Explication des normes minimales de sécurité

Bavo Van den Heuvel
Cellule Sécurité SPP Intégration sociale

12 janvier 2005 v1.4

POD Maatschappelijke Integratie
SPP Intégration Sociale

Programme de la journée

- 9h-12h: 1re partie sur les normes minimales de sécurité
- 12h-13h: pause de midi
- 13h-15h: 2e partie sur les normes minimales de sécurité
- 15h-16h: audit de sécurité dans les locaux du CPAS pour joindre la pratique à la théorie

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Cellule Sécurité

Cellule Sécurité: aider les CPAS, sur le plan de la sécurité, à se connecter à la Banque-carrefour de la sécurité sociale

Pour toute question sur les flux et la BCSS:

- VVSG: chris.boens@vvsg.be
- BCSS:
  - **Tel: 02/509 58 27**
  - **E-mail: OCMW-CPAS@SmalS-MvM.be**

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Mission

- La mission de cette cellule est:
  - **l'organisation de la politique de sécurité du SPP IS**
  - **l'organisation d'actions de sécurité au profit des 589 CPAS**
- Objectif du helpdesk: fournir de l'aide et des informations aux conseillers en sécurité
- E-mail: helpdesk.security@mi-is.be
- Tel: 02/509.83.48 (tous les mardis)

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Objectif de cette formation

- Objectif de la formation: transposer les normes minimales de sécurité dans les CPAS
- CPAS avancés
- CPAS débutants

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Demandes de formation

- Nous souhaitons obtenir de chaque CPAS un top 5 de leurs questions
- A envoyer à helpdesk.security@mi-is.be
- Base pour les FAQ
- E-mail de rappel
- Posez vos questions maintenant

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

A propos des risques qui sont prévenus:

1 Confidentialité

- Définition: la **confidentialité** est la mesure dans laquelle le droit et la **possibilité** de lire, copier ou consulter sont **limités à un groupe défini de personnes habilitées**.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Non-respect de la confidentialité

Exemples de détournement de données tirées de la BCSS:

- **Assurances**
- **Une agence matrimoniale**
- **Une entreprise d'aliments pour enfants**

Intérêts commerciaux vs données correctes.

Autres exemples.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

A propos des risques qui sont prévenus:
2 Intégrité

- Définition: l'intégrité signifie l'exactitude et l'intégralité de l'information et de son traitement.
- En pratique: facile en format électronique, plus difficile sur papier.
- Fautes intentionnelles ou non:
  - **Les fautes intentionnelles sont par exemple la manipulation de documents importés, de programmes et de traitements et la modification non autorisée de fichiers.**
  - **Les fautes non intentionnelles sont par exemple les erreurs de programmation, les pannes et les erreurs dans la saisie des données.**
- Exemples

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Non-respect de l'intégrité

S'il n'y a pas d'intégrité…

Un cambriolage chez vous porte atteinte à l'intégrité de votre propriété privée

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

A propos des risques qui sont prévenus: 3 Disponibilité

- **Définition de la disponibilité:** pouvons-nous, en tant qu'utilisateurs autorisés, disposer à temps des données dont nous avons besoin pour l'exécution de nos tâches?

5040D mediabox tbv digitale informatiedragers
kbr6205810

5040D mediabox, t.b.v. brandwerende opberging van digitale informatiedragers (zoals CD-R, diskettes, datatapes e.d.). Buitenmaat 32.5x40x31.8cm, binnenmaat 22x13x15cm. Deze mediabox heeft de tetst van 1 uur in de volle brand voor digitale informatiedragers goed doorstaan. Bij een omgevingstemperatuur van ongeveer 1000°C blijft de binnentemperatuur beneden het kritieke punt van 52°C. Kan zeer goed in combinatie met brand- en braakwerende archiefkast worden gebruikt.

€ 259.86

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Disponibilité insuffisante

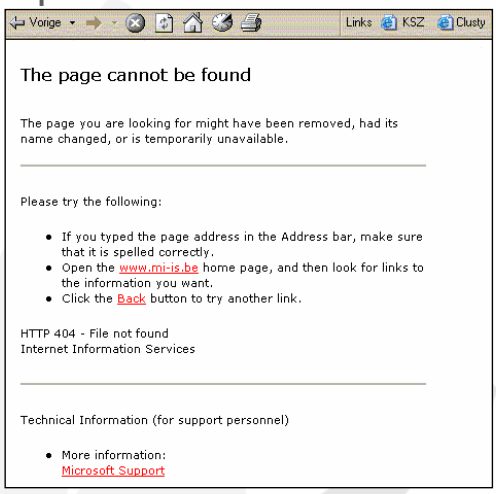
- Si les données ne sont pas disponibles, le CPAS ne peut plus fonctionner, avec tout ce que cela entraîne comme drames humains et politiques.
- Contradiction entre confidentialité et disponibilité.

Banksys-betaalsysteem weigert dienst bij 127.000 aankopen

Afgelopen zaterdagmiddag, uitgerekend tijdens een van de belangrijkste verkoopweekends van het jaar, lieten de betaalautomaten van Banksys het bij 127.000 transacties afweten. Het ging om 100.000 betalingen via Bancontact/Mister Cash en 27.000 betalingen met kredietkaarten Visa en Mastercard. Banksys had gisteren nog geen uitleg voor de onverwachte panne, maar het vermoeden luidt dat het centrale computersysteem het probleem veroorzaakte.

Banksys reageert met de melding dat de pannes slechts iets meer dan 3 procent van de debettransacties vertegenwoordigden, en iets meer dan een kwart van de kredietkaartbetalingen, maar de handelaars en warenhuizen die werden getroffen door de pannes waren er niet blij mee. Retailers schatten de schade op enkele miljoenen euro, de distributeursfederatie Fedis denkt zelfs aan een omzetverlies van 20 procent. Zelfstandigenorganisatie Unizo denkt zelfs een vergoeding te eisen aan Banksys. Ze gaat daarvoor vandaag rond de tafel zitten met de operator. "Honderdzevenentwintigduizend gemiste transacties is veel, laat daar geen twijfel over bestaan", zegt distributiehoofd Luc Ardies van Unizo. "Bovendien zegt het cijfer niet alles over het probleem en de geleden schade: de panne veroorzaakte ook een chaos op een erg druk moment, er zijn consumenten die hun winkelkarretje of hun waren noodgedwongen moesten laten staan."

(RMe)
Algemeen, pagina 3

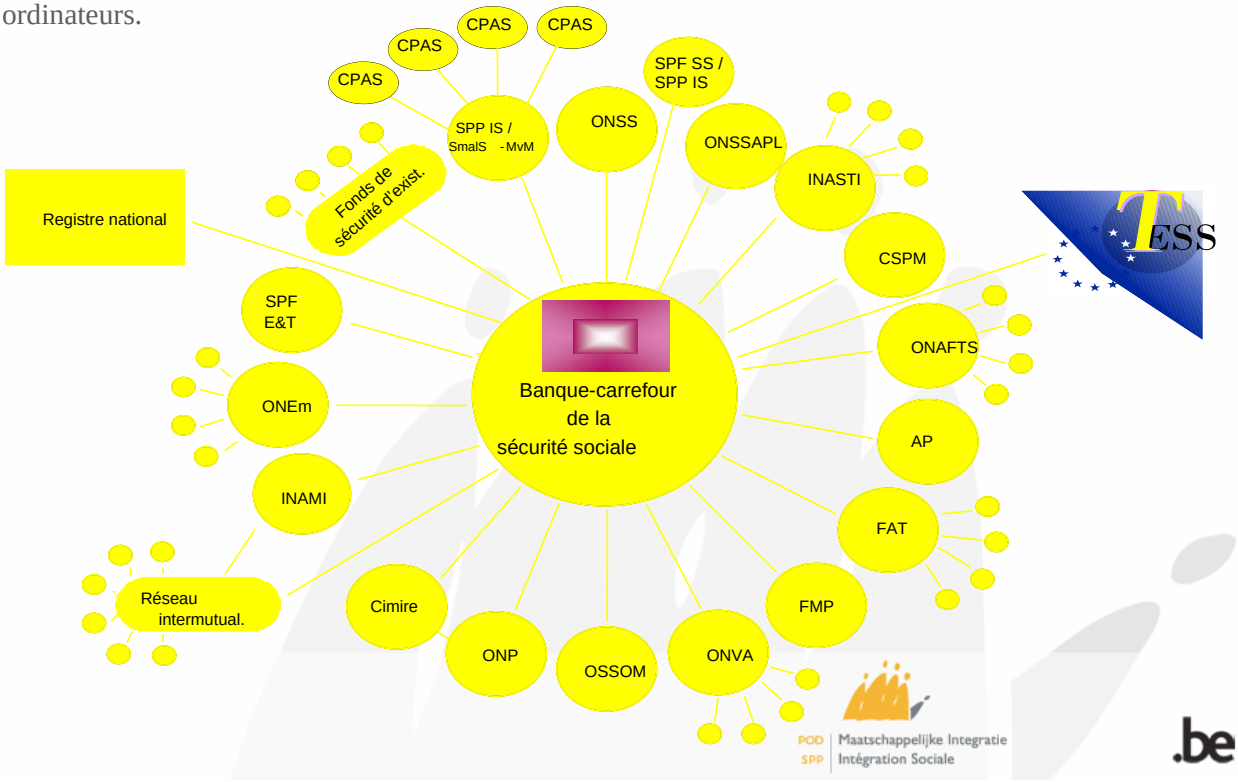


POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Banque-carrefour

- La Banque-carrefour est un réseau électronique entre les institutions de sécurité sociale et le registre national. Les différentes institutions sont reliées entre elles par leurs ordinateurs.



Les messages pour les CPAS

- Consultation des registres national, bis et de la Banque-carrefour, du registre d'attente pour les demandeurs d'asile
- Intégration du dossier revenu d'intégration dans les répertoires de la BCSS et du SPP IS (SmalS-MvM)
- Modification d'une ligne d'intégration dans les répertoires
- Consultation du répertoire secondaire du SPP IS: infos d'autres CPAS
- Consultation du répertoire des personnes de la Banque-carrefour: où les personnes sont-elles connues?

Les messages pour les CPAS

- Attestation multifonctionnelle provenant des CPAS et destinée aux organismes assureurs et au secteur des allocations familiales
- Attestation de carrière (secteur des indépendants)
- Consultation de l'assurabilité auprès des organismes assureurs
- Déclaration revenu d'intégration au SPP IS (A053)

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Normes minimales de sécurité

Source:
http://www.bcss.fgov.be/documentation/fr/s%E9curit%E9/v2002.253.normes.pdf

2.1 Champ d'application des normes:

- La mise en application et la vérification des normes minimales de sécurité auprès de tiers qui traitent des données sociales à caractère personnel (…) appartiennent en premier lieu au CPAS ayant confié les travaux aux tiers.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Normes minimales de sécurité

- Le SPP IS peut, sur base des questionnaires qui lui sont transmis par les CPAS, faire effectuer, après notification préalable, des contrôles par un organisme externe dans des CPAS sur le respect de certains points spécifiques des normes minimales de sécurité.
- Les normes s'appliquent en outre au traitement des seules données sociales à caractère personnel.

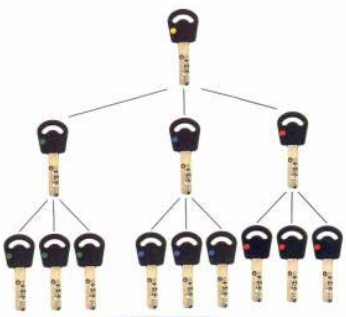
POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Normes minimales de sécurité

2.2. Interprétation des normes

- Il appartient aux institutions de sécurité sociale de mettre en œuvre les mesures de sécurité les plus appropriées compte tenu de leur situation spécifique et de l'importance des moyens de fonctionnement à sécuriser.



POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.1 "Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit disposer d'une politique formelle de sécurité de l'information qui est actualisée en permanence."

Sécurité de l'information: la prévention et la réparation des dommages aux données sociales et des violations illégitimes de la vie privée des intéressés.

(Art. 1 AR 12/08/93 Sécurité de l'information)

Source:
http://www.bcss.fgov.be/documentation/fr/s%E9curit%E9/v2002.253.normes.pdf

But de la politique de sécurité de l'information:

- **sensibiliser** aux risques
- **mettre en place une organisation**
- **favoriser la coordination et l'exécution** des mesures de sécurité
- **augmenter** le **niveau de confiance dans l'informatique** au sein de l'institution.

4.2.1.1 Conseiller en sécurité

- Le conseiller en sécurité est là pour aider le CPAS
- Tâches
- La **responsabilité** du conseiller en sécurité

Cf. aussi **12 AOÛT 1993 – Arrêté royal relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale** Chapitre II (dans ce sens, un CPAS est une institution de sécurité sociale)

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Rapport annuel

AR 12/08/93 Art. 8. Le rapport comprend **au moins**:

1° un aperçu général de la situation en matière de sécurité, de l'évolution au cours de l'année écoulée et des objectifs qui doivent encore être atteints;

2° un résumé des avis écrits et la suite qui y a été réservée;

3° un aperçu des travaux

4° un relevé des résultats des contrôles

5° (...)

6° (...)

7° un relevé des campagnes menées

8° un aperçu de toutes les formations suivies et prévues.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.2 Communiquer l'identité

4.2.1.2. "**communiquer l'identité de son conseiller en sécurité** et de ses adjoints éventuels au Comité de surveillance de la Banque-carrefour de la sécurité sociale" (aujourd'hui le Comité sectoriel de la sécurité sociale)

- Envoyer à: SPP IS, à l'attention de Gilles Kempgens, boulevard Anspach 1, 1000 Bruxelles.
- Aussi le nombre d'heures attribuées
- Approuvé par le CPAS

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.3 Plan de sécurité approuvé

4.2.1.3. "disposer d'un **plan de sécurité approuvé** par l'instance responsable de l'institution concernée."

Il faut "disposer" d'un plan de sécurité approuvé.

Un plan de sécurité est un plan composé de plusieurs parties:

- évolution de l'année précédente
- projets du CPAS pour les 3 années à venir
- évaluation des coûts et du temps nécessaire pour la réalisation des actions

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.4 Avoir des crédits de fonctionnement

- disposer des **crédits de fonctionnement** nécessaires
- **approuvés**
- dans un **budget de sécurité** défini séparément
- **afin de pouvoir prévoir l'exécution de son plan de sécurité**

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.5 Heures du conseiller

4.2.1.5. "communiquer au SPP IS le **nombres d'heures qu'elles ont officiellement attribuées à leur conseiller en sécurité** et à ses adjoints éventuels **pour l'exécution de leurs tâches**"

- Indication de la quantité de travail pouvant être effectuée
- Officiellement sur papier
- Combiner avec d'autres tâches

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.6 Carte professionnelle pour soins de santé

4.2.1.6. “les **conseillers en sécurité** concernés **veillent**, au sein de leur propre institution, **à l’utilisation sécurisée de la carte professionnelle pour soins de santé** comme prévu aux articles 42 à 50 de l’arrêté royal du 22 février 1998”

- Inventaire: cartes SIS et SAM et lecteurs
- La carte amovible est-elle laissée sans surveillance?
- La carte professionnelle est-elle conservée dans un endroit sûr?

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

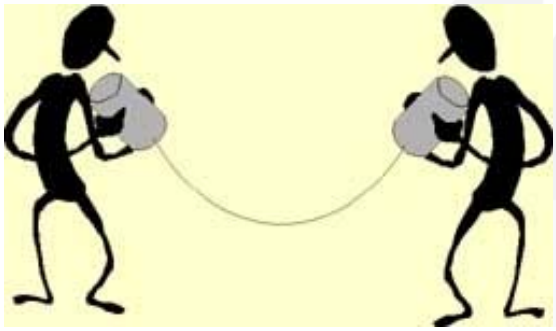
4.2.1.7 Communication au conseiller

4.2.1.7. “**disposer de procédures en vue de la communication d’informations au conseiller en sécurité** de sorte que ce dernier possède les données lui permettant d’exécuter la mission de sécurité qui lui est confiée.”

- données actuelles et correctes pour le conseiller en sécurité
- transmettre quoi?

Canal de communication:

- **informations non sensibles:** e-mail et fax
- pas d’e-mail ou de fax pour les **informations** “**sensibles**”



POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.8 Concertation des parties impliquées

4.2.1.8. "**disposer de procédures ayant pour objectif d'organiser la concertation avec les différentes parties impliquées** afin d'associer plus étroitement les conseillers en sécurité aux travaux de l'institution."

- Sécurité: beaucoup de personnes impliquées
- Concertation centrale
- Régularité

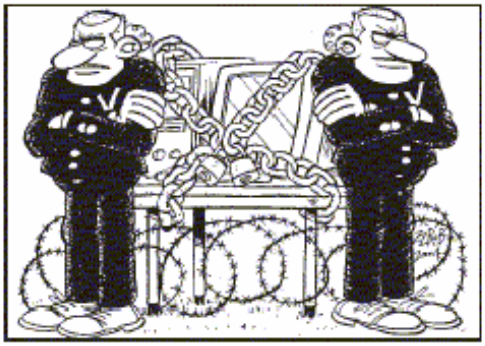
POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.3 Sécurisation physique et sécurisation de l'environnement

Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit:

- **limiter les accès aux bâtiments et aux locaux**
- **prendre des mesures pour la prévention, la protection, la détection, l'extinction et l'intervention concernant l'incendie, l'intrusion et les dégâts des eaux**
- disposer d'une **alimentation électrique alternative**



Zorg voor goede fysieke beveiliging van computerapparatuur

.be

4.3.1 Accès aux bâtiments et locaux

4.3.1. "**limiter** aux personnes autorisées et **contrôler**, aussi bien pendant qu'en dehors des heures de service, les **accès aux bâtiments et aux locaux**."

- Le CPAS a un rôle public
- Badge, clé, passe-partout
- Contrôle social
- Difficultés

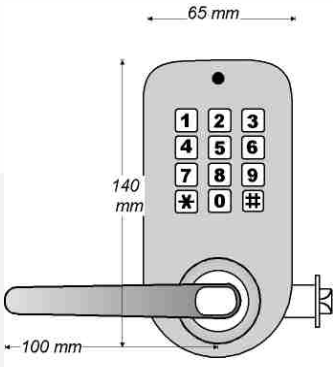
Collapsible gates with cross-lattice

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

En pratique

- Inventorier: qui a accès à quoi, quand et comment?
- Difficultés: localisations dispersées, vieux bâtiments (classés), ferme-portes, évacuation (personnes: sortir, services de secours: entrer)
- Vos expériences



Left hand lock

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.3.2 Prévention, protection, détection

4.3.2. "**prendre des mesures pour la prévention, la protection, la détection, l'extinction et l'intervention concernant l'incendie, l'intrusion et les dégâts des eaux**."

- Base: cartographier les lieux
- Obstacles physiques simples
- Types d'intrusions, méthode du cambrioleur

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

En pratique

- Ralentir l'intrusion!!! (aussi par des obstacles simples)
- Méthodologie: cartographier les lieux
- Types d'intrusion, méthode du cambrioleur

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

En pratique

- Physique et discipline!
- Système de détection des intrusions: code, fausses alarmes, transfert alternatif, alimentation de secours
- Local des serveurs: aération, température, porte, détecteurs, prévention incendie, poussière

4.3.3 Alimentation électrique alternative

4.3.3. “disposer d’une **alimentation électrique alternative** permettant de clôturer sans risque les opérations informatiques”

- UPS (uninterruptible power supply: alimentation non interruptible)
- Objectif: éviter la perte de données
- Inventorisation: serveurs, périphériques nécessaires => importance de l’UPS
- Choix des produits: logiciels, service, installation, tests, entretien
- Attention: ne pas brancher d’imprimantes, fax, lampes, haut-parleurs sur l’alimentation de secours
- Entretien: toutes les alimentations de secours (serveur, alarme, central téléphonique, éclairage de secours, central incendie, …)

Dans la presse

De Morgen on line / telexberichten - Microsoft Internet Explorer provided by MERCURE for INTPMI

Meer en meer pc's besmet met schadelijke software (17/11 08:23)

(Belga) Meer en meer pc's worden besmet met schadelijke software die gebruikmaakt van de telefoonlijn om automatisch nummers te vormen die te veel aanrekenen. Vaak gaat het om nummers met de prefix 0903 (1,25 euro per minuut). Dat schrijft Le Soir woensdag.

Volgens de krant kan de factuur van de slachtoffers van de fraude oplopen tot meer dan 1.000 euro. Volgens Cécile Coppin, coördinator van internettoezicht bij Economische Zaken zijn er sinds het begin van het jaar meer dan 500 klachten binnengekomen, met een toename sinds juli. Vaak gebeurt het dat bij het surfen op het internet dergelijke programma's worden gedownload op de harde schijf van de gebruiker. Volgens een studie van antivirusuitgever Symantec in de Benelux - die volgende week verschijnt - is één computer op drie besmet met zo'n programma. (dwm) *(Belga)*

Microsoft bindt strijd aan tegen spyware

Microsoft brengt, op algemeen verzoek, een eigen programma op de markt dat de computer van zijn klanten beschermt tegen spyware. Maar of de uiteindelijke versie gratis zal zijn, valt nog af te wachten. 'We mogen onze marktpositie niet misbruiken', luidt het bij de softwaregigant.

Er is lang over gepalaverd geweest, en Microsoft heeft het zelfs al eens staalhard ontkend, maar sinds vorige week staat het er wel: een testversie van Microsofts antispyware-toepassing is vrijelijk te downloaden van de website van het bedrijf. Dat gebeurde een beetje op algemeen verzoek: Windows staat wereldwijd op zo'n 95 procent van alle computers geïnstalleerd, en nog eens zo'n 89 procent van diezelfde computergebruikers surft over het internet met Internet Explorer, de webbrowser van het bedrijf. En spyware komt bij uitstek binnen op pc's die onder die software draaien, omdat de makers van al die vuiligheid misbruik maken van 'gaten' in Windows en Explorer. "We moesten onze verantwoordelijkheid opnemen", zegt woordvoerder Frank De Graeve van Microsoft België. Spyware is in geen tijd een huizenhoog probleem geworden bij internetgebruikers. (RMe) (Eigen berichtgeving 05:25)

(c) EFA

4.4.1 Accès aux données

4.4 Sécurisation logique de l'accès

4.4.1. "**sécuriser l'accès aux données** nécessaires à l'application et à l'exécution de la sécurité sociale **par un système d'identification, d'authentification et d'autorisation.**"

Identification: identifier l'utilisateur.

Authentification: le contrôle de l'identité de quelqu'un, avant qu'il n'y ait autorisation.

Autorisation: sur la base d'une table d'autorisation (qui a accès à quoi et quand), le système donnera à l'utilisateur authentifié accès à certain(e)s applications/systèmes/fichiers.

"Your logon password is XB#2D940. Write it down and don't lose it again."

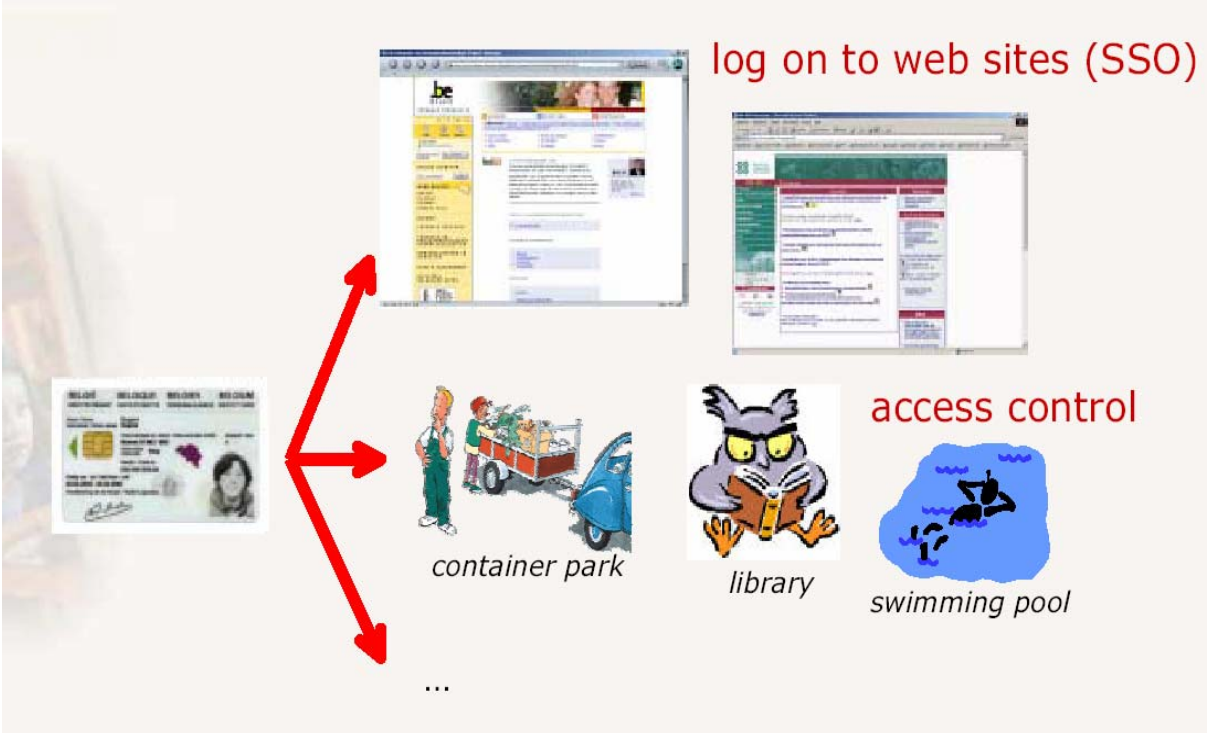
Attaques

Password length	Time needed 26 characters per letter	Time needed 36 characters per letter	Time needed 52 characters per letter
1	325 nanoseconds	4.5 microseconds	6.5 microseconds
2	84 microseconds	0.16 milliseconds	0.34 milliseconds
3	2.2 milliseconds	5.83 milliseconds	0.017 seconds
4	0.057 seconds	0.21 seconds	0.91 seconds
5	1.49 seconds	7.55 seconds	47.53 seconds
6	38.61 seconds	4.53 minutes	41.18 minutes
7	16.73 minutes	2.72 hours	1.48 days
8	7.25 hours	4.08 days	77.34 days
9	7.86 days	146.93 days	11.01 years
10	204.23 days	14.48 years	572.58 years
11	14.54 years	521.35 years	29.77 millennia
12	378 years	18.77 millennia	1.55 million years

Politique de mot de passe

- Importance de la politique de mot de passe
- Complexité du mot de passe (phrase)
- Mémorisation du mot de passe
- Changement du mot de passe
- Sur papier dans le coffre-fort?
- Lisible dans la table du logiciel social?
- Aspect juridique
- Possibilités e-ID (carte d'identité électronique)

Carte d'identité électronique



POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.4.3 Copie de sécurité

4.4.3. "mettre en place un système de **copie de sécurité (back-up)**, régulièrement contrôlé, **permettant de s'assurer**, en cas de sinistre total ou partiel, **qu'aucune perte de données irréparable ne puisse survenir** (données nécessaires à l'application et à l'exécution de la sécurité sociale ainsi que celles concernant les applications et le système d'exploitation)."

Pourquoi?

- réseau de la sécurité sociale: données décentralisées
- **données relatives à vos clients CPAS**: conservées chez vous seulement
- **perte de données** chez vous: conséquences
- **aussi les données des applications et systèmes d'exploitation**
- en cas de sinistre: redevenir entièrement opérationnel à partir de rien.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Schéma de rotation des médias

weekdag	MediumNr	Week 1	MediumNr	Week 2	MediumNr	Week 3	MediumNr	Week 4	MediumNr	Week 5
maandag	1	Dagelijkse incrementele back-up	7	Dagelijkse incrementele back-up	1	Dagelijkse incrementele back-up	7	Dagelijkse incrementele back-up	1	Dagelijkse incrementele back-up
dinsdag	2	Dagelijkse incrementele back-up	8	Dagelijkse incrementele back-up	2	Dagelijkse incrementele back-up	8	Dagelijkse incrementele back-up	2	Dagelijkse incrementele back-up
woensdag	3	Dagelijkse incrementele back-up	9	Dagelijkse incrementele back-up	3	Dagelijkse incrementele back-up	9	Dagelijkse incrementele back-up	3	Dagelijkse incrementele back-up
donderdag	4	Dagelijkse incrementele back-up	10	Dagelijkse incrementele back-up	4	Dagelijkse incrementele back-up	10	Dagelijkse incrementele back-up	4	Dagelijkse incrementele back-up
vrijdag	5	Dagelijkse volledige back-up	11	Dagelijkse volledige back-up	5	Dagelijkse volledige back-up	11	Dagelijkse volledige back-up	5	Dagelijkse volledige back-up
	6	Back-up Informatica-omgeving	12	Back-up Informatica-omgeving	6	Back-up Informatica-omgeving	12	Back-up Informatica-omgeving	6	Back-up Informatica-omgeving
	I	Wekelijkse Back-up 1	II	Wekelijkse Back-up 2	III	Wekelijkse Back-up 3	IV	Wekelijkse Back-up 4	V	Wekelijkse Back-up 5

4.4.2 Système de logging

4.4.2. "**un système de logging pour les données à caractère personnel** nécessaires à l'application et à l'exécution de la sécurité sociale."

Quoi?

- Logging: données historiques (qui, quoi, quand)

Pourquoi?

- Rôle du conseiller en sécurité
- Utile aussi pour la lutte contre les virus etc.

! Intégrité du logfile: localement et pour le logiciel social

Attention: une politique de conservation des loggings doit également être mise sur pied

SYSLOG, qui est très utilisé, a beaucoup de points faibles: pp. 2-5 dans www.giac.org/practical/GSEC/Kenneth_Nawyn_GSEC.pdf

4.4.4 Détecter les infractions à la sécurité

4.4.4. “installer **un système <u>et</u> des procédures formelles et actualisées** permettant de **détecter des infractions à la sécurité, de les suivre et de les réparer.”**

- **Tâches manuelles**: examiner les logfiles, examiner le trafic internet
- **Suivi** des infractions à la sécurité
- **Réparation** des infractions à la sécurité

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

4.4.5 Relation partie préfixe – identité de l’utilisateur

4.4.5. “Lorsque, dans la zone “USERID” de la partie préfixe d’un message qu’elle adresse à la Banque-carrefour, l’institution reprend le numéro du programme qui a généré le message qu’elle adresse à la Banque-carrefour (…) **Dans ce cas, c’est donc au CPAS qu’il revient de faire la relation entre le numéro de programme qu’il reprend dans la partie préfixe du message qu’il adresse à la Banque-carrefour et l’identité de la personne physique qui émet le message**.”

Quoi?

Le CPAS doit faire en sorte que la Banque-carrefour puisse toujours savoir a posterori quelle personne physique a échangé des messages électroniques avec elle.

Pourquoi?

Pour savoir, en cas de problème, qui en est à l’origine.

Comment?

Par le programme utilisé pour la communication avec la Banque-carrefour. Le conseiller en sécurité doit toujours tenir à jour un inventaire de l’identité des utilisateurs pour pouvoir faire correspondre les numéros d’utilisateurs et les noms.

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

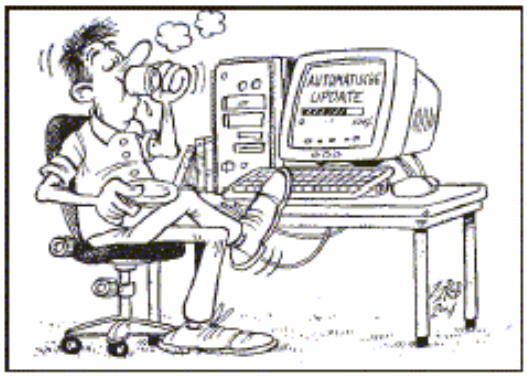
4.5 Les applications

4.5. Développement, production et maintenance des applications

Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit :

4.5.1. **disposer de procédures formelles et actualisées pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes** afin d'éviter qu'une seule et même personne n'assure le contrôle de ce processus.

4.5.2. **disposer de procédures formelles et actualisées en vue d'élaborer la documentation lors du développement de nouvelles applications et lors de la maintenance des applications et systèmes existants.**



Installeer tijdig softwarereparaties (verkregen van een betrouwbare bron)

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Procédures

4.5.1. **disposer de procédures formelles et actualisées pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes** afin d'éviter qu'une seule et même personne n'assure le contrôle de ce processus.

4.5.2. **disposer de procédures formelles et actualisées en vue d'élaborer la documentation lors du développement de nouvelles applications et lors de la maintenance des applications et systèmes existants.**

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Clause “escrow”

- Déposer le code-source du logiciel auprès d’un intermédiaire
- Réclamable en cas de faillite ou autre mise en demeure
- Auprès d’un notaire ou d’une firme spéciale
- Vérifier que ça fonctionne!
- Pour chaque nouvelle version, un nouveau dépôt

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.6.1 Limiter l’accès et détecter les infractions à la sécurité

4.6 Protection du réseau

4.6.1. **Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit:**

4.6.1.1. **limiter l’accès au(x) système(s) informatique(s)** aux personnes/objets identifiés, authentifiés et autorisés.

4.6.1.2. **installer un système et des procédures formelles et actualisées permettant la détection, le suivi et la réparation d’infractions au niveau de la sécurité**.

Systèmes informatiques: les appareils et les ordinateurs physiques utilisés pour le traitement des données

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.6.3 Réseau secondaire

4.6.3. Les **institutions de sécurité sociale du réseau secondaire <u>peuvent</u>** utiliser l'extranet de la sécurité sociale pour leurs liaisons TCP/IP externes à la sécurité sociale. Pour leurs liaisons directes avec les réseaux TCP/IP externes à la sécurité sociale:

- les **institutions concernées du réseau secondaire doivent mettre en œuvre des mesures de sécurité qui sont et restent conformes aux mesures prises au niveau de l'extranet de la sécurité sociale.**

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Pare-feu (firewall)

- Un PC non protégé est piraté en 20 minutes
- Responsabilité de l'administration: le fait de ne pas prendre de mesures de protection est aussi punissable! (faire particulièrement attention dans le cas des réseaux sans fil)

Platform	Total attacks	Attacks / day	Attacks / hour
XP SP1	139,024	8,177	341
OS X	138,647	8,155	339
Win SBS	25,222	1,400	61
XP SP2	1,386	82	3.4
XP with ZoneAlarm	848	50	2.1
Linspire	795	46	1.9

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

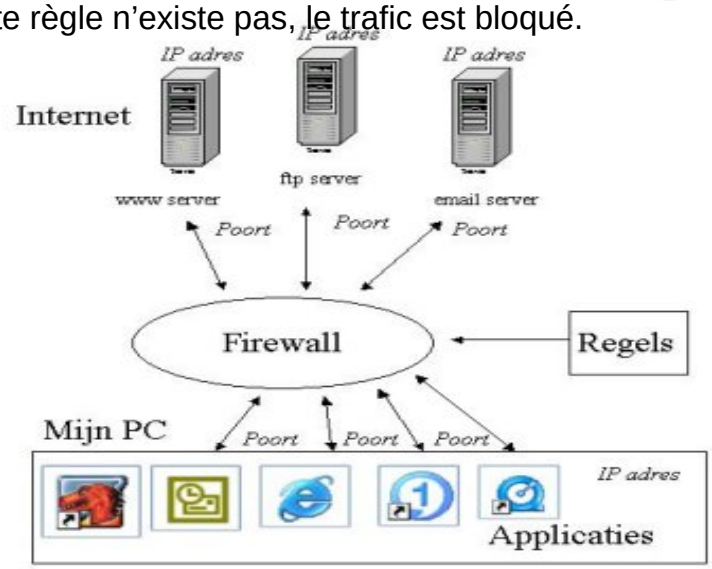
Fonctionnement du pare-feu: vue d'ensemble

Un pare-feu filtre, sur la base d'un ensemble de règles, tout le trafic entrant et sortant.

Une règle décrit sur quel port quelle application fonctionnant localement peut communiquer avec un serveur (www, ftp, e-mail, etc.) sur internet.

Au moment où une connexion est établie (de l'extérieur vers l'intérieur ou de l'intérieur vers l'extérieur), le pare-feu contrôle s'il existe dans la base de données une règle permettant ce trafic.

Si cette règle n'existe pas, le trafic est bloqué.



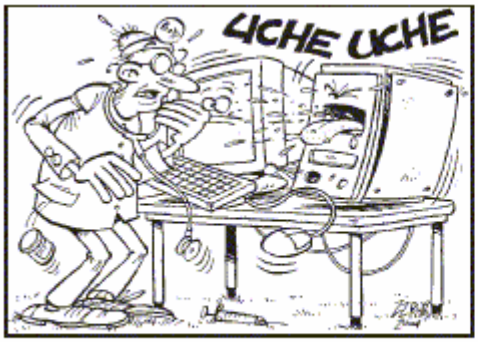
4.9 Virus

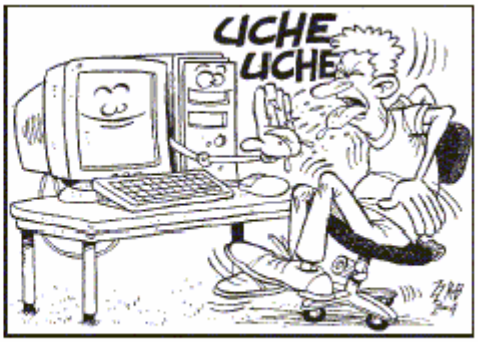
4.9. Protection contre les infections par les virus informatiques

Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit:

4.9.1. **disposer d'un manuel d'utilisation relatif à la prévention d'infections par les virus**, au fonctionnement du logiciel antivirus installé et aux actions à entreprendre en cas d'infection par un virus.

4.9.2. **installer un logiciel antivirus actualisé** afin de prévenir, de détecter et de corriger des infections par des virus informatiques.





Installeer een virusscanner en houdt deze up to date

Lutte contre les virus et autres

- Sources de virus
- Chaînes de lettres
- **Logiciels espions (spyware)**
- Canulars (hoax)
- Macro-virus
- ***Il vaut mieux prévenir que guérir***
  - Veillez à ce que votre système d'exploitation et vos logiciels soient à jour
  - Ayez un antivirus (et des fichiers de définition de virus) récent(s) dans votre système
  - Exécutez régulièrement (si possible automatiquement) l'antivirus
  - Contrôlez avant d'ouvrir/de télécharger/d'installer

Actions en cas d'infection:

- Ne paniquez pas, n'éteignez PAS votre poste de travail, notez ce que vous avez vu, empêchez toute propagation à d'autres ordinateurs, prévenez (pas par e-mail) l'administrateur système/l'administrateur local du PC, n'utilisez pas votre poste de travail avant qu'il ne soit 'désinfecté', n'allez pas travailler sur un autre poste de travail avec vos disquettes/cartes mémoire, avertissez votre entourage, de préférence par téléphone.

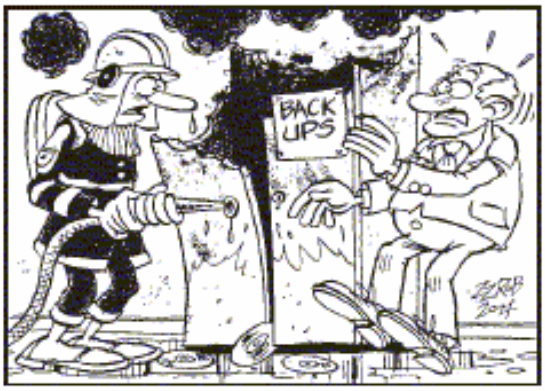
L'administrateur:

- Essayer de détecter le virus, l'antivirus peut éliminer lui-même certains virus, aller chercher des informations sur la façon d'éliminer le virus sur le site web du fournisseur de votre antivirus (y accéder par un autre PC), éliminer le virus de toutes vos disquettes, essayer de remédier au moyen des back-ups aux dommages qui ne sont pas réparables par l'antivirus, comprendre comment l'infection a pu se produire

Utilisation de l'e-mail/d'internet

- Utilisation, groupe-cible
- Abus
- Contrôle/logiciel de contrôle
- Chasse aux sorcières
- Signature numérique/cryptage
- Sanctions: top-down, gradation, statut de la personne
- Nétiquette
- Justice
- On peut faire beaucoup de prévention en rendant certaines choses impossibles à réaliser pour l'utilisateur

Plan de continuité



Maak en test regelmatig een backup en bewaar deze op een veilige plek

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Inventaire

4.8. Inventaire

Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit disposer d'un **inventaire du matériel informatique et des logiciels qui est mis à jour en permanence.**

Inventaire = qu'utilisons-nous pour l'instant et pour quoi?

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Analyse des risques

4.7.1. **réaliser une analyse des risques** permettant l'élaboration d'un plan de continuité.

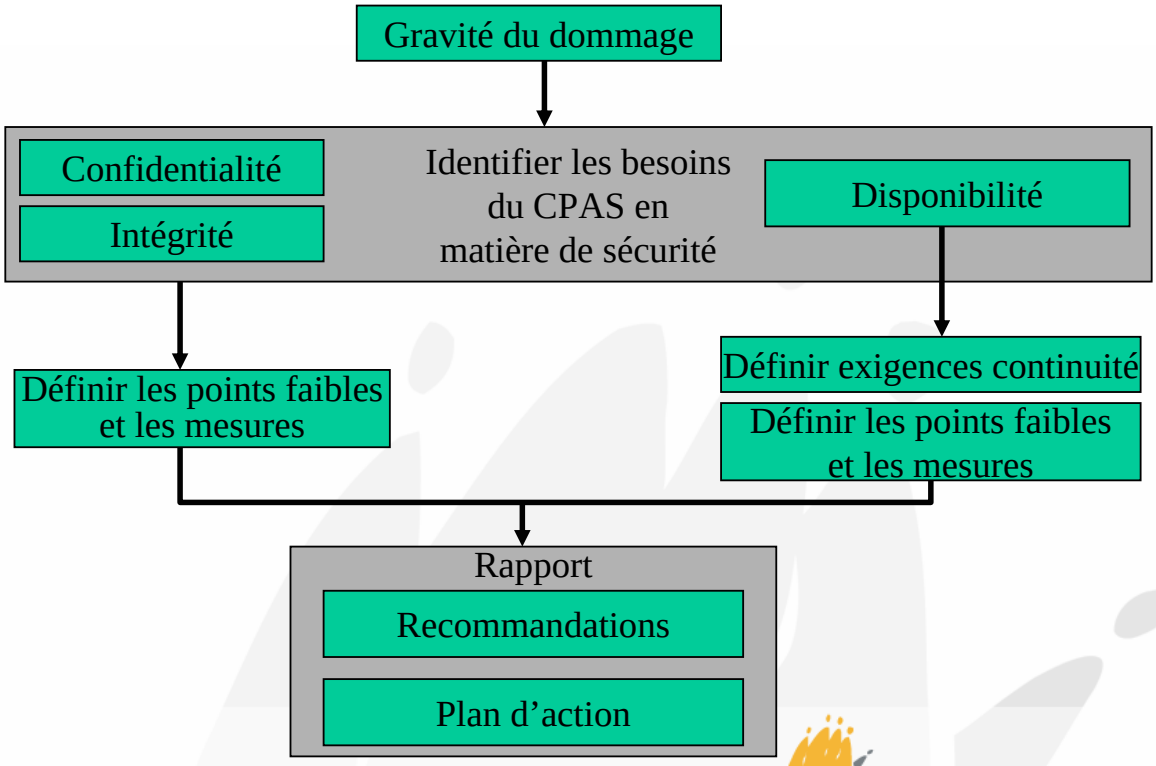
points faibles qui – en cas de **sinistre** – gênent le travail du CPAS

mesures pour faire en sorte que – en cas de **sinistre** – le **CPAS puisse recommencer à travailler après x jours**

Classer les risques

=>se faire une idée des coûts et bénéfices des investissements en matière de sécurité.

Schéma



Plan de continuité

4.7.2. **élaborer**, tester et maintenir un **plan de continuité** afin de pouvoir garantir les missions de sécurité sociale de l'institution. **En outre, elle doit prévoir un centre de migration informatique en cas de sinistre partiel ou total.**

Plan de continuité: vise spécifiquement la situation qui suit un sinistre et doit fournir une réponse à la question: "Comment continuer?".

Centre de migration informatique: la commune dont dépend le CPAS a souvent de nombreux bâtiments. Un centre de migration peut abriter temporairement le redémarrage des activités du CPAS.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

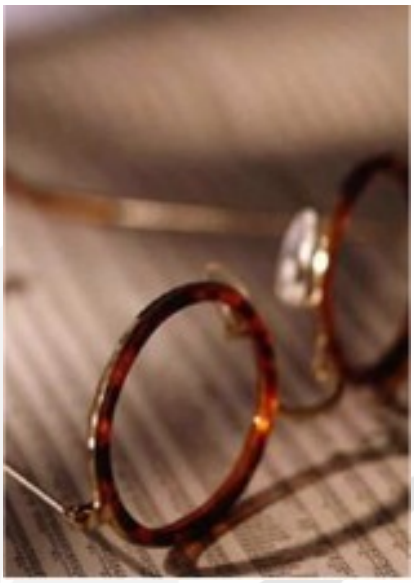
Audit

4.10. Surveillance/audit

Chaque institution de sécurité sociale connectée au réseau de la Banque-carrefour doit **organiser, au moins une fois tous les quatre ans, un audit concernant la situation de la sécurité tant au niveau logique que physique**.

Mutuel

Check-list



POD SPP Maatschappelijke Integratie Intégration Sociale

.be