De beveiliging van de toegang tot gegevens is vaak een probleem omdat niet duidelijk is wie wat mag. Ook is niet altijd duidelijk wie eindverantwoordelijk is voor het bepalen van de bevoegdheden. Als dan ook nog een deel van de activiteiten wordt uitbesteed, is de chaos compleet. Het hoogste management zal moeten ingrijpen.

Gegevensbeveiliging aan alle kanten lek

Door: Jaap van der Wel en Nanne Homma, nabewerking Ernst Mellink.

De gegevenstoegang van geautomatiseerde systemen is vaak slecht beveiligd. Dit is een serieus probleem waarvoor veel directies beducht zijn omdat het maar niet lukt dit gedegen op te lossen. Eén van de gevolgen is privacyverlies. Als bijvoorbeeld gegevens over kredietpositie en betaalgedrag ruim toegankelijk zijn binnen de organisatie, vergroot dit de kans dat een malafide medewerker die in handen krijgt en doorspeelt. Zwakke toegangsbeveiliging bezorgt administratieve automatisering een slechte naam, een reden voor
directies om terughoudend te zijn met ambitieuze automatiseringsplannen. Zwakke toegangsbeveiliging kan ook leiden tot een risicomijdende opstelling van directies door elektronische communicatie met de buitenwereld - bijvoorbeeld email - te blokkeren. Het lagere rendement van ICT wordt dan op de koop toe genomen. Uitbesteden van bedrijfsactiviteiten compliceert het vraagstuk van toegangsbeveiliging. Arbo-artsen bijvoorbeeld, die vaak op het kantoor van hun opdrachtgever werken, kunnen gewoonlijk de eigen bedrijfsgegevens niet benaderen.

Oorzaak

De oorzaak van de problemen is niet de beveiligingstechniek want die is de afgelopen jaren juist beter geworden. Voor bedrijfssystemen zijn er systemen voor Public Key Infrastructuren (PKI), firewalls etc. En encryptie schermt de gegevens van een laptop beter af dan het slotje van de leren aktetas van vroeger.
De oorzaak is gewoonlijk een combinatie van beheersproblemen. Allereerst is vaak onoverzichtelijk wie wat mag, omdat de rechten van medewerkers zijn geregistreerd in verschillende systemen. Ook moeten vaak te veel verschillende administratieve functies worden beheerd, met als gevolg te veel werk.

Daarnaast weet de beslisser vaak niet wie wat mag, omdat het toegangsbeheer voor hem is weggestopt in systeem tabellen of firewallinstellingen. Hij delegeert het werk daarom maar aan mensen die dat wel snappen en kijkt er niet meer naar om. Een volgend punt is dat de functies van informatiesystemen vaak niet aansluiten op de behoeften van de organisatie. Dat is het geval als de meeste autorisaties toegang geven tot maar weinig gegevens (veel werk voor autorisatiebeheer) of tot overvloedig veel. Informatiesystemen sluiten ook niet aan op de behoeften van de organisatie als functiescheiding onvoldoende mogelijk is, wat weer kan leiden tot ongecontroleerde inzage van systeembeheerders in vertrouwelijke bedrijfsgegevens.
Organisaties die het beheer van toegangsrechten willen verbeteren, lopen ook tegen de vraag op wie eindverantwoordelijk is om vast te stellen welke medewerker van de organisatie welke gegevens mag inzien of wijzigen. De vraag komt aan de orde bij het ontwerp van toegangsbeveiliging. Dan moet de hoeveelheid gegevens waaraan de gemiddelde autorisatie toegang geeft, worden afgewogen tegen de aanpassingkosten van het informatiesysteem en de beheerskosten.

Hulpmiddelen voor toegangsbeveiliging

Het begrip Role Based Acces Control (RBAC) speelt een belangrijke rol bij toegangsbeveiliging. Het is een methodische aanpak die afkomstig is van het Amerikaanse National Institute of Standards and Technology (NIST). Vrijwel alle fabrikanten hebben hierop hun software voor toegangsbeveiliging gebaseerd. RBAC gaat uit van 'rollen', gestandaardiseerde takenpakketten die voor meerdere gebruikers geschikt zijn. Aan die 'rollen' worden
bijbehorende onderdelen van het geautomatiseerde systeem verbonden - vaak vele tientallen. De voordelen van deze methode zijn werkbesparing en de mogelijkheid om zonder specialistische ICT-kennis de toegangsrechten te laten beheren. Voor meer informatie zie:
http://csrc.nist.gov/rbac

Vanuit de software voor toegangsbeveiliging worden regelmatig de applicatiesystemen gevoed met actuele toegangsrechten. De gebruiker moet nog wel op ieder systeem afzonderlijk inloggen. Deze logins kunnen worden overgenomen door software voor Single Sign-On (SSO) waardoor de gebruiker maar eenmaal door een authenticatieproces heen hoeft. SSO kan goed gecombineerd worden met RBAC. Met SSO hoeven gebruikers minder passwords te onthouden en bellen daardoor minder vaak de helpdesk voor een 'password reset' met als gevolg meer comfort en werkbesparing.

Complicatie

De meest basale situatie is de organisatie met beperkte hoeveelheid vertrouwelijke gegevens. De organisatietop bestuurt de toegang en delegeert in de praktijk die taak naar het hoofd financiële administratie voor de toeghang tot de boekhouding, naar het hoofd personeelszaken voor de personeels-administratie etc. Een complicatie ontstaat als de omgeving van een organisatie veel over heeft voor de gegevens die zijn geregistreerd. Dat is bijvoorbeeld het geval bij banken, de Belastingdienst of bij opsporingsdiensten. De directie van dergelijke organisaties doet er dan goed aan om het toekennen van bevoegdheden strikt door te voeren, door bijvoorbeeld de toegang van systeembeheerders tot grote concentraties van vertrouwelijke gegevens zo veel mogelijk te blokkeren.

Beheersproblemen

1 Het is onoverzichtelijk wie wàt mag
In veel organisaties zijn verschillende Windows- en Unix-servers, mainframes en mid-rangesystemen aanwezig in het netwerk. Elk platform heeft zijn eigen systeemspecialist die het toegangsbeheer inricht. Sommige (of de meeste?) applicatiesystemem hebben eigen gebruikersbeheermodules met eigen databases die alleen via een eigen terminal of eigen software programma benaderbaar zijn. Iemand die een toegangsrecht wil, loopt de kans om van de ene afdeling naar de andere en weer terug te worden gestuurd. Bij hoeveel organisaties duurt het niet weken voordat een nieuwe medewerker tot al zijn applicaties toegang heeft? Als iemand van afdeling verandert, behoudt hij in de praktijk gewoon de toegangsrechten voor het werk van de vorige afdeling.
Aanpak
Het is verstandig om alle gegevens over gebruikers samen te brengen in één centrale directory, zodat persoonsgegevens slechts één keer hoeven te worden ingevoerd. Beheerders van toegangsrechten kunnen dan in één oogopslag zien welke toegangsrechten iemand heeft, en dus ook welke hij niet meer nodig heeft. Er is wel een scheiding nodig tussen persoonsgegevens die publiekelijk bekend mogen zijn en geheime gegevens die de toegang tot systemen mogelijk maken van personen of groepen van personen.
Het is gewoonlijk niet haalbaar om de 100% oplossing te vinden die alle applicaties en platformen ondersteunt, en waarin alle functies, rollen en taken worden ingepast. Resultaat bereikt men met een stapsgewijze aanpak, beginnend bij de organisatiedelen waar de problematiek het grootst is.

2 Te veel functiebeschrijvingen
Tal van organisaties hebben veel functieomschrijvingen. Zoals bijvoorbeeld een organisatie met een personeelsbestand van 30 à 40 duizend mensen en ongeveer 15 duizend functie/taakomschrijvingen en circa 20 duizend systeemobjecten. Als voor al deze functies de specifieke toegang moet worden geregeld, ontstaat er een onontwarbare knoop. Gewoonlijk blijkt dat ook als de beheersgegevens worden gecentraliseerd.
Aanpak
Het lijnmanagement kan het beste de werkzaamheden van de organisatie in een gestandaardiseerde rollen/takenset beschrijven en aan medewerkers toewijzen. Deze rationaliseringsslag kan wel veel energie kosten omdat het nogal wat vereist: het slopen van verworven koninkrijkjes, het afbouwen van opgebouwde gewoonterechten en het opzij zetten van misplaatste gevoelens van onmisbaarheid bij medewerkers.
Daarna kunnen lijnmanagers gemakkelijker de toegangsrechten up-to-date houden bij iedere functieverandering of ontslag van medewerkers. Zij zijn daarvan immers beter op de hoogte dan de afdeling ICT.

3 Regels bedrijfsprocessen niet aangepast
De reikwijdte die sommige bedrijfsprocessen hebben gekregen is in de loop der jaren gegroeid. Naarmate men meer gebruik ging maken van netwerktechnologie zijn meer systemen gekoppeld en zijn meer mogelijkheden toegevoegd. Soms overschrijden die mogelijkheden de bedrijfsgrenzen. Door die groei zijn vaak ook de toegangsrechten van gebruikers uitgebreid. Het is echter de vraag of na een fusie van twee verzekeraars, en een reorganisatie, het wel nodig is dat gebruikers van de nieuwe hypotheekafdeling ook inzage hebben in de medische gegevens van de ziektekostenpolis.
Aanpak
Systemen moeten aansluiten bij de bestaande omgeving en procedures. Een verfijnde toegangsregeling in het systeem kan niet anders dan met maatwerk gerealiseerd worden. Realisme op dit punt in projecten versterkt de geloofwaardigheid en kans van slagen.

4. De beslisser weet niet wie wat mag
Het management is verantwoordelijk voor toegangsrechten maar beschikt vaak niet over het inzicht wie wat (wellicht: te veel) kan; zeker niet als in firewalls allerlei extra deurtjes zijn aangebracht voor medewerkers buiten de organisatie en voor ingehuurde krachten binnen de organisatie. Dergelijke informatie is meestal te technisch en dus voor hen niet inzichtelijk.
Aanpak
Het management moet een duidelijk, compleet overzicht van toegangsrechten, voor medewerkers van hun afdeling krijgen. Om het management nauwer bij het beheer te kunnen betrekken is het noodzakelijk om de beheerapplicatie gebruik te laten maken van voor het management begrijpelijke termen die een duidelijke relatie hebben met het dagelijks zakendoen. Er zijn twee vormen:
- Toegang op basis van beleidsregels die hoog in de organisatie zijn vastgesteld, zoals inzicht voor de directie in alle personeels gegevens. Deze regels worden slechts sporadisch aangepast, en zullen dus geen grote hoeveelheid beheerswerk vergen.
- Toegang op basis van rollen. Deze vorm is afhankelijk van veel sneller wisselende zaken zoals organisatie-indeling, afdelingen, functiewijzigingen etc. en zal dus meer beheerswerk vergen. Beheerswerk is vooral belangrijk in organisaties waar steeds andere mensen te maken krijgen met dezelfde gegevens, zoals dat het geval is in de zorg of als vaak met projecten wordt gewerkt.
Producten die voor applicaties en firewalls de toegangsregels uit businessregels kunnen vertalen, zijn beschikbaar en kunnen door het lijnmanagement zelf worden gebruikt bij het beheer van toegangsrechten.

5. Onvoldoende functiescheiding bij toegangsbeheer
Het toegangsbeheer wordt in veel organisaties uitgevoerd door technisch specialisten. Zij kunnen zichzelf allerlei toegangsrechten toekennen of op een andere manier gegevens inzien, zonder dat iemand dat in de gaten heeft.
Aanpak
Door de invoering van een systeem voor Role Based Access Control (zie eerder kader) kunnen het technisch systeembeheer en het beheer op de toegangsregels van elkaar gescheiden worden. Deze aanpak is ook geschikt om het aantal beheerhandelingen terug te dringen indien het management het aantal rollen in de organisatie beperkt. Bij zeer hoge niveaus van geheimhouding, kan ook encryptie van de gegevens worden overwogen, waardoor zelfs voor systeembeheerders de gegevens niet meer te raadplegen of te veranderen zijn.

De eindverantwoordelijkheid voor de toegang tot gegevens in de zorg heeft een eigen variant. Volgens de regels van het College Bescherming Persoonsgegevens bepaalt niet de organisatietop maar de patiënt wie toegang heeft tot zijn medische gegevens, voor zover dat niet ongewenst is wegens bijvoorbeeld psychische problemen. Uiteraard heeft de behandelend arts met de organisatie om hem heen ook toegang tot gegevens van zijn patiënten. Binnen de zorg worden vertrouwelijke gegevens steeds meer geconcentreerd en voor veel zorgmedewerkers steeds gemakkelijker bereikbaar, bijvoorbeeld door het ontsluiten van papieren patiëntendossiers op het ziekenhuisnetwerk. Om de eisen van discretie, te stellen aan de medewerkers, niet te hoog te laten oplopen, is verfijnen van de toegangsbeveiliging noodzakelijk. Dat kan bijvoorbeeld het geval zijn als steeds meer apothekers onderling 'slikgegevens' uitwisselen, waardoor steeds meer vertrouwelijke gegevens onder handbereik van steeds meer apothekers en hun assistenten komen.

Verbeteren

Verbeteren van de toegangsbeveiliging vereist opheffen van de beheersproblemen (zie kader). Verbeteren vereist de steun van het hoogste management en die steun komt alleen als voordelen, aanpak en kosten duidelijk zijn. De inventarisatie van voordelen maakt allereerst concreet de huidige kring van medewerkers met toegang tot vertrouwelijke gegevens en gaat na tot welke kring die kan worden verkleind zonder dat onacceptabele hinder ontstaat. Een tweede voordeel is een groter rendement van ICT door de elektronische deuren die tot nu toe gesloten waren, op een gecontroleerde manier open te zetten. Een derde voordeel is lagere beheerskosten door minder beheerswerk. De aanpak moet duidelijk maken wie bevoegd is om toegang te verschaffen (het lijnmanagement) en hoe verbeterde beheersprocedures worden geïmplementeerd. Uit de aanpak kunnen de benodigde investeringen worden afgeleid. Als die te hoog uitvallen, dan moet de aanpak worden beperkt tot een deel van de organisatie of de probleemvelden.
Tijdig bijstellen van ambities voorkomt dat een pad wordt ingeslagen dat gaandeweg onhaalbaar blijkt te zijn. Goed is goed genoeg en legt een basis voor latere, verdere verbetering.

De auteurs

Mr. drs. J.A. van der Wel is directeur van Comfort-IA.
Ing. N.L. Homma is security-consultant bij Bull Nederland.

Nabewerking door Ernst Mellink, ICT Architect bij More-Secure Consultants BV.

Dit artikel is eerder geplaatst in de AUTOMATISERINGS GIDS van 05 september 2003 (nummer 36) pagina 17, uitgebracht door Ten Hagen Stam Uitgevers.

Contact:

More-Secure B.V.
Da Costalaan 14
3768 GH Soest
M: +31 (0)6 5357 9338 | F: +31 (0)35-524 7857
E: info@more-secure.nl | W: www.more-secure.nl