

# Praktische tips om inbraak en (cyber)diefstal in uw bedrijf te voorkomen!



Ieder bedrijf heeft geld of goederen in huis die aantrekkelijk zijn voor inbrekers. En vergeet de cyber-criminelen niet! Zij zijn niet uit op spullen, maar op geld, vertrouwelijke informatie (klant informatie, bankgegevens, intellectueel eigendom, bedrijfsgeheimen) of persoonsgegevens (voor identiteitsfraude). Deze praktische tips helpen u een inbraak, overval of diefstal te voorkomen.

1

## Maak het inbrekers lastig om uw pand binnen te komen

- **Spreek vreemden aan**  
Inbrekers doen vaak vooronderzoek. Maak het ze niet te gemakkelijk. Spreek daarom vreemden in en rond uw bedrijfspand aan. Er is niets tegen op een beleefd: 'Kan ik u ergens mee helpen?'.
- **Laat bezoekers zich altijd melden bij binnenkomst**  
Bezoekers die bij binnenkomst van een bedrijf gewoon door kunnen lopen, dat is vragen om ongewenst bezoek en diefstal van spullen. Laat uw medewerker bezoekers begeleiden in uw pand, zo voorkomt u dat bezoekers 'verdwalen' en rondsnuffelen.
- **Kies voor certificaatsleutels en stel regels aan het sleutelgebruik**  
Certificaatsleutels zijn niet na te maken, behalve door degene die het bijbehorende certificaat bezit. Houd goed bij wie welke sleutels in zijn bezit heeft en laat medewerkers voor ontvangst tekenen. Controleer regelmatig of iedereen zijn sleutel nog heeft. Zorg ervoor dat medewerkers hun sleutels inleveren als ze uit dienst gaan.
- **Plaats hang- en sluitwerk dat voldoet aan de SKG-normen**  
SKG is de onafhankelijke Stichting Kwaliteit Gevelbouw. SKG geeft met een sterrenstelsel aan hoe lang het hang- en sluitwerk een inbreker die met gereedschap probeert binnen te komen, tegenhoudt. 2 sterren staat voor 3 minuten, 3 sterren voor 5 minuten.
- **Plaats inbraakwerend beslag en eventueel dievenklauwen op deuren**  
Deuren die naar buiten draaien, voorziet u van minimaal 3 dievenklauwen of veiligheidsscharnieren. Anders lukt het dieven vrij eenvoudig de scharnierpennen te verwijderen en zijn ze zo binnen.

2

## Voorkom een grote buit

- **Maak het de inbreker moeilijk om buit te verzamelen**  
Berg voertuig sleutels of waardevolle spullen bijvoorbeeld op in een inbraakwerende (en verankerde) kast of sluit het magazijn af met een inbraakwerende deur. Deze maatregelen hebben het meeste effect in combinatie met een inbraakalarmsysteem. Anders weet de inbreker dat hij alle tijd heeft om de kast of deur open te breken.
- **Plaats camera's (Live View)**  
Camera's worden steeds geavanceerder. Ze kunnen draaien, inzoomen en zelfs kentekens herkennen. Handig is dat u de beelden thuis of onderweg ook live via internet kunt bekijken, bijvoorbeeld op uw smartphone. Daardoor kunt u de particuliere alarmcentrale (PAC) of de politie (Live View) mee laten kijken bij een inbraakalarm.
- **Creëer een inbraakwerend compartiment**  
Dit kan met inbraakwerende rolluiken (SKG-gekeurd), slagvaste vitrines en gevelelementen met inbraakwerend glas.

---

- **Installeer een mistgenerator**

Als door een inbraak uw alarmsysteem met daaraan gekoppelde mistgenerator wordt geactiveerd, vult de mistgenerator uw winkelpand binnen enkele seconden met een ondoorzichtige mist. De inbreker ziet geen hand meer voor ogen en maakt dat hij wegkomt. Zonder buit. Want wat je niet ziet, kun je ook niet meenemen.

3

### Bescherm uw bedrijfsgegevens tegen cybercrime

- **Zorg voor een firewall**

Een firewall houdt de meeste aanvallen van hackers, computervirussen, spyware en ransomware buiten. Laat uw systeembeheerder de firewall goed instellen, want fabrieksinstellingen bieden meestal onvoldoende bescherming.

- **Installeer een up-to-date anti-virussysteem**

Bescherm alle apparatuur die (in)direct met internet in verbinding staat, zoals uw computers en server. Er zijn diverse betaalde en zelfs gratis anti-virusoplossingen verkrijgbaar. Gebruik altijd de laatste versie.

- **Voer alle software-updates direct uit**

Een software-update is in feite een gratis bescherming tegen alle beveiligingsproblemen die tot dan toe bekend zijn. Hiermee voorkomt u dat uw website, server of computers in handen vallen van hackers die met automatische tools het internet afspeuren naar beveiligingslekken.

- **Zorg voor bewustwording bij uw medewerkers**

Bespreek de cyberrisico's van uw bedrijf met uw medewerkers en maak heldere afspraken over jullie aanpak om cybercrime te voorkomen.

- **Maak dagelijks een back-up**

Laat elke werkdag uw bestanden opslaan op een medium buiten het netwerk (zoals een losse harde schijf of tape) en berg deze apart van de server op. Controleer ook regelmatig of het back-upstelsel goed functioneert. Het zou zonde zijn als u bij schade alsnog met lege handen staat.