Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
4062028

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 6 juli 2022
Onderwerp Preventie cybercrime voor het midden- en kleinbedrijf

Ondernemingen in het midden- en kleinbedrijf zijn kwetsbaar voor cybercrime en worden er vaak slachtoffer van. Het is daarom van belang ondernemers te helpen de weerbaarheid van hun onderneming te versterken. Zo kan slachtofferschap worden tegengegaan en de schade worden beperkt. Deze brief schetst de inspanningen van het kabinet om het midden- en kleinbedrijf (hierna: mkb) te ondersteunen om veiliger te zijn voor cybercrime. Hiermee wordt uitvoering gegeven aan de motie-Ephraïm c.s.[1] en de motie-Hermans c.s.[2] Deze brief is een aanvulling op de eerder dit jaar verstuurde brief over de voortgang van het Digital Trust Center[3] en beschrijft de preventieve voorlichting en andere maatregelen die genomen worden om ondernemers te faciliteren in het vergroten van hun online veiligheid. De aanpak van cybercrime omvat naast de in deze brief genoemde inspanningen diverse andere activiteiten, zoals opsporing en verstoring. Over deze activiteiten is uw Kamer periodiek geïnformeerd. Voor een toelichting op de bredere aanpak van cybercrime verwijs ik kortheidshalve naar de meest recente brief hierover.[4]

Cybersecurity-incidenten zijn in het mkb wijdverbreid. Een deel daarvan is te wijten aan cybercrime. In 2021 heeft zich bij 25% van de bedrijven van 10 of meer medewerkers een incident met een interne oorzaak voorgedaan, zoals storingen van ICT-systemen, en bij en 10% een incident met een externe oorzaak, zoals cybercrime. Tegelijkertijd laten CBS-data zien dat (basale) veiligheidsmaatregelen door veel bedrijven niet worden genomen.[5] Hier is nog een wereld te winnen. Door basismaatregelen te nemen wordt het cybercriminelen minder makkelijk gemaakt om netwerken binnen te komen en schade aan te richten, direct of indirect.

[1] Kamerstukken II, 2021 – 2022, 26 684, no. 682.
[2] Kamerstukken II, 2021 – 2022, 35 788, no. 120.
[3] Kamerstukken II, 2021 – 2022, 26 643, no. 817.
[4] Kamerstukken II, 2020 – 2021, 26643, no. 768.
[5] opendata.cbs.nl/#/CBS/nl/dataset/85180NED/table?ts=1650540851138. Voor bedrijven tussen de 50 en 250 werknemers was dit 37% en 15% (respectievelijk intern en extern incident)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Hoewel volledige veiligheid niet bestaat, kunnen basismaatregelen veel criminaliteit voorkomen. Het is daarbij van belang te constateren dat het mkb een heterogene groep is. Er bestaan grote verschillen in omvang (klein, midden en groot mkb), sectoren en mate van cyberveiligheid.

Doelstelling: verhogen cyberweerbaarheid van mkb-ondernemers

Zoals hierboven gemeld wordt het mkb vaak slachtoffer van cybercriminaliteit. Het doel van onze inspanningen is daarom de cyberveiligheid te verhogen, effecten van incidenten te minimaliseren en cyberrisico's inzichtelijk te maken. Daarbij geldt als uitgangspunt dat de ondernemer in eerste instantie zelf verantwoordelijk is voor de maatregelen die genomen moeten worden. De overheid heeft een faciliterende rol. Zij verschaft de informatie en instrumenten om bedrijven in staat te stellen risico's af te wegen en de nodige maatregelen te treffen.

Bij het verhogen van de veiligheid ligt de nadruk op het stimuleren van het gebruik van diverse veiligheidsmaatregelen door bedrijven, zoals omschreven in de vijf basisprincipes van het Digital Trust Center.[6] Door het delen van algemene en specifieke dreigingsinformatie kan het Digital Trust Center bijdragen aan het minimaliseren van de effecten van externe incidenten. Met het uitbreiden van de onderzoeken en diensten die als doel hebben de cyberweerbaarheid van het Nederlandse mkb in kaart te brengen, ontstaat bovendien meer inzicht in de cyberrisico's voor het mkb. Daarnaast is er winst te behalen door bedrijven nog meer te stimuleren zelf veiligheids- en risicoanalyses uit te voeren. CBS-data laten zien dat slechts de helft van de bedrijven met meer dan 10 werknemers op reguliere basis een risicoanalyse uitvoert.[7] Een verhoogde inzet op bekendheid van de tools van het Digital Trust Center kan veel bedrijven stimuleren hier de nodige stappen in te zetten.[8]

Behoefte mkb
Om ondernemers goed te kunnen ondersteunen is het van belang aan te sluiten op hun behoeften. Daarom is in de afgelopen periode met ondernemers en hun vertegenwoordigers gesproken over cyberveiligheid en hoe deze te verhogen. Uit die gesprekken komt het volgende naar voren.

- Het tegengaan van cybercriminaliteit is strategisch belangrijk, maar niet het enige probleem waar het mkb mee kampt. Het is gewenst om niet uitsluitend op cyberveiligheid te focussen, maar er wel structureel aandacht voor te hebben.
- Relatief veel mkb-ondernemers onderschatten de ernst en risico's van cybercriminaliteit. Het is daarom belangrijk om in te zetten op voorlichting en bewustwording.
- Als ondernemers wordt aanbevolen een groot aantal vrij complexe handelingen te verrichten, kan dit leiden tot een averechtse reactie. Het is wenselijk de communicatie eenvoudig te houden en de hoeveelheid communicatie te beperken.
- Het Digital Trust Center is het landelijk aanspreekpunt voor ondernemers in de niet-vitale sectoren. Echter, veel ondernemers hebben behoefte aan hulp dichter bij huis. Er is behoefte aan spreiding van kennis en informatie op regionaal en lokaal niveau.

[6] www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
[7] opendata.cbs.nl/#/CBS/nl/dataset/85179NED/table?ts=1654249573230
[8] www.digitaltrustcenter.nl/tools

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Brancheorganisaties, Regionale Platforms Veilig Ondernemen, gemeenten en samenwerkingsverbanden van het Digital Trust Center kunnen voor ondernemers een belangrijke rol in spelen. Het Digital Trust Center zet daarom in op het opzetten en/of versterken van samenwerkingsverbanden die regionaal of branchegericht zijn. Op dit moment zijn er 44 samenwerkingsverbanden bij het Digital Trust Center aangesloten. Het streven is dat dit eind 2023 50 samenwerkingsverbanden zijn.

Deze brief gaat eerst in op de voorlichting van het Digital Trust Center, daarna op het stimuleren van gedragsverandering via samenwerkingsverbanden en ten slotte wordt kort het nader onderzoek behandeld.

Voorlichting Digital Trust Center

In de afgelopen jaren heeft het kabinet via publiekscampagnes (zoals 'Eerst checken, dan klikken' en 'Doe je updates') ingezet op het verhogen van de bewustwording van cybercrimerisico's. De doelgroep was het bredere publiek in het algemeen. In de bijlage van deze brief is, zoals toegezegd aan de Kamer, een overzicht van campagnes voor bewustwording van online veiligheid opgenomen.[9]

Om meer bewustwording én gedragsverandering te bereiken intensiveert het Digital Trust Center zijn voorlichtingsactiviteiten. Deze zijn opgedeeld in drie onderdelen. Ten eerste wordt het Digital Trust Center beter onder de aandacht gebracht bij ondernemers. Het is dé organisatie van de Rijksoverheid waar ondernemers voor hun informatie over cyberveiligheid terecht kunnen. Een grotere bekendheid van het Digital Trust Center bij ondernemers stelt hen in staat passende informatie te vinden om de basisveiligheid op orde te krijgen. Een voorbeeld hiervan is dat het Digital Trust Center eind juni een campagne start om het risico van phishing onder de aandacht te brengen, waardoor de bewustwording hierover toeneemt en het Digital Trust Center beter bekend wordt. De campagne is gebaseerd op een grootschalig onderzoek naar phishing. De resultaten van het onderzoek worden gepubliceerd op www.rijksoverheid.nl en www.digitaltrustcenter.nl. Het Digital Trust Center heeft bovendien het doel om in de komende vier jaar het aantal bezoekers op de website te verhogen van 200.000 naar 300.000 per jaar.

Ten tweede zal het Digital Trust Center de instrumenten die de ondernemer helpen passende maatregelen te nemen voor cyberveiligheid, uitbreiden. Op dit moment zet het Digital Trust Center twee instrumenten in: de zelfscan-tool op basis van de vijf basisprincipes van online veiligheid (de basisscan) en de risicoanalyse-tool.[10] Deze helpen ondernemers kwetsbaarheden te vinden en de juiste (basis)maatregelen te nemen. Het Digital Trust Center zal dit aanvullen met een tool die kleine bedrijven op weg helpt, waaronder ZZP-ers die geen tot weinig kennis hebben van, of interesse hebben in, cyber security. De tool wordt zeer praktisch, in begrijpelijke taal en activerend. Centraal bij alle voorlichting van het Digital Trust Center staan de concrete handelingsperspectieven voor ondernemers. Het is namelijk cruciaal dat de stap van weten naar doen wordt gemaakt.

[9] Toezegging Minister van Justitie en Veiligheid tijdens Commissiedebat Online Veiligheid en Cybersecurity op 1 december 2021.
[10] Deze twee instrumenten zijn reeds functioneel en toegankelijk op www.digitaltrustcenter.nl/tools.

Ten derde zal het Digital Trust Center het direct informeren van individuele bedrijven over concrete dreigingsinformatie via de daartoe ingerichte informatiedienst opschalen. Over deze nieuwe dienstverlening is de Kamer op 2 juni 2021 en 7 februari 2022 geïnformeerd.[11] Over de voortgang van deze informatiedienst heeft uw Kamer op 27 juni jl. een overzicht ontvangen, zoals toegezegd bij het Commissiedebat cybersecurity en online veiligheid van 9 april jl. Dit overzicht laat zien dat bij een steeds groter aantal cyberincidenten individuele bedrijven zijn gewaarschuwd en een handelingsperspectief aangereikt hebben gekregen. Tot slot biedt het Digital Trust Center met een besloten community met een sterk groeiend aantal aangesloten leden (nu meer dan 1100) ondernemingen de mogelijkheid actuele en relevante informatie uit te wisselen. Hier wordt steeds meer gebruik van gemaakt.

<u>Stimuleren gedragsverandering via samenwerkingsverbanden</u>

In recente gesprekken met mkb-organisaties komt sterk naar voren dat weten nog geen doen is. Voorlichting en bewustwording zijn een noodzakelijk startpunt, maar niet voldoende. De ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat zijn daarom gezamenlijk twee acties gestart: pilots onder de vlag van de City Deal Lokale weerbaarheid Cybercrime, waar ook het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties bij betrokken is, en de pilot Samen Digitaal Veilig. Het doel hiervan is om in bestaande en nieuwe samenwerkingsverbanden de cyberveiligheid te vergroten, te leren welke activiteiten het meest effectief zijn en deze breder te kunnen inzetten. Daarnaast wordt inmiddels samengewerkt met de Kamer van Koophandel en wordt gewerkt aan de ondersteuning bij incidenten. Hieronder gaan we nader op deze punten in.

Innovatieve pilots City Deal "Lokale weerbaarheid cybercrime"
In de City Deal "Lokale weerbaarheid cybercrime" zijn de afgelopen jaren lokale en regionale innovatieve pilots gestart om de weerbaarheid van mkb-ondernemers te verhogen. Uit evaluaties van deze eerste pilots blijkt dat ondernemers blij zijn met tips en handleidingen via digitale kanalen, waaronder die van het Digital Trust Center. In de praktijk blijkt het voor mkb-ondernemers lastig deze in te voeren in de eigen onderneming. In pilots van de afgelopen jaren werden ondernemers met raad en daad ondersteund door ICT-studenten of ICT-leveranciers om de in scans gesignaleerde risico's aan te pakken en de geadviseerde maatregelen daadwerkelijk door te voeren. Voortbouwend op de eerste positieve resultaten van deze lokale en regionale pilots hebben de ministeries van Justitie en Veiligheid en Binnenlandse Zaken en Koninkrijksrelaties, en het Digital Trust Center in maart 2022 opnieuw middelen beschikbaar gesteld voor nieuwe innovatieve mkb-cyberpilots. De uitvraag onder Platforms Veilig Ondernemen, gemeenten en regionale samenwerkingsverbanden Veiligheid heeft ertoe geleid dat in april 2022 is gestart met zes nieuwe mkb-projecten, waaronder:

- Sterkere schakels versterken de keten (Regiobureau Integrale Veiligheid Oost-Brabant)
  Dit project ontwikkelt een methodiek waarbij de grote bedrijven de kleinere toeleveranciers ondersteunen bij het opschroeven van de informatiebeveiliging. Dat helpt de weerbaarheid van individuele bedrijven en daarmee van de gehele keten.

[11] Kamerstukken II, 2020 – 2021, 26 643, no. 760; Kamerstukken II, 2021 – 2022, 26 643, no. 817.

- Living Lab Cyberweerbaarheid & Ransomware mkb (Gemeente Groningen)
  Hier komen activiteiten samen die tot nu toe door publiek-private samenwerking in de regio Noord Nederland zijn ontplooid op het gebied van bijvoorbeeld bewustwording, training en scans. De nadruk ligt in eerste instantie op ransomware bij financieel dienstverleners. Dit is de basis voor de selectie van verwante uitdagingen voor het mkb. Deze worden vervolgens met de overheid, het onderwijs en de ondernemers (de " "drie O's") gezamenlijk opgepakt. Het Living Lab Cyberweerbaarheid wordt ondergebracht op drie bestaande fysieke locaties in Noord Nederland.

- Evidence based cybersecurity gedragsinterventie gericht op drie basisprincipes van veilig ondernemen (Platform Veilig Ondernemen Den Haag)
  Dit project ontwikkelt een interventie gericht op drie van de vijf basisprincipes van veilig digitaal ondernemen: het inventariseren van kwetsbaarheden, het uitvoeren van updates en het voorkomen van malware.

De pilots zijn in april 2022 gestart en zullen medio 2023 zijn afgerond. HBO-kennisinstellingen zullen de pilots daarna evalueren. Gemeenten en Platforms Veilig Ondernemen kunnen succesvolle pilots vervolgens landelijk invoeren. Deze activiteiten worden opgenomen in het nieuwe meerjarige actieprogramma Veilig Ondernemen 2023-2026 van het Nationaal Platform Criminaliteitsbeheersing. Het versterken van de mkb-weerbaarheid tegen cybercrime zal daarin – net als in het vorige actieprogramma - een speerpunt zijn.

Project 'Samen Digitaal Veilig'
Het project Samen Digitaal Veilig is onderdeel van nieuwe samenwerkingsafspraken tussen de ondernemersorganisaties (MKB-Nederland en BOVAG) en de ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat. Het project richt zich op het weerbaar maken van bedrijven. Het platform Samen Digitaal Veilig biedt onder meer een elektronische leeromgeving voor medewerkers, met korte informatieve films en toetsen. Brancheorganisaties spelen in de verspreiding van die informatie een belangrijke rol. Zij kunnen, als vertrouwde partner van de bedrijven in de eigen branche, de leeromgeving onder de aandacht brengen. MKB-Nederland en het Digital Trust Center hebben voor de brancheorganisaties diverse bijeenkomsten georganiseerd om het project meer bekendheid te geven, branches aan te sporen meer activiteiten op het gebied van cyberweerbaarheid te ontplooien en hen mee te nemen in de mogelijkheden van het project. Inmiddels hebben meerdere brancheverenigingen interesse getoond in het project. De pilotfase van dit project is bijna afgerond. Komend half jaar wordt aan de hand van de evaluatie van de pilot het vervolg bezien.

Voorlichting met Kamer van Koophandel
Het Digital Trust Center is intensief gaan samenwerken met de Kamer van Koophandel om via zijn kanalen ondernemers te bereiken en te helpen bij het vergroten van hun cyberweerbaarheid. De Kamer van Koophandel heeft een groot bereik bij ondernemers. Bij deze samenwerking is de inhoudelijke kennis van het Digital Trust Center gecombineerd met de landelijke spreiding en het netwerk van de Kamer van Koophandel. Insteek hierbij is om met kwalitatief hoogstaande, inhoudelijke, maar laagdrempelige middelen veel bedrijven te bereiken. Hiertoe zijn korte films ontwikkeld over verschillende basismaatregelen die genomen kunnen worden voor het verhogen van de cyberweerbaarheid. Een voorbeeld hiervan is een video over phishing, die inmiddels ongeveer 100.000 keer is bekeken.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Hulp bij incidenten via brancheverenigingen
In gesprekken met ondernemers en branchevertegenwoordigers en in de Kamer is opgeroepen een ondersteuningsfunctie van brancheverenigingen voor ondernemers te bezien. Er zijn in de eerste plaats commerciële cybersecuritydiensten in de markt waar ondernemers gebruik van kunnen maken. Bovendien bieden verzekeraars cyberverzekeringen aan, waar hulp bij incidenten in het algemeen een onderdeel van is. Er zijn daarnaast initiatieven die het ontstaan van extra ondersteuning voor het mkb via brancheverenigingen op termijn mogelijk maken. Het Digital Trust Center stimuleert regionale en sectorale samenwerkingsverbanden en faciliteert mkb-ondernemers via zijn website. Om de ondernemer zo goed mogelijk te bereiken wordt het Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden uitgebreid. Daar is samenwerking met brancheverenigingen, gemeenten en regionale Platforms Veilig Ondernemen voor nodig. Zo kan de communicatie en daarin vervatte informatie worden toegesneden op de noden en wensen van de ondernemer. In de nieuwe Nederlandse Cyber Security Strategie wordt nader ingegaan op het LDS en op de motie-Van Ginniken over het aanvullend faciliteren van hulp bij incidenten voor ondernemers.

Onderzoek

Om de kennis op het gebied van het ontwikkelen en verspreiden van gedragsveranderende interventies verder te versterken is meer onderzoek nodig. Deze zomer start het onderzoek "Human factors in cybersecurity in het mkb" dat zich richt zich op gedragsverandering: het ontvankelijk maken van mkb-ondernemers voor informatie en vervolgens het daadwerkelijk toepassen van deze informatie. De resultaten van het onderzoek worden omgezet in een *two-pager* en *toolkit,* en gepubliceerd op de website van het Digital Trust Center. Er wordt vervolg geven aan dit onderzoek met een nieuwe opdracht aan TNO om verder onderzoek te doen naar welke gedragsinterventies het meest effectief zijn om gedragsverandering te stimuleren bij het invoeren van de vijf basisprincipes. Met de resultaten van dit onderzoek worden de communicatiemiddelen en tools van het Digital Trust Center verder verbeterd.

De Haagse Hogeschool heeft in opdracht van MKB-Nederland en het Ministerie van Justitie en Veiligheid een verkennende studie verricht om meer zicht te krijgen op de cyber-ketenweerbaarheid in verschillende economische sectoren.[12] De belangrijkste aanbevelingen zijn om actuele informatie over cyberrisico's te delen in bedrijfsketens, en dat bedrijfsketens hun cyberveiligheid moeten vergroten. Vervolgonderzoek ziet op het ontwikkelen van een aantal "gouden regels" om mkb-ondernemingen te helpen de cyberweerbaarheid in de keten te versterken.

Vervolg

Deze brief bevat een aantal concrete acties die recent in gang zijn gezet. Die acties laten zien dat dit kabinet actief aan de slag is met het bevorderen van de cyberweerbaarheid van het mkb. Daarmee is een goede start gemaakt. Maar de aanpak staat niet stil.

[12] www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/expertisecentra/coecs/rapport-cyber-ketenweerbaarheid-digi.pdf

Ook in de nieuwe Nederlandse Cyber Securitystrategie en in het nieuwe Actieprogramma Veilig Ondernemen van het Nationaal Platform Criminaliteitsbeheersing heeft de weerbaarheid van het mkb de aandacht. Op basis van ervaringen en nieuwe inzichten uit onderzoek wordt de aanpak verder ontwikkeld.

De Minister van Justitie en Veiligheid,

D. Yeşilgöz-Zegerius

De Minister van Economische Zaken en Klimaat,

M. Adriaansens

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Bijlage:

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Onderstaand overzicht betreft de campagnes ter bewustwording van online veiligheid, zowel in Nederland als in andere lidstaten van de Europese Unie, zoals toegezegd door de Minister van Justitie en Veiligheid in het Commissiedebat Online Veiligheid en Cybersecurity op 1 december 2021.

Overzicht van campagnes voor bewustwording van online veiligheid in Nederland

Alert Online
Alert Online is een jaarlijks terugkerende bewustwordingsmaand in oktober, de Europese cybersecuritymaand.[13] Alert Online richt zich op het creëren van bewustwording rondom online veiligheid, op het vergroten van kennis over online veiligheid en op het stimuleren van en helpen bij digitaal veilig gedrag bij diverse doelgroepen. Dit wordt gedaan door kennisoverdracht via online kanalen en met een specifiek partnernetwerk van organisaties in Nederland (o.a. bedrijven, maatschappelijke organisaties, (Rijks)overheden en wetenschap). De campagne loopt met partnerbijeenkomsten door het hele jaar heen, maar kent een zwaartepunt in de maand oktober (de Europese cybersecuritymaand), waarin honderden partners bewustwordingsactiviteiten organiseren.

Doe je updates
Eind 2019 is door het Ministerie van Economische Zaken en Klimaat, in nauwe samenwerking met het Ministerie van Justitie en Veiligheid, de campagne «Doe je updates» gestart.[14] Inmiddels zijn er vier rondes van de campagne geweest, waarbij de focus (steeds) meer op het stimuleren van gedragsverandering is komen te liggen. De meest recente ronde was begin 2022. Het doel is om consumenten voor te lichten over de noodzaak van het regelmatig updaten van slimme apparaten en daarvoor handelingsperspectieven te bieden. Deze updates beveiligen de meeste slimme apparaten. Consumenten zijn hier echter beperkt van op de hoogte. Het overbrengen van deze kennis is daarom van belang voor de digitale weerbaarheid van burgers. De campagne is via online kanalen, radiocommercials en muziekdiensten verspreid. In de campagnes van de Ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat wordt verwezen naar www.veiliginternetten.nl en voor het bedrijfsleven naar www.digitaltrustcenter.nl.

Eerst checken dan klikken
In 2019 heeft de campagne 'eerst checken, dan klikken' gedraaid.[15] Dit was een campagne op TV, radio, social media en geprinte media rondom het thema phishing. Het verkrijgen van toegang tot systemen via phishing is een veelgebruikte techniek in het uitvoeren van een grootschaliger digitale aanval, bijvoorbeeld voor de uitvoering van een ransomware-aanval. Daarnaast kan iemand door phishing verleid worden belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens voor systemen of gegevens die voor fraude kunnen worden gebruikt. Phishing gebeurt vaak via e-mails, maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.

Naast de campagne-slogan 'eerst checken, dan klikken' zijn in deze campagne ook andere thema's naar voren gebracht: veilige wachtwoorden, het doen van updates, het maken van back-ups en het gebruiken van virusscanners. Rondom

[13] www.veiliginternetten.nl/alertonline/
[14] www.veiliginternetten.nl/doejeupdates/
[15] www.veiliginternetten.nl/maakhetzeniettemakkelijk/

deze basismaatregelen is op de website www.veiliginternetten.nl meer aandacht geweest in de vorm van video's die het risico van cybercrime schetsen en het handelingsperspectief bieden om dat risico te verkleinen.[16] Om de verspreiding van de campagneboodschap te versterken is een convenant opgericht waar 25 publieke en private partijen aan deelnemen.

Politie - daderpreventie
Gedurende de coronacrisis heeft de politie in april 2020 de campagne "GameChangers" gestart die zich richt op jongeren.[17] Via online uitdagingen en games kunnen jongeren hun digitale vaardigheden testen en ontwikkelen. Zo leren ze cybercrime te herkennen en wordt hen getoond hoe ze hun vaardigheden binnen de wettelijke kaders kunnen inzetten. Met de uitdagingen zijn prijzen te winnen, zoals een politie-ervaring. Wegens succes is de campagne verlengd tot 1 juni en zijn nieuwe uitdagingen toegevoegd.

De in 2019 door de politie uitgevoerde campagne "je bent maar één klik verwijderd van cybercrime" richtte zich specifiek op het voorkomen van daderschap bij jongeren.[18] In het voorjaar van 2020 is door de politie een snelle, toegespitste start gemaakt met het vervolg van deze campagne aangezien jongeren door de coronacrisis veel online zijn.

Specifieke communicatie naar jongeren, senioren, laaggeletterden
De doelgroepen jongeren, senioren en laaggeletterden zijn de afgelopen jaren specifieker benaderd ter preventie van cybercrime en online fraude, onder meer door communicatie via respectievelijk scholieren.com, ouderenbonden, en www.oefenen.nl.

Senioren en veiligheid
Sinds 2020 wordt de campagnemaand "Senioren en Veiligheid" georganiseerd om senioren meer weerbaar te maken.[19] Hiervoor is onder meer voorlichtingsmateriaal over online fraude en cybercrime verspreid en zijn vrijwilligers van ouderenbonden voorgelicht om hierover de juiste informatie te geven aan senioren.

Slachtofferhulp Nederland
In mei 2020 is de campagne "Van oplichting naar opluchting" van Slachtofferhulp Nederland van start gegaan. Deze campagne deelt de verhalen van slachtoffers van *phishing* en andere vormen van online criminaliteit. Slachtoffers worden gestimuleerd te praten over het delict, waarbij zij online steun kunnen vinden bij lotgenoten. Het doel is om schaamte weg te nemen en de impact van slachtofferschap te verkleinen.

[16] www.veiliginternetten.nl/5-tips-basisveiligheid/
[17] publicaties.politie.nl/changeyourgame/
[18] www.politie.nl/nieuws/2019/februari/13/00-9456-jongeren-een-klik-verwijderd-van-cybercrime.html
[19] www.maakhetzeniettemakkelijk.nl/senioren-en-veiligheid

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Overzicht van campagnes voor bewustwording van online veiligheid in de Europese Unie[20]

België
In België hebben de afgelopen jaren meerdere bewustzijnscampagnes plaatsgevonden op de thema's phishing, wachtwoorden, twee-factorauthenticatie en updates. Hierbij wordt een breed netwerk van overheidsdiensten, bedrijven en maatschappelijke organisaties betrokken om de campagneboodschap zo goed mogelijk onder de bevolking te verspreiden.

Duitsland
Landelijke informatie- en bewustzijnscampagne onder het motto #einfachaBSichern (eenvoudig jezelf beschermen), die ingaat op IT-veiligheid voor consumenten. Deze campagne richt zich op het risicobewustzijn van gebruikers van IT-producten en hun vaardigheid om 'competent, autonoom en op lange termijn gericht' met opkomende problemen om te kunnen gaan. In deze campagne wordt de stelling 'offline geen goed idee, online ook niet' gebruikt om onveilige online situaties te vergelijken met een 'offline' situatie waar de onveiligheid sneller duidelijk wordt.

Estland
In Estland zijn in de afgelopen jaren meerdere campagnes georganiseerd rondom dit thema. Vanaf 2017 zijn in opvolgende jaren de onderstaande thema's aan bod gekomen:

- updaten van IoT-apparatuur;
- op lokaal niveau bij scholen, buurthuizen en huisartsen spreken over cyber hygiëne;
- campagne gericht op senioren, met name over veilige wachtwoorden, updates, back-ups, phishing links en online fraude, en om in het algemeen de basisveiligheid te verhogen;
- Veilig thuiswerken tijdens de Covid-19 pandemie
- veilig stemmen, met name bij online stemmen.

Finland
Verschillende campagnes gericht op het algemeen publiek en bedrijven:

- 2018 'Pidempi Parempi': een campagne voor bewustwording over veilige wachtwoorden
- 2018 – 2022: campagne over data- en informatieveiligheid.
- Daderpreventiecampagnes gericht op jongeren, met name om jongeren met IT-vaardigheden bewust te maken dat er ethische en legale manieren van het inzetten van deze vaardigheden zijn.

Frankrijk
Verschillende campagnes zijn georganiseerd rond thema's als veilige wachtwoorden, updates, back-ups en phishing. en ten tijde van de covid-19-pandemie om grootschalige cybercrime en fraude tegen te gaan toen dat thema werd misbruikt om toegang tot mogelijke slachtoffers te krijgen. Doorlopende campagnes worden georganiseerd rond de website www.cybermalveillance.gouv.fr.

[20] Dit overzicht is gebaseerd op de reacties op een uitvraag via het European Union Crime Prevention Network (EUCPN) aan alle EU-lidstaten.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

Luxemburg
Gedurende de afgelopen vijf jaar hebben twee campagnes gelopen: één gericht op online veiligheid van senioren, en één over online pesten. Bij de eerste campagne werden jongeren aangemoedigd om oudere generaties te helpen met het vergroten van hun online veiligheid. Doorlopend wordt de bevolking via de politie op de hoogte gesteld van actuele cybercrime- en online fraudevormen.

Letland
Campagne gericht op zogenaamde '*tech support scam*'[21], middels een brede campagne in samenwerking met ouderenorganisaties, vakbonden, grote werkgevers en apothekersnetwerken. Het doel was om mensen elkaar te laten waarschuwen voor cybercrime en online fraude.

Oostenrijk
Doorlopende communicatie via www.saferinternet.at, een website waar informatie te vinden is over (veilig gebruik van) internet, en veel onderwerpen die met preventie van online criminaliteit te maken hebben. Met name de samenwerking met NGOs op dit vlak blijkt in Oostenrijk effectief.

Polen
Een landelijke campagne in Polen en Tsjechië door samenwerking tussen de twee overheden. Meerdere door de politie georganiseerde lokale campagnes gericht op cybercrime en online fraude, zoals 'let op dreigingen uit cyberspace', en advertenties over online veiligheid in bussen en trams.

Portugal
Jaarlijks in februari rondom de 'Safer Internet Day' vindt er een campagne plaats om bewustwording over online veiligheid te vergroten. In deze campagne wordt voor een nauwe samenwerking met scholen gekozen om jongeren effectief te bereiken.

Roemenië
Meerdere campagnes, gericht op
- Jongeren: zowel slachtofferschap als daderschap. Bekendmaken met de risico's van cybercrime en de risico's van betrokkenheid bij cybercriminaliteit
- Jongeren: campagne gericht op het voorkomen van het worden van geldezel.[22]
- Algemeen publiek: brede campagne over de risico's van cybercrime en online fraude, en over cyber hygiëne, met name het nemen van basismaatregelen.

Zweden
Campagne gericht op senioren onder de titel 'probeer me niet voor de gek te houden'. Middels uitlegvideo's en educatief materiaal wordt bewustzijn vergroot over hoe men zich beter tegen cybercrime en (met name) online fraude kan weren. Dit is een samenwerking tussen de Zweedse politie en seniorenorganisaties.

[21] De 'tech support scam' is een vorm van online criminaliteit waarbij een malafide beller probeert om het slachtoffer *remote-access-tooling* (RAT) te laten installeren onder het mom van 'hulp bij computerproblemen', waarna toegang tot de computer van het slachtoffer kan worden verkregen en criminele handelingen kunnen plaatsvinden, zoals het overmaken van geld naar de rekening van de crimineel.
[22] Een geldezel of *money-mule* is iemand wiens bankrekening en/of pinpas misbruikt wordt voor het wegsluizen van veelal crimineel geld. Dit betreft vaak (kwetsbare) jongeren.

Vergelijking tussen campagnes in Nederland en de rest van Europese Unie

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
6 juli 2022

Ons kenmerk
4062028

In vergelijking met andere landen is het volgende op te merken over de campagnes die in Nederland zijn georganiseerd.

De genoemde thema's lijken veel op elkaar
De door lidstaten genoemde thema's gaan veelal over het nemen van basismaatregelen van cybersecurity en het herkennen en bewust zijn van risico's van cybercrime en online fraude. Veel campagnes zijn er op gericht door informatieverstrekking burgers bewust te maken van online risico's en wat zij hiertegen kunnen doen. Dit komt in grote lijnen overeen met de campagnes die in Nederland georganiseerd zijn.

De genoemde doelgroepen komen overeen
De landen die aandacht hebben besteed aan identificatie van verschillende doelgroepen richten hun communicatie veelal op het algemene publiek, jongeren en senioren. Andere segmenteringen dan deze worden bij lidstaten niet genoemd. Ook dit komt grotendeels overeen met de Nederlandse aanpak, waar naast het algemene publiek ook jongeren, senioren, laaggeletterden en mkb-bedrijven als specifieke doelgroep gelden.

Daderpreventie komt in andere lidstaten minder voor
De door lidstaten genoemde campagnes, met uitzondering van Roemenië en Finland, zijn met name te categoriseren als slachtofferpreventie: zorgen dat mensen minder risico lopen om slachtoffer te worden. In Nederland en de bovengenoemde landen is er ook aandacht voor daderpreventie: het zorgen dat mensen (met name jongeren) niet het verkeerde pad opgaan en hun IT-vaardigheden ten positieve inzetten.