WEMAG CONSULTING

WEMAG Consulting, Bernstrasse 99, Postfach, 3122 Kehrsatz
Tel.: 031 960 36 36 FAX: 031 960 36 37 E-Mail: info@wemag.ch www.wemag.ch

Definition utilisateur 2

Table des matières

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1 Définition d'utilisateur

1.1 Utilisateur "QSECOFR"

L'utilisateur "QSECOFR" est → Délégué de sécurité avec la classe d'utilisateur ***SECOFR**

La priorité supérieure dans l'iSeries a l'utilisateur "QSECOFR". Il a l'autorisation, sur presque toutes les données dans l'iSeries ainsi que sur beaucoup de fonctions système que seulement il peut exporter. Cela vaut pour tous les utilisateurs "QSECOFR"; ou pour les utilisateurs avec la classe d'utilisateurs *SECOFR.

Au cas où un utilisateur perd son mot de passe, le QSECOFR doit lui assigner un nouveau. Il n'a toutefois pas la possibilité d'aller voir le mot de passe. Si le QSECOFR peut assigner un nouveau mot de passe à un utilisateur, il a aussi la possibilité, s'admettait maintenant avec ce mot de passe en tant que ces utilisateurs annoncer et ainsi des données confidentielles recevoir.

S'annonce comme QSECOFR, seulement une personne doit pouvoir qui jouit d'une confiance pleine !

L'Autorisation

Pour pouvoir saisir ou modifier un utilisateur ou un profil de groupe, vous devez lui annoncer avec l'utilisateur "QSECOFR". Seulement l'utilisateur "QSECOFR" est autorise à modifier tous les utilisateurs.

Remarque : Si la classe d'utilisateurs est assignée à un profil des utilisateurs avec *SECADM, ce profil des utilisateurs pourrait également modifier ou saisir les autres profils des utilisateurs.

Remarque:
On ne devrait pas travailler dans le GISA avec l'utilisateur " QSECOFR"
*ou un utilisateur avec la classe d'utilisateurs *SECOFR !*

Également aucun utilisateur devrait être existant avec le nom "GISA" et ni le mot de passe "GISA" ou le nom "QSECOFR" et le mot de passe "QSECFR" sur votre système !
Effectivement le mot de passe ne devrait jamais être identique au nom de l'utilisateur.

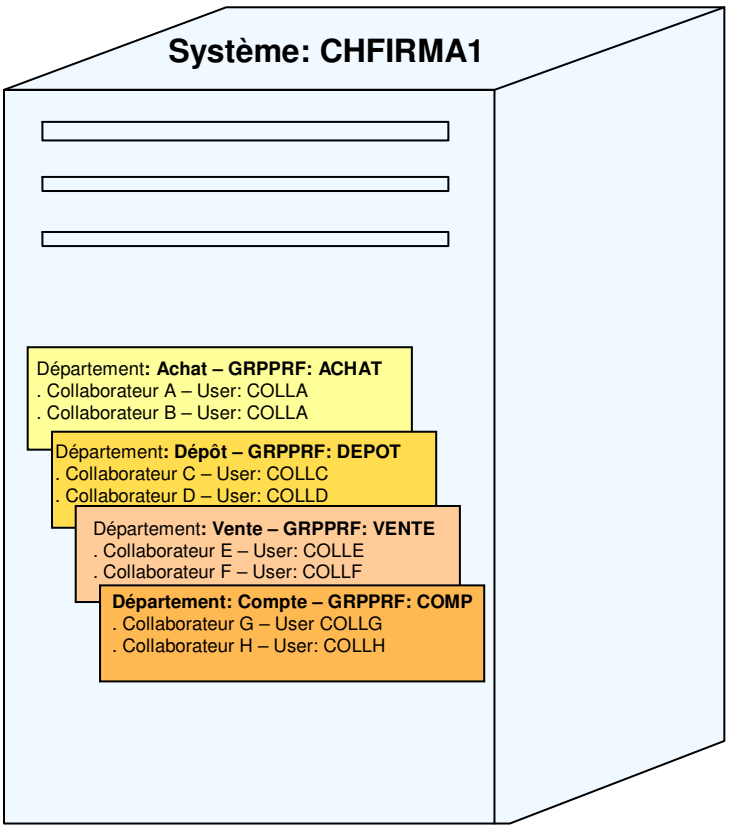
Recommandation!
Au cas où le mot de passe du profil QSECOFR n'était plus connu, devait un profil des utilisateurs spécial (p. ex. QSECOFR1) être existant. Avec ce profil, on ne travaille pas, il sert seulement pour le cas d'urgence. Le profil est organisé de telle sorte que le mot de passe ne coule jamais. Le mot de passe est gardé à une place sûre. Si on est annoncé avec ce profil, le mot de passe du QSECOFR peut être défini à nouveau.

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.2 Profil de groupe (GRPPRF)

Nous vous recommandons de résumer vos utilisateurs dans des groupes et ouvrir les profils de groupe correspondants dans l'iSeries, afin que l'autorisation puisse être donnée exclusivement au moyen des profils de groupe.
Des profils de groupe sont statiques et s'orientent après l'agencement de l'entreprise. Chaque utilisateur est enregistré dans son profil de groupe de département.
Avec un changement de personnel, ainsi le nouvel utilisateur peut être ouvert et avec l'attribution du profil de groupe correspondant et il est autorise immédiatement pour son domaine d'application.

Un profil de groupe est également saisi dans les profils des utilisateurs.



WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.3 Définition des profiles d'utilisateur

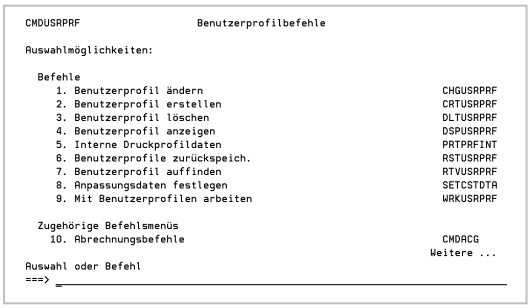
Pour la définition de vos utilisateurs respectivement pour la définition de l'autorisation nous recommandons vous la procédure suivante :

1. Classez vos collaborateurs dans des groupes et définissez avec chaque profil des utilisateurs le profil de groupe correspondant.
2. Définissez un profil des utilisateurs pour chacun de vos collaborateurs qui travaille sur votre système.
3. Maintenant, pour chaque groupe, un menu distinct peut être fourni. Sur ce menu se trouvent les programmes qui sont nécessaires pour le groupe en question.
4. Si l'autorisation doit être répartie encore plus, le module d'autorisation du GISA peut être utilisé.

1.3.1 Profil d'utilisateur

Pour créer un profil de groupe ou un profil d'utilisateur, on doit travailler avec l'utilisateur: QSECOFR.

Avec l'ordre **go cmdusrprf** vous recevez le menu avec les ordres pour les profiles d'utilisateurs.



Choisissez l'ordre « 9 Travailler avec des profils des utilisateurs », après vous recevez les choix suivants :

1 = Créer
2 = Modifier
3 = Copier
4 = Effacer
5 = Afficher
12 = travailler avec des objets d'un propriétaire.

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

Definition utilisateur 6

Naturellement il est le plus simple, si un profil des utilisateurs existant peut être copié. (Choix 3 = copier).

En copiant aussi bien qu'en la saisie les champs suivants doivent être pris en considération :

1. Au profil de groupe

Profile d'utilisateur Mot de passe	USRPRF PASSWORD	ACHAT *NONE	Nom du profil de groupe le profil de groupe n'est pas permit de s'annoncer
Statues	STATUS	*DISABLED	le profil de groupe n'est pas permit de s'annoncer
Classe d'utilisateur	USRCLS	*USER	
Texte "Description"	TEXT	Dép. Achat	Description de profil
Autorisation spécial	SPCAUT	*NONE	la plupart des utilisateurs n'ont pas besoin une autorisation spécial
Attention: 			*on doit **jamais** attribuer l'autorisation spécial ***ALLOBJ,** parce que cet utilisateur a l'accès sur **TOUTES** les données.* *Aussi **jamais**, l'autorisation spéciale ***SPLCTL** ne peut être assignée, puisque l'utilisateur a d'ailleurs l'accès à **TOUS** les fichiers spool.*
Profil groupe	GRPPRF	*NONE	au profil de groupe, ce champ doit être mis sur : *NONE
Propriétaire	OWNER	*USRPRF	le propriétaire d'un objet, qui est créer par un profil de groupe, appartient à la groupe

1.3.2 Caractéristiques d'un profil de groupe normal:

- Mot de passe *NONE
- Statues *DISABLED
- User Class *USER
- Autorisation spécial *NONE
- Propriétaire *USRPRF

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

2. Au profil d'utilisateur

Profil d'utilisateur Mot de pas d'utilisateur	USRPRF PASSWORD	COLLA xxxx	Nom du profil d'utilisateur Mot de passe pour ce profil d'utilisateur
Statues	STATUS	*ENABLED	le profil d'utilisateur est actif et il est permit pour l'annoncer
Classe d'utilisateur	USRCLS	*USER	
Texte "Description"	TEXT	Collaborateur A	Description de profil
Autorisation spécial	SPCAUT	*JOBCTL	afin que les fonctions soient garanties, les utilisateurs ont besoin de l'autorisation spéciale *JOBCTL.
Attention: 			*on doit **jamais** attribuer l'autorisation spécial ***ALLOBJ,** parce que cet utilisateur a l'accès sur **TOUTES** les données.* *Aussi **jamais**, l'autorisation spéciale ***SPLCTL** (voir aussi la description suivante « l'autorisation des Outqueues pour les listages » et « permission des Outqueues pour les impressions confidentielles ») ne peut pas être assignée, puisque l'utilisateur a d'ailleurs l'accès à **TOUS** les fichiers spool.*
Profil groupe	GRPPRF	EINKAUF	cet utilisateur a l'autorisation de groupe ACHAT
Propriétaire	OWNER	*GRPPRF	le propriétaire d'un objet, qui est créer par un profil de groupe, appartient à la groupe

1.3.3 Caractéristiques d'un profil d'utilisateur normal:

- Mot de passe xxxx
- Statues *ENABLED
- User Class *USER
- Autorisation spécial *JOBCTL

Avec profil de groupe

- Propriétaire *GRPPRF

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.3.4 Autorisation des Outqueues pour des listages

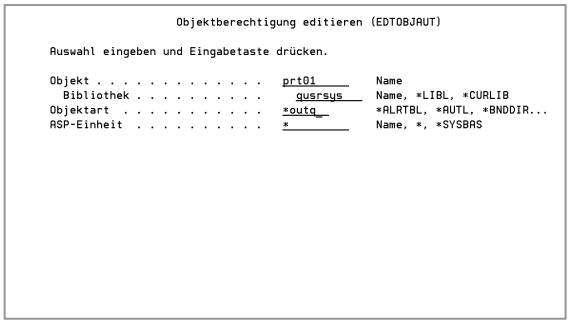
Remarque:
Dans l'autorisation spécial (SPCAUT) peut être activé l'autorisation *SPLCTL (Spool control). Cette autorisation spéciale **n'est pas** recommandée, parce que avec cette autorisation l'utilisateur a le droit pour **tous** les fichiers spool. Plutôt dans les Outqueues normaux, l'autorisation devrait être définie ***PUBLIC avec *CHANGE.**

Avec l'ordre EDTOBJAUT (edit object authority) peut être modifié une Outqueue.

Exemple:

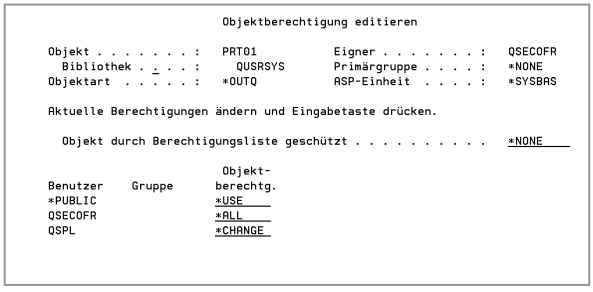
1er écran:

Objet Outqueue désiré p.ex. **PRT01**
Bibliothèque **QUSRSYS**
Genre d'objet ***OUTQ**



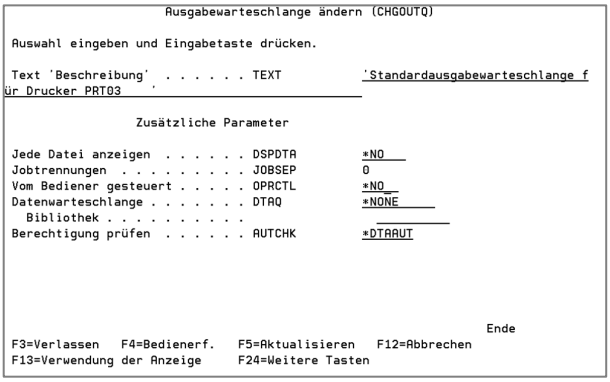
2ème écran

Utilisateur	*Group*	*Autorisation d'objet*
***PUBLIC**		***CHANGE**



WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

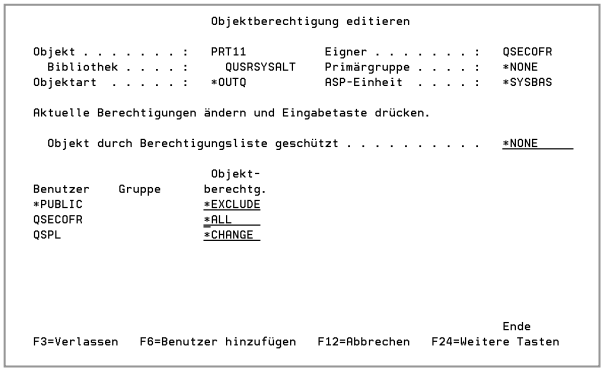
Avec l'ordre WRKOUTQ vous recevez une liste de vos imprimantes respectivement de votre Outqueues. Avec le choix « 2 modifier », les champs « contrôler de l'utilisateur » **OPRCTL sur « *NO »** et « Autorisation examiner » **AUTCHK sur « *DTAAUT »** peut être adapté.
OPRCTL → *NO signifie : Cette file d'attente et ses entrées ne peuvent pas être manipulées ou modifiées par un utilisateur avec une autorisation de renchérissement d'emploi, à moins que, il a aussi d'autres autorisations spéciales.
AUTCHK → *DTAAUT signifie : « chaque utilisateur peut tous les fichiers spool dans la file d'attente commander avec une autorisation de suppression, d'adjonction et de lecture ». Des fichiers spool appartiennent au profil que le fichier spool a fourni.



Tous les Outqueues, sur lesquels des listes et documents normaux (bulletins de livraison, etc.), ont imprimé, sont ä définir comme décrivent toute à l'heure.

1.3.5 Permission des Outqueues pour les impressions confidentielles

Pour des listes confidentielles, comme par exemple des bulletins de salaire, on doit définir des Outqueues spéciales.



Utilisateur *PUBLIC → Autorisation sur *EXCLUDE

Avec la commande WRKOUTQ on doit mis le champ « examiner autorisation »
AUTCHK → sur *OWNER.
OWENER veut dire:
L'utilisateur doit disposer de l'autorisation de propriétaire pour la file d'attente de dépenses, pour réussir le contrôle de la légitimation pour la file d'attente de dépenses. L'utilisateur possède l'autorisation de propriétaire, s'il est un propriétaire de la file d'attente de dépenses ou un profil de groupe utilise en commun ou exporte un programme avec le propriétaire de file d'attente qui se charge de l'autorisation de propriétaire.

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.4 Définitions supplémentaires

1.4.1 Enregistrements

Si un nouvel utilisateur dans l'iSeries est ouvert, pour cet utilisateur, l'ordre ADDDIRE doit également être mis en œuvre.
L'enregistrement de liste est nécessaire p. ex. pour l'ordre CPYFRMSTMF qui entre autres dans le programme « VESR familiarisent » (DEB032V*) sont utilisés.

Suggérez l'ordre ADDDIRE et complétez-vous des champs suivants :

ID utilisateur	USRID	COLLA	Nom du profil d'utilisateur
Adresse		CHFIRMA	Nom du système
Description d'utilisateur	USRD	Collaborateur A	Description du profil

1.4.2 Utilisateurs dans d'autres modules

Avec quelques applications, un utilisateur doit être défini en plus dans le module. Si les modules suivants ont utilisé on doit définir un utilisateur pour le module:

. InfoStore
. IRIS
. FINANZ
. PROFIT
. FAX-Modul
. GISA (si le module d'autorisation est utilisé)

Module E-Mail
Dans le module de courrier électronique doit être considérée que l'utilisateur qui démarre les programmes Background, a besoin de l'autorisation *ALL pour tous les profils utilisateur.

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.4.3 Valeurs du système concernant le mot de passe

De plus, il vaut considérer que pour la définition du mot de passe, des valeurs de système sont existent également. Les valeurs de système suivantes doivent être prises en considération:

Valeur du système	Description		Valeur
QPWDEXPITV	Intervalle pour purge de mot de passe	Intervalle en jour	*NOMAX, 1-366
QPWDLMTAJC	Des signes cohérents dans un mot de passe limiter	Signes voisins	0 = autorisé, 1 = pas autorisé
QPWDLMTCHR	Des signes dans le mot de passe limiter	Signes dans le mot de passe autorisé	*NONE
QPWDLMTREP	Une répétition de signe dans un mot de passe limiter	Signes dans le mot de passe	0 = on peut répéter 1 = ne peut pas répéter 2 = ne peut pas répéter séquentiel
QPWDLVL	Étape de mot de passe	Etape de mot de passe	0 = pour les profils des utilisateurs des mots de passe des signes de 1-10 deviennent soutenaient 1 = pour les profils des utilisateurs des mots de passe des signes de 1-10 deviennent soutenaient. Des mots de passe AS/400 Net Server pour Windows 95/98/ME Clients sont été supprimé. 2 = pour les profils des utilisateurs des mots de passe des signes de 1-128 deviennent soutenaient 3 = pour les profils des utilisateurs des mots de passe des signes de 1-128 deviennent soutenaient. Des mots de passe AS/400 Net Server pour Windows 95/98/ME Clients sont été supprimé.
QPWDMAXLEN	Longueur maximale du mot de passe	Longueur de mot de passe maximale	1-128
QPWDMINLEN	Longueur minimale du mot de passe	Longueur de mot de passe minimale	1-128
QPWDPOSDIF	Des positions de signe dans un mot de passe limiter	Des positions de signe dans un mot de passe	0 = pouvoir être même 1 = ne pouvoir pas être même
QPWDRQDDGT	Chiffres dans un mot de passe nécessairement	Chiffres dans un mot de passe	0 = pas nécessaire 1 = nécessaire
QPWDRQDDIF	Contrôle pour des mots de passe doubles	Mot de passe nouveau	0 = peut être le même mot de passe que avant 1 = ne peut pas être les derniers 32 2 = ne peut pas être les derniers 24 3 = ne peut pas être les derniers 18 4 = ne peut pas être les derniers 12 5 = ne peut pas être les derniers 10 6 = ne peut pas être les derniers 8 7 = ne peut pas être les derniers 6 8 = ne peut pas être les derniers 4
QPWDVLDPGM	Validation pour mot de passe	Bibliothèque programme de test de mot de passe	Nom, *REGFAC, *NONE Nom

Si dans le système QPWDLVL (étape de mot de passe) la valeur est placée à 0 ou à 1, la minuscule et la majuscule n'est pas pris en considération, devient toutefois la valeur 2 ou 3 pondérés, c.-à-d. que les mots de passe sont plus long que 10 signes, on doit tenir compte, de la minuscule et la majuscule. La minuscule et la majuscule dans le mot de passe sont prises en considération.

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.4.4 Concept pour des mots de passe

Afin que les valeurs de système mentionnées ci-dessus puissent être définies, pour la définition des mots de passe, un concept devrait exister.

Ici un article de la revue "Midrange MAGAZIN, novembre 2000".

Tipps für den Umgang mit Passwörtern

kLykotten*mUmpel gegen Anja

Wir leben in einer Zeit der Passwort-Inflation.
Wo früher "geheime Parolen" nur berechtigten bekannt waren, herrscht heute mehr und mehr ein nachlässiger Umgang damit. Die auf Informationstechnik spezialisierte Sicherheitsberatung TÜV NORD SECURITY GmbH aus Hamburg gibt praktische Tipps zum Umgang mit den kleinen Wörtern.

"Wo ist denn der aktuelle Projektstatus für den Umzug unserer Filiale in Bauzen? Der Chef braucht ihn dringend!" ertönt es morgens um 10.00 Uhr in einem Bankunternehmen in Frankfurt.

"Den hat der Mayer zusammengestellt. Aber der ist heute krank." "Hast Du das Passwort für den Computer?" "Warte mal, der hat doch ein Segelboot. Auf dem Foto da steht auch der Name: Probier's mit Serendipity." "Passt nicht!" "Dann den Namen seiner Frau – Anja. Ist ja praktischer, weil kürzer." "Bingo! Danke Kollege!"

Eine Situation, wie sie täglich vorkommt: Passwörter werden nach Praktikabilität gewählt – Namen von Ehefrauen und –männern, Kindern, Hunden, Katzen, Booten oder einfache Tastaturkombinationen wie QWERTZ. Zudem gelten die Wörter meist sehr lange, weil keiner daran denkt, sie zu wechseln.

Gefahr durch Social Hacking

Nach der Erfahrung der Hamburger IT-Sicherheitsberatung TÜV NORD SECURITY müssen für den Passwortklau nicht immer aufwendige Techniken eingesetzt werden. Vielmehr werden PINs grosszügig weitergegeben, im Supermarkt am EC-Kassenterminal allzu offensichtlich eingetippt. In Firmen sind sie häufig dem Zimmerkollegen bekannt oder leicht zu erraten. Hier gelten strikte Regeln: Ein Passwort, das mehr als eine Person kennt, ist wertlos. Ein Passwort, das Bezug auf die eigene Person hat, ist wertlos. Hacker-Profis gehen systematisch vor: Mit so genannten Sniffer-Programmen, die Informationen im Netz abfragen, Tastaturrecordern, die unbemerkt auf einem PC installiert werden und alle Tastaturanschläge speichern oder Passwort-Decodern werden unverschlüsselte oder schwach verschlüsselte Passwörter aus den Systemdateien ausgelesen.

Ein zusätzlicher Sicherheitsfaktor ist das regelmässige Wechseln der Passwörter, da selbst leistungsstarke Rechner einige Zeit benötigen, um Millionen von Begriffen zu scannen: Ein Passwort, das nicht monatlich gewechselt wird, ist wertlos.

Sicherheit durch Fantasie

Die Sicherheitsstrategie eines Unternehmens muss konkrete Anweisungen für die Passwortfindung geben, die entweder von Systemadministratoren oder den Anwendern selbst umzusetzen sind. Um letzteres sicherzustellen, können in Servern Vorgaben gespeichert werden, die nur Passwörter akzeptieren, die ganz bestimmte Anforderungen erfüllen – so etwa Länge, Sonderzeichen, gemischte Schreibweise, kleine reine Zahlenkombination u. a.

*Auf den ersten Anblick mögen die Bedingungen verwirren, aber wer sagt, dass sich ein User nicht den Begriff "kLykotten*mUmpel" merken kann"?*

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

De plus peut être examiné par exemple sur le côté Internet www.datenschutz.ch sous (**Passwort-Check**) contrôles de mot de passe, la sécurité de vos mots de passe.

Mots de passe sûrs

- Au moins une longueur de 8 signes
- ne se composer pas seulement des chiffres
- contenu des lettres minuscule et majuscules en ordre "illogique"
- contenue au moins une signe (* + # $ % & / ( ) = ! " -)
- ne contenue pas les mêmes signes plusieurs fois d'affilés
- plusieurs notions combinent ensemble
- pas de noms, pas de désignations de produit ou des notions de l'environnement de travail
- n'ont pas de relation matérielle vis-à-vis du propriétaire, de sa famille, de son travaille ou de son hobby
- ne pas désigner d'objet cela tombe à l'œil au lieu de travail
- ne pas contenir de notion qui arrive ou pourraient arriver dans des dictionnaires ou ouvrages de référence
- ne contient aucun mot voire, phrases ou semblable
- aucun échantillon de clavier n'est comme par exemple "qwertz"

Des mots de passe modifier régulièrement (au moins tous les 30 jours)!

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch

1.5 Module autorisation

Pour des autorisations au niveau « programmes »; nous vous recommandons notre module d'autorisation. Avec le module d'autorisation existe la possibilité des définitions de sécurité au niveau maison et/ou programmes. Pour certains profils de groupe ou pour différents utilisateurs, des programmes ou des fonctions peut être autorisent respectivement bloqué.

Dans le module d'autorisation, un utilisateur aussi bien qu'un profil de groupe peut être saisis. Vous pouvez autoriser ainsi ou bloquer pour un groupe des programmes ou fonctions souhaités ou bien pour un utilisateur autoriser ou bloquer des programmes ou fonctions souhaités.

Ainsi il est aussi possible qu'un groupe ne soit pas autorisé pour un programme ou une fonction, toutefois un utilisateur particulier de ce groupe reçoive une autorisation.

WEMAG Consulting, Bernstrasse 99, Case postale, 3122 Kehrsatz
Tél.: 031 960 36 36 FAX: 031 960 36 37 E-mail: info@wemag.ch www.wemag.ch