White box security : une autre approche de la cybersécurité?

Autor(en): **Gerber, Christophe**

Objekttyp: **Article**

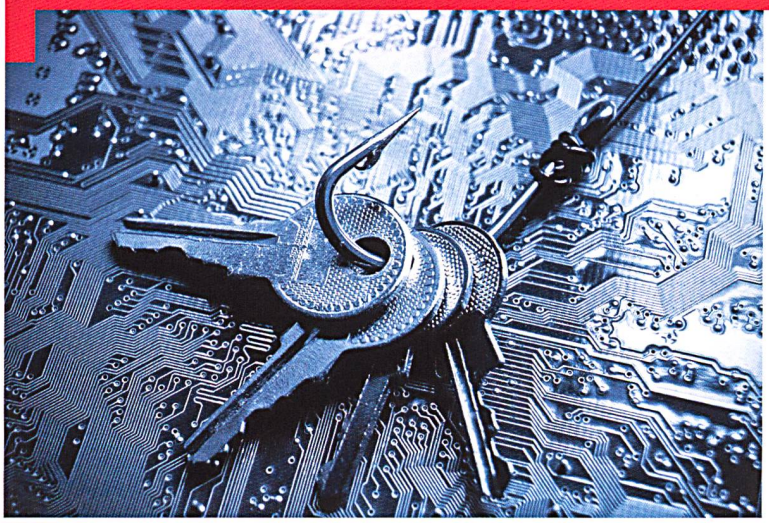
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2018)**

Heft [2]: **Numéro Thématique 2**

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-823457



Cyber

White box security – Une autre approche de la cybersécurité ?

Lt-col EMG Christophe Gerber
Responsable Défense & Cybersécurité chez ELCA

Si de nombreux écrits apportent des solutions afin de mieux se défendre contre des cyberattaques, par des mesures de monitoring, de protection et d'intervention, voire de contre-attaques, force est de constater que peu de monde s'intéresse à la sécurité intrinsèque des systèmes informatiques. C'est-à-dire, comment les concevoir et les opérer de la manière la plus sûre possible.

Lorsque l'on parle de cybersécurité, on considère que 3 propriétés principales nécessaires doivent absolument être protégées :

- Confidentialité : le système (ou la donnée) ne doit pas être disponible ou visible à des individus, entités ou processus non-autorisés ;
- Disponibilité : le système (ou la donnée) est accessible et utilisable, sur demande, par une entité autorisée ;
- Intégrité : le système (ou la donnée) est précise, correcte, complète et n'a pas été modifiée.

L'expérience montre que des lacunes dans la qualité sont toujours à la base d'une faille de sécurité ou de son exploitation par une partie adverse. Par exemple :

Une erreur de traitement dans un cas particulier pourrait amener à l'indisponibilité d'un système. Ledit système pourrait par la suite se retrouver indisponible (par accident), s'il se retrouvait dans ce même cas particulier, ou alors une personne malveillante pourrait pousser le système à se retrouver dans ce cas particulier. Il s'agirait de l'exploitation d'une faille. Dans les 2 cas, une erreur de conception génère une indisponibilité. Le cas particulier n'ayant pas été testé.

Une organisation malveillante implémente un module permettant l'extraction de données et l' envoie vers un emplacement de récupération. Ce module est introduit dans notre système informatique, soit lors de la fabrication soit ultérieurement par envoi distant. Un meilleur contrôle de l'intégrité du système n'aurait pas permis cette implémentation d'un module inconnu. Une attaque par déni de service (DoS) paralyse un site de commerce en ligne ou un guichet e-gouvernement pour les citoyens. La porte d'entrée dudit site n'a pas été conçue de manière à tenir une surcharge et l'utilisation de mesures de protection (p.ex. système de file d'attente) n'avait pas été prévue ou n'a pas fonctionné. Une analyse de risque adaptée aurait dû identifier cette menace potentielle et une architecture adéquate aurait ainsi pu être mise en place.

Ces considérations qualitatives sont à prendre en compte sur la chaîne de conception et fabrication de tout système informatisé. Cette chaîne couvre l'analyse des risques et menaces, l'architecture & design et finalement les tests et l'assurance qualité.

De manière plus importante encore, tout changement important de la topologie et des fonctionnalités du système devrait faire l'objet d'une nouvelle analyse sous la forme de l'amélioration continue.

Si de telles bonnes pratiques sont indispensables lorsque l'on développe ses propres systèmes – on parle notamment de Secured Development Lifecycle (SDLC), la chose se complexifie lorsque l'on n'a pas de propre capacité de production et que l'on doit acquérir ses systèmes informatiques auprès de fournisseurs externes.

Dans un tel cas, toujours dans l'optique d'une meilleure compréhension de son système IT (white box), il s'agit de mettre en place des mesures de contrôle auprès de ses sous-traitants. On parle dans ce cas de sécurisation de la chaine d'approvisionnement (supply chain security).

Souveraineté numérique : Passage obligé ?

Lorsque l'on veut assurer une bonne sécurité de sa chaîne d'approvisionnement, il est également important d'en identifier les maillons critiques ou les éléments stratégiques : les joyaux de la couronne, et de les traiter avec souveraineté.

De quoi parle-t-on ? Terme à la mode et souvent galvaudé, il convient d'en définir le périmètre. Selon Wikipédia, la souveraineté est : « *La qualité d'une organisation (en principe un état) de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'elle est appelée à réaliser* ».[1]

La ferveur de la digitalisation a amené une autre notion de souveraineté, la souveraineté numérique : « *la souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques* ».[2]

Si naturellement, cette notion s'applique à l'Etat et ses infrastructures, le principe est tout à fait transposable à une entreprise ou un particulier qui vont également devoir se poser des questions sur la maitrise qu'ils souhaitent garder sur leurs systèmes ou sur leurs données critiques.

Une erreur serait de considérer la souveraineté numérique comme la solution miracle où il suffit d'investir à grands fonds dans des capacités de production indigènes et de créer une économie protégée. Il est au contraire important de décider consciemment ce que l'on souhaite maintenir sous forme de compétence indigène (indigène pour une entreprise revient à dire avec propre capacité de développement) et de nourrir cette capacité de production avec un réel marché. Pour les éléments ne pouvant être développés de manière indigène, il s'agit de mettre en place une sécurisation des fournisseurs en établissant les contrôles le long de la chaine d'approvisionnement :

- Sélection des fournisseurs, en vérifiant leur provenance, stratégie, capacité à fournir dans le long terme, même en cas de tension avec le pays en question ;
- Vérification technique, tests « à cœur ouvert » des systèmes, en favorisant une approche de logiciel ouvert (open source), afin de vérifier si les fonctionnalités demandées sont implémentées et si le système ne comporte pas de portes dérobées par exemple.

Force est de constater que, aujourd'hui encore, nombre d'entreprises et de services étatiques n'ont pas les moyens humains afin de faire ces contrôles. Quant à la sélection des fournisseurs, les processus d'achat (réglementations OMC aidant) ne tiennent que rarement compte de la notion de souveraineté !

Une menace contre notre souveraineté numérique : le CLOUD act américain ?

Le *Clarifying Lawful Overseas Use of Data* Act ou CLOUD Act (H.R. 4943) est une loi fédérale des États-Unis de 2018 sur la surveillance des données personnelles, notamment dans le Cloud.

Elle permet aux forces de l'ordre (fédérales ou locales, y compris municipales) de contraindre les fournisseurs de services américains, par mandat ou assignation, à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux Etats-Unis ou dans des pays étrangers. Cette loi permet notamment aux forces de l'ordre américaines d'obtenir les données personnelles d'un individu ou d'une entreprise sans que ceux-ci en soient informés, ni que son pays de résidence ne le soit, ni que le pays où sont stockées ces données ne le soit.

Une bataille judiciaire opposait depuis 2013 Microsoft et le gouvernement américain: en cause, un mandat de perquisition délivré par le gouvernement visant à obtenir le contenu d'un compte e-mail dont les données étaient conservées dans un des nombreux centres d'hébergement de Microsoft hors des Etats-Unis, en l'occurrence en Irlande.

La ratification très discrète du *Cloud Act* (Clarifying Lawful Overseas Use of Data Act) le 23 mars dernier rend l'exercice inutile et le vide de sa substance. Le texte était noyé dans le vote du budget de l'Etat. Celui-ci n'a pas été discuté. Le tour est joué. Désormais, les forces de police n'ont pas à se justifier (obtenir un mandat) pour obtenir des données, peu importe leur lieu de conservation.

Impact pour les autres pays....

Cette loi permet également au président de conclure des accords d'échange de données sans l'approbation du Congrès. Elle donnerait également aux Etats tiers la possibilité d'obtenir des données de leurs propres citoyens.

Les associations de défense des consommateurs craignent – à raison – que cela ne soit le théâtre d'abus, notamment de la part d'Etats étrangers ou de services de renseignement étrangers (ce à quoi certains seraient tentés de répondre: ils n'ont semble-t-il jusqu'ici pas eu besoin de cela). On craint également un renforcement de l'Etat contre le particulier et une atteinte supplémentaire au respect de la vie privée, donc (partiellement du moins) secrète

Les Etat-Unis vont ainsi, dès à présent, pouvoir aller chercher légalement les données détenues par les sociétés américaines, quel que soit l'endroit où ces données se trouvent dans le monde. On peut donc s'attendre à ce que les Etats-Unis en profitent pour faire de l'ingérence dans les affaires d'autres pays, et ouvrent la voie à ce que ces pays fassent de même.

1 https://fr.wikipedia.org/wiki/Souverainet%C3%A9

2 Pierre Bellanger, « Le président de Skyrock, » *Les Echos*, 30 août 2011.

Très pratique.... Il n'y a plus besoin d'envoyer des espions pour aller voler des disques de données dans nos banques par exemple.... Aujourd'hui, lorsque vous stockez vos données dans un cloud, elles sont répliquées à de nombreux endroits dans le monde sans contrôle.

Cela rend caduques les offres des grands fournisseurs américains dans des datacenters « locaux. »

Des solutions ?

Il s'agit de faire une bonne analyse de risque et de menaces lorsque l'on décide de sortir des données et des services dans un cloud. De ne laisser sortir que les données qu'on est prêt à montrer à ses concurrents et à des Etats tiers.

Il y a des moyens techniques : p.ex. ELCA développe des outils de sécurisation des données dans le CLOUD. De tels outils, développés dans un pays neutre comme la CH, en code « open source », donc le contenu du logiciel est complètement ouvert et disponible pour son utilisateur qui peut y faire les contrôles qu'il souhaite.

La solution ultime : rendons-nous indépendants du CLOUD public et créons un vrai CLOUD souverain en Suisse.

Les siècles passés ont vu naitre des projets ambitieux et stratégiques sur notre infrastructure stratégique, par exemple les traversées des Alpes. Dès aujourd'hui, le monde numérique devrait aussi être un lieu de projets stratégiques pour notre pays !

C. G.

A l'époque de ces radios VHF SE 412, un système de criptage venait se greffer par-dessus la radio émetrice et réceptrice. Aujourd'hui cependant, les radios intègrent les systèmes de cryptologie, à l'instar du système radio SE X35.