Toegangscontrole software: bouwen of kopen?

Als een onderneming overweegt nieuwe technologie aan te schaffen om de efficiëntie te verbeteren, de productiviteit te verhogen, de operationele kosten omlaag te brengen of zijn strategische voorsprong te verbeteren, geldt maar één vraag: bouwen of kopen?

De kritische analyse die dan plaatsvindt, helpt bij het bepalen of het voordeliger is om de eigen mensen een op maat gesneden oplossing te laten ontwikkelen, of een bestaande, generieke software oplossing te kopen die een breed scala aan geïntegreerde functionaliteiten biedt.

Voor een organisatie die een geautomatiseerde oplossing overweegt om de fysieke identificatie en toegangscontrole te beheren, kan dit een forse uitdaging vormen. Is het beter om intern een fysiek beveiligings- en toegangsprogramma (physical security and access management, PIAM) te ontwikkelen voor de behoefte aan compliance, operationele en kwalitatieve waarden, of kan er beter een generieke (commercial, off-the-shelf: COTS) oplossing worden aangeschaft? Enig begrip van de verschillen tussen beide benaderingen kan veel voordeel opleveren, maar het blijft een moeilijke keuze. Je moet bij de keuzebepaling rekening houden met drie belangrijke factoren: kosten, maatwerk en gemak.

Kosten

Bij de overweging van de aanschaf van een COTS-oplossing of een in-house oplossing, vormen de kostenposten een belangrijke, zo niet vaak doorslaggevende factor. Het voordeel van een COTS-oplossing is dat die kosten onderhandelbaar zijn en vooraf kunnen worden afgesproken. Eventuele aanvullende kosten of maatwerk-ontwikkelingen kunnen voor de aanvang van het project worden gekwantificeerd, en er kan een schema worden opgesteld voor de levering van upgrades of andere aanpassingen. Dat laatste is zeker van belang voor wat betreft de budgettering. Bovendien leveren COTS-oplossingen gewoonlijk een betere ROI op de lange termijn, dankzij hun meer stabiele functies, hogere betrouwbaarheid en de mogelijkheid deze op een kleinere schaal in te zetten, vergeleken met een in-house oplossing. Daarentegen moeten in de kostenberekening voor een in-house oplossing ook worden meegenomen de onkosten die gepaard gaan met het tijdsintensieve proces van het ontwikkelen van de toepassing, het inzetten van eigen personeel en het vaststellen van de kosten voor ontwikkeling, testen en ondersteunen. Bij de

ontwikkeling moet ook rekening worden gehouden met de workflow die een grote verscheidenheid aan systeemprocessen kan integreren. Dat betekent dat wanneer één set van privileges verandert, fysiek dan wel logisch, die verandering automatisch aanvullende revisies zal triggeren in andere sets. Uiteindelijk zal bepaald moeten worden of een 'eigen' oplossing de efficiëntie daadwerkelijk zal verhogen, of een tastbare ROI zal opleveren die groter is dan die van een COTS-oplossing.

Maatwerk

Software-leveranciers zijn zeer goed op de hoogte van compliancy-voorschriften en wetten, opgelegd door de regering en andere wetgevende instanties, en zij hebben hun assortiment ontwikkeld, gebouwd en verfijnd om de functionaliteiten te leveren die nodig zijn om aan deze voorschriften van zowel de zakelijke als de regelgevende kant te voldoen, evenals aan de technologische eisen. In de meeste gevallen zal het software-programma standaard, out-of-the-box voldoen aan de compliancy-eisen van de klant.
Het effectief beheren van identiteiten in een organisatie roept veel problemen op, naast het voldoen aan de compliancy-eisen die de diverse instanties hebben opgesteld. Zaken als risiconiveaus, gebiedseigenaar en voorwaarden voor toegang, evenals het koppelen van identiteiten met alarmen, het beheren van badge/autorisatie-systemen enzovoort, moeten vaak al draaien om het management in staat te stellen, proactief beveiligingsbeleid en regels te handhaven. Daarom kunnen 'eigen' oplossingen wel eens zeer tijdrovende, dure en inefficiënte manier zijn om een identeit te beheren.

Gemak

Met software die alleen is ontwikkeld om fysieke identiteits- en toegangscontrole te beheren, kunnen alle soorten van identiteit worden beheerd, waaronder vaste en tijdelijke werknemers, aannemers, dienstverleners, verkopers en bezoekers. Deze software is ontworpen om details van een fysieke identiteit te beheren, zoals biografische en biometrische informatie, evenals resultaten van de beveiligingscontroles en historisch gebruik. Behalve dat het programma informatie uit diverse systemen verzamelt met betrekking tot het toegangsniveau, worden deze informatie en de toepassingen (bijvoorbeeld fysieke identiteit beheer, functiegebaseerde toegang, transactie controlesporen) geautomatiseerd in één enkele web-based interface die eenvoudig te beheren en te gebruiken is.

Een belangrijk punt ter overweging met betrekking tot een software-pakket is het aspect van de service/support. Met de aankoop van COTS softwarepakketten kan meteen – of op een later tijdstip – worden meegenomen de ondersteuning van de helpdesk van de leverancier, updates, bug-reparaties, continue maatwerklevering, toekomstige implementaties en dergelijke. Voor wat betreft de 'eigen' software oplossingen moet het service/support aspect meegenomen worden in het originele pakket. Wat is het risico als je de kennisbasis verliest wanneer de technologie-afdeling verandert, of zelfs wordt opgeheven? Het is natuurlijk makkelijk is om in-house ondersteuning te hebben, maar tenzij die ondersteuning alleen gericht is op het PIAM software pakket, kan de oplossing van problemen wel eens veel kostbare tijd in beslag nemen en werknemers weghalen van hun normale taken.

Conclusie

Recente trends onderschrijven de conclusie dat organisaties er beter aan doen om met derde partijen te werken, met professionals dus, voor wat betreft hun grootschalige identiteitsbeheersystemen. Die leveranciers bieden toepassingsgerichte oplossingen die ze hebben gebouwd op basis van de best practices en die een bewezen track record hebben in de PIAM markt. ■