Informatiebeveiliging in het MKB

Rijk Prosman

12 november 2019

PvIB Platform voor InformatieBeveiliging

ASPECT® ICT

STELLING 1

“Het MKB is goed bezig als het gaat om informatiebeveiliging”

STELLING 2

“De MKB-er is zelf aan zet om informatie-beveiliging (nog) beter te organiseren”

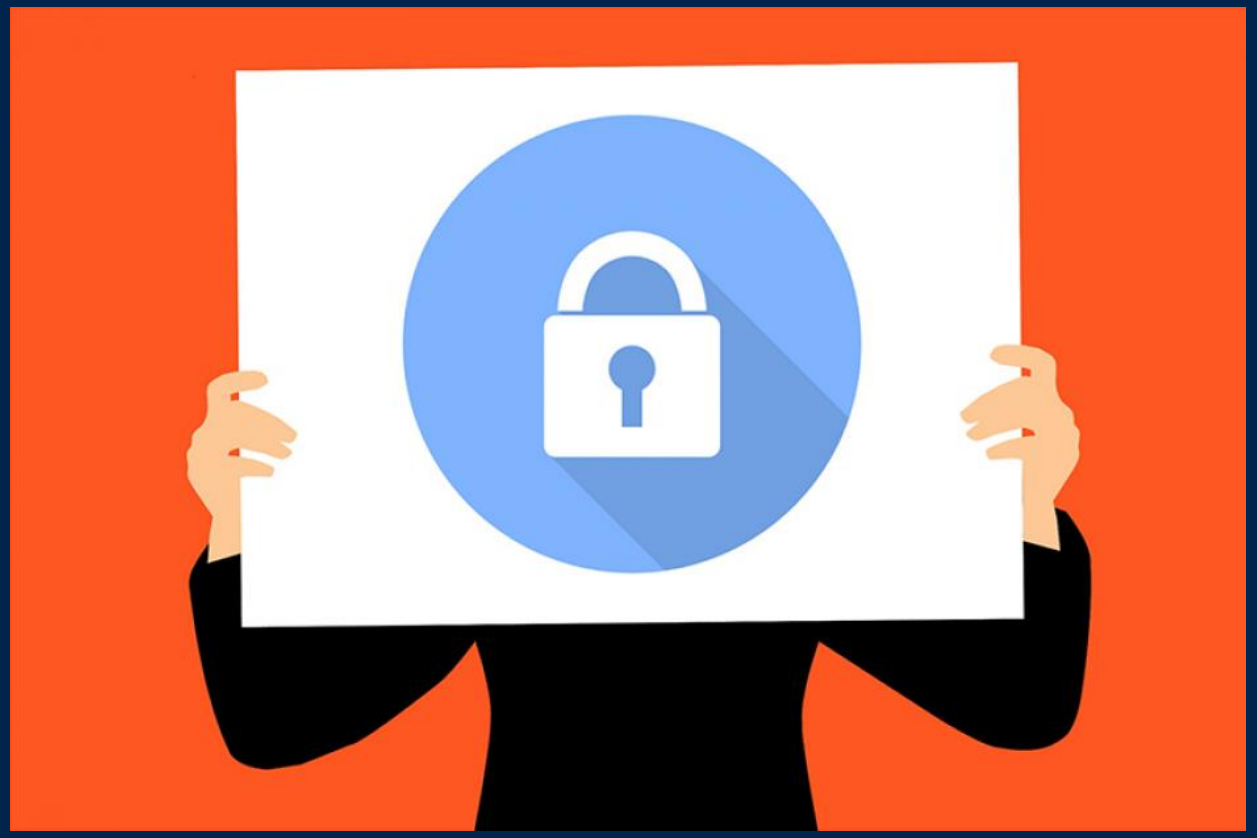
STELLING 3

“Er is geen winst te behalen om informatie beveiliging in het MKB te verbeteren. De ondernemer doet toch maar waar hij zelf zin in heeft.”

MKB vs Grootbedrijf

- Aandeelhouder bij MKB is ook vaak de ondernemer
- MKB is gewend om meer risico’s te nemen

Praktijkvoorbeeld - Persoonsgegevens



MKB vs Grootbedrijf

- Aandeelhouder bij MKB is ook vaak de ondernemer
- MKB is gewend om meer risico’s te nemen
- MKB denkt niet in normen
- MKB doet makkelijker aannames
- MKB blijft (meer) onder de radar van de media
- Snelle realisatie van zaken binnen MKB

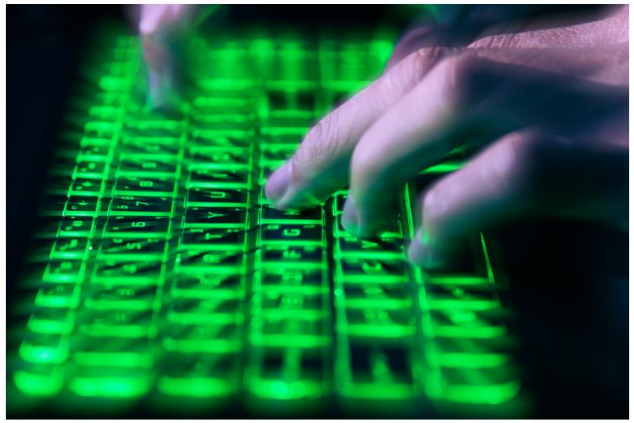
Praktijkvoorbeeld - Mobile Device Management

ASPECT® ICT

MKB vs Grootbedrijf

- Aandeelhouder bij MKB is ook vaak de ondernemer
- MKB is gewend om meer risico’s te nemen
- MKB denkt niet in normen
- MKB doet makkelijker aannames
- MKB blijft (meer) onder de radar van de media
- Snelle realisatie van zaken binnen MKB
- Controller vaak bij kleine bedrijven verantwoordelijk voor IT en IB

Mkb legt verantwoordelijkheid Cyber Security bij ICT-dienstverlener



Het is niet eenvoudig voor ICT-beheerders om ondernemers in het mkb bewust te maken van cyberrisico's, blijkt uit onderzoek van Centraal Beheer. Zes op de tien ICT-beheerders vindt dat zijn mkb-klanten te weinig maatregelen treffen ter bescherming. Mkb-ondernemers onderschatten de cyberrisico's of denken goed beschermd te zijn. Dit laatste is vaak niet het geval, want afgelopen jaar werd een derde van het mkb geconfronteerd met een cyberincident.

Ondanks dat het merendeel van de mkb-bedrijven (75%) zichzelf als verantwoordelijke voor cyber security ziet, hebben ICT-beheerders (42%) het gevoel dat de verantwoordelijkheid rondom cyber security op hen wordt afgeschoven. Volgens de mkb-ondernemers (68%) behoort cyber security tot de zorgplicht van de ICT-dienstverlener. Het is hierbij opvallend dat slechts 22% van de ICT-beheerders aangeeft dat er duidelijke afspraken zijn vastgelegd. Juist hierdoor loopt de ICT-beheerder het risico aansprakelijk te worden gesteld bij cyberincidenten. Een derde van de mkb-bedrijven geeft aan dit ook daadwerkelijk te zullen doen.

Cyber security nog niet hoog op agenda mkb

Menselijk handelen wordt gezien als een van de grootste cyberrisico's. Toch doet bijna twee derde van de mkb-bedrijven niets om het bewustzijn van medewerkers te vergroten. En heeft nog geen kwart een informatiebeveiligingsbeleid. Het komt dus niet uit de lucht vallen dat ICT-beheerders (60%) zich zorgen maken over de digitale veiligheid van hun mkb-klanten. Ze slagen er echter nog niet in om de mkb-ondernemer te overtuigen van het belang van cyber security. Bijna de helft van de ICT-beheerders heeft hier moeite mee.

Bron: https://www.emerce.nl/wire/mkb-legt-verantwoordelijkheid-cyber-security-ictdienstverlener

ASPECT® ICT

MKB krijgt aandacht

En wel van hackers:

- Steeds geraffineerdere aanvallen
- Steeds hogere losgeld bedragen
- Steeds grotere impact op de bedrijfsvoering

Praktijkvoorbeeld – Bedrijf op slot

Welk bord zorgt er voor dat u uw snelheid aanpast?

En met Flitsmeister aan? ☺

A. **Maximumsnelheid**
B. **Adviessnelheid**
C. **Beide**
D. **Geen van beide**

ASPECT® ICT

Opgelegde aandacht voor Cyber Security

AVG
VOOR HET MKB

ASPECT® ICT

Echte aandacht voor Cyber Security

- Waar ligt een ondernemer wakker van?
- Wat is het effect wanneer de business wordt getroffen?
- Hoe lang mogen systemen (c.q. informatie) niet beschikbaar zijn?

Continue aandacht voor Cyber Security

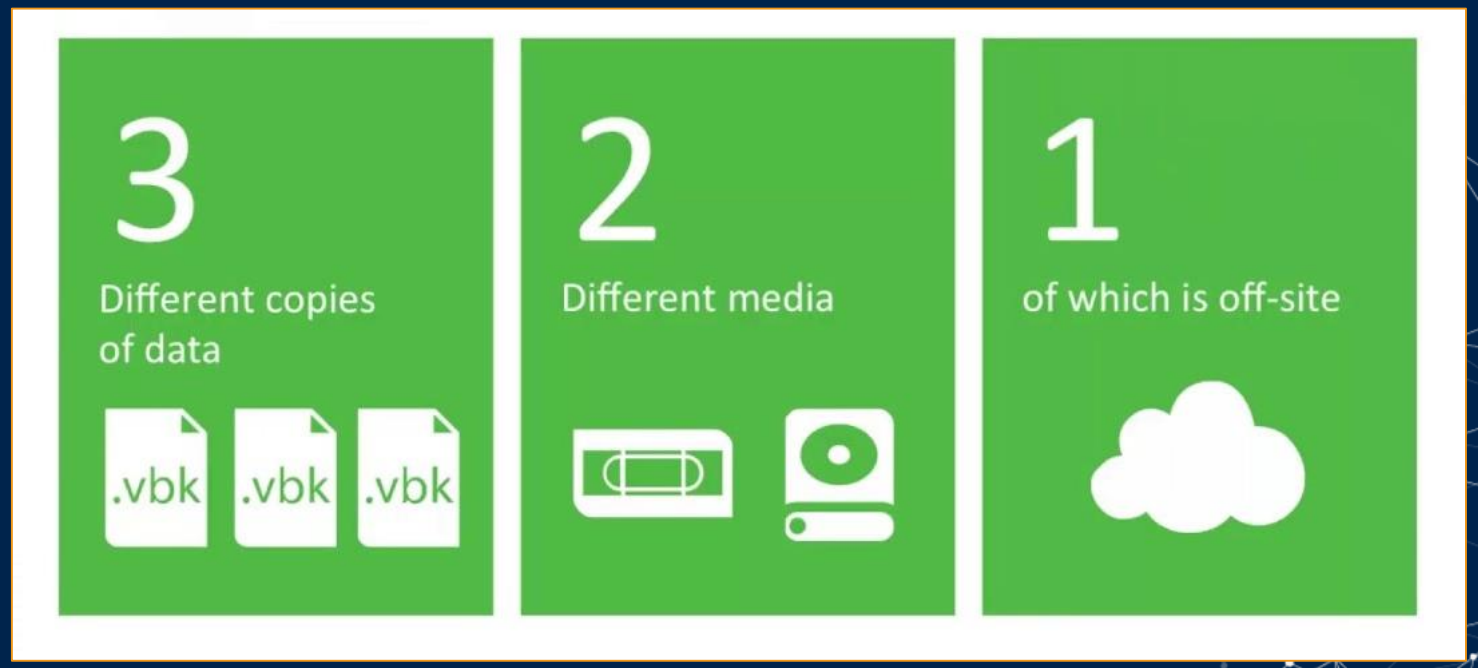
- IB beleid
- Risico analyses
- Security & vulnerability scans
- Awareness

Pragmatische aanpak!

ASPECT® | ICT

Laaghangende appels

- Backup (3-2-1 principe)
- Patch Management
- Twee-staps verificatie



ASPECT® ICT

Maatregelen lastiger te implementeren:

- Logarchivering
- Security Information & Event Management (SIEM)
- Aansluiting bij Security Operating Center (SOC)
- Mobile Device Management

Toch een norm?

ISO 27001 GECERTIFICEERD

CIS Controls®

NTA 7516 (nl)
Medische informatica – Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie)

ASPECT® ICT

ISO27001 vs CIS CONTROLS

ISO27001:

- Dwingt om structureel bezig te zijn met zowel technische als organisatorische onderwerpen
- Nodig om een management systeem (ISMS) op te zetten en te onderhouden
- Kent 114 maatregelen waar je aantoonbaar over nagedacht moet hebben

CIS Controls:

- CIS Controls zijn meer technisch (praktisch) van aard
- De CIS Controls houden rekening met het (IT-)volwassenheidsniveau van de organisatie
- Onderscheid voor kleine, middel en grote organisaties
- Kent totaal 183 maatregelen, maar voor kleinere organisaties (IG1) zijn dit er maar 43 die voor een goede basis zorgen voor informatiebeveiliging

ASPECT® | ICT

CIS CONTROLS

Implementation Groups

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

183 Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

140 Controls

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

43 Controls

ASPECT® ICT

CIS Controls®

V7.1

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Controls	IG1	IG2	IG3
Basic	11	38	47
Foundational	22	70	88
Organizational	10	32	36
Totaal	43	140	171

NTA 7516

NTA 7516 beschrijft in techniek neutrale termen de eisen waaraan e-mail, met daarin persoonlijke gezondheidsinformatie, zou moeten voldoen.

Vrij beschikbaar via:
www.werkenmetnen7510.nl

OPEN VRAAG

Hoe kunnen we er voor zorgen dat het informatiebeveiliging nog beter op de agenda komt van het MKB?

Be A Player, Not A Victim

Volledige filmpje: https://www.youtube.com/watch?v=xXdN5kMioRQ

Soms kun je een oplossing niet vinden omdat je vasthoudt aan je eigen verwachtingen.

OM DENKEN