

De operatie **'VERNIEUWING EN UITBREIDING BEVEILIGINGSCAMERA'S'** voor bedrijven-terrein De Stad en De Scheper afgerond



Op deze bedrijventerrein werden 44 nieuwe camera's geïnstalleerd door onze partner Trigion Brand en Beveiligings-techniek uit Schijndel.

Alle Camera's geven zowel overdag als 's nachts gekleurde en

heldere beelden, waardoor er altijd sprake is van een goede bewijslast. De ANPR (automatische kentekenplaat herkenning) brengt de kentekenplaat goed in beeld. Of het nu gaat om een schade, aanrijding, bedreiging of diefstal, zowel uzelf als de politie zal met behulp van de camerabeelden eenvoudig de oorzaak

kunnen achterhalen en de daders opsporen.

Met medewerking MKB-Nederland, Gemeente Oirschot, Politie en Brandweer leveren wij u een systeem met een groter gevoel van veiligheid en bescherming. De systemen zijn continu onderworpen aan vernieuwing en verbetering met terugkoppeling aan u als gewaardeerd deelnemer aan het collectief.

Mits u lid bent natuurlijk van SBBO, want zonder loyaliteit van deelname aan het collectief kunnen we geen continuïteit waarborgen. Zie voordelen van lidmaatschap op www.oirschotveilig.nl

Wij wensen u veel leesplezier.

Tico Dekkers

Voorzitter SBBO en Oirschot Veilig

Algemene Verordening **GEGEVENSBESCHERMING**

De opslag en het uitlezen van de beeldopnamen is geregeld in de Algemene Verordening Gegevensbescherming, de verder te noemen AVG wet en de Gemeentewet.

De bewakingscamera's zijn geplaatst in Oirschot op De Stad en de Scheper ten behoeve van de bescherming van personen, gebouwen eigendommen en goederen. Dit ook vanuit het begrip Oirschot Veilig. Mede vanuit het Keurmerk Veilig Ondernemen (KVO). Met de duidelijk zichtbare camerabewaking kan bij incidenten een veroorzaker van problemen mogelijk worden

getraceerd. In dit geval van opslag en uitlezen van beeldopnamen op het bedrijventerrein is de AVG van toepassing. Het gaat hier om privacywetgeving. Bevoegd gezag ligt bij de Autoriteit Persoonsgegevens. Er is geen sprake van cameratoezicht met betrekking tot de handhaving van de openbare orde (zoals dit het geval is in het centrum en de uitgaansgebieden). De Stichting SBBO is hiervoor verantwoordelijk. Daar het systeem op De Stad en De Scheper voldoet aan die eisen is een melding bij de Autoriteit Persoonsgegevens en eventueel het CBP niet noodzakelijk.

BRANDVEILIGHEID

in uw bedrijf

Bent u eigenaar van een gebouw of gebruikt u een gebouw? Dan bent u verantwoordelijk voor de brandveiligheid en brandpreventie.

Voor brandpreventie gelden landelijke regels. Die regels staan in het Bouwbesluit 2012. In sommige gevallen heeft u een omgevingsvergunning voor brandveilig gebruik nodig. Of u moet een gebruiksmelding voor brandveilig gebruik doen bij de gemeente. Helaas onderschatten ondernemers het risico van brand, vooral de gevolgen die kunnen ontstaan na brandschade. Maar liefst 60% van de Nederlandse bedrijven gaat failliet binnen twee jaar na een calamiteit. De reden? Het verlies van klantrelaties.

Preventiemaatregelen

Voorkomen is uiteraard beter dan genezen. Daarom is het belangrijk om preventiemaatregelen te nemen en te onderhouden. Het nemen van preventieve maatregelen is belangrijk voor het beperken van de



gevolgschade en om het risico op brand in de eerste instantie te minimaliseren. Daarnaast is het ook belangrijk voor uw verzekeraar – de kans is anders groot dat de schade niet wordt gedekt. De schade-uitkeringen door brandverzekeraars worden steeds hoger, waardoor de premies verhoogd worden en de preventie eisen verzaamd worden. Denkt u dan bijvoorbeeld aan het op tijd laten uitvoeren van de juiste keuringen en goed onderhoud. Als na een brand blijkt dat u daar niet aan hebt voldaan, dan is er een grote kans dat de schade niet vergoed wordt.

Hoe zit het met uw RI&E (risico analyse & evaluatie) en met uw BHV plan? (bedrijfshulpverlening) Heeft u hulp nodig neem dan contact op met: <https://www.rie.nl/>

De 10 MEEST VOORKOMENDE misverstanden over CYBERCRIME



1. “Ik ben niet interessant voor cybercriminelen”

Een veelvoorkomend misverstand: men leeft in de illusie dat ze geen interessant doelwit zijn voor digitale criminelen of hackers. Dit is niet waar. Jouw data is namelijk altijd interessant voor hackers.

2. “Ik heb een complex wachtwoord met speciale tekens, dit is daarom nooit te raden”

Een 5 teken wachtwoord duurt 3 minuten om te kraken. Een 12 tekenwachtwoord duurt 655 jaar.

3. Een “Tweestap” verificatie is niet nodig, want ik heb een lang wachtwoord”

Je hebt een lang wachtwoord en dan ben je er toch? Niet helemaal. Mocht je je wachtwoord toch prijsgeven, kunnen hackers nog niet direct je account in. Door het instellen van tweestap verificatie voeg je een extra beveiligingslaag toe bij een lang wachtwoord. Bij de belangrijkste accounts kun je dit zelf toevoegen.

4. “Updates voer ik enkel uit als er ook interessante wijzigingen van toepassing zijn”

Producenten van besturingssystemen, browsers en andere programma's, zoals Apple, Microsoft Office, Adobe Reader en Oracle Java, brengen geregeld updates uit om beveiligingslekken te verhelpen. Verouderde software is de belangrijkste oorzaak van hacks.

5. “Openbare wifi netwerken zijn altijd veilig”

Bij openbare en onbeveiligde wifi netwerken (free wifi) is het voor anderen mogelijk om te zien wat je op het internet doet en welke gegevens je verstuurt. Verstuur dus geen gevoelige informatie over netwerken die je niet kent of niet vertrouwt. Of gebruik een VPN. Versleutel thuis je draadloze netwerk met een lang wachtwoord om te voorkomen dat kwaadwillenden je internetverkeer kunnen onderscheppen.

6. “Ik gebruik de cloud en loop geen risico om cyber slachtoffer te worden”

De cloud is als het ware een externe harde schijf, gekoppeld aan het internet. Deze cloud is vanuit iedere locatie te raadplegen, wat het een zeer gebruiksvriendelijke manier maakt om gegevens op te slaan. Zonder een uniek en lang wachtwoord met een tweede stap verificatie, is echter ook jouw cloud omgeving gemakkelijk te hacken. Dus ook bij het gebruik van een cloud omgeving blijft het belangrijk dat je aandacht hebt voor beveiliging.

7. “Een cyber aanval plegen vergt veel technische kennis en is dus niet voor iedereen weggelegd”

De wereld van de cybercrime professionaliseert in hoog tempo. Er zijn tegenwoordig zelfs websites waar criminelen simpelweg de software kunnen bestellen die ze nodig hebben voor hun digitale delicten:

cybercrime-as-a-service (CAAS). Daarmee groeit ook het risico om slachtoffer te worden

8. “Investeren in digitale veiligheid is te duur”

De jaarlijkse schade door cybercrime voor de Nederlandse economie bedraagt inmiddels meer dan 10 miljard euro per jaar. In 2019 is ruim 55% van het midden- en klein bedrijf minstens één keer slachtoffer geworden van cybercrime. De schade door een digitale aanval loopt snel op, omdat je dagelijkse werkzaamheden niet meer (volledig uitgevoerd kunnen worden).

9. “Aangifte doen van cybercrime is zinloos”

Sommige mensen denken dat aangifte doen van cybercrime geen zin heeft, omdat de politie er niets mee doet. Dit is een misverstand. Iedere aangifte is namelijk een puzzelstukje om een zaak op te kunnen lossen. De realiteit is echter wel dat cybercriminelen wereldwijd en anoniem opereren. Het is daarom een grote uitdaging voor politie om deze criminelen te pakken en het oplossingspercentage is helaas laag. Toch blijft het heel belangrijk om te melden.

10. “Mijn IT'er is verantwoordelijk voor mijn digitale veiligheid”

Het is een veelvoorkomend misverstand: ondernemers die denken dat hun IT'er de digitale veiligheid regelt. Dit is niet vanzelfsprekend! Uw IT'er is voornamelijk bezig met het draaiende houden van uw systemen. Maar dit betekent niet dat hij per definitie aandacht (of kennis) heeft voor uw digitale veiligheid. Dit misverstand kan ervoor zorgen dat u onbewust een groot risico loopt op schade door een digitale aanval.

www.hackhelpdesk.nl



CAMERA in BEELD

Camera in Beeld is een systeem van de politie waar burgers en bedrijven vrijwillig hun beveiligingscamera(s) kunnen aanmelden. Dankzij deze informatie weten wij per straat welke beveiligingscamera's beschikbaar zijn.

Als er een misdrijf is gepleegd waarbij camerabeelden kunnen helpen om de daders op te sporen, kunnen wij die beelden gericht opvragen bij de camera-eigenaren. Ook SBBO heeft zijn camera's ondergebracht onder protocol Camerabeelden beveiliging SBBO leden.

Even **VOORSTELLEN...**



De politie staat graag in verbinding met de maatschappij en als wijkagent wil ik graag een verbindende factor zijn tussen ondernemers en politie.

Ondernemers maar ook andere inwoners van Oirschot zijn soms ook gevestigd op de bedrijventerreinen waar wij als politie niet altijd even goed zicht hebben. Dit heeft vaak meerdere redenen maar neemt niet weg dat wij als politie dat als een groot gemis ervaren. Ik vind het daarom dan ook fijn dat we met de SBBO het K.V.O.-certificaat opnieuw hebben behaald.

Als politie willen we dan ook graag met u in contact blijven om samen het gevoel van veiligheid op de industrieterreinen te vergroten.

Als wijkagent heb ik regelmatig overleg waarbij zaken besproken worden en we van elkaar weten wat er speelt in de wijken en industrieterreinen en wat er op dat moment eventueel nodig is voor wat betreft politionele inzet. We willen vooral laagdrempelig zijn en trachten daarmee de meldingsbereidheid te verhogen.

Het doen van een melding of zelfs het doen van aangifte hebben we een stuk eenvoudiger gemaakt. Dit laatste kan tegenwoordig ook online via de site www.politie.nl. is de politie nog steeds telefonisch te bereiken op **0900-8844** maar u kunt mij ook rechtstreeks mailen met uw vraag of opmerking op het volgende emailadres: perry.van.zuydam@politie.nl



Het bestuur van

SBBO

*Wenst U fijne feestdagen
en een gelukkig nieuwjaar!*


Oirschot Veilig
Samen werken aan veiligheid!

Stichting Beveiliging Bedrijventerreinen Oirschot

Postbus 196, 5688 ZK Oirschot

T 0499 37 81 93

E info@oirschotveilig.nl

www.oirschotveilig.nl

www.facebook.com/stichting.oirschotveilig

Trigion brand en beveiliging

Van Leeuwenhoekweg 1

5482 TK Schijndel

T 088 29 86 750

www.trigion.nl

Promeon Security B.V.

Surveillance en bewaking

Moorland 3F

5688 GA Oirschot

T 0499 84 72 66

E info@promeon.nl

www.promeon.nl