Ongeautoriseerd inzien zorgdata soms vanuit zeer onverwachte hoek

Niets is wat het lijkt te zijn. Deze nogal cynische uitdrukking is helaas vaak van toepassing, zeker in de ICT-wereld. In The Wallstreet Journal van 19 april 2017 stond een schokkend artikel over een Amerikaans IT-beveiligingsbedrijf, Tanium genaamd. Het bedrijf heeft toekomstige klanten gedurende enkele jaren de mogelijkheid geboden live in het netwerk van ziekenhuizen te kijken en heeft ook video's daarvan op YouTube gezet. Dat alles zonder dat de ziekenhuizen daar toestemming voor gaven. Terwijl het artikel in The Wallstreet Journal achter een betaalmuur zit, is er toch berichtgeving hierover die vrij te volgen is. De zaak kwam aan het rollen toen het El Camino ziekenhuis in Santa Clara County in Californië erop attent werd gemaakt dat 15 seconden durende filmpjes op YouTube te zien waren met informatie van het managementsysteem van het ziekenhuis. De ziekenhuisdirectie was hoogst verbaasd en verontwaardigd dat de leverancier van de software, die ze in 2010 aanschafte, minimaal gedurende vijf jaar deze vreemde handelswijze heeft gebezigd. Dat het om die jaren gaat blijkt uit de datering van de enkele honderden filmpjes op YouTube, die overigens inmiddels allemaal verwijderd zijn. De filmpjes waren ook te zien op het bedrijfsnetwerk van het cybersecurity-bedrijf.

El Camino Hospital

Het ziekenhuis heeft laten weten dat ze niet op de hoogte waren van dit gebruik van hun data en nooit toestemming gaf voor enige verkooppresentatie. Het ging om management informatie van het ziekenhuis, maar nooit om directe patiënteninformatie, benadrukt men. EL Camino Hospital is duidelijk not amused. Het ziekenhuis heeft inmiddels laten weten dat haar relatie met Tanium beëindigd zijn vanwege deze kwestie. Wat de software van het bedrijf deed, staat bekend als zogenaamde endpoint-security. Daarbij gaat het er om dat de software er voor zorgt dat alle PC's, smartphones, tablets en andere aan het ICT-systeem te koppelen apparaten de meest recente updates van programmatuur hebben, veilig zijn en niet te gebruiken als toegangspoort voor hackers. De binnendringers kwamen echter van een tegenovergestelde richting. In een artikel in de Business Insider staat een leuke vergelijking met een conciërge van je kantoor die allerlei onbekende lieden je bedrijfsruimtes laat zien om aan te tonen hoe goed hij het pand bewaakt.

Verdediging

Inmiddels heeft de topman van Tanium, Orion Hindawi, een verklaring uitgegeven die op zich weer veel bevreemding wekt. In die verklaring geeft hij aan dat enkele klanten geen bezwaar hebben tegen het verzorgen van demo's met hun bedrijfsgegevens. Die toestemming zou dan schriftelijk vastgelegd zijn. Gezien de gevoeligheid van bedrijfsgegevens op managementniveau verbaast deze uitspraak al. Hij vervolgt met de opmerking dat er in het specifieke geval met het EL Camino Hospital zonder toestemming gebruik gemaakt is van een demo-omgeving bij de klant. De IT-afdeling van het ziekenhuis zou met gebruik van fictieve data een demonstratie-database met gegevens hebben aangemaakt om dingen uit te testen met de leverancier of voor instructie aan eigen personeel. Hiermee suggereert hij dat de IT-afdeling van het ziekenhuis dit gebruik mogelijk zou hebben gemaakt en goedgekeurd. Het

ziekenhuis heeft in een reactie echter laten weten nooit geweten te hebben wat Tanium aan het doen was en nooit toestemming gaf om enig materiaal te laten gebruiken voor verkoopuitingen van Tanium.

Moraal

Wat van deze casus te leren is dat gevaren in (zorg)ICT-land niet altijd uit de hoek komen van waaruit je ze verwacht. Kortzichtige beslissingen bij een leverancier bedoeld voor winst op de korte termijn kan het vertrouwen met de klanten op de lange termijn ernstig schaden. Het verdient daarom aanbeveling altijd kritisch te blijven tegenover de eigen ICT-leveranciers en alert te reageren op vreemde gebeurtenissen met of rond de software die ze leveren.

W.J. Jongejan