DE HAAGSE HOGESCHOOL

Hoe cybersecure is het mkb?

Nulmeting cybersecurity in het mkb

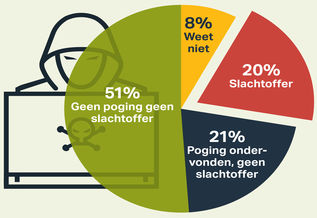
Onderzoeksopzet en respons

Via 20 brancheorganisaties zijn in de periode september 2016 t/m juli 2017 digitale enquêtes uitgezet bij hun mkb leden. In totaal hebben **800** directeuren de vragenlijst ingevuld.

Niet alle vragen zijn door alle respondenten ingevuld, waardoor de respons niet altijd 800 is. Zie het rapport voor de exacte aantallen per vraag.

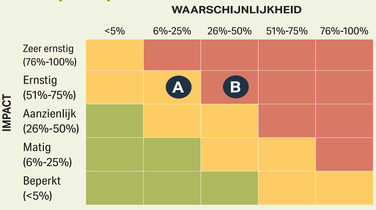
- < 10 medewerkers **60%**
- 10 - 50 medewerkers **29%**
- 50 - 250 medewerkers **11%**

Slachtoffers van cybercrime



Bedrijven met meer dan **50 medewerkers** zijn significant vaker slachtoffer van een cybercrime (**39,1%** van deze groep), dan bedrijven met **10 a 50 medewerkers** (**21,8%** van deze groep) en bedrijven met minder dan **10 medewerkers** (**15,1%** van deze groep).

Risicoperceptie



Impact: Voor 62% is het bedrijf volledig afhankelijk van IT.
Waarschijnlijkheid is de kans dat
- *uw bedrijf* komend jaar slachtoffer wordt van een cybercrime: 20% A
- een *soortgelijk bedrijf* komend jaar slachtoffer wordt van een cybercrime 41% B

Soorten cybercrime

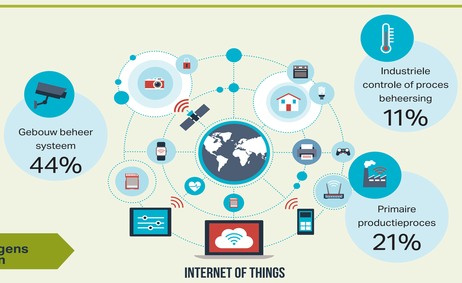
Bedrijven worden slachtoffer van de volgende cybercrimes:

Infrastructuur

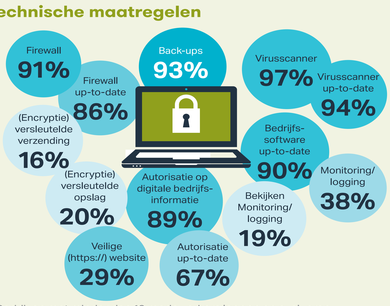
Alle bedrijven zijn via kantoor-automatisering verbonden met het internet, **59%** is hiervoor afhankelijk van een extern beheerde server.

Bedrijven hebben de volgende Internet of Things apparatuur verbonden met het internet

18% werkt volgens security by design



Technische maatregelen



Bedrijven met minder dan 10 medewerkers loggen en evalueren significant minder vaak activiteiten op het bedrijfsnetwerk, hebben minder vaak een firewall en maken minder vaak back-ups.

Organisatie maatregelen

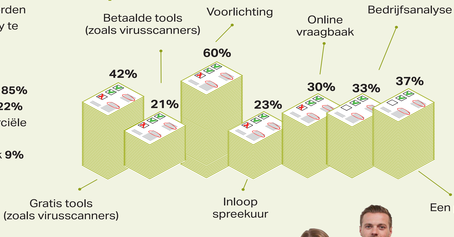
- 40% Verplicht om wachtwoorden met regelmaat te wijzigen
- 37% Regels over het omgaan met vertrouwelijke informatie
- 28% Regels over het gebruik van ICT voor privé-doeleinden
- 65% Verplicht gebruik sterke wachtwoorden
- 70% Werknemers hebben geleerd om goed op te letten bij het doen van onlinebetalingen
- 83% Werknemers hebben geleerd om geen e-mail van onbetrouwbare afzenders te openen
- 8% Protocol hoe te handelen bij cybercrime
- 33% Regels over het afgeven van bedrijfsgegevens
- 33% Regels over omgaan met onbekende bestanden
- 24% Regels voor het doen van online betalingen
- 16% (veiligheids)audits
- 75% Werknemers hebben geleerd om geen gevoelige informatie op internet te verstrekken
- 19% Informatiebeveiligingsbeleid
- 5% Scenario's voor cybercrime
- 29% Schriftelijke weergave ICT infrastructuur
- 60% Werknemers worden bewust gemaakt van online risico's

Hulpbehoefte

76% wil geholpen worden om hun cybersecurity te versterken via:

1. Brancheorganisatie **85%**
2. Landelijke website **22%**
3. Betaalbare commerciële partijen **21%**
4. Een lokale helpdesk **9%**
5. Concullega's **5%**

Top 7 wensen



Bedrijven zijn bereid

Contact

Raoul Notté MA MSc
r.j.notte@hhs.nl

Lisanne Slot MSc
l.k.slot@hhs.nl

Centre of Expertise
Cyber Security
coecs@hhs.nl

dehaagsehogeschool.nl

let's change
YOU. US. THE WORLD.