Personnel et cybersécurité, politique interne et sensibilisation

Webinaire – 10/12/2021

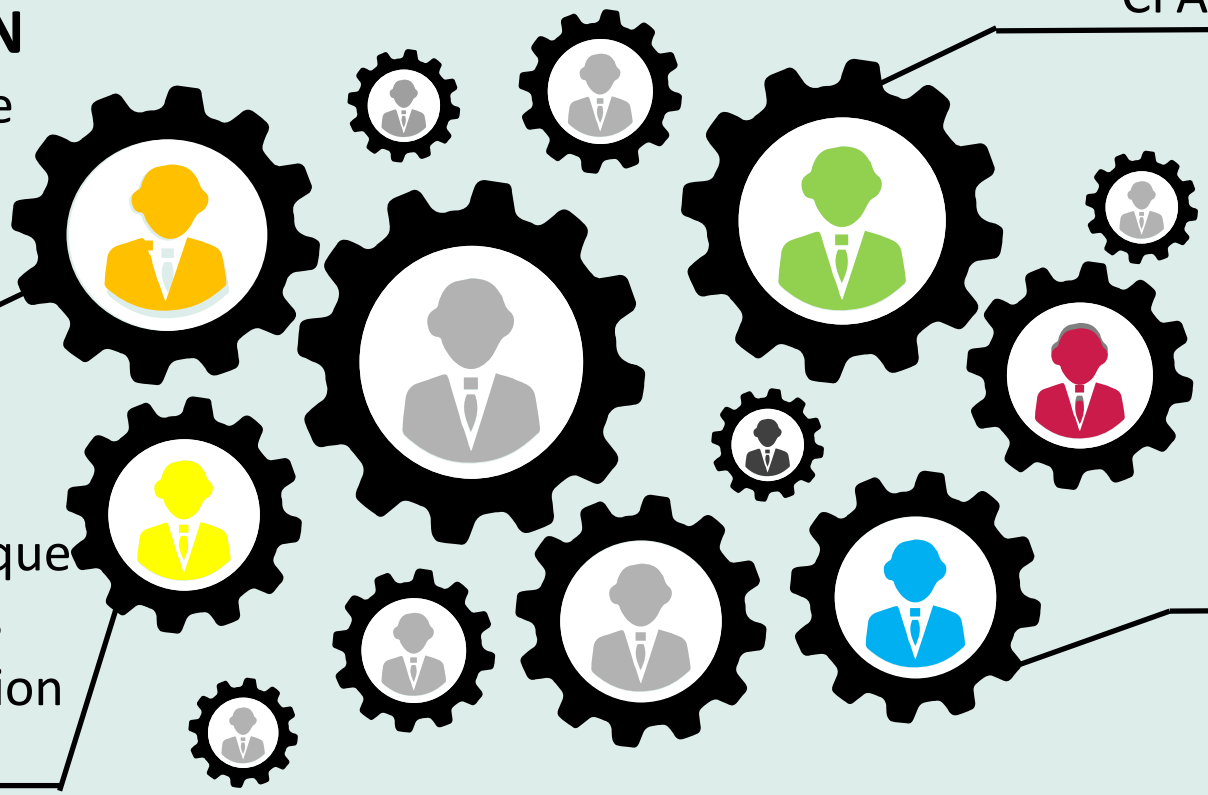
Union des Villes et Communes de Wallonie asbl

Wallonie

Nos invités

Caroline JEDWAB
Contrôle Interne et DPD
CPAS de Namur

Frederic GELISSEN
Security Governance Leader
Associé Procsima-group



Fabrice LECLERCQ
Gestion informatique
Ville de Seraing
Membre du RIC

Benoit JOSEPH
1er Directeur Spécifique
Département des systèmes d'information
Ville de Liège

Menu de la séance

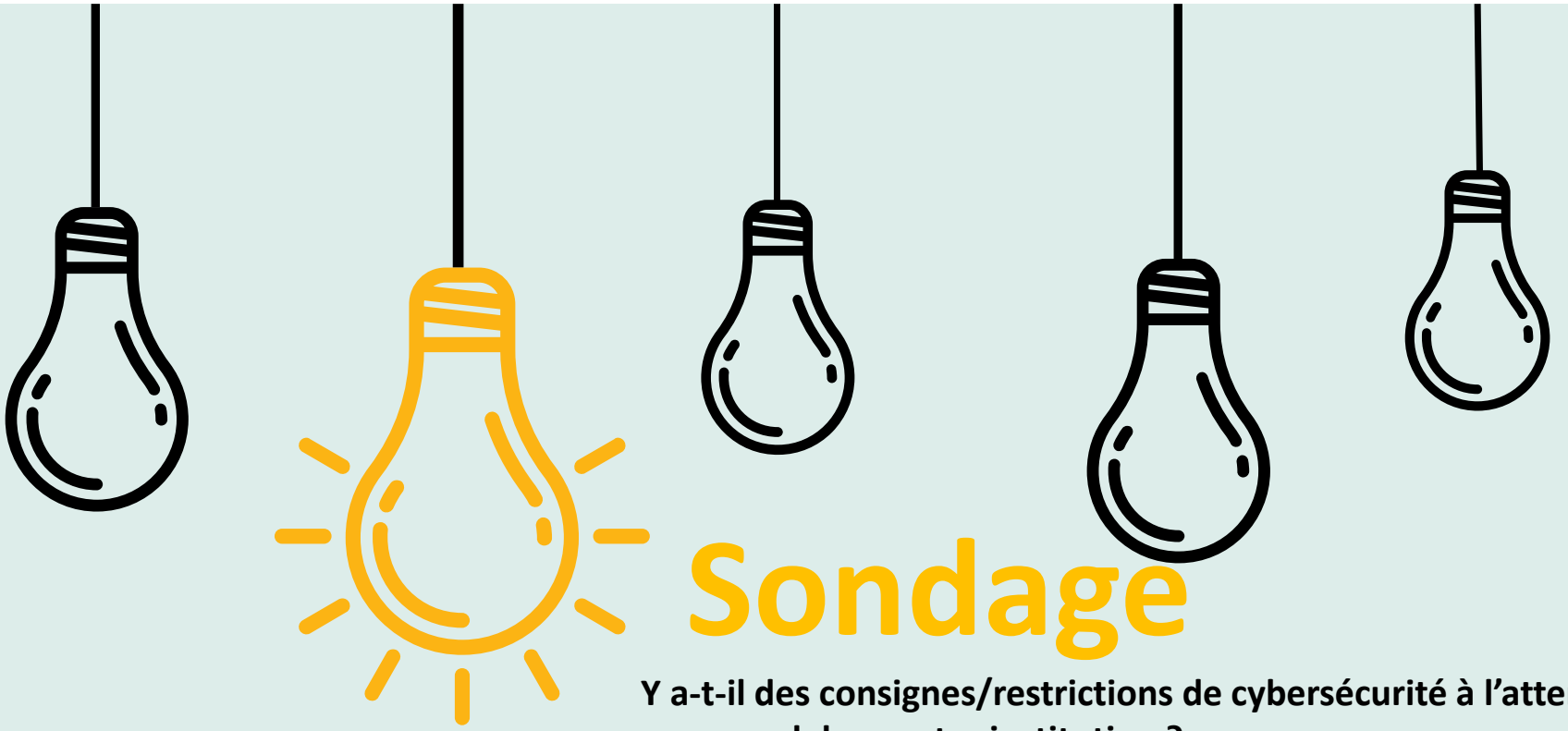
01 Quelle politique interne mettre en place à l'attention du personnel

02 Politique de cybersécurité à l'attention du personnel : respect et sensibilisation

03 Partage d'expériences, du côté du CPAS de Namur

04 Partage d'expérience : le retour de Seraing sur la cyberattaque

05 Partage d'expérience : le retour de Liège sur la cyberattaque



Sondage

Y a-t-il des consignes/restrictions de cybersécurité à l'attention du personnel dans votre institution ?

Vous sentez-vous suffisamment armé.e et outillé.e pour édicter des règles internes de cybersécurité ?

Êtes-vous davantage inquiet.ète par le risque de cyberattaques depuis que le télétravail est plus fréquent ?

01 02 03 04

Quelle politique interne mettre en place à l'attention du personnel

Frederic Gelissen

Security Governance Leader

Associé Procsima-group

Agenda

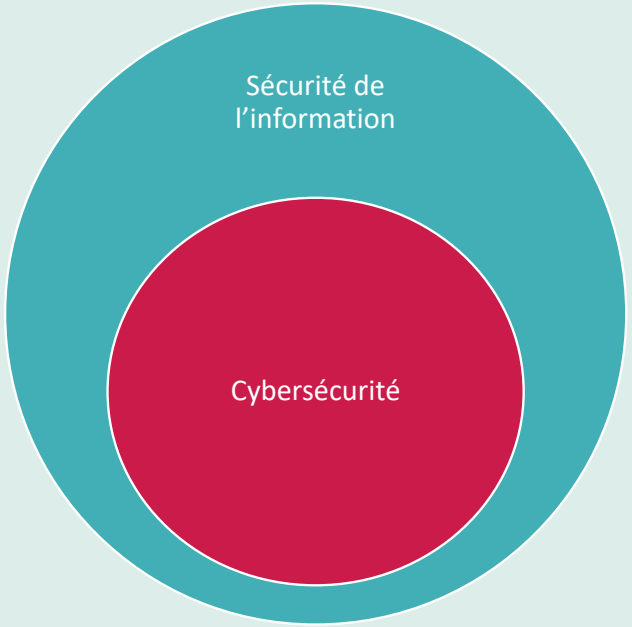
✓ Cyber sécurité et sécurité de l'information
✓ Quelles sont les menaces ?
✓ Sujet de la politique interne et de sensibilisation
✓ Mettre en place les politiques de sécurité
✓ Télétravail - est-ce plus risqué ? …
✓ Contrôles (restrictions) - avantages et limites

Cybersécurité et sécurité de l'information

CYBER = Internet

Cybersécurité = sécurité contre les diverses menaces d'internet

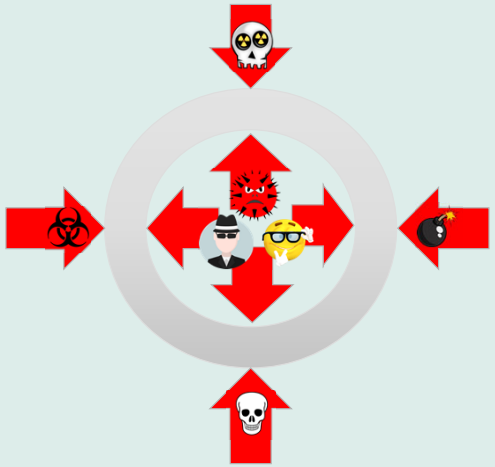
Sécurité de l'information = Sécurité contre TOUTES les menaces



Menaces

De nombreux dangers à l'extérieur et à l'intérieur de l'entreprise

- Des personnes malveillantes (hackers, espionnage, terrorisme, mafia)
- Des employés négligents ou fâchés
- Des systèmes mal conçus, mal gérés ou défaillants
- Des procédures et des flux mal pensés ou non suivis



Sujets de la politique interne et de sensibilisation

~30 sujets

- Mots de passe
- Email
- Logiciels malveillants
- Phishing
- Usurpation d'identité
- Ingénierie sociale
- Réseaux sociaux
- Confidentialité sur le Web
- Protection de votre ordinateur à la maison
- Télétravail
- Smartphones
- Appareils mobiles
- Voyager en toute sécurité
- Cloud Computing
- Principe du « bureau propre »
- Sécurité physique
- Contrôle de l'accès
- BYOD (Bring Your Own Device)
- Protection des renseignements personnels

Sujets de la politique interne et de sensibilisation

- Le bon usage d'Internet au travail
- Classification de l'information
- Cycle de vie de l'information
- Propriété intellectuelle
- Protéger les données des cartes de paiement
- Ransomware
- Fuites des données
- Rapports d'incidents
- Email professionnel compromis (BEC)
- Menace interne involontaire

Mettre en place une politique

Qualités d'une bonne politique

- Simple à comprendre pour son audience
- Non technique
- Concise
- Aisément transformable en actions concrètes
- Accessible (publication)

Mettre en place une politique

Collecte d'info
Atelier

Responsabilisation

Accessible par tous

Communication

En continu
Tests
Plateforme de sensibilisation

Parties prenantes
Actions
Suivi

Le télétravail - Risqué ?

NON ! Si on respecte quelques principes simples :

- Utiliser le matériel et les services de l'entreprise
- Ne pas prêter ses PC, smartphone, tablette professionnels à la famille
- Toujours utiliser une connexion sécurisée (VPN, Bureau virtuel d'entreprise)

Pour le service IT :

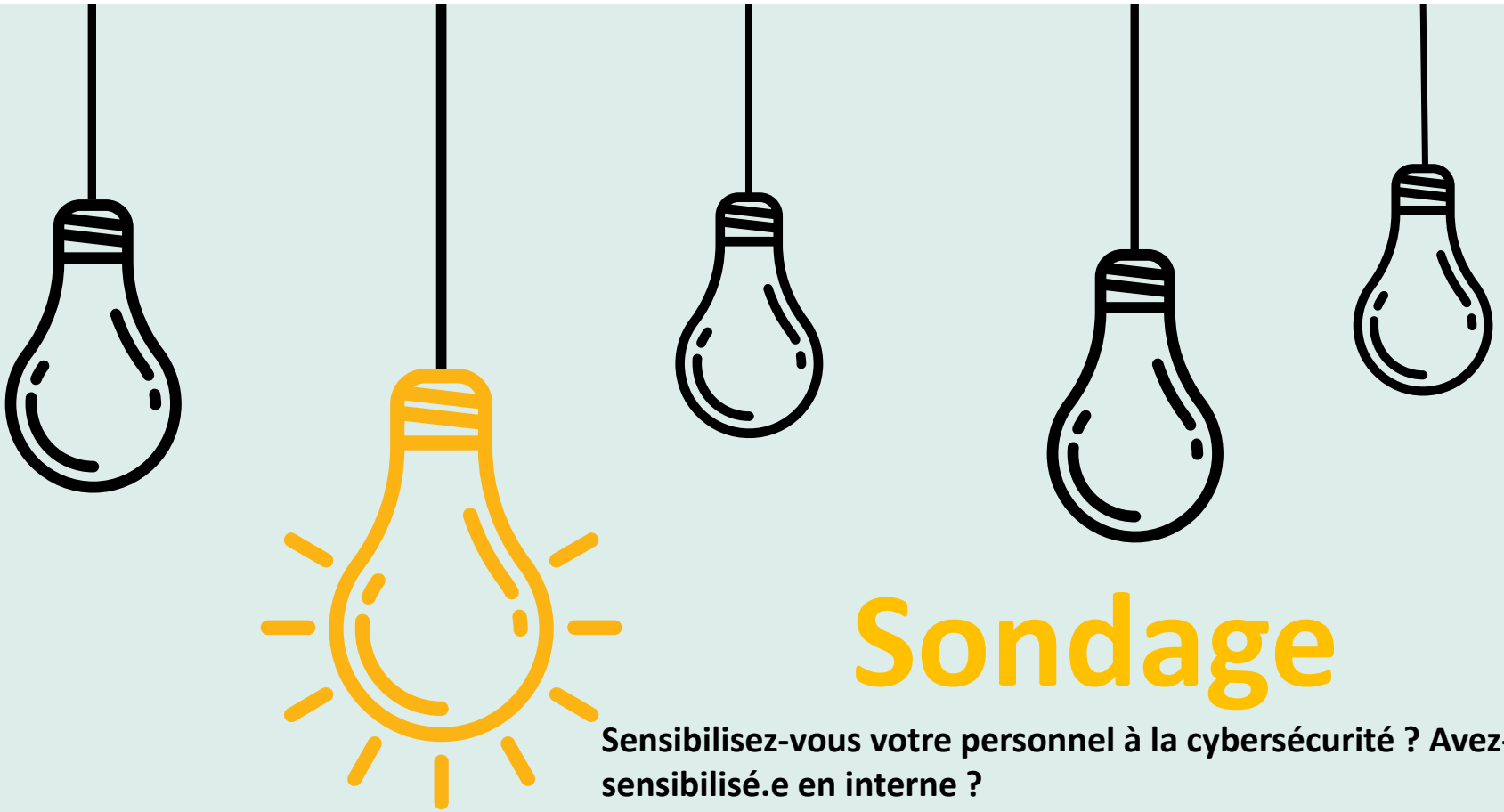
- Mettre en place une authentification à 2 facteurs
- Sécuriser O365
- Distribuer du matériel ou un PC virtuel sécurisé au personnel en télétravail

Mesures techniques pour limiter le risque

Les mesures techniques et la configuration des outils IT permettent de limiter les risques mais ne sont pas une solution infaillible, surtout si on y pense trop tard.

Sécurité dès la conception ➔ inclure la sécurité dès le design du service IT mais aussi du processus métier

Sécurité par défaut ➔ dans le doute, la sécurité maximum est activée !



Sondage

Sensibilisez-vous votre personnel à la cybersécurité ? Avez-vous été sensibilisé.e en interne ?

Estimez-vous que vos collègues sont suffisamment conscientisés à la cybersécurité ?

01 02 03 04

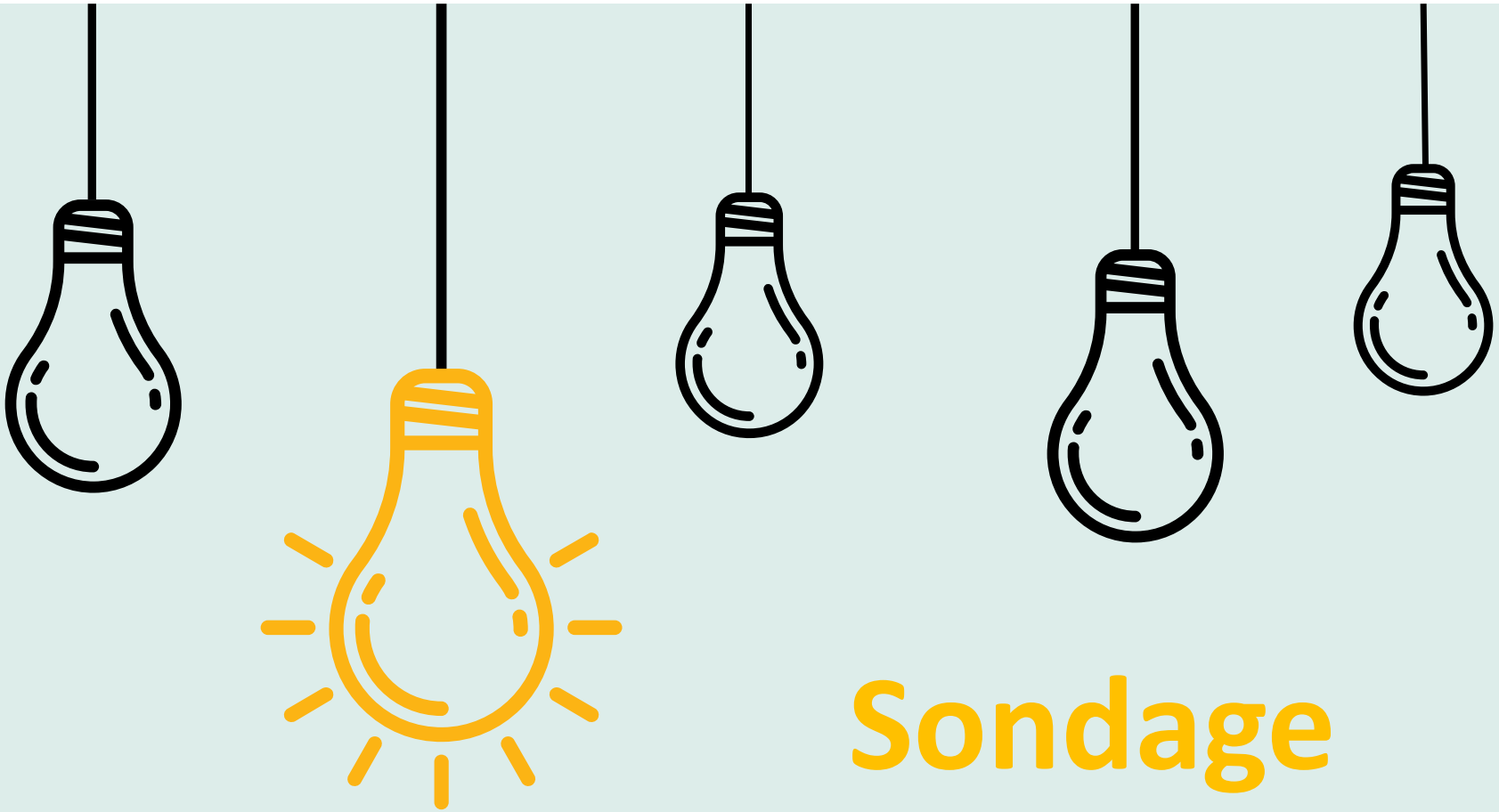
Politique de cybersécurité à l'attention du personnel : respect et sensibilisation

Frederic Gelissen

Security Governance Leader

Associé Procsima-group

- ✓ Confiance et entraide (sécurité construite par tous le monde)
  - ✓ Comment créer ce climat de confiance? (personne n'est à l'abri donc dédramatisons, l'union fait a force, des relais dans les départements, réagir vite voire anticiper…)
- ✓ Sensibilisation et formation (outil canaux, fréquence/processus)
- ✓ Autres mesures de prévention des risques (assessments périodiques, tests, assurances,..)



Sondage

Y a-t-il une personne en charge de la cybersécurité au sein de votre institution ?

01 02 03 04

Partage d'expériences,
du côté du CPAS de Namur

Caroline Jedwab

Contrôle Interne et DPD

CPAS de Namur

Mon rôle en termes de cybersécurité

Septembre 2018 : Déléguée à la protection des données (DPO/DPD)

Octobre 2018 : **Conseillère en sécurité de l'information (CSI)**

Travail sur 4 niveaux

- ✓ Élaboration des procédures
- ✓ Respect des procédures
- ✓ Sensibilisation
- ✓ Avis (nouveaux outils, nouveaux traitements)

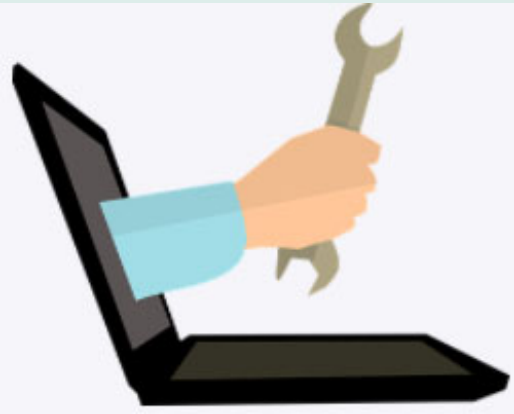
En partenariat constant (journalier!) avec le département IT

Les consignes de cybersécurité à l'attention du personnel

1. Document de référence : **La charte des utilisateurs des systèmes d'information**

- Travail coordonné par la DPD en collaboration avec le DG, le Dir. IT, le Resp. tech. IT, le DRH, le DF et le Dir. Tech.
- Validé par le Codir et les instances (BP, syndicats, Conseil) et annexe du RT
- Sujets en lien avec la cybersécurité :
  - ✓ la politique du mot de passe
  - ✓ la localisation des données professionnelles
  - ✓ les pratiques non autorisées
  - ✓ la protection du matériel de téléphonie mobile
  - ✓ les recommandations en matière de télétravail
  - ✓ la procédure de contrôle des systèmes d'information et d'examen de l'utilisation faite par les utilisateurs et les sanctions associées

2. **Choix d'outils** discutés et validés en Codir sur proposition du dépt IT/DPD



- ✓ PC de télétravail avec virtualisation de postes
- ✓ Clés USB sécurisées
- ✓ Notification de spam mis en quarantaine
- ✓ Filtrage des sites internet consultables (Youtube, mailbox perso., …)

Les respect des consignes

L'approche

- ✓ Information
  - lors de la révision de la Charte
  - lors des séances d'accueil
  - mails « Focus » sur des points sensibles ou ayant posé problème

JC

ven. 30/04/2021 15:32

JEDWAB Caroline

Focus - Que faire si vous abîmez ou perdez du matériel du CPAS?

À ⊞ CPAS

Que faire en cas de détérioration, de vol ou de perte de matériel du CPAS ?

Le téléphone d'entreprise et le matériel informatique (matériel et logiciel) sont des outils de travail qui appartiennent au CPAS et qui sont mis à la disposition des utilisateurs.

Tout équipement mis à disposition doit être géré en bon père de famille.

Mais certaines choses arrivent néanmoins…

Vous laissez tomber le smartphone de service qui se brise en mille morceaux
Vous ne trouvez plus votre badge d'accès
Vous laissez le pc de télétravail dans le coffre de votre voiture et on le vole
Les clés du bureau et le smartphone de service étaient dans le sac que l'on vient de vous arracher dans la rue
…

Que faire ???

En cas de vol ou de perte de matériel, l'utilisateur doit prévenir son supérieur hiérarchique et contacter **dans les meilleurs délais** (certaines actions en lien avec la sécurité informatique et des données doivent être prises au plus vite afin de limiter les risques réels ou potentiels):

Les respect des consignes

- ✓ Engagement formel : signature
  - de la Charte par les nouveaux
  - du Code de déontologie par les agents disposant de privilèges avancés sur les systèmes
- ✓ Rappel constant
  - Charte à valider lors de chaque passage sur internet

CPAS Namur

Utilisateur : **jedwab**

Vous accédez à Internet par le réseau du CPAS de Namur. Ceci est un outil **professionnel**.

L'usage d'internet est monitoré (surveillance et filtrage). Conformément à la charte des utilisateurs des systèmes d'information du CPAS, un rapport général d'activités est susceptible d'être transmis à l'autorité.

Toute tentative de contournement de la sécurité mise en place peut mettre en péril l'intégrité de toute l'infrastructure informatique.

Pour utiliser la connexion internet du CPAS vous devez accepter la charte des utilisateurs des systèmes d'information du CPAS.

Pour consulter la charte des utilisateurs des systèmes d'information du CPAS.

J'accepte la charte des utilisateurs des systèmes d'information du CPAS.

Les respect des consignes

Les difficultés

- ✓ Les mails de sensibilisation sont très peu lus
- ✓ Manque de temps et de compétence en communication (affiches, plaquettes, jeux,...)
- ✓ Difficultés à conscientiser sur la gravité potentielle de l'enjeu

Une cyberattaque au CPAS de Namur…

- ✓ Plusieurs centaines de tentatives journalières…
- ✓ Un cryptovirus en 2016
- ✓ Personnes de contact
- ✓ Se préparer au mieux…

Plan de continuité du système informatique

- Anticiper ce qui peut l'être
  - ✓ Améliorer notre système de défense
  - ✓ Préparer la gestion de crise

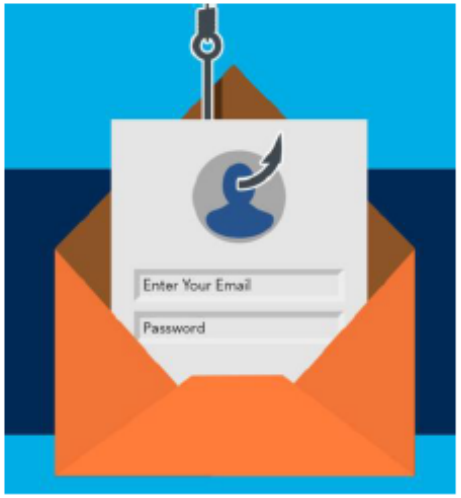
Sensibilisation du personnel

Deux niveaux de sensibilisation

- ✓ Sensibilisation personnel/Conseillers
- ✓ Codir et département IT

Sujets

- ✓ Outils et procédures
- ✓ En lien avec l'actualité
  - Risque accru: télétravail, Covid, Black Friday, …
  - « Opportunité » d'attention : Saint-Luc Bouge



Covid-19 et période de confinement :

Attention aux risques de hameçonnage !

Le hameçonnage (ou « phishing ») est une forme de cybercriminalité dans laquelle la victime (potentielle) est approchée par e-mail, sms, messagerie instantanée, médias sociaux ou téléphone. L'escroc se fait passer pour quelqu'un d'autre. Il peut s'agir d'une banque, d'un fournisseur d'énergie ou d'une société de technologie, mais aussi d'un ami ou d'un membre de la famille.

Le but est de "pêcher" ("phishing" en anglais) des données sensibles, comme des informations personnelles, des mots de passe, des données de carte bancaire ou de crédit. Une fois qu'il s'est emparé de ces données, l'escroc a les coudées franches : il peut par exemple accéder aux principaux comptes de la victime et ainsi dérober son argent ou usurper son identité.

La firme de sécurité Kaspersky a constaté aux environs de la période du Black Friday une forte hausse des attaques d'hameçonnage (phishing), par lesquelles des pages de paiement en ligne sont contrefaites. Le nombre d'incidents a augmenté de 208 pour cent et a donc plus que doublé.

Cyberattaque : soyons tous vigilants !

La Clinique Saint-Luc de Bouge subit une cyberattaque visible depuis ce dimanche. Cela a une influence majeure sur son activité : ce lundi, plus de 1000 consultations, examens et rendez-vous médicaux en hôpital de jour sont annulés et ce n'est probablement qu'un début.

Cyberattaque à la Clinique Saint-Luc de Bouge : un millier de consultations annulées ce lundi

Source : www.rtbf.be – article du 10/10/2021

Les attaques de ce type sont le fait de pirates qui font entrer dans le système informatique de l'entreprise un virus qui bloque purement et simplement l'accès au système informatique ou qui crypte les fichiers et les rend illisibles. Les pirates demandent une somme d'agent à l'entreprise pour délivrer les données. Indépendamment de savoir si on paie ou non la rançon, cela peut avoir des conséquences catastrophiques en matière de poursuite de l'activité pouvant aller jusqu'à des jours d'inaccessibilité des outils informatiques et des données.

Le CPAS n'est pas à l'abri !

Ces attaques sont actuellement très fréquentes, elles ont lieu partout et aussi à côté de chez nous, dans des structures a priori bien organisées et bien protégées : La Clinique Saint-Luc de Bouge, la Ville de Liège, ...

JC

ven. 30/04/2021 15:42

JEDWAB Caroline

À voir !! Webinaire – comment réagir en cas de cyberattaque?

À ⊞ codir; ⊞ tech; ⊞ Développement

Vous avez transféré ce message le 30/09/2021 17:14.

Bonjour à tous,

Le sujet des cyberattaques ne nous occupe pas directement pour l'instant (heureusement !!! 😉) mais le webinaire d'ING relayé par Santhéa est vraiment très concret et accessible à chacun.
En tant que membre du Codir et du département informatique, vous êtes directement concernés par le sujet.

Le témoignage du DG et du Directeur Informatique du CHwapi (hôpital de Tournai) est vraiment pratico-pratique et pertinent.
Le DG du CHwapi conclut le webinaire et son expérience de cyberattaque par ces mots : « *Il faut oser la rigueur de la sécurité* ». Tout un programme (que nous avons déjà bien entamé !), nous en reparlerons…

Quand vous avez un moment, je vous invite vivement à regarder ce webinaire de 50 minutes aussi passionnant qu'un bon polar (ou presque…) !
Le lien : Health Care - FR - NEP Webinars (nepgroup-webinars.com) (fonctionne avec Google Chrome et Firefox) ou via l'intranet/CPAS Tube (dans les outils communs CPAS Tube)/ « Webinaire cyberattaque CHwapi »

Belle journée,
Caroline

Sensibilisation du personnel

Test de phishing en novembre 2021

- ✓ Elaboré en interne
- ✓ A destination de tous les utilisateurs disposant d'un accès
- ✓ Test de la transmission de l'identifiant et du mot de passe pour bénéficier d'une offre alléchante et urgente
- ✓ Clôture du test par un mail de debriefing expliquant les éléments qui auraient dû attirer l'attention des destinataires

On n’a pas anticipé

- ✓ L’émoi suscité par ce test (beaucoup de réactions « - » et quelques « + »)
  - Frustration de s’être « fait avoir »
  - Notion de « faute » fort présente (et non d’apprentissage)
  - Espoir suscité par l’appât financier
- ✓ La difficulté du test

On a constaté

- ✓ Réactions fort différentes en fonction
  - Des agents qui ont encodé leurs données ou pas
  - De la culture professionnelle des agents
- ✓ Les résultats ne sont pas bons: la sensibilisation déjà réalisée n’a pas porté les fruits espérés
- ✓ Personne n’est à l’abri, même les agents sensibilisés

Avec un peu de recul

- ✓ Difficulté des tests à davantage faire monter en puissance
- ✓ Importance du groupe de travail
  - pour préparer: aspects sécurité mais pas que…
  - pour assumer: les réactions au(x) test(s)

Bilan global du test

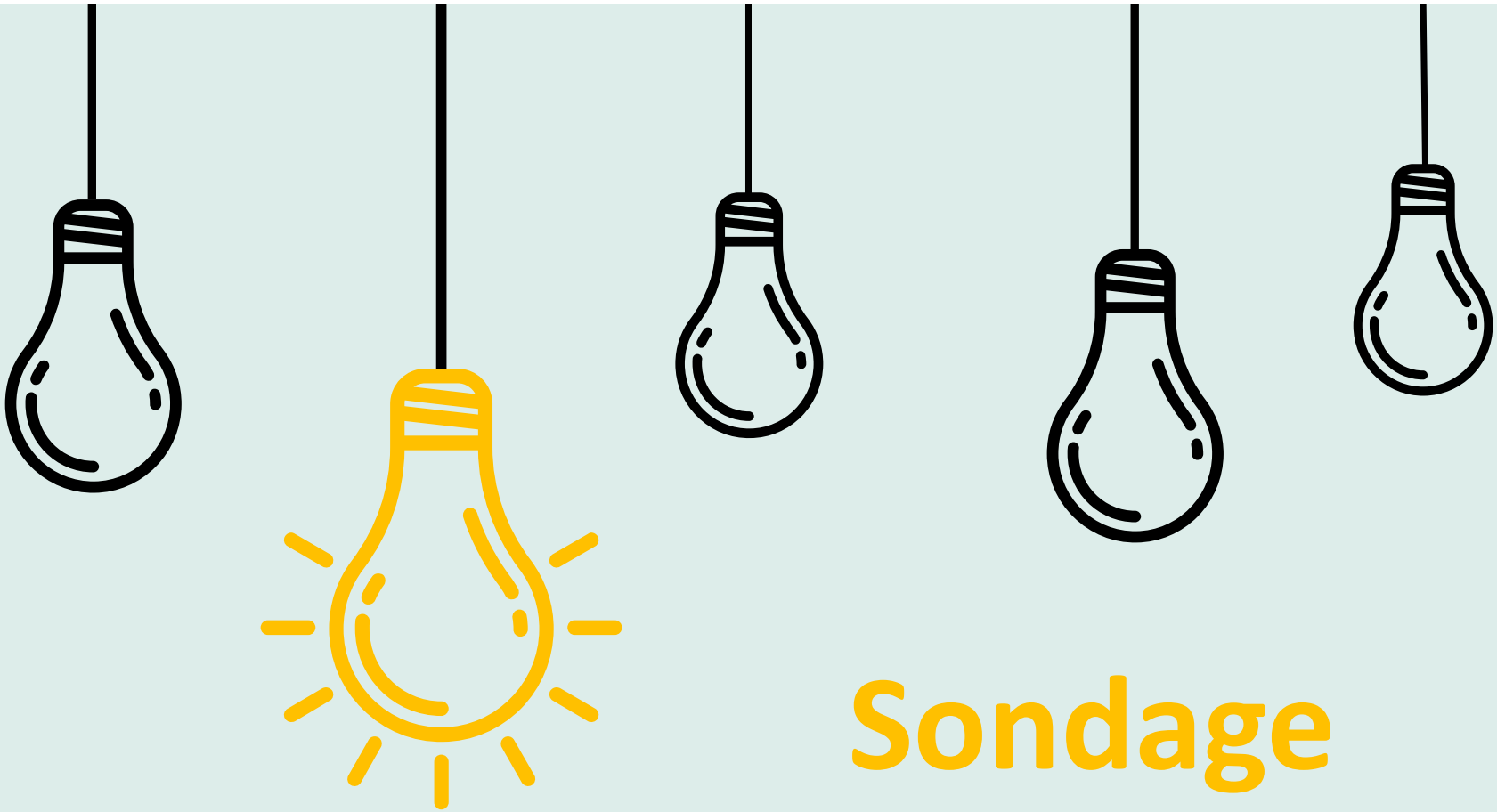
- ✓ On a appris sur le niveau de sécurité de l'organisation
- ✓ Le niveau de conscience globale de l'organisation par rapport au risque de phishing a assurément augmenté
- ✓ Mais le prix à payer est très élevé et la poursuite de la démarche sera complexe

Merci de votre attention !

Caroline Jedwab

caroline.jedwab@cpasnamur.be

081/71.23.40



Sondage

Votre institution a-t-elle déjà subit une cyberattaque ou une tentative de cyberattaque ?

01 02 03 04

Partage d'expériences,
le retour de Seraing sur la cyberattaque

Fabrice LECLERCQ

Gestion informatique

Ville de Seraing

I. La cyberattaque

I. I Le constat

- Au matin du 4 février, nous nous sommes rendu compte que l'ensemble des données avaient été cryptées sur nos serveurs Windows et que les backups ainsi que les backups des backups avaient été effacés.

I. II Les premières réactions

- Nous avons immédiatement porté plainte à la police qui nous a mis en relation avec la Federal Computer Crime Unit (CCU) et avec la Federal Computer Emergency Response Team (CERT).
- Ces entités nous ont donné de précieux conseils qui nous ont permis de récupérer les backups (sans payer la rançon) à l'exception d'un job corrompu. Ils nous ont également fourni une liste de coordonnées de sociétés spécialisées dans la gestion de ce type de crise.

  => Nous avons souscrit au service de l'une d'entre elles qui nous a accompagnés durant la remise en état de l'infrastructure et qui nous accompagne encore aujourd'hui pour sa fortification.
- Nous avons signalé l'incident auprès de l'Autorité de protection des données (APD)

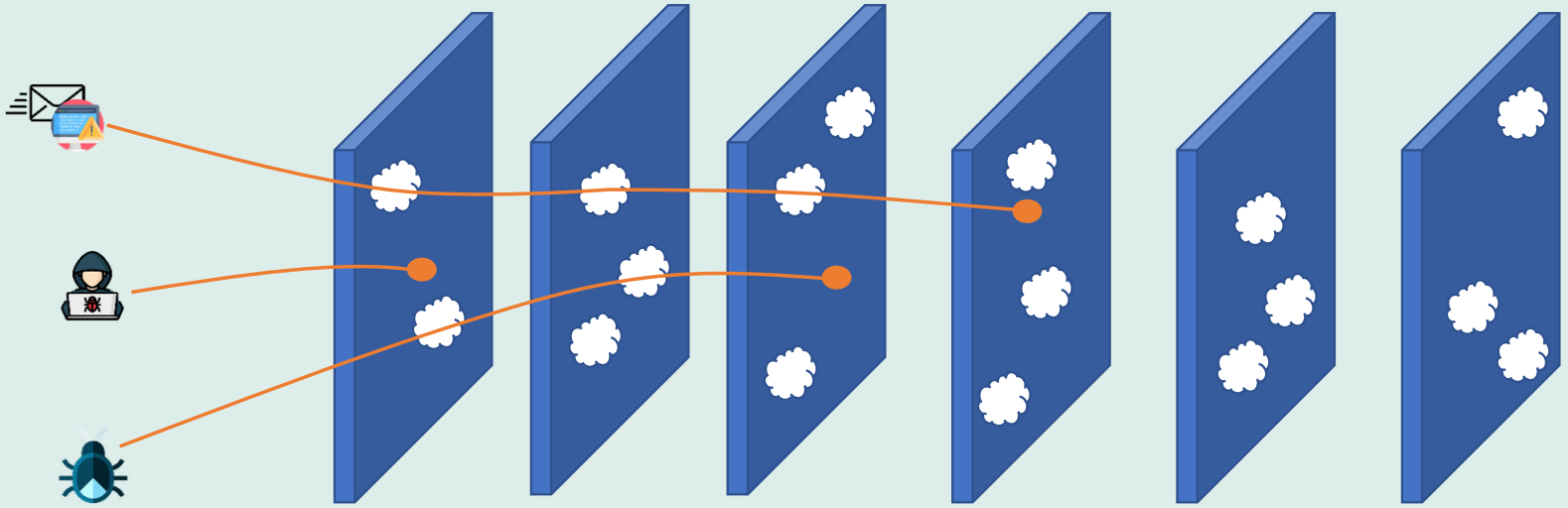
Remarque : les informations corrompues qui n'ont pas pu être restaurées ont dû être reconstruites.

I. III le modus operandi des assaillants

- Les assaillants se sont introduits sur le réseau de la Ville via l'exploitation d'une faille de sécurité sur le pare-feu
- Ce qui leur a donné accès à des identifiants stockés dans la mémoire du pare-feu
- Suite à cela, ils ont utilisé ces identifiants pour se connecter dans le réseau via VPN et se créer un compte dans le domaine avec suffisamment de droits pour lancer un encryptage automatique des données sur les serveurs
- Une petite note avait été mise à disposition sur le bureau de chaque serveur pour nous inviter à entrer en contact avec les pirates afin de connaître le montant de la rançon

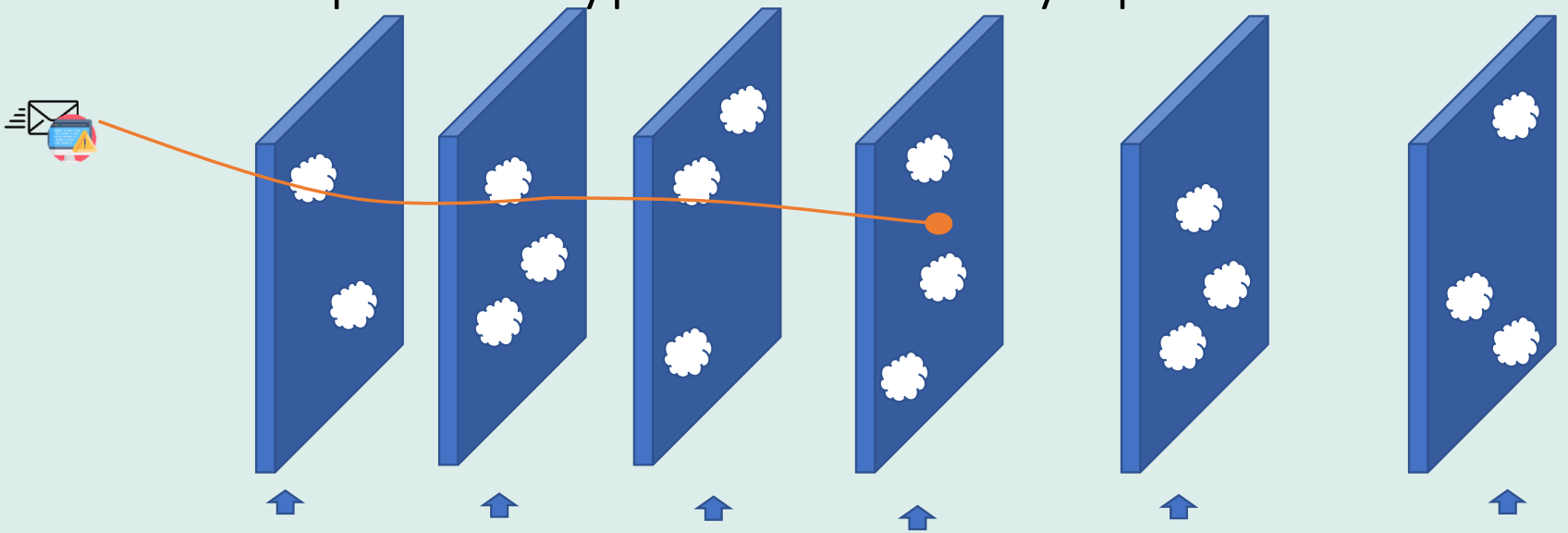
II. Les mesures de sécurité prises suite à l'incident

II.I Le modèle du fromage suisse



II. Les mesures de sécurité prises suite à l'incident

II.II Exemple un cryptolocker envoyé par mail



II.II La feuille de route pour la Ville de Seraing

- ✓ Modification de la politique des mises à jour de l'infrastructure
  - ✓ Définition criticité /exposition
  - ✓ Consultation régulière des sites énumérant les failles de vulnérabilité découvertes
  - ✓ Tenue d'un registre des vérifications et des MAJ
- ✓ Modification de la politique des sauvegardes
  - ✓ Backup de backup sur support externalisé (Cassettes (RDX) conservées dans un coffre dans un autre bâtiment)
  - ✓ Vérification des backups avec test de restauration
  - ✓ Tenue d'un registre

II.II La feuille de route pour la Ville de Seraing

- ✓ Mise en place d'un système de double identification pour les connexions à partir d'Internet (VPN, …)
- ✓ Changement de tous les mots de passe utilisateur et système
  - ✓ Mise en place d'un serveur d'identification
- ✓ Renforcement du cloisonnement entre les différents sous-réseaux
- ✓ Mise en place d'un système de détection d'actions malveillantes dans le réseau

II.II La feuille de route pour la Ville de Seraing

- ✓ Ajout d'une couche protectrice sur le serveur de mails et d'un système d'analyse du comportement des pièces jointes
- ✓ Ajout d'une couche de protection pour les « WebServices »
- ✓ Mise en place d'une DMZ
- ✓ Campagne de sensibilisation destinée au personnel de la Ville via une plateforme de formation automatisée et spécialisée.
- ✓ Remplacement du Wifi par un système à la gestion centralisée et permettant la mise en place de fonctions de sécurité plus élaborées.

III. La nécessité d'investir dans ses ressources humaines.

- Le personnel des services informatiques doivent disposer du temps nécessaire pour :
  - Se former de manière continue car ce domaine d'activité évolue très rapidement
  - Documenter l'infrastructure, ce qui permet :
    - des interventions plus rapides et efficaces
    - de déceler d'éventuelles failles de conception
  - Effectuer les contrôles de routines concernant les MAJ en carences sur l'infrastructure et le bon fonctionnement des backups
  - S'assurer de la bonne exécution des contrats passés avec les sous-traitants
  - Réaliser un « DRP »
  - Effectuer de la veille technologique
  - Gérer des projets d'amélioration continue de l'infrastructure
- Malheureusement, souvent, ces services ont à peine les ressources pour réaliser la charge de travail nécessaire pour le fonctionnement quotidien (Helpdesk, dossiers administratif,…)

III. La nécessité d'investir dans ses ressources humaines.

- Le recours à la consultance est souvent nécessaire dans le domaine informatique car :
  - Les consultants ont un bagage théorique ET pratique dans des domaines très pointus.
  - Le personnel des services informatiques des villes et communes ont souvent une pratique généraliste

  <u>Cependant :</u>
  - Les consultants ne réaliseront que le travail défini par un cahier des charges => il est donc indispensable, au moment de sa rédaction, d'avoir une idée précise des besoins et une connaissance technique suffisante.
  - Il est nécessaire de vérifier le travail réalisé avant de le réceptionner, ce qui nécessite les connaissances techniques adéquates.
  - Un prestataire de service ne se sentira jamais autant concerné par les intérêts de votre organisation qu'un employé.
    - La raison principale de l'existence de cette faille de sécurité sur notre Firewall était une cogestion avec un prestataire de service chargé de réaliser les mises à jour nécessaires.
    - Lorsque nous avons demandé à ce prestataire pourquoi les mises à jours n'étaient pas appliquées, celui-ci nous a répondu : "Parce que vous ne nous l'avez pas demandé."
    - Afin d'éviter tout quiproquo à l'avenir, c'est maintenant le service Informatique de la Ville qui réalise les mises à jour.

IV. La collaboration entre la direction et le service Informatique de l'organisation.

- La sécurité d'un système informatique comporte divers facettes :
  - des aspects techniques
  - la gestion des droits d'accessibilité aux ressources (RN, fichiers,…)
  - la gestion des restrictions (sur les sites Internet,…)
- Les aspects techniques sont gérés par le service informatique et idéalement contrôlés par des tiers spécialisés (par exemple : Pentesting)
- Cependant pour la gestion des droits et des restrictions, cela doit faire l'objet d'une étroite collaboration avec la Direction et le DPO
- Si cela n'existe pas, envisager de mettre en place un comité « sécurité » ayant autorité pour traiter (entre autres) ces questions ?

IV. Quelques ressources

- Plateforme de formation en ligne pour sensibiliser le personnel au différents aspects de la cybersécurité :
  - https://www.knowbe4.com/
  - https://www.k-asap.com/fr/
- Plateforme de formation en ligne pour apprendre l'*ethical hacking* et la cyberdéfense :
  - https://tryhackme.com
  - https://www.hackthebox.com/
- Guide pour La maîtrise de son informatique, au sein d'un pouvoir local réalisé par le RIC (réseau des informaticiens communaux et des CPAS)
  - http://www.ric.be/public/maitrise/view

01 02 03 04 05

Partage d'expériences,
le retour de Liège sur la cyberattaque

Benoit JOSEPH

1er Directeur Spécifique
Département des systèmes d'information
Ville de Liège

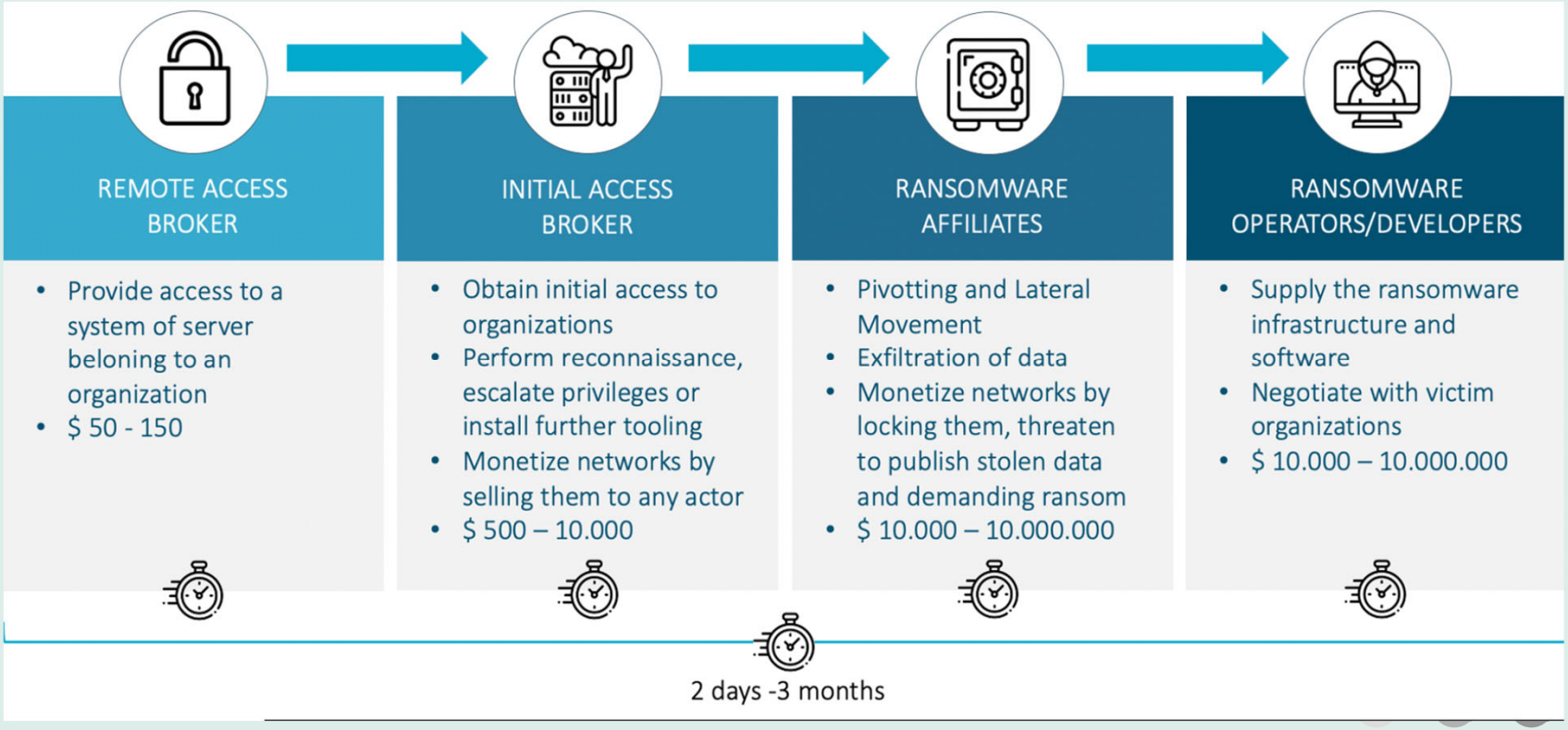
Plan de présentation

✓ Caractéristiques de l'attaque
✓ Vecteurs de l'attaque
✓ Identification et premières réactions
✓ Impacts
✓ Mesures prises suite à l'attaque

Caractéristiques de l'attaque

- ✓ Ransomware RYUK
  - ✓ Capacité d'auto-réplication sur le réseau
  - ✓ Capacité de « réveiller » les ordinateurs pour se propager le plus largement possible
  - ✓ Arrêt de tout système ou processus qui pourrait empêcher l'attaque
  - ✓ Chiffrement des données et systèmes de l'ensemble des serveurs Windows et des PC infectés
    - ✓ Capacité de chiffrement à distance
- ✓ Menée en plusieurs étapes distinctes et réalisées par des groupes criminels spécialisés
  - ✓ Notion de Ransomware as a service
  - ✓ Ciblage des éléments critiques de l'infrastructure (Active directory, système de sécurité,…)

Caractéristiques de l'attaque



Caractéristiques de l'attaque

- ✓ Conclusion
  - ✓ L'attaque subie par la Ville ne doit rien au hasard. Elle s'est déroulée selon un schéma bien établi
  - ✓ Les attaquants étaient organisés et « professionnels »
  - ✓ Le niveau de menace est considérable
    - ✓ Comparé à la menace représentée par les virus ou les attaques plus classiques

Vecteurs de l'attaque

- ✓ Les attaquants ont accédé à un de nos systèmes via un compte compromis
- ✓ Les investigations n'ont pas permis de déterminer la façon dont ce compte avait été compromis.
  - ✓ Un mail de phising est une hypothèse **vraisemblable**
- ✓ L'attaque a eu lieu durant la nuit un dimanche
  - ✓ Ce qui est un élément récurrent dans ce type d'attaque afin de minimiser le risque de réponse face à l'incident.

Identification et premières réactions

- ✓ Etape de l'identification
  - ✓ Indisponibilité et présence d'erreurs dans le comportement de plusieurs services
  - ✓ Remontée d'utilisateurs indiquant l'impossibilité d'ouvrir une session
  - ✓ Constat du chiffrement des postes clients et des serveurs
  - ✓ Identification du ransomware RYUK
- ✓ Ces étapes ont été très rapides
  - ✓ De l'ordre de 30 minutes
  - ✓ Début du diagnostic avant 8h le lundi matin

Identification et premières réactions

- ✓ Premières actions
  - ✓ Arrêt d'urgence de tous les systèmes
  - ✓ Première communication vers les référents informatiques et les utilisateurs
    - ✓ Extinction de tous les postes client (avec retrait physique des prises)
  - ✓ Communication de l'incident à l'autorité
    - ✓ Premier constat de l'ampleur
  - ✓ Contact avec les services ouverts aux citoyens
    - ✓ Affaires citoyennes, urbanismes, …
  - ✓ Ouverture du sinistre auprès de notre assurance

Identification et premières réactions

- ✓ Actions du jour 1
  - ✓ Réunion de crise avec les experts dépêchés par notre assureur
    - ✓ Planification des actions techniques à mener
    - ✓ Vérification que tous les moyens de communication étaient coupés
      - ✓ En effet, la probabilité que l'attaquant soit toujours dans notre infra était élevée
  - ✓ Etablissement des services à restaurer prioritairement
  - ✓ Préparation des solutions de contournement pour les services les plus critiques
    - ✓ Affaires Citoyennes (RN/Pop/EC)
    - ✓ RH
      - ✓ Nous étions fin de mois. Solution pour assurer la paie

Identification et premières réactions

- ✓ Plan d'actions suivi
  - ✓ Sécurisation des moyens de communication
  - ✓ Sécurisation et rétablissement du cœur de notre infrastructure
    - ✓ Système de virtualisation, active directory, …
    - ✓ Mise en place d'un nouvel antivirus et d'un SOC d'urgence
  - ✓ Sécurisation et restauration des services par ordre de priorité et de criticité
  - ✓ Réinstallation du parc PC
    - ✓ Avec l'aide et la solidarité de nombreuses organisations publiques (Province, intercommunale, communes, …)
- ✓ Communication régulière avec
  - ✓ La hiérarchie
  - ✓ Les référents informatiques
  - ✓ L'ensemble de l'administration

Impacts

- ✓ Arrêt de la quasi-totalité des systèmes et applications
- ✓ Interruption du service aux citoyens
- ✓ Difficultés de fonctionnement très conséquentes pour la totalité de l'Administration
- ✓ Nécessité de reconstruire une part importante de notre infrastructure et de restaurer le fonctionnement de l'ensemble de nos serveurs Windows
  - ✓ Les serveurs Linux ont été épargnés par cette attaque
- ✓ Nécessité de réinstaller la totalité de notre parc PC
- ✓ **Le retour « à la normale » aura pris plus de 6 mois**

Mesures prises suite à l'attaque

- ✓ Contexte initial
  - ✓ Charte informatique existante et intégrée au règlement de travail
    - ✓ Sensibilisation à la manipulation des données à caractère personnel et/ou sensible
  - ✓ Disponibilité d'une plateforme de eLearning (OASE)
    - ✓ Avec une section dédiée à la sécurité informatique
  - ✓ Information au personnel lors de campagne de phising
    - ✓ Via un mail général
    - ✓ Via une news sur l'intranet
  - ✓ Sur le plan technique
    - ✓ Présence de l'ensemble des mesures de sécurité « classiques »
      - ✓ FW, proxy, antivirus, politique de mot de passe, protection contre la brute force, compte utilisateurs non privilégiés,…

Mesures prises suite à l'attaque

- ✓ Sur le plan de l'organisation
  - ✓ **Volonté de placer la formation en sécurité IT sur le même pied que les formations obligatoires**
    - ✓ Approche ciblée à avoir car nombre important d'agents à former
  - ✓ **Prise de conscience de la responsabilité collective en matière de sécurité informatique**
  - ✓ Respect plus strict des dispositions déjà existantes
  - ✓ Rappel systématiques des règles et bonnes pratiques à chaque alerte de sécurité
    - ✓ Contact avec l'utilisateur, investigation de l'alerte, sensibilisation
  - ✓ Préparation de l'évolution de la charte
    - ✓ précision et renforcement des devoirs des utilisateurs en matière de sécurité informatique
      - ✓ En particulier lors de l'utilisation de périphériques privés
    - ✓ Rappel et renforcement des prérogatives du DSI en la matière

Mesures prises suite à l'attaque

- ✓ Sur le plan technique
  - ✓ Segmentation du réseau interne et application du firewall entre chaque zone
    - ✓ Ex: chaque étage d'un bâtiment est une zone, les zones contenant des PC ne peuvent pas « se parler »
  - ✓ Application de règles de filtrage (FW) très strictes entre les zones
  - ✓ Application de règles de filtrage sur chaque serveur pour ne permettre que ce qui est nécessaire à l'application hébergée
  - ✓ Segmentation et sécurisation de notre active directory
    - ✓ Restreindre l'accès aux ressources critiques de l'infra
  - ✓ Souscription à une suite de sécurité globale
  - ✓ Mise en place d'un SOC
    - ✓ security operation center : surveillance et remédiation 24/7/365
  - ✓ Personnel affecté au suivi systématique des alertes de sécurité
    - ✓ Contact avec l'utilisateur, investigation, rappel des bonnes pratiques

En conclusion et…
pour aller plus loin

Campagne nationale de sensibilisation à la cybersécurité – Lutte contre le Phishing – CERT
- Pour obtenir les outils promotionnels : https://www.safeonweb.be/fr/materiel-de-campagne

Réseau des informaticiens communaux (RIC)
- « La maîtrise de son informatique, au sein d'un pouvoir local »

http://www.ric.be/public/maitrise/view

Sur safeonweb
- Faites le test du Phishing : https://www.safeonweb.be/fr/quiz/test-du-phishing

Vidéos de sensibilisation - CCB
https://ccb.belgium.be/fr/publication/webinaires-pour-les-organisations

Nos webinaires en replay
- **« Pouvoirs locaux, développez votre stratégie de cybersécurité » - Juin 2021**

https://www.uvcw.be/formations/webinaires/2528

Espace "E-Gov, TIC et simplification administrative" - Site UVCW
https://www.uvcw.be/e-gov/accueil

Votre espace eCampus
- Procédure de connexion : https://vimeo.com/518713611/f3c95176c9

Merci pour votre participation !

À bientôt !