Uitgebreide toegangsbeveiliging

Kan iedereen bij u verkooporders invoeren? In een kleine organisatie kan dat. Kwestie van vertrouwen, en handig als er eens iemand ziek of op vakantie is. Maar terwijl uw organisatie groeit, groeit de kans op problemen. Onbedoelde invoerfouten, facturen die zonder controle worden verstuurd. De noodzaak van functiescheiding wordt groter. De modules *Uitgebreide toegangsbeveiliging I* en *Uitgebreide toegangsbeveiliging II* zorgen ervoor dat iedereen zijn taak in AccountView kan uitvoeren. Maar ook niet meer dan dat.

Wat kan ik ermee?

De standaardbeveiliging van AccountView bestaat uit gebruikersnamen en wachtwoorden. Een eenvoudige maar doeltreffende toegangsbeveiliging die in kleinere organisaties uitstekend voldoet. Maar terwijl het aantal gebruikers van AccountView groeit, groeit ook de kans op fouten in de boekhouding, oneigenlijk gebruik of zelfs misbruik. U wilt per gebruiker delen van het pakket kunnen afschermen.

Uitgebreide toegangsbeveiliging I

Dat is precies waarvoor *Uitgebreide toegangsbeveiliging I* is bedoeld. U geeft per gebruiker aan, tot welke administraties deze toegang heeft, en welke bedrijfsgegevens daadwerkelijk kunnen worden benaderd. Een medewerker van de debiteurenadministratie zal alleen toegang hebben tot debiteurgegevens in de administratie waarin deze worden bijgehouden; de financial controller zal vrijwel alle bedrijfsgegevens kunnen opvragen en heeft mogelijk toegang tot meerdere administraties. Met *Uitgebreide toegangsbeveiliging I* kunt u de functiescheiding in uw organisatie ook in AccountView doorvoeren.

De module verdeelt AccountView in onderdelen. Voorbeelden van dergelijke onderdelen zijn grootboek, artikelen, boekingen, rapporten en verslagen. Voor elk onderdeel kunt u aangeven of het mag gebruiken, en zo ja, op welke manier (opvragen, toevoegen, verwijderen, wijzigen). Iemand die mag opvragen in het onderdeel *Debiteuren*, kan alle debiteurrapporten opvragen. U kunt per gebruiker aangeven tot welke administraties deze toegang heeft. De vastgelegde toegangsrechten gelden automatisch voor al die administraties, dus daar hebt u geen omkijken meer naar.

Bij het vastleggen van toegangsrechten maakt u gebruik van rollen. In een rol legt u de rechten voor bepaalde onderdelen vast, of sluit u expliciet bepaalde onderdelen uit. De AccountView-onderdelen worden weergegeven in een overzichtelijke boomstructuur, vergelijkbaar met de Windows Verkenner, waarin u per rol rechten toekent of uitsluit. De rollen geven als het ware uw organisatiestructuur en uw functiescheidingen weer. Die rollen koppelt u vervolgens aan gebruikers. Dit systeem biedt grote voordelen bij het wijzigen van rechten, omdat u alleen de rol hoeft te wijzigen. De wijziging geldt dan automatisch voor alle gebruikers met die rol. Ook maakt u sneller nieuwe gebruikers aan: rollen koppelen en klaar. Dergelijke functionaliteit vindt u normaal gesproken alleen in grote beveiligingssystemen, maar in *Uitgebreide toegangsbeveiliging I* is het standaardfunctionaliteit.

Dagboeken nemen een speciale plaats in, vandaar dat daarvoor speciale functionaliteit is toegevoegd. U kunt per dagboek aangeven welke gebruikers toegang hebben tot dat dagboek.

Uitgebreide toegangsbeveiliging II

De module *Uitgebreide toegangsbeveiliging II* breidt dit alles nog uit met gebruikersgroepen, rechten per administratie en rechten per menu-optie. Daardoor kunt u precies bepalen, tot welke menu-opties van een bepaald onderdeel van een bepaalde administratie de gebruikers toegang hebben. Daarnaast kunt u gebruikers indelen in groepen en per groep rechten verlenen. Dit biedt nog een extra niveau naast gebruikers, waardoor u de rechten nog flexibeler kunt toekennen en onderhouden.

Om de module te completeren zijn instellingen voor wachtwoorden toegevoegd; niet alleen algemene instellingen maar ook instellingen per gebruiker. Daarmee kunt u er bijvoorbeeld voor zorgen dat gebruikers hun wachtwoord regelmatig veranderen, en dat ze niet steeds twee wachtwoorden afwisselen. De combinatie van gebruikersnaam en wachtwoord blijft immers de kern van uw toegangsbeveiliging, en verdient daarom extra aandacht.

Toegangsbeveiliging is niet voor iedereen dagelijkse kost. Misschien dat het bovenstaande vragen oproept. Maar juist voor toegangsbeveiliging geldt dat u niet voorzichtig genoeg kunt zijn. Met *Uitgebreide toegangsbeveiliging I* verzekert u zich van degelijke extra bescherming en een relatief eenvoudige inrichting. Voor grote organisaties of gevoelige informatie is *Uitgebreide toegangsbeveiliging II* een uitkomst. Een complexe maar betrouwbare module, waarmee u uw toegangsbeveiliging tot op de honderdste millimeter

nauwkeurig kunt afregelen. We raden u aan om hiervoor uw leverancier in te schakelen. Beide modules zijn erop gericht om de onderhoudskosten tot het absolute minimum te beperken.

Wat koop ik ervoor?

- ☑ *Uitgebreide toegangsbeveiliging I*:
  - ☑ Administraties afschermen per gebruiker
  - ☑ Dagboeken afschermen per gebruiker
  - ☑ AccountView-onderdelen afschermen per toegangsbeveiligingrol
  - ☑ Meerdere toegangsbeveiligingrollen toekennen per gebruiker
  - ☑ Standaardrapportage: gebruikers en rollen
- ☑ *Uitgebreide toegangsbeveiliging II*:
  - ☑ Gebruikersgroepen
  - ☑ Menu-opties van AccountView-onderdelen afschermen per toegangsbeveiligingrol
  - ☑ Meerdere toegangsbeveiligingrollen toekennen per gebruiker per administratie
  - ☑ Meerdere toegangsbeveiligingrollen toekennen per gebruikersgroep per administratie
  - ☑ Extra algemene wachtwoordbeveiligingen: minimumlengte, maximale geldigheidsduur en het aantal oude wachtwoorden dat moet worden onthouden
  - ☑ Extra wachtwoordinstellingen per gebruiker: of het wachtwoord al dan niet verloopt, of het wachtwoord moet worden gewijzigd na inloggen, en of de gebruiker het wachtwoord zelf kan wijzigen
  - ☑ Standaardrapportage: gebruikersgroepen en toegangsanalyse

Wat levert het op?

Het is lastig om besparingen voor dergelijke modules te kwantificeren. De vergelijking met verzekeringen dringt zich op: voor een relatief laag bedrag (in dit geval zelfs eenmalig!) kunt u grote problemen voorkomen. En hoe meer gebruikers, hoe meer problemen kunnen optreden.

- ☑ *Uitgebreide toegangsbeveiliging I*:
  - ☑ Scherm inkoopboeken af voor verkopers, en verkoopboeken voor inkopers. Iemand die zowel kan verkopen als inkopen staat aan grote verleidingen bloot.
  - ☑ Beperk de rechten van magazijnmedewerkers tot de voorraadonderdelen.
  - ☑ Maak aparte rollen met uitgebreidere beperkingen aan voor nieuwe medewerkers. Zodra ze zijn ingewerkt hoeft u alleen de rol te verwijderen.
  - ☑ Alleen de systeembeheerder mag wachtwoordinstellingen wijzigen en gebruikers toevoegen.
- ☑ *Uitgebreide toegangsbeveiliging II*:
  - ☑ Beperk de rechten van verkopers en inkopers tot het invoeren van orders. Alleen het hoofd van de afdeling mag orders verwerken.
  - ☑ Beperk de rechten van magazijnmedewerkers tot het invoeren van ontvangsten. Alleen het hoofd magazijn mag magazijnoverboekingen en breuk invoeren.
  - ☑ Alleen de boekhouding mag de eindejaarsverwerking uitvoeren.
  - ☑ Alleen de systeembeheerder mag administraties organiseren en controleren.

Uw financiële administratie is het hart van uw onderneming. Beveiligingsproblemen, of ze nu per ongeluk of bewust zijn veroorzaakt, kunnen u geld kosten. Veel geld. De kosten van de module *Uitgebreide toegangsbeveiliging I* vallen in het niet bij het verlies van de leads van een beurs, of bij het verlies van uw debiteurgegevens als gevolg van een actie van een rancuneuze ex-medewerker. De module *Uitgebreide toegangsbeveiliging I* kost u waarschijnlijk minder dan één te laag geprijsde factuur. Risico's lopen is onvermijdelijk, maar soms zijn ze gemakkelijk en goedkoop te reduceren.

Wat kost het?

U investeert € 195,- voor *Uitgebreide toegangsbeveiliging I*, en € 595,- voor *Uitgebreide toegangsbeveiliging II* (excl. BTW). *Uitgebreide toegangsbeveiliging I* is een uitbreiding op *Team* of *Business*. *Uitgebreide toegangsbeveiliging II* is een uitbreiding op *Business* en *Uitgebreide toegangsbeveiliging I*.