Intrusion informatique : 2^e vague de reconnections, bilan et perspectives un mois après

1 mois après une intrusion d'ampleur dans son environnement informatique, le Service public de Wallonie vous propose un état de la situation et une série de perspectives pour les semaines à venir.

Rappelons tout d'abord que, grâce à la détection rapide de l'intrusion par les équipes du SPW Digital et à la décision dans la foulée de nous couper d'Internet, cette effraction dans notre système informatique n'a pas entraîné de vols, d'exfiltrations massives, de cryptages ou de destructions de données. Aucune demande de rançon n'a non plus été formulée. **Le CCB et Microsoft n'ont par ailleurs trouvé aucune preuve de revendications ou de tentatives de vente de données issues du SPW sur le *Dark web*.**

Le Service public de Wallonie a également **porté plainte**. L'enquête a été confiée au Parquet fédéral. Une information judiciaire est donc en cours. Le respect de son secret est crucial pour aider notamment la Justice à identifier l'auteur de l'intrusion.

Soulignons néanmoins qu'**aucun système public ou privé n'est à l'abri à 100% d'une intrusion aussi ciblée et sophistiquée**. Ce type de menace a nécessité (et nécessitera encore demain) une mobilisation exceptionnelle que nous avons mise en œuvre immédiatement avec l'aide de nos partenaires (Microsoft, NRB, CCB et d'autres tel que Proximus).

Pourquoi cela prend du temps?

La restauration de l'environnement IT du SPW exige un travail titanesque dans un délai très serré, dont il est important de mesurer l'ampleur. Au-delà de l'analyse du schéma de l'intrusion (indispensable pour lutter contre la persistance de la menace), **l'environnement informatique du SPW a dû être renforcé pour une meilleure sécurité et un meilleur monitoring.**

Concrètement et sans entrer dans les détails naturellement confidentiels de notre sécurité, **la « maison digitale SPW » s'est dotée de nouveaux outils de détection qui lui permettent 24/7 de rapidement repérer toute tentative d'intrusion et de neutraliser cette menace en évitant un nouveau confinement informatique généralisé.**

Nous sommes donc clairement **mieux armés aujourd'hui qu'hier**, même si à nouveau personne ne peut se prétendre invulnérable.

Un plan de restauration de notre environnement informatique par vagues

On ne modifie cependant pas l'architecture informatique de plus de 800 applications et de milliers de serveurs en 15 jours; c'est une refonte structurelle qui va prendre plusieurs mois, voire plusieurs années. A côté de cet objectif à long terme, le SPW travaille depuis le 17 avril en parallèle à un objectif à court terme de restauration de ses outils afin d'assurer au mieux la continuité de ses services et d'impacter au minimum ses usagers.

Notre stratégie de reconnexion prévoit des **vagues successives de reconnexion de nos outils en fonction des garanties de sécurité et des services prioritaires pour nos usagers.**

Pour rappel, **une première vague de restauration a été lancée la semaine dernière.** Il s'agit avant tout d'applications **"fondatrices" et transversales**, comme des outils d'authentification, des bases de données ou des plateformes d'échanges de données.

Si cette étape a entraîné peu d'effets directement visibles pour nos usagers, c'était une **première étape cruciale pour restaurer de manière robuste et durable notre environnement informatique.** Notons cependant que cette première vague a permis la récupération de notre **Géoportail**, essentiel en interne notamment pour la gestion des permis, mais aussi en externe pour de nombreux partenaires (communes, notaires, architectes, etc.).

La récupération de nos bases de données et/ou d'échanges de données a aussi mis fin aux dommages collatéraux de notre confinement sur nos partenaires, dont le **TEC** (ex: nouveau abonnement) ou le **FOREM** (nouveau compte titres-services).

Enfin, cette 1ère vague a aussi eu des effets de bord positifs comme la **remise en ligne de toute une galaxie de sites**, dont plusieurs portails thématiques: fiscalite.wallonie.be; emploi.wallonie.be; environnement.wallonie.be; mobilite.wallonie.be; etc.

2ème vague importante cette semaine avec Wallonie.be et ses démarches

Comme promis, et les fondations de la première vague posées, cette semaine a permis la **restauration d'une nouvelle salve d'applications beaucoup plus concrètes pour nos usagers.**

Ainsi, **nous venons ce vendredi de reconnecter non seulement notre site faitier Wallonie.be**, outil central de notre communication externe, mais son site annexe **Mon Espace sera à nouveau en ligne d'ici quelques heures**. Toutes les démarches et leurs fonctionnalités ne seront pas encore 100%

opérationnelles, mais les plus usitées seront disponibles. Il s'agit notamment des demandes de primes habitation, de plans de paiements pour les taxes ou de subsides pour les entreprises.

Sur le plan interne, nos agents recouvrent la pleine possession des outils hydrologiques, fiscaux ou de gestion des dossiers européens.

3ème vague dès la semaine prochaine

Une 3ème vague est d'ores et déjà prévue la semaine prochaine. Le retour de 3 applications est particulièrement attendu à cette occasion:

- **PacOnWeb**: le guichet électronique des agriculteurs qui va leur permettre de rentrer leur déclaration de superficie, étape indispensable aux paiements des aides agricoles européennes. **Initialement prévue début de semaine prochaine, elle est accessible depuis cet après-midi.** Par ailleurs, pour permettre aux agriculteurs de rentrer leurs dossiers dans le respect de leurs contraintes, **la date butoir initialement prévue le 26 mai a été reportée par le Gouvernement au 13 juin inclus.**
- **L'écosystème Certificats verts (CV)** : une partie de celui-ci a déjà été reconnecté cette semaine et des mesures de contournement (papier) ont été proposées permettant aux détenteurs de ces CV (principalement des entreprises) de faire leurs relevés, de demander leur état de compte, de vendre ou d'annuler des CV. **Une dernière partie de cet écosystème, qui permet de vendre à l'international, est à cette heure toujours hors service. Sa reconnexion est cependant imminente ;**
- **Le Guichet des pouvoirs locaux** : essentiel pour les communes dans le cadre de leurs obligations vis-à-vis de la Région, pouvoir de tutelle.

Notons aussi, en interne, que nos agents récupéreront, après les outils cartographiques la semaine dernière, leurs applications de gestion des dossiers de demandes de permis urbanistiques et environnementaux.

Nous terminons un sprint mais nous entamons un marathon

Avec ces trois premières vagues, nous avons concentré notre stratégie à la **réactivation d'applications transversales qui ont des effets « levier »** importants. Elles sont la **colonne vertébrale** de l'administration et garantissent **l'exécution de ses missions essentielles.**

Attention, cela **ne veut pas dire que la crise est bientôt derrière nous.** Nous venons simplement de **terminer un sprint et nous entamons un marathon.** Avec ces 3 vagues, nous venons de restaurer les 50 applications les plus importantes. Il nous en reste des centaines à reconnecter, voire à reconstruire !

C'est pourquoi, en vue d'un retour vers une administration complètement fonctionnelle, nous travaillons dès à présent aux étapes suivantes de notre stratégie.

La suite de celle-ci se traduira tout d'abord par **3 nouvelles vagues de reconnexion** (le détail sera fourni la semaine prochaine) avant d'entamer **une phase d'industrialisation** où, en catégorisant les applications, nous ambitionnons des reconnexions par lots.

Soyons clairs... on ne parle pas de semaines, mais sans doute de mois avant une reconnexion totale.

Cette crise nous oblige à être ambitieux

Pour conclure, cette intrusion et la crise majeure qu'elle nous fait aujourd'hui traverser offrent au moins une opportunité : celle de nous obliger collectivement à être ambitieux quant à l'environnement informatique de nos institutions publiques et surtout à continuer à investir structurellement dans sa protection.

Nous tenons enfin à **remercier nos usagers et nos partenaires pour leur patience et leurs nombreux messages de soutien**. Qu'ils sachent que notre mobilisation reste intacte.