Liège

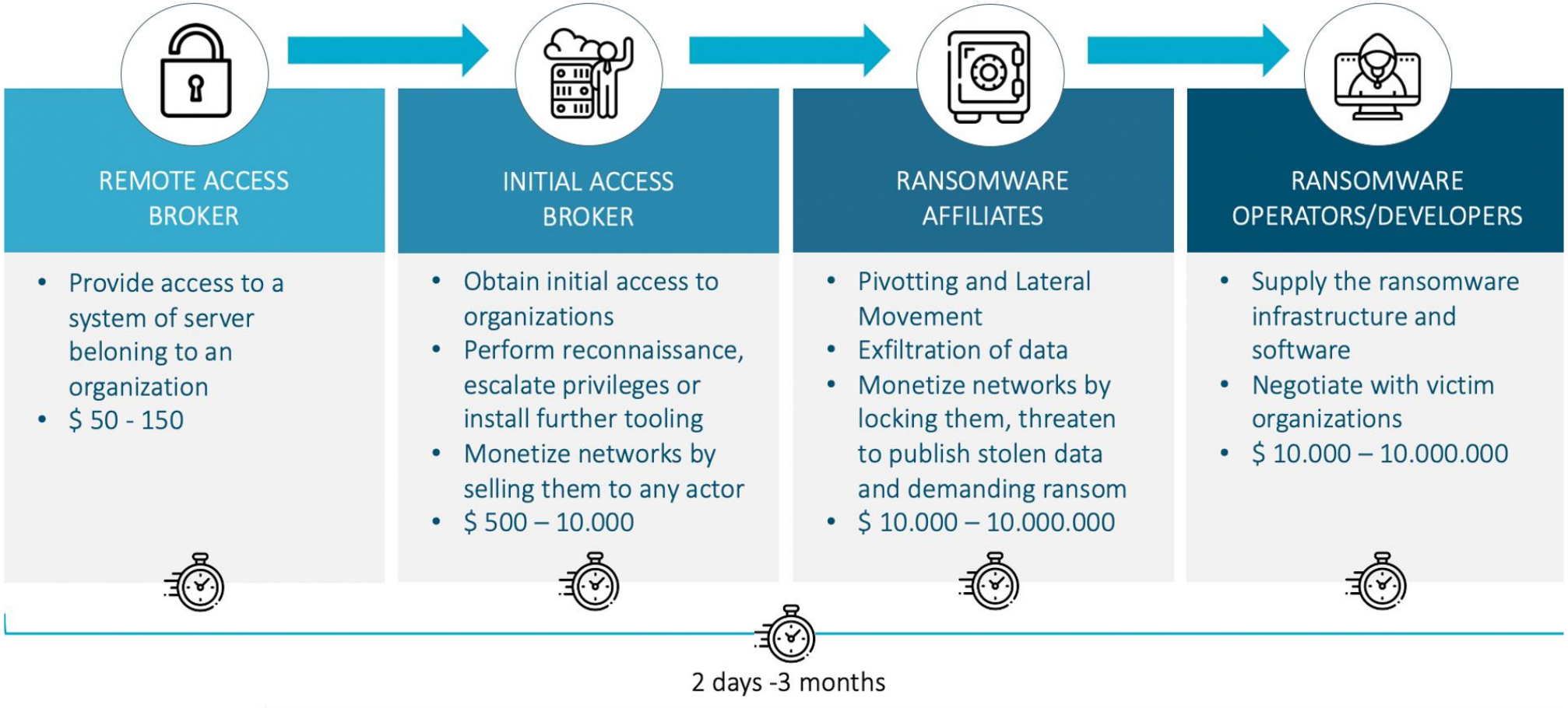
Webinaire Cybersécurité

Ville de Liège
29/03/2022

Plan de présentation

✓ Caractéristiques de l’attaque
✓ Vecteurs de l’attaque
✓ Identification et premières réactions
✓ Impacts
✓ Mesures prises suite à l’attaque
✓ Focus sur les communications
✓ Analyse organisationnelle

Caractéristiques de 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

Caractéristiques de l'attaque

- ✓ 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

- ✓ Accès initial via un compte compromis
- ✓ Le phishing 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

- ✓ 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

Identification et premières réactions

- ✓ Premières actions
  - ✓ **Arrêt d'urgence de tous les systèmes**
  - ✓ Premières communications
    - ✓ vers les référents informatiques et les utilisateurs
    - ✓ Communication de l'incident à l'autorité
    - ✓ Contact avec les services ouverts aux citoyens
      - ✓ Affaires citoyennes, urbanisme, …
  - ✓ Déclaration du sinistre auprès de notre assurance
    - ✓ Risque couvert sur base **d'un audit préalable**

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 l'attaquant n'avait plus d'accès à nos systèmes
      - ✓ En effet, la probabilité que l'attaquant **soit toujours présent** était élevée
  - ✓ Etablissement de la liste des services prioritaires

  - ✓ Travaux initiaux de redémarrage des services les plus critiques
    - ✓ Affaires Citoyennes (RN/Pop/EC)
      - ✓ Soutien du RN
    - ✓ RH
      - ✓ Soutien de notre prestataire SEGI

Identification et premières réactions

- ✓ Plan d'actions suivi
  - ✓ Sécurisation des moyens de communication
  - ✓ Sécurisation et rétablissement du cœur de notre infrastructure
  - ✓ **Mise en place d'un SOC d'urgence**
  - ✓ Sécurisation et restauration des services par ordre de priorité et de criticité
  - ✓ Réinstallation du parc PC
    - ✓ 1800 ordinateurs
    - ✓ Avec **l'aide et la solidarité de nombreuses organisations publiques** (Province, Intercommunales, communes, …)

Impacts

- ✓ Arrêt de la quasi-totalité des systèmes et applications
- ✓ **Interruption du service aux citoyens**
- ✓ Nécessité de reconstruire une part importante de notre infrastructure
  - ✓ 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
  - ✓ Disponibilité d'une plateforme de eLearning (OASE)
    - ✓ Avec une section dédiée à la sécurité informatique
  - ✓ Information au personnel lors de campagne de phishing
    - ✓ Via un mail général, via une news sur l'intranet
  - ✓ Sur le plan technique
    - ✓ Présence de l'ensemble des mesures de sécurité « classiques »
  - ✓ Nous étions assurés

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

Mesures prises suite à l'attaque

- ✓ Sur le plan de l'organisation
  - ✓ 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
    - ✓ **Information sur les données collectées par les systèmes de sécurité**

Mesures prises suite à l'attaque

- ✓ Sur le plan technique
  - ✓ Sécurisation du réseau à tous les niveaux
    - ✓ **ne permettre que ce qui est nécessaire** aux applications hébergées
      - ✓ Segmentation du réseau, application de règles de filtrage (FW) très strictes entre les zones, application de règles de filtrage sur chaque serveur
  - ✓ Sécurisation du cœur de l'infrastructure
    - ✓ 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

Mesures prises suite à l'attaque

✓ Coûts humains et financiers conséquents

✓ Aide à venir via IMIO et le subside de la Région Wallonne

- ✓ Webinaire le 27 avril

Focus sur les communications

- ✓ Communications avec
  - ✓ L’autorité communale
  - ✓ Les experts mandatés par notre assureur
  - ✓ L’administration et nos collègues
  - ✓ Le Citoyen
  - ✓ La RCCU
  - ✓ L’APD

Focus sur les communications

- ✓ Communication avec l'autorité communale
  - ✓ La crise a été gérée par le DSI et le **Directeur Général**
  - ✓ Le DSI (vers Monsieur le Directeur Général)
    - ✓ Etats de situation réguliers
    - ✓ Formulation des points de décision stratégique
  - ✓ Monsieur le Directeur Général pour
    - ✓ L'information au Collège
    - ✓ Les décisions stratégiques
    - ✓ Communication vers l'ensemble du personnel
      - ✓ Modalités de travail, …

Focus sur les communications

- ✓ Communication avec Les experts mandatés par notre assureur (Northwave)
  - ✓ En charge de l'investigation sur le déroulement de l'attaque
    - ✓ Licence de **détective privé**
    - ✓ **Négociateur agréé**
    - ✓ Collaboration avec différentes polices européennes
  - ✓ Communication avec le DSI
    - ✓ Plan de sécurisation et de remise en route
  - ✓ Communication avec le Directeur Général (et le DSI)
    - ✓ Rapport concernant l'attaque et les mesures prises
- ✓ Remarque :
  - ✓ Northwave a vérifié si notre attaquant était placé sur « liste noire »
  - ✓ Si tel est le cas, aucune rançon ne peut être versée même si vous êtes couverts

Focus sur les communications

- ✓ Communication avec L'administration et nos collègues
  - ✓ Le DSI
    - ✓ informations opérationnelles aussi rapidement que possible
    - ✓ Point d'attention pour
      - ✓ Les services directs aux citoyens
      - ✓ Les services prioritaires
  - ✓ La Direction Générale
    - ✓ Communication vers le personnel
      - ✓ concernant les modalités de travail, …

Focus sur les communications

- ✓ Communication avec le Citoyen
  - ✓ Conférence de presse du Collège
  - ✓ Gestion par le service communication
    - ✓ Au travers du site Internet
    - ✓ Sur base des informations fournies par le DSI

Focus sur les communications

- ✓ Communications avec la RCCU
  - ✓ Dépôt de plainte
    - ✓ Par le DSI (Directeur) et le Département Juridique. A noter l'absence de soutien ou/et de réaction.
  - ✓ Mise en relation avec Northwave
  - ✓ Pas de prise en charge opérationnelle dans notre cas

Focus sur les communications

- ✓ Communication avec l'APD
  - ✓ Gérée par la DPO
    - ✓ Sur base des données reçues du DSI
  - ✓ Déclaration initiale dans le délai légal
    - ✓ Risque d'exfiltration de données, impact, …
  - ✓ Déclaration ultérieure
    - ✓ Une fois le rapport des experts fournis

Focus sur les communications

✓ Communication avec l'APD

- ✓ Déclaration extrêmement fastidieuse et redondante : 15 pages
- ✓ Des questions "difficiles". Ex : nombre minimal de personnes concernées, nombre maximal de personnes concernées
- ✓ Déclaration uniquement par voie informatique et par internet
- ✓ Aucun retour concret suite aux déclarations : un AR automatique.

Focus sur les communications

✓ Communication publique : par voie de communiqué de presse

✓ Question de la communication aux citoyens concernés :

- ✓ choix de se contenter de la communication publique et de répondre au cas par cas (2 demandes) sur base de l'analyse des experts qui estiment probable que les données n'ont pas été publiées.

Analyse organisationnelle

- Importance de définir le rôle de chacun : qui fait quoi en interne, en externe
- Maîtriser la communication
- S'assurer en cyber-risque
- Investir
  - dans la sécurité informatique
  - dans la formation des agents

Merci pour votre attention!