Groupe de travail

Sécurité des Systèmes de l'Information de l'IN2P3

Thierry Mouthuy – Chargé de mission SSI de l'IN2P3

Le programme

Les données des laboratoires
L'organisation de la SSI
Les accès au SI
Le contrôle
L'état des lieux

Ceci n'est pas une liste exhaustive, ni un cours.
C'est juste une sensibilisation à certains aspects...

Les données des laboratoires

Les données = Base principale de notre connaissance
Les préserver est une **OBLIGATION !**

Classification des données

Secret défense, caractère personnel, diffusion restreinte...
Secret professionnel, secret des correspondances,...

Problèmes potentiels : **Fuite et/ou diffusion**

- Fuite volontaire, ou non, espionnage, social engineering, perte accidentelle
- Impact éventuel au pénal et au civil ! Impact financier
- Services gratuits → Revente d'information !?, pas de garantie de confidentialité, d'intégrité ni de disponibilité

Les données des laboratoires

Solutions à la fuite des données?

- Une organisation
  - Définir des politiques communes et acceptées
- Une sensibilisation des utilisateurs
  - Comment éviter le social engineering ?
  - Comment éviter l'utilisation de services gratuits ?
- Des solutions techniques ?
  - Le filtrage des connexions
  - Le chiffrement est une bonne solution (portables, clefs USB,...)

Les données des laboratoires

Comment éviter l'utilisation des services gratuits ?

- Proposer des alternatives...
- Soit les interdire....
- En tous cas, EDUQUER, SENSIBILISER !

p.ex. Différents types de clouds :

- cloud privé
- cloud hébergé (CNRS)
- cloud communautaire (p.ex. commun aux universités)
- cloud public (p.ex. Google)

L'organisation de la SSI

Organisation de la SSI au CNRS

Contexte difficile pour les RSSI/CSSI au CNRS

- Informatique diffuse ! Beaucoup d'unités...
- Peu de moyens humains et financiers
- Beaucoup d'offres alléchantes du type « Cloud »
- Nomadisme (portables, smartphones...)
- BYOD – Mélange des sphères

Nouvelle structure au CNRS (DSI)

→ Louis Di Benedetto et François Morris (adjoint)

Fonctionnaire de sécurité et de défense

→ Philippe Gasnot

Organisation SSI

Politique CNRS : 2006 !

Constat :

- CSSI : 60 % en moyenne – 80 % dans les ERR
- Pas de PSSI (10 % dans ERR, 3 % dans les autres)
- Niveau faible de chiffrement des portables

Groupes de travail

- Règles élémentaires de sécurité → PSSI générique
- Recommandations techniques aux DU et utilisateurs
  - Notes aux DU sur le vol des portables et le chiffrement
  - Plan d'actions à mettre en place par unité
- Traitement des incidents – action concertée Cert/Certa
- Sensibilisation

Organisation SSI

- **Pilotage CNRS : DSI – Rôle du FSD à clarifier**
- **Problème des unités mixtes ! Qui pilote ?**
  Université, école, ...
- **Couche supplémentaire : IN2P3**

En pratique, les 3 instances ont un rôle :

⇒ Les tenir toutes au courant

⇒ Travailler ensemble

L'accès au Service de l'Information

Les accès

Nos données sont en général protégées de l'extérieur !
Mais l'accès externe est possible ! Et ouvert !

Les mots de passe : En général la protection tient à une simple chaîne de caractères...

Exemples :

- Login
- Messagerie
- Web
- SVN...

Accès non contrôlé : p.ex. teamviewer...
Solution ? Bomgar (hébergé au CC) et filtrage total ?

Les accès

- Mots de passe
  - Nécessité d'avoir des mots de passe solides
  - Nécessité de les changer régulièrement (vieillissement !)
  - Nécessité d'avoir des mots de passe différents !
- Risques en cas de perte ?
  - Accès frauduleux → perte de confidentialité
  - Envoi de spam → atteinte à l'image, blacklist, …
  - ...

Exemples de problème :

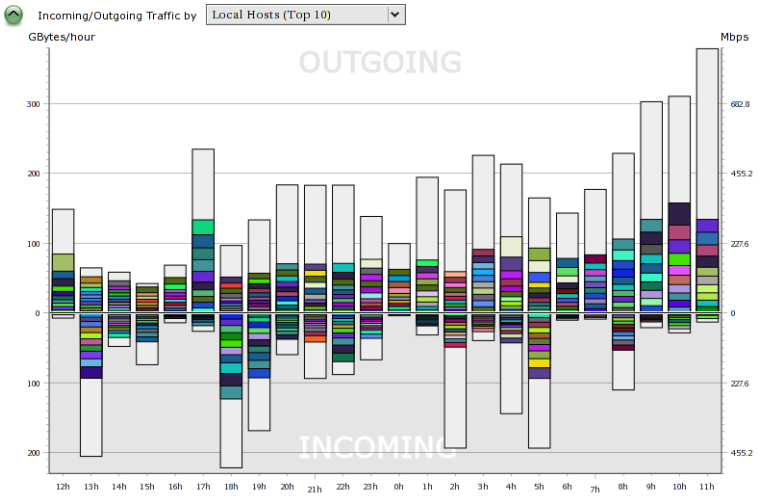
- Un service web piraté stockait les mots de passe en clair !
- Le Phishing

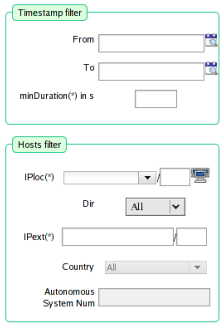
Le contrôle et les traces

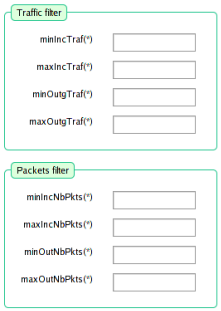
Le contrôle

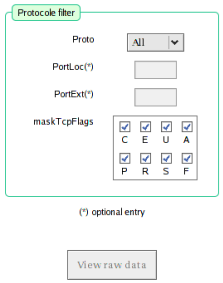
Nouveau système d'enregistrement des logs et d'analyse ZNETS (Th.Descombes et I.Zakari-Toure du LPSC)

- Déployé dans tous les labos
- Analyse sur 15 minutes et alertes
- Graphiques d'utilisation
- Interrogation simple









FirstTime	LastTime	IpLocal	Dir	IpExtern	ASNum	Proto	PtLoc	PtExt	TcpFlg	IncTraf	OutgTraf	IncPkts	OutgPkts	Duration
Aggregation period started at : 2012-10-09 12:00:00														
11:17:26	11:45:12	134.158.17.56	>	173.194.34.1		6	*	80	APSF	52	104	1	2	00:27:46
11:43:17	11:45:15	134.158.17.56	>	173.194.34.8		6	45785	80	APSF	52	104	1	2	00:01:58
11:45:52	11:45:52	134.158.17.56	>	212.27.48.3	12322	6	52768	110	APSF	573	468	11	9	00:00:00
11:47:03	11:47:03	134.158.17.56	<	61.134.47.198	4134	1	8	0		28	0	1	0	00:00:00
11:47:03	11:47:03	134.158.17.56	>	61.134.47.198	4134	1	*	0		0	28	0	1	00:00:00
11:45:50	11:47:50	134.158.17.56	<	193.51.224.6	2200	6	42969	80	APSF	8603	723	8	8	00:02:00
11:52:36	11:52:40	134.158.17.56	>	137.138.210.206	513	1	8	0		0	420	0	5	00:00:04
11:52:37	11:52:40	134.158.17.56	<	137.138.210.206	513	1	0	0		336	0	4	0	00:00:03
21:33:10	11:52:46	134.158.17.56	>	134.158.66.63	789	1	8	0		0	420	0	5	7 days 14:19:36
15:32:56	11:52:46	134.158.17.56	<	134.158.66.63	789	1	0	0		420	0	5	0	2 days 20:19:50
14:03:24	11:52:54	134.158.17.56	>	139.124.70.130	2200	1	8	0		0	420	0	5	8 days 21:49:30
02:32:52	11:52:54	134.158.17.56	<	139.124.70.130	2200	1	0	0		420	0	5	0	09:20:02
07:46:00	11:53:10	134.158.17.56	>	212.27.42.94	12322	6	47184	993	APS	638	778	6	9	04:07:10
11:53:26	11:53:26	134.158.17.56	<	221.2.209.46	4837	6	64	6000	S	40	0	1	0	00:00:00
07:55:36	11:55:58	134.158.17.56	>	193.251.214.116	3215	6	*	993	APRSF	2374	1127	14	13	04:00:22
11:46:09	11:56:09	134.158.17.56	>	134.158.69.22	789	6	*	119	APSF	2599	2229	29	33	00:10:00
11:57:36	11:57:36	134.158.17.56	>	188.92.145.71	44919	6	33334	80	APSF	794	432	5	5	00:00:00
11:57:37	11:57:39	134.158.17.56	>	134.158.69.50	789	6	*	443	APRSF	39845	2598	30	32	00:00:02
11:57:37	11:57:39	134.158.17.56	>	134.158.69.50	789	6	*	80	APSF	1586	950	8	12	00:00:02
07:46:00	11:59:49	134.158.17.56	>	134.158.66.63	789	6	*	993	APRSF	150611	14258	158	154	04:13:49
07:45:54	11:59:58	134.158.17.56	>	134.158.69.140	789	6	54564	5223	APS	1752	1512	17	12	04:14:04

L'état des lieux à l'IN2P3

Etat des lieux

Problèmes récurrents :

- **Vol de portables** :
  - 9 en 2011 (dont 1 avec des documents très sensibles – Aucun chiffré !) et 1 smartphone
  - 11 jusqu'à octobre 2012 (dont 2 chiffrés !)
- **Phishing** ! 17 personnes en 2011 – 1 seule en 2012
- TOR (anonymiseur) – Interdit sur nos réseaux
- **P2P** : 20 utilisations → 2 plaintes Colombia et 1 Renater
- **Hébergement externe** en augmentation !

Exemple de problème :

- **vol de mot de passe** de messagerie (probablement dans un cyber café) → une utilisation frauduleuse de notre passerelle d'envoi de mails pour diffuser massivement du spam

Etat des lieux

Chiffrement des portables

- Environ 2700 portables à l'IN2P3
- Lettre envoyée aux DU
- Constat : Taux de chiffrement trop faible !

	Pas de réponse	Pas de chiffrement	<= 10 %	<= 50 %	100 %
Nouveaux PC	**4**	**5**		**5**	**4**
Anciens PC	**4**	**10**	**5**		

Conclusions

Conclusions

Messages à faire passer à tous nos utilisateurs !!!

- Jamais de demande de mot de passe par les SI
- Attention au vol de mot de passe !
- Changer et diversifier vos mots de passe

- Réfléchir aux données manipulées – les garder au laboratoire ou les chiffrer !
- Chiffrer systématiquement ce qui peut l'être !

- Attention aux appareils très mobiles (smartphone etc) !

- La SSI doit être présente à toutes les étapes...
  ⇒ aussi dans les développements logiciels !

  Intégrez votre CSSI dans la boucle !