Impacts de la LPM chez les fournisseurs

La Loi de Programmation Militaire (LPM) n'a pas que des impacts chez les Opérateurs d'Importance Vitale (OIV), elle en a aussi chez leurs fournisseurs. Les systèmes acquis par les OIV, et intégrés dans le Système d'Information d'Importance Vitale (SIIV) se doivent de respecter la LPM. Cette qualification « LPM » impose aux fournisseurs d'intégrer au sein de leurs systèmes, mais aussi de leur entreprise de nouvelles activités. **Ces activités sont les suivantes :**

- Intégration de nouvelles technologies dans les systèmes
- Eprouver la sécurité des systèmes
- Intégrer de la sécurité dans les projets
- Effectuer de la veille sécuritaire (Maintien en Conditions de Sécurité)
- Assurer l'intégrité des livraisons
- Maintenir le versionning du système

Les contrats entre les OIV et leurs fournisseurs évolueront pour intégrer ces points.

Intégration de nouvelles technologies

Pour obtenir la qualification « LPM », un système doit intégrer désormais les fonctions suivantes :

- Identification / Authentification nominative
- Gestion de profils et de droits (RBAC)
- Remontée d'événements de sécurité
- Supervision
- Durcissement

Certains systèmes sont basés, au moins en partie, sur des équipements électroniques ; par exemple les équipements qui composent un réseau de télécommunication mobile, ou une solution de pilotage d'un réseau électrique. Il n'est plus rare de voir que certains constructeurs n'hésitent pas à mettre en avant les avantages « cyber » de ces équipements. Ces équipements embarquent alors les technologies suivantes :

- SNMP pour la supervision de l'équipement. Le protocole SNMP V3 sera préféré au SNMP V 2c. La version 3 embarque des options de sécurité très intéressantes comme :
- Une identification et une authentification
- Du contrôle d'intégrité. Il est dommage que le protocole de calcul d'intégrité retenu par le groupe de travail ne soit pas SHA-256.
- Du chiffrement

  Bien que la partie Request (requête initiée par la console de supervision vers l'équipement), et la partie Trap (Information envoyée par l'équipement vers la console de supervision suite à un franchissement de seuil) soient définies dans la Version 3 du protocole SNMP, aucun système que j'ai pu croiser n'a implémenté le protocole SNMP V3 pour la partie trap. La partie trap repose alors sur la version 2c.

  Le SNMP V2c n'embarque qu'une seule propriété de sécurité : La communauté.

  Le SNMP V1 est à bannir, la version de ce protocole n'étant pas du tout sécurisé.

  Bon à savoir, le protocole SNMP embarque des fonctions de téléchargement de configuration.

- Syslog pour la remontée des événements de sécurité vers le collecteur central
- Du NTP pour la gestion du temps. Le successeur du protocole NTP sera le NTS. Il deviendra le standard une fois disponible.

- Radius pour l'Identification / Authentification nominative. L'équipement peut alors dialoguer avec un annuaire X500 (type Active Directory), soit directement avec l'annuaire, soit via un Proxy Radius. Le Proxy Radius se révèle être efficace dans les cas suivants :
- Je cherche à protéger mon équipement. Je le localise dans la zone privée. La zone privée ne peut pas communiquer directement avec la zone publique. La communication ne peut se faire qu'à travers un équipement de la Zone Démilitarisée (DMZ). Le Proxy Radius, hébergé en DMZ, effectue une rupture protocolaire. (Cf. schéma 1).
- Mon équipement sait dialoguer en Radius, mais mon annuaire X500 ne dialogue qu'en Kerberos (par exemple). Le Proxy Radius sert alors de passerelle (Cf. schéma 2).

Radius embarque aussi la gestion de profils (RBAC), les droits étant gérés directement dans l'équipement.

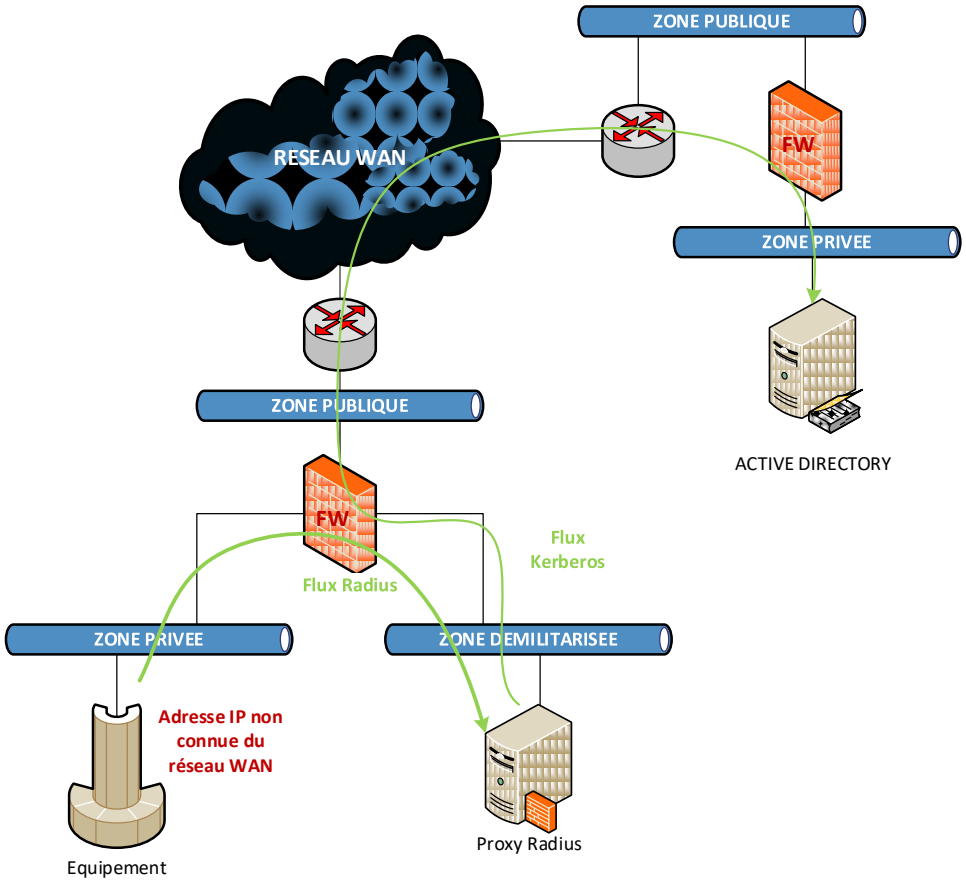

Schéma 1.

Schéma 2.

Eprouver la sécurité des systèmes

L'intégration des technologies de sécurité dans les systèmes ne suffit pas. Les systèmes devront être éprouvés en matière de sécurité en passant des tests comme celui de pénétration (pentest), d'injection de données erronées. Le code devra aussi être audité.

Les fournisseurs vont devoir s'équiper de laboratoires, de plateformes où leurs systèmes subiront les attaques connues à ce jour. L'outil Kali (Open Source), une référence en la matière semble incontournable. L'outil Nessus (Editeur et payant) semble être un complément voir une alternative.

Le pentest interne, ainsi que l'injection de données erronées, ou toutes actions visant à déstabiliser le système, permet de s'assurer d'un certain niveau de robustesse face aux cyber-attaques. Cependant on ne peut pas être juge et partie. Un auditeur externe apportera l'accréditation de ce niveau de sécurité.

Une Certification ANSSII peut-être un atout commercial pour certains systèmes, voire un pré-requis dans certains cas.

Intégrer la sécurité dans les projets

Lorsque l'on travaille sur la conception, le développement, et la mise au point d'un SIV, la discrétion est de mise. L'entreprise devra se remettre en question pour intégrer de la sécurité autour de ses projets. Elle se posera les questions suivantes (liste non exhaustive) :

- **Combien de niveaux de sécurité dois-je définir ?**

  Le niveau de sécurité doit être différent suivant que le projet adresse un niveau « Confidentiel Défense » ou « Secret Défense », d'un niveau « 1er niveau de sécurité.

- **Quelle sécurité périmétrique physique dois-je mettre en place ?**

  En raison du niveau de sensibilité, certains projets devront se dérouler dans des lieux clos à accès contrôlés.

- **Que dois-je vérifier lors du recrutement des membres de l'équipe sur ce projet ?**

  Si le projet a un niveau Secret-Défense, les personnes travaillant sur ce projet devront être habilitées en conséquence.

- **Dois-je avoir un Système d'Information Projet distinct ? Où vais-je stocker les documents, les livrables produits ? Quelle sécurité dois-je leur apporter ?**

  Un projet produit bon nombre de documents. Outre les documents projets (Planning, Suivi des actions, Outil de gestion des risques, Suivi budgétaire, Compte rendu de réunion), d'autres documents propres au projet sont produits. La fuite de certains de ces documents peuvent entrainer un risque sur le projet où le système. Il convient donc de leur apporter une sécurité adaptée, tant sur le support de stockage, que leurs accès, et leurs sauvegardes.

- **Comment vais-je communiquer avec mon client ? Avec quel niveau de sécurité ?**

  N'oublions pas que l'Internet est écouté. L'échange de documents, d'informations sensibles s'effectuera à travers des conteneurs sécurisés (comme des 7z sécurisés avec RSA 256, ou le produit Zed).

Toutes les réponses à ces questions seront décrites dans un document qui se nomme le PASI (Plan d'Assurance Sécurité Informatique). Ce document est un document contractuel que doivent exiger tous les clients, pas uniquement les OIV, qui mettent entre les mains de tiers le développement de systèmes sensibles.

Effectuer de la veille sécuritaire

Le fournisseur devra opérer sur son système une Maintenance en Condition de Sécurité (MCS). Cette activité garantit à l'utilisateur que le fournisseur veille à la détection des vulnérabilités, et à leur

remédiation. Pour cela, il devra s'abonner à des Computer Emergency Response Team (CERT). Il devra aussi produire son propre CERT ou au moins un portail, où il publiera des propres bulletins de sécurités liés à ses systèmes.

Si ses produits sont intégrés dans des SIIV chez des OIV, il a une obligation légale de s'abonner au CERT de l'ANSII (https://www.cert.ssi.gouv.fr/).

C'est une nouvelle activité pour les fournisseurs, impliquant la création d'un département, ou d'un service dédié à cette activité. Ce département pourra prendre en charge les activités pentesting, et de MCS. Inclure dans ce département un gentil hacker (White Hat) est judicieux.

Assurer l'intégrité des livraisons

A travers ces quelques mots, « *préalablement à l'installation de toute nouvelle version, l'opérateur s'assure de l'origine de cette version et de son intégrité* », la règle N° 4 de la Loi de Programmation Militaire impose désormais un contrôle d'intégrité de tout ce qui va être intégrer au système, que ce soient des nouvelles versions ou des correctifs, (Software or firmware).

Tant pour le fournisseur, que pour l'OIV, de nouvelles tâches sont à ajouter en amont et en aval de la livraison.

Maintenir le versionning du système

Toujours au sein de la règle N° 4, « Maintien en condition de sécurité », celle-ci impose que « *l'opérateur installe et maintienne toutes les ressources matérielles et logicielles de ses SIIV dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité* ». Cette règle est impactante pour les fournisseurs.

Jusqu'à la LPM, les fournisseurs bâtissaient des solutions, et les maintenaient dans les versions de leur création. Il n'est pas rare de croiser dans des sites industriels des systèmes dont les technologies n'ont pas évolué depuis 20 ans. La durée de vie d'un système industriel peut aller jusqu'à 25 ans de ma connaissance.

Tout système en exploitation qui n'est pas dans des technologies supportées par leurs éditeurs subit la sentence du bastion. Leur niveau de vulnérabilité est tel que la seule protection qui peut être mise en place est la réduction de la surface d'exposition. Adieu donc les Windows 95, Windows 98, Windows XP, Windows NT, Windows Server 2008; ou les vielles version de Linux comme Red Hat Hurricane, Appolo, Hedwig.

Pour qu'un système conserve son homologation LPM, il devra reposer sur les dernières versions des technologies, ou les avant-dernières.

Ainsi une nouvelle activité vient d'apparaitre chez les fournisseurs, celle du portage. Les applications devront être portées de versions en versions, puis testées, puis recettées, au moins les tests de non régression. Pour les utilisateurs finaux, cela engendre des compagnes de déploiements régulières.

Certaines entreprises ont bien compris que la cybersécurité devient un enjeu majeur pour leurs clients, et que ce sujet prend de plus en plus d'importance. Bon nombre d'entre-elles ont entrepris un programme de transformation pour répondre à ce besoin.

Liens :

https://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Version_3
https://www.itsgroup.com/fr/actualites/avis-dexpert-la-securite-du-temps-informatique
https://fr.wikipedia.org/wiki/Kali
https://www.kali.org/
https://fr.wikipedia.org/wiki/Nessus_(logiciel)
https://fr.wikipedia.org/wiki/Red_Hat_Linux