Frank Brokken / f.b.brokken@rug.nl

Elektronisch patiëntendossier

Frank Brokken is security manager bij het CIT. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

Deze bijdrage is eerder (20 juli 2009) gepubliceerd in de Volkskrant.

'De Volkskrant' van zaterdag 11 juli j.l. publiceerde het artikel 'Privacy niet gewaarborgd met papieren dossier'. In het artikel staat, kort samengevat, de stelling verkondigd door Andy Wiesenthal, directeur informatievoorziening van Kaiser Permanente, dat de privacy van patiënten door een elektronisch patiëntendossier (EPD) even goed wordt gewaarborgd als door een papieren dossier. Hij staat niet alleen met die stelling. Judy Faulkner, directeur van Epic Systems dat het EPD levert, is het met hem eens.

Discussiebijeenkomst

Ik ben niet verbaasd wanneer een verzekeringsmaatschappij en een softwarefabrikant hun eigen producten aanprijzen. Ik zou de voordelen ook breed uitmeten: gemak en leesbaarheid van de informatie, maar vooral de toegankelijkheid van het dossier worden als grote pluspunten genoemd.

Maar is het niet zo dat wanneer de vos de passie preekt de boer op z'n ganzen moet passen? Zou het echt allemaal zo mooi zijn als het wordt voorgeschoteld? Vanuit medisch perspectief is dat vast wel het geval. Maar het is moeilijk de inhoud van het artikel op waarde te schatten zolang niet goed is vastgelegd wat nou eigenlijk met 'privacy' wordt bedoeld.

Ik ga me niet branden aan een definitie van privacy, maar interpreteer privacy in dit verband losjes als het voorkomen dat medische gegevens ter beschikking komen aan personen of instanties die daarvoor niet uitdrukkelijk toestemming hebben gekregen. Iets anders geformuleerd: wie geen inzage had in het papieren dossier dient dat ook niet te hebben in het EPD. En daarmee kom ik dan op het terrein van de informatiebeveiliging. Is het EPD in dezelfde mate beveiligd als het papieren dossier? Enige tijd geleden was ik aanwezig bij een discussiebijeenkomst over het EPD in Groningen. Een van de sprekers was een arts die ook enthousiast het EPD aanprees en wist te vertellen dat de beveiliging van het EPD prima was geregeld. Zou dat echt zo zijn?

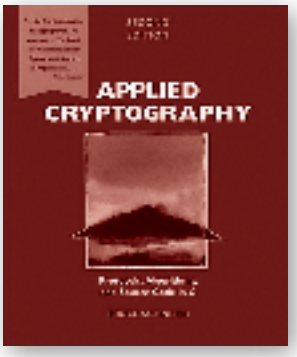
Yes we can

Even terug naar het papieren dossier: volgens het artikel gaat de beveiliging van het papieren dossier niet verder dan een paperclip en stempel 'vertrouwelijk' op een enveloppe. Dat is in ieder geval wat, maar het houdt natuurlijk niet over. De vraag rijst of dat mapje met bijbehorende paperclip dan ook eenvoudig door derden kan worden ingezien. Een willekeurige map kan wellicht wel eens uit een afdelingsbalie van een ziekenhuis worden ontvreemd. Maar het blijft een toevallig gevonden dossier.

Bij een geforceerde inbraak ligt dat uiteraard iets anders. Wie inbreekt in of zich anderszins geforceerd toegang verschaft tot een archief, kan ongetwijfeld alle daarin opgeslagen informatie vinden, kopiëren en meenemen. Dat is in het verleden in Nederland al wel eens gebeurd.

Laten we ons nu eens op de beveiliging van het EPD richten. Een beetje geschiedenis: aan het eind van de jaren negentig publiceert Bruce Schneier een prachtig boek: 'Applied Cryptography' (Wiley) waarin hij de dan bekende en beschikbare mathematische technieken om elektronische data te beveiligen op een rijtje zet.

Deze technieken zijn nu, zo'n tien jaar later,



nog echt niet verouderd en wie nu elektronisch zijn of haar rekeningen betaalt, maakt 'achter de schermen' gebruik van precies die technieken en methodes die Schneier beschreef. Schneier zelf heeft geruime tijd daarna gemeend dat het probleem van de beveiliging hiermee wel was opgelost. 'Yes, we can', maar dan in technisch opzicht.

Achterdeurtjes

Helaas blijkt het iets anders te lopen. Rond 2003 realiseert Schneier zich dat de achterliggende wiskunde prima is, maar dat er veel meer aan de hand is. Fouten in software en kwaadaardige software leiden tot achterdeurtjes die door hackers kunnen worden gebruikt om zich toegang te verschaffen tot computers en hun programmatuur, waaronder het EPD. In Secrets and Lies (Wiley) noemt hij een paar bronnen van dergelijke fouten:

De wiskunde is weliswaar OK, maar computerprogramma's zijn geen wiskunde. Veruit de meeste programma's worden door mensen gemaakt. Mensen maken fouten. Naar schatting en herhaaldelijk ondersteund door resultaten van onderzoek zit er een ernstige fout in elke paar honderd regels programmatekst. Zo'n ernstige fout is dan vaak weer een opening voor misbruik door een hacker. Een beetje programma bestaat al snel uit vele duizenden regels programmatekst. Maar het is niet alleen het deel van een EPD dat voor de beveiliging zorgt dat tot problemen kan leiden.

Programma's die in computers zijn geïnstalleerd, draaien allemaal onder regie van een besturingssysteem, zoals (meestal) Windows. Een besturingssysteem is ook een programma, dat vaak uit miljoenen regels code bestaat. Ook daar zitten dan weer fouten in waardoor het EPD indirect kwetsbaar wordt. Dit is geen theoretisch probleem: vrijwel dagelijks worden er nieuwe fouten in besturingssystemen gevonden en gepubliceerd.

Er is meer: wilt u een relatief veilige computer? Knip dan de draad van de internetverbinding door. Dat doet natuurlijk vrijwel niemand. De computer moet immers ook mail kunnen versturen, en we moeten allemaal kunnen internetten. Ook daarbij worden weer programma's gebruikt die op zich niks met het EPD te maken hebben, maar die zelf ook fouten kunnen herbergen die ook weer toegangsroutes tot het EPD kunnen openen.

En dan hebben we, last but not least, de gebruiker zelf. De goede, oude gebruiker die vindt -net zoals sommige mensen dat met auto's hebben- dat de computer 'het gewoon moet doen' en met een gerust hart van alles en nog wat downloaden van het internet en in hun computer installeren. Helaas kan dat ook betekenen dat de gebruiker, al dan niet bewust, programma's installeert die opnieuw een achterdeurtje naar het EPD kunnen openen.

Kortom, ook al zou het EPD op zich veilig zijn (wat zeer waarschijnlijk niet het geval is), dan nog zijn er vele manieren waarop kwaadwilligen zich toegang kunnen verschaffen tot de computer die wordt gebruikt om het EPD te raadplegen.

Doordat niemand en niks specificaties voor software vastlegt, kan iedereen maar aanboeren wat-ie wil. En dat gebeurt. Time to market wordt belangrijker dan kwaliteit en veiligheid. Zo werkt dat, totdat we gedwongen worden ons gedrag te veranderen. En dat is in de computerwereld echt nog niet het geval.

ISO-normering

Ik geloof niet zoveel van de uitspraken van Wiesenthal en Faulkner. Ze zijn zelf belanghebbenden en ik wil het analyserapport nog wel eens zien waaruit blijkt dat het EPD echt zo veilig is (als een papieren dossier).

De crux zit 'm in het inzicht van Bruce Schneier: wil je komen tot beveiliging, dan moet dat ook op het niveau van de programmatuur worden afgedwongen. Wie beroerde software levert, krijgt een boete of intrekking van de productielicentie. Net zoals er ISO-normen zijn voor bedrijven dienen ISO-normen voor software te worden ingevoerd. Organisaties als ziekenhuizen dienen op hun beurt aansprakelijk te kunnen worden gesteld voor het gebruik van ondeugdelijke (lees: ongecertificeerde) software.

Zover zijn we nog lang niet. Voorlopig kan elke grappenmaker die hacken tot hobby heeft en zich in een uithoek van de wereld (of hier om de hoek) bevindt met een beetje moeite inbreken in een computer. Ook die waarop het EPD kan worden geraadpleegd. Dat zijn niet een paar duizend potentiële diefjes van een papieren dossier, dat zijn miljoenen al dan niet georganiseerde hackers die voor de lol of met financieel gewin in het achterhoofd een slaatje menen te kunnen slaan uit het EPD.

Het EPD net zo veilig als het papieren dossier? De toegankelijkheid van het EPD wordt als groot pluspunt genoemd. Maar toegankelijkheid voor wie? Als de vos de passie preekt, boer pas op je ganzen....

Frank B. Brokken
Verliest wel zijn haren, maar niet zijn streken...