La Sécurité du Système d'Information de l'UHSP ?

Mais c'est très simple...(*)

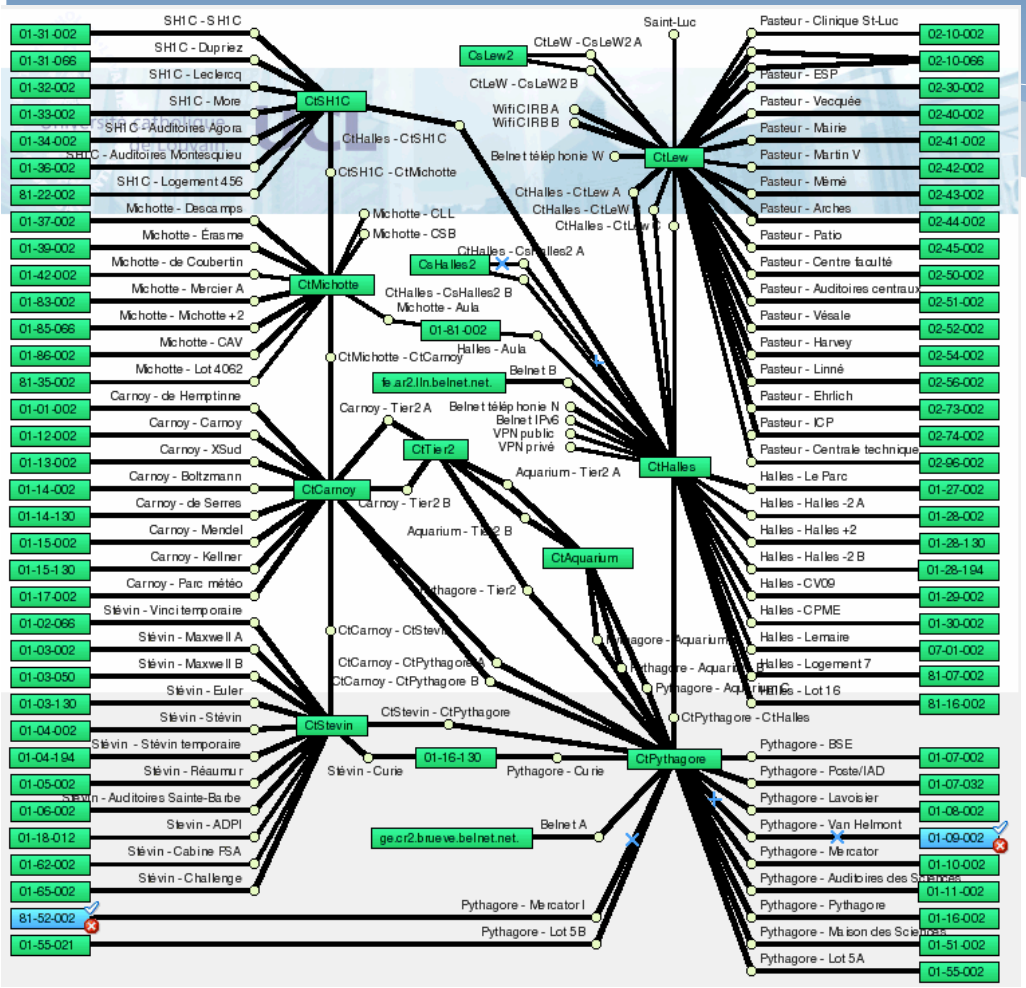
Kazansky – RSSI

Eugène Aisberg (1905 – 1980)

UHSP en chiffres

* 35.000+ étudiants – 120+ nationalités
* 9.000+ primo-arrivant/an
* 6.000+ enseignants, chercheurs, staff
* 6 sites : Houte-si-plou, Woluwé, Mons, Tournai, Charleroi, Saint-Gilles
* 50.000+ comptes actifs (LDAP / AD)
* 330.000+ personnes connues (FGS)

UHSP - Le réseau



- 100 bâtiments
- 25.000 prises réseaux
- 13.000 prises raccordées
- 8.000 postes de travail
- 500+ serveurs
- 7 routeurs (de quartier)
- 600+ commutateurs
- 900+ bornes WIFI

Sécurité Système d'Information

* Sécurité Informatique...
  * Qu'est-ce que cela évoque pour vous ?
  * Qu'est-ce que cela évoque pour votre entourage, vos amis, vos voisins ?
  * Quels mots-clefs ressortent le plus ?
  * Pourquoi faut-il se préoccuper de sécurité informatique ?

Actifs de l'UHSP

* Actif : ce qui a de la valeur
  * A prendre au sens des assurances…
  * Ce qu'il faut préserver, protéger
  * Exemples :
    * bâtiments, matériel, étudiants, cours, brevets, données d'expériences, cotes d'examen…
  * Menaces, dégradation d'actifs :
  * Exemples :
    * Incendies, vols, accidents, pannes, fraudes…

Actifs Numériques de l'UHSP

* Actifs numériques
  * spécifiques :
    * Les actifs propres du Système d'Information
      * Serveurs, logiciels, salles informatiques
    * Sous contrôle Service Informatique
  * a-spécifiques :
    * Les actifs de l'UHSP portés par le SI
      * Cotes d'examen dans une DB, brevet de recherche
      * PC portable d'un chercheur en voyage
    * Hors contrôle Service Informatique !

Actifs Numérique - Protection

* Deux aspects de protection des actifs (numériques)
  - Sécurité
    - En anglais : safety
    - Prévention/gestion d'incidents imprévus
    - Exemples :
      - Panne d'un serveur, fibre optique coupée lors d'un chantier, délestage, crash disque…
  - Sûreté
    - En anglais : security
    - Prévention/gestion d'incidents volontaires
    - Exemples :
      - Intrusion dans un serveur, manipulation de données, sabotage, envoi de spams…

Actifs Non Numérique - UHSP

Deux services avec un cadre légal de fonctionnement

- Sécurité
  - Service de sécurité et de radioprotection
  - A l'UHSP, service interne (SIPP)
  - Lois sur le bien être au travail, harcèlement, prévention incendie…
- Sureté
  - Service de gestion de la sûreté des personnes et du patrimoine immobilier
  - A l'UHSP, service externe (Gardiennage)
  - Loi sur la sécurité privée et particulière (loi Tobback)…

Actifs Numérique - UHSP

Pas de service SSI mais un RSSI (janvier 2012)

- Positionnement dans l'UHSP
  - Mandat de l'Administrateur Général
  - En staff du Directeur du Système d'Information
  - Fonction transversale dans l'université
- Couvre tous les aspects
  - Spécifiques et A-Spécifiques
  - Sécurité et sûreté (safety & security)
- Cadre légal pauvre (pour le fonctionnement)
  - Loi vie privée 1992, Loi cybercriminalité 2000
  - Loi communications électronique 2005
  - CCT 81 sur la cybersurveillance
  - **NEW !! RGPD (mai 2018)**

Actifs Numérique - RGPD

Effets du RGPD

- …
- …

Actifs Numérique - UHSP

Fonctionnement à créer depuis ~ 0.

- Articulation autour de trois fonctions
  - Conseiller (missions de prévention)
  - Coordinateur (gestion d'incidents p.ex.)
  - Gestionnaire d'identité (données de signalétique)
- Respect des 7 attributs de sécurité
  - Disponibilité
  - Intégrité
  - Fiabilité
  - Confidentialité
  - Authenticité
  - Traçabilité
  - Irrévocabilité

Trois fonctions de sécurité

Exemples d'actions comme…

- Conseiller
  - Mise en place de politiques de sécurité
  - Intégration dans des projets
  - Sensibilisation – diffusion de bonnes pratiques
- Coordinateur
  - Gestion de plaintes internes ou externes
  - Monitoring pro-actif
  - Audit de sécurité
- Gestionnaire d'Identité
  - Monitoring qualité des données
  - Correction des données de signalétique
  - Gestion des exceptions

Conseiller

Exemples d'interventions dans des processus :

- Déploiement d'imprimantes et photocopieurs en réseau
- Externalisation du processus de recrutement HR
- Enquête sur le comportement alcool, drogue, tabac des adolescents européens en relation avec leurs contacts sur les réseaux sociaux
- Enquête alcool (consommation vs parcours étudiant)
- Projet de recherche d'étude de "noms de fichiers" dont le contenu serait illégal
- Installation d'un nœud de sortie du réseau Tor
- Election du recteur par voie électronique

Coordinateur

Exemples d'interventions dans des incidents :

- Serveur informatiques hacké participant à des attaques
  - De "distributed denial of service" externes
  - D'exfiltration de données externes
- Hacking d'hébergement Web
  - Déni de services
  - Phishing au détriment de banques
- Vol de matériel
  - Quid des données ? Vols ciblés ?
- "Vol" de mots de passe
  - Pour des campagnes de spamming
  - Pour du blanchiment de connexions internet
- Incidents légaux
  - Non respect de la loi propriété intellectuelle
  - Non respect de la loi vie privée

Gestionnaire d'identité

Exemples d'interventions en matière de gestion de :

- Données de signalétique dans le FGS
  - Monitoring de changement
  - Validation des demande de changement
  - Gestion des doublons
  - Coordination des corrections entre services UCL
- Demande d'exception pour continuer à utiliser les services du système d'information
  - Jointure de contrats
  - Fin de thèse tardive
  - Année sabbatique
- La grille IDM des droits d'accès aux informations et services

Monitoring / Contrôle

Outils de monitoring et de contrôle:

- Réseaux
  - Netflow (En RT pour mail, vpn)
  - Observium, Netdisco
  - IDS : Suricata (WIFI étudiant)
  - Firewalls : IDS/IPS/NG FW (Mode actif/blocage possible)
  - OpenDNS (Mode actif/blocage possible)
  - Tapping
- Journaux de bord (Octopussy)
  - SMTP
  - DHCP
  - RADIUS
  - Portail et serveurs Web
  - iCampus, Moodle
- Scanner de vulnérabilité
  - Nessus

About UHSP

* Le 15 décembre 1965, les étudiants et les professeurs de la section francophone de l'Université catholique de Louvain, deux ans avant le « Walen buiten » de la frange catholique flamande, cherchent un terrain pour implanter la nouvelle Université. Ils décident symboliquement d'installer le nouveau campus francophone à Houte-Si-Plou, hameau situé à proximité d'Esneux, sur le territoire de la commune liégeoise de Neupré. [...] (From Wikipedia)
* Université de Houte-Si-Plou, espace de réflexion démocratique
* L'expression « Houte Si Plou » est bien connue des Liégeois et même des habitants de Wallonie. Elle sert de réponse évasive et moqueuse à toutes sortes de questions indiscrètes. Pour beaucoup de personnes, il s'agit d'un endroit « reculé », au sens propre et au sens figuré, peuplé d'habitants incultes et illettrés.C'est un lieu-dit situé à la limite de Neupré et d'Esneux en province de Liège [...] (From houtesiplou.be)