



HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

Schaduw IT

R. (Ruud) Buurma, L. (Benjaminse) en M.T.A. (Marcel) Klaver
november 2020

OPENBAAR

Agenda

1

1. Introductie
2. Risico's
3. Oplossingsrichtingen
4. Samenvatting



Introductie Voorstellen



L. (Lodewijk) Benjaminse
directeur

lodewijk.benjaminse@hodari.nl

071-2032385



M.T.A. (Marcel) Klaver
adviseur

marcel.klaver@hodari.nl

06-82059693



R. (Ruud) Buurma
adviseur

ruud.buurma@hodari.nl

06-26396625



Introductie

Veel voorkomende schaduw IT



Introductie

Definitie en voorbeelden

Schaduw IT (Gartner):

“alle IT (zowel software als hardware) die buiten
(het zicht en beheer van) de IT-afdeling valt”

Enkele voorbeelden:

- persoonlijke apparaten zoals smartphones, tablets en USB-sticks;
- hardware die niet onder verantwoordelijkheid van IT valt;
- applicaties die eindgebruikers op eigen initiatief gebruiken;
- applicaties die afdelingen zelf regelen.



Introductie

De cijfers

Gartner survey onder 200 CIO's (2018):

- 83% gebruikt clouddiensten die niet vooraf zijn goedgekeurd;
- 30% van digitale inbraken in 2020 komen door schaduw IT;
- 30% tot 40% van de IT-uitgaven in grote organisaties zijn schaduw IT.

Onderzoek bij grotere organisaties toont aan dat:

- 23% van de respondenten de infrastructuur actief scant;
- 14% zo af en toe de bezem door het netwerk haalt;
- de overige 63% in feite het probleem negeert.



-
1. Introductie
 2. Risico's
 3. Oplossingsrichtingen
 4. Samenvatting



Risico's

Oorzaken

mensen:

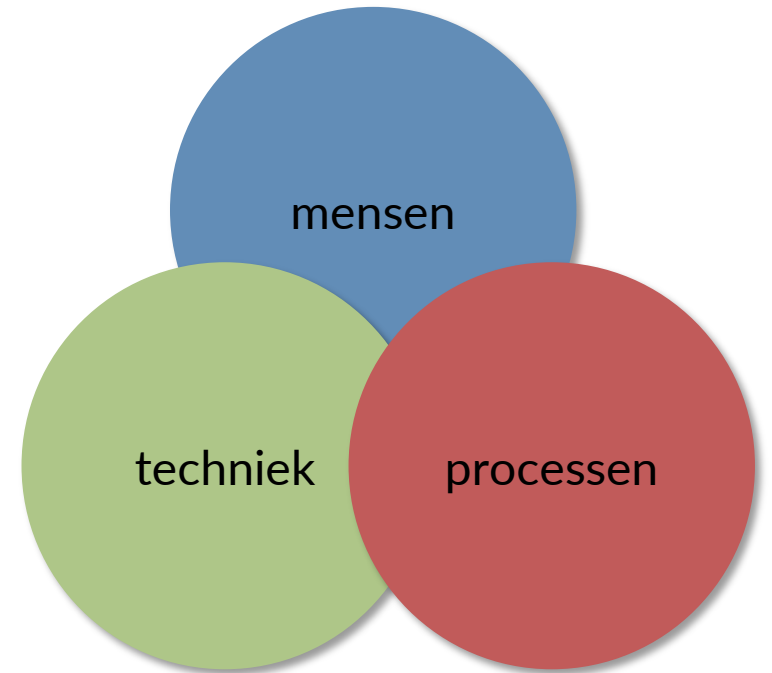
- jarenlange gewenning en cultuur;
- gemak van aanschaffen en gewenning aan apps door privégebruik;
- toename van thuiswerken en onbekendheid met de risico's.

techniek:

- technisch niet dichtgetimmerd;
- BYOD / toestaan van privéapparatuur voor zakelijk gebruik;
- legacy systemen worden vergeten.

processen:

- onbekendheid met formeel beleid en procedures;
- trage IT-afdeling;
- te vaak 'nee' gehoord, conform beleid.



Risico's

Bedreigingen en risico's

Risico's van schaduw IT:

- non-compliance;
- ontbreken van contractuele afspraken;
- gebrek aan (zekerheid over de) veiligheid van je data;
- slecht beheer van autorisaties;
- inefficiëntie;
- gebrek aan beheersing van de kosten.

Compliance en regelgeving.

- SOx;
- Basel II;
- GLBA;
- COBIT;
- ISO 27001;
- GAAP;
- IFRS;
- ITIL;
- PCI DSS;
- TQM;
- GDPR / AVG.



-
1. Introductie
 2. Risico's
 3. Oplossingsrichtingen
 4. Samenvatting



Oplossingsrichtingen

Risico analyse methodiek

Stap 1: Identificeren van risico's:

risico = kans x effect

Stap 2: Risico mitigatie strategieën:

- Transfer
- Avoid
- Accept
- Reduce

Stap 3: Bepalen van treatment plans.



Oplossingsrichtingen

Mensen

Het belangrijkste aspect om schaduw IT in goede banen te leiden is en blijft de mens:

- duidelijke *tone at the top*;
- eindgebruikers bewust maken van de risico's van schaduw IT;
- kijk als IT-afdeling kritisch naar jezelf;
- creëer een vertrouwenscultuur.



Oplossingsrichtingen

Techniek

Preventie:

- Op netwerk niveau:
 - blacklist vs. whitelist van applicaties / websites;
 - alleen managed devices toestaan op netwerk.
- Op device niveau:
 - niet toestaan van software installaties.

Detectie:

- Op netwerk niveau:
 - network discovery;
 - specialistische software die netwerkverkeer analyseert.
- Op device niveau:
 - specialistische software die gebruik van applicaties bewaakt.



Oplossingsrichtingen

Processen en beleid

- beleid omtrent het gebruik van IT(-middelen);
- overzicht van goedgekeurde en afgekeurde software/hardware;
- heldere acceptatiecriteria en toetsingsprocedure;
- snelle time-to-market van IT-afdeling;
- implementeer proces voor schaduw IT;
- goede communicatie tussen business en IT:
 - agile *way of work*: product owners uit de business;
 - wiki's, confluence en nieuwsbrieven;
 - inloopuurtje, kennissessies of brainstormsessies;
 - formaliseren van overleg- en communicatiestructuren.



1. Introductie
2. Risico's
3. Oplossingsrichtingen
4. Samenvatting



Samenvatting

Manage schaduw IT

Belangrijkste punten uit deze presentatie:

- schaduw IT is eigenlijk niet tegen te houden;
- creëer bewustzijn;
- maak het bespreekbaar;
- monitor actief;
- bied alternatieven.



HODARI draagt bij aan betere informatiebeveiliging en privacy. Wij helpen organisaties aantoonbaar grip te krijgen op informatiebeveiliging en privacy door vraagstukken op het gebied van governance, risk en compliance op te lossen.

Wij bieden kwalitatief hoogwaardige oplossingen waarbij de meest complexe vraagstukken tot in detail zijn opgelost. Wij hebben ruime ervaring opgedaan binnen verschillende sectoren en handelen binnen projecten naar aanleiding van fusies en overnames, reorganisaties, bevindingen van accountants of opmerkingen van toezichthouders.

HODARI B.V.

071-2032385

hodari.nl

L. (Lodewijk) Benjaminse

lodewijk.benjaminse@hodari.nl