Vertrouwelijkheid patiënt-gegevens in het geding?

De zorgsector komt soms negatief in het nieuws als het gaat over bescherming van persoonsgegevens. Het College Bescherming Persoonsgegevens (CBP) heeft onderzocht of zorginstellingen voldeden aan de wettelijke eisen. Het onderzoek richtte zich op de toegang tot persoonsgegevens door onbevoegde medewerkers. Maar hoe gaat men om met de gelegenheid die geboden wordt aan cliënten die toegang krijgen tot patiëntendossiers als personeel de kamer verlaat?

tekst André van Soest

De volgende casus beschrijft een fictieve situatie waaruit mogelijke risico's blijken. Een cliënt wil een afspraak in het ziekenhuis maken om mogelijke allergieën te laten onderzoeken. In eerste instantie is er de komende maanden geen ruimte voor het uitvoeren van het onderzoek. Maar de medewerkster leeft mee met de cliënt en kijkt of zij ergens tussen geplaatst kan worden. De afspraak kan toch binnen een week met een medische specialist plaatsvinden.
De cliënt meldt zich volgens afspraak bij de specialist. Deze vraagt de persoonlijke gegevens van de cliënt op via de computer. Vervolgens wordt een priktest uitgevoerd. Halverwege de test wordt de specialist gebeld dat er een dubbele afspraak is gemaakt en de andere cliënt in een behandelkamer wacht. De specialist zegt tegen zijn cliënt dat hij een kleine twintig minuten weg is en omdat zij toch even moet wachten op de reactie van de priktest is dat geen probleem. De cliënt ziet dat het computerscherm niet vergrendeld is en dat haar gegevens zichtbaar zijn op het scherm. Zij vraagt zich af of dossiers van andere cliënten ook op te vragen zijn...

RISICO'S

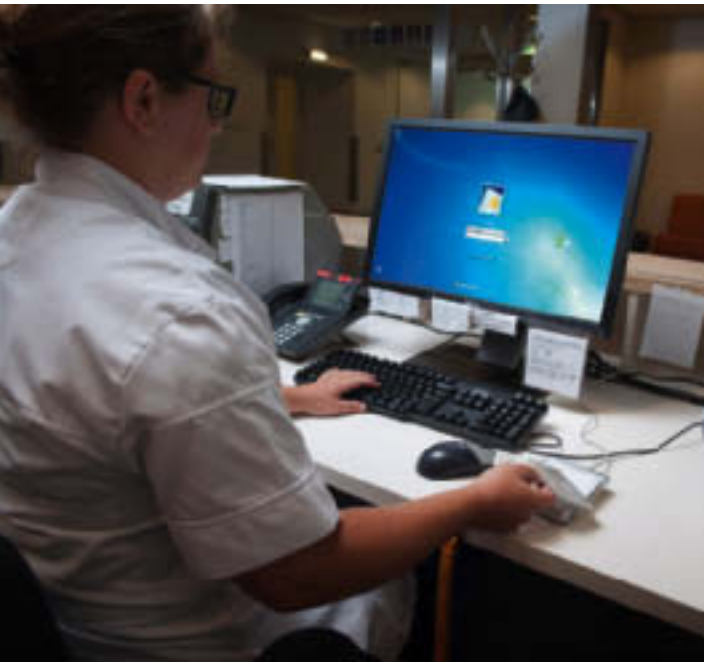
Welke informatierisico's heeft het ziekenhuis in deze casus mogelijk gelopen? De vraag is ook of er een kans bestaat dat het ziekenhuis deze risico's daadwerkelijk loopt?
De medisch specialist laat zijn cliënt voor langere tijd alleen en vergeet zijn scherm te vergrendelen.

- De cliënt is daardoor in de gelegenheid om dossiers met vertrouwelijke informatie van andere cliënten in te zien. Hierdoor komt de privacy van andere cliënten in gevaar.
- Artikel 13 van de Wet bescherming persoonsgegevens (WBP) verplicht het ziekenhuis om maatregelen te treffen om onbevoegde toegang tot medische gegevens te voorkomen. Het CBP kan het ziekenhuis sancties opleggen.
- Een kwaadwillende cliënt kan malware op de computer installeren.

MAATREGELEN

In de casus wordt duidelijk dat je van te voren helder moet krijgen welke risico's je loopt. Is overal aan gedacht? Zijn medewerkers op de hoogte van alle regels en richtlijnen? Wat zou er zijn gebeurd als de cliënt inderdaad kwaadwillend was en malware had kunnen installeren? Of dat bekend zou worden dat een cliënt medische dossiers van andere cliënten kan inzien doordat medisch personeel de computer niet vergrendelt?
Om te voorkomen dat bovengenoemde risico's werkelijkheid worden, zal een aantal maatregelen getroffen moeten worden:

- Communiceer regels en richtlijnen naar de medewerkers en maak duidelijk dat overtreding van de regels kan leiden tot sancties.
- Voorkom onbevoegd toegang tot vertrouwelijke gegevens.
- Richt een managementsysteem in voor informa-



tiebeveiliging (ISMS) en voor risicomanagement (NEN 7510). Laat een risicoanalyse uitwijzen welke maatregelen nodig zijn en welke niet.
- Voorkom dat malware geïnstalleerd kan worden.

BEWUST MAKEN VAN RISICO'S

Het management moet medewerkers bewust maken van de privacyrisico's die bijvoorbeeld het niet vergrendelen van de computer, of het laten slingeren van patiëntendossiers met zich meebrengt. Zorg ervoor dat aandacht wordt besteed aan regels en richtlijnen als onderdelen van een bewustwordingstraject. Neem dit onderwerp mee in periodieke werkoverleggen of bijeenkomsten. Door alleen een e-mail de organisatie in te sturen wordt de verantwoordelijkheid bij de medewerkers gelegd en de kans dat medewerkers dit zien als een 'gewone' mededeling is dan ook groot.
Het treffen van sancties is niet leuk maar soms wel noodzakelijk. Het management moet er voor gezorgd hebben dat medewerkers op de hoogte zijn van de regels en richtlijnen en wat de consequenties zijn van overtreding. Laat de beveiligingsfunctionaris in eerste instantie zelf een ronde maken over de verschillende afdelingen en aangeven welke zaken nog niet voldoen aan de gecommuniceerde regels en richtlijnen. Denk hierbij aan de zogenaamde sluitrondes die door beveiligingsfunctionarissen worden uitgevoerd. Zij laten een briefje achter, waarop staat dat het raam niet is afgesloten of de stekker van de waterkoker nog in het stopcontact zit.
Communiceer bevindingen naar de medewerkers en zorg ervoor dat medewerkers de middelen krijgen om regels en richtlijnen op te volgen.

ONBEVOEGDE TOEGANG TOT PERSOONSGEGEVENS

In artikel 13 Wbp is bepaald dat "de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking". Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
Het ziekenhuis moet dus maatregelen treffen om onbevoegde toegang tot persoonsgegevens te voorkomen. In deze case betreft het de toegang door een onbevoegde tot medische gegevens. De wet maakt geen onderscheid tussen medewerkers van het ziekenhuis of een cliënt. In de situatie dat een cliënt zich toegang verschaft tot de gegevens zal dit mogelijk leiden tot een grotere maatschappelijke discussie, dan in de situatie dat een onbevoegde medewerker toegang heeft.

NEN 7510

Inrichten van een managementsysteem en uitvoeren van risicoanalyses lijkt in eerste instantie op het doodschieten van een vlieg met een kanon in plaats van een vliegenmepper te gebruiken. Het gaat ook niet om dat ene aspect, het vergrendelen van het computerscherm. Het inrichten van een ISMS is een verplicht onderdeel van deze norm. Door het uitvoeren van een risicoanalyse weet je als organisatie welke risico's je loopt en welke 'passende' maatregelen je moet nemen. Bij het beveiligen van vertrouwelijke informatie gaat het er om of de organisatie zich bewust is van de risico's. Dan kan de organisatie bepalen of zij dit risico accepteert of dat ze maatregelen moeten nemen.

INSTALLEREN MALWARE

Een kwaadwillende cliënt kan malware op de computer installeren. Deze situatie zal niet zo gauw voorkomen, omdat een cliënt die een afspraak maakt er niet van uit kan gaan dat de specialist wordt weggeroepen en hij het scherm niet vergrendelt. Een risicoanalyse zal dit moeten uitwijzen. ■

André van Soest is adviseur bij LBVD Informatiebeveiligers, www.lbvd.nl