Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Help! Mijn gegevens zijn op internet gelekt

Hoe beperk ik de schade?

Factsheet FS-2011-05
versie 1.3 | 7 oktober 2014

In de media is regelmatig te lezen dat organisaties of diensten zijn gehackt en dat daarbij vertrouwelijke (klant)informatie is buitgemaakt. Die informatie wordt vervolgens vaak online gepubliceerd. Een voorbeeld uit juni 2012 is het lekken van wachtwoorden van gebruikers van LinkedIn.

Zodra hackers de buitgemaakte informatie publiek maken, kan iedereen misbruik maken van deze gegevens. Als uw (persoons)gegevens ertussen zitten, kan dit ernstige gevolgen hebben voor u, uw omgeving en uw werkgever.

In dit factsheet geven wij aan wat de gevolgen kunnen zijn als uw gegevens (zoals e-mailadres, creditcardnummer, gebruikersnaam en wachtwoord) gelekt zijn en op internet gepubliceerd worden. Ook geven we tips wat u kunt doen om de gevolgen/schade hiervan te beperken.

De belangrijkste feiten

- Kwaadwillenden zetten informatie online die zij hebben buitgemaakt, bijvoorbeeld op Pastebin.com. Veel van deze datalekken bevatten persoonsgegevens, waaronder inloggegevens.
- Als buitgemaakte informatie op internet gepubliceerd wordt, is misbruik van deze gegevens een reëel risico.
- Wanneer u hetzelfde e-mailadres, gebruikersnaam en wachtwoord gebruikt voor meerdere toepassingen (privé en zakelijk), lopen ook deze toepassingen en de erin opgeslagen gegevens risico.
- Als uw gegevens mogelijk gelekt zijn, kunt u het beste direct al uw wachtwoorden vervangen die mogelijk gelekt zijn, beheeromgevingen in de gaten houden en eventueel uw werkgever informeren.
- Door verschillende gebruikersnamen en wachtwoorden voor verschillende toepassingen te gebruiken, kunt u de schade van een datalek beperken voor andere dan de gehackte toepassingen.

Wat is er aan de hand?

De laatste jaren vormen datalekken een groeiende dreiging voor organisaties en personen. Datalekken kunnen op verschillende manieren ontstaan (zie kader op de volgende pagina). Steeds meer datalekken ontstaan door het buitmaken van gegevens bij het hacken van websites en databases. Deze gegevens worden dan bijvoorbeeld op internet gepubliceerd. Deze handelswijze biedt geen direct geldelijk gewin voor de aanvaller. Deze datalekken zijn dan ook voornamelijk het gevolg van aanvallen door hacktivisten (aanvallers die handelen vanuit activistische motieven). Bekende voorbeelden van groepen hacktivisten zijn Anonymous en Lulzsec. Hun doel lijkt te zijn om veel media-aandacht voor hun handelen te genereren. Door vaak en veel gegevens te publiceren lukt hen dit regelmatig.

Het is maar de vraag of de recente media-aandacht voor datalekken duidt op een toename van het aantal aanvallen. Daarvoor ontbreekt het aan een volledig beeld van hoeveel datalekken plaatsvinden. Dit komt doordat bij een gerichte aanval zowel de aanvaller als de getroffen organisatie veelal buiten de publiciteit willen blijven. Dit is een belangrijk verschil met hacktivistisch gemotiveerde

aanvallen. Voor een reeks voorbeelden van datalekken in Nederland, kunt u terecht op de website van Bits of Freedom dat tot begin 2013 een overzicht bijhield van Nederlandse datalekken[1].

Naast alle publiciteit hebben datalekken ook gevolgen voor u als gebruiker. Onlinediensten en websites slaan uw gegevens op, maar beveiligen hun systemen soms onvoldoende. Aanvallers maken misbruik van de zwakke beveiliging om binnen te dringen en bemachtigen zo de opgeslagen gegevens. Vervolgens kunnen ze met deze gegevens doen wat ze willen: sommige aanvallers maken de gegevens beschikbaar voor iedereen op internet. Dit is ongewenst en zorgt ervoor dat u risico loopt. Bij dit type datalek zijn vaak de volgende gegevens online terug te vinden:

1. e-mailadressen;
2. gebruikersnamen;
3. wachtwoorden (eventueel versleuteld);
4. NAW-gegevens;
5. burgerservicenummer;
6. creditcardnummers.

Wat kan mij overkomen?

De aanvaller die de gegevens in eerste instantie heeft buitgemaakt kan deze voor allerlei doeleinden misbruiken. Als uw gegevens ook nog gepubliceerd zijn, kunnen ook anderen deze gebruiken om in te loggen op alle plaatsen waar u deze inloggegevens gebruikte. Daarmee kunnen zij uw inloggegevens en in het verlengde daarvan ook uw online-identiteit misbruiken. Dit kan hen in staat stellen om namens u e-mail te versturen of financiële transacties uit te voeren – al zijn er in dit laatste geval vaak aanvullende beveiligingsmaatregelen getroffen door uw bank. Daarnaast krijgen zij ook inzage in de gegevens die u gebruikt heeft om zich in te schrijven. Deze kennis kan dienen als opstap naar vervolgaanvallen.

Manieren waarop datalekken ontstaan

- *Misbruik van kwetsbaarheid in database of website*
  Het misbruiken van een kwetsbaarheid in een database of website om zonder toestemming toegang te krijgen tot de opgeslagen informatie.
- *Verlies en/of verwaarlozing van data*
  Voorbeelden hiervan zijn het verlies van informatiedragers (datatapes, USB-sticks, etc.) en het (onbewust) op straat zetten of weggooien van data zonder deze onleesbaar te maken.
- *Fysieke diefstal van apparatuur*
  Hierbij is het doelwit bijvoorbeeld een laptop of smartphone, waarbij opgeslagen gegevens (vaak als bijvangst) in handen komen van de dief.
- *Gerichte aanval*
  Eveneens inbreken op een website of database, maar dan met het doel de verkregen informatie te gaan misbruiken voor bijvoorbeeld spionage, identiteitsdiefstal of chantage.

[1] Bits of Freedom, Zwartboek Datalekken. https://www.bof.nl/category/zwartboek-datalekken/

Gebruik van uw zakelijke e-mailadres voor privédoeleinden

- Als u een zakelijk e-mailadres gebruikt voor privédoeleinden zoals een datingsite, webwinkel of sociale media, kan dit ongewenste gevolgen hebben.
- Als zo'n website met succes wordt aangevallen, kunnen kwaadwillenden afleiden waar u werkt. Zo kunnen zij proberen om met het e-mailadres en het gelekte wachtwoord toegang te krijgen tot uw werkomgeving.
- Als uw wachtwoorden voor diensten voor privégebruik gelijk zijn aan het wachtwoord voor uw werk, kunnen kwaadwillenden eenvoudig inloggen en toegang krijgen tot (gevoelige) informatie van uzelf en uw werkgever, of dit misbruiken om gevoelige informatie van anderen te krijgen.

Wanneer uitgelekte gegevens uw zakelijke e-mailadres bevatten, kan dit extra gevolgen hebben. Dit geldt ook als het gaat om diensten waarbij u uw zakelijk e-mailadres gebruikt voor privédoeleinden (zie kader).

Een ander mogelijk gevolg van een datalek is een toename van spam omdat uw e-mailadres openbaar is geworden en daardoor toegankelijk voor aanvallers. Deze spam en andere ongewenste e-mails kunnen ook gerichter zijn dan voorheen, omdat het duidelijk is op welke website u geregistreerd bent.

Hoe kom ik erachter dat mijn gegevens gelekt zijn?

U kunt er op verschillende manieren achter komen dat uw gegevens gelekt zijn. Door de huidige trend om buitgemaakte en/of gelekte gegevens te publiceren kunt u online uw gegevens aantreffen. Hackers publiceren de gegevens echter op veel verschillende plaatsen waardoor het moeilijk is dit te monitoren. U kunt deze vinden door hier zelf op te monitoren[2] of door gebruik te maken van één van de diverse betaalde of onbetaalde diensten[3].

Een andere manier is het volgen van berichtgeving in de media waarin het datalek bekendgemaakt wordt. Deze worden ook bijgehouden en geregistreerd door bepaalde instanties, zoals in het verleden door Bits of Freedom. Als de getroffen organisatie zelf op de hoogte is, kunnen zij u ook informeren. Dit is echter in Nederland nog niet verplicht[4]. Hier kunt u dus als klant nu nog niet op rekenen.

[2] Door bijvoorbeeld gebruik te maken van Google Alerts

[3] Let er op dat u aan deze diensten alleen de hoogste noodzakelijke informatie overhandigt; geef dus nooit uw wachtwoord aan derden.

[4] Het wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens in verband met de invoering van een meldplicht voor datalekken is op dit moment in behandeling bij de Tweede Kamer.

Wat kan ik doen om de gevolgen van een lek in de toekomst te verkleinen?

1. *Gebruik zakelijke e-mailadressen niet voor privédoeleinden (en omgekeerd)*. Zo houdt u deze twee informatiestromen gescheiden en mogelijke gevolgen voor uzelf en uw werkgever beperkt.
2. *Gebruik verschillende e-mailadressen voor verschillende categorieën diensten voor privégebruik*. Hierbij kunt u bijvoorbeeld denken aan een e-mailadres dat u uitsluitend gebruikt om met uw vrienden te corresponderen of een e-mailadres voor registratie bij webwinkels. Daarnaast kunt u een anoniem e-mailadres gebruiken waar geen persoonsgegevens zoals naam, geboortejaar, woonplaats, etc. in voorkomen. Zo krijgen aanvallers geen extra informatie over u op basis van uw e-mailadres. Dit beperkt hen in hun mogelijkheden voor het uitvoeren van een gerichte aanval.
3. *Geef uw gegevens alleen aan organisaties die u vertrouwt*. Aangezien u bij het afgeven van uw persoonsgegevens de controle erover uit handen geeft, dient u dit alleen te doen bij organisaties die u vertrouwt. Als u een organisatie niet vertrouwt, gebruik dan bij voorkeur een alias en/of een apart e-mailadres bij registratie.
4. *Maak gebruik van sterkere mogelijkheden van toegangsbeveiliging*. Steeds meer online diensten bieden de mogelijkheid tot het gebruik van zogenoemde tweefactor-authenticatie (ook wel tweestapsverificatie). Hierbij dient u naast kennis over het wachtwoord ook te beschikken over bijvoorbeeld een mobiele telefoon waarop bij elke sessie een nieuw wachtwoord verschijnt. Zonder deze mobiele telefoon kunnen kwaadwillenden niet inloggen op de betreffende dienst, ook al beschikken zij wel over uw wachtwoord. Tweefactor-authenticatie is standaard meestal niet ingeschakeld, u zult dit per dienst moeten configureren. Veel populaire diensten zoals Twitter, Facebook en DigiD ondersteunen deze manier van aanmelden.
5. *Gebruik sterke wachtwoorden, in het bijzonder voor het inloggen op gevoelige toepassingen*. Voorbeelden hiervan zijn toepassingen voor uw werk of internetbankieren. Controleer de eigenschappen van uw wachtwoorden op http://jewachtwoord.nl om erachter te komen of deze sterk genoeg zijn.
6. *Gebruik niet overal hetzelfde wachtwoord en/of gebruikersnaam*. Gebruik verder voor gevoelige toepassingen, zoals internetbankieren, exclusieve wachtwoorden en gebruikersnamen die u niet bij eenvoudige toegangsbeveiliging gebruikt (zoals toegang tot een forum over uw hobby).
7. *Wijzig uw wachtwoorden regelmatig*. Hiermee voorkomt u dat kwaadwillenden lange tijd uw wachtwoord kunnen misbruiken.
8. *Zeg inactieve registraties op*. Als u geen gebruik meer maakt van een onlinedienst, kunt u uw inschrijving bij deze dienst het beste beëindigen.

Als gegevens gelekt zijn bij een bedrijf uit de Verenigde Staten, zal het bedrijf hoogstwaarschijnlijk verplicht zijn om getroffen klanten op de hoogte te brengen. Daar is in bijna alle staten wetgeving ingevoerd die bedrijven verplicht tot een dergelijke melding. In zulke gevallen zult u bijvoorbeeld door een e-mailbericht op de hoogte worden gesteld.

Mijn gegevens zijn gelekt. Wat kan ik doen?

Mocht u ontdekken dat uw gegevens deel uitmaken van een datalek, dan kunt u een aantal stappen zetten om de potentiële schade te beperken:

1. Verander direct uw wachtwoord van alle toepassingen waar uw gegevens gelekt zijn. Ook als u slechts vermoedt dat uw gegevens gelekt zijn, is het raadzaam uw wachtwoord direct te veranderen[5]. Daarnaast is het aan te bevelen om gebruikersnamen en wachtwoorden voor andere toepassingen te veranderen wanneer die hetzelfde zijn als de gelekte toegangsgegevens.
2. Houd uw persoonlijke onlinebeheer-omgevingen ('Mijn X'), afschriften van betaalrekeningen, creditcards etc. in de gaten en wees alert op ongebruikelijke activiteiten[6]. Laat getroffen rekeningen en/of creditcards direct blokkeren. Als u ongebruikelijke activiteit op uw internetbankieromgeving waarneemt, neem dan direct contact op met uw bank[7].
3. Indien het (ook) werkgerelateerde informatie betreft (zoals uw zakelijke e-mailadres), informeer dan uw werkgever. Zo is uw werkgever op de hoogte en kan hij (indien nodig) maatregelen treffen.

Aangifte doen?

Indien het datalek is ontstaan door computervredebreuk ('hacking'), kunt u hiervan aangifte doen. Het is zeker aan te bevelen om dit te doen als blijkt dat er misbruik gemaakt is van uw gegevens of als u financiële schade heeft geleden. U doet aangifte op het politiebureau in uw gemeente. Het is verstandig om hiervoor een afspraak te maken en daarbij te vragen naar een digitaal rechercheur, zodat iemand met kennis van zaken uw aangifte op kan nemen.

Indien uw gegevens per ongeluk zijn gelekt (bijvoorbeeld door onbedoelde publicatie op internet), is de partij die deze heeft gelekt waarschijnlijk niet strafrechtelijk aansprakelijk. U kunt in dit geval geen aangifte tegen deze partij doen. Wel kunt u deze partij langs civielrechtelijke weg aansprakelijk stellen indien u van mening bent dat deze nalatig heeft gehandeld. Als een derde partij misbruik maakt van de gelekte gegevens, kunt u wel aangifte doen tegen deze derde partij.

[5] Doe dit alleen vanaf een vertrouwde computer waarvan de basisbeveiliging op orde is. Als deze computer besmet is met malware, kan ook uw nieuwe wachtwoord bekend worden.

[6] Meer informatie over het opmerken van een datalek via ongebruikelijke activiteit: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201209_en.pdf.

[7] Voor meer informatie over het melden van fraude bij internetbankieren kunt u terecht bij de Fraudehelpdesk, www.fraudehelpdesk.nl.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55 | F 070-322 25 37
Publicatienr: FS-2011-05 | Aan deze informatie kunnen geen rechten worden ontleend.