# PI Nieuws maart 2022

## Diefstal door hack salarisverwerker

Een cybercrimineel is er in geslaagd om maar liefst 5500 accounts te kraken bij een landelijke salarisverwerker in de VS. Hij maakte gebruik van gestolen emailadressen en wachtwoorden en probeerde die gewoon uit. Eenmaal ingelogd op het account paste hij het bankrekeningnummer aan naar die van hem. Op die manier wist hij maar liefst 800.000 dollar over te 'verdienen'.

Uit deze case kun je een aantal beveiligingslessen leren. In de eerste plaats dat je nooit een wachtwoord moet hergebruiken. Gebruik voor elk account een verschillend en moeilijk te raden wachtwoord. Ten tweede is het bij dit soort accounts met veel gevoelige gegevens belangrijk dat er een tweede factor wordt gebruikt. Hiermee maak je het kwaadwillenden al een stuk lastiger om binnen te komen. In de derde plaats verbaast het me dat er geen controle plaats vond op het wijzigen van een bankrekeningnummer.

Zie ook: Diefstal door het hacken van accounts salarisverwerker

## Website van de maand

Cybersecurity professionals gebruiken veel – bij voorkeur Engelstalig – vakjargon. Om de brug tussen gebruikers en deze professionals te slaan is er door Cyber Veilig Nederland een cybersecurity woordenboek opgesteld. Eind vorig jaar is er weer een nieuwe editie uitgekomen. Een handige woordenlijst die ik er regelmatig bij pak. Nu weet ik ook wat whaling of Xaas is! En voor de liefhebbers: om plagiaat te voorkomen staat er ook een fopwoord in.

Zie: https://cyberveilignederland.nl/woordenboek

## Zorgplicht ICT dienstverleners inzake security

Een ICT dienstverlener die ICT diensten aan derden levert doet er verstandig afspraken te maken over de beveiliging en kan zich niet verschuilen achter de opmerking dat de klant er niet om gevraagd heeft en/of dat hierover geen afspraken zijn gemaakt.

Volgens de rechter is het moeilijk voorstelbaar dat ICT dienstverleners een totaalpakket ICT leveren als daar ook geen beveiligingsmaatregelen onderdeel van zijn. Zonder het gesprek over beveiliging aan te gaan, kan de klant er dus op vertrouwen dat de ICT-dienstverlener dit als onderdeel van de koop- en dienstverleningsovereenkomst regelt. Verder geeft de rechter ook nog aan dat het geen verschil maakt of de hosting door de ICT dienstverlener zelf wordt gedaan of dat deze wordt uitbesteed.

Meer lezen: zorgplicht ICT dienstverlener

## Boete DPG Media

Onder de AVG hebben betrokkenen recht op inzage of wissing van hun persoonsgegevens die worden verwerkt. Om deze inzage af te kunnen handelen moeten bedrijven natuurlijk wel zeker weten dat degene die dit verzoek indient ook echt de betrokkene is. Daarom zal er altijd iets van identificatie plaatsvinden. Waar je wel op moeten letten is dat je hierbij niet onevenredig veel persoonsgegevens verwerkt (dataminimalisatie).

Recent heeft de toezichthouder DPG Media een boete van 525.000 euro opgelegd omdat ze in het kader van de identificatie betrokkenen vroeg een ID bewijs te uploaden. Dit is volgende de toezichthouder meestal een te zwaar middel omdat er op een ID-bewijs heel veel persoonsgegevens staan. Als je dit al doet moet je betrokkenen er in ieder geval op wijzen om bepaalde gegevens te blurren. Maar beter is het te kijken naar alternatieven waarbij er zoveel mogelijk identificatie plaatsvindt aan de hand van persoonsgegevens die al verwerkt worden. Bijvoorbeeld door deze identificatie te laten plaatsvinden in een persoonlijke accountomgeving. En als verzoekers die niet hebben door een identificatie aan de hand van klantnummers in combinatie met een naam, adres en/of emailadres van een verzoeker.

De toezichthouder wijst verder op dat je nooit zeker weet of de verstrekte kopie authentiek is en dat in zijn algemeenheid geldt dat de verwerking van ID-bewijzen een groot risico met zich mee brengt voor betrokkenen.

Meer lezen: Boete DPG Media

## Stop device fingerprinting

Onder druk van privacy activisten en de politiek gaan meer en meer sites er toe over om het gebruik van cookies beter in te regelen bijvoorbeeld door deze niet meer te gebruiken of - als ze dat wel doen - daar eerlijk en duidelijk toestemming voor te vragen. Maar er zijn nog genoeg websites die hun best doen om onze gegevens te verkopen of te gebruiken om ons te volgen of advertenties aan te bieden. Zo blijkt uit een onderzoek van de consumentenbond dat meer dan 1/3$^{e}$ van de websites gebruik maakt van zogenaamde fingerprints. Meestal zelfs voordat je een cookie OK scherm krijgt te zien.

“Device fingerprinting” is een techniek die gebruikmaakt van het feit dat computers altijd van elkaar verschillen. Denk aan verschillen in besturingssysteem, browserversie, schermresolutie en nog veel meer gegevens. Met die unieke combinatie kan een bezoeker herkend worden.

Wil je dit verhinderen maak dan gebruik van een privacyvriendelijke browser als Mozilla Firefox. Google Chrome beschermt je niet. Maar je kunt wel een extensie installeren om deze beveiliging toe te voegen. Bijvoorbeeld CanvasFingerprintBlock.

Lees meer: Fingerprinting