

Over scannen en te vrije beschikbaarheid van informatie

Steeds meer papieren archieven komen on-line beschikbaar. Dat is handig want om archiefstukken te raadplegen, is nu een wandeling naar het archief niet meer nodig. Archieven kunnen zelfs 'geoutsourced' worden zoals dat in inmiddels aanvaard Nederlands heet. Ook kunnen gefuseerde organisaties, dat komt in de ziekenhuiswereld bijvoorbeeld veel voor, hun archieven gemakkelijk aan elkaar beschikbaar stellen.

Door Jaap van der Wel

Bij archiefontsluiting hoort ook beheersing van de informatietoegang. Beheersing van de informatietoegang is echter een notoir probleem. Elektronische archieven onderscheiden zich daarmee niet van gewone informatiesystemen, waarvan de gegevens-toegang vaak aan alle kanten lek is. Dat heeft verschillende gevolgen, welke hangt af van de bedrijfstak. In de medische wereld springt privacyverlies als eerste in het oog. In de bankwereld of bij de belastingdienst bieden lekke informatiesystemen meer ruimte dan nodig aan malafide medewerkers. Hoe meer mensen toegang hebben tot financiële gegevens, hoe groter het risico dat iemand een handeltje begint met een onduidelijk bureau voor "handelsinformatie". In iedere bedrijfstak kan de gang van zaken leiden tot een risicomijdende opstelling van directies. Dat uit zich dan bijvoorbeeld in terughoudendheid met ambitieuze automatiseringsplannen. Ook overdreven voorzichtigheid met e-mail en internet komt in tal van organisaties voor. Directies nemen het lagere rendement van ICT-investeringen daarmee op de koop toe.

De oorzaak van de problemen met toegangsbeveiliging is niet de beveiligingstechniek, die is de afgelopen jaren juist beter geworden

met bijvoorbeeld Smartcards en Public Key Infrastructure (PKI). Beveiligingsproblemen worden veroorzaakt door management. Dat heeft onvoldoende oog voor de eisen die de in omvang toenemende informatiesystemen stellen, namelijk beheersing van de toenemende complexiteit van het toegangsbeheer. Te vaak worden beveiligingsoplossingen ad-hoc getroffen waardoor er uiteindelijk een oosterse kashba ontstaat waarin alleen de mensen die er al jaren wonen, de weg kunnen vinden, zie verder het kader over oorzaken.

Een betere beveiliging kan forse investeringen vergen en veel van dit soort projecten lopen halverwege stuk. Dat is alleen te voorkomen door niet teveel hooi op de vork te nemen en de aandacht te beperken tot de belangrijke problemen, zie het kader over oplossingen. Alleen daar waar beveiliging in lijn moet worden gebracht met de eisen, is actie geboden. Beveiligingseisen zijn niet alleen hoger bij grotere organisatieomvang maar ook bij fraude- en privacy gevoelige gegevens. Hierna volgen enkele typerende situaties.

Het meest overzichtelijk is de organisatie met beperkte hoeveelheid vertrouwelijke gegevens zoals een handelshuis. De organisatietop bestuurt de toegang en delegeert in de praktijk die taak naar het hoofd financiële administratie voor de toegang tot de boekhouding, het hoofd personeelszaken voor de personeelsadministratie, 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,



Oorzaken

1 Teveel functiebeschrijvingen

In sommige organisaties is een praktijk ontstaan waarbij de toegangsrechten sterk zijn toegesneden op de individuele medewerker. In deze wildgroei kunnen organisaties met 3.000 medewerkers gemakkelijk 3.000 functie/taakomschrijvingen hebben. Meer is ook mogelijk als medewerkers meerdere functies hebben in het geautomatiseerd systeem zoals één voor gewoon medewerker en één voor ondernemingsraadlid. Als dan het informatiesysteem ook nog eens uit 1000 objecten bestaat (en dat is voor een beetje bedrijfssysteem al snel het geval) dan is de knoop de systeembeheerders niet meer te ontwarren.

2 Functies sluiten niet aan op de behoefte van de organisatie

De functies van informatiesystemen sluiten vaak niet aan op de behoeften van de organisatie. Sommige informatiesystemen geven inzage in alles als men toegang heeft tot dat systeem. Dat is bijvoorbeeld het geval met gescande archieven waarvan de indexgegevens tekortschieten om daarop een fatsoenlijke autorisatie te baseren. Zonder autorisatiemogelijkheden

komen gewone gegevens en uiterst vertrouwelijke op één grote hoop. Soms, zoals in de zorg is dat moeilijk te voorkomen. Gegevens kunnen op onverwachte momenten nodig zijn in een spoedsituatie. In dat geval is een logregistratie van raadplegingen nodig en een procedure om mensen aan te spreken op onnodig raadplegen. In andere gevallen geven individuele autorisaties toegang tot heel weinig gegevens en zijn veel autorisatie instellingen nodig. Dat genereert veel beheerswerk, waarvoor vaak de tijd ontbreekt. In dat geval blijven medewerkers te lang verouderde toegangsrechten houden.

3 Onoverzichtelijk wie wat kan

Het management van een organisatie zou overzicht moeten hebben van de toegangsrechten die iedere medewerker heeft in de geautomatiseerde systemen. Door verschillende oorzaken is dat overzicht vaak niet voorhanden.

- In de praktijk worden toegangsrechten geregeld met vele lijstjes van medewerkers en rechten. Dat komt doordat verschillende toepassingen en systemen, waaronder die voor het elektronisch archief, ieder een eigen registratie heb-

ben voor toegangsrechten. Je kunt dit gemakkelijk herkennen als iemand begint aan een nieuwe functie. Deze medewerker zal dan namelijk een tocht moeten ondernemen langs vele beheersafdelingen voordat hij of zij kan werken op het geautomatiseerd systeem. Ik ken gevallen waarin een dergelijke tocht weken duurt. Als degene weer vertrekt, dan komt er van weghalen van toegangsrechten niets terecht. Zo kunnen de toegangsrechten zich hoog opstapelen bij mensen die wel eens van afdeling veranderen.

- Belangrijke toegangsrechten zitten diep verstopt in de techniek van firewalls, netwerkinstellingen en andere technische zaken. Het management dat wil begrijpen hoe het zit, moet men genoegen nemen met lastig te begrijpen technische beschrijvingen.

4 Onvoldoende functiescheiding bij het toegangsbeheer

Het toegangsbeheer wordt in veel organisaties uitgevoerd door technische specialisten. Zij kunnen zichzelf allerlei toegangsrechten toekennen of op een andere manier gegevens inzien zonder dat het management daarvan weet.

de belastingdienst of bij opsporingsdiensten. De directie van dergelijke organisaties doet er dan goed aan om beveiligingsoplossingen strikt te implementeren. Zo moet de toegang tot grote concentraties van vertrouwelijke gegevens voorkomen worden, ook voor systeembeheerders.

Organisaties in de zorgsector hebben te maken met een eigen variant voor beveiligingseisen. Als hoofdregel bepaalt hier de patiënt, niet de organisatietop, wie toegang heeft tot zijn medische gegevens. Uiteraard heeft de behandelende arts met de organisatie om hem heen ook toegang tot gegevens van zijn patiënten. Juist in de zorgsector is aandacht nodig voor toegangsbeveiliging doordat papieren patiëntendossiers steeds meer beschikbaar komen op computernetwerken. Dat is bijvoorbeeld ook het geval bij apothekers die slikgegevens uitwisselen, waardoor meer apothekers en hun assistenten meer gegevens onder handbereik krijgen. In deze sector is het nodig om te registreren wie de gegevens raadpleegt en deze loggegevens ter beschikking te stellen aan de patiënt die

het betreft. Volgens onderzoek van het Nederlands Patiënten en Consumenten Platform (NPCF) willen patiënten deze procedure.

Aan de slag

Verbeteren van de toegangsbeveiliging lukt alleen met de steun van de organisatietop. Deze steun hangt af van een concreet plan waarin voordelen, aanpak en kosten duidelijk zijn gemaakt. De voordelen bestaan uit een combinatie van verkleinen en vergroten van de toegang tot gegevens en het verlagen van de beheerslasten voor autorisatiebeheer. Veiligheidsvoordeel ontstaat door verkleinen van de bestaande kring van medewerkers met toegang tot vertrouwelijke gegevens tot vlak voor het punt waarbij hinder ontstaat bij het werk doordat gegevens door afscherming geregeld niet meer beschikbaar zijn op het moment dat die nodig zijn. Productiviteitsvoordeel ontstaat door vergemakkelijken of versnellen van de toegang tot gegevens door geregeld nodig zijn. Beperken van de wachttijd op autorisaties na functiewijziging is een voorbeeld, evenals gecontroleerd openzetten van elektronische deuren naar e-mail en internet.

De kosten bestaan uit de benodigde investeringen om de lijnorganisatie waar nodig te standaardiseren / verduidelijken en voor de aanschaf en inrichting van middelen voor het beheer van gegevenstoegang en aanpassing van bestaande software. Als die investeringen te hoog uitvallen moet de aanpak worden beperkt tot een deel van de organisatie of tot één van de informatiesystemen. Tijdig bijstellen van ambities is belangrijk omdat het voorkomt

dat een pad wordt ingeslagen dat gaandeweg onhaalbaar blijkt. Goed is goed genoeg. ■

Mr. drs. J.A. van der Wel (jvdwel@comfort-ia.nl) is directeur van Comfort-IA. Referentie: Informatiesystemen aan alle kanten
lek van J.A. van der Wel en N. Homma (Bull Nederland B.V), Automatisering Gids dd. 5 september 2003.

Overzicht van oplossingen

1 Reduceren van het aantal functiebeschrijvingen

Onder de regie van het lijnmanagement worden de rollen / takensets gestandaardiseerd. Daarop kunnen standaardpakketten worden gebaseerd met toegangsrechten voor het informatiesysteem ("profielen"). Deze rationaliseringsslag is niet altijd gemakkelijk omdat het soms slopen van koninkrijkjes vereist en overdragen van geliefde taken en opgebouwde gewoonterechten.

Na deze stap is de organisatie overzichtelijker en kunnen lijnmanagers al wat gemakkelijker zelf de toegangsrechten up-to-date houden bij iedere functieverandering of ontslag van medewerkers. Zij zijn daarvan beter op de hoogte dan de afdeling ICT of de helpdesk.

2 De toegangsmogelijkheden laten aansluiten bij het dagelijks werk

De aanduidingen voor de toegangsrechten ("Business regels") moeten een duidelijke relatie hebben met het dagelijkse zakendoen. Er zijn twee basisvormen:

Toegang op basis van beleidsregels die hoog in de organisatie zijn vastgesteld, zoals inzicht voor de directie in alle personeelsgegevens. Deze regels zijn weliswaar grofmazig maar hebben als voordeel dat deze slechts sporadisch worden aangepast en daarom weinig beheerswerk vergen.

Toegang op basis van rollen, een vorm die afhankelijk is van organisatieindeling en functies van mede-

werkers. Deze regels maakt een fijnmaziger toekenning van rechten mogelijk maar vereist ook meer beheerswerk. Efficiënte hulpmiddelen voor beheerswerk zijn vooral punt van aandacht in organisaties waar de functieinhoud van mensen vaak wijzigt, bijvoorbeeld als vaak met projecten wordt gewerkt. Vrijwel iedere organisatie heeft te maken met systemen die niet volgens de bovenstaande principes zijn opgezet doordat die in de loop van de jaren zo zijn gegroeid. Dan kan aanpassen van de toegangsregeling tot kostbaar maatwerk leiden. Om dit soort projecten te laten slagen is een projectplanning nodig met een prioriteitstelling waarmee de aandacht wordt beperkt tot alleen belangrijke problemen.

3 Inzichtelijk maken wie wat kan

Overzicht ontstaat door alle gegevens over toegangsrechten samen te brengen in één centrale registratie met een ver-

taalslag van de dieptechnische instellingen. Zo kan, bijvoorbeeld ingeval van schorsing of ontslag, de toegang tot informatiesystemen vlot worden geblokkeerd.

4 Functiescheiding doorvoeren

Door scheiden van het beheer van logische toegangsrechten en het technisch systeembeheer kunnen technici niet zondermeer toegang krijgen tot gegevens. Gegevensencryptie is hiervoor een optie. Vroeger was dit alleen weggelegd voor heel bijzondere gevallen maar tegenwoordig wordt encryptie steeds betaalbaarder. Systeembeheerders zijn vaak afhoudend met gegevensencryptie omdat het dan omslachtig wordt om foutjes te herstellen. Niettemin bepalen niet zij maar het lijnmanagement en de directie de prioriteiten. En foutjes voorkomen door zorgvuldiger werken en testen moet in de plaats komen van gemakkelijk foutjes herstellen.