



**Kaasstad
Kapitaal**



INFORMATIE OVER DIGITALE WEERBAARHEID | POLITIE

DIGITALE WEERBAARHEID

Deze informatiebrief dient als een naslagwerk waarin de voorbeelden worden beschreven die ik heb besproken heb tijdens mijn presentatie voor Kaasstad Kapitaal.

Beoordeling van digitale weerbaarheid bij investeringen in ICT-ondernemingen

Bij het overwegen van een investering in een ICT-bedrijf of een organisatie die digitale diensten levert, is het van belang niet alleen te kijken naar de technologische innovatie of marktpositie, maar ook naar de mate van digitale weerbaarheid. Cybersecurity en operationele continuïteit zijn directe indicatoren voor risicobeheersing en bedrijfsstabiliteit. Onderstaande aandachtspunten kunnen worden gebruikt als onderdeel van de due diligence-procedure om de volwassenheid van de onderneming op het gebied van informatiebeveiliging te beoordelen.

Tip 1 – Inzicht in het cybersecuritybeleid

Tijdens de beoordeling van een onderneming is het essentieel om inzicht te verkrijgen in de wijze waarop dataveiligheid is ingericht:

- Controleer of er minimaal gebruik wordt gemaakt van meervoudige authenticatie (2FA),
- of er een aantoonbaar effectieve back-upstrategie aanwezig is en
- of segmentatie van data op servers wordt toegepast. Deze maatregelen verkleinen het risico op dataverlies, ongeautoriseerde toegang en bedrijfsstilstand.

Tip 2 – Beveiliging en beheer van klantaccounts

Voor ondernemingen met een groot aantal gebruikers- of klantaccounts is het raadzaam te onderzoeken welke maatregelen worden genomen om accountveiligheid te waarborgen. Onvoldoende bescherming kan leiden tot accountovernames (account takeovers) en directe financiële schade. Beoordeel ook of de onderneming haar klanten identificeert en verifieert conform het [Know Your Customer](#)-principe, om fraude en misbruik te kunnen voorkomen. Tijdens mijn presentatie heb ik de interventie [No More Leaks](#) uitgelegd, waarbij accounts gratis worden gecontroleerd of het bijbehorende wachtwoord niet ergens is gelekt op het internet.

Tip 3 – Beschikbaarheid van een digitaal noodpakket

Onderzoek of de onderneming beschikt over een actueel en getest digitaal noodpakket. Dit omvat onder meer vastgelegde procedures voor het geval de digitale infrastructuur geheel uitvalt of niet bereikbaar is. Controleer of cruciale bedrijfsinformatie, contactgegevens en herstelinstructies ook buiten digitale systemen beschikbaar zijn. Een dergelijk noodplan is van belang voor de continuïteit van de bedrijfsvoering bij cyberincidenten of technische storingen.

Naast de drie tips die ik gegeven heb in mijn presentatie, voeg ik hieronder nog nuttige websites toe waar veel informatie te halen is over digitale weerbaarheid en veiligheid.

Check je Hack

De politie is actief in het bestrijden van cybercriminaliteit. In datasets die in beslag genomen zijn, zitten soms privégegevens van burgers die door criminelen zijn misbruikt. Als het mogelijk is, maakt de politie datasets doorzoekbaar. Met de checkfunctie kunt u controleren of uw e-mailadres in een dataset voorkomt. Klik [hier](#) voor de website.

Digi Hulp lijn

Heb je vragen over je computer, e-reader, mobiel of het internet? Kom je er digitaal niet helemaal uit? Onze ervaren medewerkers helpen je graag. Bel 0800-1508 (gratis) voor meer informatie. Digi Hulplijn is van maandag t/m vrijdag tussen 08.00 – 22.00 uur en zaterdag tussen 09.00 - 18.00 uur bereikbaar. Klik [hier](#) voor de website.

Dubbelzoveilig.nl

'Dubbel beveiligd is dubbel zo veilig' is een campagne die mensen helpt om hun e-mail- en socialmedia-accounts beter te beschermen door op een gemakkelijke wijze uit te leggen hoe e-mail voorzien kan worden van tweestapsverificatie, ook wel 2FA genoemd. Klik [hier](#) voor de website.

Fraudehelpdesk.nl

De Fraudehelpdesk wil zoveel mogelijk voorkomen dat de Nederlandse bevolking slachtoffer wordt van fraude. De Fraudehelpdesk biedt fraudeslachtoffers een helpende hand door hen te adviseren en naar de juiste instantie te verwijzen. Daarnaast proberen we slachtofferschap te voorkomen door burgers en bedrijven bewust te maken van fraude-risico's en praktische tips te geven over hoe zij die risico's kunnen beperken. Klik [hier](#) voor de website.

Hack Helpdesk

Veel ondernemers zijn zich (vaak) onvoldoende bewust van de risico's op een cyberincident en de impact ervan op de bedrijfs-continuïteit. Als het je toch overkomt, ben je onvoldoende voorbereid en weet je niet hoe je moet handelen. Bovendien, met enkele maatregelen kun je het risico dat je slachtoffer wordt al flink verkleinen. Speciaal voor ondernemers is er nu de Hackhelpdesk voor gratis eerste hulp bij cybercrime. Klik [hier](#) voor de website.

Offlimits

Heb jij of iemand in je omgeving, te maken met online grensoverschrijdend gedrag? Of ben jij online iemands grenzen overgegaan? Offlimits is er voor je. Zij bieden praktische hulp, geven persoonlijk advies en tips. Je kunt gratis en anoniem met hen chatten, mailen en bellen. Klik [hier](#) voor de website.

Internetsporen.nl

Het doel van de site internetsporen.nl is om gedupeerden/slachtoffers van internet gerelateerde delicten op eenvoudige wijze uit te leggen hoe zij sporen van het internet kunnen veiligstellen. Maar deze gegevens zijn vaak vluchtig en er moet dus snel gehandeld worden. Om deze gegevens toch te achterhalen, hebben wij op onze site een aantal pagina's gemaakt met tips om de digitale sporen veilig te stellen. Klik [hier](#) voor de website.

Laat je niet interneppen

Zo'n 2,2 miljoen mensen kregen in 2023 te maken met online criminaliteit. Door de slimme manieren van online misleiding kan iedereen in de val trappen. Interneppers ofwel internetcriminelen doen zich voor als iemand anders om jouw gegevens te stelen of om je op te lichten via mail, sms of WhatsApp. Het bericht of de mail komt op het eerste gezicht van iemand die je vertrouwt. Zoals een vriend, een medewerker van een winkel met een mooie aanbieding of zelfs van je bank. Als ze voor je staan trap je er misschien niet zo snel in, maar online is dat een stuk lastiger. De beste manier om hiermee om te gaan? De afzender checken en als je het niet vertrouwt of twijfelt: wegstappen. Klik [hier](#) voor de website.

Slachtofferhulp

Je kunt op verschillende manieren contact met Slachtofferhulp opnemen: per [e-mail](#), [chat](#), telefoon (0900 -0101 of 088 - 746 00 00) en social media. We doen ons best om je vraag meteen te beantwoorden, zodat je snel weer verder kunt. Is er meer nodig om je zo goed mogelijk te helpen? Of wil je liever een 1 op 1 gesprek? Dan maken we een afspraak met een van onze medewerkers. Bij je thuis of op een kantoor van Slachtofferhulp in je regio. Klik [hier](#) voor de website.

Slachtofferwijzer

Op Slachtofferwijzer vind je informatie over slachtofferschap en hulpverlening. Ook is Slachtofferwijzer een plek waar je herkenning vindt: je kunt je herkennen in de verhalen van anderen. En waar je erkenning vindt: door de informatie en het lezen van de verhalen van anderen weet je dat jij niet gek bent. Dat het niet jouw schuld is. Dat je je nergens voor hoeft te schamen en dat je niet alleen bent. Daarnaast heb je via Slachtofferwijzer makkelijk toegang tot de hulp die bij jou past. Klik [hier](#) voor de website.

Stop Heling

De politie, gemeenten en rijksoverheid werken actief aan het bestrijden van heling. Het verkopen van gestolen spullen (oftewel heling) levert geld op. Als dat verkopen niet meer lukt, zijn inbraak en diefstal voor de dief minder aantrekkelijk. En zijn we allemaal veiliger. Klik [hier](#) voor de website.

Veilig Bankieren

De website www.veiligbankieren.nl van de Nederlandse Vereniging van Banken is het belangrijkste gezamenlijke platform dat de banken in Nederland gebruiken om hun klanten voor te lichten op het gebied van fraude en veiligheid en de manier waarop zij daaraan een bijdrage kunnen leveren. Veilig bankieren is een zaak van ons allemaal. Klik [hier](#) voor de website.

Veiliginternetten.nl

Op Veiliginternetten.nl kunnen mensen terecht voor tips, tricks en praktische stap-voor-stap-uitleg over hoe zij veilig kunnen omgaan met hun online privacy, maar ook hoe zij veilig gebruik kunnen maken van wifi, wat ze kunnen doen en laten op sociale media, en hoe zij hun kinderen helpen veilig online te zijn. De doelgroep van veiliginternetten.nl is de burger, de ZZP-er, de consument en overheden. Klik [hier](#) voor de website.

Zo werkt fraude

Deze website is een initiatief van de Nederlandse Vereniging van Banken (NVB) en de gezamenlijke banken. De website hoort bij de campagne 'Frauderen, zo werkt het!' dat door de NVB is ontwikkeld om Nederlanders bewust te maken van hoe fraude werkt en hoe je je ertegen kunt beschermen. Klik [hier](#) voor de website.

No More Leaks

Nieuwsberichten over grote datalekken verschijnen steeds vaker. Het merendeel van de slachtoffers is zich niet bewust van het feit dat hun inloggegevens door cybercriminelen verhandeld worden. [No More Leaks](#) voorkomt misbruik van deze gegevens.

Digitaal weerbaarder worden

Algemeen wordt er aangenomen dat voornamelijk ouderen slachtoffer worden van internet gerelateerde misdrijven maar het blijkt dat jongeren hiervan ook steeds vaker slachtoffer worden. Jongeren kunnen ontzettend goed "klikken en klakken" maar weten helaas niet wat er "onder de schermpjes" gebeurt. Men leeft in een digitale bubbel die niet altijd de echte feiten laat zien. Hieronder een aantal sites waar je geleerd wordt hoe het internet werkt, hoe je digitaal weerbaarder wordt en veiliger gebruik kunt maken van het internet.

Hackshield

HackShield is een gratis online game voor kinderen van 8 tot 12 jaar, waarin ze op een speelse manier leren hoe ze zichzelf én hun omgeving kunnen beschermen tegen cybercriminaliteit en andere online gevaren. Ze worden daarbij opgeleid tot Cyber Agents, die onder meer leren over onderwerpen als internetgevaaren, phishing, nepnieuws en online pesten. Dus mocht u (klein)kinderen, neefjes of nichtjes in deze leeftijd, attendeer ze op [HackShield](#), want ik weet zeker dat zij dit erg leuk vinden om te spelen en dat zij een stuk wijzer zullen worden!

Digitale-Weerbaarheid.nl

De site [digitale-weerbaarheid.nl](#) heeft als doel mensen te helpen veilig, bewust en weerbaar gebruik te maken van internet en digitale middelen, met praktische informatie, tips en antwoorden op vragen over online veiligheid en privacy. Daarnaast zijn er meerdere gratis cursussen beschikbaar om digitaal weerbaarder te worden, zodat je veiliger gebruik kunt maken van het internet.

Mochten er nog vragen zijn? Schroom dan niet om contact met mij op te nemen via onderstaande gegevens want ...

"Voorkomen is nog altijd beter dan genezen"



Website:
www.politie.nl

E-mailadres:
barend.frans@politie.nl

LinkedIn:
[Barend Frans](#)

