Medische data zichtbaar te koop op World Wide Web: een waarschuwing

Het is de grootste angst van zorgmedewerkers en IT-beveiligingsspecialisten die zich om veilig gebruik van zorgdata bekommeren dat een hacker medische verwerft en te koop aanbiedt. In de krochten van het internet is nu een voorbeeld daarvan te zien. Het betreft een aanbod op een forum op het internet waar illegale handel in gegevens plaatsvindt, waaronder inloggegevens en databases. Iemand met de naam "Databox" biedt daar een forse database te koop aan. Daarin: "Fields: Gender, Full name, Phone-number, Mobile-number, Address, Email, medication and more." Die laatste twee wijzen op een gestolen database met medische informatie. Matthijs Koot, IT-beveiligings-specialist, bezorgt als hij is over privacy-kwesties, tipte mij over het bestaan van deze "advertentie". Zijn proefschrift uit 2012, genaamd "Measuring and Predicting Anonimity", beantwoordde vragen als "Hoe anoniem zijn geanonimiseerde gegevens?' en 'In hoeverre is het mogelijk geanonimiseerde gegevens te de-anonimiseren?".

"Advertentie"

De aanbieder van de data draagt de toepasselijke naam "Databox". Op het forum heeft hij/zij de status "God". Dat kan afhangen van de "prestaties", maar ik vernam dat zo'n status ook gewoon te koop is. De persoon die op dat underground-forum de data te koop aanbiedt heeft het over een database met 4,4 miljoen "records". Hij of zij laat een screenshot zien met de persoonsgegevens van een man van 49 jaar waarop wel de persoonsgegevens te zien zijn. Essentiële data op de afbeelding heb ik gezwart. De kop van het dataveld

Diagnose(Diagnostico) is te zien, maar niet de inhoud. Theoretisch is het mogelijk dat de persoon die dit koopaanbod doet opschept over data die hij/zij niet bezit en indruk probeert te maken door te bluffen. De inhoud van het aanbod suggereert echter wel dat een gestolen/gekopieerde mega-database de basis is voor dit aanbod. Bovendien lijkt de opmerking “Dumped it this year” de indruk te wekken dat de gegevens afkomstig zijn uit hacking door hem of haar zelf.

Afkomstig van?

De data hoeven niet noodzakelijkerwijs uit een ziekenhuisomgeving te komen. Het kan ook afkomstig zijn van een ziektekostenverzekeraar of een overheidsinstelling die zich bezighoudt met de zorg. In het bericht van “Databox” noemt deze een “record count van 100k. Daarmee bedoelt hij/zij dat er een sample-bestand is met 100.000 regels waaraan de eventuele koper kan zien dat het om serieuze data gaat. Dat wijst erop dat het bij de personen in de bestanden waarschijnlijk om ambtenaren gaat. Naar verluidt staan alleen al in de voorbeeldgegevens ook medicatiegegevens van ruim 100 ambtenaren, waaronder iemand van de Colombiaanse luchtmacht. Dat was af te leiden uit onderdelen van de mailadressen in de bestanden.

Wat gebeurt ermee?

Het misbruik van gestolen persoonsgegevens met medische data beschreef ik eerder op 21 mei 2019

Grofweg kan men het misbruik in vier categorieën indelen.

- Diefstal van de medische identiteit. Met iemands medische gegevens probeert men medische diensten te verkrijgen: voorschriften voor medicatie(opiaten bijv.), medische ingrepen, valse verzekeringsclaims
- Financiële fraude met gebruikmaking van tot een persoon herleidbare informatie bij banken en creditcard-

maatschappijen. Medische dossiers bevatten namelijk vaak informatie over betaalwijze, bankgegevens etc.

- Gebruik maken van gevoelige zorgdata om individuen te bedreigen, af te persen of te beïnvloeden. Daarbij kan het om echte buitgemaakte data zijn, maar ook gemanipuleerde data. VIP's en bekende publieke personen zijn extra kwetsbaar. Zulke gegevens kunnen worden misbruikt voor gerichte phishing, chantage en andere narigheid. Denk aan medicatie die verband houdt met gevoelige onderwerpen, zoals hiv-remmers en psycho-actieve-geneesmiddelen,.
- Buitgemaakte data kunnen gebruikt worden bij verder gaande cyberaanvallen. Zo kan informatie gebruikt worden om nieuwe aanvallen uit te voeren met buitgemaakte toegangs-/authenticatie-informatie.

Nederland

Nu zult u zeggen, Colombia is ver weg en niet te vergelijken met Nederland. Niets is minder waar. Digitaal gezien bestaan er geen afstanden. Trouwens ook in Nederland kennen we veel datalekken in de zorg. De Autoriteit Persoonsgegevens(AP) meldde op 19 september 2019 dat de zorg opnieuw koploper datalekmeldingen was bij de AP. Die publiceerde een handleiding over hoe te handelen bij een datalek in de zorg. Bovendien maakte de AP zelfs een brochure "5 tips voor zorginstellingen om datalekken te voorkomen". Het is dus van belang dat zorgaanbieders en apotheken hun informatiebeveiliging voldoende op orde hebben, en dat de kans op menselijke fouten zo klein mogelijk is.

NEN7510

In Nederland moeten zorgsystemen trouwens verplicht voldoen aan een beveiligingsnorm, de NEN7510″. Deze norm sluit een hack of menselijke fout niet uit, maar is voor de lezer misschien prettig als geruststellende afsluiter. Zowel

Matthijs Koot als mij zijn geen één-op-één vergelijkbare incidenten bekend in Nederland. De door mij hierboven beschreven casus dient al een herinnering gezien te zijn aan het belang van privacy en goede informatiebeveiliging met betrekking tot gezondheidsgegevens.

W.J. Jongejan, 4 september 2020

Afbeelding van S K via Pixabay