Stichting Beveiliging Bedrijven Hardinxveld-Giessendam

Nieuwsflits november 2020

Van het bestuur

Beste ondernemers,

In deze voor velen van u onzekere tijd, beperken we ons in de nieuwsflits tot aandachtpunten van politie en brandweer.

Tevens een ingezonden stuk met tips voor veilig thuiswerken, door Jan Mudde, lid van onze KVO-werkgroep. Mocht u ook tips met collega-ondernemers willen delen dan kunt u dat doorgeven via: secretariaat@sbbhg.nl

Incidentcijfers en het belang van camera's

De camera's en verlichte informatieborden bij in-/uitgangen van de bedrijventerreinen bewijzen hun nut, met name het nut van preventie. In de afgelopen maanden zijn slechts enkele meldingen bij de politie binnen gekomen, waaronder 2 x diefstal. De politie heeft deze zaken in behandeling. Daarnaast zijn door de camera's veel kentekens van voertuigen geregistreerd (hits) die een vermelding hebben (verdacht, geen motorrijtuigenbelasting betaald of onverzekerd). Deze kentekens worden door de politie verder onderzocht.

Afgevaardigden bedrijventerreinen in KVO-werkgroep

Boven Hardinxveld	Rob den Breejen	rob@breejen-shipyard.nl
Nieuweweg	Dietrik vdn Berg	info@gebrvandenberg.nl
Langeveer/Rivierdijk	Arnold Noordermeer	a.noordermeer@boermantransport.nl
De Peulen	Jan Mudde	j.mudde@giessen.nl
Blauwe Zoom	Jan de Hoop	jdh@gebroedersblokland.nl

In de werkgroep hebben verder zitting afgevaardigden van Gemeente, Politie*, Brandweer*, Camera Uitleesruimte, Alert Security en Intersafety.

Projectleider/tevens bestuurslid is Chris Tol chris.tol@kpnmail.nl

Bijzonderheden kunt u melden bij de afgevaardigde op uw terrein

** Voor namen en email-adressen politie en brandweer →– zie pag 2*

Van de Politie

Aangifte bereidheid

Dat in de afgelopen periode slechts tweemaal een aangifte bij de politie is gedaan is natuurlijk goed nieuws, maar het kan ook zijn dat er wel degelijk meerdere incidenten zijn geweest, maar dat daarvan geen aangifte is gedaan. Het is voor slachtoffer(s)/ benadeelde(n) van belang dat de dader(s) worden opgespoord. Ook is het van belang dat de overheid (politie) kennis krijgt van de veiligheid op de bedrijventerreinen, zodat zij hun beleid van toezicht etc. daarop kunnen aanpassen.

Bij heterdaad kunt u altijd 112 bellen! In andere gevallen kunt via 0900-8844 een afspraak maken om aangifte te doen; dit kan ook digitaal via www.politie.nl Het verdient aanbeveling om bij uw aangifte aan te geven dat het bedrijventerrein met camera's is beveiligd en dat uw bedrijf al dan niet ook eigen camera's heeft. De politie alleen is gerechtigd om de ANPR-camerabeelden bij de CUR uit te kijken.

Project Camera in Beeld

In de vorige nieuwsflits is gevraagd of u wilt meewerken aan het politieproject "Camera in Beeld". De politie registreert alle bedrijven die voorzien zijn van camera's, zodat daar wellicht gebruik van gemaakt kan worden bij calamiteiten. Slechts een paar bedrijven hebben zich aangemeld. U kunt zich alsnog laten registreren, via www.politie.nl , thema 'Camera in Beeld'.

Wijkagent operationeel expert, Antoinet de Bruijn
Wijkagenten, Tiny Hol, Willem Doesberg en Jaap Hartkoorn.
Afdeling.D2.WP.Hardinxveld@zuid-holland.politie.nl.

Van de Brandweer

Buiten opgeslagen brandbare goederen op eigen terrein vallen onder de verantwoordelijkheid van de ondernemer zelf. Vaak is men zich niet bewust van de risico's die een dergelijke opslag met zich meebrengt. Als brandweer staan wij voor minder branden, minder slachtoffers en minder schade.

Meer informatie?
Heeft u vragen of wilt u meer informatie? Neem dan contact op met de brandweer via **brandveiligleven@brw.vrzhz.nl** of bekijk onze website: www.brandweer.nl

R. (Ruud) Alblas, adviseur Risicobeheersing Brandweer Zuid-Holland Zuid

Ingezonden door Jan Mudde, lid KVO-werkgroep

Gezond en veilig thuiswerken

Beveiliging en veiligheid, zaken die nauw met elkaar zijn verbonden. Preventie hoort in feite ook in dit rijtje thuis. Over thuis gesproken….. nu we met veel mensen meer en vaker thuiswerken, verdient de plaats waar we dat doen extra aandacht. Denk bijvoorbeeld aan de stoel waarop medewerkers thuis hun "productie" draaien. Door aan het zitten, de werkhouding en voldoende beweging aandacht te besteden, kunnen lichamelijke klachten worden voorkomen. In sommige situaties past het dat medewerkers hun bureaustoel mee naar huis nemen, soms gaat dit niet. Juist dan is het ook belangrijk om de medewerkers bewust te maken van een juiste houding en hen daarin desgewenst te ondersteunen met een goede (tijdelijke) stoel, een beeldscherm-verhoger, zit-/sta-bureau of polssteun etc. Maar ook een zit- of werkplek advies kan al een groot verschil maken.

Voor tips om veilig digitaal thuis te werken → Zie pag 3

8 TIPS OM VEILIG THUIS TE WERKEN !

1 Let extra op phishingmails

Phishing is het meest succesvolle middel voor hackers om binnen te dringen in organisaties. De mails worden steeds realistischer, specifieker en moeilijker te herkennen. Doordat er tijdens het thuiswerken minder contact met collega's is, worden mails minder snel opgemerkt.

2 Wees alert op nepnieuws

Juist in deze tijd is er sprake van een toename van websites die nepnieuws publiceren. Bijvoorbeeld een site die een lijst met een onjuist aantal COVID-19 besmettingen toont. Dergelijke sites kunnen in staat zijn om kwaadaardige software en virussen op uw computer te installeren.

3 Gebruik twee-staps-verificatie

Dit is een dubbele beveiliging. Naast het opgeven van een gebruikersnaam en wachtwoord moet u een extra code opgegeven die via een app of SMS wordt verzonden. Hackers hebben dan aan uw gebruikersnaam en wachtwoord niet meer genoeg om op uw account in te loggen.

4 Installeer updates

Thuis hebben we steeds meer apparaten die verbonden zijn met het internet. Deze apparaten zijn vaak kwetsbaar. Hackers kunnen hierdoor toegang krijgen tot privé of zakelijke gegevens. Zorg er daarom voor dat beschikbare updates regelmatig worden geïnstalleerd.

5 Beveilig uw (WiFi-)netwerk

Er zijn twee belangrijke zaken om uw netwerk thuis beter te beveiligen: zorg er altijd voor dat uw WiFi-netwerk beveiligd is met een wachtwoord en dat uw router/modem altijd is voorzien van een aangepast wachtwoord.

6 Houd uw werkomgeving privé

Zorg ervoor dat niemand toegang heeft tot uw werkcomputer. Ook familie en kinderen niet. Zij kunnen onbedoeld kwaadaardige software downloaden of bestanden openen die ze niet mogen zien. Let er op dat gesprekken privé blijven en vermijd het afdrukken van gevoelige informatie.

7 Een versleutelde verbinding

Zorg er voor dat als u vanaf afstand toegang heeft tot bedrijfssystemen, u altijd gebruik maakt van versleutelde verbindingen. Dit kan o.a. door het gebruik van VPN-oplossingen. Vraag uw ICT-beheerder of dit voor u is geregeld.

8 Check www.veiliginternetten.nl

Op de website www.veiliginternetten.nl staan veel tips, tricks en praktische handleidingen om veiliger te kunnen internetten. Met regelmaat worden er nieuwe onderwerpen behandeld en handreikingen gegeven hoe u veiliger gebruik kunt maken van het internet.

Aspect ICT | Handelsstraat 4 | 3371XC Hardinxveld-Giessendam | 0184-675400