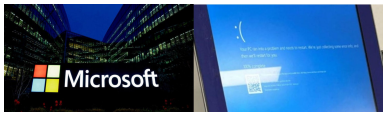
http://pierrealainmillet.fr/la-panne-bleue-a-qui-accorder-sa-confiance-numerique

la panne bleueâ€¦ à qui accorder sa confiance numérique ?

- Numérique -



Date de mise en ligne : vendredi 19 juillet 2024

Stupéfaction ce vendredi 19, une "panne informatique mondiale" qui arrête les aéroports, les hôpitaux, des bourses, des milliers d'entreprisesâ€¦ Très vite, la cause est identifiéeâ€¦ une mise à jour d'un outil de sécurité inclus dans les systèmes Microsoft, et donc installé sur des millions de machinesâ€¦. On lit souvent que c'est un antivirus, mais c'est plus exactement un "EDR" [[1], un outil plus moderne qu'un antivirus classique, qui contrôle non pas seulement les flux de données entrant dans votre ordinateur, mais le comportement de tous les équipements connectés qu'on appelle des *« points de terminaison »* [2]. Ces outils très modernes et récents reposent sur de l'intelligence artificielle qui analyse des millions de comportements d'équipements pour apprendre à identifier un comportement anormalâ€¦

La France semble moins touchée que les USA, l'Australie ou l'Inde, entre autre car des infrastructures importantes comme les aéroports, la SNCF, les hopitaux, utilisent d'autres solutions que celles de Microsoft.

Pas d'écran bleu ce 19 juillet pour les services du SITIV !

Et nos communes ? Pour celles du SITIV, tout va bien, puisque nous avons développé ces services « EDR » avec une autre solution, HarfangLab, certifiée par l'ANSSI . Cela ne veut pas dire qu'il ne peut pas y avoir de panne, mais d'une part, nous ne sommes pas dépendants d'un géant mondial dont on peut penser qu'il fait tout pour se sortir de cette panne, mais sans doute avec ses propres prioritésâ€¦ Et d'autre part, il n'y a que les professionnels de l'éditeur Crowdstrike et sans doute certains experts de Microsoft qui sauront exactement pourquoi il y a eu cette panne. Aucune transparence surtout pour de petits acteurs comme les simples usagers ou même nos collectivités locales, et aucune chance de pouvoir évoquer des dédommagements !

Oui, des solutions libres, publiques et souveraines sont un enjeu essentiel du numérique

Certains informaticiens qui ont l'habitude des solutions Microsoft sont inquiets et même parfois opposés aux solutions alternatives dites « libres », c'est à dire dont les codes sources sont publics et peuvent être revus, et corrigés, par tous ceux qui le veulent (et le peuventâ€¦). Et Microsoft, comme tous les géants du numérique comme Google ou Facebook sont d'excellents commerciaux qui donnent le sentiment que rien n'est cher, voir que tout est gratuit. Pourtant ils battent tous les records de chiffre d'affaire, donc dans les faits, on paie très cher.

D'ailleurs les collectivités qui paient des licences et des services Microsoft le savent bien. On commence par une offre alléchante de bureautique pour quelques dizaines de postes, et puis on ajoute la messagerie, et puis le serveur de document, et un jour on s'aperçoit qu'il faut une centaine de licences, et qu'il faut non seulement les licences originales, mais aussi des services complémentaires, et Microsoft rappelle que les licences sont valables pour un certaine nombre d'utilisateurs, et qu'il faut payer plus quand il y en a plusâ€¦ et à la fin, le directeur des finances demande *« mais pourquoi on paie aussi cher ? »*

Avec les Territoires Numériques Ouverts, la métropole, la ville de Lyon et le SITIV sont en avance !

Cet exemple de la panne géante Microsoft est illustrative. Personne n'est à l'abri d'une panne, même pas les géants du numérique ! Il faut donc apprendre à se protéger, avoir des spécialistes et des responsables de la sécurité numérique, avoir une stratégie de sécurité numérique, sensibiliser tous les usagers et professionnelsâ€¦

C'est ce que fait le SITIV depuis des années. Il est d'ailleurs reconnu par le label ExpertCyber du gouvernement. Et il est l'opérateur de la plateforme TNO (Territoires Numériques ouverts) de la métropole, la ville de Lyon et donc le SITIV au service de 35000 agents et élus. Cette plateforme libre, souveraine, sécurisée issue d'un appel à projet « France Relance Numérique » est opérationnelle et en plein déploiement dans les trois collectivités, et donc pour les 7 communes du SITIV.

Et le SITIV est devenu récemment le premier opérateur en France à bénéficier du service *« agent connect »* mis en place avec l'ANSSI, l'ANCT, la DINUM pour sécuriser l'identité numérique des collectivités, des élus et des agentsâ€¦ Pour ceux qui connaissent, c'est le même principe que le compte « France connect » que nous pouvons tous utiliser pour accéder aux services des impôts, des retraitesâ€¦ mais destiné aux fonctionnaires et à leurs systèmes d'information.

Avec cette plateforme TNO et le service agentconnect, le SITIV construit patiemment une confiance numérique publique pour répondre aux de cybersécurité !

agentconnect

---

[1] (en anglais un « Endpoint Detection & Response »)

[2] d'où la dénomination endpoint detectionâ€¦