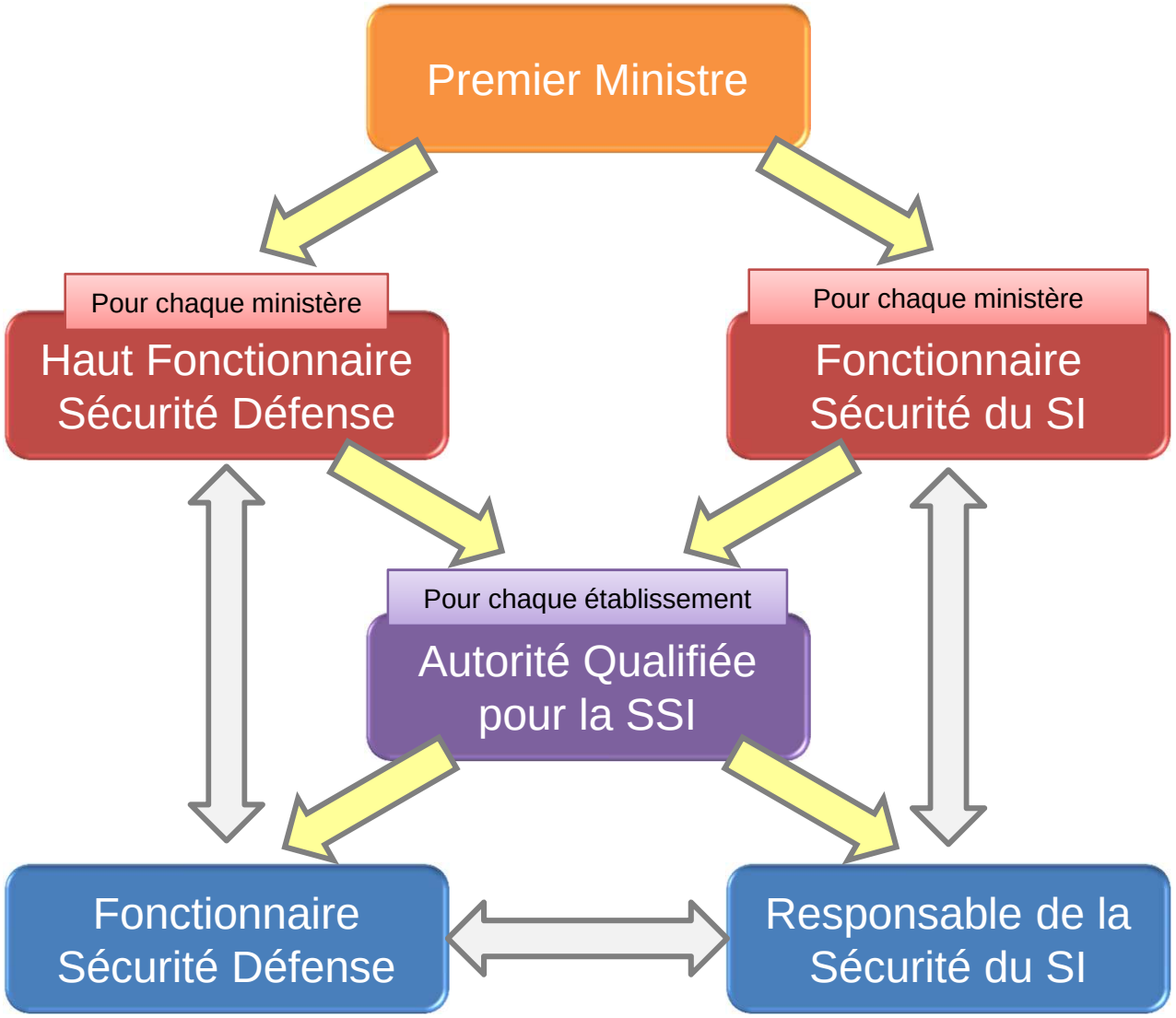
SSI : Sécurité des Systèmes d'Informations

SSI

Désignation d'un RSSI :
Une chaine fonctionnelle simple et directe



Rôles dans la SSI

Autorité Qualifiée pour la SSI (AQSSI) :

- Le chef d'établissement : **Arnaud POITOU**
- Définit la politique SSI ou PSSI pour son organisme
- Assure la responsabilité du niveau de sécurité requis
- Veille à la mise en œuvre des dispositions réglementaires
- Arbitre et contrôle la mise en place de la PSSI

Fonctionnaire Sécurité Défense (FSD) :

- Nommé par l'AQSSI pour l'établissement : **Jean-Yves HASCOET**
- Correspondant local du HFDS
- Protège le patrimoine scientifique et technique
- Assure la protection du secret
- Prépare et exécute les plans de Défense et de Sécurité

Responsable de la Sécurité du Système d'Informations (RSSI) :

- Désigné par l'AQSSI pour l'établissement : **Corentin L'HOSTIS**
- Seconde et conseille l'AQSSI dans la mise en place de la PSSI
- Connait et suit l'ensemble des activités SI du site
- Suit les moyens nécessaires à la mise en œuvre de la PSSI
- Suit l'état des menaces
- Interaction forte avec le FSD ainsi qu'avec le **CIL**

Contexte réglementaire et législatif

Protection des données personnelles

- Loi N° 78-17 du 6 janvier 1978
  dite « Informatique et Libertés »
- Modifiée en 2004 pour s'adapter à la
  directive européenne du 24 octobre 1995
- Règlement européen d'avril 2016 (RGPD)

Confiance numérique

- Référentiel Général de Sécurité (RGS)
  Arrêté du 13 juin 2014 pour les autorités administratives échangeant des informations avec des usagers ou entre autorités.
- Règlement européen iEDAS N° 910/2014

Sécurité des Systèmes d'Information

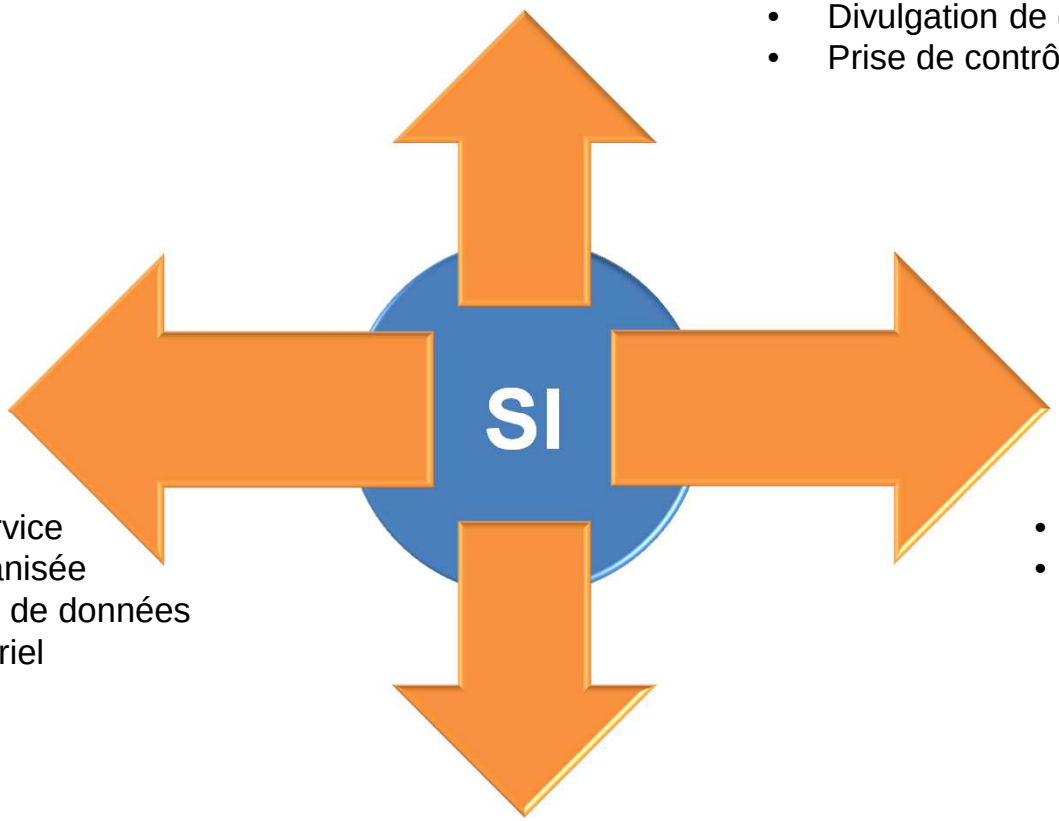
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la Nation
- PSSIE ou PSSI de l'Etat : circulaire du Premier Ministre N°5725/SG du 17 juillet 2014

République Numérique (oct 2016)

Menaces

Déstabilisation

- Défiguration
- Divulgation de données
- Prise de contrôle



Sabotage

- Déni de service
- Panne organisée
- Destruction de données ou de matériel

Cyber-Criminalité

- Hameçonnage
- Rançongiciels

Espionnage

- Hameçonnage ciblé / Ingéniérie sociale
- Vol ou exfiltration de données

Réponse aux menaces

Ce qui ne marche pas	Ce qu'il faut faire
Sécurité pour la sécurité	Sécurité pour répondre à un besoin (cadres réglementaires & législatifs)
Sécurité à 100 %	Niveau de sécurité cohérent avec les enjeux
Approche globale et absolue	Démarche progressive

Conclusion générale

Pour toute préoccupation relative à la Sécurité des Systèmes d'Informations

- Un contact unique : **Corentin L'HOSTIS**
- Une adresse fonctionnelle dédiée RSSI@ec-nantes.fr

Menaces sur la messagerie

Menaces sur la messagerie

Une attaque banale

Webmaster / ➡Cher Monsieur / Madame

Cher utilisateur votre boîte aux lettres de stockage Limit vous avez dépassé le 2.GB Lt est déterminé par l'administrateur ACTUELLEMENT 2.30GB, ne peut pas Envoyer ou recevoir de nouveaux messages jusqu'à ce que vous validez votre Email Again

Cliquez sur le lien ci-dessous pour terminer la boîte aux lettres Pour 2.30GB

http://server-fr.tripod.com

Merci
administrateur du système

Zimbra / salut utilisateur

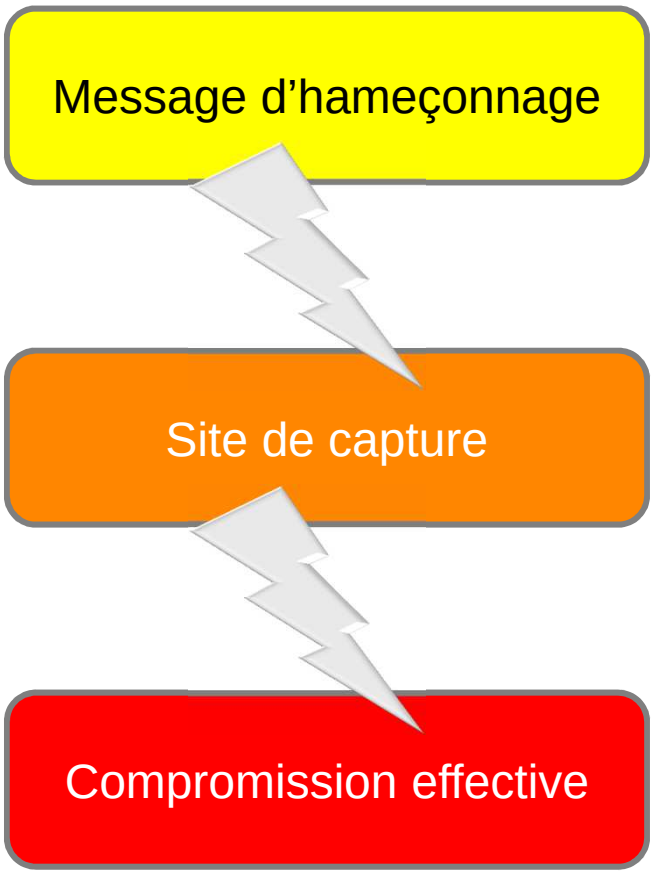
salut utilisateur

Votre compte Zimbra doit être vérifié pour éviter De-activation. Vous avez utilisé 5,98 Go de 6 Go qui a été alloué t par votre administrateur. Vous vous tenez un risque de votre compte étant fermé si non vérifié aujourd'hui.
Octobre 18-2016 00:28:50 -0500
Vous avez moins de 24 heures.
Pour vérifier compte,cliquez: http://frenchunivgrade-001-dept-nakjsak.tripod.com/

Pour la vérification s'il vous plaît visitez: http://frenchunivgrade-001-dept-nakjsak.tripod.com/

L'équipe de compte d'utilisateur

Un piège bien rodé



- Éléments d'autorité
- Urgence et vulnérabilité
- Lien pour action

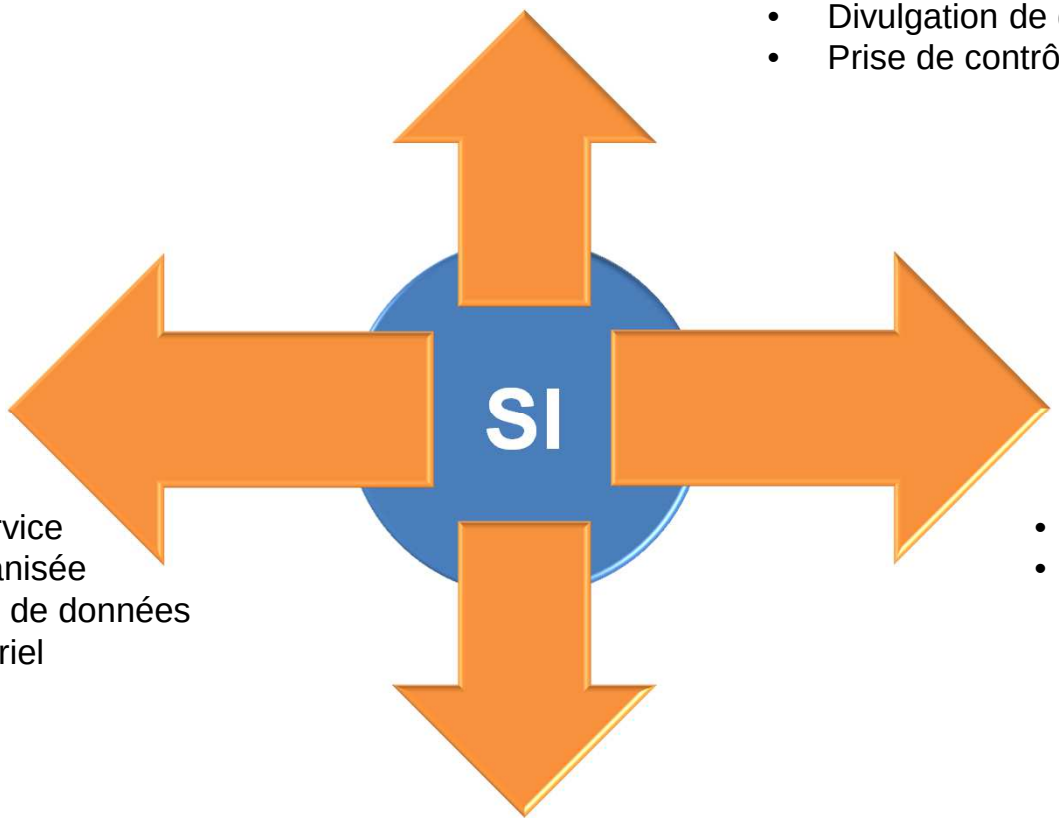
- Contrefaçon de site officiel
- Hébergement extérieur
- Redirection vers le site ECN

- Prise de contrôle
- Exploitation
- Elargissement

Eventail des menaces

Déstabilisation

- Défiguration
- Divulgation de données
- Prise de contrôle



Sabotage

- Déni de service
- Panne organisée
- Destruction de données ou de matériel

Cyber-Criminalité

- Hameçonnage
- Rançongiciels

Espionnage

- Hameçonnage ciblé / Ingéniérie sociale
- Vol ou exfiltration de données

Coûts et conséquences

- Fermeture du compte (mesure conservatoire)
  DSI / RSSI
- Déclaration d'incident
  RSSI
- « Nettoyage » voire déblacklistage
  DSI / Prestataire

2 heure/homme

- Réponses aux signalements
  DSI / RSSI

2 heures/homme

- Echanges avec la victime
  DSI / RSSI / FSD
- Résolution de l'incident et retour à la normale
  DSI / RSSI

2 heures/hommes

Menace facilement évitable

- Vigilance sur la messagerie
  - Expéditeur et signature
  - Cohérence du message
  - Liens
- Comportements à risques
  - Mot de passe faible ou dupliqué
  - Facilité à fournir ses identifiants
  - Ignorance des menaces
  - Méconnaissance des conséquences
- Isolement et silence
  - Pas de discussion avec les collègues ou responsables
  - Pas de demande de confirmation

Illustration

Gaspard TRÉLOIN, victime d'un hameçonnage
Compte fermé le 21/11/16

Réaction le 22/11/16 par un mail vers un service de l'ECN :

From: Gaspard.Treloin@eleves.ec-nantes.fr
To: Direction.SI@ec-nantes.fr
Subject: Problème de connexion serveur pédagogique

Bonjour madame/monsieur,

Je vous contacte car j'ai un problème de connexion sur le serveur pédagogique https://hippocampus.ec-nantes.fr/login/index.php

Même en rentrant mon identifiant correct et mon mot de passe la connexion "échoue" , que ce soit sur mon smartphone ou sur mon PC.

mon identifiant : gtreloin2016
mon mot de passe : Canard37170

J'ai cru comprendre que c'est votre service que je devais contacter afin de palier à ce soucis.
Excusez-moi d'avance si je me suis trompé.
Cordialement

Gaspard Tréloin EI1

Une montée en puissance

Amazon / Your invoice pending

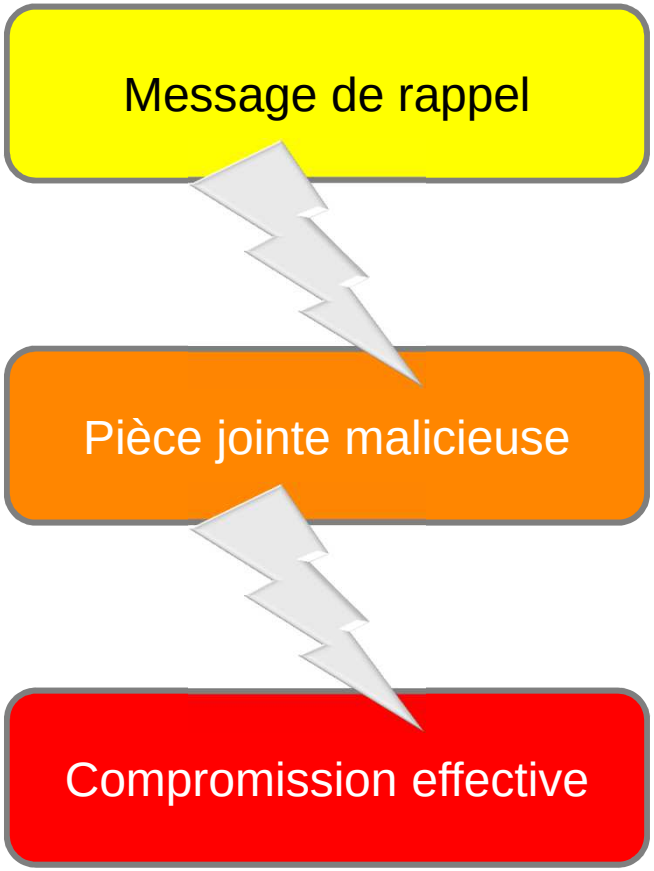
```
Good day,

Thank you for your order. We'll let you know once your item(s) have
dispatched.You can check the status of your order or make changes to it by
visiting Your Orders on Amazon.co.uk.
Order Details

Order #D:A-2584844-3936591
Placed on September 26, 2013

Order details and invoice in attached file.

Need to make changes to your order? Visit our Help page for more information and
video guides.

We hope to see you again soon.

Amazon.co.uk
```

Apple / Votre facture

eBay / Avoir sur votre dernier achat

…

Une mécanique implacable



- Acteurs du eCommerce
- Menace ou récompense
- Pièce jointe à vérifier

- ZIP, PDF, SCR, COM …
- Exécutable caché dans la PJ
- Amorce de compromission

- Prise de contrôle
- Cryptage / verrouillage
- Demande de rançon

Coûts et conséquences

- Perte totale des données
  Utilisateur
- Menaces sur les périphériques (disques amov. / réseau)
  Utilisateur / Communauté
- Tentatives de paiement
  Utilisateur

inestimable

- Déclaration d'incident et prise de preuves
  DSI / RSSI

1 jour / homme

- Echanges avec la victime
  DSI / RSSI / FSD
- Réinstallation du poste
  DSI / Informaticiens de proximité / Prestataire

4 heures/hommes

Prévention et Mitigation

Attaques sur des facteurs humains

→ Prévention par la prise de conscience

Attaques sur des conduites à risque

→ Cloisonnement pour limiter le risque

Silence et culpabilité des victimes

→ Dialogue et retours d'expériences

SVP-DSI@ec-nantes.fr + RSSI@ec-nantes.fr

Conclusion

Merci de votre accueil

Merci de votre attention

Des questions ???

SVP-DSI@ec-nantes.fr + RSSI@ec-nantes.fr