INFORMATIE
BEVEILIGINGS
DIENST

VNG Overijssel

‘Als je deze sessie mist, word je gehackt’ - Informatieveiligheid

Jule Hintzbergen

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

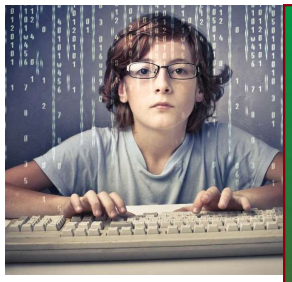
Waarom?

Soorten aanvallen

Gericht

Ongericht

Door wie



Eenvoudig - Complex

Met welk doel

INFORMATIE
BEVEILIGINGS
DIENST

Zijn er voorbeelden van gerichte aanvallen?

HÂCK//19
THE HAGUE

INFORMATIE BEVEILIGINGS DIENST

Zijn er voorbeelden van gerichte aanvallen bij gemeenten?

Hallo D

Hier is mijn nieuwe accountinformatie.

ING Bank
Accountnaam: A
Bankrekeningnummer: 06

Ik wil dat mijn volledige salaris voor juni wordt overgeschreven naar dit nieuwe account.
Laat me weten wanneer de wijziging is aangebracht.

3

Erg bedankt,
A

Hoi A

Als je mij deze week nog je nieuwe rekeningnummer en tenaamstelling doorgeeft, kan je salaris van juni naar het nieuwe nummer.
Anders wordt het vanaf salaris juli.

Groet, D

2

Hallo D

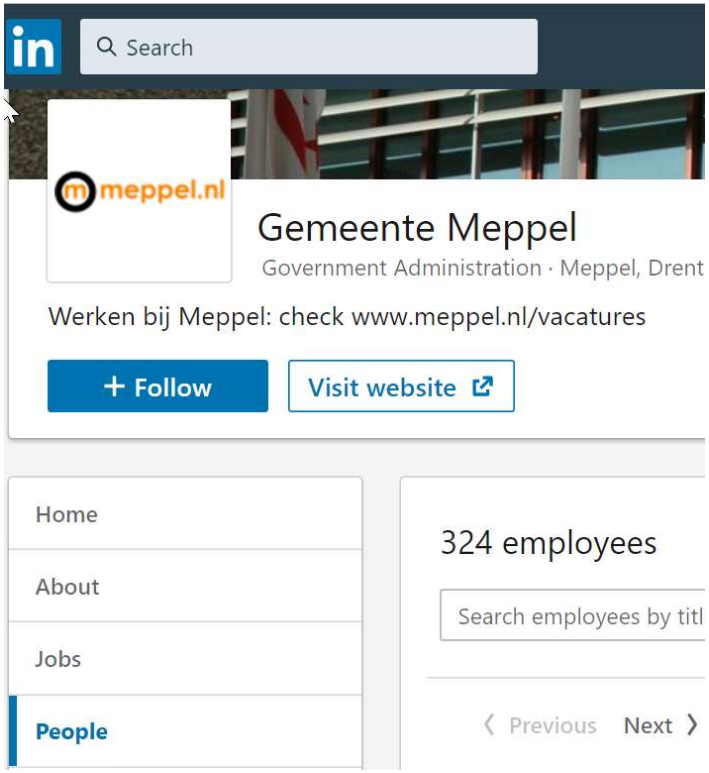
Ik heb mijn bank gewijzigd en wil mijn salarisgegevens wijzigen. Kan de wijziging van kracht worden voor de huidige betalingsdatum?

1

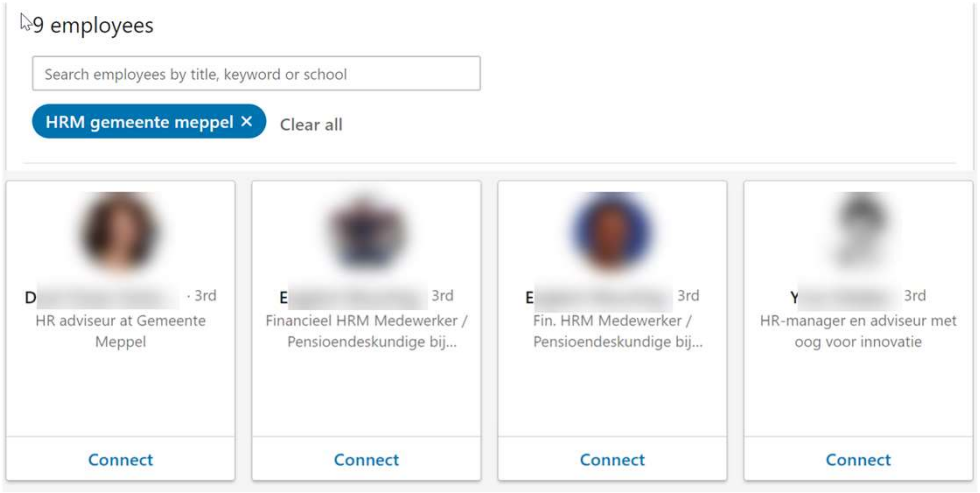
Erg bedankt,
A

INFORMATIE BEVEILIGINGS DIENST

Hoe komen hackers aan gemeentelijke e-mail adressen?



Diverse openbare bronnen:
LinkedIn, openbare aanbestedingsdocumenten, website van gemeente, etc.



INFORMATIE
BEVEILIGINGS
DIENST

Wat kun je doen tegen zulke phishing mails?

Bewustwording bij alle medewerkers.
Sommige afdelingen extra aandacht.

Juiste/sluitende procedures.

Twee factor authenticatie voor zowel telewerken, maar ook voor online webmail van de gemeente.

INFORMATIE
BEVEILIGINGS
DIENST

Hoe vaak vinden ongerichte aanvallen plaats?

Elke dag !

INFORMATIE
BEVEILIGINGS
DIENST

Waar controleren hackers op bij ongerichte aanvallen?

INFORMATIE
BEVEILIGINGS
DIENST

Wat ging er ook alweer mis in Lochem?

Een mogelijkheid om een server te beheren vanaf afstand was bereikbaar voor iedereen op internet.

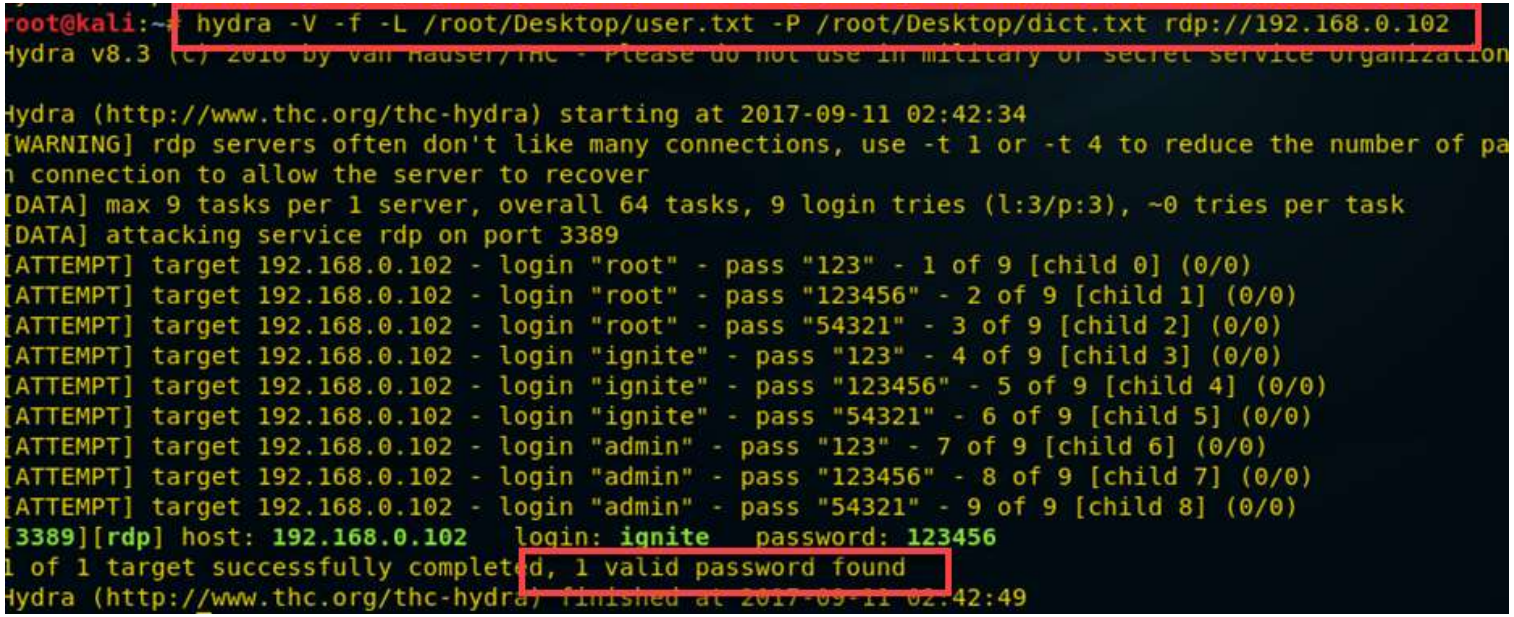
Daarna was het mogelijk om een gebruikersnaam met wachtwoord te raden door gebruik van slecht wachtwoord.

Vergelijkbaar met een achterdeur met een zwak slot zonder camerabewaking.

INFORMATIE
BEVEILIGINGS
DIENST

Wat ging er ook alweer mis in Lochem?

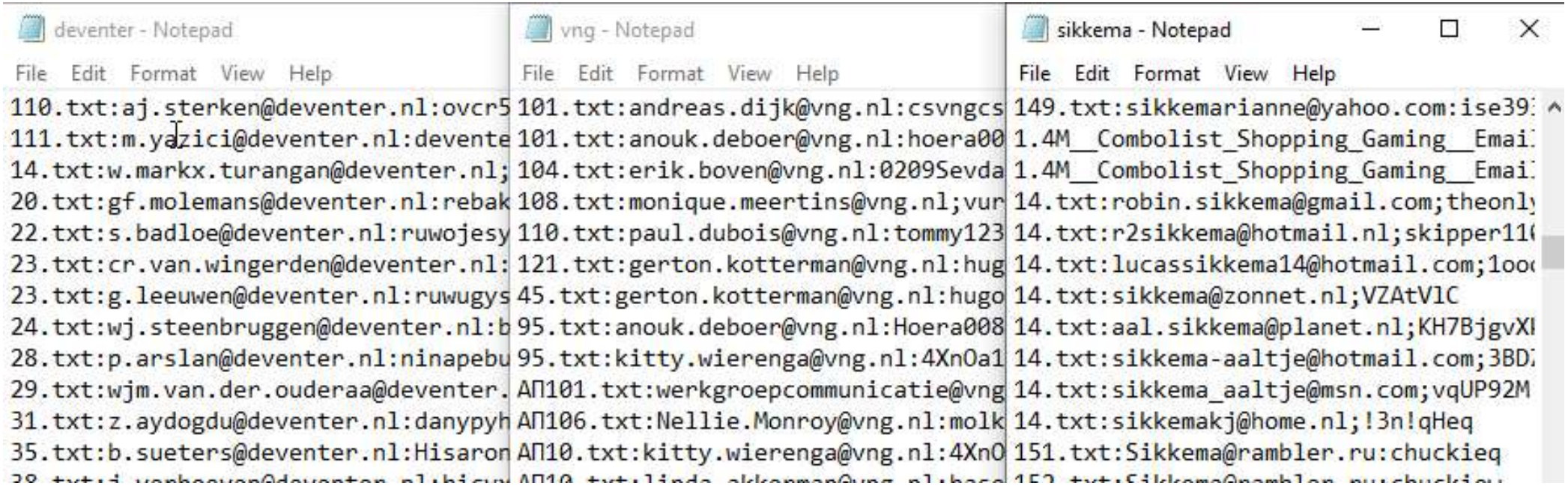
- Langere tijd ongemerkt allerlei gebruikersnamen en wachtwoorden geprobeerd
- De tools om zo'n aanval uit te voeren zijn eenvoudig, gratis en door iedere kwaadwillende uit te voeren.



INFORMATIE
BEVEILIGINGS
DIENST

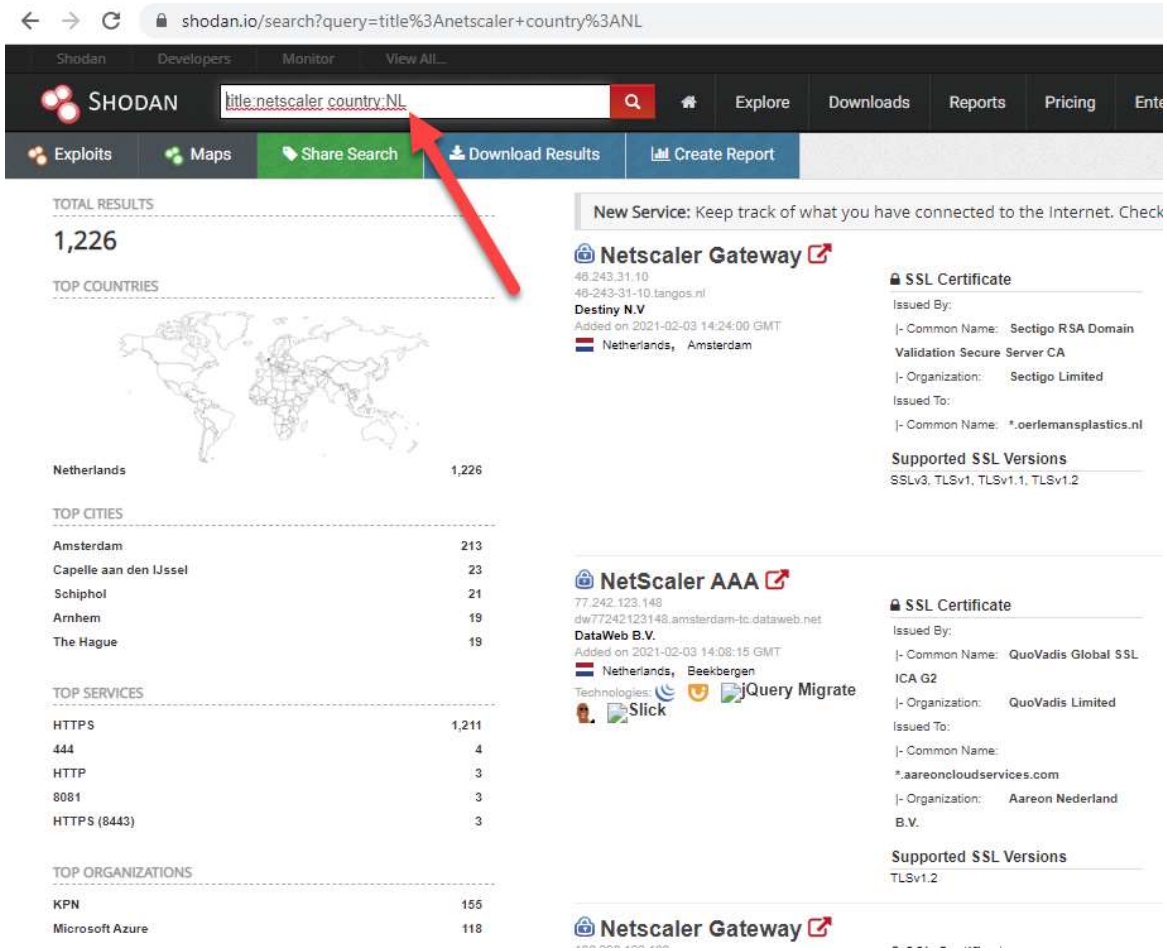
Hoe komen hackers aan die wachtwoorden?

Wachtwoorden databases met miljoenen wachtwoorden zijn beschikbaar.



INFORMATIE
BEVEILIGINGS
DIENST

Hoe weten de hackers waar toe te slaan?

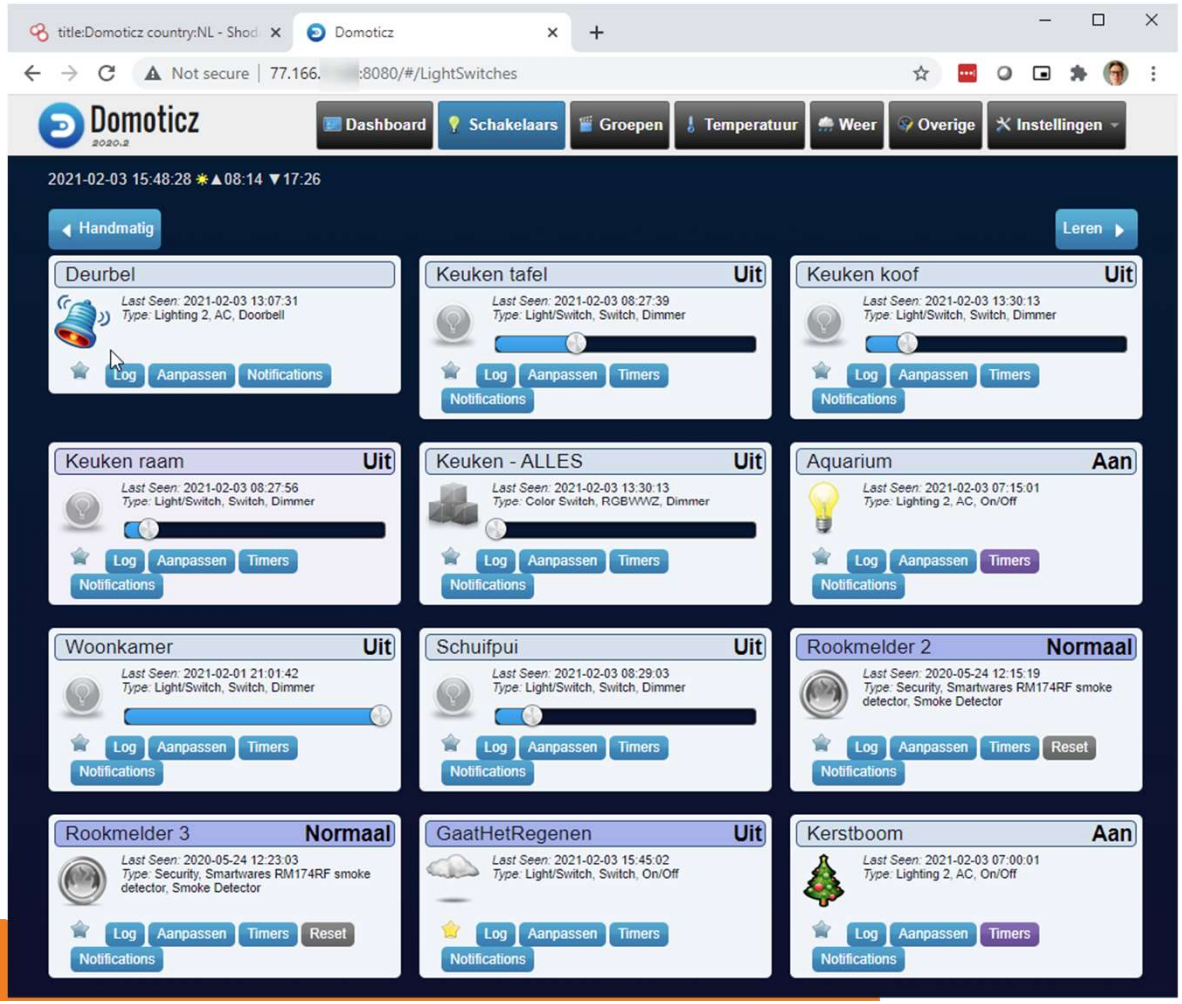


Shodan – Google voor security onderzoekers

Makkelijk een overzicht te genereren van alle Citrix Netscaler/Gateway servers.

INFORMATIE
BEVEILIGINGS
DIENST

Heb je ook een eenvoudiger voorbeeld?

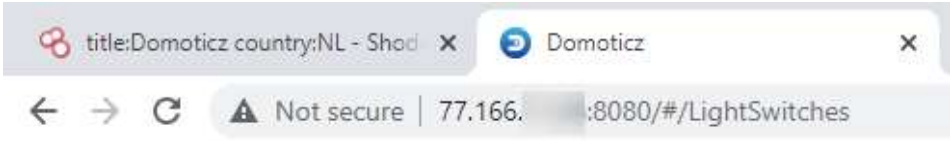


Deze persoon in Nederland heeft als hobby Domotica.

Ook vanaf zijn mobiel als hij onderweg is kan hij zijn slimme systemen thuis bedienen.

Alleen de rest van de wereld ook…

Iedereen die de volgende link opent, kan de schakelaren bedienen:



INFORMATIE
BEVEILIGINGS
DIENST

Wat moet ik doen als ik een hacker vermoed op ons netwerk?

Digitaal forensisch onderzoek

In tegenstelling tot een inbreker van een woning, wil een digitale inbreker vaak zo lang mogelijk in de omgeving blijven, maar laat wel sporen na.

Vaak uitbesteden -> externe expertise – GGI veilig (retainer)

INFORMATIE
BEVEILIGINGS
DIENST

Dreigingsbeeld

INFORMATIE
BEVEILIGINGS
DIENST

Aansprekende incidenten

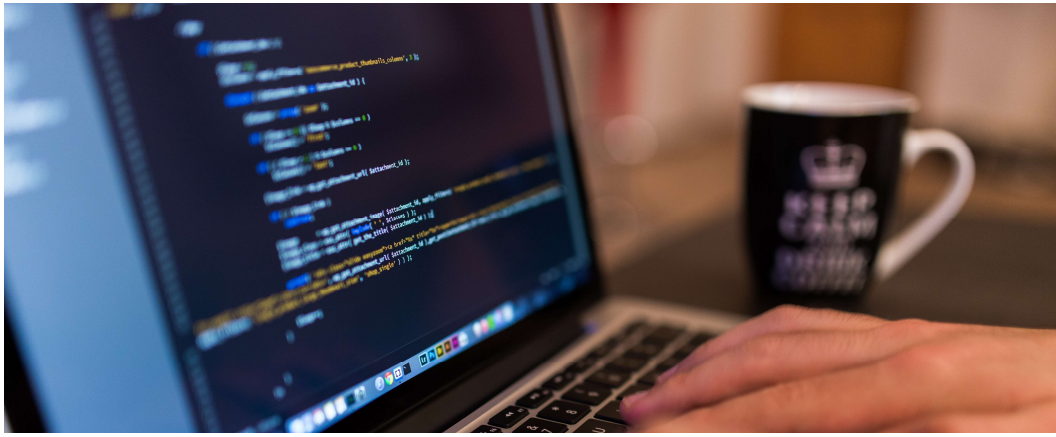
- Datalekken in de eigen organisatie sinds de meldplicht
- Lochem 2019
- Universiteit van Maastricht 2019
- Verplicht afschakelen Citrix 2020
- Hof van Twente
- Solarwinds (generiek: aanvallen via een software maker)
  - Cisco
  - Fireeye
  - MS
- Hacken waterleiding bedrijf via beheertoegang

NE22

INFORMATIE
BEVEILIGINGS
DIENST

Dreigingen 2020-2021

- **Intern en onbedoeld**
- **Extern, bedoeld maar ongericht**
- **Extern, bedoeld en gericht**
- **Intern en bedoeld**



Dia 17

NE22 ik zou alleen de 4 bullets opnemen, de rest gewoon toelichten met voorbeelden
Nausikaa Efstratiades; 2-2-2021

NE23

INFORMATIE BEVEILIGINGS DIENST

Risico’s

Risico’s voor de ambtelijke organisatie

- Bedrijfscontinuïteit
- Integriteit van gegevens
- Datalekken

Risico’s voor openbaar bestuur en politiek

- Imagoschade
- Financiële schade
- Schade aan democratische processen

Risico's voor inwoners en ondernemers

- Gegevens in verkeerde handen
- Dienstverlening van de gemeente niet beschikbaar
- Ontwrichting van alledaagse processen

Dia 18

NE23 ook hier alleen de hoofdpunten noemen en deze toelichten, anders erg veel tekst. Misschien dat je deze sheet zelfs weg kunt laten

Nausikaa Efstratiades; 2-2-2021

INFORMATIE BEVEILIGINGS DIENST

Handelingsperspectief

INFORMATIE
BEVEILIGINGS
DIENST

Voer regie over risicomanagement

Advies:

- Positioneer de CISO binnen de gemeente
- Koppel risicomanagement aan de P&C-cyclus
- Spreek management aan op de juiste dingen doen
- De CISO adviseert over maatregelen en ondersteund

INFORMATIE
BEVEILIGINGS
DIENST

Besef dat techniek niet de belangrijkste factor is

Ook uit de vorige uitgaven van het dreigingsbeeld blijkt:

- **De meeste fouten zijn menselijke fouten**

Advies:

- Informatiebeveiliging vereist strategie
- Techniek moet wel op orde zijn, maar heb ook aandacht voor de menselijke kant
- Bij uitbesteding: houd grip op de leverancier

INFORMATIE
BEVEILIGINGS
DIENST

Cultiveer een veilige organisatie

Advies:

- Faciliteer bewustwording processen en zorg dat iedereen meedoet
- Vraag naar de status van het Incidentmanagement beleid en het incident management proces
- Laat incidenten oefenen om de weerbaarheid te vergroten
- Heb zicht op beveiliging van ketenpartners
- Directie en management geven het goede voorbeeld

- **Zet het op de agenda!**

INFORMATIE
BEVEILIGINGS
DIENST

Bied veilige gereedschappen

Advies:

- Spreek verantwoordelijken aan op het faciliteren van veilig werken en gegevens uitwisselen met burgers
- Faciliteer veilige gegevens uitwisseling met burgers en bedrijven
- Investeer in veilige gereedschappen
  - Zoals 2-factor authenticatie

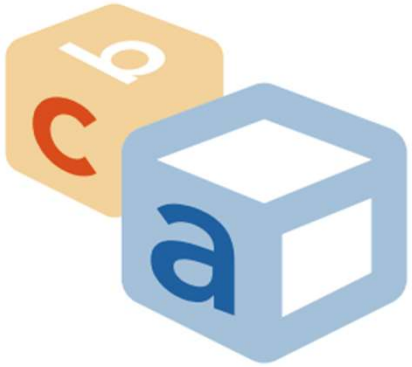
INFORMATIE
BEVEILIGINGS
DIENST

Zorg voor een open cultuur

Advies:

- Laat rapporteren over incidenten
- Vraag van de grotere incidenten een evaluatieverslag om op die manier inzicht te krijgen wat er verbeterd kan worden
- Zorg dat medewerkers kunnen leren van incidenten
- Een afreken cultuur draagt niet bij tot meer veiligheid, incidenten blijven onder de pet

INFORMATIE
BEVEILIGINGS
DIENST



Faciliteer dat de basis op orde komt

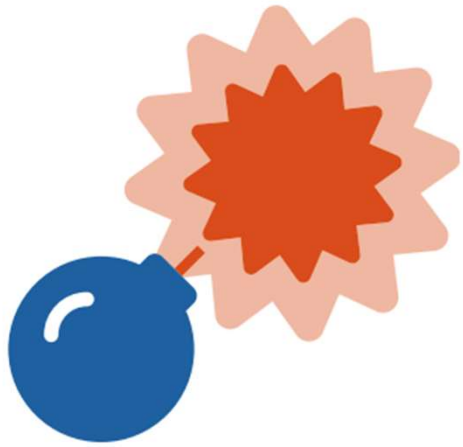
Advies:

- De meeste incidenten kunnen worden voorkomen door de basis op orde te hebben.
- De IBD heeft hiervoor een programma opgezet: VDW – Verhogen Digitale Weerbaarheid:

1. Weten wat je in huis hebt (configuratiemanagement op orde)
2. Up-to-date houden (patch- en changemanagement
3. Veilig inrichten ICT omgeving (hardening en middelen)
4. Toegangsbeheer op orde, veilig inloggen, 2FA
5. Monitoren wat er gebeurt, trends herkennen

INFORMATIE
BEVEILIGINGS
DIENST

Oefen en wees voorbereid op incidenten



Advies:

- Vraag het management over de status van bedrijfscontinuïteit plannen, hoe zijn zij voorbereid?
- Faciliteer oefenen met incidenten
- Inzicht hebben in wie wanneer nodig is
- Overweeg een retainer voor forensisch onderzoek (via GGI veilig)
- Maak een watermeter lijstje

INFORMATIE
BEVEILIGINGS
DIENST

Samenvattend

- De gemeente is kwetsbaar
- Jullie hebben een belangrijke rol in verhogen van de digitale weerbaarheid van de bedrijfsvoering
- Versterk:
  - Verhogen Digitale Weerbaarheid (De basis op orde)
  - Informatiebeveiliging op de agenda krijgen en houden
  - Maak managers verantwoordelijk voor de beveiliging van hun processen
  - de menselijke schakel
  - Versterk de CISO
  - Samen organiseren, vertel de IBD wat behoeften zijn

INFORMATIE
BEVEILIGINGS
DIENST

Dreigingsbeeld

INFORMATIE
BEVEILIGINGS
DIENST

Nassaulaan 12
2514 JS Den Haag

CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)

info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie

INFORMATIE
BEVEILIGINGS
DIENST

Ondersteuningsproducten van de IBD

- Algemeen:
  - https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
- Verhogen digitale weerbaarheid:
  - https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid
- 2-factor authenticatie:
  - https://www.informatiebeveiligingsdienst.nl/product/handreiking-2-factor-authenticatie-2fa-voor-gemeenten/
- Incident response en oefenen:
  - https://www.informatiebeveiligingsdienst.nl/product/factsheet-gehackt-hoe-nu-verder/
  - https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/
- Plan van aanpak bedrijfscontinuïteit:
  - https://www.informatiebeveiligingsdienst.nl/product/plan-van-aanpak-bedrijfscontinuiteitsbeheer/

3 punten:

1. Hacks zijn doorgaans ongericht
2. De IBD is er voor gemeenten om bij te staan bij beveiligingsincidenten, maar ook om te adviseren bij preventie (voorkomen is beter dan genezen)
3. De gemeente moet aan de slag met het programma Verhogen Digitale weerbaarheid (VDW) om beter voorbereid te zijn (zorg dat je de basis op orde hebt en zo de grootste dreigingen het hoofd kunt bieden

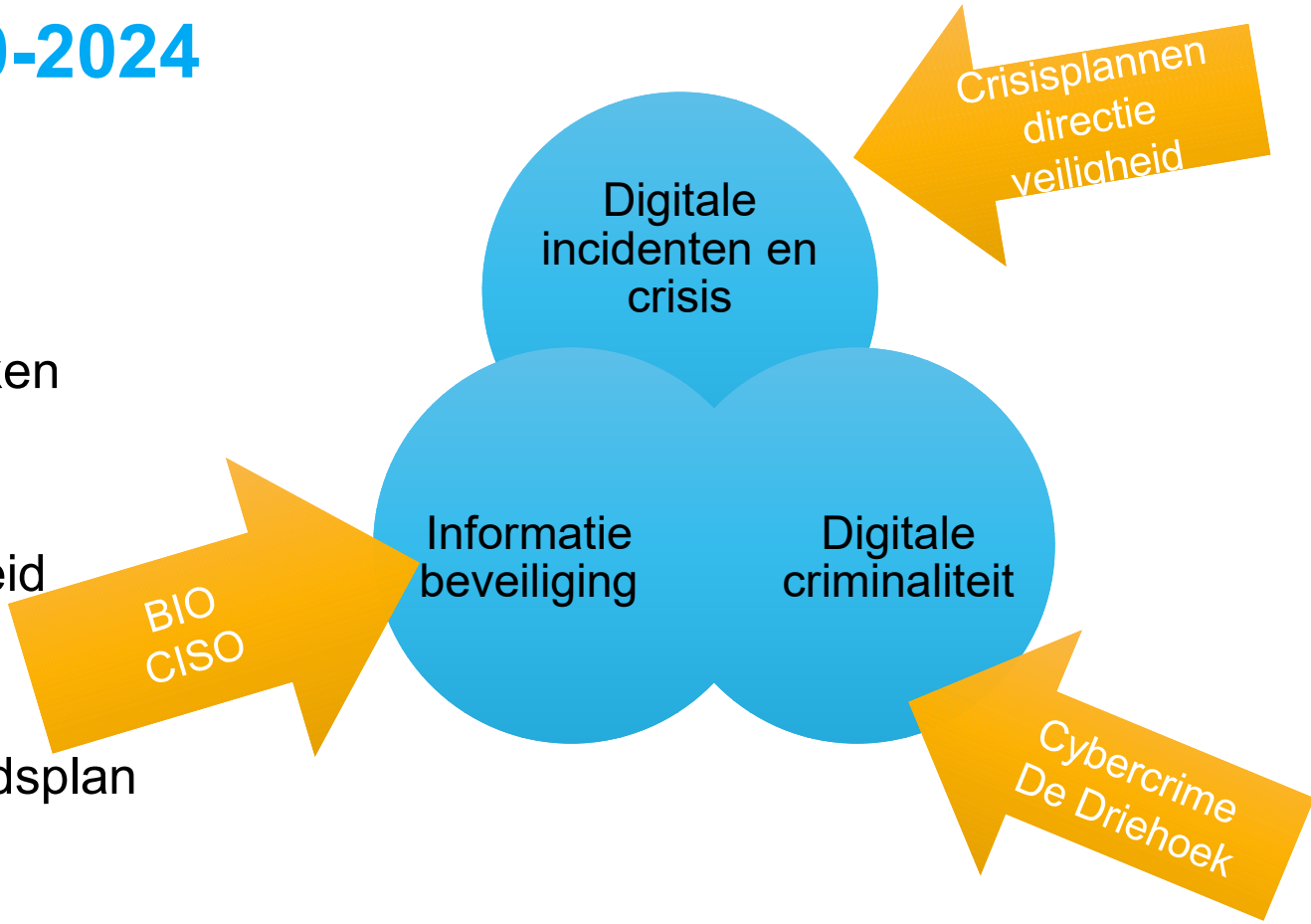
NE24

INFORMATIE BEVEILIGINGS DIENST

Digitale agenda 2020-2024

Kernpunten:

- incidenten melden bij IBD
- Incidentenbestrijdingsplan maken
- intergemeentelijke solidariteit
- periodiek oefenen: weerbaarheid
- agenderen in B&W
- opnemen in Integraal Veiligheidsplan
- budget vrijmaken
- gebruik maken van voorzieningen en programma's (IBD)



NE24 opzich handige en nuttige sheet, maar misshcien toch beter hieruit halen, veel info in korte tijd.
Nausikaa Efstratiades; 2-2-2021

INFORMATIE
BEVEILIGINGS
DIENST

Backup sheets over de IBD

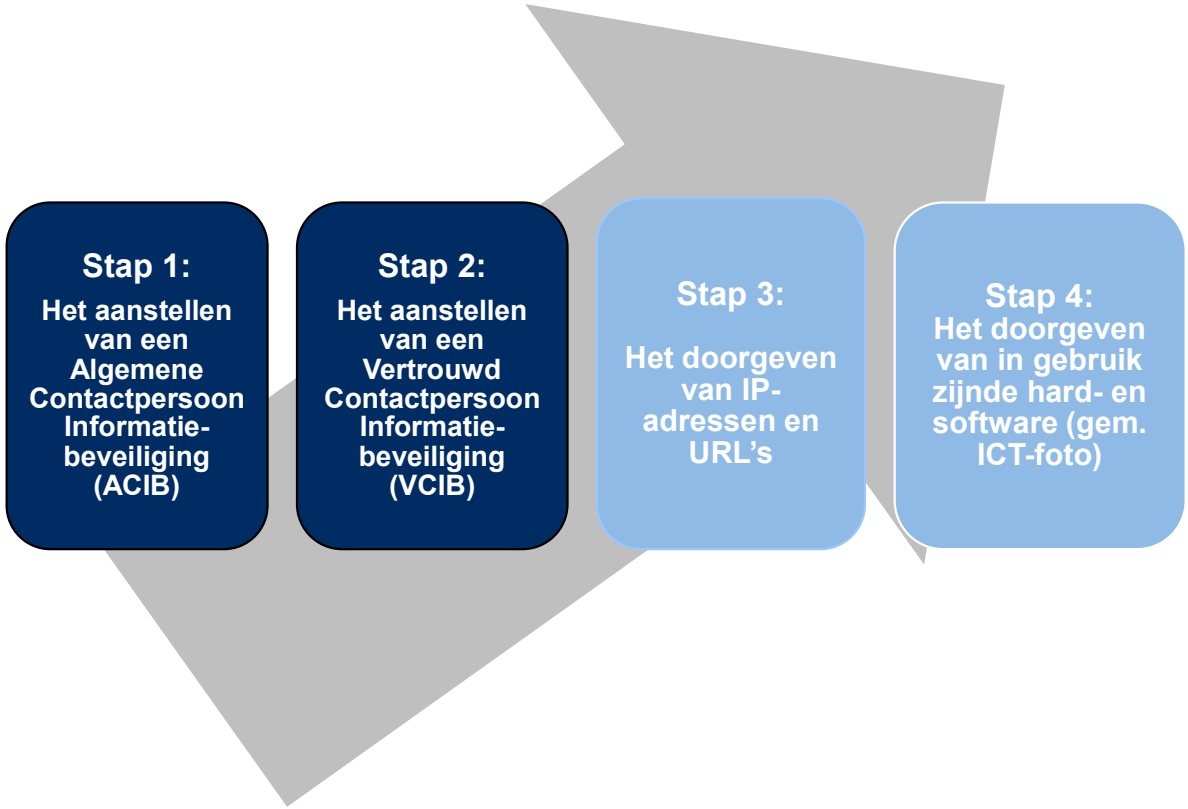
INFORMATIE
BEVEILIGINGS
DIENST

De IBD

- Gezamenlijk initiatief alle Nederlandse gemeenten vanuit behoefte van gemeenten aan coördinatie en ondersteuning bij informatiebeveiliging
- IBD is de CERT van alle gemeenten en gemeentelijke samenwerkingsverbanden, aangewezen door minister in 2020
- Schakelpunt gemeenten met het Nationaal Cyber Security Centrum (NCSC) sinds 2013
- 2019 - Privacy ondersteuning

INFORMATIE
BEVEILIGINGS
DIENST

Aansluiten bij de IBD



INFORMATIE
BEVEILIGINGS
DIENST

Kracht IBD

- Juiste contactpersonen van alle gemeenten en hun leveranciers met één druk op de knop bereikbaar bij incidenten (stap 1 & 2)
- Kennisdeling en kennisvermeerdering door ervaringen en uitwerkingen van alle gemeenten
- Belangenbehartiging naar ketenparttners
- Vraagbundeling – ook richting partijen als de Politie, Fraudehelpdesk, Centraal Meldpunt Identiteitsfraude, Autoriteit Persoonsgegevens, Internationale CERT's, etc.
- Focus op de doelgroep (gem. CISO's en informatiebeveiligers) en samenwerking met VNG voor bestuurlijke awareness.
- Vanaf 2019 ook focus op FG's en PO voor privacy
- 2020 secundair uitbreiding focus naar GS

INFORMATIE
BEVEILIGINGS
DIENST

Taken van de IBD

1: CERT: preventie, detectie, coördinatie en oplossing

2: Projecten & Advies, Informatieveiligheid en Privacy

3: Kennisdelen en –vermeerderen, IB en Privacy

INFORMATIE
BEVEILIGINGS
DIENST

CERT (ondersteuning incidentmanagement)

- Preventie (Stap 4)
  - Kwetsbaarheden (obv CVE, meldingen leveranciers, Responsible Disclosure, meldingen gemeenten, meldingen burgers)
  - Helpdesk
- Detectie (Stap 3)
  - IP adressen monitoring bij NCSC
  - Nationaal Detectie Netwerk
  - Dmarcian (DMARC monitoring)
  - Samenwerking SOC GGI Veilig
  - Threat Intelligence, (toekomst Landelijk dekkend stelsel van CERT's)
- Coördinatie (24x7)
  - Incidentmanagement
  - Coördinatie tussen gemeenten onderling en met leveranciers
  - Woordvoering & Communicatieadvies

INFORMATIE
BEVEILIGINGS
DIENST

Projecten & Advies

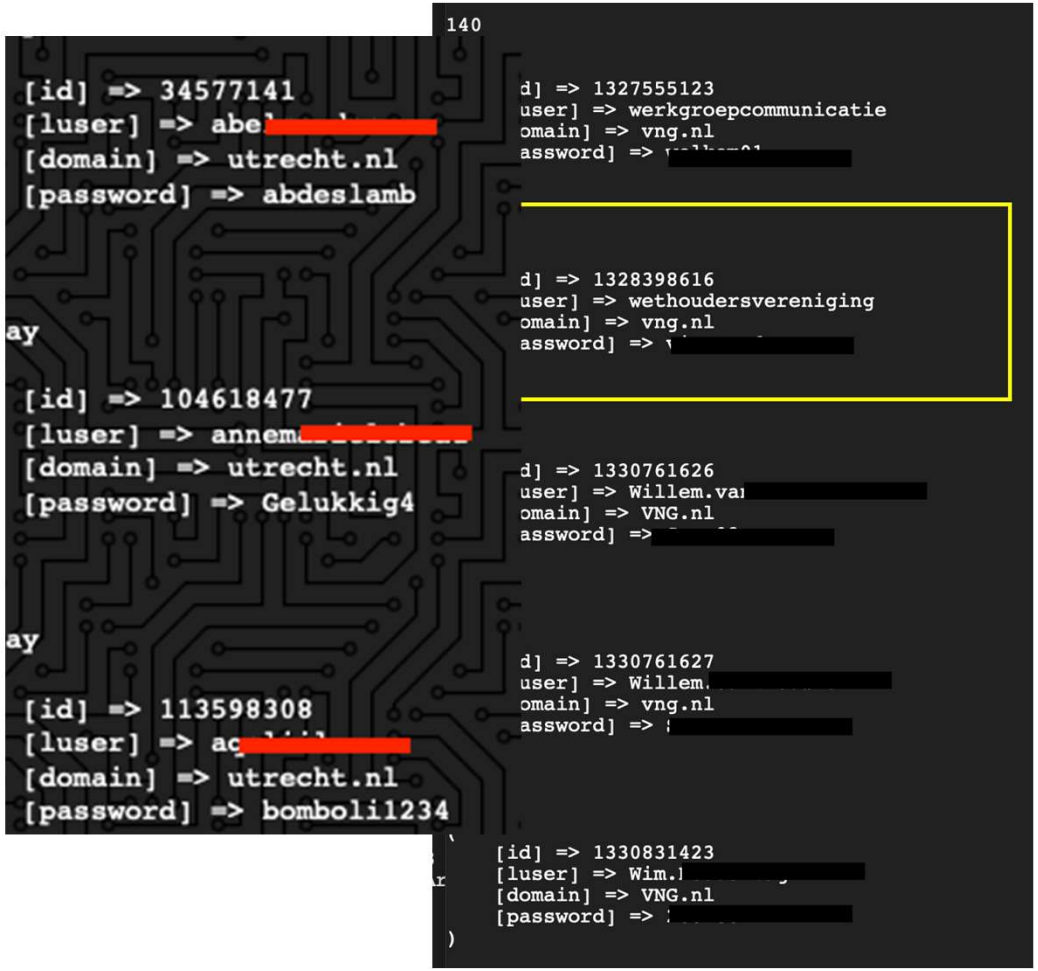
- Schrijver en beheer BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten)
- Co auteur van de BIO (Baseline Informatiebeveiliging Overheid)
- Aanpak BIO specifiek voor gemeenten
- Operationele producten als handvat voor implementatie
- Projecten van VNG/VNG Realisatie en / of meerdere gemeenten
- Verhogen Digitale Weerbaarheid
  - Module 1: De basis op orde
  - Modele 2: Monitoring & Response
  - Module 3: Awareness
  - Module 4: BCM
  - Module 5: ICS/SCADA

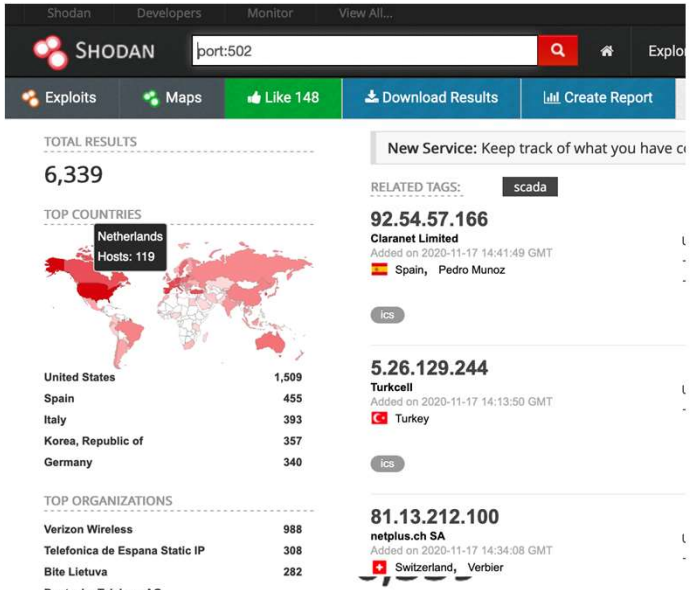
https://www.ibdgemeenten.nl/projecten/

INFORMATIE
BEVEILIGINGS
DIENST

Kennisdelen en -vermeerderen

- Collectieve aanpak: Samen organiseren (Voorbeeld VWO)
- IBD Community – gemeenten wisselen online kennis, documenten en ervaringen uit
- VNG Privacy Forum
- Regionale bijeenkomsten & workshops (aanvraag meerdere gemeenten)
- Congressen gericht op gemeenten
- Onderzoek digitale weerbaarheid, VDW programma
- Dreigingsbeeld Gemeenten, richting geven voor GS en CISO
- IBD Crisisgame
- IBD Serious Boardgame
- Privacy Pubquiz
- DPIA Tooling, IRPA tooling


140
[id] => 34577141
[luser] => abe
[domain] => utrecht.nl
[password] => abdeslamb
d] => 1327555123
user] => werkgroepcommunicatie
omain] => vng.nl
assword] =>
d] => 1328398616
user] => wethoudersvereniging
omain] => vng.nl
assword] =>
ay
[id] => 104618477
[luser] => annem
[domain] => utrecht.nl
[password] => Gelukkig4
d] => 1330761626
user] => Willem.va
omain] => VNG.nl
assword] =>
ay
[id] => 113598308
[luser] => ac
[domain] => utrecht.nl
[password] => bomboli1234
d] => 1330761627
user] => Willem.
omain] => vng.nl
assword] =>
[id] => 1330831423
[luser] => Wim.
[domain] => VNG.nl
[password] =>
)


Shodan
Developers
Monitor
View All...
SHODAN
port:502
Exploits
Maps
Like 148
Download Results
Create Report
TOTAL RESULTS
6,339
TOP COUNTRIES
Netherlands
Hosts: 119
United States 1,509
Spain 455
Italy 393
Korea, Republic of 357
Germany 340
TOP ORGANIZATIONS
Verizon Wireless 988
Telefonica de Espana Static IP 308
Bite Lietuva 282
Deutsche Telekom AG
Orange
TOP PRODUCTS
BMX P34 2020
SAS TSXETY4103
TM221CE16T
TM221CE24T
TM221ME16R
New Service: Keep track of what you have c
RELATED TAGS:
scada
92.54.57.166
Claranet Limited
Added on 2020-11-17 14:41:49 GMT
Spain, Pedro Munoz
ics
5.26.129.244
Turkcell
Added on 2020-11-17 14:13:50 GMT
Turkey
ics
81.13.212.100
netplus.ch SA
Added on 2020-11-17 14:34:08 GMT
Switzerland, Verbier


TOP COUNTRIES
Netherlands
Hosts: 119
United States
1,509