MENUKAART

Maatregelen datalek

Eind september werd bekend dat hackers de contactgegevens van alle politiemedewerkers buit hadden gemaakt. Na onderzoek lieten de inlichtingendiensten de politie weten dat zeer waarschijnlijk een statelijke actor verantwoordelijk is voor het cyberincident. Met andere woorden: we gaan ervan uit dat een ander land of daders in opdracht van een ander land verantwoordelijk is. Vanzelfsprekend zijn onmiddellijk forse beveiligingsmaatregelen ingezet tegen deze aanval en we monitoren alles continu.

Mogelijk vraag je je nu af wat je zelf nog kunt doen. In deze menukaart kun je lezen wat er allemaal mogelijk is om jezelf en de organisatie weerbaarder te maken.

Klik op één van de buttons voor meer informatie

Digitaal

> Terug naar overzicht

Wat was er al van mij online bekend?

Er is een aantal zoekslagen die je kunt maken

Hoe weet ik of er in de toekomst iets van mij online komt?

Ik heb mezelf opgezocht online, maar kan niks vinden. Hoe weet ik of er in de toekomst toch iets van mij online komt?

Social Media

Jouw eigen gebruik of dat van jouw naasten

Communicatiemiddelen

Een vertrouwelijk gesprek via Teams of telefoon?

Outlook

Denk na over naamgeving van bestaande en nieuwe distributielijsten.

DIGITAAL

Wat was er al van mij online bekend?

> Terug naar overzicht

- Zoek in (bijvoorbeeld) Google eens naar jezelf. Vul voorletters, roepnaam, achternaam, adres of woonplaats in van jezelf. Eventueel kun je dit ook doen voor je partner of personen uit jouw gezin/familie/naasten.

  Check dit eenmalig en doelgericht, want hoe vaker je zoekt hoe vindbaarder je in een zoekmachine wordt.

- Zoek op diezelfde manier ook eens op je (werk)telefoonnummer.

- Verder is het slim om via de website haveibeenpwned.com te kijken of jouw privé e-mailadres en telefoonnummer al bekend is. Het team Informatie Beveiliging monitort de website (haveibeenpowned.com) op het voorkomen @politie.nl gegevens.

  Let op, doe dit niet met politiegegevens zoals jouw dienst e-mail of telefoonnummer en denk altijd na bij wat je naar externe websites stuurt. De website is een gratis dienst, wat risico's met zich mee kán brengen. Ons eigen Security Operations Centre (SOC) monitort op de dienstgegevens en zal contact opnemen indien nodig.

- Kijk ook eens op Checkjehack.nl

DIGITAAL

Hoe weet ik of er in de toekomst iets van mij online komt?

> Terug naar overzicht

Misschien komt er nu niets naar voren bij het online zoeken. Maar mocht jouw privé e-mailadres, naam of wachtwoord in de toekomst ergens opduiken, dan wil je dat wellicht wel weten. Dan kun je het volgende doen:

- Via haveibeenpwned.com/NotifyMe kun je je privé e-mailadres invullen. Je krijgt dan een e-mail op het moment dat jouw mailadres voorkomt in de database van HaveIBeenPwned. Deze service is gratis en vereist geen account.

DIGITAAL

Social Media

> Terug naar overzicht

Hoe gebruik je jouw social media of wat adviseer je je naasten hierover?

- Wees voorzichtig met het delen van informatie over je werk en werklocatie op sociale media.
- Gebruik een besloten account, zodat alleen mensen met jouw toestemming kunnen meekijken.
- Deel nooit operationele informatie op sociale media.
- Bespreek ook met jouw directe privé-omgeving wat zij op sociale media zetten (over jou).
- Ga niet in op werk gerelateerde discussies op sociale media.
- Maak geen verbinding met Wifi als dit niet nodig is. Zeker openbare Wifi-netwerken zijn onveilig.
- Zet je locatievoorzieningen alleen aan voor apps waarvoor het nodig is.
- Scherm je profielen af, voor tips zie: veiliginternetten.nl
- Loop je privacy instellingen regelmatig door.
- Wees je bewust van het sociale mediagebruik van mensen in je directe privé-omgeving. Denk bijvoorbeeld na over de (volledige) namen die jij en je gezinsleden gebruiken op sociale media.

DIGITAAL

Communicatiemiddelen

Een vertrouwelijk gesprek via teams of telefoon?

- Spreek een codewoord af wanneer je met elkaar contact hebt, zegt de beller het woord en de persoon die wordt gebeld antwoordt met een afgesproken antwoord. Bijvoorbeeld: “Hallo Krant”, “Hey Brievenbus”.
- Als je niet altijd op deze manier een gesprek wilt starten, maar tijdens het gesprek denkt dat het wel een beetje een vreemd gesprek is, vraag dan om het codewoord, bv “appelboom”. (Uiteraard vrij voor eigen interpretatie).
- Als je dit binnen je team afspreekt en dit niet deelt met anderen, weet je op die manier in elk geval dat je altijd met een (vertrouwd) persoon spreekt.
- Wees alert in (video)telefoongesprekken wanneer er een trage verbinding is, er niet snel op jouw vraag wordt gereageerd of iemand echt afwijkend gedrag vertoont. Verbreek de verbinding en zoek eventueel via een andere manier opnieuw contact met elkaar.

Scheiden van werk/ privé / ‘vuile’ telefoons

- Denk na wanneer je welke telefoon meeneemt en waar je deze voor gebruikt

Telefoonnummers vervangen in het geval van zorgen of dreiging

- Richting de NSGBO is deze behoefte geuit, het verzoek om een nieuwe simkaart kan gedaan worden bij de eenheidsleiding. Na akkoord kan dit aangevraagd worden gedaan via *BlueShop- ICT-middelen aanvragen*.
- 5.1.2.i .

Let op: Op dit moment wordt er gewerkt aan de opschaling van dit proces bij de dienst IV

DIGITAAL

Outlook

> Terug naar overzicht

- **Denk na over naamgeving van bestaande en nieuwe distributielijsten**
  Momenteel loopt de NSGBO uit met dienst IV om te kijken of dit als dienst kan worden aangeboden

- **Zorg voor minimale informatie in het Outlook-visitekaartje**
  De opdracht is aan de Dienst IV gegeven om dit automatisch voor iedereen te doen.
  Zelf alvast je foto of andere zelf toegevoegde informatie verwijderen?
  Kijk in de lijst Vragen en Antwoorden op BlueThema Datalek

Ik word benaderd of gevolgd

> Terug naar overzicht

Hoe herken ik dit? (fysiek)

Klik voor meer informatie

Hoe herken ik dit? (digitaal)

Klik voor meer informatie

IK WORD BENADERD OF GEVOLGD

Hoe herken ik dit? (fysiek)

> Terug naar overzicht

- Personen begeven zich gedurende langere periode in de omgeving van de locatie.
- Personen maken foto’s van medewerkers, het pand, aanrijroutes, vluchtwegen en beveiligingsmaatregelen.
- Dezelfde kentekens worden gedurende langere periode gesignaleerd in de omgeving.
- Collega’s worden gevolgd naar de parkeerplaats, het OV, thuis, etc.
- Personen houden zich zonder duidelijke reden op (bv. hangen bij de ingang van het bureau).
- Personen kijken weg op het moment dat oogcontact wordt gezocht.
- Personen maken omtrekkende bewegingen zodra zich (herkenbare) politiecollega’s in de omgeving bevinden.
- Personen geconstateerd rondom ingang of nooduitgang.
- Let tijdens woon-werkverkeer op of anderen belangstelling hebben voor je reisbewegingen.

Collega’s die afgeschermd werken, hebben een eigen handelingskader gekregen.

IK WORD BENADERD OF GEVOLGD

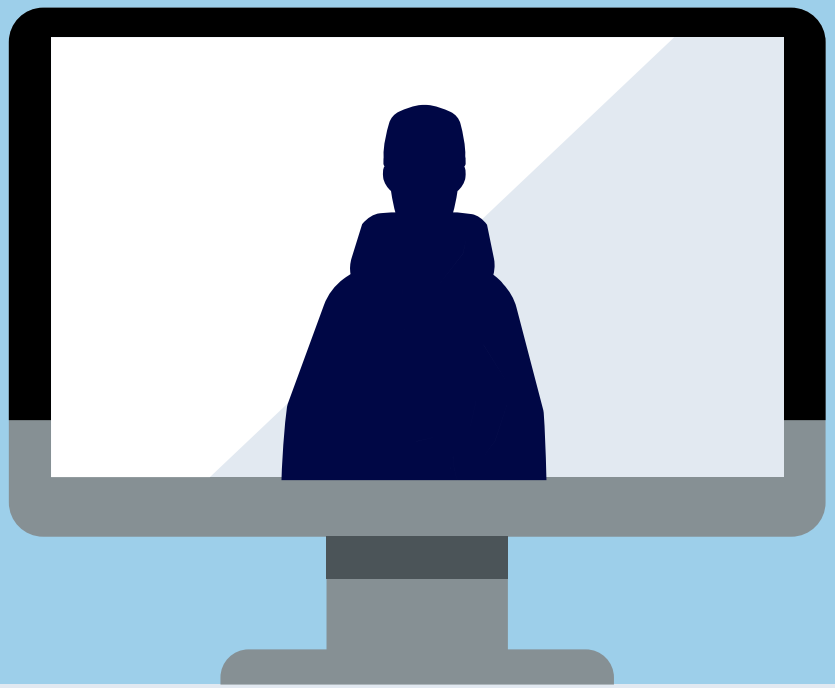
Hoe herken ik dit? (digitaal)

> Terug naar overzicht

Belt iemand jou op van buiten jouw team met een bijzonder verzoek of een korte vraag en vertrouw je het niet?

- Bel diegene dan terug op het nummer dat al bij jou bekend is, of leg contact via een ander medium. Bijvoorbeeld: je word gebeld, en je stuurt je antwoord per mail, of je wordt gemaild en dan bel je terug.

- Check ook online op de website van de aivd



Melden van incidenten

> Terug naar overzicht

Het meldpunt wordt steeds gevoed met de laatste inzichten

Acuut? Bel OVD.
Bij gevaar 112

Niet acuut? Bel je leidinggevende.
Vanuit de NSGBO wordt gezorgd dat zij weten wat ze moeten doen.

Achtergrondinformatie

> Terug naar overzicht

Doe-het-zelf tips over online veiligheid en weerbaarheid

Download Deel 1
Download Deel 2
Download artikel social engineering

Video statelijke dreiging: de politiemedewerker als doelwit

Bekijk

E-learning Altijd Alert Goud is beschikbaar in het Leermiddelenportaal.

Meer informatie

Handelingskader statelijke dreiging

Download

*alleen PC/Citrix.

Op dienstreis of vakantie naar het buitenland?

Handige tips

Wat is hacken eigenlijk?

Meer informatie