SCHUBERG PHILIS

De invloed van “cloud” op het dreigingslandschap…

Frank Breedijk – ISACA RISK event 2019

Legitimate a CC NC ND image by Seth Anderson
https://www.flickr.com/photos/44124372363@N01/7830947420/

SCHUBERG PHILIS

THIS IS A TRANSFER SLIDE

PLEASE DO NOT DELETE

> whoami

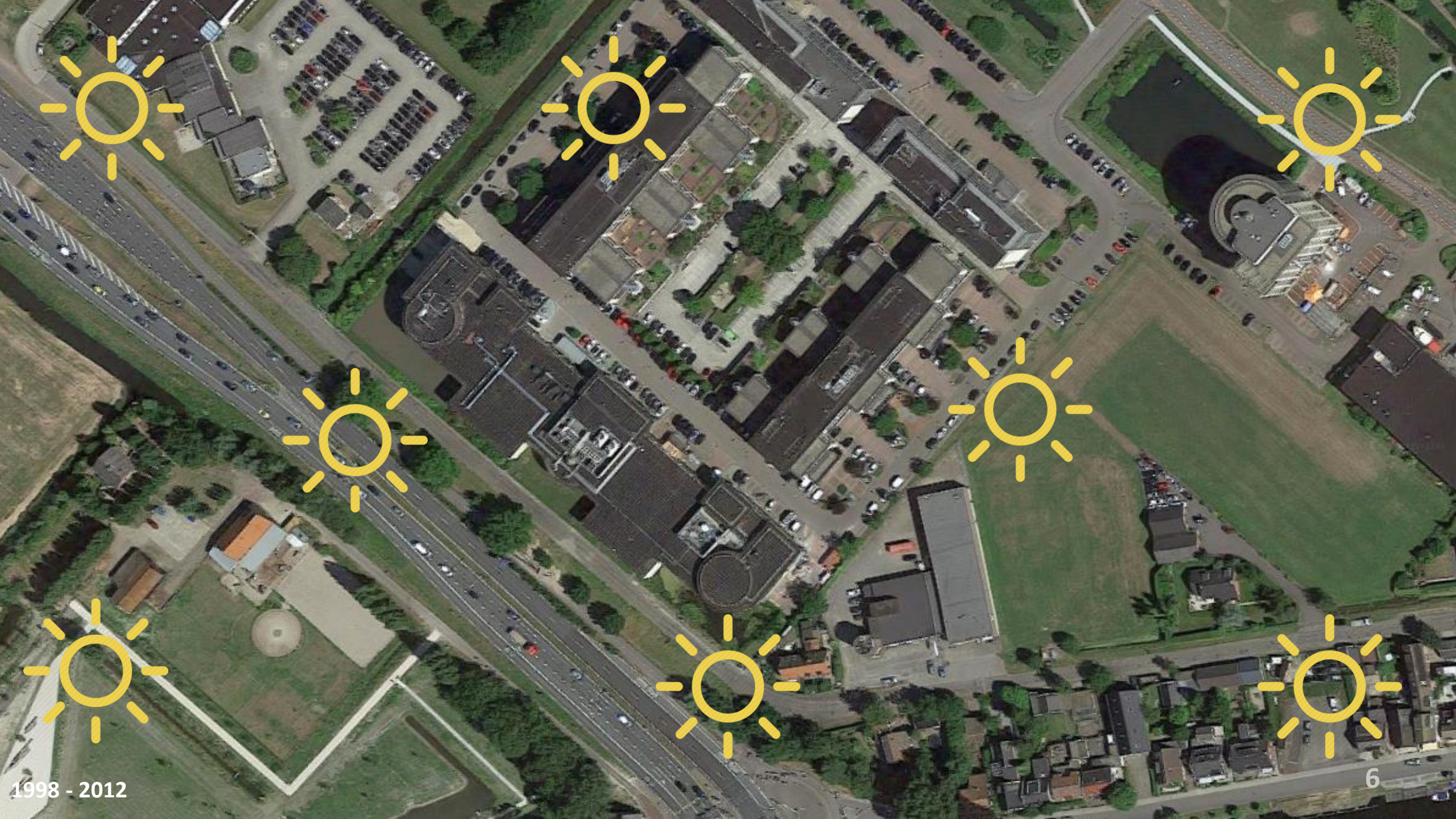
- Frank Breedijk
- CISO Schuberg Philis

- Cloud and open source enthousiast
- Ik woon in een stal uit 1751

- fbreedijk@schubergphilis.com

Opa verteld…

- Shared hosting vs decated hosting
- Intrede van virtualisatie
- Private / Community cloud
- Public cloud



1998 - 2012

Shared of ‘dedicated’ hosting

1924 Ford Model T Coupe '772U' 1 a CC ND image by Jack Snell
https://www.flickr.com/photos/59972430@N00/23467122488/

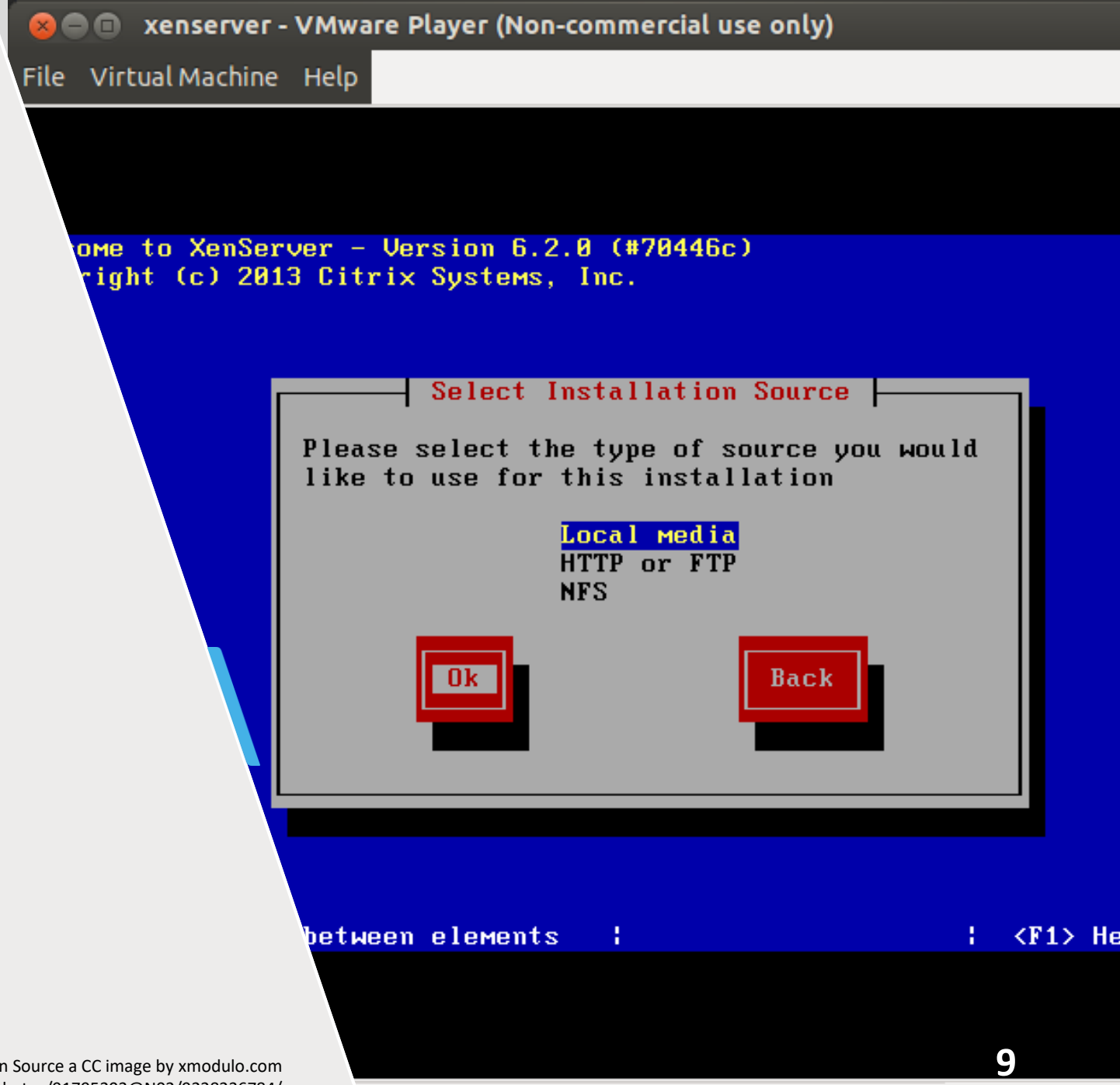
The fort ‘Datacenter’

- Met wie deel je je servers
- Nadruk op:
  - Fysieke beveiliging
  - Netwerk Segmentatie
  - Scheiding van kritiek en niet kritiek
- Oorzaak van de meeste incidenten
  - Malware
  - Niet patchen

IMG_20140829_140731 a CC image by Robert
https://www.flickr.com/photos/12967790@N00/14885417370/

Virtualisatie

- Nieuwe dreigingen:
  - Delen van dezelfde hardware
  - Verschillende machines delen dezelfde kernel
- ”Opgeloste” dreigingen
  - Software wordt niet meer op software nivo gedeeld

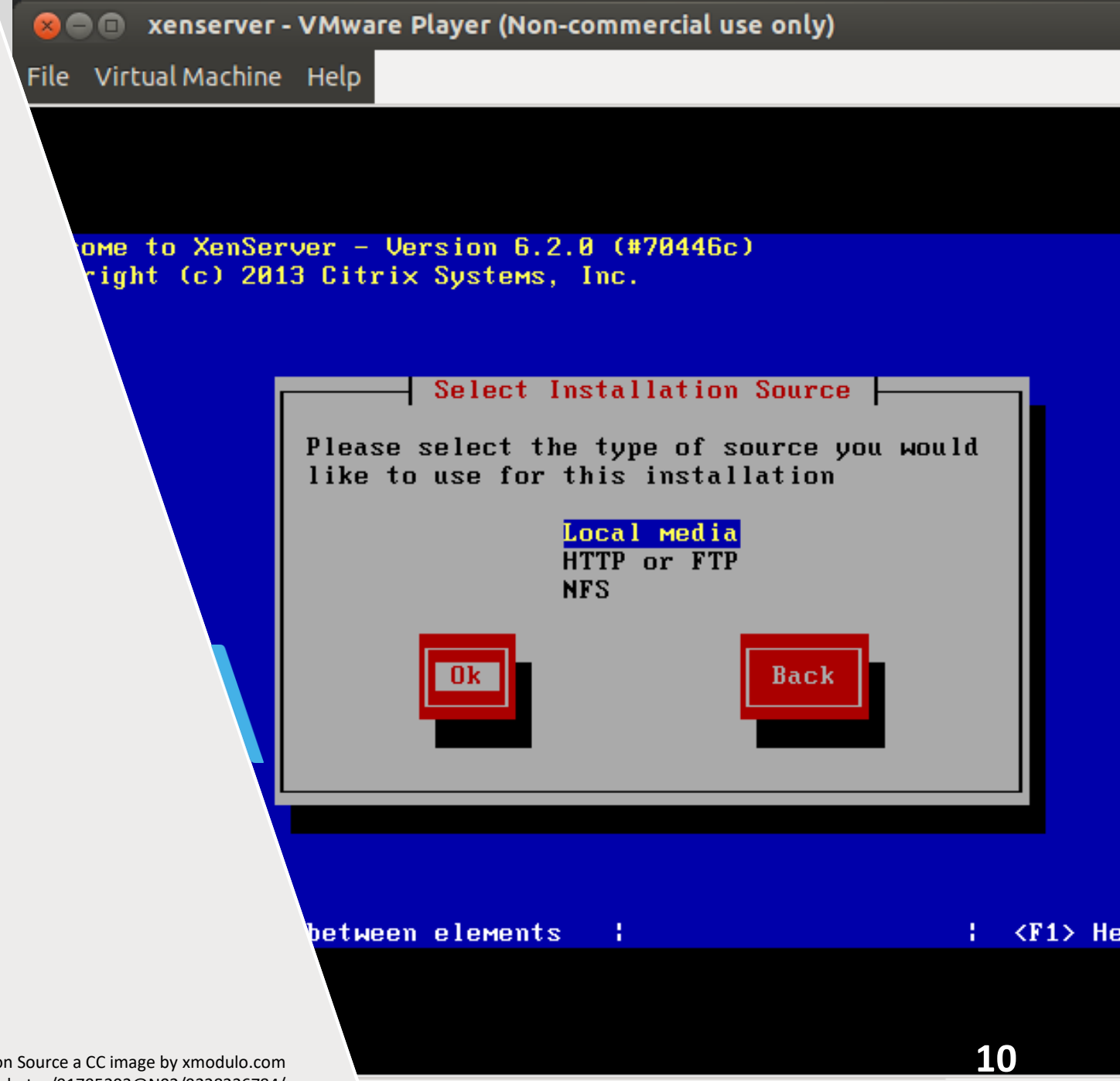


SCHUBERG PHILIS

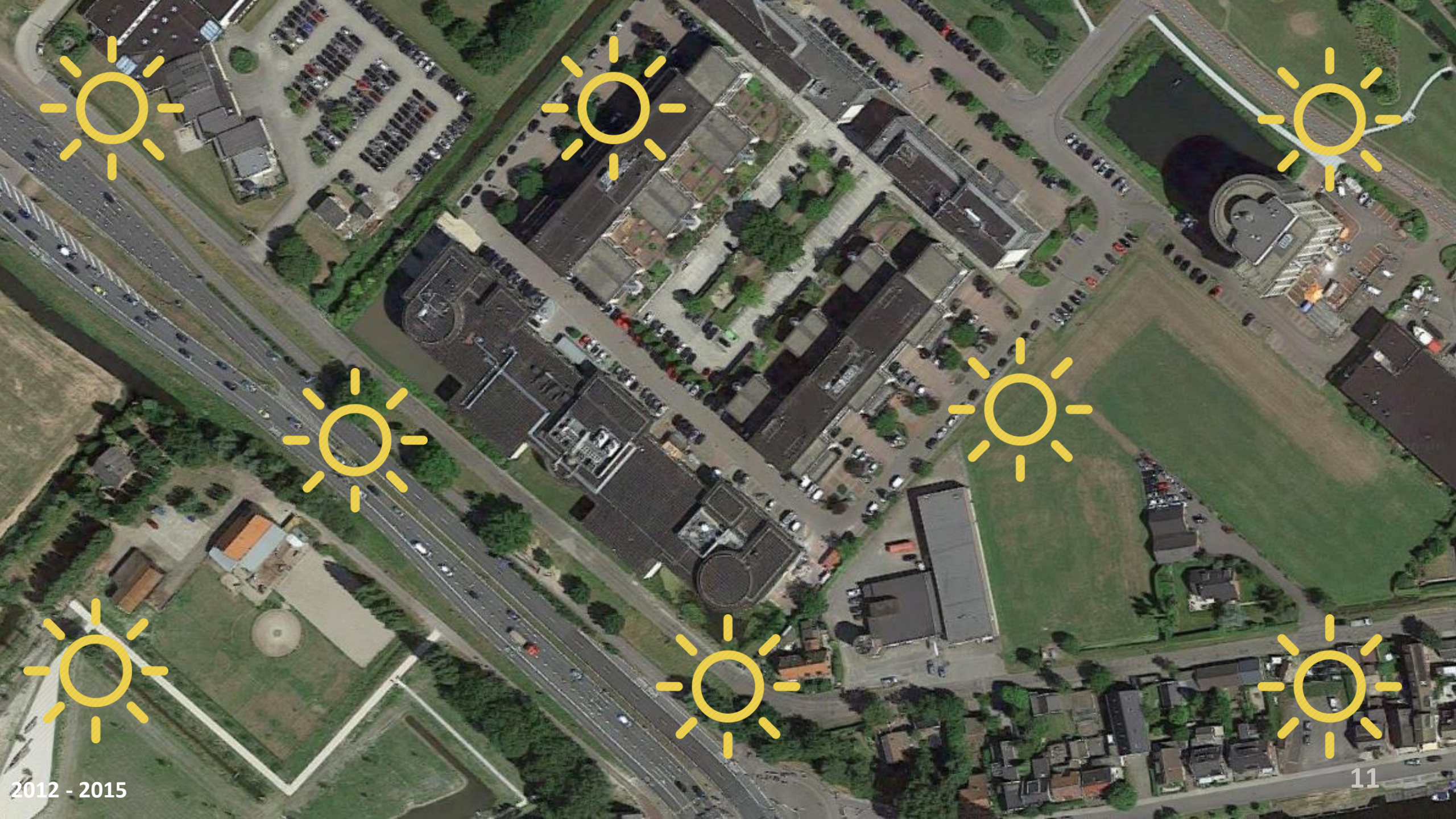
Install XenServer on VMware Player - Select Installation Source a CC image by xmodulo.com
https://www.flickr.com/photos/91795203@N02/9228236784/

Virtualisatie

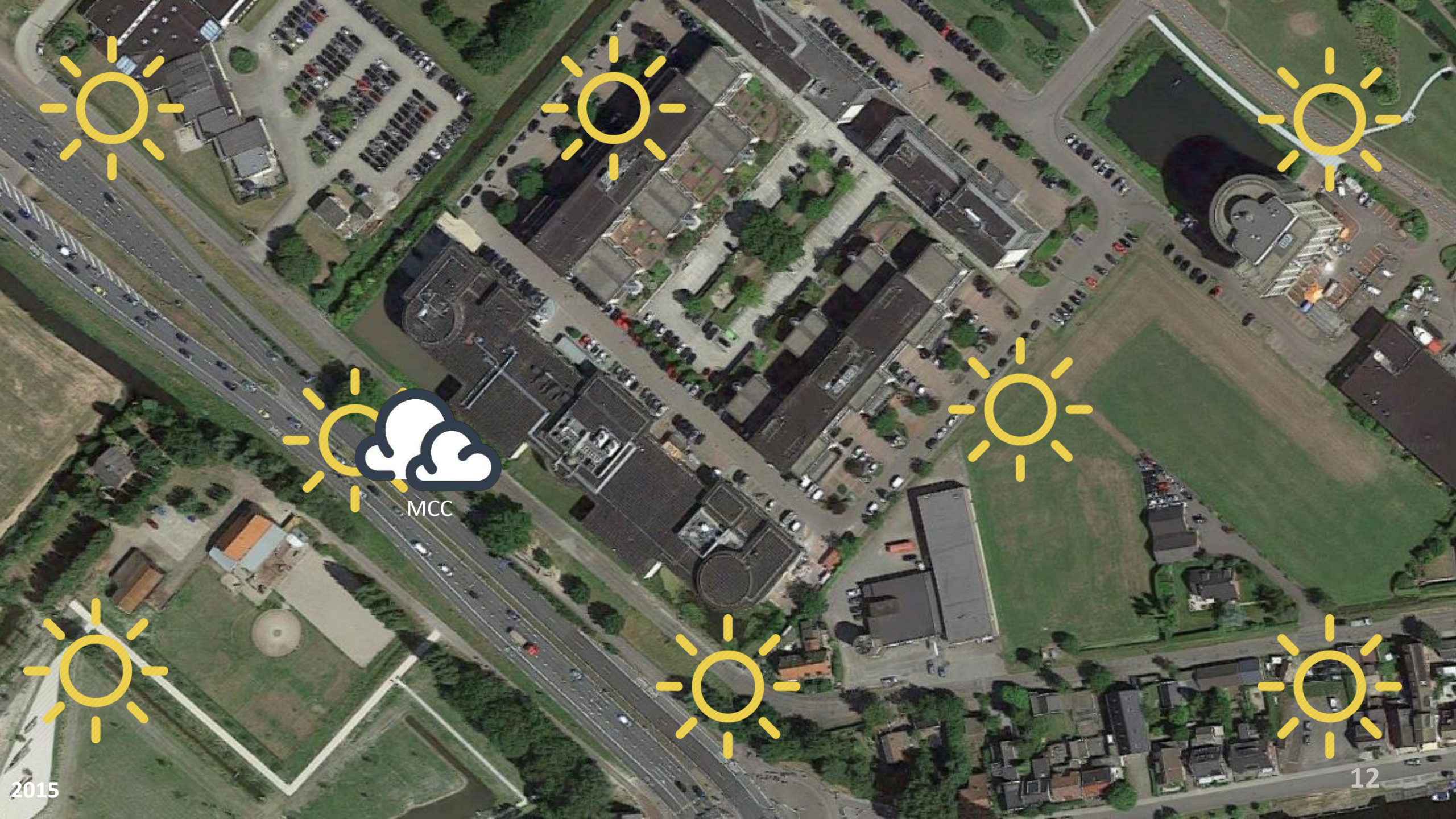
- Nadruk op:
  - Fysieke beveiliging
  - Hardware / kernel segmentatie
  - Hypervisor escape
- Oorzaak van de meeste incidenten
  - Malware
  - Niet patchen
  - DDoS (2013)



Install XenServer on VMware Player - Select Installation Source a CC image by xmodulo.com
https://www.flickr.com/photos/91795203@N02/9228236784/



2012 - 2015



2015

Private / “Community” cloud

FARM:shop private hire party a CC NC image by Laura Billings
https://www.flickr.com/photos/14784969@N08/6225824429/

Wat is er anders…

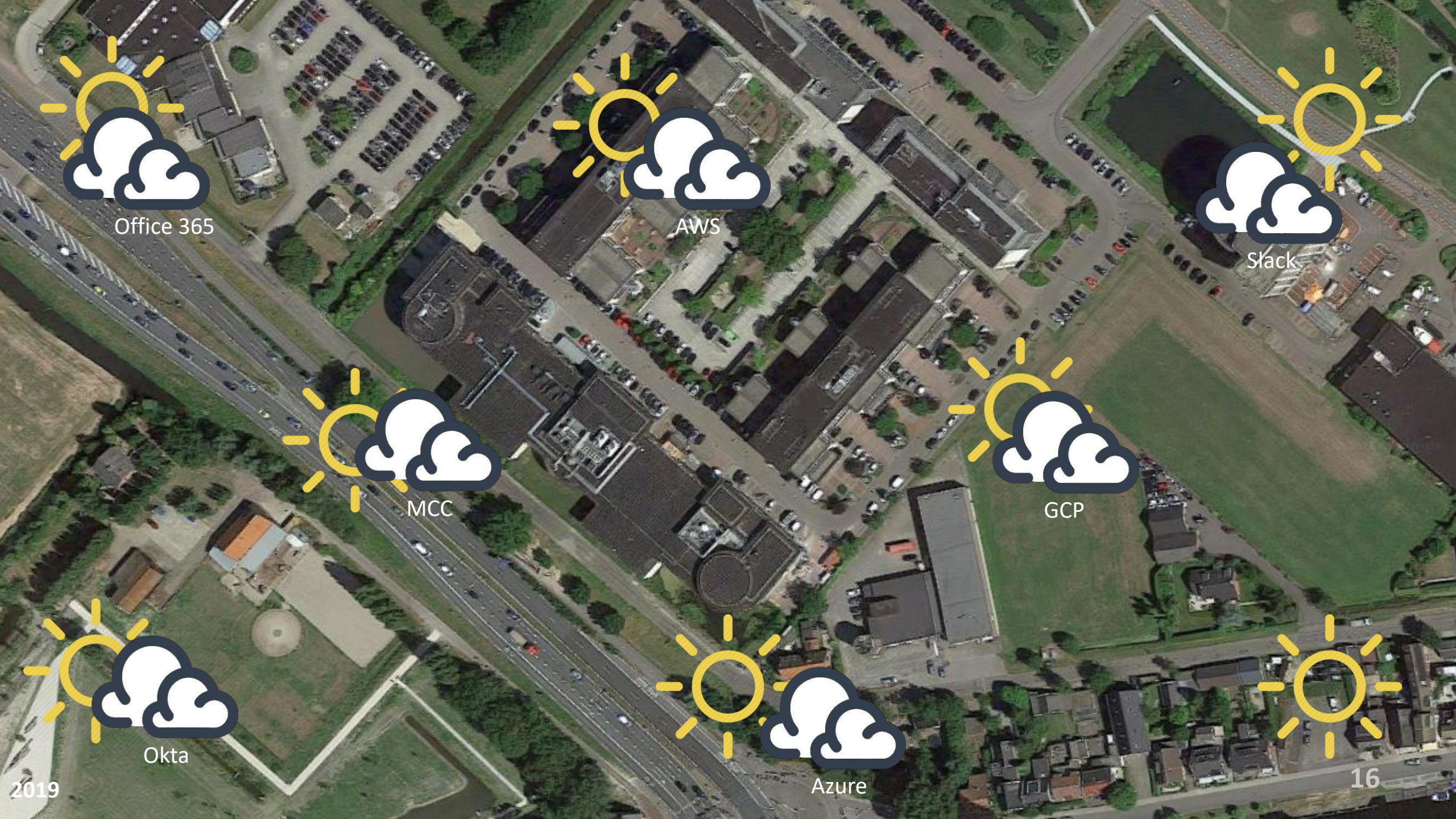
- T.o.v. virtualisatie
  - Hardware/kernel nu gedeeld met ”anderen”
  - Orchestratie laag met een API
- T.o.v. public cloud
  - Beperkte groep medehuurders
  - Physieke locatie bekend
  - Mogelijkheid tot audit

FARM:shop private hire party a CC NC image by Laura Billings
https://www.flickr.com/photos/14784969@N08/6225824429/

Security

- Nadruk op:
  - Hypervisor escape
  - Hardward / kernel segmentatie
  - Fysieke beveiliging
- Oorzaak van de meeste incidenten
  - Malware
  - Niet patchen
  - Applicatie security

FARM:shop private hire party a CC NC image by Laura Billings
https://www.flickr.com/photos/14784969@N08/6225824429/


Office 365
AWS
Slack
MCC
GCP
Okta
Azure

Public cloud

Holi. a CC NC ND image by ¡arturii!
https://www.flickr.com/photos/7617410@N02/16805986366/

Wat is er anders…

- Je weet niet precies met wie je de ruimte deelt
- Je weet niet precies waar je data staat
- Grote cloud partijen kunnen niet iedere klant laten auditen
- Buitenlandse partijen

Holi. a CC NC ND image by ¡arturii!
https://www.flickr.com/photos/7617410@N02/16805986366/

Security…

- Nadruk op:
  - Compliance
  - Lock in
  - Fysieke locatie
- Oorzaak van de meeste incidenten
  - Malware
  - Niet patchen
  - Niet juist inrichten van rechten
  - Applicatie fouten

Holi. a CC NC ND image by ¡arturii!
https://www.flickr.com/photos/7617410@N02/16805986366/

Help?

Sunny with a chance of meatballs
Sony Pictures Animation 2009

Hypervisor escape

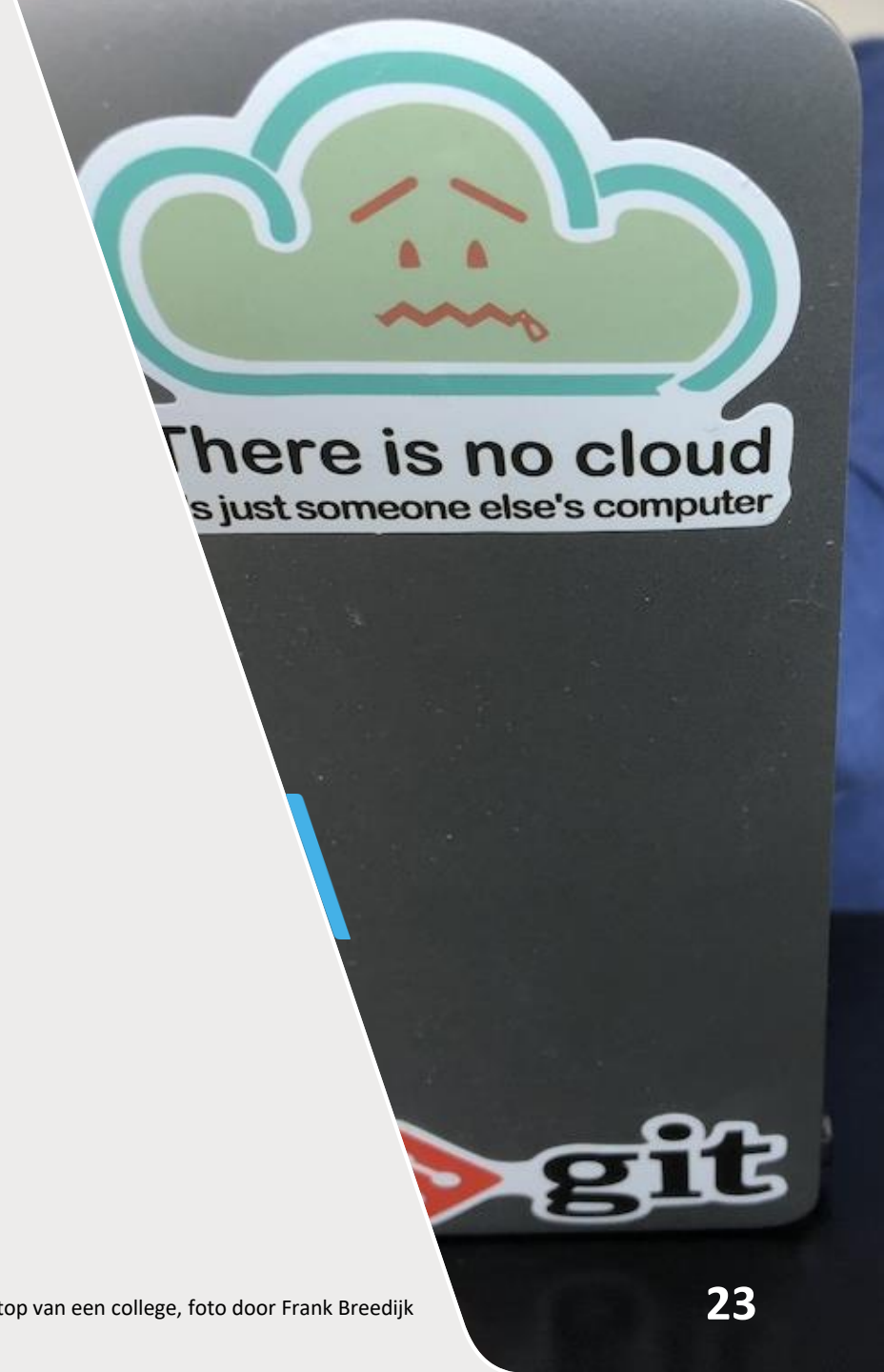
- Veel gevallen met kleine impact op para-virtualisatie
  - Paravirtualisatie niet populair meer
- Meltdown + Spectre
  - Cloud vendors waren de eersten

Incidenten?

- Niet patchen
- Gebrekkige access control
- Onbedoeld bloodstellen van gevoelige services
- Ransomware
- Applicatiefouten

There is no cloud…

- It’s just someone else’s computer?
- Als dat zo is, waarom wil ”men” het dan zo graag?
- Is dit wel de juiste blik?



Laptop van een college, foto door Frank Breedijk

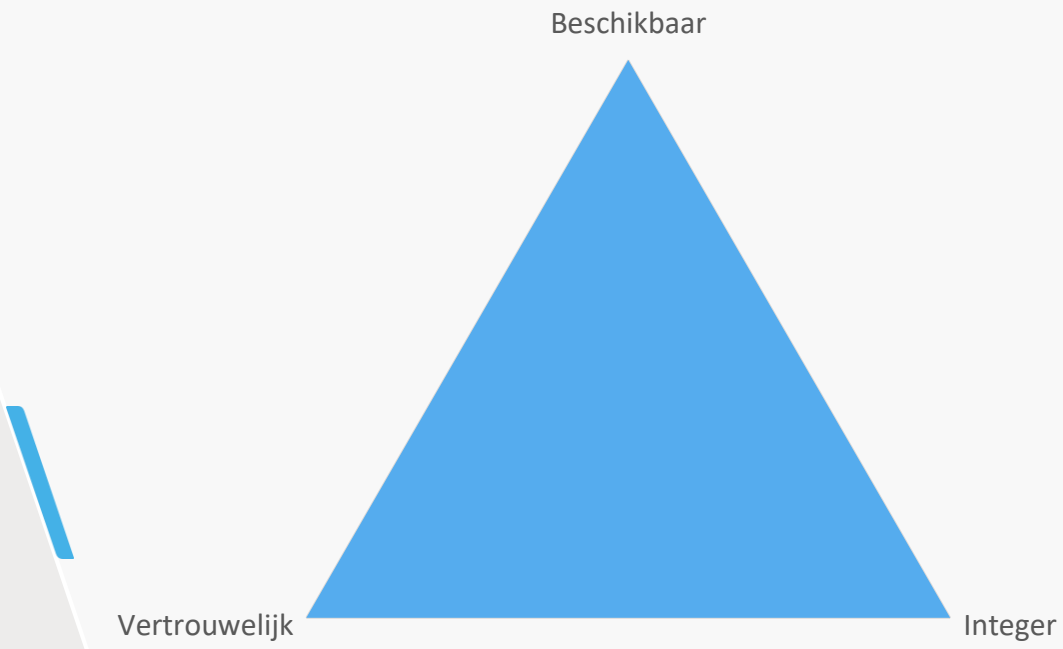
Moderne cloud infrastructuren…

Golden gate bridge, San Fransisco USA - Original image from Carol M. Highsmith's America, Library of Congress collection.
Digitally enhanced by rawpixel. A CC image by rawpixel
https://www.flickr.com/photos/153584064@N07/46201778672/

Beschikbaarheid

- Niet alleen meer uptime

- Beschikbaarheid van informatie is functionaliteit
- Functionaliteit die de eind-gebruiker niet bereikt is geen functionalitiet
- Bedrijven moeten ‘agile’ zijn om te overleven
- Geen hele serverparken meer nodig om b.v. A.I. te doen



Agility?

- Met zo min mogelijk operations mensen net zoveel operations doen als nodig is
- Ontwikkelaars in staat stellen zo veel mogelijk functionaliteit zo snel mogelijk bij de eind-gebruikers te krijgen

150725-F-YW474-128 a CC NC image by U.S. Pacific Fleet
https://www.flickr.com/photos/compacflt/20009404191/

Hoe dan?

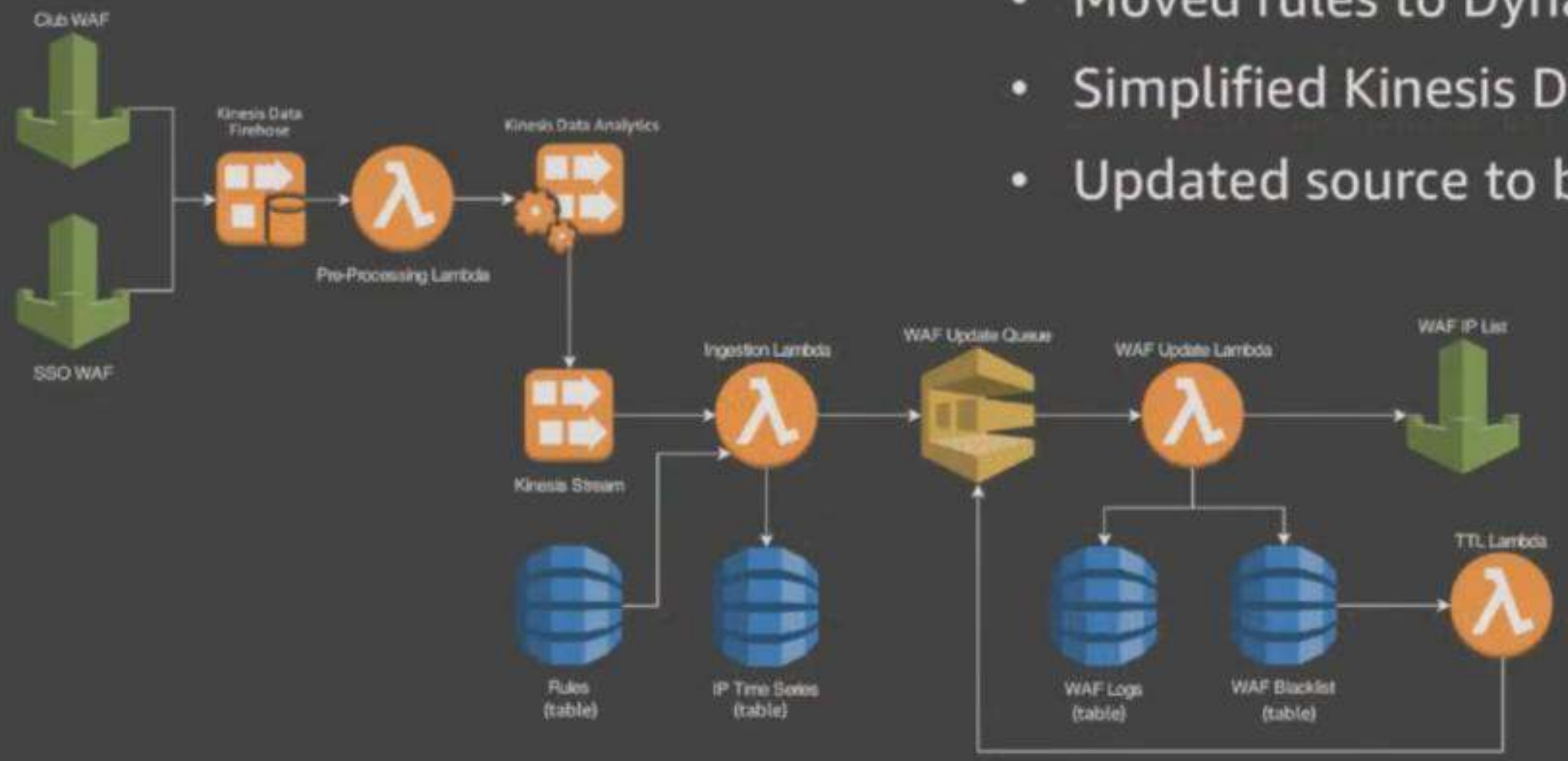
- Commodity / uitontwikkeld
  - Services ipv servers
- IT voor IT
  - Services, PaaS ipv servers
- “Onderscheidende” applicaties
  - Cloud native of containers

150725-F-YW474-128 a CC NC image by U.S. Pacific Fleet
https://www.flickr.com/photos/compacflt/20009404191/

https://www.youtube.com/watch?v=zyP-pfij86s

Second iteration

- Simplified whitelist architecture
- Moved rules to DynamoDB table
- Simplified Kinesis Data Analytics
- Updated source to be WAF logs



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Snoepwinkel

- De mogelijkheden / functionaliteiten van een moderne cloud provider zijn (bijna) eindeloos

Ren Ren Le Bao'an Boulevard Shenzhen a CC NC image by Chris
https://www.flickr.com/photos/76224602@N00/4348333928/

Ren Ren Le Bao'an Boulevard Shenzhen a CC NC image by Chris
https://www.flickr.com/photos/76224602@N00/4348333928/

Colorful Gum Tabs a CC image by Marco Verch
https://www.flickr.com/photos/30478819@N08/45917981931/

Moderne cloud vs. IaaS

Cloud security ≠ IaaS security

Colorful Gum Tabs a CC image by Marco Verch
https://www.flickr.com/photos/30478819@N08/45917981931/

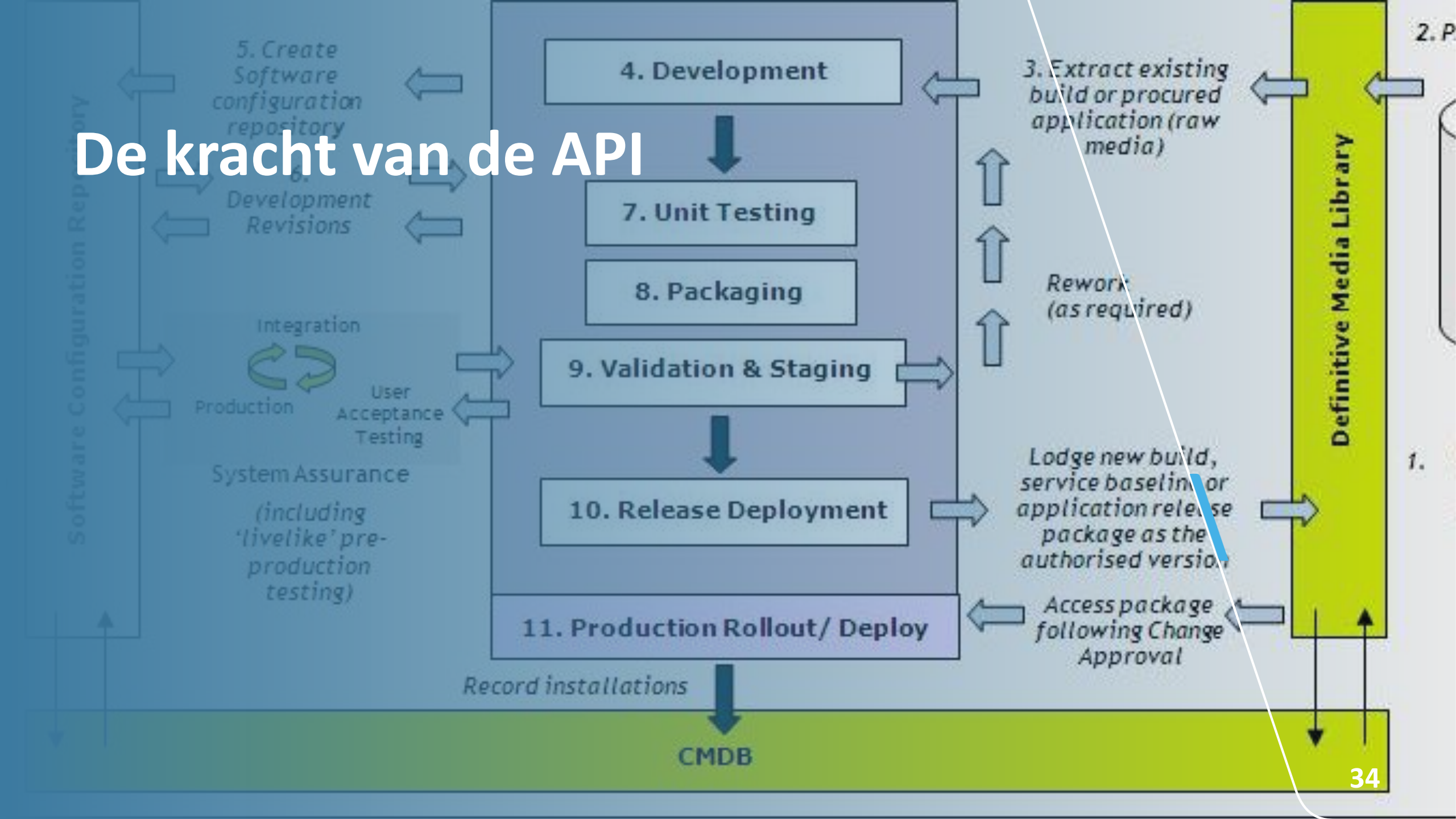
Iedereen wil security…

Werner Vogels tijdens AWS Summit 2018 in Den Haag
Door Frank Breedijk

SaaS kan helpen

- Als IT geen core business is
- Als IT wel je core business is, maar de applicatie niet “spannend” is
- Als de applicatie niet “onderscheidend” is

De kracht van de API



Via de API kun je…

- Een altijd up to date overzicht krijgen van alles in je landschap
- Weten waar je data staat
- Weten dat je data versleuteld is
- Verkeerde configuraties detecteren
- én oplossen

She thinks my json's sexy... Said no one ever a CC ND iamge by Matthew Ragan
https://www.flickr.com/photos/45199237@N04/21131398981/

Consolidatie

- Veel van de oplossingen nu nog zelf bouw
- Derden zijn in dit gat gestapt
- Security is *de* dominante non-functional voor clouds
- Verwacht dat cloud providers dit gaan aanbieden

SCHUBERG PHILIS

2983e2 P900 Wide-eyed wonder of Christmas a CC NC ND image by Jenny Pansing
https://www.flickr.com/photos/25171569@N02/23876843182/

Niet het einde van de wereld

Sunny with a chance of meatballs
Sony Pictures Animation 2009

Cloud craftsmenship manifesto…

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/

Cloud craftsmenship manifesto…

I am a craftsman and I use cloud technologies, because I apply my craftmanship to cloud technologies, I am a Cloud Craftsman.

I recognize that cloud technologies, if applied correctly, offer great benefits in terms of availability, reliability, scalability and agility.

I recognize that, like any other technology, cloud technology is not a silver bullet.

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/

Cloud craftsmenship manifesto…

I recognize that not all cloud solutions are created equally. I will do my best to select the solution that best fits my specific situation.

I recognize that, in the cloud, I will have to trust and rely on the abilities of the provider. I will do my best to validate this trust.

I recognize that effective, efficient and secure usage of cloud technologies is a responsibility that is shared between the user and the provider.

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/

Cloud craftsmenship manifesto…

I recognize that effective, efficient and secure uadge of cloud technologies is in both the interest of the user and provider.

I intend to read, understand and/or use the best practices and tooling recommended by the provider to the greatest extend possible in my situation.

I intend to stand on the shoulders of giants. May before us have developed tools and practices for the effective, efficient and secure usage of cloud technologies. I will adopt their work as much as I can.

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/

Cloud craftsmenship manifesto…

I recognize that cloud technologies are repaidly evolving, this means I will have to keep up with the current state of the cloud technologies I intend to use and are available to me. After all, a fool with a tool is still a fool.

I recognize that automation is the key to reliability, reproducability and recoverability. I will embrace automation of my work as the way forward.

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/

Cloud craftsmenship manifesto…

I recognize that, in the cloud, I cannot just rely on others to provide security for me.

I am a Cloud Craftsman, not because it is easy, but because it is necessary and I am up for the challenge.

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/

http://craftsmanship.cloud

The blacksmith a CC NC ND image by psaRas
https://www.flickr.com/photos/148231543@N08/36198187330/