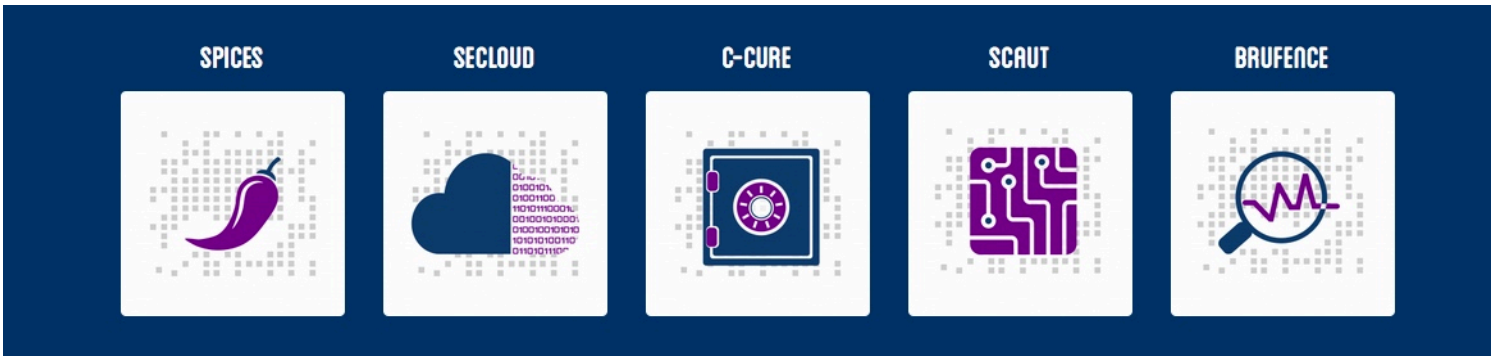
DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

LA RÉGION BRUXELLOISE MISE SUR LA SÉCURITÉ INFORMATIQUE

Publié le 10 septembre 2015



La Secrétaire d'Etat bruxelloise à la Recherche scientifique, Fadila Laanan, le dit sans détour: bien sûr qu'elle utilise les services informatiques disponibles sur le web! Y compris à titre privé. Mais pour ce qui est de stocker toute sa vie dans le « Cloud », elle a encore quelques réticences… « Est-ce vraiment sûr? » s'interrogeait-elle en début de semaine, lors du lancement du programme de recherche "Secur'IT".

Au vu des chiffres du CERT (Cyber emergency team), le service fédéral d'intervention d'urgence en sécurité informatique, il y a de quoi se poser la question. En 2014, quelque 800 incidents par mois ont été rapportés au CERT. Au cours des six premiers mois de l'année (2014), plus de 750.000 ordinateurs ont été infectés par un virus en Belgique. Et la tendance est à la hausse.

Évolution du nombre d'incidents et notifications mensuels recensés par le Cert depuis sa création en 2010. (Cliquer pour agrandir)

Huit millions en trois ans pour la recherche en « Secur'IT »

La Secrétaire d'Etat a pu mesurer combien cette question de sécurité informatique mobilisait également les scientifiques des universités, des entreprises et des hautes écoles implantées dans la Région bruxelloise.

A l'occasion du démarrage du programme Secur'IT, subsidié par la Région via Innoviris et ses actions « Bridge » (7,8 millions d'euros de budget en trois ans), les coordinateurs des cinq projets financés cette année sont venus détailler leurs recherches. Elles entrent dans trois sous-thématiques:

- - La sécurité du réseau et des entreprises grâce au design
- - La gestion efficace et sûre des grands volumes de données (le « Big data »)
- - Une meilleure authentification des utilisateurs (des services, lors de paiement, etc.)

Affiner la lutte contre le « cambriolage informatique »

L'un de ces nouveaux projets, « SPICES », dirigé par des chercheurs de l'ULB, fait le lien avec des travaux en phase d'atterrissage pilotés ces deux dernières années par la société Sogeti Belux, située à Evere. Les recherches de Sogeti impliquaient déjà une équipe de l'ULB, mais aussi de l'Université de Gand et de Sirris, une organisation qui propose ses services et son expertise technologique aux entreprises.

Ce projet de sécurité des « Big datas », financé en partie par la Région bruxelloise, se clôture en octobre. Il portait sur la mise au point d'un système de détection des intrusions dans les réseaux informatiques ou les serveurs d'une entreprise. Le prototype est quai finalisé et prêt à être testé.

« Les intrusions dans les systèmes informatiques représentent un risque majeur », souligne Yves de Beauregard, patron de Sogeti BeLux. « On peut tenter de s'en protéger en multipliant les barrières, les firewalls et autres systèmes de blocage. Mais l'effet pervers de cette multiplication de barrières, outre le coût important et permanent que cela représente, est que cela aiguise aussi l'appétit des hackers. En mettant en place de nouveaux systèmes de sécurité, on risque d'attiser leur intérêt… Pour ces pirates, il y a là de nouveaux « défis » à relever… »

Détecter les signes avant-coureurs

L'approche suivie par ce précédent consortium de recherche a donc pris le problème par un autre bout. « Tout comme les cambriolages dans les maisons, les intrusions informatiques sont annoncées par des signes diffus », reprend Yves de Beauregard.

« Avant de réellement passer à l'action, un cambrioleur va d'abord venir repérer les lieux. Il va tester la fermeture de vos fenêtres, de vos portes. Il va sonner afin de vérifier s'il y a quelqu'un à la maison. En ce qui concerne les intrusions dans les systèmes informatiques, cela se passe également de la sorte ».

« Notre système de détection s'intéresse à la détection de ces événements qui peuvent annoncer une intrusion. Quand les hackers s'en prennent à votre système, ils laissent des traces. Détecter ces signes avant-coureurs, qui créent des comportements qui ne sont pas habituels dans les systèmes, permet de réagir plus efficacement, en investissant massivement et ponctuellement dans des mesures de sécurité adaptées.

Le projet SPICES, qui démarre actuellement, s'inscrit dans la droite ligne de cette thématique. Au point qu'Yves de Beauregard parle quasiment de Spin-off...

> ***Principaux risques de piratage informatique en Belgique***
>
> *Dans son rapport de février 2015, le Cyber emergency team fédéral détaille la nature des incidents informatiques qui ont touché les ordinateurs/réseaux informatiques en Belgique. Trois grandes familles d'incidents sortent du lot.*
>
> *- Dans 30,5 % des cas, il s'agissait d'incidents de « scan ». Des cas de scanning de bases de données en vue d'y détecter des points faibles.*
> *- Dans 29,5 % des cas, les incidents portaient sur des attaques avec des vers ou de virus.*
> *- Dans 21% des cas, les incidents rapportés concernaient des interventions de hackers « white hat ». Ces « bons » hackers signalaient des failles de sécurité dans les réseaux, les sites, les serveurs, etc.*
>
> *Le reliquat concernait notamment des cas de pishing (5,5%), de serveurs infectés (3,5%), de spams involontaires (5%). Les attaques de type « déni de service » (blocage des serveurs) ne concernaient que 0,5% des cas recensés.*