KMO cijfers

UNIZO Studiedienst | T 02 212 25 31
studiedienst@unizo.be | www.unizo.be/onderzoek-en-statistiek

Oktober 2017

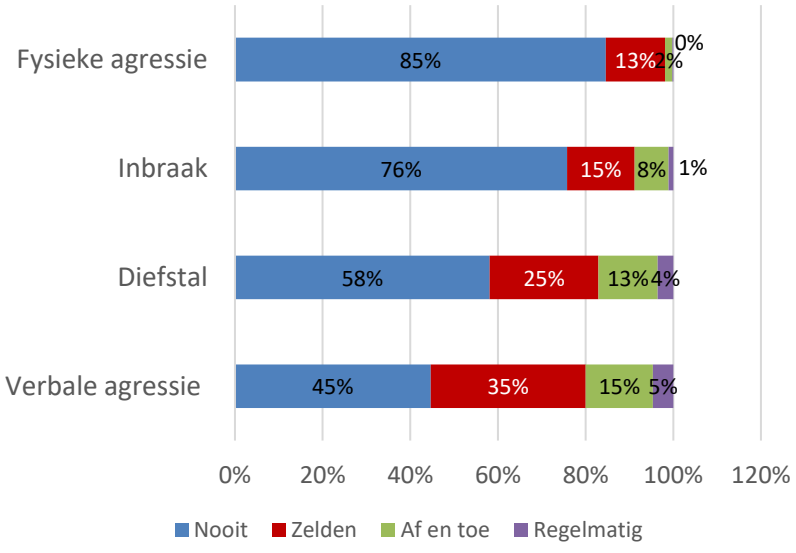
Veiligheid

- ✓ *Een op de vier ondernemers werd de voorbije 5 jaar slachtoffer van diefstal/inbraak*
- ✓ *Zeven op de tien ondernemers investeerden reeds in beveiligingssystemen*
- ✓ *55% heeft interesse in een BIN-z, of is reeds lid*
- ✓ *Drie op de tien ondernemers werd het voorbije jaar slachtoffer van phishing en één op de tien ondernemers werd gehackt*
- ✓ *10% van de ondernemers heeft zich verzekerd tegen cybercriminaliteit, maar 41% vindt het risico op een cyber issue te beperkt om zich beter te beschermen tegen cybercrime.*

In september 2017 bevroegen we 475 ondernemers over het thema veiligheid.

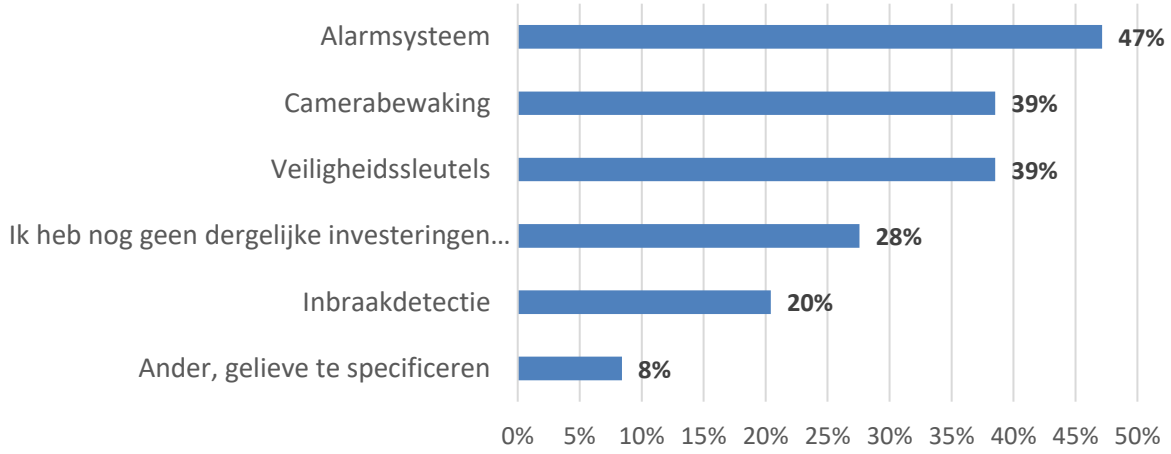
Inbraak, diefstal en agressie

Om te beginnen vroegen we onze ondernemers of ze de voorbije 5 jaar te maken kregen met fysieke of verbale agressie enerzijds, en inbraak of diefstal anderzijds. 15 % van de respondenten kreeg *af en toe* te maken met verbale agressie, 5 % *regelmatig*. Fysieke agressie komt eerder *zelden tot nooit* voor, behalve in de vervoerssector komt dit af en toe (11%) tot regelmatig (11%) voor. Verder gaf 13% aan dat ze *af en toe* slachtoffer zijn geweest van diefstal. Dit waren voornamelijk ondernemers uit detailhandel, horeca- en automobielsector. Bij maar liefst 4 % werd er *regelmatig* ingebroken. Ook werd er bij 8% van de bevraagde ondernemers *af en toe* ingebroken, bij 76% nog *nooit*.



Hoe beveiligt de gemiddelde ondernemer zich vandaag?

Zeven op de tien (72%) van de bevraagde ondernemers investeerde reeds in (technologische) beveiligingssystemen. Dat is een kleine stijging (+4%) ten opzichte van vorig jaar. Voornamelijk alarmsystemen zijn populair (47%), maar ook camerabewaking (39%), veiligheidssleutels (39%) en inbraakdetectie (20%).



We vroegen ook of (en hoe) de toegang tot de zaak/winkel wordt gecontroleerd. Bij ongeveer 40% is er vrije toegang (of niet van toepassing), ongeveer 30% werkt op afspraak en 21% heeft een onthaal/receptie. Verder controleren ondernemers hun zaak via videofoon (9%) en via een badgesysteem (8%). Slechts 1% doet beroep op een bewaker.

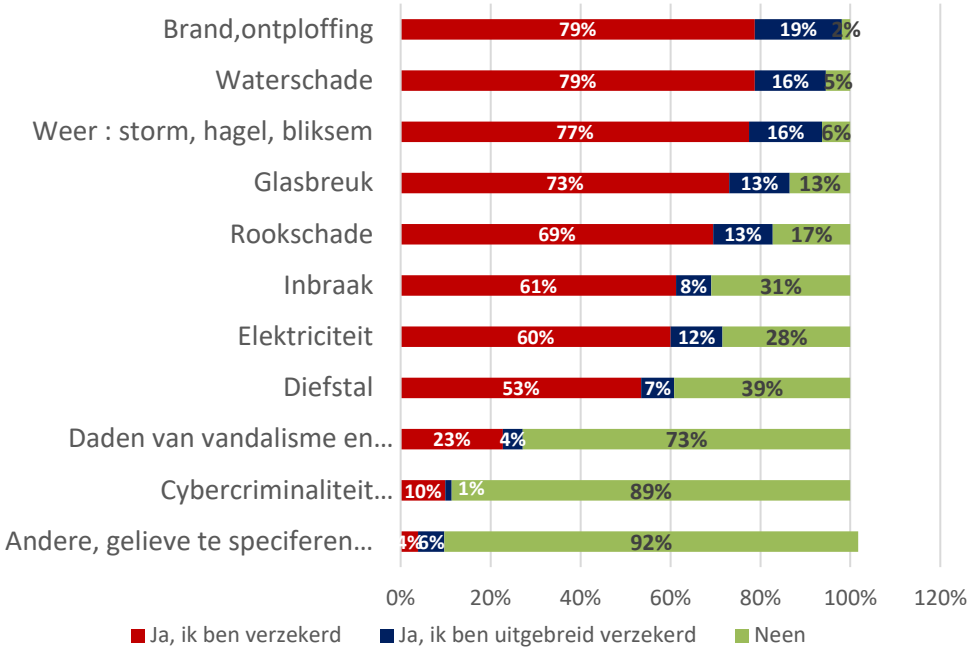
Op de vraag of men op de hoogte is van de wettelijke bepalingen inzake de plaatsing en het gebruik van camerabeelden antwoordde 41% van de ondernemers goed op de hoogte te zijn. Bijna zes op de tien (59%) kent deze regels niet! De helft van deze groep geeft aan hier meer over te willen weten, de andere helft trekt er zich niet veel van aan.

Wanneer u een bewakingscamera wilt plaatsen en gebruiken, moet u voldoen aan de regels van de **camerawet**. Het belangrijkste is dat u de privacy commissie op de hoogte moet brengen via een aangifteformulier en dat u dit kenbaar dient te maken via een specifiek pictogram. Voor bewakingscamera's op de arbeidsplaats moet **CAO nr. 68** worden nageleefd. Tot slot willen we er nog op duiden dat de **privacywetgeving** verbiedt om camerabeelden te verspreiden. Alle uitgebreide info (bv. bewaartermijn etc.) kan u vinden op de website van de privacy commissie.

Is de gemiddelde ondernemer goed verzekerd?

Ondernemers lijken zich in het algemeen goed te verzekeren tegen allerlei veiligheidsrisico's. Bijna iedereen heeft een verzekering voor brand en ontploffing, waterschade en gevolgen van slechte weersomstandigheden (hagel, bliksem, storm, …). 70% van de bevraagde ondernemers is verzekerd tegen inbraak en 60% tegen diefstal. Ook heeft maar liefst een tiende van de ondernemers zich

verzekerd tegen cybercriminaliteit. Slechts een vierde van de ondernemers heeft zich verzekerd tegen daden van vandalisme en kwaadwilligheid (zoals bv. terrorisme).

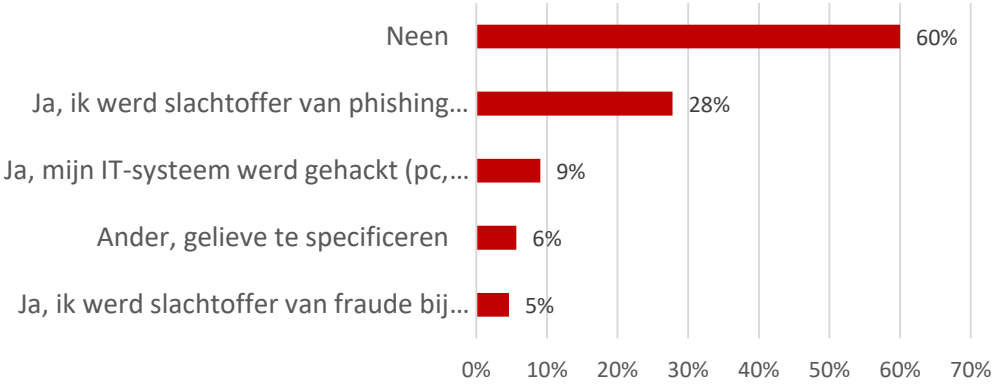


Buurtinformatienetwerk voor zelfstandigen (BIN-z)

Zo'n 43% van de respondenten geeft aan mee te willen doen aan een Buurt Informatie Netwerk voor zelfstandigen (BIN-z). Eén op tien (12%) is reeds lid van een BIN-z, 31% weet het niet en 13% zegt duidelijk geen deel te willen uitmaken van een BIN-z. Deze cijfers zijn vrij gelijkaardig als in 2016.

Cybercriminaliteit

Verder vroegen we aan de respondenten of zij het voorbije jaar getroffen werden door een vorm van internetcriminaliteit. Zo'n 32% van de bevraagde ondernemers werd slachtoffer van phishing. Vaak gaat het ook om een poging tot phishing. Daarnaast werd bij maar liefst een op de tien ondernemers het IT-systeem gehackt en een op de twintig ondernemers was slachtoffer van fraude bij online



betalingen. Vooral groothandelaars blijken een risicogroep voor cybercrime; 67% werd slachtoffer van phishing en 27% van hacking. Het is deze sector die zich ook voornamelijk hiertegen heeft verzekerd (27%).

De grote meerderheid van de bevraagde ondernemers (56%) neemt zelf de beveiligingsmaatregelen en beschikt eerder over een beperkt pakket (firewall, antivirus, …), 20% gaat iets verder en beschikt daarenboven over uitgebreide beveiligingstools (degelijk back-up systeem, encryptiesoftware, VPN, …). Een vijfde van de respondenten besteedt IT-beveiliging uit aan een externe IT-partner. Hiervan is 10% niet op de hoogte van de genomen maatregen en 14 % overlegt regelmatig hierover met zijn leverancier. Op de vraag of er een IT-gedragscode (= duidelijke afspraken rond gebruik van sociale media, (mobiele) apparaten, wachtwoorden, …) wordt gehanteerd, antwoord 36% ja. Dit is een daling ten opzicht van vorig jaar toen de verdeling 50/50 was.

Wanneer we polsen waarom men kiest voor een eerder beperkt veiligheidsbeleid, dan kregen we de volgende antwoorden. 41% vindt het risico dat er zich een cyber issue voordoet te beperkt, 28% vindt dat de kosten niet opwegen tegen de baten en 26% is niet op de hoogte van de mogelijkheden om zich te beschermen. Deze cijfers zijn zeer vergelijkbaar met 2016.

Cybercriminaliteit is een niet te onderschatten fenomeen. Veel ondernemers voelen dit aan als een ver-van-mijn-show, maar niet is minder waar. UNIZO raadt ondernemers aan om zich goed te beschermen tegen cybercriminaliteit. UNIZO stelt reeds heel wat informatie ter beschikking: 1) de UNIZO advies pocket ‘Veilig omgaan met ICT en het internet’. 2) Het Centrum voor Cybersecurity in België (CCB) heeft een gids samengesteld met een aantal (basis- en meer geavanceerde) cybersecuritymaatregelen. 3) Ook op Safeonweb.be vindt men heel wat informatie over online beveiliging. Safe on web heeft ook een phishingtest gemaakt waarmee u kan testen of u in staat bent om een phishingmail te herkennen. Verdachte mails kan u altijd doorsturen naar verdacht@safeonweb.be. 4) UNIZO biedt ook professioneel advies aan via Expert@Board. U kan hierbij beroep doen op de KMO-Portefeuille (subsidies) waarbij de Vlaamse Overheid 30% tot 40% van uw factuur betaalt. Tot slot adviseert UNIZO haar leden om frauduleuze praktijken steeds te melden bij het Belgische meldpunt voor cyberincidenten (CERT.be) alsook om klacht in te dienen bij de politie indien u ook slachtoffer bent.