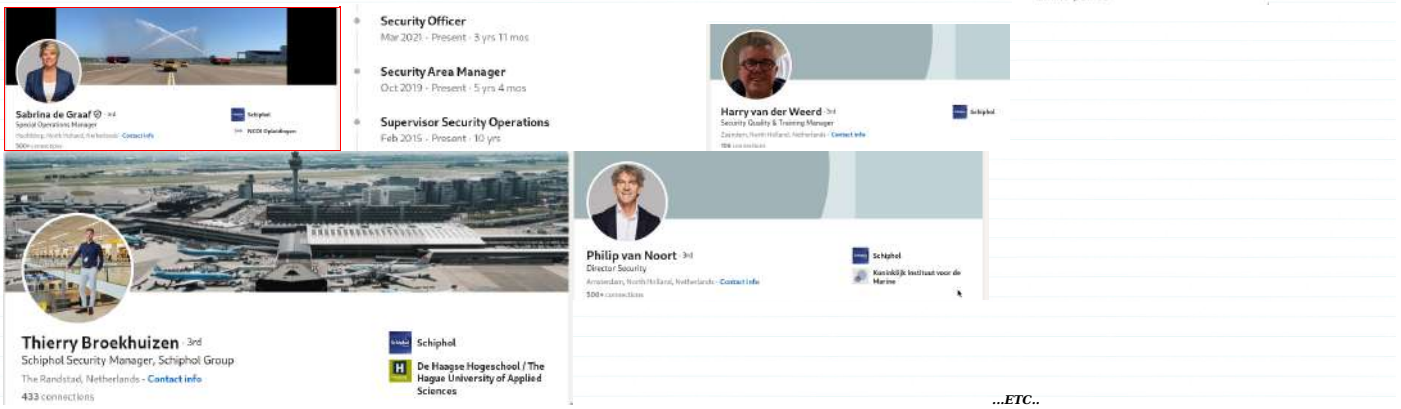
Examples picked from a very long list of blatant security and compliance issues
highlighting the overall conundrum in **6** areas of security management within High-Risk Vital Infrastructure context.

Schiphol Group

Royal Schiphol Group is een luchthavenonderneming met een belangrijke maatschappelijke opdracht. Royal Schiphol Group is eigenaar en exploitant van Amsterdam Airport Schiphol, Rotterdam The Hague Airport en Lelystad Airport en heeft een meerderheidsbelang in Eindhoven Airport. De luchthavens van de groep creëren waarde voor de samenleving en de economie, met veiligheid als essentiële factor. Alle Nederlandse luchthavens van de

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate





...ETC..

www.schiphol.nl/en/schiphol-group/***management***-royal-schiphol-group/

Learning **:(# Publishing & Leaking large quantities of *sensitive* "inside" information, 24/7 to public internet,\ ..thus to unauthorized people => incl. *hostile actors*..**
Via: documents (digital & physical), photo / video, social media, *network protocol layers*, out-sourced systems, unfiltered meta-data, work chats in public area's, etc...

Learning **:(# '*Ignoring*' mandatory essential risk management rules & regulations, shifting responsibility to 'others', + false positive status statements in reports.**

Hedzer Komduur 1st
Director Safety and Environment and CISO at Royal Schiphol Group
The Randstad, Netherlands · Contact info
500+ connections

Royal Schiphol Group
Technische Universiteit Delft

About

I am driven, like assessing the big picture, but also have a keen eye for details, both in business and in people.

Experience

Royal Schiphol Group
Full-time · 7 yrs 9 mos

- **Director Safety and Environment and CISO**
  Oct 2022 - Present · 2 yrs 4 mos
  Schiphol, North Holland, Netherlands

  Safety Manager Schiphol Airport
  Responsible for HSE Office, Airport Fire Brigade, Crisis & Safety Training and the European Entry Exit (EES) program
  Chair of Information Security Board
  Stakeholder management on a local, national and international level
  Representative of Schiphol in Regional Policy Team of the Safety Region Kennemerland in case of crises, disasters and disruptions of public order pertaining to the airport

  Leadership, Airport Management and +7 skills

- **Acting Director Safety, Security and Environment**
  Sep 2022 - Oct 2022 · 2 mos

  Responsible for Security Policy, 24/7 Security Operations, Corporate Investigations, HSE Office, Airport Fire Brigade, Crisis & Safety Training and the European Entry Exit (EES) program
  Stakeholder management on a local, national and international level
  Representative of Schiphol in Regional Policy Team of the Safety Region Kennemerland in case of crises, disasters and disruptions of public order pertaining to the airport

  Leadership, Airport Management and +7 skills

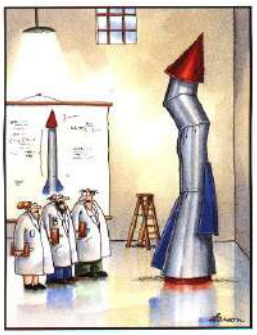
- **Deputy Director Safety, Security and Environment**
  Jun 2020 - Sep 2022 · 2 yrs 4 mos
  Schiphol, North Holland, Netherlands

  Responsible for Security Policy, 24/7 Security Operations, Corporate Investigations, Airport Fire Brigade and Crisis & Safety Training

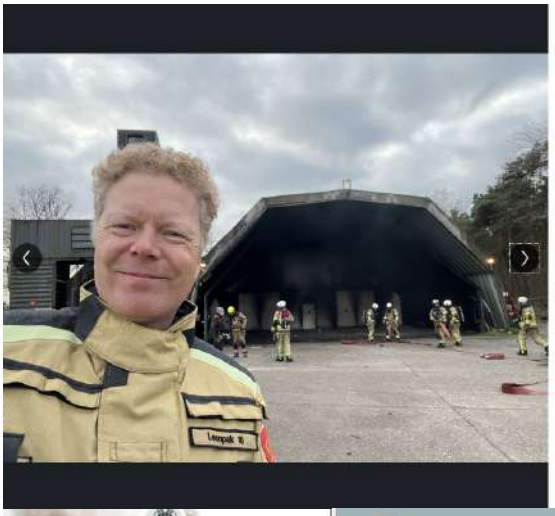
TNO Prins Maurits Laboratory

Hedzer Komduur, M.Sc.
Research Scientist
Rocket Technology

TNO



"It's time we face reality, my friends. ...
We're not exactly rocket scientists."



Hedzer Komduur
Director Safety and Environme...
1mo •

+ Follow

Today colleague Robert-Jan Ooteman and myself visited part of the Royal Schiphol Group Fire Brigade as they were doing live drills at Training Base Weeze . No less than seven different scenarios over the course of today, to be followed by joint multidisciplinary drills with the Royal Netherlands Marechaussee tomorrow and the day after. Impressed by the good spirit and utter professionalism displayed throughout! Thanks Alex Hagenbeek and the team for your dedication and preparation, the AFOs and instructors for their insights, and special thanks to Vincent Sanders and his team for having me tag along on his TAS. It feels good to know you all are on watch!

148 5 comments

Like Comment Repost Send

Add a comment...

Most relevant

Alex Hagenbeek • 3rd+
Officier PrePareatie bij Schiphol Group
1mo

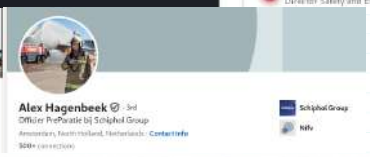
We hebben er met elkaar weer een leerzame en gezellige week van gemaakt.

Show translation

Like · 3 | Reply · 2 Replies

Hedzer Komduur Author
Director Safety and Environment a...
1mo

Robert-Jan Ooteman · 3rd
Senior Manager Fire Brigade & Crisis Safety Training Schiphol Airport



Alex Hagenbeek · 3rd
Officier PrePareatie bij Schiphol Group

Schiphol | Hedzer Komduur — Royal Schiphol Group N.V. (NL) — https://www.schiphol.nl/nl/sch

Schiphol Royal Schiphol Group Onze organisatie Nieuws & Per

Director Safety & Environment

Hedzer Komduur

'Luchthavens vind ik machtig interessant: het zijn plekken waar elke dag tienduizenden mensen bij elkaar komen. Om te reizen naar familie, vrienden, of voor zaken. Dagelijks spannen duizenden mensen zich in om al die reizigers van dienst te zijn. Iedereen die je op Schiphol ziet heeft zijn eigen, unieke verhaal. Ik zorg er samen met mijn team voor dat al die mensen elke dag veilig kunnen reizen en werken op Schiphol, en we onze overlast richting de omgeving zoveel mogelijk beperken. Zaken als de energietransitie vragen ook op veiligheidsgebied de nodige inspanningen, dus geen dag is hetzelfde. Voor mijn werk heb ik zelf vaak via Schiphol gevlogen en ben ik op hele bijzondere plekken geweest. Ik kijk er naar uit om onze dochter kennis te laten maken met een van mijn favoriete steden ter wereld: New York. Hier liggen voor mijn vrouw en mijzelf mooie herinneringen, die we graag met haar willen delen.'

```
* images.ctfassets.net/biom0eqyyi6b/6W4gp9ayaJGZRY773MAGgB/d01a85a5fa63d620aa1ff2340617fd7c/hedzer_komduur.jpg
X-Cache: Miss from cloudfront
X-Amz-Cf-Pop: AMS58-P2
  Server: Contentful Images API
  Access-Control-Allow-Origin: *
ETag: "1cc5c434858063b40d90718ad57c923c"
Last-Modified: Thu, 27 Oct 2022 12:13:57 GMT
```

Return-Path: <Hedzer Komduur *schiphol.nl>
Received: from [40.107.21.44] (EUR05-VI1-obe.outbound.protection.**outlook.com**) with Microsoft Exchange Server **v15.20.8230.016***
X-MS-Exchange-CrossTenant-id: **27776982-d882-41b2-95ac-322f28d5a2ce**
X-MSExch-espionage-profiling-**Correlation-Key:** XVcbQREdvUWTRc4XdcqZQx==
X-MS-Exchange-CrossTenant-mailboxtype: **HOSTED**
x-ms-**Public**traffictype: Email
Disposition: automatic-action/**MDN-sent-automatically;** displayed

On Mon, 9 Dec 2024 [redacted]
"Komduur, Hedzer" <Hedzer.Komduur@schiphol.nl> wrote:

> Geachte heer/mevrouw,
>
> Onderstaande e-mail ontving ik via collega Odette Rudolf. Als CISO voor de luchthaven Amsterdam Schiphol vernemen ik graag welke acties wij in uw ogen zouden moeten nemen. Tevens wijs ik u op de mogelijkheid van het doen van een Responsible Disclosure via https://www.schiphol.nl/nl/pagina/responsible-disclosure-melding/
>
> Met vriendelijke groet,
>
> Hedzer Komduur
>
> -----Original Message-----
> From: [redacted], Odette <[redacted]schiphol.nl>
> Sent: Monday, 9 December 2024 [redacted]
> To: Komduur, Hedzer <Hedzer.Komduur@schiphol.nl>
> Subject: FW: uitnodiging gesprek
> Importance: High
>
> Hi Hedzer
>
> Zoals zojuist besproken onderstaand email van *Anna.
>
> mvg
>
> Odette [redacted]
> Bedrijfsrechercheur RSG

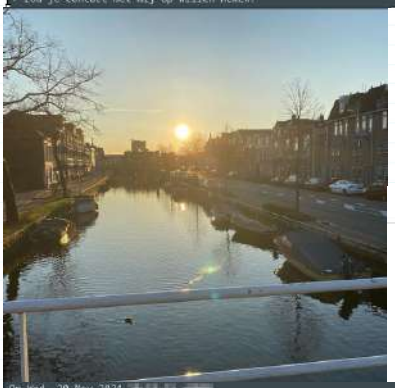
To: [redacted] Odette" [redacted]@schiphol.nl>
Subject: Re: verzoek contact
Date: Wed, 20 Nov 2024 [redacted]

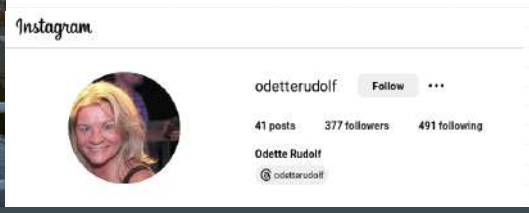
Zou jij deze 2 vragen eerlijk beantwoord willen krijgen binnen de organisatie ?

Waarom, worden er IT systemen gebruikt voor verwerking van vertrouwelijke operationele gegevens waarvan men weet dat die niet echt voldoen aan de voorschriften en geen functioneel IPS hebben?
Waarom, deelt Schiphol Group (zonder expliciete toestemming van personen) hoeveelheden vertrouwelijke informatie over medewerkers, partners, klanten en bezoekers met 10+ beruchte Amerikaanse bedrijven? Zonder enige 'noodzaak', in overtreding van AVG/GDPR, GW.Art.10 en eigen beleid documenten. Maakt 't ook voor hostile actors eenvoudiger om aan ID diefstal en Social Engineering, Chantage/ Omkoping/Beinvloeding te kunnen doen, toch?

* schiphol.nl/en/page/data-processing-badge-center/
* customer.bookingbug.com/?client=schiphol
* evesta.schiphol.nl/evesta/prod/inloggegevensvergeten
* etc.

On Tue, 19 Nov 2024 10:31:28 +0000
[redacted] Odette" <Odette [redacted]@schiphol.nl> wrote:
> Beste Anna
>
> Zou je contact met mij op willen nemen?





On Wed, 20 Nov 2024 [redacted]
[redacted] Odette" [redacted]@schiphol.nl> wrote:

> Beste Anna?
>
> Leuke foto heb je bijgevoegd! Al voelt het een beetje ongepast

Dat "ongepast" "gevoel" is dus een van de kernpunten.. [spiegeltje aan de wand ;-)
omdat opvallend veel ''security'' functionarissen binnen en rond de Schiphol Airport organisatie zichzelf en de rest roekeloos Extra kwetsbaar maken door o.a. "ongepast" delen van allerlei informatie over zaken waar ook kwaadwillenden gretig gebruik van maken om ....
Te veel beveiliging functionarissen hebben blijkbaar (nog) niet de nodige "awareness" van welke vergaande negatieve gevolgen er zijn van o.a. dergelijke 'social media' publicaties en niet-versleutelde email conversaties, gebruik van ms-sharepoint-cloud, etc.. (negeren van de essentiele "Need to know" regel) :: tot dat ..ieder voor zich eens flink op de snufferd gaat en 't aan eigen lijve ondervind wat er aan covert activities gaande achter de schermen.
Iemand had er bijvoorbeeld ook voor _moeten_ zorgen dat de email systemen geen Leesbevestiging naar buiten sturen (maarja o.a. de Schiphol CISO mist 't broodnodige aan motivatie om 't werk echt degelijk te doen, blijkt.). En ook jij had er basis weet & awareness van moeten hebben, wat de gevolgen zijn als informatie lekkages voorkomen, ..door nalatigheid van C-Level management.

* Is daardoor deels ook dweilen met de kraan open met de jip & janneke bureaucraten 'verbeter projecten' :(
?!= [[Of.. men kiest nu alsnog on wel goed functionerende basis awareness Training te gaan regelen voor Alle beveiliging mensen. Zoals o.a. MI6 en Mossad en '...' gerelateerde functionarissen die krijgen om überhaupt 'security' taken naar behoren uit te kunnen voeren zonder brokken te maken.]
Zo lang mensen zoals jij als "Bedrijfsrechercheur BSG - Afdeling Bedrijfsbeveiliging" , eenduidig onvoldoende awareness en context kennis training krijgen, blijf je een easy target voor pro's die fratsen willen uithalen via de Schiphol Airport infrastructuur, natuurlijk :([Security & Compliance maturity level 7]

Nog een tip:
Overschrijf zelf je 'social media' publicaties met wat semi willekeurige plaatjes en teksten die helemaal niets met jou te maken hebben, incl een profiel foto van een actrice of stripfiguur ofzo. Wis ook facebook en andere soorten commentaren bij posts van nogal specifieke functionarissen in sleutelposities bij andere high-risk organisaties..
? - Tenzij, je maar al te graag t.z.t. eens zelf flink de pineut wil zijn wat betreft ID diefstal, Chantage, APT's op personal devices, enz.. enz..

Author : Dijkstra, Björn
Creator : Microsoft® Word 2016
Create Date : 2020:08:07 15:00:57+02:00

Schiphol

Aanvraagformulier Special Operations op Schiphol

Dit formulier is bedoeld voor het aanvragen van een speciaal verzoek (special operations) op Schiphol. Onder special operations verstaan wij een gepland en georganiseerd verzoek, bijeenkomst of activiteit met zichtbare impact op Schiphol en haar bedrijfsvoering.

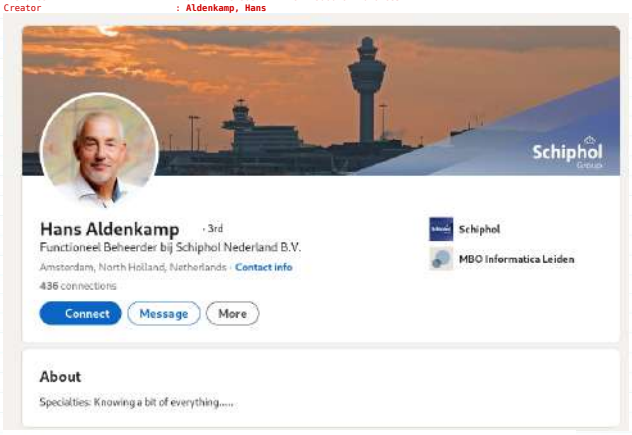
Onderwerp*
Omschrijf kort het onderwerp van je aanvraag.

Voor- en achternaam*

Organisatie*

Telefoonnummer*
Vul hieronder je contactgegevens in, zodat we je kunnen bereiken.

* 2.2.1_Werkinstructie_Manager_planner.pdf
Create Date : 2024:03:04 08:28:10+01:00
MSIP Label 5237ac 88-813e-467d-90ba-6ce 279e 3edc 8 Name: 5237ac88-813e-467d-90ba-6ce279e3edc8
MSIP Label 5237ac 88-813e-467d-90ba-6ce 279e 3edc 8 Set Date: 2022-08-24T10:00:37Z
MSIP Label 5237ac 88-813e-467d-90ba-6ce 279e 3edc 8 Site Id: 27776982-d882-41b2-95ac-322f28d5a2ce
Document ID : uuid:e16c36a1-60ea-4548-a631-fc63c467d584
Instance ID : uuid:b428f5d8-7774-49f7-9dbb-c7ffd70fce34
Creator : Aldenkamp, Hans



Ervaring

Schiphol
25 jaar 5 maanden

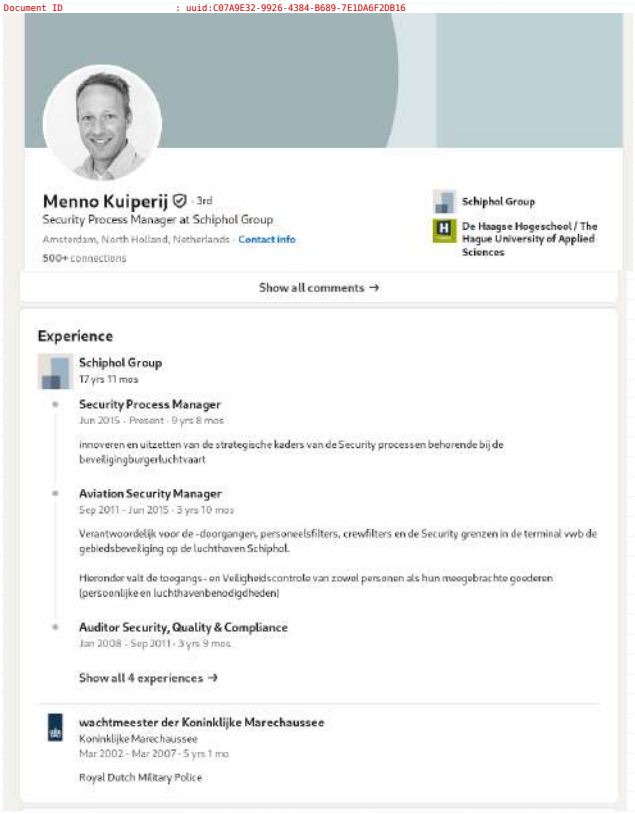
- **Functioneel Beheerder LMS**
  mrt. 2021 - heden · 3 jaar 11 maanden
  Schiphol

- **Manager Safety Training Center (VTC) Schiphol**
  mrt. 2016 - mrt. 2021 · 5 jaar 1 maand
  Amsterdam Area, Netherlands
  Het Veiligheidstrainingcentrum (VTC) Schiphol is al decennia hét trainingscentrum als het om de veiligheid op Schiphol gaat. Wij beschikken over een uitstekend en ervaren team van trainers maar ook de laatste trainingsmiddelen. Veel mensen kennen het VTC Schiphol vanwege zijn bijzondere brandweeroefenplaats.

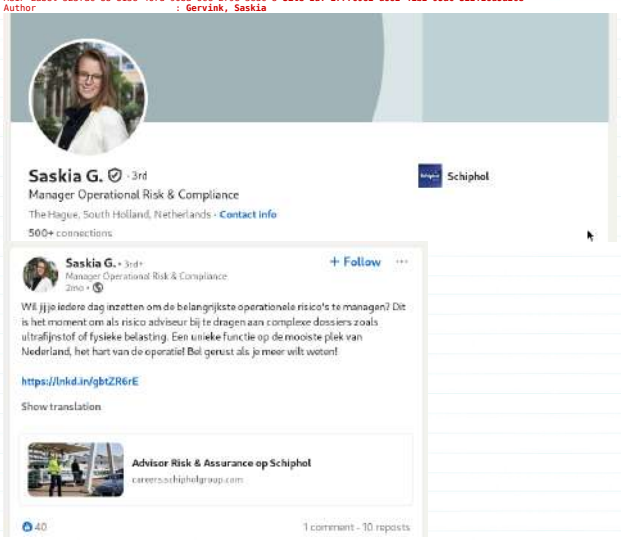
- **Information Security Advisor**
  sep. 2007 - mrt. 2016 · 8 jaar 7 maanden
  Amsterdam Area, Netherlands
  Providing the organization with Information Security (IS) advices when needed; develop Information Security policies; setting up and maintaining a governance structure for IS; Chairman of the tactical Information Security taskforce at Schiphol.

- **Operations Manager**
  sep. 1999 - sep. 2007 · 8 jaar 1 maand
  Performed special Operations within the Passenger Operations Department. Involved

* Acces_Policy_2025__ENG_.pdf
Producer : Microsoft® Word voor Microsoft 365
MSIP Label 5237ac 88-813e-467d-90ba-6ce 279e 3edc 8 Site Id: 27776982-d882-41b2-95ac-322f28d5a2ce
MSIP Label 5237ac 88-813e-467d-90ba-6ce 279e 3edc 8 Enabled: True
Creator : Kuiperij, Menno
Creator Tool : Microsoft® Word voor Microsoft 365
Create Date : 2024:12:17 12:19:39+01:00
Document ID : uuid:C07A9E32-9926-4384-B689-7E1DA6F2DB16

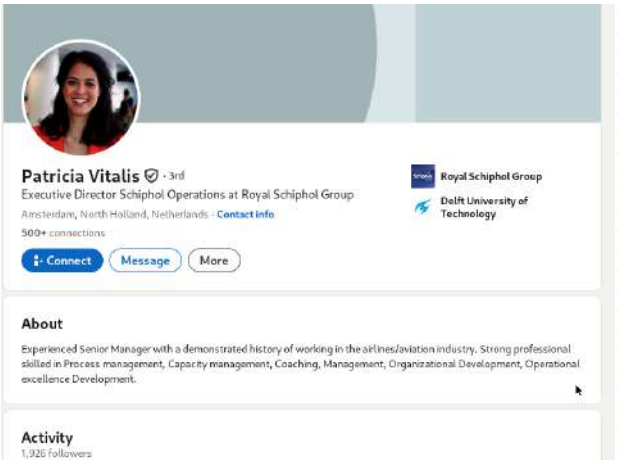


* License_to_Operate_for_Ground_Handlers_Version_Final_Setting_23_October_2023.pdf
Creator Tool : Microsoft® Word for Microsoft 365
Create Date : 2023:10:25 17:52:09+02:00
Document ID : uuid:12A312F9-390E-45D0-9B3D-8C9C2D2CA181
MSIP Label 5237ac 88-813e-467d-90ba-6ce 279e 3edc 8 Site Id: 27776982-d882-41b2-95ac-322f28d5a2ce
Author : Gervink, Saskia

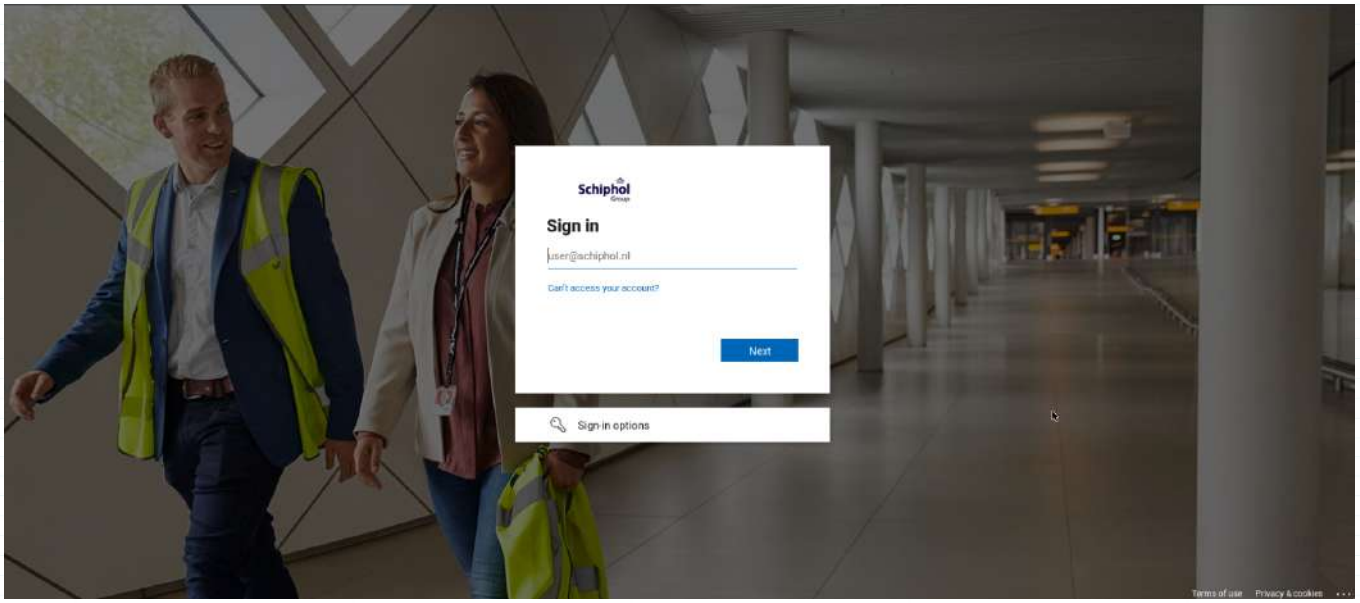


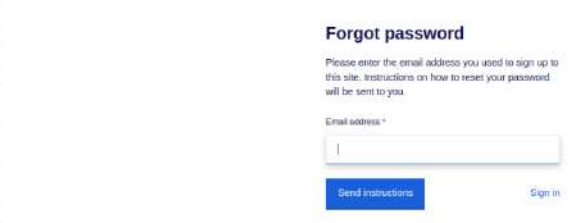
* Safety___Security_Q_A__2024___-_EN.pdf
* Safety___Security_instruction_employees.pdf
* ...

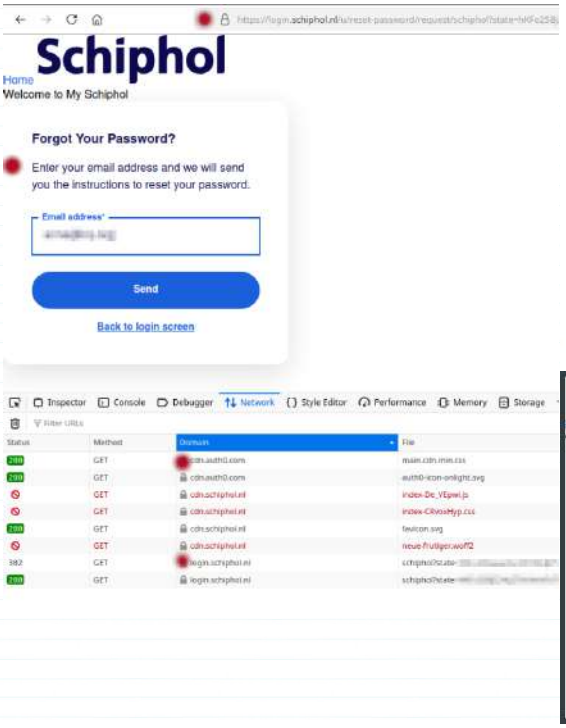
COO



 # Remote (covert) Access is "*allowed*", to Vital Infra and operational elements.
 # Admin rights access from unknown sources is also "*allowed*" (by CISO & Co),
without any *need* to expose those powerful functions to unknown/unauthorized outsiders all over the world (incl. China, Russia, USA, etc.)
 # No functional IPS/IDS possible, due to lacking '*security*' architecture.
 # No functional detection of (large quantities) of Classified information extraction.
 # [classified info]
 # [classified info]



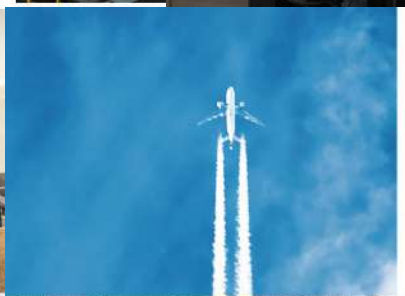




***

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2015	0	0	0	0	0
2016	2	0	0	2	0
2017	3	0	0	4	3
2018	0	0	0	1	1
2019	2	1	3	0	1
2020	10	3	7	8	2
2021	5	4	6	5	1
2022	2	1	5	3	2
2023	3	0	2	0	0
2024	1	1	7	4	0
Total	28	10	30	27	10



GSE is the indispensable link in all logistical processes at an Airport. In total we maintain approximately 1500 pieces motorized and 750 non-motorized vehicles, owned by various KLM departments and third parties.

We maintain a great diversity of vehicles needed for the ground handling of aircrafts. This maintenance work is complex because of the variety of vehicles operating at Amsterdam Airport Schiphol. But we have all the expertise.

KES B.V.

 # Ivory Tower: Lack of *wanting* to be "in control" of security and compliance = risk-managment ?

Lennert l'Amie (1985) is als senior manager bij Schiphol verantwoordelijk voor zo'n beetje alle digitale processen van de luchthaven. Hij stuurt een team met 150 IT-professionals aan, en dit altijd met een glimlach.

'Ik doe alleen dingen waar ik energie van krijg. Dat klinkt wellicht egoïstisch, maar het maakt dat ik altijd met enthousiasme door kan en dat reflecteert op mijn omgeving.' Respect voor anderen vindt l'Amie echter even belangrijk als eigenschap. 'Wie je ook bent, wat je ook doet, je draagt altijd bij aan de successen van het bedrijf.'

Uitdagingen de rode draad

Complexe situaties en uitdagingen lopen al vanaf het begin als een rode draad door de carrière van volledige operations. In 2015 lonkt een heel andere operatie: die van Schiphol. L'Amie start bij Schiphol Telematics, om in 2019 verder te groeien bij Schiphol Group tot senior manager business platform operations.

Leiders cruciaal voor groei

'Goede (op)leiders zijn cruciaal in mijn groei geweest. De keuze voor een functie is minder relevant. Ik kies voor de manager die me uitdaagt, die me iets kan leren en die me ruimte geeft om mezelf te ontwikkelen en te falen. Dat heeft me elke keer geholpen om een vervolgstap te zetten, waarbij zij wellicht al veel eerder zagen dat dat moment zou komen.'

Wat de toekomst betreft, zal volgens l'Amie het onderscheidend vermogen van bedrijven bepaald worden door de snelheid van het kunnen reageren op verandering. 'Nieuwe leiders omarmen verandering als een constante. Ze blijven inspireren en een diverse en inclusieve cultuur creëren.'

Schiphol kleedt Schiphol Telematics uit

18. december 2019

18. december 2019

Een groot deel van de taken van Schiphol Telematics, onderdeel van Schiphol Group, wordt uitbesteed aan Conscia, Alliaq en Securelink. Van de telecomoperator voor de luchthaven blijft een regieorganisatie over. Een deel van de medewerkers kan bij Schiphol Telematics blijven werken.

Schiphol Telematics (ST) is zo'n twintig jaar de telecomoperator op en rond de luchthaven Schiphol. Het bedrijf levert diensten op het gebied van ip-netwerken, internet, vaste en mobiele netwerken en internet-of-things.
Moederbedrijf Schiphol heeft besloten om de operationele taken van ST in handen van derden te leggen. Daar zou meer technologische en innovatieve kennis zitten om goed in te kunnen blijven spelen op nieuwe ontwikkelingen en klantbehoeften op de luchthaven.

Na een zoals ST het noemt, 'uitvraag' in de markt voor het outsourcen van de IT-beveiligingswerkzaamheden zijn drie bedrijven geselecteerd: Conscia, Alliaq en Securelink. De looptijd van de contracten is vijf jaar. Over de waarde van de overeenkomsten worden geen mededelingen gedaan.

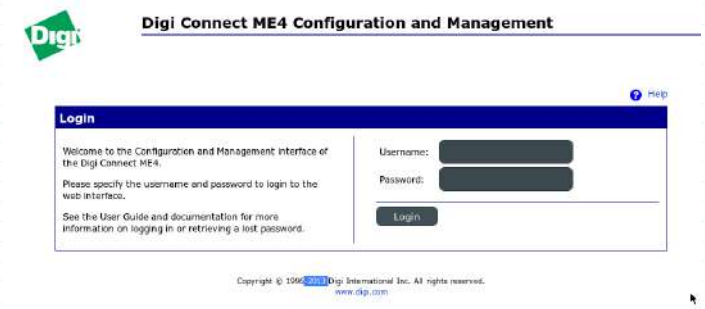
IT-beveiligingsintegrator Securelink, tegenwoordig onderdeel van de Franse netwerkdienstverlener Orange, krijgt de verantwoordelijkheid voor de beveiliging van dataconnectiviteit en communicatieoplossingen.

#

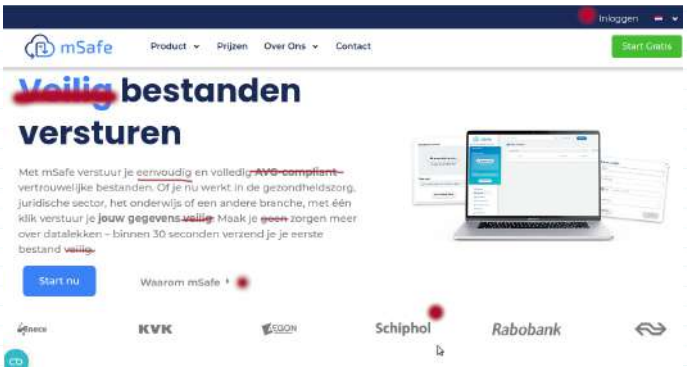
```
inetnum:        89.248.140.104 - 89.248.140.111
netname:        AAS-NL
descr:          A.A.S. T/ICT
country:        NL
admin-c:        ED679-RIPE
tech-c:         ED679-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-STNET
created:        2015-12-11T10:56:54Z
last-modified:  2015-12-11T10:56:54Z
source:         RIPE

person:         Eddy Dobma
address:        Schiphol
phone:          +31(0)610339753
nic-hdl:        ED679-RIPE
mnt-by:         MNT-STNET
created:        2008-12-09T12:12:19Z
last-modified:  2021-06-08T13:11:40Z
source:         RIPE

% Information related to '89.248.128.0/20AS42517'
```

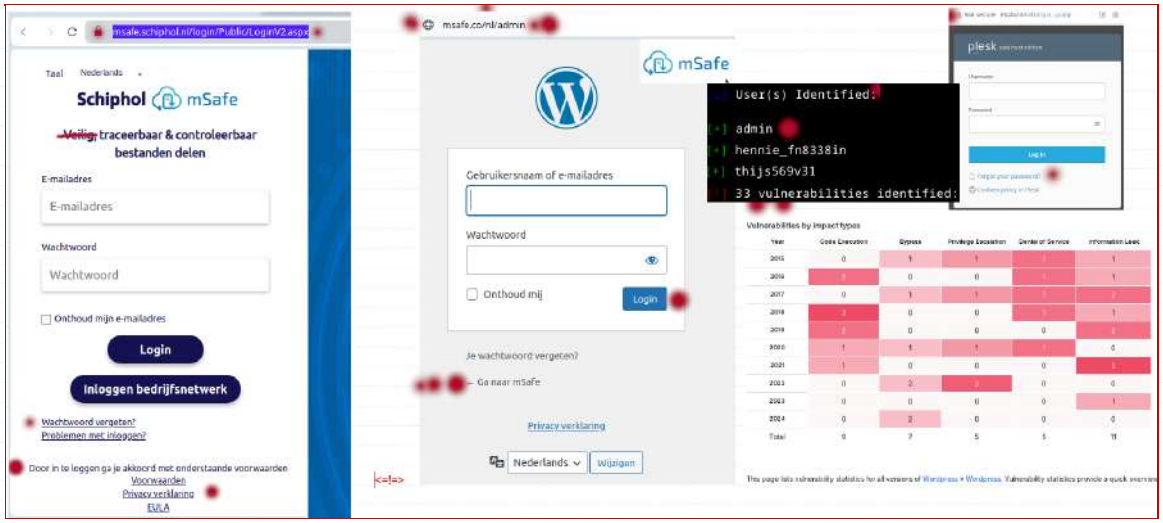
```
77.241.224.0/20 Route   Schiphol Telematics B.V. #.
89.248.128.0/20 Route   Schiphol Telematics B.V  #.
109.69.224.0/21 Route   Schiphol Telematics B.V. #.
185.130.240.0/22 Route  Schiphol Telematics B.V. #.
2a00:1ae8::/32 Route    Schiphol Telematics B.V. #.
```

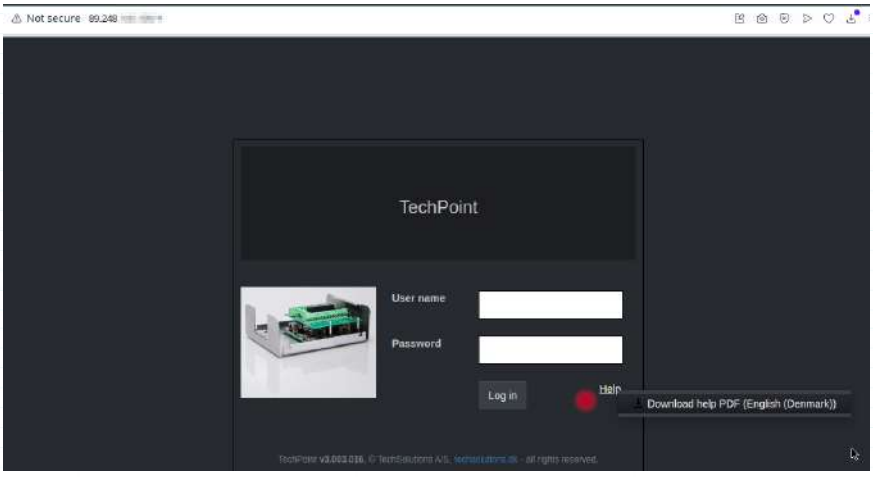
https://77.241.235.132/ [SiteManager 1139 [Mobile broadband]


Digi Connect ME4 Configuration and Management
Help
Login
Welcome to the Configuration and Management interface of the Digi Connect ME4.
Please specify the username and password to login to the web interface.
See the User Guide and documentation for more information on logging in or retrieving a lost password.
Username:
Password:
Login
Copyright © 1996-2017 Digi International Inc. All rights reserved.
www.digi.com


PROFLEET
Login
Home
Logoff
Help
Password change
Identification
Old password
New password
New password confirmation
Quick start guide display
Confirm
Cancel

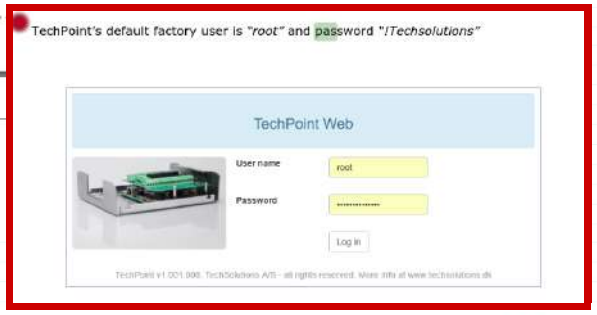

Inloggen
mSafe
Product
Prijzen
Over Ons
Contact
Start Gratis
Veilig bestanden versturen
Met mSafe verstuur je eenvoudig en volledig AVG-compliant vertrouwelijke bestanden. Of je nu werkt in de gezondheidszorg, juridische sector, het onderwijs of een andere branche, met één klik verstuur je jouw gegevens veilig. Maak je geen zorgen meer over datalekken – binnen 30 seconden verzend je je eerste bestand veilig.
Start nu
Waarom mSafe
KVK
Schiphol
Rabobank

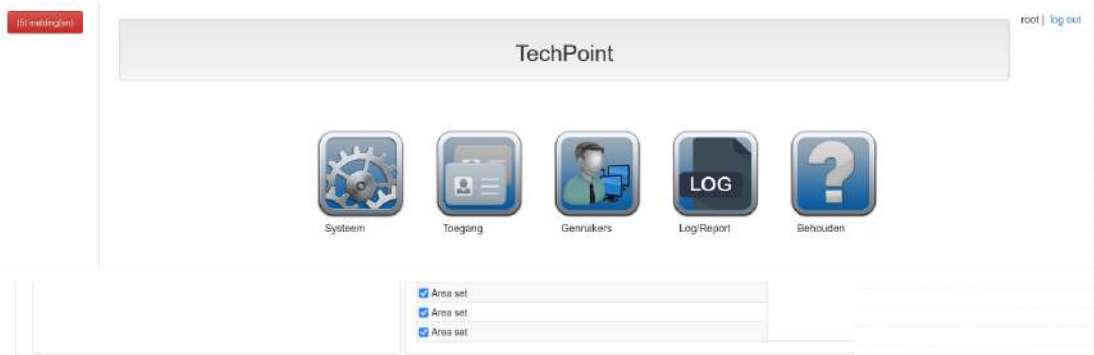

msafe.schiphol.nl/login/Public/LoginV2.aspx
Taal
Nederlands
Schiphol mSafe
Veilig traceerbaar & controleerbaar bestanden delen
E-mailadres
Wachtwoord
Onthoud mijn e-mailadres
Login
Inloggen bedrijfsnetwerk
Wachtwoord vergeten?
Problemen met inloggen?
Door in te loggen ga je akkoord met onderstaande voorwaarden
Voorwaarden
Privacy verklaring
EULA
msafe.com/nl/admin
mSafe
Gebruikersnaam of e-mailadres
Wachtwoord
Onthoud mij
Login
Je wachtwoord vergeten?
Ga naar mSafe
Privacy verklaring
Nederlands
Wijzigen
User(s) Identified:
admin
hennie_fn8338in
thijs569v31
33 vulnerabilities identified:
plesk
Vulnerabilities by impact types

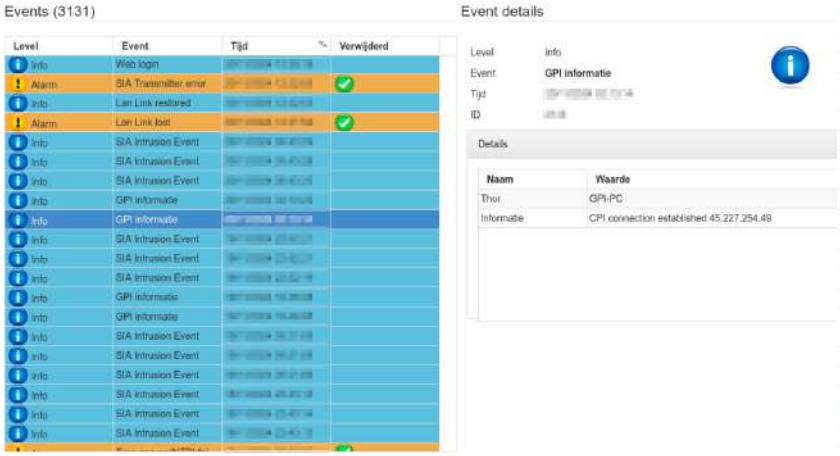

Not secure
TechPoint
User name
Password
Log in
Help
Download help PDF (English (Denmark))

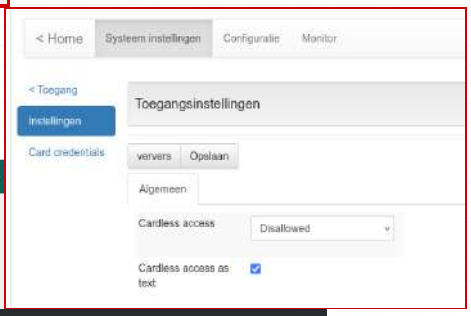
TechSolutions A/S
Innovative Security Products

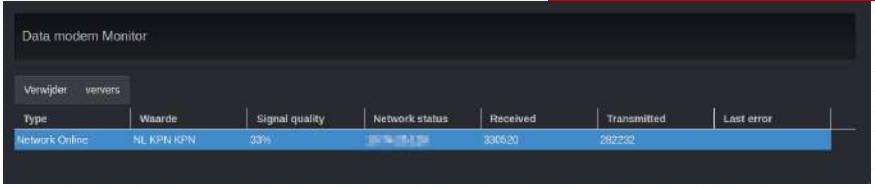
TechPoint Installation Guide Rev. 1.27

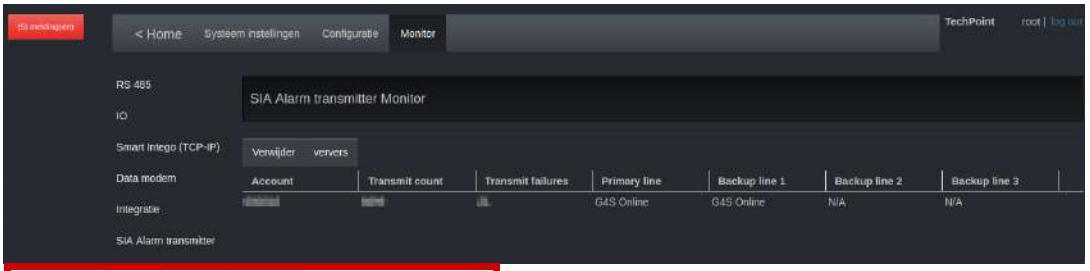


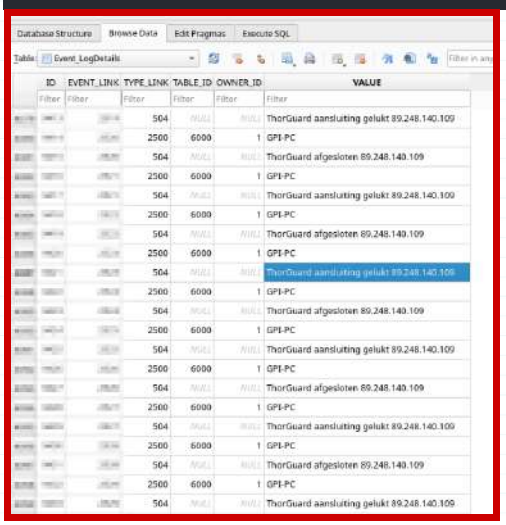












29 februari

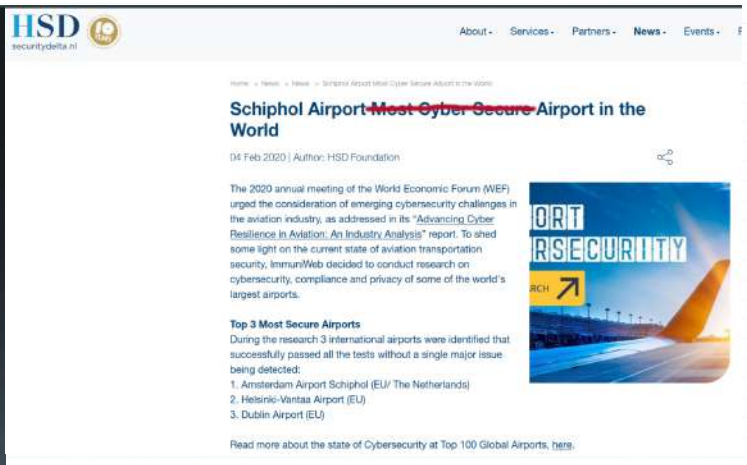
Tap&go met je Digital Travel Credential!

Remote access, Infra layout and Vulnerability detection
.. is **allowed** by CISO & IT Manager & COO & CEO :(

```
Host: 185.130.242.12     nginx 1.25.5
Host: 185.130.242.13     nginx 1.25.5
Host: 109.69.228.86    Microsoft IIS httpd 10.0
Host: 109.69.226.44     [Remote-Web-Access]
Host: 109.69.227.52     [Remote-Web-Access]
Host: 109.69.231.220     ZyXEL ZyWALL http config
Host: 109.69.228.85    Microsoft IIS httpd 10.0
Host: 109.69.224.156     [Remote-Web-Access]
Host: 109.69.230.84     [Remote-Web-Access]
Host: 109.69.224.188     [Remote-Web-Access]
Host: 109.69.229.106     [Remote-Web-Access]
Host: 109.69.228.84     Microsoft IIS httpd 10.0
Host: 109.69.226.164     [Remote-Web-Access]
Host: 109.69.225.205     [Remote-Web-Access]
Host: 109.69.224.45     Mongoose httpd
Host: 109.69.230.85     [Remote-Web-Access]
Host: 77.241.235.116     [Remote-Web-Access]
Host: 77.241.233.132     [Remote-Web-Access]
Host: 77.241.237.84     [Remote-Web-Access]
Host: 77.241.234.52     [Remote-Web-Access]
Host: 77.241.227.132     DrayTek Vigor ADSL router httpd
Host: 77.241.230.172     DrayTek Vigor ADSL router httpd
Host: 77.241.233.7     Microsoft HTTPAPI httpd 2.0 (SSDP/
UPnP)
Host: 77.241.227.148     FRITZ!Box http config
Host: 77.241.231.4     [Remote-Web-Access]
Host: 77.241.228.116     [Remote-Web-Access]
Host: 77.241.225.116     [Remote-Web-Access]
Host: 77.241.232.154     [Remote-Web-Access]
Host: 77.241.232.152     [Remote-Web-Access]
Host: 77.241.234.20     [Remote-Web-Access]
Host: 77.241.232.151     [Remote-Web-Access]
Host: 77.241.225.252     lighttpd
Host: 77.241.230.132     DrayTek Vigor ADSL router httpd
Host: 77.241.235.228     [Remote-Web-Access]
Host: 77.241.225.236     FRITZ!Box http config
Host: 77.241.235.100     Mongoose httpd
Host: 77.241.224.180     [Remote-Web-Access]
Host: 77.241.233.124     [Remote-Web-Access]
Host: 77.241.236.132     DrayTek Vigor ADSL router httpd
..ETC..
```

```
Host: 77.241.233.164     [Remote-Web-Access]
Host: 77.241.232.150     [Remote-Web-Access]
Host: 77.241.232.149     [Remote-Web-Access]
Host: 77.241.230.140     [Remote-Web-Access]
Host: 77.241.228.68     [Remote-Web-Access] Server
Host: 77.241.227.28     FRITZ!Box http config
Host: 77.241.235.132     Apache httpd
Host: 77.241.230.92     DrayTek Vigor ADSL router httpd
Host: 77.241.231.212     DrayTek Vigor ADSL router httpd
Host: 77.241.229.148     [Remote-Web-Access]
Host: 77.241.232.148     [Remote-Web-Access]
Host: 77.241.227.20     [Remote-Web-Access]
Host: 77.241.232.146     [Remote-Web-Access]
Host: 77.241.229.12     [Remote-Web-Access]
Host: 77.241.236.148     [Remote-Web-Access]
Host: 77.241.233.10     [Remote-Web-Access]
Host: 77.241.225.108     [Remote-Web-Access]
Host: 77.241.234.204     [Remote-Web-Access]
Host: 77.241.229.156     Digi-Connect-ME4 1***
Host: 77.241.230.60     [Remote-Web-Access]
Host: 77.241.224.188     DrayTek Vigor ADSL router httpd
Host: 77.241.232.153     [Remote-Web-Access]
Host: 77.241.230.76     DrayTek Vigor ADSL router httpd
Host: 77.241.230.204     [Remote-Web-Access]
Host: 77.241.232.147     [Remote-Web-Access]
Host: 77.241.224.124     Apache httpd
Host: 77.241.230.84     DrayTek Vigor ADSL router httpd
Host: 77.241.227.236     FRITZ!Box http config
Host: 77.241.233.36     [Remote-Web-Access]
Host: 77.241.233.11     Apache httpd
Host: 77.241.238.108     DrayTek Vigor ADSL router httpd
Host: 77.241.231.220     DrayTek Vigor ADSL router httpd
Host: 77.241.229.148     [Remote Admin Access] DrayTek Vigor ADSL router sshd 2.0 (protocol
2.0)
Host: 77.241.231.156     [Remote Admin Access] OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
Host: 77.241.225.92     [Remote Admin Access] (protocol 2.0)
Host: 77.241.235.116     [Remote Admin Access] OpenSSH 8.5 (protocol 2.0)
Host: 89.248.140.244     [Remote Admin Access] OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
Host: 89.248.133.212     [Remote Admin Access] OpenSSH 5.5p1 Debian 6 (protocol 2.0)
Host: 89.248.130.125     [Remote Admin Access] Dropbear sshd 2019.78 (protocol 2.0)
Host: 89.248.131.212     [Remote Admin Access] DrayTek Vigor ADSL router sshd 2.0 (protocol
2.0)
..ETC..
```

P.R. Propaganda, ==> Creating a "False sense of *Security*"



Challenge

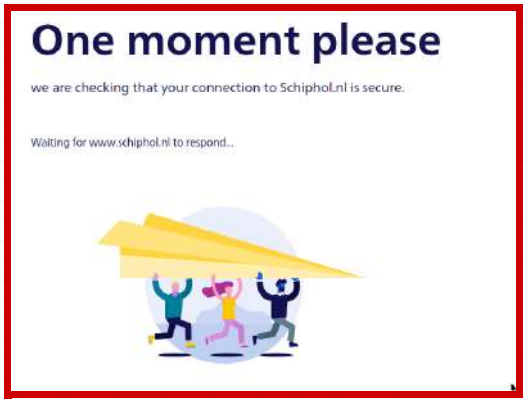
Remind other people of the rules

Working safely starts with you, but don't keep it to yourself. Help other people and keep each other alert. Take a critical look at your own performance, be open to feedback and draw people's attention to any unsafe behaviour. And don't forget to give compliments too!

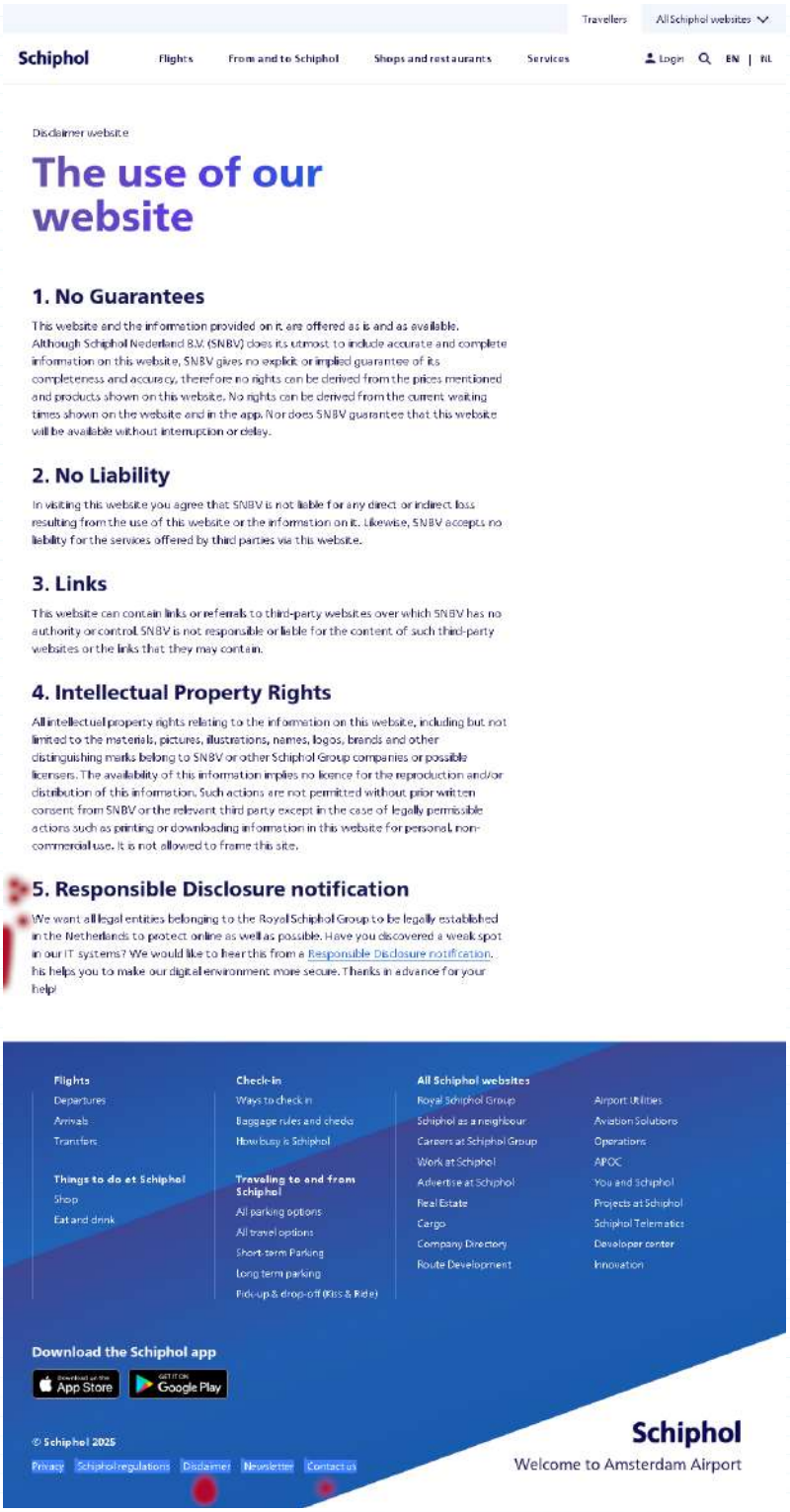
Golden Rule 1: I speak out about unsafe working practices

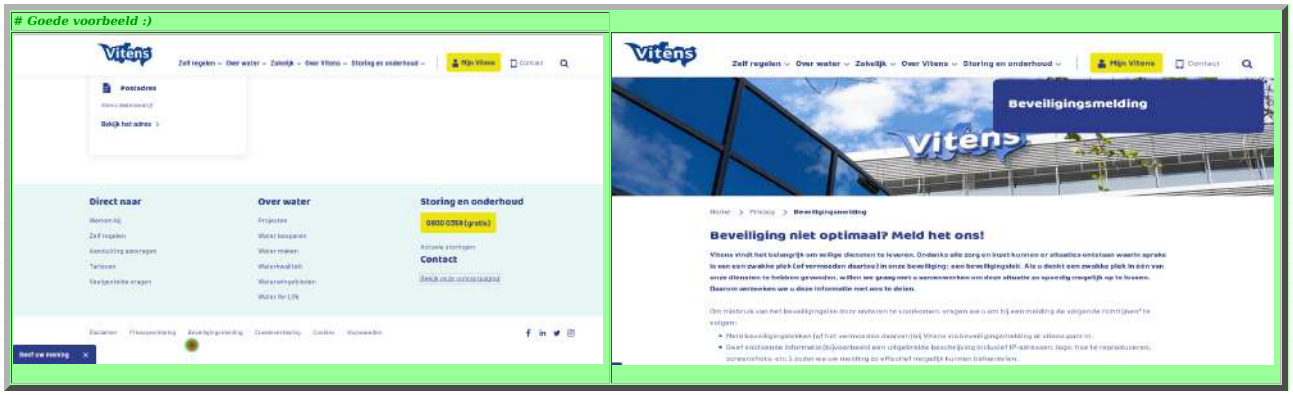
- Take immediate action in the event of an unsafe situation.
- Take responsibility for your own safety and that of others.
- Address colleagues about unsafe or irresponsible behaviour.
- Report unsafe situations immediately so that colleagues can learn from them.
- Discuss safety dilemmas with your manager.
- Accept it when colleagues speak to you about unsafe behaviour.

Downloads: Safety for everyone



https://www.schiphol.nl/en/**disclaimer**/





Modify Date : 2018:11:05 08:46:47Z

What to do if you find a vulnerability in our system

If you find a vulnerability in our IT system we would like you to tell us about it immediately, so that we can take whatever measures are necessary to solve the problem as quickly as possible. We take all notifications of security issues in our IT systems very seriously. To be able to respond to these notifications responsibly, we would like to make the following agreements with you. Have you found a problem, and you are wondering how it should be reported? We would like to hear about it immediately, in the following way.

- Email your findings as quickly as possible to responsible [full stop] disclosure [at] schiphol [full stop] nl. If possible, encrypt this email using Schiphol's PGP key; this will prevent your information from falling into the wrong hands.
- In the email explain how you encountered this issue, so that we can reproduce it. Describe the problem and provide the relevant IP address or URL.
- Include your own contact details, such as an email address or telephone number. We can then get in touch with you to work together on a secure solution.
- We will respond as quickly as possible to report on ongoing progress.

https://www.schiphol.nl/en/page/responsible-disclosure-notification
 # Deliberately creating a narrow scope, to avoid 'hearing' about sec issues which by law have to be reported and resolved :(

If you discover a flaw in or breach in the IT systems of one or more of Royal Schiphol Group's legal entities that has its registered office in the Netherlands, then please let us know. It is important that we take every possible measure and precaution to give ourselves the best digital protection available. For that reason, we ask you to handle digital security responsibly and that you carefully study the rules for Responsible Disclosure notifications. Thanks in advance for your cooperation.

What can be reported

Please let us know if you encounter problems with our digital systems, such as:

- Remote Code Execution
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Injection vulnerabilities
- Broken authentication and session management
- Encryption-related flaws
- Unauthorized access to data
- APIs that are insufficiently protected

Exceptions

Before reporting a vulnerability, make sure to check if it is not listed in the exceptions:

Exceptions Responsible Disclosure (0.1 MB pdf)

 # Wrong Exclusions lists, showing that there is an Ivory Tower ostrich-politics structure within C-level management & "*security*" dept.

Responsible Disclosure Exceptions

Application

- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non sensitive endpoints
- Missing cookie flags on non sensitive cookies
- Missing security headers which do not present an immediate security vulnerability
- Missing DNS entries
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms.
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking on pages without sensitive actions
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, ..)
- Hyperlink injection/takeovers
- Mixed content type issues
- Cross-domain referer leakage
- Anything related to email spoofing, SPF, DMARC or DKIM
- Username / email enumeration
- E-mail bombing
- HTTP Request smuggling without any proven impact
- Homograph attacks
- XMLRPC enabled
- Banner grabbing /Version disclosure
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Weak SSL configurations and SSL/TLS scan reports
- Not stripping metadata of images
- public API keys without proven impact

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate.
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited, may be excluded or be lowered in severity
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks.
- Vulnerabilities that are limited to non-current browsers (older than 3 versions) will not be accepted
- Attacks requiring the usage of shared computers, man in the middle or compromised user accounts

- Recently disclosed zero-day vulnerabilities in commercial products where no patch or a recent patch (< 2 weeks) is available. We need time to patch our systems just like everyone else - please give us 2 weeks before reporting these types of issues.
- Attacks requiring unrealistic user interaction

Author : **Jong, Rob de**
Creator : Microsoft® Word 2016
Create Date : 2020:08:03 10:03:34+02:00

 # Harsh self-Contradictions and false promises, in legal and security statements :(

Wat mag je van ons verwachten?

- Indien je bij de melding van een door jouw geconstateerde kwetsbaarheid in een ICT-systeem van Schiphol aan bovenstaande voorwaarden voldoet, zal Schiphol geen juridische consequenties verbinden aan deze melding.
- Schiphol behandelt een melding vertrouwelijk en deelt persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit juridisch verplicht is.
- We sturen je binnen vijf werkdagen een ontvangstbevestiging.
- Op korte termijn kan je een reactie op een melding verwachten. Hierin vermelden we de beoordeling van de melding en een verwachte datum voor een oplossing.
- We houden je op de hoogte van de voortgang in het oplossen van het probleem.
- Schiphol lost het door jou geconstateerde beveiligingsprobleem zo snel mogelijk op. We streven ernaar om dit binnen 90 dagen te doen. Na de oplossing kunnen we in overleg bepalen of en op welke wijze we over het probleem extern communiceren.

 # <=!=>

Be careful not to break the law

Please take great care when looking into the security of our IT systems, as you may accidentally break Dutch or international laws. This may open you up to possible criminal charges. The rule of law supersedes the rules set out by Amsterdam Airport Schiphol, so take great care to ensure you are not engaging in any illegal activities that we are required to report to the authorities.

Royal Schiphol Group Responsible Disclosure Hall of Fame

- De disclosure moet opgelost zijn vóór het plaatsen van je naam en details. Dit betekent dat je naam niet geplaatst wordt zolang Schiphol er voor kiest om het (nog) niet op te lossen.
- De melding wordt automatisch van de hall of fame gehaald na twee jaar.

Op onze Responsible Disclosure Hall of Fame kunnen wij plaatsen:

- Jouw voornaam, achternaam en/of pseudoniem (naar jouw keuze)
- Omschrijving van de gevonden kwetsbaarheden
- Aantal van gevonden kwetsbaarheden per melder

Royal Schiphol Group would like to thank the following people for their contribution to keeping Schiphol Group's information provision secure.

View the 2025 Responsible Disclosure Hall of Fame

Who	Number of notifications

View the 2024 Responsible Disclosure Hall of Fame

Who	Number of notifications
Arif Nawaz Minhas	1
Martin van Wingerden	1
Kasper Karlsson	1
Hassaan Muhammed	1

Latest update: 8 August 2024

 # ST did buy a ISO27001 certificate from corrupt auditor, illegally, without actual compliance.

10. Security and confidentiality

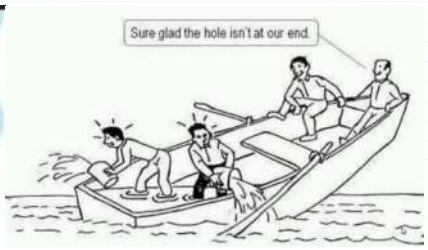
10.1. As a result of the ISO norm 27001:2005 that ST possesses, ST must comply with strict regulations with respect to security and information security. Within this framework, ST has the right to set additional criteria for the contracting party with respect to security and confidentiality. These additional criteria may concern accessibility, and an additional agreement may be required, for example with respect to co-locations and/or access.

10.2. ST ensures the security of service(s) and/or equipment as far as possible.

10.3. ST complies with the legal requirements concerning the security of registrations and personal data wherever this may be applicable.

10.4. ST is obliged to take sufficient measures to protect the confidentiality of all data vis-a-vis third parties, in whatever form, within the framework of this agreement, where ST knew (or should have known) that this was confidential. This is guaranteed within the ST organisation.

General terms and conditions of trading 5



 # Schiphol group & ST: "*Security*"=> Kastje => Kastje => Muur => Zwart gat..
 # responsible.disclosure@schiphol.nl ; access@schiphol.nl ; badgecenter@schiphol.nl ;
 # Evasion of taking responsibilities.

* Example _α_

1) Security issues report send to: responsible.disclosure@schiphol.nl
2) Takes 4 days before anyone responds (outsourced to ***external*** BV with jnr's instead of pro's..?)
3) Ask for irrelevant extra info, blindly follow written procedure without understanding the context.
4) Don't handle it, but say they will forward it on, to ST IT Dept.
5) **Nothing** further happens... **no** response, **no** update, **no** fix, ***nothing..***

Thank you for your recent contact with our team. We have been working on your responsible disclosure issue. As promised, we would like to update you as to the progress of the request.

Schiphol CSIRT handles the responsible disclosures of Schiphol Group.

In this case, it concerns an IP address provided by the ISP service of Schiphol Telematics to an external customer, which falls outside the Schiphol CSIRT mandate.

However, we have contacted Schiphol Telematics to inform them about this security issue at one of their customers.

Best regards,

Schiphol CSIRT
Responsible.disclosure@schiphol.nl

==> !? Misleading statements by Schiphol Group.

- Op korte termijn kan je een reactie op een melding verwachten. Hierin vermelden we de beoordeling van de melding en een verwachte datum voor een oplossing.
- We houden je op de hoogte van de voortgang in het oplossen van het probleem.
- Schiphol lost het door jou geconstateerde beveiligingsprobleem zo snel mogelijk op. We streven

* Example _β_

Automatisch antwoord: Schiphol access pas verloren

From Access <Access@schiphol.nl>
To

Geachte heer, mevrouw,

Wij hebben uw mail/registratieformulier in goede orde ontvangen.
Vanwege enorme drukte is onze verwerkingstijd opgelopen. U dient rekening te houden met een verwerkingstijd van 15 werkdagen.

Zodra uw verzoek is verwerkt krijgt u hier een schriftelijke bevestiging van.

Indien u een verzoek heeft gedaan voor het resetten van en eVesta account, kunnen wij u melden dat de verificatiebrieven op maandag en donderdag per post worden verstuurd.

Wij hopen u hiermee voldoende te hebben geinformeerd.

Met vriendelijke groet,
Team Area & Access Control

*** Example _Δ_**

```
X-Originatororg: schiphol.nl
X-Ms-Exchange-Crosstenant-Authas: Internal
X-Ms-Exchange-Crosstenant-Authsource: VI1PR04MB3055.eurprd04.prod.outlook.com
X-Ms-Exchange-Crosstenant-Id: 27776982-d882-41b2-95ac-322f28d5a2ce
X-Ms-Exchange-Crosstenant-Mailboxtype: HOSTED
```

Not read: Schiphol access card verloren

From: **Badgecenter**
Onderwerp: Schiphol access card verloren
Verzonden: Vrijdag 1 november 2024 (UTC+01:00) Amsterdam

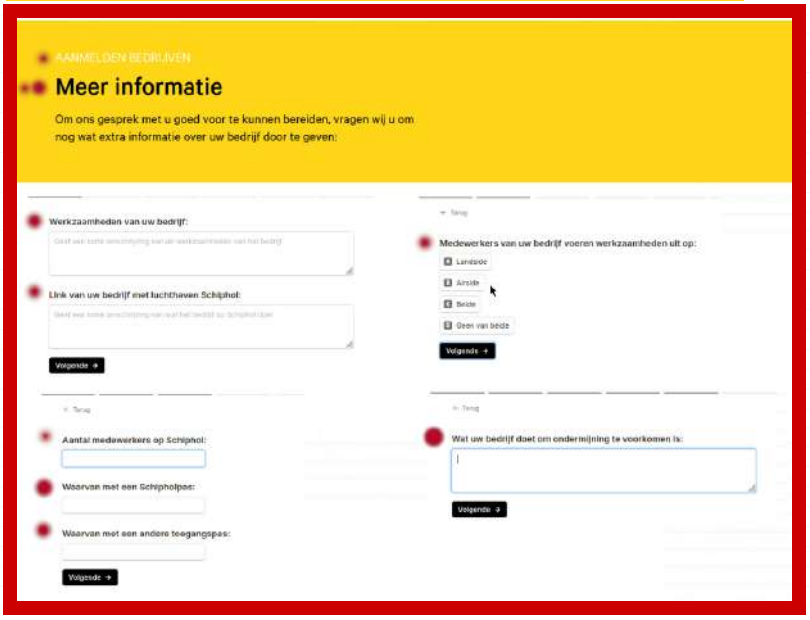
is verwijderd op donderdag 7 november 2024 08:08 UTC+01:00) Amsterdam

---
message/disposition-notification

Final-recipient: RFC822; Badgecenter@schiphol.nl
Disposition: automatic-action/MDN-sent-automatically; deleted
X-MSExch-Correlation-Key: xml6BSh5hEagfdX+xroizQ==
Original-Message-ID: .....
X-Display-Name: Badgecenter

!# Project is not even compliant with Wbni, BIO, AVG/GDPR, ISO27001, NIS2, etc..
#-------!------->> Remote system access and modification by unauthorized entities is allowed. *Even from China, Russia, USA, etc..
 # [classified info] *
 # [classified info] Kmar;MinBZK/MinJenV;NCTV
 # [classified info] IL&T / RDI


Over ons
Samenwerken aan misstanden op de luchthaven Schiphol
De georganiseerde criminaliteit probeert de luchthaven Schiphol en de mensen die daar werken, te misbruiken voor bijvoorbeeld diefstal en smokkel. Daarom werken Belastingdienst, Douane, FIOD, gemeente Haarlemmermeer, Koninklijke Marechaussee, Openbaar Ministerie, Politie, RIEC Noord-Holland, KLM en Schiphol Group al lange tijd samen om ondermijnende criminaliteit en misstanden op luchthaven Schiphol aan te pakken. Ook andere bedrijven zijn onderdeel van de aanpak door barrières tegen criminaliteit op te werpen. Samen houden we de luchthaven sterk. Naar aanleiding van de rapportage "Ondermijning op en rond luchthaven Schiphol" is de urgentie bekrachtigd en de aanpak verder geïntensiveerd.


AANMELDEN BEDRIJVEN
Meer informatie
Om ons gesprek met u goed voor te kunnen bereiden, vragen wij u om nog wat extra informatie over uw bedrijf door te geven:
Werkzaamheden van uw bedrijf:
Link van uw bedrijf met luchthaven Schiphol:
Volgende
Medewerkers van uw bedrijf voeren werkzaamheden uit op:
Landside
Airside
Beide
Geen van beide
Volgende
Aantal medewerkers op Schiphol:
Waarvan met een Schipholpas:
Waarvan met een andere toegangspas:
Volgende
Wat uw bedrijf doet om ondermijning te voorkomen is:
Volgende


Meer informatie
Om ons gesprek met u goed voor te kunnen bereiden, vragen wij u om nog wat extra informatie over uw bedrijf door te geven:


Bedankt!


LESMATERIAAL
TIPS
MELDEN
VERHALEN
Samen werken aan een veilige en integere luchthaven
RIEC
KLM
Schiphol

2 Schiphol's security areas

Introduction

Amsterdam Airport Schiphol makes every effort to ensure a secure environment for everyone. Both passengers and staff are screened at various points in the airport. Take, for example, the security checkpoint at the staff entrance in the terminal. This check is intended to make sure that you are not carrying any dangerous items with you. Everyone of any age, male and female, security staff and airline captains alike must pass through this security checkpoint. In addition, security staff also screen all goods that you want to take with you, such as hand baggage, hold baggage and tools.

All of these security measures are necessary at Schiphol in view of the various attacks on airports and aircraft in the past. Schiphol has put a comprehensive set of security measures in place to prevent the possibility of such an attack.

Measures to ensure a secure environment are not only important to Amsterdam Airport Schiphol, they are

compulsory under Dutch and international law, and regular checks are carried out to ensure that Schiphol fulfils its obligations.

Security areas

Amsterdam Airport Schiphol is divided into the following security areas:

Security areas
Airside Security Restricted Area - Critical Parts
Airside Non-Security Restricted Area's
Airside Demarcated Area's
Landside Secured Premises by A.A.S.

These security areas are described in Chapter 5 of the 'Toegangsbeleid beschermde en bedrijfsbeveiligde gebieden Amsterdam Airport Schiphol (Access Policy A.A.S.)'.

3 Schiphol's passes and tests

Types of passes

Schiphol uses a variety of passes for people and vehicles to give access to Airside Security Restricted Area - Critical Parts, Airside Non-Security Restricted Areas, Airside Demarcated Areas and /or Landside Secured Premises by A.A.S. The number of people who have access to these areas is kept to a minimum. Schiphol Passes are provided only to people in regular employment at the airport and who meet legal requirements as well as Schiphol's own requirements. The colour and letter codes on a pass indicate the areas it gives you access to, as set out in brief in the table below.

Colour / letter	Area
Green	Access to the passenger areas in the terminal
Blue	Access to airside perimeter roads
Orange	Access to the passenger areas in the terminal and airside perimeter roads
Grey	Access to Schiphol-East business park
Black background on pass	Access to Schiphol-East business park
Letter B on the pass	Access to the baggage areas
Letter P on the pass	Access to the aprons

Schiphol Passes are also available for visitors. Passes for visitors do not have a photograph. Visitors, like staff members, must wear their pass so that it is clearly visible at all times, and must always be accompanied by a Schiphol Pass holder authorised to accompany visitors. The Schiphol Pass holder is personally responsible for the visitor.

Types of tests

One of the conditions that needs to be met to quality for a Schiphol Pass providing access to a security-restricted area is the successful completion of a safety and security test. When applying for a pass for the first time, you will

5 Rules for use of the Schiphol Pass

Rules for use of Schiphol Pass

The Schiphol Pass is a strictly personal access pass. Only the pass holder is entitled to the rights granted by his or her respective pass. The pass holder is the person whose name is stated on the pass itself. The following rules apply to the use of your Schiphol Pass:

- Always display your Schiphol Pass clearly when in the Airside Security Restricted Area - Critical Parts, Airside Non-Security Restricted Areas, Airside Demarcated Areas or Landside Secured Premises by A.A.S. and ensure that others do too.
- Never lend your Schiphol Pass to anyone else.
- Never allow someone to tag along with you on your Schiphol Pass. For instance, do not let people through a door or into a lift.
- Do not use the Schiphol Pass outside working hours or for personal ends. For instance, you are prohibited from using the pass to wave off or collect friends or family from a gate.

Correct Schiphol Pass

Employers are responsible for ensuring that employees have a Schiphol Pass for the areas in which they carry out their work.

Misuse of Schiphol Pass

Misuse of a Schiphol Pass can be grounds for the pass being immediately confiscated or blocked without further justification from the airport operator.

Reporting a lost Schiphol Pass

If you lose your Schiphol Pass you must report this immediately to the Badge Center on +31 (0)20 6012626 during office hours, or to the Security Control Center on +31 (0)20 6013000 outside of office hours.

 # If only.. this section 6 would actually be properly <u>enforced</u> by C-Level & CISO (+Kmar & MinBZK)
 # But it clearly is not :(

6 Enforcement and sanctions

Need for enforcement

Without Safety & Security rules, it is likely that dangerous situations would soon arise. These rules will unfortunately be broken at times, which is why Amsterdam Airport Schiphol has established enforcement measures and sanctions related to the Safety & Security rules.

Supervision

Security staff and officials appointed by Amsterdam Airport Schiphol provide supervision at the airport to ensure that rules are adhered to. These individuals can stop you for violating a rule, and report you. They will provide identification upon request.

http://193.136.66.99/airobs/wp-content/uploads/2021/02/Schiphol-SafetySecurityPocketGuide.pdf

You have a part to play in keeping Schiphol safe on a day-to-day basis. By following the security and safety rules you help ensure not only your own safety, but also the safety of your colleagues and of your customers. Schiphol safety is a team effort. This 'Safety & Security Pocket Guide' sets out the most important safety and security regulations in force at Amsterdam Airport Schiphol.

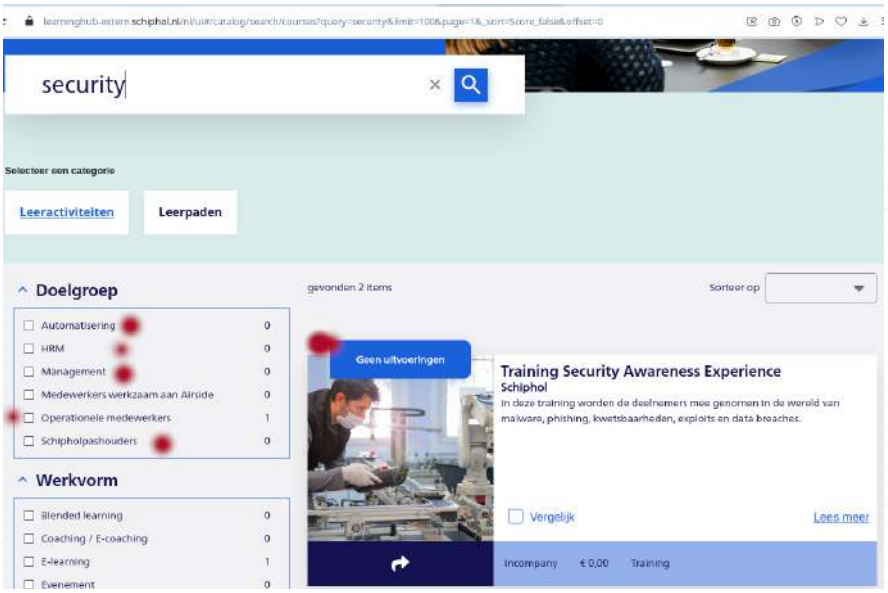
B.I. Otto

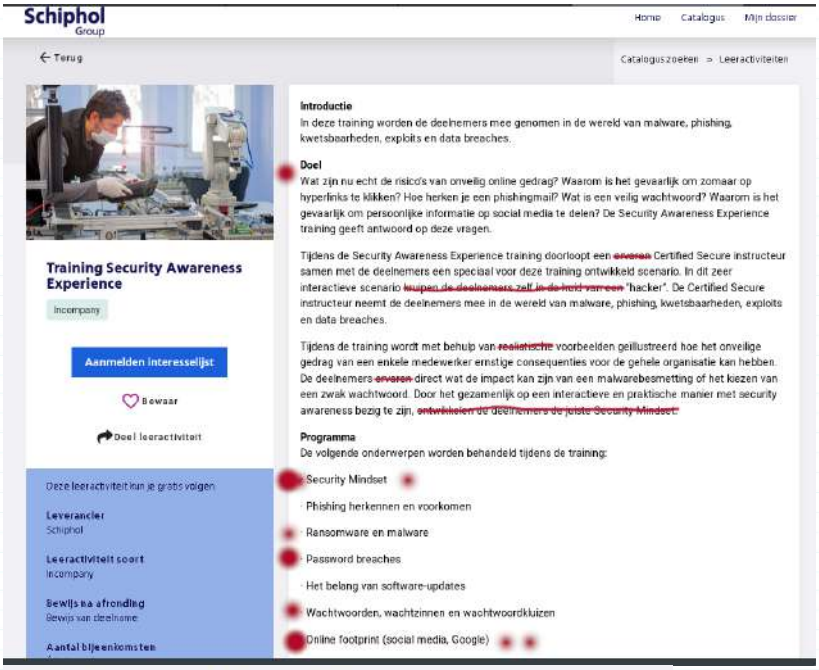
Executive Vice President &
Chief Operations Officer Schiphol Group

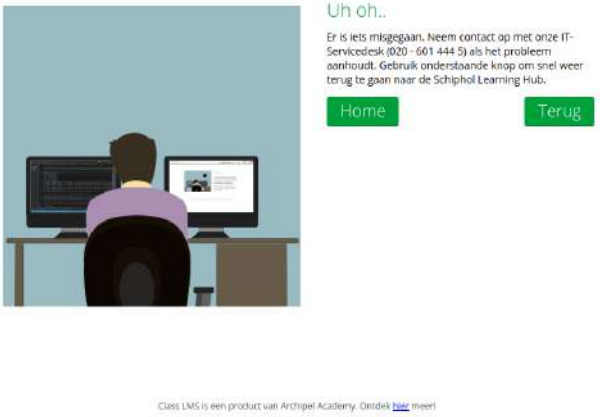
Pocket Guide Safety & Security

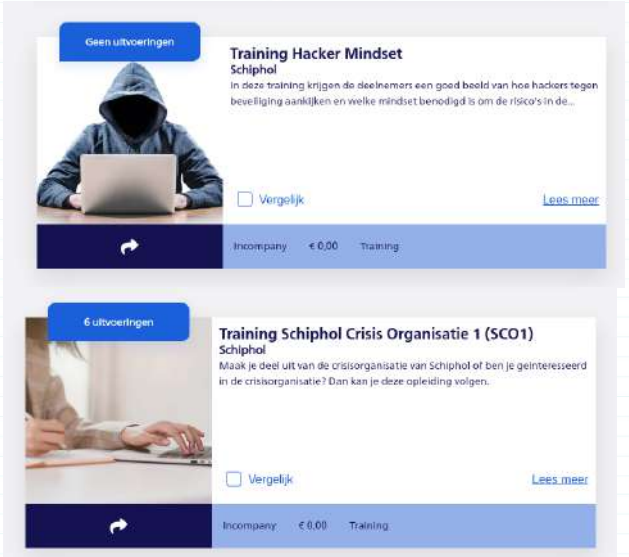
As of 1 March 2024, the Safety & Security Pocket guide is no longer available. In preparation for the Safety & Security test to obtain a Schiphol pass, e-learning(s) are available in the Schiphol Learning Hub.

More information on the e-learning(s) can be found here →









To: Aladar.....@schiphol.nl, ismael....@schiphol.nl
Cc: hedzer.komduur@schiphol.nl, Jaap.winter@schiphol.nl, j.winter@vu.nl
Subject: Re: Intrigerende vacatures: Security Officer / Manager
Date: Thu, 14 Nov 2024

Hallo,

Een nieuwsgierige retorische vraag:
Waarom krijgt Schiphol Airport de beveiliging al zo lang niet daadwerkelijk op orde ?

Als je als snr security officer weer eens door de luchthaven Schiphol loopt, valt het al te vele jaren telkens weer op dat er zelfs wat basis beveiliging principes niet daadwerkelijk tot uitvoering blijken te komen.

Bijvoorbeeld:
q) 'security' medewerkers die schaamteloos gezellig over vertrouwelijke operationele zaken kletsend met elkaar, vanuit een publieke hal naar een beveiligde zone lopen dmv NFC pasje naast een toegang deur, en niet op of om kijken wie er achter hun aan mee naar binnen glipt.
r) een leverancier monteur van netwerk gekoppelde hardware devices, zonder begeleiding/toezicht van schiphol security medewerker, aan apparaten aan sleutelen is waar vertrouwelijke data doorheen gaat. op het scherm zichtbaar is dat met met 'admin' rechten bezig is; even naar een andere plek lopen en daarvoor netjes screen lock activeren; maar vervolgens terug komen en voor iedere omstander zichtbaar de opvallend eenvoudige toegangscode invoeren (geen 2fa o.i.d.). Ook op een rol-kar de documentatie en opdracht bon laten liggen als er naar een andere plek (buiten zicht) heen en weer gelopen blijft worden.
Heb eens bekeken of dat apparaat en die leverancier überhaupt wel daadwerkelijk voldoen aan bijv een van de ISO27xxx normen, en dat blijkt niet het geval te zijn.
Dus, welke 'Security Officer' heeft er goedkeuring gegeven om dat maar aan de Schiphol netwerk infra te laten koppelen ?
s) wat Schiphol IT medewerkers via hun 'smart-phone' en/of tablet 'admin' toegang hebben tot delen van de vitale infra van de luchthaven, dmv een trust-relationship tussen apparaat en de infra (blind trust in somewhat dysfunctional IAM ?). En blijkbaar zich daar niet zo bewust van zijn welke gevolgen 't kan hebben als ''iemand anders'' het apparaat in handen krijgt, fysiek of covert-remote-digitaal. Tenminste, die indruk zou iemand kunnen krijgen als die ziet hoe roekeloos sommige medewerkers die apparaten 'even' onbeheerd laten rondslingeren of in de trein infra configuraties doen met omstanders die mee kunnen kijken.
t) het opvalt dat Schiphol Telematics (ST.nl), een wildgroei aan IT infra heeft laten ontstaan, waarbij het voorkomen van "attack surface" een ondergeschoven kindje blijkt te zijn bij het ijverige meer meer meer IT prestige projecten feest. De vragen "Is het überhaupt echt nodig!?" & "Kan 't ook veel veiliger en eenvoudiger binnen reeds bestaande elementen!? ipv weer iets er bij te gaan doen" lijken door geen CISO serieus op tafel gelegd te worden.
Ook blijken wat "outsourcing" partners er wat met de pet naar te gooien, en ST blind te vertrouwen op beloftes op papier ipv gezond verstand controle [o.a. Cloudflare, Inc. & Pulsant Limited]
..)
..)
z) dat het melden van een "security incident" bij een medewerker, best het ene oor in en het andere weer uit kan gaan zonder dat die medewerker de verplichte kleine moeite wil doen om het ook als incident te rapporteren of door te geven naar iemand die wel actie wil ondernemen. Met andere woorden, men blijkbaar meldingen niet zo serieus wil nemen als 't ze op dat moment persoonlijk niet uitkomt (zit immers geen belonging waardering aan gekoppeld om 't te doen).

*** in (z) zit 'm ook de crux als het gaat om waarom Schiphol management het alsmaar niet voor elkaar krijgt om de oh zo mooie woorden in beleidsdocumenten om te zetten naar een zichtbaar Functionele operationele structuur.**

Is natuurlijk ook voorspelbaar dat het mis blijft lopen als men bijvoorbeeld weet dat 'security officers' niet afgerekend/beloond worden op tastbare resultaten maar alleen op de uurtjes dat ze 'werken'. Dat is vragen om struisvogel politiek en afschuiven van verantwoordelijkheden naar 'anderen'.
Neem bijvoorbeeld de huidige "Director Safety and Environment and CISO at Royal Schiphol Group" waarbij men het blijkbaar geen integriteit belangenverstrengeling lijkt te vinden dat iemand 2 petten op heeft waarbij er eigenlijk functiescheiding zou _moeten_ zijn om te zorgen dat een slager niet zijn eigen vlees laat goedkeuren vanuit een machtspositie.
Wat ook opvalt is dat de "CISO" klaarblijkelijk zelf zich niet zo veel lijkt aan te trekken van "Security Awareness" Trainingen en essentiële beveiliging principes ? Althans, die indruk zou men kunnen krijgen als men ziet dat die persoon zonder schaamte roekeloos opvallend veel en gedetailleerde Informatie over zichzelf en de organisatie zo maar deelt met de wereld en hostile actors.
Daardoor zichzelf en de organisatie en de nationale vitale infrastructuur / staatsveiligheid roekeloos extra in gevaar brengt, wetende dat die informatie gebruikt blijkt te worden voor o.a.: Omkoping/Chantage; Profilering; Identiteit diefstal; Social Engineering; APT's via persoonlijke apparaten; Spionage & Sabotage; enz.. ; enz..

:(linkedin.com/in/hedzer-komduur-39ba7a5/
"I am driven, like assessing the big picture, but also have a keen eye for details, both in business and in people."
* schiphol.nl/nl/schiphol-group/director-safety-en-environment/

Met andere woorden, het Schiphol bestuur het blijkbaar prima lijkt te vinden als de "Need to know" basis beveiliging regel compleet genegeerd mag worden, als het gaat om persoonlijke winst belangenverstrengelingen, zoals publiek opscheppen over hoe fantastisch men zou zijn voor een overbetaalde bureaucraten positie ?
Als men dan ook ziet hoe veel als vertrouwelijk geclassificeerd behorende INTERNE data de organisatie 24/7 naar het publieke internet lekt via vele wegen..., omdat/doordat de CISO en alle andere Security Officers er blijkbaar geen zin in hebben om er (naar wettelijke verplichtingen behorende) zeer eenvoudig voor te _zorgen_ dat alle interne&gevoelige "meta-data" die niemand anders iets aan gaat, er uit gewist/gefilterd is alvorens computer bestanden en emails naar Buiten gaan. Zo ook nogal wat IT services producten die nog exact laten weten welke software en versie en security instellingen ze hebben, via netwerk communicatie protocollen roekeloos met de wereld gedeeld blijft worden, ondanks dat iedere security professional donders goed weet dat die informatie gebruikt word om specifieke kwetsbaarheden te vinden/identificeren voor gerichte long term covert intrustions. [*t2] Als die extra details informatie hoeft helemaal niet beschikbaar gemaakt te worden, is immers verder nergen voor "nodig". => "Elementary, my dear Watson!"

Wat ook opvallend is, is dat er geen functioneel beleid met pro-active procedures actief blijkt te zijn om spionage en criminele infiltratie buiten de organisatie en infrastructuur te houden.
Ook op dat vlak zijn er vooral oh zo mooie P.R. type woorden op papier gezet, bijv: schiphol.nl/nl/werken-op-schiphol/pagina/help-ondermijning-te-voorkomen-en-te-bestrijden/
Extra beschamende feit daarbij is dat die website waar naar verwezen is [www.sterkeluchthaven.nl] zelf opvalt ivm gebrek aan voldoen aan wettelijke en beveiliging voorschriften.
Met andere woorden, een bureaucraat heeft 't bedacht en gemakzuchtig maar ergens over de schutting gegooid voor verdere uitvoering, Zonder de noodzakelijke controles uit te willen voeren?
? laat de slager z'n eigen vlees maar al te graag goedkeuren door slinks goedkeuring te "kopen" bij bedrijven die zogenaamde 'pen-test' en audits services verkopen (..met een uitkomst die de opdrachtgever wenst te krijgen..)

En zo zijn er nog wel wat observaties en bevindingen, als het gaat om een Machiavellisme spel dat roekeloos gespeeld blijkt te worden, ondanks dat het gaat om de veiligheid van ons allen zelf.

Waarbij men tot de conclusie zou kunnen komen dat de onderstaande vacatures er vooral zijn voor de "De nieuwe kleren van de keizer" Show, zoals uitvoering en handhaving verantwoordelijkheden steeds verder op alsmaar meer sub-functionarissen af te schuiven, zonder tastbare resultaat verplichtingen.
Ipso facto: Er een zwijgcultuur gecultiveerd blijkt te worden, in ruil voor een riant 'loon'.

--
https://careers.schipholgroup.com/vacatures/it-en-data/senior-cyber-security-manager
https://careers.schipholgroup.com/vacatures/it-en-data/cyber-security-manager
https://careers.schipholgroup.com/vacatures/security/security-process-developer
https://careers.schipholgroup.com/vacatures/security/security-auditor
https://careers.schipholgroup.com/vacatures/security/security-quality-training-manager
https://careers.schipholgroup.com/vacatures/techniek-en-bouw/strategic-advisor-center-of-excellence
https://careers.schipholgroup.com/vacatures/it-en-data/people-lead-asset-and-information-management-aim
-
https://careers.schipholgroup.com/vacatures/techniek-en-bouw/business-information-security-officer
+Begeleiden van eigenaren aangaande maatregelen ter versterking van cyberweerbaarheid.
+Vertalen van het security jaarplan naar concrete acties voor eigenaren.
+Verbeteren van (security) processen in het kader van de ""PCDA""-cyclus.
+In kaart brengen van risico's en dreigingen bij diverse assets op IT en OT-gebied.
++Adviseren (gevraagd en ongevraagd) van de organisatie.
+Meedraaien in IT/OT projecten als vertegenwoordiging van security
"
?=> anw.ivdnt.org/article/zwijgcultuur

Maar hoe dan ook, C'est la vie.

? Mocht het zo zijn dat er iemand binnen het bestuur van Schiphol Group, of MinBZK, er wel degelijk waarde aan zou willen hechten om het Risicomanagement en Compliance op beveiliging van Luchthaven Schiphol, alsnog aantoonbaar naar behoren goed op orde te maken binnen korte tijd?
Dan kan dat zeer eenvoudig gerealiseerd worden door de huidige Ivoren Toren structuur CISO te vervangen, en er een type op die functie te zetten die wel vakkundig open en integer naar eer en geweten afgerekend/beloond gaat worden puur en alleen op basis van daadwerkelijk onafhankelijke geteste/gecontroleerde resultaten.
Dus 0,- krijgt en er uit vliegt, als blijkt dat de mooie woorden op papier niet daadwerkelijk waar gemaakt zijn.
Als een CISO persoonlijk Verantwoordelijk gesteld gaat worden voor feitelijke handhaving van uitvoering, gaat inherent Schiphol Luchthaven wel veel beter om met het beveiliging en compliance op orde krijgen en houden,
toch ? ;-)

> On Wed, 12 Feb 2025 12:07:15 +0000
> Juridisch <juridisch@onderzoeksraad.nl> wrote:
>
> Your message
>
> To: Juridisch
> Subject: Re: Opvolging gesprek
> Sent: Wednesday, February 12, 2025 11:07:24 AM (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
>
>> was read on Wednesday, February 12, 2025 1:07:15 PM (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna.

To: Juridisch <juridisch@onderzoeksraad.nl>
Subject: Re: Read: Re: Opvolging gesprek

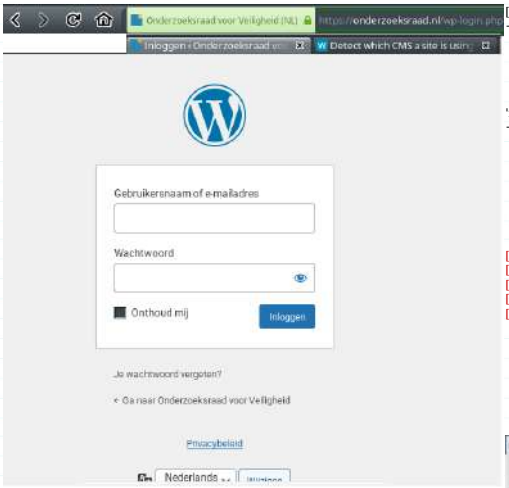
Is het "onderzoeksraad voor de veiligheid" bestuur nog van plan om iets zinvols te gaan ondernemen om die zeer ernstige misstand z.s.m. de nodige aandacht te gaan geven, alvorens 't nog erger mis loopt ?
Of steekt men net als het Schiphol bestuur en NCTV en ILenT, de koppen liever bureaucratisch in 't warme zand, en roept men tzt "geen active herinnering aan"/"Wir haben es nicht gewußt" als de media bekend maakt wat er gaande is en wie er Niet volgens taakbeschrijving in actie gekomen zijn...

Ter info:
o.a. jullie website/webserver [onderzoeksraad.nl has address 85.209.110.220 @ Fundaments B.V.] is ook niet compliant met BIO, AVG, enz. Dus in overtreding van regelgeving veiligheid.
Is zelfs al langere tijd volledige toegang door onbevoegden. Blijkbaar zonder dat men daar erg in heeft, of 't geheel niet interesseert ?

Men geeft dus zelf het verkeerde Voorbeeld, waardoor jullie adviezen ook niet zo serieus genomen kunnen worden?

Lijkt zelfs niemand een probleem te vinden dat o.a. deze (BBN2) vertrouwelijke data ook in handen van derden komt:
 ** https://onderzoeksraad.nl/home/meldingen-luchtvaart/

?-> onderzoeksraad.nl/home/werkwijze/informatie-verzamelen/

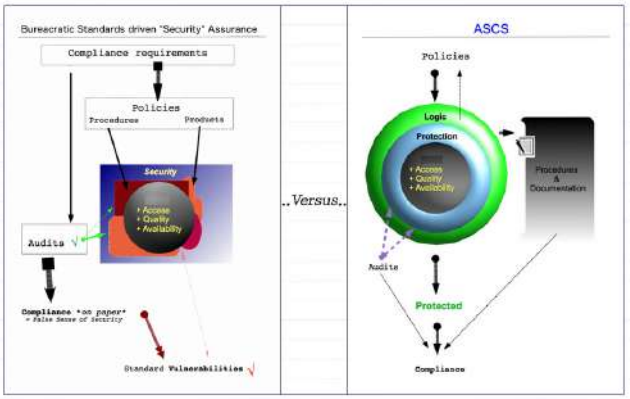


[+] WordPress version 6.6.2 identified (Outdated, released on 2024-09-10).
+] Headers
| Interesting Entries:
| - Server: Apache
| - Content-Security-Policy: default-src * 'unsafe-eval' 'unsafe-inline' data: filesystem: about: blob: ws: wss:; base-uri 'self';
| - Referrer-Policy: origin-when-cross-origin
| - Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
+] sitepress-multilingual-cms
| Location: https://onderzoeksraad.nl/wp-content/plugins/sitepress-multilingual-cms/
|
| Version: 4.6.15 (100% confidence)
| Found By: Meta Generator (Passive Detection)
| - https://onderzoeksraad.nl/, Match: 'WPML ver:4.6.15 stt'
| Confirmed By: Readme - Stable Tag (Aggressive Detection)
| - https://onderzoeksraad.nl/wp-content/plugins/sitepress-multilingual-cms/readme.txt

[i] User(s) Identified:
[+] nover
[+] ingrid
[+] lisanne
[+] wp-zimpa

connect.onderzoeksraad.nl 77.242.112.135
mail.onderzoeksraad.nl 77.242.112.137
remote.onderzoeksraad.nl : 77.242.112.134
vpn.onderzoeksraad.nl 77.242.112.132
www.onderzoeksraad.nl 85.209.110.220 / 2a03:3400:8:200::2
www2.onderzoeksraad.nl ""
:(

 # Fixing the Risk-management => Security & Compliance issues, can only be done if.. C-Level management wants to allow it to be fixed..?
 # When it is allowed and sanction by leadership, then the structure can be corrected within ~1 year (without extra financial investments nor products)
By using the simple "Safeguard ™" method. With full result warranty and open scope public verification.



- When choosing the *bureaucratic standards* driven "security" assurance approach, your organisation puts its own control & autonomy in 2nd place.
- ASCS, lets an organisation actually be in control of its self !

ASCS is a coherent method to melt the technology parts with group psychology & dynamics aspects of an organisation together in a self-balancing structure.

Side effects:

- Simplification of organisation and infrastructure
- Serious operational cost reductions
- Shorter change project turnaround
- Increasing in-house competence
- Inherent flexibility & resilience
- Justifiable best practice

Etymology

The name ***Sciphol*** appears in an official document from 1447.[10]

11 September 1447.

Gegeven in den Hage den XI*den in Septembri int jair ons Heeren duesent vierhondert seven ende veertich.*

Henrich van Borselen, heer van *der Veere*, geeft, als collator der kerk van *Aemstelreveen*, vergunning aan Reynen Struys, pastoor dier kerk, om vier maden lands, liggende

5

66

in *Aelsmerbanne* in *Sciphol*, te verkoopen en de opbrengst te besteden tot de stichting van een nieuw kerkgebouw in plaats van het oude, hetwelk vergaan is.

Brief op perkament met het zegel van den heer van *der Veere* in rood was.

Archief, lade A 10, N. 3, 1.

One of many explanations of the possible origin & meaning of the name:

Gathering wood

The word Sciphol first appears in old documents from around 1450 and refers to a stretch of land. This area was part of Aalsmeer, located south of Amstelveen, but was most certainly not a lake or sea. It was in fact a marshy area where people could go to gather wood. Schip Holl dates from the 15th century and combines the Gothic words 'Skip' (meaning wood, timber) and Holl (low-lying land). Later on a fort was also built on this spot, which carried the same name.

On September 19 in 1916, farmers in the vicinity of Fort Schiphol hear a strange hum in the air. A little later they see a plane landing, a Farman biplane of the Aviation Department of the Dutch Army. This is the beginning of Schiphol airport.