Webwinkel Vilans, kenniscentrum voor langdurende zorg, gehackt

Op donderdag 3 januari 2019 hebben klanten van de webshop van Vilans bericht gekregen dat de database van de webshop gehackt geweest is. Vilans is een vrij grote grotendeels gesubsidieerde organisatie die stelt kenniscentrum te zijn voor de langdurende zorg en als doel heeft om deze zorg te vernieuwen en te verbeteren. Ze ondersteunt vooral zorgprofessionals die in de online-webshop rapporten en brochures kunnen bestellen. Ook particulieren kunnen er bestellingen doen. In het bericht dat klanten per email kregen is te lezen dat een hack heeft plaatsgevonden, ontdekt is en het gat gedicht is. Op de website van Vilans en op het Twitter-account is niets te lezen over de hack. Persoonsgegevens zijn door de hacker buitgemaakt. Vilans waarschuwt dat die informatie gebruikt kan worden voor phishing mail en raadt aan om het wachtwoord voor de webshop te wijzigen. Zoals zo vaak met dit soort berichten is het interessant om niet alleen te kijken naar datgene wat men meldt staat maar ook naar wat er niet in staat

Wat is Vilans?

Vilans is zoals gezegd een ondersteunende organisatie voor de langdurige zorg. Ze houdt zich bezig met entameren en begeleiden van innovatie & onderzoek, kennisdeling en advies &

Implementatie. Voor haar financiën is ze voor vrijwel geheel afhankelijk van subsidies. In 2017 was het personeelsbestand 167 FTE. In 2017 ontving Vilans op een begroting van 38 miljoen euro 4,8 miljoen aan instellingssubsidie en 27,5 miljoen aan projectsubsidies. Aan niet projectgebonden activiteiten ging 116.000 euro om. Dat zullen waarschijnlijk de inkomsten uit de webshop zijn. De webshop verkoopt rapporten en brochures over langdurige zorg op veel terreinen, niet alleen aan zorgverleners, en zorgbestuurders, maar ook aan particulieren.

Hack

Duidelijk is dat er een hack door een persoon geweest is. Het is ontdekt en het lek is gedicht . Niet duidelijk is hoe het heeft kunnen gebeuren, hoe lang het datalek bestaan heeft en wanneer dat precies heeft plaatsgevonden. Heeft de hacker gedurende meerdere dagen rond kunnen neuzen in de database? Heeft de hacker malware in het systeem geïmplanteerd? Een aanwijzing in die richting kan zijn dat Vilans waarschuwt voor phishing-mail waarin om bitcoin-betaling wordt gevraagd. Men vraagt om dat soort mail bij aantreffen in de eigen mailbox te verwijderen.

Omvang buit

Vilans maakte bekend dat de hacker persoonsgegevens heeft kunnen inzien. Men mag gevoeglijk aannemen dat die ook gekopieerd zijn. Vilans maakte **NIET** bekend welke persoonsgegevens allemaal buitgemaakt zijn. In een web-shop kunnen naast de adres- en emailgegevens ook betaalgegevens zoals creditkaart-data eventueel buitgemaakt zijn.

Melding aan AP?

Ook meldt Vilans niet aan haar klanten of er van het datalek melding gemaakt is bij de Autoriteit Persoonsgegevens. Dat dient binnen 72 uur na het ontdekken van het datalek te gebeuren. Het is niet aannemelijk dat Vilans de melding

achterwege zal laten, maar richting klant is het wel zorgvuldiger dat de organisatie zoiets meldt.

Uitgebreidheid hack

Het is overduidelijk dat de webwinkel de toegangsweg voor de hacker geweest is. Doordat klantgegevens weglekten moet Vilans dat wel aan de betrokkenen melden. Het is echter de vraag of de hack beperkt is gebleven tot de webwinkel. Via de webwinkel zou in theorie bij onvoldoende compartimentering en onvoldoende beveiliging ook het achterliggende ICT-systeem van de Vilans-organisatie gecompromitteerd kunnen zijn.

Kwetsbaar

Het moge duidelijk zijn dat organisaties die direct of indirect bij de zorg betrokken zijn ook grote risico’s lopen om gehackt te kunnen worden. Deze hack bij Vilans is er een voorbeeld van. Door de melding aan de klanten is het in ieder geval naar buiten gekomen. Het blijft de vraag of er niet veel meer geslaagde hack-pogingen in de zorg zijn. Veelal wordt er bij computerstoringen in de zorg alleen melding gemaakt van de verstoring en niet van de oorzaak.

W.J. Jongejan, 3 januari 2019