Cybersécurité à l'hôpital

Dr B. Debande
Directeur général administratif et financier

Le CHIREC en chiffres

- 3 sites hospitaliers (1050 lits)
- 2 sites hospitalisation de jour
- 4 polycliniques

- 3.591 salariés (3.163 ETP) – turnover annuel ~10%
- ~1000 médecins indépendants – turnover annuel ~5%
- 1800 étudiants/stagiaires/… - turnover annuel 100%

L'IT à l'hôpital

- Un savant assemblage de 200-250 applications
  - Quasi toutes synchronisées en temps réel (un véritable écosystème)
  - 24h/24 – 7j/7
  - Sur une infrastructure locale mais de plus en plus hébergées chez les fournisseurs dans le cloud

- Critique pour le fonctionnement
  - Support à la prise en charge patient au quotidien et sur le long terme
  - Optimisation/Efficience

Un écosystème applicatif très complexe et potentiellement instable indispensable au fonctionnement de l'hôpital

La citadelle de Bonifacio, au sud de la Corse, est située à près de 60 mètres au-dessus de la mer. Tout au long de son histoire, la violence des attaques ennemies avait poussé les ingénieurs à réinventer en permanence le système de défense. Les travaux titanesques que cela avait nécessité ont duré 6 siècles, transformant ainsi la ville en un véritable mille-feuille de fortifications

Moyens mis en œuvre - technique

- Mesures classiques de sécurité périmétrique (firewall, MFA,segmentation …)
  - SOC – la coûteuse sonnette d'alarme, qui sonne très/trop souvent
  - Analyse temps réel de la messagerie
- Mises à jour régulières des trop nombreux « trous » de sécurité
  - Mise en place récente d'un CERT santé au niveau fédéral
  - Comment mettre à jour des systèmes qui tournent 24/7
  - Comment anticiper l'impact de ces mises à jour sur les 250 applications
  - A faire en période de moindre d'activité (00h00 → 05h00…)
- Se préparer au pire
  - Backups sur un réseau séparé
  - Procédures pour un redémarrage rapide sur des systèmes sains, complexité de la réinitialisation du parc de PC (3500 postes = environ 8 jours de 24h…)

Moyens mis en œuvre - technique

- Tout cela peut/doit être fait, en plus des activités classiques d'une équipe infrastructure dont la taille ne peut pas évoluer (financement insuffisant) à moins d'amputer d'autres activités

- Tous ces outils ne sont rien sans les compétences humaines pour les mettre en œuvre et surtout assurer une surveillance constante
  - Comment attirer et conserver les expertises dans ce domaine à l'heure où toutes les entreprises recherchent ces profils ?
  - Comment assurer une permanence 24/7 avec des équipes sous-dimensionnées
  - Risque majeur = risque humain vu la petite taille des équipes


gettyimages
Credit: zaricm

Moyens mis en œuvre - humain

- Le maillon faible se situe entre la chaise et le clavier
  - Les mesures de sécurité assurent la fermeture des portes et un contrôle strict à l'entrée
  - Mais quasi tous les collaborateurs peuvent/doivent pouvoir ouvrir les fenêtres… qui deviennent un point d'entrée de choix
- Les techniques et la qualité des phishing évoluent constamment
  - Population ciblée (organigrammes)
  - Messages de plus en plus crédibles (merci l'IA)
  - Techniques de vente !
  - Plus seulement le mail…

Moyens mis en œuvre - humain

- Se préparer au pire = **comment assurer la sécurité des patients en cas de cyberattaque** (et pas comment continuer à fonctionner comme avant)

- Extension du plan de continuité en cas de panne, mais durée d'interruption probablement plus longue

- L'hôpital est un écosystème fragile
  - Travail de longue haleine : interviewer, challenger, tous les services médicaux, mais aussi de support, …
  - 1 an à raison d'une journée par semaine
  - Et quand tout est bouclé, il faut recommencer car l'écosystème a évolué
  - Intérêt = prise de conscience (parfois difficile) du risque et de l'impact sur son activité mais aussi sur celle des autres

Moyens mis en œuvre - humain

- Former/informer les collaborateurs aux techniques de la cybercriminalité
  - 3591 salariés (3163 ETP) – turnover annuel ~10%
  - Environ 1000 médecins indépendants – turnover annuel ~5%
  - 1800 étudiants/stagiaires/…
  - → plus de 2000 nouvelles personnes par an !
- Divers moyens média
  - Écrans d'information pour le personnel
  - Alertes sur tous les écrans lors de l'identification d'un phishing massif
  - Formations dans les services
  - Campagnes de faux phishing

Cela porte ses fruits au niveau conscientisation collective mais le fort turnover du personnel, en particulier des étudiants, n'aide pas

Tout ceci ne supprime pas le risque, mais le diminue

Espoirs, rêves, (dés)illusions…

- Mieux réguler le secteur des applications informatiques de santé
  - Accepteriez-vous de voler dans un avion piloté par 250 applications plus ou moins sécurisées, que le pilote tente de faire fonctionner ensemble et pendant tout le vol ?

- Interdire le paiement des rançons
  - Ne règle pas tout car les données ont une valeur intrinsèque

- Mutualiser les ressources et les efforts
  - Rôle des réseaux hospitaliers ? Oui mais…
    - Une seule IT (convergence humaine)
    - Outils identiques (convergence logicielle - 250 applications)
    - Configuration identique des logiciels

    → Une seule gouvernance…