© 2004-2012 ORIfin Holland - 105_beveiliging_orifin.wpd - aanmaakdatum 19-03-2012

BEVEILIGING

Algemeen

Binnen ORIfin zijn op diverse plaatsen beveiligingen aan te brengen om ongeoorloofd gebruik tegen te gaan. Zo zijn er beveiligingen op het niveau van programmaös, administraties, dagboeken en kostenplaatsen. Daarnaast ligt er nog een beveiliging op het gebruik van de diverse relatie-rubrieken. Deze laatste beveiliging wordt in deze beschrijving apart als laatste beschreven, omdat deze niets heeft uit te staan met de andere beveiligingen.

De basis van al deze beveiligingen wordt gelegd in een bestand waarin voor elke gebruiker enkele gegevens zijn opgenomen, zoals de gebruikersidentificatie (verkort: user-ID), de volledige naam en het wachtwoord dat benodigd is op ORIfin op te starten. In dit bestand zijn ook de beveiligingen opgeslagen. De informatie in het bestand is gecodeerd, zodat de informatie zonder bijbehorend programma niet leesbaar is.

Groepen gebruikers

Naast het feit dat u de rechten kunt opgeven per gebruiker, kunt u die ook opgeven voor groepen gebruikers. U kunt dan een gebruiker lid maken van één of meer van deze groepen, waardoor de gebruiker minimaal de rechten krijgt van deze groepen.

➜ Als er een beveiliging is aangebracht voor de gebruiker EN voor de groepen waar de gebruiker deel van uitmaakt, dan gaan de rechten van de gebruiker vóór de rechten van de groepen.

➜ Als er verschil is tussen de rechten van meerdere groepen waar de gebruiker deel van uitmaakt, dan zullen de rechten van toepassing zijn van de groep met de meeste rechten.

Standaard-gebruiker

Zijn er voor een gebruiker geen individuele rechten of groepsrechten opgegeven, dan wordt gekeken naar de rechten van de ñstandaard-gebruikerò(= default user). Aan deze standaard-gebruiker kunnen op dezelfde wijze als bij een gewone gebruiker (of groep) rechten worden toegekend.

Diverse autorisaties, een overzicht

Per toegekende autorisatie kan worden aangegeven welk recht de betreffende gebruiker of groep heeft. Dat kan gaan van minimale rechten tot maximale rechten. Een autorisatie kan het volgende niveau hebben, mat daarnaast de uitwerking bij de diverse beveiligingen:

Niveau + benaming	Administratie	Programma	Dagboeken	Kostenplaatsen
0 geen rechten	**opstarten niet toegestaan)ô**	**opstarten niet toegestaan**	**inzage en gebruik niet toegestaan**	**inzage en gebruik niet toegestaan**
3 inzagerechten	**opstarten toegestaan maar met waarschuwing**	**opstarten toegestaan, alleen inzage e.d. mogelijk**	**inzage toegestaan, gebruik niet toegestaan**	**inzage toegestaan, gebruik niet toegestaan**
6 muteerrechten	**idem, zonder waarschuwing**	**idem, muteren ook mogelijk**	**inzage en gebruik toegestaan**	**inzage en gebruik toegestaan**
9 beheersrechten	**idem**	**idem, beheersfuncties ook mogelijk**	**idem**	**idem**
T leveranciers-rechten	**n.v.t.**	**idem, volledige functionaliteit (alleen voor leverancier)**	**n.v.t.**	**n.v.t.**

© 2004-2012 ORIfin Holland - 105_beveiliging_orifin.wpd - aanmaakdatum 19-03-2012

)ô- Als de betreffende gebruiker beheersrechten heeft voor het programma waarmee de rechten kunnen worden vastgesteld, zal die gebruiker de administratie WEL op kunnen starten.

Beveiliging voor het opstarten van administraties

De ORIfin-beheerder kan via programma ñAlgemene set-up ORIfinò aangeven of er een beveiliging moet worden gelegd op het opstarten van administraties.

Er is ook de mogelijkheid om een gebruiker het recht te geven een administratie op te starten, maar met waarschuwing. Deze mogelijkheid kan worden gebruikt als er bijvoorbeeld sprake is van een archief-administratie waarvan het de bedoeling is om geen wijzigingen meer aan te brengen.

➜ **De ORIfin-beheerder kan per administratie (via ñSet-up administraties per werkplekò) bepalen welke kleuren het ORIfin-logo heeft in het menu en linksboven in de kop van alle onderdelen. Die kleuren moeten worden gezien als eenvoudig hulpmiddel om de gebruiker er aan te herinneren of wel in de juiste administratie wordt gewerkt. N.B.: Als de ORIfin-beheerder NIET heeft aangegeven dat de ORIfin-instellingen zoveel mogelijk centraal moeten worden opgeslagen, zullen de kleuren op elke werkplek moeten worden ingesteld.**

Beveiliging op het gebruik van programmaôs

Per programma kan worden aangegeven of een gebruiker al dan niet dat programma op mag starten. Door verschillende autorisaties te gebruiken kan de betreffende gebruiker de mogelijkheid krijgen het programma op te starten met alleen inzage-rechten, met normale gebruiksrechten (muteren e.d.) of met beheers-rechten.

In diverse programmaôs mogen gebruikers die voor dat programma beheersrechten hebben net iets meer dan gewone gebruikers.

Voorbeeld: De ORIfin-beheerder kan bepaalde periodes afschermen om in te boeken. Een gebruiker met beheersrechten voor het programma ñOnderhoud boekingenò mag echter altijd in alle beschikbare periodes boeken.

Beveiliging op het gebruik van dagboeken

De ORIfin-beheerder kan via programma ñInstellingen financiële administratieò van de betreffende admini-stratie aangeven of er een beveiliging moet worden gelegd op het gebruik van dagboeken.

Van elk dagboek kan worden aangegeven of een gebruiker dat dagboek mag gebruiken en zo ja, of dat mag om boekingen in te brengen of alleen maar om informatie op het scherm of de printer uit te draaien. Dit geldt zowel voor dagboeken transacties als voor dagboeken verplichtingen en dagboeken budgetten.

Als een gebruiker geen inzagerechten heeft voor een dagboek, zullen alle boekingen op dat dagboek voor die gebruiker niet zichtbaar zijn. Omdat lijsten in dat geval niet compleet zullen zijn, zal een waarschuwing van deze strekking boven de betreffende lijsten verschijnen.

➜ Als een gebruiker voor een bepaald programma beheersrechten heeft, overruled dat de dagboek-rechten en zullen alle boekingen gewoon zichtbaar zijn.

Beveiliging op het gebruik van kostenplaatsen

De ORIfin-beheerder kan via programma ñInstellingen financiële administratieò van de betreffende admini-stratie aangeven of er een beveiliging moet worden gelegd op het gebruik van kostenplaatsen.

Van elke kostenplaats kan worden aangegeven of een gebruiker die kostenplaats mag gebruiken en zo ja, of die kostenplaats ook gebruikt mag worden tijdens het inbrengen van boekingen of alleen maar om informatie op het scherm of de printer uit te draaien.

© 2004-2012 ORIfin Holland - 105_beveiliging_orifin.wpd - aanmaakdatum 19-03-2012

Ook voor kostenplaats-groepen kan worden aangegeven of een gebruiker deze groepen mag gebruiken of niet. Aangezien bij het inbrengen van boekingen niet rechtstreeks kan worden geboekt op kostenplaats-groepen, maakt het voor kostenplaats-groepen niet uit of een gebruiker alleen maar inzage-rechten heeft of ook gebruiksrechten.

Als een gebruiker geen inzagerechten heeft voor een kostenplaats, zullen de boekingen op die kostenplaats voor die gebruiker wel zichtbaar zijn)ômaar met sterren op de plaats van het nummer en de naam van de kostenplaats. Omdat lijsten in dat geval niet compleet zullen zijn, zal een waarschuwing van deze strekking boven de betreffende lijsten verschijnen.

)ô= Als ook de bedragen niet zichtbaar zouden zijn, zouden er op diverse overzichten verschillen D/C ontstaan.

➜ Als een gebruiker voor een bepaald programma beheersrechten heeft, overruled dat de kostenplaats-rechten en zal alle informatie gewoon zichtbaar zijn.

Effect op beveiliging dagboeken bij debiteuren / crediteuren

Bij het uitdraaien van lijsten facturen / betalingen werkt de beveiliging dagboeken alleen op de dagboeken waarmee de facturen zijn ingebracht. Als een deel van de termijnen valt onder dagboeken die ten gevolge van de beveiliging niet mogen worden getoond, zullen die termijnen wel zichtbaar zijn, maar zonder bedrag. Aangezien de beveiliging geen invloed heeft op de betalingen, kan het bij deze facturen lijken alsof er meer is betaald dan gefactureerd.

Omdat er over het algemeen dus vreemde effecten kunnen optreden in dit programma vanwege de beveiliging, wordt aangeraden om alle gebruikers die een volledig overzicht mogen uitdraaien voor dit programma beheersrechten te geven.

Beheerder: welke rechten geeft u uzelf?

Het is verstandig om uzelf alle beheersrechten te geven voor alle programmaôs binnen ORIfin. Er kan u zodoende niets ontgaan van de uitgebreidere mogelijkheden.

Aan de andere kant is het ook handig als u weet wat een ñgewoneò gebruiker precies voor zich ziet en wat een ñinzageò gebruiker kan of juist NIET kan. Vandaar de volgende tip.

Tip: Neem uzelf 3x op in de gebruikerstabel. 1x met beheersrechten voor alle programmaôs, 1x met ñgewoneò rechten voor alle programmaôs en 1x met inzagerechten voor alle programmaôs.

© 2004-2012 ORIfin Holland - 105_beveiliging_orifin.wpd - aanmaakdatum 19-03-2012

Samenvatting

Beveiliging is mogelijk op:

- administraties
  - opstarten niet toegestaan
  - opstarten toegestaan, maar met waarschuwing
  - opstarten wel toegestaan

- menu (programmaÕs)
  - opstarten niet toegestaan
  - alleen inzage / tonen / lijst
  - muteren toegestaan
  - beheer-functies toegestaan

- dagboeken en kostenplaatsen (+ -groepen)
  - gebruik niet toegestaan
  - alleen inzage / tonen / lijst
  - gebruik wel toegestaan
    - voor kostenplaatsgroepen: rechten gelijk aan ñalleen inzage / tonen / lijstò

© 2004-2012 ORIfin Holland - 105_beveiliging_orifin.wpd - aanmaakdatum 19-03-2012

Berekenen autorisatie per beveiliging:

- Zijn individuele rechten opgegeven?
  - Zo ja: deze gelden
  - Zo nee: is gebruiker lid van één of meer groep(en) waarvoor rechten zijn opgegeven?
    - Zo ja: de rechten gelden van de groep met de meeste rechten
    - Zo nee: zijn rechten opgegeven voor de standaard-gebruiker?
      - Zo ja: de rechten gelden van de standaard-gebruiker
      - Zo nee: de gebruiker heeft geen rechten.

Beveiliging op relatie-rubrieken

Via programma ñOnderhoud specificatie databaseò kan per relatierubriek worden aangegeven of de rubriek alleen te benaderen is voor bepaalde gebruikers of gebruikersgroepen. De werking is eenvoudig: als er één of meer gebruikers-identificaties en/of groeps-identificaties zijn opgegeven, wordt de rubriek gezien als ñbeveiligdò. Alleen die personen (en leden van groepen) die staan genoemd, mogen dan die rubrieken benaderen EN personen die de betreffende programmaós opstarten met beheersrechten.

© 2004-2012 ORIfin Holland - 105_beveiliging_orifin.wpd - aanmaakdatum 19-03-2012