ORDRE DES MEDECINS
CONSEIL NATIONAL
ORDE DER ARTSEN
NATIONALE RAAD

Veiligheid van de via Internet verzonden gegevens

Doc	a084020
Publicatiedatum	20/02/1999
Origine	NR
Thema's	Informatica Beroepsgeheim

Een provinciale raad doet de Nationale Raad een aantal vragen geworden van het X forum vzw over medische gegevens en telematica:

1. mogen artsen, uiteraard met inachtneming van de deontologische voorschriften en waarborgen in verband met het beroepsgeheim, onderling medische gegevens uitwisselen via Internet en/of data raadplegen die betrekking hebben op medische gegevens van patiënten die door hen behandeld worden?
2. er bestaan op dit ogenblik internationaal erkende en gewaardeerde pakketten (o.a. PGP) die alle waarborgen bieden betreffende de encryptering van de uitgewisselde gegevens. Mogen deze pakketten gebruikt worden voor het bewaren en uitwisselen van medische gegevens, zoals onder vraag 1 beschreven?
3. genoemde encrypteringspakketten werken met een dubbele sleutel, een (geheime) private sleutel en een publieke sleutel die best zoveel mogelijk verspreid wordt. Het is een goede gewoonte en een bijkomende waarborg om de echtheid van deze publieke sleutel te laten certifiëren door een betrouwbare partij. Is de Orde van geneesheren bereid om deze rol op zich te nemen ofwel volledig (door zelf te certifiëren) ofwel gedeeltelijk (door dit werk aan een andere door haar erkende betrouwbare partij over te laten)?

Daarnaast stelt de provinciale raad de vraag of er via Internet vertrouwelijke medische gegevens mogen uitgewisseld worden.

Antwoord van de Nationale Raad:

De Nationale Raad onderzocht in zijn vergadering van 20 februari 1999 uw brief van 6 januari 1999 betreffende de uitwisseling van vertrouwelijke medische gegevens via Internet, alsook van de documentatie die erbij gevoegd was.
: De Raad heeft het genoegen u ingesloten een nota te bezorgen over de veiligheid van de via Internet verzonden gegevens.
In verband met de vragen die het Medisch Discussieforum voorlegt, worden de volgende antwoorden geformuleerd :

1. de uitwisseling van gegevens via Internet dient te gebeuren overeenkomstig de instructies opgenomen in de adviezen van 16 april 1994 en 22 april 1995.
2. de programma's die gebruik maken van een asymmetrische codering voor de uitwisseling van de gegevens en deze die gebruik maken van een symmetrische codering voor de bewaring van de gegevens bieden een afdoende bescherming afhankelijk van het soort van algoritme en van de lengte van de sleutels waarvan gebruik wordt gemaakt, alsook van de eerbiediging van de aanbevolen beveiligingsmaatregelen. In de huidige omstandigheden bieden de RSA-sleutels

van minstens 1024 bytes bevrediging op het gebied van beveiliging
3. zoals reeds eerder werd meegedeeld (advies van 22 april 1995 -1.6-), kan de Orde der geneesheren de taak van de certificatie van de publieke sleutels op zich nemen.

Nota betreffende de veiligheid van de via Internet verzonden gegevens :

Het is algemeen bekend dat gegevens die circuleren op Internet gelezen kunnen worden door personen die geen belang hebben bij de uitwisseling van deze gegevens. Daarnaast staat sinds lang vast dat deze zelfde personen toegang kunnen krijgen tot de inhoud van de computerdiskettes wanneer de computers aangesloten zijn op het telefoonnet. De bescherming van de toegang met behulp van paswoorden is een illusie geworden. De codekrakers (Hackers) maken er een spelletje van om, soms aan de hand van uiterst krachtige technische middelen, de blokkades die individuen, bedrijven en instellingen uitzetten om zich te beschermen, te achterhalen en te omzeilen.
De Chaos Computer Club heeft schurken voortgebracht die werken voor het grove banditisme, de maffia's, de Staten ! Afrekeningen zijn geen uitzondering, sommige individuen hebben een stevige reputatie opgebouwd dankzij hun sterke staaltjes van decodering, sommigen werden opgesloten in de gevangenis, anderen zijn overleden in verdachte omstandigheden (1), velen lopen nog rond.

De krachttoeren die de hackers uithalen dienen niet alleen om hun honger naar het belangeloos kraken van codes te stillen.

Idustriële spionage wordt toegepast op grote schaal en met behulp van middelen die in verhouding staan tot de macht van de concurrerende bedrijven. Recente voorbeelden, onder meer in de automobielindustrie, illustreren dit. Deze praktijken blijken evenwel frequent toegepast te worden. Soms volstaat een eenvoudige controle van de bestemmelingen van de elektronische post om commercieel of technisch nuttige informatie te vergaren.

Dankzij de enorme werkkracht van de computermiddelen zijn de aanleg van bestanden en het beheer van databanken er heel wat makkelijker op geworden en binnen het bereik van iedereen. We konden zien hoe er alsmaar meer databanken opgericht werden in de gezondheidssector, door artsen, ziekenhuizen, verzekeringsmaatschappijen, enz. In ons land werd een Kruispuntbank voor de gegevens van de sociale zekerheid in het leven geroepen.
Er werd een Europese wetgeving opgesteld tot bescherming van de persoonlijke levenssfeer (2). België zette deze richtlijn om in de wet van 8 december 1992 (3). Ofschoon er een wettelijk kader bestaat voor de bescherming van de persoonsgegevens, wordt nog vaak en agressief jacht gemaakt op deze gegevens. Door de veralgemening van de informatica en van de elektronische gegevensuitwisseling kan immers toegang verkregen worden tot privé-gegevens, niet alleen in de computers waarin ze opgeslagen zijn, maar ook terwijl ze circuleren op de netwerken !
Hun bescherming is dan ook cruciaal geworden.

Sinds jaar en dag trachten de Staten achter de geheimen te komen van hun buurlanden. Dit komt het duidelijkst tot uiting in de activiteiten van de geheime diensten. Al heel lang maken de beveiligingssystemen gebruik van codering van de gegevens om ze onleesbaar te maken. Dit ligt aan de oorsprong van de codediensten in de ambassades.

Diegene die een niet te doorbreken code heeft, is de winnaar. Het avontuur van de Enigma-machine die ontwikkeld werd in de laatste oorlog is ons welbekend. Eens te meer is het de informatica die, door haar vermogen en rekensnelheid, de wiskundigen

de mogelijkheid geboden heeft om voor de codering algoritmen op te stellen. Deze worden alsmaar complexer en langer, worden op een willekeurige wijze gekozen en staan algemeen bekend als een totale bescherming biedend.
Zoals dat hoort, worden vervolgens alsmaar krachtigere computers ingezet om de code te trachten doorbreken. En het blijft maar escaladeren ... Beveiligingsfirma's organiseren zelfs wedstrijden tussen codekrakers om gekende algoritmen uit te testen en hun eventuele breekbaarheid aan te tonen (4).
Daarnaast publiceert de pers bravourestukjes van jonge genieën in de wiskunde die algoritmen uitwerken die zogezegd ondoorbreekbaar zijn, maar waarvan wij het latere lot niet kennen (5).

In werkelijkheid is het belangrijk dat de Internetgebruikers behoorlijk ingelicht worden over wat zij doen en over de risico's die zij lopen **afhankelijk van het soort communicatie dat zij verwezenlijken**.

De gevaren zijn immers verschillend wanneer het gaat over het toegankelijk laten van een databank op een site, het doorgeven van aankoop- of bankorders of het doorzenden van gegevens via een postserver aan een geïdentificeerde persoon.

Beweren dat Internet zo lek is als een mandje klopt volledig. Het is trouwens de toegankelijkheid ervan die Internet zo aantrekkelijk maakt. De regel nooit het nummer van bankkaarten of van andere kaarten aan het netwerk toe te vertrouwen, wordt bij elke aanvang van een transanctie in herinnering gebracht op het scherm. Net zo min als men aan de post persoonlijke brieven toevertrouwt in een open omslag of op een briefkaart, mag men natuurlijk geen enkel schriftelijk document van enig persoonlijk belang toevertrouwen aan Internet. Anders loopt men immers het risico dat niet alleen de postbode maar de hele wereld zijn geheimen kent.

Elk persoonlijk gegeven dat circuleert op het net moet onleesbaar worden gemaakt voor diegenen die er geen belang bij hebben.

De Europese Organisaties steunen uitdrukkelijk de noodzaak van toegangscontroles, cryptografie, certificatie van de sleutels en digitale ondertekening (6). Er wordt werk gemaakt van de standaardisering van de procedures (7). In België staat de wet van 19 december 1997 het gebruik van cryptografie onbeperkt toe (8).

De Nationale Raad heeft tot nu toe niet toegelaten dat databanken met medische gegevens over rechtstreeks of onrechtstreeks identificeerbare personen permanent op Internet blijven staan.
In dit opzicht werden initiatieven ontmoedigd met betrekking tot de terbeschikkingstelling van medische dossiers, zelfs al zijn ze beschermd door toegangscodes die gecontroleerd worden door de betrokken patiënten, dienstdoende artsen, enz.

Alleen over de uitwisseling van medische gegevens tussen artsen via een server die dienst doet als brievenbus werden regels opgesteld (9, 10, 11, 12).
De Nationale Raad heeft de provinciale raden gelast de overeenkomsten na te kijken tussen artsen en leveranciers van diensten en te controleren of de instructies in verband met de beveiliging van de gegevens nagekomen worden.

In verband met deze overeenkomsten brengen wij enkele werkingsmodaliteiten in herinnering die duidelijk bepaald moeten worden :

- de server mag voor geen andere toepassingen gebruikt worden dan voor de overdracht van medische gegevens.
- hij mag alleen gecodeerde gegevens bevatten en mag geen toegang hebben tot de sleutels.

- de gegevens die de server bevat dienen automatisch gewist te worden nadat ze opgevraagd werden door de bestemmeling en in elk geval na een korte termijn van maximum 10 of 15 dagen -wanneer deze zijn brievenbus niet geraadpleegd heeft.
- het systeem moet open zijn, m.a.w. toegankelijk voor alle artsen-gebruikers, hetgeen de aanwending van een standaardformaat leesbaar door de gebruikelijke programma 's veronderstelt.
- de beheerder van het systeem is verantwoordelijk voor de controle van de beveiligingsprocedures.

De artsen die gebruik maken van het gegevensuitwisselingssysteem moeten toezien op de eerbiediging van het beroepsgeheim en zijn verantwoordelijk voor de beveiligingsmaatregelen. Dit veronderstelt onder meer dat :

- de codeersleutels door de arts uitsluitend binnen zijn computer aangemaakt mogen worden.
- het gebruikte algoritme voldoende betrouwbaarheidswaarborgen moet bieden rekening houdend met de thans geldende kennis terzake, in het bijzonder wat betreft de lengte van de asymmetrische sleutels (13) en de lengte van het symmetrische gedeelte.
- de publieke sleutels gecertificeerd moeten worden door een vertrouwensmandataris.
- de geheime sleutel beveiligd moet zijn door een paszin, die regelmatig gewijzigd wordt afhankelijk van de omstandigheden, en bewaard moet worden op een afzonderlijke drager wanneer het gaat over een terminal die door verschillende gebruikers wordt gebruikt.

De Nationale Raad heeft voorgesteld dat hij de publieke sleutels certificeert. Dit houdt in dat hij er zijn elektronische handtekening op plaatst en aldus de authenticiteit van deze sleutel waarborgt.

De provinciale raden hebben onder meer tot taak een controle uit te voeren van de vertrouwelijkheidswaarborgen die geboden worden door de overeenkomsten tussen artsen en leveranciers van elektronische brievenbussen. Dit houdt in dat zij de betrouwbaarheid van de algoritmes beoordelen en nagaan of de door de Orde voorgestane beveiligingsmodaliteiten vervuld worden.

Het probleem van de certificatie van de sleutels die toekomen bij de provinciale raden rijst op nationaal niveau.

Het blijkt onontbeerlijk een structuur in het leven te roepen voor de uitwisseling van informatie tussen de provinciale raden en de Nationale Raad om de gecertificeerde sleutels door te zenden, informatie te verstrekken over de goedgekeurde overeenkomsten en over de vooruitgang van het onderzoek aangaande de technieken, enz. Een dergelijk hulpmiddel zou uitstekend kunnen functioneren via elektronische briefwisseling en enkele zeldzame vergaderingen vergen.

Tot besluit kunnen wij stellen dat de vertrouwelijkheid van de gegevens die uitgewisseld worden via Internet perfect verzekerd kan worden via een coderingssysteem waarbij gebruik wordt gemaakt van betrouwbare methoden waarvan de degelijkheid overvloedig bevestigd wordt door de wetenschappelijke literatuur (14, 15) .

Referenties :

1. http:\\www.lalettre.com/nexs/jan/201099_4.html
2. Richtlijn 95/46/EG/ van 24 oktober 1995

3. Wet van 11 december 1998 houdende omzetting van Richtlijn 95/46/EG
4. DES Challenge III, RSA Laboratories, http://www.rsa.com/rsalabs/des3/index.html
5. Magee, A. Teenager cracks e-mail code. The Times of London, 13 Jan. 1999
6. Permanent Comité van de Europese Artsen : Security in Clinical Information Systems, BMA paper, 24/08/1998
7. Comité Européen de Normalisation CEN/tc 251/wg6
8. Wet van 19 december 1997
9. Elektronisch brievenbussysteem - Laboratoria. Tijdschrift Nationale Raad 63-20
10. Telematisch gestuurde communicatie van de briefwisseling. Tijdschrift Nationale Raad 63-22
11. Elektronische brievenbussystemen. Tijdschrift Nationale Raad 65-22
12. Elektronische Post - Medisch geheim. Tijdschrift Nationale Raad 69-13
13. Dragan, R. Encryption. PC Magazine June 9, 1998
14. Toward An Electronic Patient Record '95 Orlando, F. March 1995
15. Barber, B. Treacher, A. & Louwerse C.P. Towards Security in Medical Telematics. IOS Press. Amsterdam 1996

Bovenstaande nota wordt ook overgemaakt aan de andere provinciale raden.