Naar een nieuw toegangscontrolesysteem

Toegang: meer dan tech

Bij het succesvol en probleemloos functioneren van een toegangscontrolesysteem draait het om meer dan alleen techniek en ICT. Actuele gegevens, heldere werkprocessen op de beheerafdeling en juiste informatievoorziening zijn minstens zo belangrijk voor een goede dagelijkse werking. Frans Visser *

Een moderne organisatie van enige omvang beschikt vandaag de dag over een elektronisch toegangscontrolesysteem met kaartlezers en pasjes. De aanschaf van zo'n systeem is geen sinecure. Vaak ligt de focus daarbij op techniek en ICT, maar in de praktijk blijkt dat ook andere zaken een belangrijke rol spelen voor het probleemloos functioneren van zo'n systeem.
Welke eisen moet een organisatie stellen aan een nieuw elektronisch toegangscontrolesysteem, en wat zijn daarbij belangrijke succesfactoren en valkuilen?

Programma van eisen

Het programma van eisen (PvE) voor een nieuw toegangscontrolesysteem wordt meestal vanuit technisch oogpunt opgesteld en beoordeeld. Met 'technisch' wordt bedoeld dat het nieuwe systeem moet voldoen aan diverse specificaties. Specificaties die meestal worden opgesteld door de afdelingen die bij het inkooptraject betrokken zijn, zoals:

- *FM of Security:* voldoet het systeem aan de eisen vanuit risicoanalyses en kan de beveiliging de toegangen goed aansturen?
- *ICT*: kan het systeem functioneren binnen de ICT-omgeving?
- *Technisch onderhoud:* past het systeem in de bestaande technische infrastructuur c.q. voldoet het aan bepaalde onderhoudseisen?
- *Inkoop:* is de investering - inclusief onderhoudskosten - op termijn verantwoord?

Het is in dit stadium vaak een valkuil om de afdeling die met het systeem gaat werken (vaak is dat de backoffice van facility management of - in grote organisaties - de security-afdeling), niet te betrekken bij het PvE-traject. En dat is een gemiste kans, want juist deze

Gebruik de doelenboom

Hoe leg je de *meer administratieve eisen* die worden gesteld aan het nieuwe systeem, zo concreet mogelijk vast? Dit is een lastige oefening waarbij gebruik gemaakt kan worden van het opstellen van een *doelenboom* *.

Met het opstellen van een doelenboom formuleer je eerst scherp de hoofddoelstellingen van de eigen organisatie. Daarna stel je jezelf per hoofddoelstelling de vraag: wat is daarvoor nodig?
De antwoorden op die vraag schrijf je op, en dan begin je weer met het stellen van dezelfde vraag aan de eerder gegeven antwoorden. Blijf deze stappen herhalen tot je op het niveau bent van concrete administratieve eisen die je kunt stellen aan het PvE. Met de doelenboom 'vertaal' je dus strategische organisatiedoelstellingen naar uiteindelijke operationele eisen aan het nieuwe toegangscontrolesysteem.

** Een doelenboom (prof. van der Dussen, 2001) wordt gebruikt om snel en efficiënt de doelstellingen en bijbehorende prestatiegegevens van de organisatie in kaart te brengen. Het is een geschikt hulpmiddel om de door het management en de interne klanten gewenste duidelijkheid over de relatie tussen doelen, prestaties en middelen tot stand te brengen.*

niek en ICT

beheerafdeling is in staat de eisen te formuleren waar de bijbehorende applicaties aan moeten voldoen om het nieuwe toegangscontrolesysteem in de dagelijkse praktijk goed te laten functioneren.

Dit beheer kan uit verschillende activiteiten bestaan:
» het up-to-date houden van persoonsgegevens (meestal koppelingen met HR-systemen);
» het up-to-date houden van afgegeven autorisaties;
» het verzorgen van rapportages (voor het management;)
» het up-to-date houden van relevante werkprocessen (bijvoorbeeld van de eigen afdeling beheer);
» het beheren van de toegangspassen en de bijbehorende draagmiddelen (uitgifte, ontvangst, voorraad, plaatsing pasfoto's).

Deze backoffice is vaak ook het centrale punt in de organisatie ten aanzien van KWIS-contacten (klachten, wensen, informatie en storingen). Het is raadzaam om de *meer administratieve eisen* die worden gesteld aan het nieuwe systeem, zo concreet mogelijk door de backoffice te laten inventariseren en vast te laten leggen. Daarbij kan een onderscheid worden gemaakt tussen *harde* en *aanvullende* eisen. Een voorbeeld van een harde eis is dat uitgereikte dagpassen aan het eind van een werkdag automatisch gedeactiveerd moeten worden. Een voorbeeld van een aanvullende eis is dat rapportages aangepast moeten kunnen worden aan de eigen huisstijl.

Menig toegangscontrolesysteem bevat verouderde data

Tip 1: Beschrijf eigen werkprocessen

Om de eisen zo volledig mogelijk op papier te krijgen, is het beschrijven van de eigen werkprocessen een goed hulpmiddel. Laat dit werk niet alleen door de backoffice zelf doen (de kans bestaat dat men blijft vastzitten aan vaste denkpatronen!), maar ook door een extern deskundige (is vaak beter in staat processen goed op elkaar af te stemmen en/of efficiënter te organiseren).
Ook is het verstandig om de ICT-afdeling hierbij te betrekken in verband met de mogelijkheden van koppelingen met andere systemen, waardoor bijvoorbeeld toekomstige mutaties van medewerkers automatisch in het toegangscontrolesysteem worden verwerkt.

Vervuiling van data
Menig toegangscontrolesysteem bevat verouderde data. Denk aan medewerkers die niet meer werkzaam zijn bij het bedrijf, autorisaties die niet meer actueel zijn, uitzendkrachten en medewerkers van leveranciers die ooit in het systeem zijn ingevoerd maar nooit zijn afgevoerd, langdurige afwezigheid van medewerkers, et cetera.
Het risico van vervuilde data is dat bepaalde personen ten onrechte toegang tot specifieke ruimten kunnen hebben. Ook kunnen rapportages aan betrouwbaarheid inboeten vanwege gegevens die niet meer kloppen.

Tip 2: Zorg voor actuele data

Stel eisen op (voor de leverancier en de eigen ICT-afdeling) die waarborgen dat het systeem zo veel mogelijk met actu- »

Tips

Bij de aanbesteding/selectie van een toegangscontrolesysteem wordt vaak gefocust op de techniek. Toch zijn ook andere aandachtspunten van belang, met name vanuit de kant van het beheer. Enkele tips:
» Laat de meer administratieve eisen aan het nieuwe toegangssysteem inventariseren en vastleggen door de afdeling die met het systeem gaat werken.
» Het kan daarbij handig zijn uit te gaan van de werkprocessen op die afdeling. Zijn die niet beschreven, zorg er dan voor dat dat alsnog gebeurt, en maak het onderdeel van het PvE.
» Eis dat het systeem zo wordt ingericht dat altijd met actuele gegevens wordt gewerkt.
» Formuleer samen met de interne klant de eisen aan gewenste rapportages.
» Eis van het systeem een bepaalde flexibiliteit, zodat ook nieuwe beheerprocessen uitgevoerd kunnen worden.

ele data werkt. Enkele voorbeelden van eisen: invoer van gegevens is alleen geautomatiseerd mogelijk vanuit het HR-systeem; aan de hand van bepaalde parameters constateert het systeem automatisch dat medewerkers langdurig afwezig zijn waarna passen geblokkeerd kunnen worden; HR geeft informatie door bij veranderingen, zoals de uitdiensttreding of pensionering van een medewerker.
Stel ook eisen op voor een rapportagetool waardoor specifieke afdelingen periodiek rapportages ontvangen over het afgeven van autorisaties. Zij kunnen deze gegevens dan controleren.

Rapportages
De aanschaf van een nieuw, geavanceerd toegangscontrolesysteem kost veel geld. Dat schept hoge verwachtingen bij het management en interne afdelingen/klanten. Om deze verwachtingen te managen is het van belang vooraf met hen in gesprek te gaan om de eisen en wensen in kaart te brengen. Meestal kan een rapportagetool, gekoppeld aan het toegangscontrolesysteem, hier uitkomst bieden. Belangrijk is dat direct eisen worden gesteld aan de gewenste rapportages waarmee de toegangsverlening gemanaged kan worden.

Tip 3: Formuleer eisen aan de gewenste rapportages

Formuleer, in samenwerking met interne klanten, eisen aan de gewenste rapportages. Voorbeeld: een rapportage moet per interne klant periodiek inzicht geven in specifieke autorisaties (inclusief de mutaties).

Formuleer samen met de interne klant de eisen aan gewenste rapportages

Geef ook wensen aan voor de lay-out en frequentie van de rapportages.
Houd ook de mogelijkheid open voor toekomstige, nieuwe rapportages.
Denk eraan dat het produceren van rapportages belastend kan zijn voor de server waar de applicatie op draait, waardoor het de voorkeur heeft om 's nachts rapportages te produceren dan wel hiervoor een aparte (gekoppelde) server in te richten.

Werkprocessen
De organisatie en de personeelssamenstelling zullen regelmatig veranderen. Dit betekent dat werkprocessen in het toegangscontrolesysteem door de beherende afdeling met enige regelmaat aangepast of uitgebreid moeten worden.
Het is van belang dat het systeem dergelijke aanpassingen mogelijk maakt. Als daaraan in het voortraject onvoldoende aandacht wordt besteed, zal mogelijk het nieuwe toegangscontrolesysteem te weinig flexibel zijn om nieuwe/andere werkprocessen te kunnen uitvoeren.
Mogelijk gevolg is dat de effectiviteit (minder resultaat dan verwacht) en de efficiency (meer kosten en tijd om alsnog het verwachte resultaat te behalen) niet voldoen aan de verwachtingen.

Tip 4: Stem werkprocessen goed af

Om het toegangscontrolesysteem goed te laten functioneren, is het ook zaak de werkprocessen van de afdeling die is belast met het beheer, goed af te stemmen met het nieuwe systeem. Denk aan het volledig beschrijven van de volgende processen:
- het aanmaken en verzenden/uitreiken van een nieuwe toegangspas. Het daarna ontvangen en activeren van de nieuwe toegangspas door de ontvanger. Het bij uitdiensttreding terugzenden, deactiveren en afsluiten door de beherende afdeling;
- het aanmaken, activeren en later deactiveren en afsluiten van toegangspassen voor specifieke doelgroepen (bezoekers, schoonmakers, gepensioneerden, leveranciers, gedetacheerden);
- het aanmaken van pasfoto's (eenduidige kwaliteit!) en plaatsing op zowel de juiste toegangspassen als in het systeem;
- het verzenden van berichten (per e-mail of sms) aan personen van uitgevoerde mutaties in het toegangscontrolesysteem.

Beheer van toegangsautorisaties
Het beheren van toegangsautorisaties (welke functie/persoon mag in welke ruimten komen op welke dagen en tijdstippen?) is een complexe, maar tegelijk belangrijke activiteit. Hier zijn volop valkuilen te bespeuren, zoals ooit afgegeven autorisaties (vaak zonder dat documentatie hiervan beschikbaar is), onduidelijkheid over wie de interne 'eigenaren' van specifieke interne ruimten zijn, gebrekkig inzicht in c.q. overzicht van de verleende autorisaties et cetera.

Een goed hulpmiddel hierbij is een opgestelde lijst van interne 'eigenaren' van specifieke ruimten waar extra beveiligingsmiddelen zijn geïnstalleerd. Voorbeelden hierbij zijn ICT-ruimten, bepaalde HR-afdelingen, Juridische Zaken, technische ruimten et cetera. FM of Security stelt de eisen op waaraan werkprocessen moeten voldoen (risicoanalyse) om in aanmerking te komen voor extra beveiligingsmaatregelen voor deze specifieke ruimten. Een uniforme aanpak van de risicobeoordeling én het aanbieden van geüniformeerde beveiligingsmiddelen zijn hierbij cruciaal om 'wildgroei' en overbodige kosten voor de organisatie te vermijden.

Om de actualiteit te borgen dient deze lijst van ruimteneigenaren minimaal ieder kwartaal gevalideerd te worden door én FM c.q. Security én de eigenaren. Op deze wijze behoudt de backoffice overzicht over interne eigenaren en actuele autorisaties voor specifieke ruimten.
Mutaties op de gegevens van de ruimteneigenaren zelf dan wel op de gegevens van de personen die geautoriseerd zijn om de specifieke ruimten te betreden, dienen door de ruimteneigenaren schriftelijk aangegeven te worden. «

SAMENVATTING!

- Bij een nieuw toegangscontrolesysteem gaat het om veel meer dan techniek en ICT. **Actuele data, heldere werkprocessen en juiste informatievoorziening** zijn minstens zo belangrijk voor een goede dagelijkse werking van het systeem.
- De **afdeling die het systeem gaat beheren**, moet **niet** worden gezien als **sluitpost**. Gebruik de daar aanwezige kennis onder meer bij het opstellen van het PvE, zodat het systeem met succes in gebruik kan worden genomen!

* Frans Visser, directeur van Fases facility & security services, samenwerkingspartner van VFM Facility Experts (info@fases.nl).