

Journée des Nouveaux Entrants

Sensibilisation SSI

Jean-Claude Chevaleyre (CSSI) – 12 Novembre 2023

Le cadre de la SSI – Sécurité des Systèmes d'Information

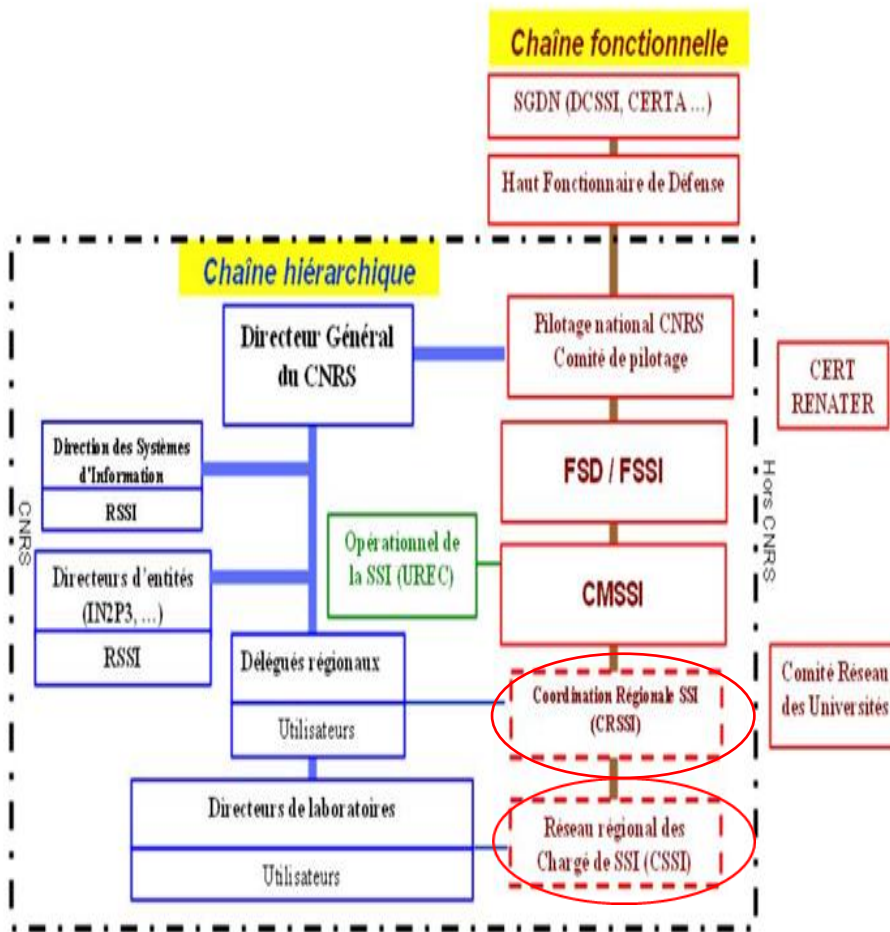


Schéma de déclinaison de la PSSI au sein du CNRS



CSSI : J-C. Chevaleyre

CSSI Adjoint : T. Mallet

3 Grandes Questions : Pourquoi , Qui , Comment

Le cadre de la SSI – Sécurité des Systèmes d'Information

Pourquoi être attentif ?

Développement exponentiel des objets connectés : PCs, Telephones, IoT, ...

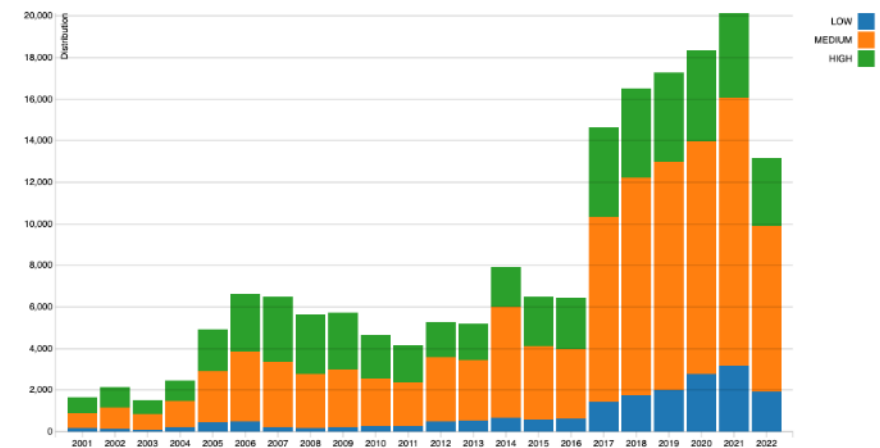
De nouveaux protocoles de communication : filaire , wifi , bluetooth, NFC



Accroissement Des Risques et Failles

CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the [NVD CVSS page](#).



Pourquoi Suite ?

Critères - Risques - Conséquences

Critères	Attaques	Conséquences
Confidentialité	Divulgateion d'information Accès non autorisé : accès à des données sensibles Détournement à des fins malveillantes	Pertes du patrimoine scientifique pertes d'avance technologique et technique pertes financières contentieux juridiques
Disponibilité	Vols Sinistres Malwares, virus, Hameçonnage, ...	Interruption de service Saturation de service Perte de données Réputation engagée
Intégrité	Modifications volontaires, accidentelles Détournements de moyens informatiques Malware, chevaux de Troie , sniffeurs	Expérimentations non crédibles Prises de décisions inadaptées Atteintes aux libertés individuelles Images de marques

Qui peut agir ? Quels sont les Acteurs ?



Le Directeur



L'Informaticien



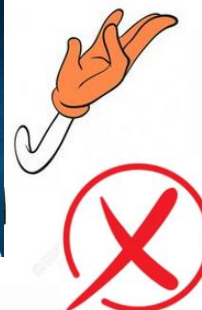
Le Chercheur
Les Collègues

**Tous Ensemble, Tous Ensemble , Qui ne saute pas dans le piège
Ne clique pas**

** toute ressemblance avec des personnages existants ou ayant existé serait purement fortuite*

Le facteur humain est actuellement
l'un des plus grands dangers pour la
SSI

Click & Collect



Comment se prémunir ?

Ne pas cliquer précipitamment ou en cas de doute

The diagram shows an email interface with the following content:

Sender: Sonia Abelona <Sonia.Abelona@cern.org>

Subject: Sonia Abelona has shared a file with you

To: [Redacted]

Body:

Dear [Redacted]

Please see the attached for your 2019 contract amendment request

Regards
Sonia Abelona
Manager at Human Resources

Contract amend...21.doc

Callout Questions:

- Is the sender familiar to you?
- Is the e-mail address correct? (for example @cern.ch)
- Does the e-mail address correspond with the sender's name?
- Is the message correctly phrased, without major typos, in a language that you can understand?
- Does the message concern you? Is it related to your work or activities?
- Is the message signed ()?
- Is the message addressed to you?
- Do you expect this attachment?

Warning: If you have answered any one of those questions with "NO" be vigilant and careful! Delete that message or check with us at abuse@clermont.in2p3.fr when in doubt.

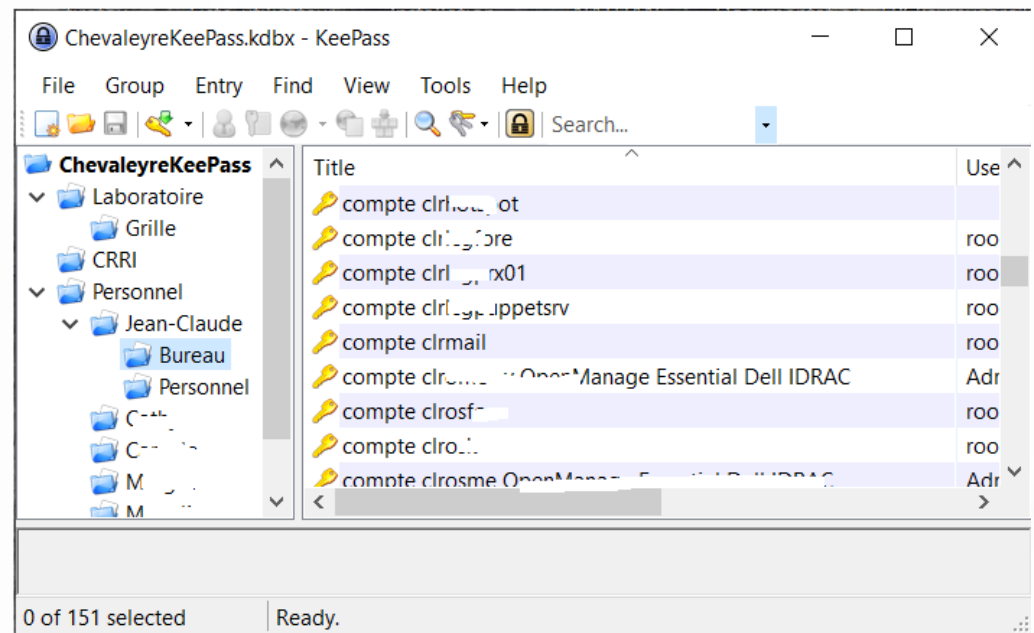
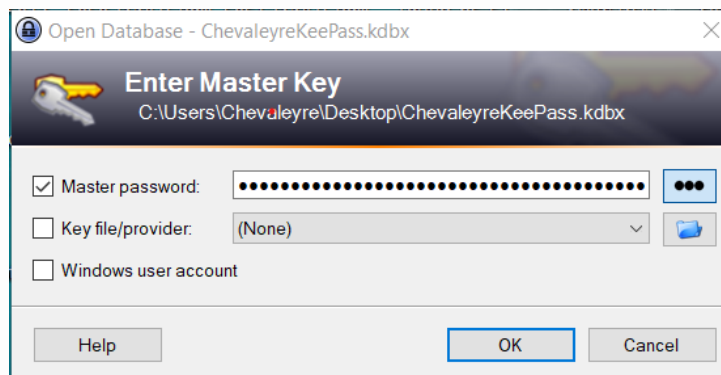
Comment agir concrètement ?

- ✎ Séparer usage professionnel et usage privée (courriel, ...)
- ✎ Des mots de passe fort (> 10 caractères , sans mot du dictionnaire, nom propre, information publique , ...), pour votre usage propre
- ✎ Un mot de passe pour chaque usage
- ✎ Votre compte courriel est devenu un élément hautement sensible



Un outils homologué ANSSI : KeePass / KeePassXC

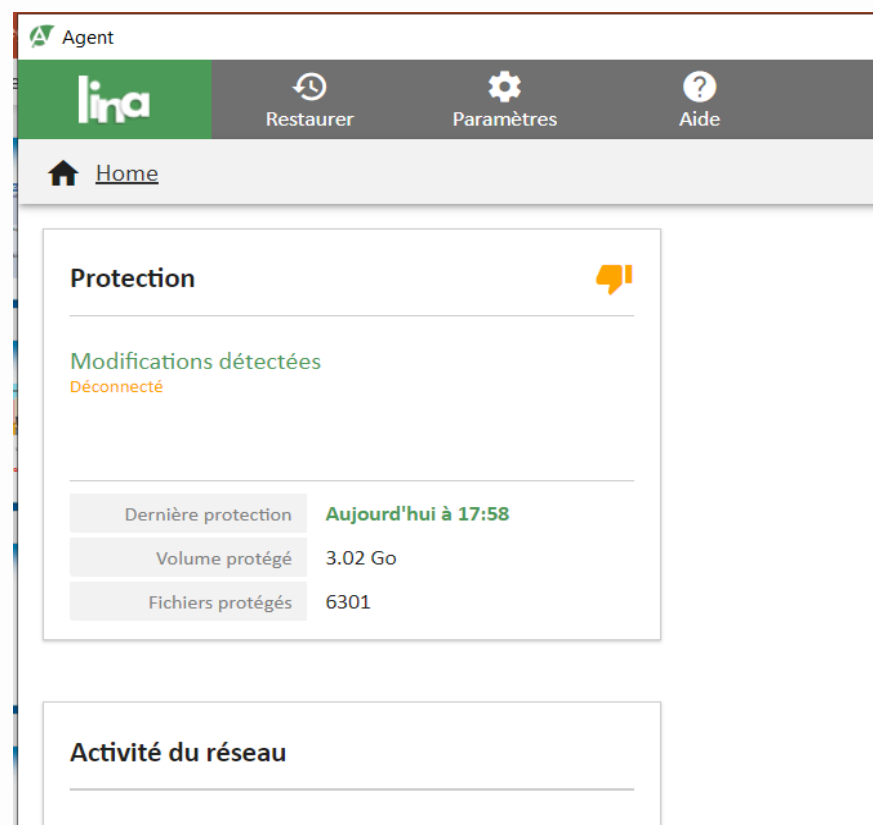
<https://keepass.info/>



Comment agir suite ?

Le chiffrement des poste nomades : Injonction du CNRS
Copier (multiples) n'est pas sauvegarder

Une sauvegarde fournit un historique des modifications d'un objet dans le temps sur un support distant. La version « n-1 » d'une version « n » corrompue ne peut-être impacté.



Un outil à disposition : **LiveNavigator** à disposition fournis par le service Informatique

Focus : La messagerie Electronique 1/5

The screenshot shows a web browser window with the Zimbra webmail interface. The browser's address bar shows the URL `lpc-mail.in2p3.fr/#6`. The Zimbra interface has a blue header with the logo and a search bar. Below the header is a navigation bar with tabs: Mail, Contacts, Calendrier, Tâches, Porte-documents, Préférences, and Notification en [X]. The 'Mail' tab is active, showing the 'Compose' screen. The 'To' field contains the email address `"Service d'assistance" <alex.jacquesson@ijclab.in2p3.fr>`, which is circled in red. The 'Cc' field is empty. The 'Subject' field contains the text `Notification en attente : Le service d'assistance partage un fichier avec vous.`. The 'Attachments' section shows a file named `Zimbra Web Client Sign In.htm (23,6 ko)`, which is also circled in red. To the right of the attachment, the text **On vous incite à cliquer** is written in red. Below the attachments, the 'Object' field contains the text `Objet: Notification en attente : Le service d'assistance partage un fichier avec vous.`. The main body of the email contains the text `ATTENTION`, `Votre document est en attente.`, and `Veuillez le télécharger et vous connecter pour le libérer.`

Focus : La messagerie Electronique 2/5

[Zimbra](#)

Sign In

Username Password

Show

☐ Stay signed in

Vous avez cliquer et rempli le formulaire !!!!

Web App Version

Default

x

Modern

The Modern Web App delivers a responsive experience across all your devices and integrates with many popular apps.

Classic

The Classic Web App is familiar to long-time Zimbra users. It delivers advanced collaboration and calendar features popular with power users on Desktop web browsers.

Default

This will sign you in according to your saved Preference. In the Modern Web App, set this preference in Settings > General > Zimbra Version. In Classic, set it in Preferences > General > Sign In.

Copyright © 2005-2025 Synacor, Inc. All rights reserved. "Zimbra" is a registered trademark of Synacor, Inc.

Focus :La messagerie Electronique 3/5

FALSE/DIFFERENT = FISHING

only valid and safe method is to completed directly by you in your favorite browser

Connexion de client Web Zimbr X

https://lpc-mail.in2p3.fr/

https://zimbra.XXX.XX
https://mail-zimbra.TTTT.VV

IN2P3

Connexion

Utilisateur

Mot de passe

Afficher

Connexion

☐ Mémoriser mes valeurs d'accès

Version

Défaut

Copyright © 2005-2025 Synacor, Inc. All rights reserved. "Zimbra" is a registered trademark of Synacor, Inc.

Focus : La messagerie Electronique 4/5

Chevaleyre Jean-Claude [CC-IN2P3] - Your mail account password will expire in 21 days - -- Mail transféré -- De: "CC-IN2P3 User Support" <no-reply@cc.in2p3.fr> À: "Jean-C Réceptior 4 ko 7:10 14 Oct

De: "CC-IN2P3 User Support" <no-reply@cc.in2p3.fr>
À: "Jean-Claude Chevaleyre" <Jean-Claude.chevaleyre@clermont.in2p3.fr>
Envoyé: Lundi 5 Février 2024 04:16:09
Objet: [CC-IN2P3] - Your mail account password will expire in 21 days

- ✘ No clickable URL
- ✘ No join piece
- ✘ no text that hides a url
- ✘ and other schemes to extract login information

Bonjour Jean-Claude,

Le mot de passe de votre compte de messagerie va expirer dans 21 jours. Veuillez le changer rapidement via l'interface web (Webclient) ou vous ne serez plus capable de vous connecter.

> Interface Web (Webclient) => Preferences => General => Changer le mot de passe

N'oubliez pas de mettre à jour ce mot de passe partout où il est utilisé (lecteurs de mails, téléphone etc.).

Veuillez contacter votre support informatique local si vous souhaitez des compléments d'information sur la procédure à suivre et sur la politique de gestion des mots de passe.

Merci de votre compréhension.
L'équipe d'administration de la plateforme de messagerie de l'IN2P3.

Dear Jean-Claude,

Your mail account password will expire within 21 days. Please change your password quickly using the web interface (Webclient) or you will not be able to login anymore.

> Web Interface (Webclient) => Preferences => General => Change Password

Remember to update this new password everywhere it is used (mail reader, smartphone, etc.).

Focus : La messagerie Electronique 5/5

Si vous avez cliqué :

☒ **Cas 1** : Vous vous en apercevez rapidement

changer tous les mots de passe sur tous les sites qui utilisent le même mot de passe et venez nous voir

☒ **Cas 2** : Vous n'avez rien vu

On le saura si votre compte est utilisé a vos dépends → il sera bloqué automatiquement si un usage inapproprié est fait avec votre compte

N'AYEZ PAS HONTE
Cela arrive à tout le monde et surtout venez
nous voir le plus rapidement possible

Conclusion

