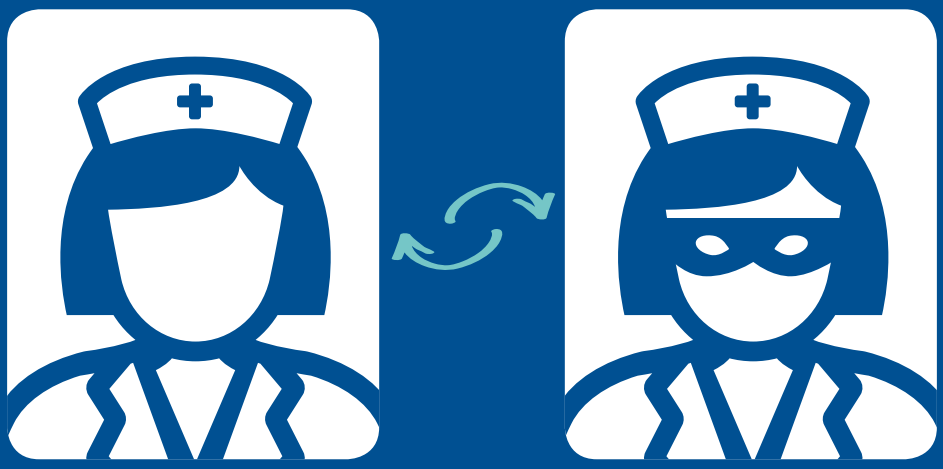
#ditisprivé



Whitepaper

Identiteitsfraude binnen de zorg

Cijfers, valkuilen en tips

#ditisprivé

Cijfers, valkuilen en tips

Identiteitsfraude binnen de zorg

Er zijn veel waardevolle gegevens te vinden binnen de zorgwereld. Informatie die cybercriminelen kunnen gebruiken om identiteitsfraude te plegen. Dat brengt dus risico's met zich mee. **In deze whitepaper lees je wat daar aan te doen is.**

#ditisprivé

De cijfers

1.724 fraudemeldingen

Dit is ruim een verdubbeling van het aantal meldingen van identiteitsfraude ten opzichte van 2015

TOP 4

1. **Fraude met adresgegevens of telefoonnummer** (393 meldingen)
2. **Paspoortfraude** (316 meldingen)
3. **Fraude met een ID-kaart** (223 meldingen)
4. **Fraude met een rijbewijs** (152 meldingen)

In 2016 voerde het meldpunt de mogelijkheid in om identiteitsfraude melden. Dat heeft mogelijk drempelverlagend gewerkt.

Bron: AD, CMI

155 gevallen identiteitsfraude per dag

56.717 gevallen per jaar

Veel? Volgens het CBS was het vier jaar daarvoor nog veel meer. Namelijk 207.505 gevallen van identiteitsfraude per jaar (577 per dag). Alleen: destijds was skimming (het kopiëren van een bankpas of creditcard) nog een heel groot probleem. Volgens experts zijn de risico's in de zorg de laatste jaren alleen maar toegenomen omdat banken de boel nu flink hebben dichtgetimmerd terwijl ziekenhuizen en zorgorganisaties nog wel kwetsbaar zijn. Zo zijn cybercriminelen zeer geïnteresseerd de persoonlijke informatie die in medische dossiers te vinden is.

Bron: Veiligheidsmonitor 2016, CBS

€ 1.726.933,- aan schade

door identiteitsfraude is er in 2016 bij Fraudehelpdesk.nl gemeld. Het gaat daarbij om misbruik van persoonlijke of zakelijke gegevens. Opvallend: in de eerste helft van 2017 lag het schadebedrag al op € 1.493.265,-. In de door de Fraudehelpdesk opgestelde lijst met grootste oplichtingsrisico's staat identiteitsfraude op nummer 4.

Bron: Fraudehelpdesk

#ditisprivé

Check, dubbelcheck: identiteitsfraude binnen de zorg

Hoe gaan identiteitsfraudeurs eigenlijk te werk? En in hoeverre is de zorgwereld tegen hun duistere praktijken opgewassen? Het begint met het besef dat er reëel gevaar dreigt en dat er actie ondernomen moet worden. Daarom: een overzicht van risico's en veelvoorkomende valkuilen.

Risico's

De slachtoffers van identiteitsfraude zijn meestal privépersonen: burgers, klanten, patiënten. Zij kunnen van alles verwachten. Van onbekende afschrijvingen op bank- of creditcardafschriften tot afwijzing voor leningen die ze nooit aangevraagd hebben of aanmaningen van incassobureaus voor producten of diensten die ze nooit afgenomen hebben. Maar ze kunnen ook opeens onder een ander adres ingeschreven zijn bij de gemeente. Of ze krijgen bij het aanvragen van een subsidie of uitkering doodleuk te horen dat die eerder al met succes is aangevraagd. Deurwaarders die beslag komen leggen op de inboedel, gedupeerden die boos verhaal komen halen, politieagenten aan de deur... Het komt allemaal voor. Kortom: ellende! Alle reden dus om er binnen de zorgwereld voor te zorgen dat criminelen geen toegang kunnen krijgen tot identiteitsgegevens en privacygevoelige informatie.

Zakelijke slachtoffers zijn er ook. Zo is er het fenomeen CEO-fraude, waarbij de crimineel zich via de mail of aan de telefoon voordoet als de grote baas van een bedrijf of organisatie. Of de medewerker zo snel mogelijk een groot geldbedrag kan overmaken. Is allemaal zeer vertrouwelijk! Als de medewerker nog vragen heeft, kan hij altijd contact opnemen met de advocaat van de zogenaamde CEO (die 'advocaat' zit uiteraard ook in het complot).

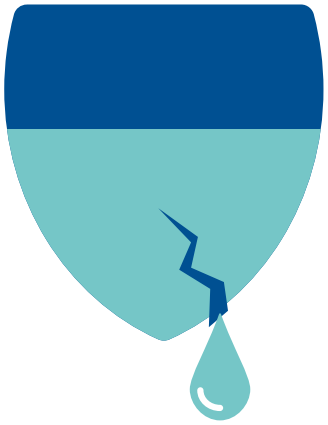
Spionage kan ook het doel zijn van cybercriminelen. Een van de technieken die ze daarbij inzetten is spearfishing, waarbij het slachtoffer een email krijgt die ogenschijnlijk afkomstig is van iemand waar hij eerder al eens contact mee heeft gehad. In dat bericht wordt hij op een vertrouwenwekkende manier aangesproken, waarbij er ook verwezen wordt naar persoonlijke interesses. De daarvoor benodigde informatie hebben de criminelen vooraf via social media verzameld. Op die manier lukt het hen om het vertrouwen van het slachtoffer te winnen en hem over te halen om op een link in de email te klikken. Het gaat daarbij om een geïnfecteerde link die ervoor zorgt dat de hackers toegang krijgen tot het computersysteem. Zeer geraffineerd, dat spearfishing. Zeer gevaarlijk dus ook.

De zorg is momenteel een aantrekkelijk doelwit voor cybercriminelen. Dat komt in de eerste plaats omdat medische dossiers op het Dark Web veel op kunnen leveren – veel meer dan creditcardinformatie. En hoewel de beveiliging van IT binnen de zorgwereld momenteel een grote prioriteit heeft en daar ook flinke stappen worden gezet, is die sector toch nog kwetsbaar. Dat blijkt ook wel uit de koppen van nieuwsberichten, zoals 'Security in zorg loopt achter op banken en overheden' en 'Ziekenhuis in de toplijst als doelwit voor cybercrime in 2017'.

Nederland heeft een fraudegevoelige zorgketen concluderen experts. Dat komt onder andere omdat een deel van de zorgbudgetten naar gemeenten zijn overgeheveld en elke gemeente daar op een andere manier mee omgaat.

Cybercriminelen weten dit ook en hebben veel misbruikmogelijkheden als zij binnen de zorgwereld door weten te dringen tot systemen en databestanden. Die lijst met mogelijkheden is behoorlijk verontrustend: van het beïnvloeden van onderzoeksgegevens tot het illegaal verkrijgen van medicijnen en van fraude met persoonsgebonden budgetten tot het onterecht declareren van zorgkosten.

#ditisprivé



Valkuilen

Cybercriminelen gebruiken veel slinkse methodes om binnen de zorg persoonlijke en medische informatie te achterhalen. De volgende drie zaken verdienen extra aandacht!

Medische dossiers mogen alleen toegankelijk zijn voor degenen die bij de behandeling van een patiënt betrokken zijn. Alleen die specialisten en medewerkers mogen een autorisatie krijgen om die medische informatie in te kunnen zien. De rest niet.

HTTPS regelt dat websites goed beveiligd zijn. Maar eerder dit jaar werd bekend dat bij een kwart van de websites van ziekenhuizen zo'n beveiligde verbinding via het https-protocol ontbreekt. Privacygevoelige informatie die patiënten via een webformulier invoeren, kunnen zo onderschept worden door cybercriminelen.

Medische apparaten zijn ook steeds vaker het doelwit van hackers. Medjacking heet dat, wat staat voor medical device hijack. Omdat veel medische apparaten nog op verouderde besturingssystemen draaien, kunnen hackers via de achterdeur toegang krijgen tot het netwerk. Daar vinden ze vervolgens patiëntinformatie waarmee ze identiteitsfraude kunnen plegen.

Tips

Enkele aandachtspunten voor de bestrijding van identiteitsfraude op organisatieniveau:

Informatie over cyberrisico's delen zou volgens experts een goede stap zijn om beveiligingsproblemen binnen de zorg te tackelen. Daarbij zou ook big data ingezet kunnen worden. Het Openbaar Ministerie en het bedrijfsleven hebben dat eerder al met succes gedaan om fraudes beter zichtbaar te maken.

Bewerkersovereenkomsten zijn belangrijk als de gegevensverwerking aan een andere partij is uitbesteed. In zo'n overeenkomst kun je precies vastleggen hoe de bewerker met de gegevens om moet gaan.

Tweefactorenauthenticatie is een must, met name bij de online patiëntportalen van ziekenhuizen. Dat is ook een nadrukkelijk tip van de Autoriteit Persoonsgegevens (AP), Alleen een gebruikersnaam en een wachtwoord is dan nog niet genoeg om toegang tot het portaal te krijgen. Er is dan nog een ander verificatiemiddel nodig, bijvoorbeeld een token of sms-code. Eind vorig jaar heeft AP een brief aan de Nederlandse Vereniging van Ziekenhuizen (NVZ) gestuurd om ziekenhuizen aan te sporen om zo snel mogelijk gebruik te gaan maken van tweefactorenauthenticatie. Ook biedt AP dit jaar op dat vlak ondersteuning aan.

De nieuwe privacywetgeving gaat natuurlijk ook enorm helpen. Dankzij de invoering van de Algemene verordening gegevensbescherming (AVG) moeten alle bedrijven en organisaties in heel Europa straks, vanaf mei 2018, op dezelfde manier te werk gaan. Voor criminelen wordt het dan een stuk lastiger om privacygevoelige gegevens en identiteitsinformatie te onderscheppen.

Tot die tijd is het extra belangrijk om alert te zijn, het gezonde verstand te gebruiken en met z'n allen te beseffen dat identiteitsfraudeurs op een steeds geraffineerdere manier te werk gaan.

#ditisprivé

10 tips

Zo geef je identiteitsfraudeurs geen kans!

1 Check bij mails met links en bijlagen eerst of het e-mailadres wel echt klopt. Bij spearfishing roept de inhoud van de mail waarschijnlijk niet meteen argwaan op. Goed kijken dus.

2 Belt of mailt de 'grote baas' met een opmerkelijk verzoek? Hoor dan meteen de alarmbellen in je hoofd. Ga niet direct in op het verzoek, maar onderzoek eerst of je daadwerkelijk met de echte directeur, bestuursvoorzitter of CEO te maken hebt.

3 Vermeld nooit een BSN in correspondentie met patiënten. Dat burgerservicenummer mogen zorgverleners alleen gebruiken om te checken of het wel om de juiste patiënt gaat, bijvoorbeeld als zij onderling gegevens uitwisselen.

4 Gebruik alleen zakelijk e-mailaccounts om zakelijke info te delen.

5 Zorg voor een lange en complexe wachtwoorden (die wachtwoorden vooral niet op een Post-It schrijven en ophangen!)

6 Wees zorgvuldig met het documentenbeheer. Neem zelf de nodige maatregelen om te voorkomen dat privacygevoelige informatie en identificatiegegevens in verkeerde handen vallen.

7 Zet privacygevoelige gegevens en identiteitsinformatie nooit op onbeveiligde media, zoals een usb-stick of laptop. Bij verlies of diefstal is er dan namelijk meteen sprake van een datalek en een kans dat criminelen die informatie gebruiken om identiteitsfraude te plegen.

8 Gebruik alleen vertrouwde Wi-Fi-netwerken. Je weet anders niet of er misschien iemand stiekem meekijkt.

9 Zorg dat computers altijd up-to-date zijn. Installeer veiligheidsupdates dus zo snel mogelijk.

10 Maak onderling duidelijke afspraken. Als medewerker moet je niet alleen precies weten wat je moet doen om identiteitsfraude en cybercriminaliteit te voorkomen, maar ook hoe je moeten handelen als het onverhoopt misgaat.

#ditisprivé

checklist

Als het toch misgaat...

✓ Zo beperk je de schade!

Is er sprake van identiteitsfraude?

☐ Meld dat dan direct aan het slachtoffer.

Het slachtoffer kan dan aangifte doen bij de politie en de identiteitsfraude online melden bij het **Centraal Meldpunt Identiteitsfraude- en fouten (CMI).**

Kan het datalek tot identificatie-fraude leiden?

☐ Meld dit dan bij de Autoriteit Persoons-gegevens via het meldloket datalekken.

Als het datalek tot identificatiefraude kan leiden geldt er een meldplicht. Die plicht geldt sinds 1 januari 2016 voor elk ernstig datalek. Organisaties moeten die melding doen bij de Autoriteit Persoonsgegevens. Dat kan via het **meld-loket datalekken**.

Heeft ransomware bestanden met persoonsgegevens versleuteld?

☐ Behandel dit dan als datalek en meld dit bij de Autoriteit Persoonsgegevens. Na een aanval met ransomware is het lastig bepalen tot welke bestanden de hacker toegang heeft gehad. Let op: ook na besmetting met ransomware is er sprake van een datalek!

Om een bestand te kunnen versleutelen, moet een hacker namelijk eerst toegang hebben tot het bewuste bestand. Er is dus een kans dat hij de gegevens heeft gekopieerd of gemanipuleerd. Wat daarbij lastig is: na een aanval met ransomware is het lastig te bepalen tot welke bestanden de hacker toegang heeft gehad. Kortom: een besmetting met ransomware kan het hele systeem en alle gekoppelde bestanden raken! Daarom geldt ook hier een meldplicht bij de **Autoriteit Persoonsgegevens**.

Meer weten?
Kijk op medireva.nl/ditisprive en schrijf je in voor de nieuwsbrief.

MediReva