Hackers bieden Australische Medicare-card-data te koop aan. Les voor Nederland

Op 4 juli 2017 werd duidelijk dat op het zogenaamde Dark Web, een alleen met een speciale browser toegankelijk deel van het internet, gegevens te koop waren van Australische Medicare-ID-kaarten. Dat zijn kaarten met een magneetstrip, die de bezitter toegang geeft tot behandeling in de eerstelijnszorg en zorg in publieke ziekenhuizen. De melding kwam van een journalist van The Guardian, die op het Dark Web voor 22 US dollar, of 0,0089 bitcoin, de data van zijn eigen medicare-card kocht. Degene die de data verkocht had sinds oktober 2016 data van tenminste 75 Medicare-kaarten verkocht. De kaarten worden uitgegeven door het Australische Department of Human Services. De details van de kaarten, zoals nummer, tenaamstelling en expiratiedatum zijn niet publiek toegankelijk en zijn alleen de eigenaar van de kaart bekend. Door criminelen wordt de informatie als waardevol beschouwd. omdat ze het mogelijk maken om nep-Medicare-kaarten te maken met bestaande gegevens. Die kunnen dan gebruikt worden voor identiteitsfraude.

Waardevol

Al enige tijd is het duidelijk dat diefstal van medische gegevens veel lucratiever is dan het bemachtigen van creditcardnummers. Cybersecurity-adviseurs denken dat medische

gegevens, inclusief de polis- en persoonsnummers(social-security-numbers of BSN) tot tien keer meer waard zijn dan creditcarddata. De gegevens op de kaarten kunnen gebruikt worden door criminelen voor de aanschaf van goederen, bijv. auto's. Ook kunnen uitbetalingen van Medicare aan de burger doorgesluisd worden naar frauduleuze bankrekeningen. Al in 2015 had een politie-eenheid een criminele groep opgespoord die Medcare-card data gebruikte om zich frauduleus terugbetalingen toe te eigenen. Een probleem in Australië is tevens dat de Medicare-card ook als identificatiemiddel(Digital Verification Service) buiten de zorg wordt gebruikt. Dat bleek toen de Australische belastingdienst, de Australian Tax Office met onmiddellijke ingang aangaf dat de Medicare-card niet meer gebruikt mocht worden als identiteitsverificatie bij belastingzaken. Het vreemde was dat nog geen 24 uur later dezelfde dienst aangaf dat de kaart weer als identificatiemiddel mocht worden gebruikt.

Overheid

Zoals te verwachten probeerde de overheid bij monde van de minister van het Department of Health Services direct het belang te downplayen onder andere dat het ging om kleine aantallen. De stelling van minister Tudge is dat het hier niet om een hack ging maar om een "traditional criminal activity" gaat en niet om een groot datalek. De minister bleek tot aan 5 juli 2017 niets van de diefstal van card-data te weten ook al waren de data al vanaf oktober 2016 te koop op het Dark Web. De berichtgeving via de pers schudde het ministerie wakker.

Medische data

Naar verluidt zijn bij de diefstal van de kaartdata niet rechtstreeks medische data in handen van criminelen gekomen. Wel zijn bij de diefstal de koppeling van naam en Medicare-nummer van de betrokkenen buitgemaakt. Om bij de medische data te komen zijn elektronische NASH en/of PKI-certificaten nodig.

Die worden echter door de overheid naar duizenden zorgverleners verstuurd en naar verluidt zijn daarvan meerdere “zoekgeraakt”. Misbruik is dus niet uit te sluiten.

Medicare

Het gecentraliseerde Medicare-ysteem stond en staat bloot aan veel kritiek en is toch doorgeduwd. Medische data worden in een centrale database opgeslagen. In noodgevallen mogen artsen de medische gegevens van burgers in “My Health Record” zonder toestemming van de patiënt inzien. De overheid mag de medische data zonder toestemming inzien als fraude vermoed wordt of bij rechtszaken. Medicare gaat ook onzorgvuldig om met data. Recent werden deels versleutelde databestanden openbaar beschikbaar gesteld die door enkele academici binnen korte tijd vergaand te ontcijferen waren. De vreemde reactie van de overheid was toen om het ontcijferen strafbaar te stellen in plaats van het te accepteren als een waarschuwing!!!

Nederland

Wat leert deze materie ons Nederlanders? Wij hebben ook een gecentraliseerd systeem met het Landelijk SchakelPunt(LSP). De data zijn niet centraal opgeslagen, maar zijn bij de bron raadpleegbaar via het LSP. De toegang is geregeld met UZI-passen en kaartlezers. Diefstal van UZI-pas en pincode van de gebruiker maakt het in principe mogelijk dat door die dief vanaf een werkstation plus kaartlezer met malafide intenties ingelogd kan worden en data opgevraagd worden. Uiteraard vindt logging plaats van het gebeurde en is de toegangsweg te identificeren, maar het kwaad is dan al geschiedt zonder dat men weet wie de dader is. Men weet alleen wiens pas gebruikt is en mogelijk welke werkplek. Bovendien zal het de gedupeerde burger niet altijd duidelijk zijn dat zijn of haar data ingezien zijn als deze geen abonnement heeft op meldingen van inzage in de medische gegevens via het LSP.

Kortom: het kan ook hier gebeuren, het is alleen de vraag

wanneer en hoe uitgebreid.

W.J. Jongejan