

Crimineel verkregen elektronisch medisch dossier tussen 250 tot 1000 dollar waard



Op 11 april 2019 publiceerde het Department of Health and Human Services (HHS) een kennisgeving over cybersecurity in de zorg. Dit departement van de V.S. is de tegenhanger van ons ministerie van VWS. [De publicatie, bestaande uit 13 sheets](#), is een briefing met als titel "Dark Web PHI Marketplace". PHI staat voor Protected Health Information. In de publicatie wijst het ministerie op de enorme consequenties van het illegaal verwerven en verhandelen van crimineel verkregen zorgdata op het schimmige deel van het internet, het Dark Web. Daarop is het mogelijk dat kwaadwillende personen/organisaties illegaal verkregen zorgdata kopen en verkopen die afkomstig zijn van datalekken. Dat soort marktplaatsen stimuleren cybercriminelen om zorgorganisaties elektronisch aan te vallen en de buit te gelde te maken. Zorgdata zijn volgens het ministerie op dit moment één van de meest winstgevende data op het Dark Web. Criminelen kunnen daar anoniem acteren zonder angst voor repercussies.

Waar is het om te doen?

Het gaat criminelen om het verkrijgen van tot een persoon herleidbare informatie (Personally Identifying Information (PII)). Niet alleen zorgdata staan in de belangstelling maar ook social media accounts, onderwijsbestanden en bestanden uit gemeentelijke administraties. Zorgdata staan speciaal in de belangstelling, omdat daar een scala van criminele

activiteiten mee uit te voeren zijn. Dat met een lager risico dan als het gaat om financiële data. Fraude met zorgdata is moeilijker te achterhalen dan financiële fraude bijv. met creditkaarten. Met informatie uit zorgdossiers zijn meerdere typen fraude uitvoerbaar.

Wat gebeurt ermee?

Grofweg kan men het misbruik in vier categorieën indelen.

1. Diefstal van de medische identiteit. Met iemands medische gegevens probeert men medische diensten te verkrijgen: voorschriften voor medicatie (opiaten bijv.), medische ingrepen, valse verzekeringsclaims
2. Financiële fraude met gebruikmaking van tot een persoon herleidbare informatie bij banken en creditcardmaatschappijen. Medische dossiers bevatten namelijk vaak informatie over betaalwijze, bankgegevens etc.
3. 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.
4. Buitgemaakte data kunnen gebruikt worden bij verder gaande cyberaanvallen, bijv. met behulp van phishing mail en vormen van oplichting. Ook kan informatie gebruikt worden om nieuwe aanvallen uit te voeren met buitgemaakte toegangs-/authenticatie-informatie.

Waarde

Het Department of HHS schat de waarde van zorgdossiers op het Dark Web **op 250 tot 1000 dollar per dossier**. De waarde is zo hoog omdat zorgdossiers vaak persoonsgegevens, financiële gegevens en medische data in een compacte vorm bevatten. In de zorg gebruiken we in Nederland het BurgerServiceNummer (BSN), waarmee ook identiteitsfraude uitgevoerd kan worden.

Kwetsbare groepen

In de publicatie noemt het departement drie specifieke groepen, waarvan de gegevens extra interessant zijn voor de criminelen.

- **Jonge kinderen.** Bij data, afkomstig van hacks, is op het Dark Web vooral de “versheid” van belang, d.w.z. dat de data niet eerder gebruikt zijn voor fraude. Data van jonge kinderen zijn dan ook “vers” te noemen. Ze kunnen gebruikt worden voor kredietaanvragen, grote aankopen, zonder dat het slachtoffer er erg in heeft. In de V.S. zijn er onvoldoende controlemechanismen om misbruik van de identiteit van een kind bij kredietfraude op te sporen.
- **Ouderen.** Daarbij speelt financiële kwetsbaarheid die geassocieerd is met de leeftijd. De Federal Trade Commission, een onafhankelijk agentschap van de Amerikaanse federale overheid, schat dat 35% van de klachten over fraude en 19% van de identiteitsdiefstal bij 65 plussers zich voordoet.
- **Overledenen.** Het is gebleken dat criminelen de gegevens van overledenen als “veiliger” zijn gaan beschouwen naarmate de bewustwording van fraude bij de burger stijgt. De identiteit van overledenen blijkt gebruikt te worden bij creditcard-fraude, belastingfraude en de aankoop van dure artikelen.

Bewustwording

Het Department of Health and Human services beoogt met de publicatie een grotere bewustwording voor de problematiek bij zorgorganisaties, zorgverleners en bij burgers. Cybersecurity is van groot belang bij zorgverleners en in zorginstellingen. Veel meer dan voorheen zal men zich bewust moeten zijn van de manier waarop bedreigingen zich voordoen. Net zoals bij steriliteit is het bij het gebruik van digitale middelen een

goede “hygiene” van groot belang. Niet alleen van de ICT-ers die in de zorg werkzaam zijn, maar vooral van de werkers zelf. Een goed voorbeeld van alerte werknemers is bijvoorbeeld de community [“Women in Cybersecurity”](#).

W.J. Jongejan, 21 mei 2019