Service public fédéral Intérieur
Service Information et Communication

communiqué de presse

25.05.2021

Le SPF Intérieur a fait face à une cyberattaque et modernise son infrastructure informatique

Correspondant: Olivier Maerens **T:** 0475/363866

E-mail: olivier.maerens@ibz.fgov.be

- Le SPF Intérieur a été la victime d'une cyberattaque complexe, sophistiquée et ciblée. Toutes les mesures nécessaires sont prises.
- L'enquête judiciaire concernant la cyberattaque est en cours. La détermination et le caractère discret de cet acteur éveillent des suspicions d'espionnage.
- En mars 2021, le Centre pour la Cybersécurité Belgique (CCB) a trouvé des pistes subtiles d'actes douteux sur le réseau du SPF Intérieur. Une analyse en profondeur a démontré qu'un attaquant avait pu s'introduire en avril 2019. Le SPF Intérieur et le CCB prennent cette situation très au sérieux.
- Les deux services ont directement mis au courant les instances officielles et ont immédiatement mené des actions afin de supprimer les pistes de l'attaquant et de bloquer l'accès.
- La situation est sous contrôle : le réseau a été nettoyé et la sécurité a été rétablie. Aucun autre détail ne peut être communiqué en raison de l'enquête en cours.

Ce qui s'est passé avant

Au début de l'année, Microsoft a été mis au courant d'une série de vulnérabilités dans ses serveurs Exchange. Il s'agit de serveurs email utilisés mondialement par des milliers d'entreprises. Microsoft a lancé le 2 mars des mises à jour pour protéger à nouveau ses systèmes. Le SPF Intérieur utilise également des serveurs Microsoft Exchange et a demandé l'assistance du CCB. Le SPF, tout comme des milliers d'entreprises à travers le monde, a été vulnérable et des « portes d'entrée » ont été découvertes sur le réseau. Celles-ci ont été fermées et les mises à jour ont été immédiatement appliquées mais le CCB a également mené un monitoring plus poussé.

C'est lors de cette enquête que les cyber-experts du CCB ont relevé des pistes subtiles d'actes douteux sur le réseau du SPF. Les premières pistes datent de avril 2019 et indiquent une cyberattaque très sophistiquée. La complexité de cette attaque indique un acteur qui dispose de cyber-capacités et de moyens étendus. Les auteurs ont agi de façon ciblée, ce qui fait penser à de l'espionnage.

Vers un réseau neuf et sécurisé

Dès que le SPF a été au courant de cette attaque, le Centre de Crise National, l'Autorité de Protection des Données, la Police Fédérale, le Parquet Fédéral, la Sûreté de l'Etat, SGRS et le SPF Affaires étrangères ont été prévenus, conformément aux directives déterminées dans le plan de cyberplan d'urgence national.

Le dossier est ouvert par le Parquet Fédéral et l'enquête est dirigée par un juge d'instruction bruxellois. Du soutien a été demandé au CCB pour évaluer l'étendue de l'attaque et pour y remédier. Le CCB a décrit un plan d'approche et a soutenu le SPF dans le cadre de son exécution. Des actions urgentes ont été entreprises : l'accès de l'attaquant a été stoppé, les malwares ont été supprimés et l'information importante a été mise en sécurité.

La situation est toujours surveillée. Pour ne rien laisser au hasard, les systèmes IBZ ont été évidemment nettoyés de façon à restaurer la sécurité.

Le SPF a entamé une modernisation complète de son infrastructure informatique en vue d'optimiser au maximum la sécurité.

Aucun autre détail concret ne peut être communiqué dans l'intérêt de l'enquête.

Rue de Louvain 1
1000 Bruxelles
T 02 488 10 00
F 02 488 19 68
info@ibz.fgov.be
www.ibz.be