# Conférence Cybersécurité du G9+

**Notes de Marie-Anne Chabin et Aurélien Conraux pour le CR2PA**

**http://www.g9plus.org/manifestation/610**
Maison des Arts et métiers, lundi 6 juin à 18h30-20h30

Face à des menaces de plus en plus importantes et hétérogènes, les Entreprises se mobilisent, les fournisseurs de solutions et de services cherchent à innover et à répondre à des besoins toujours plus diversifiés et souvent plus globaux…
La conférence G9+/Sopra Steria vise à présenter des retours d'expérience et témoignages récents, illustrant la diversité des menaces et des stratégies, ainsi qu'un panorama de nouvelles solutions innovantes et de domaines d'investissements pour le futur.

Environ 120 participants, dont une majorité de RSSI, mais aussi des universitaires et records managers.

## Présentation Jean-François Perret et Florent Halbot

### Introduction : Luc Bretones, Président Institut G9+

Les risques sont aujourd'hui bien identifiés

- Attaque externe
- Défaillance humaine involontaire
- Défaillance externe
- Défaillance humaine volontaire

Il y a toutefois un décalage entre la vision des dirigeants et la réalité ; 86% disent qu'une défaillance (humaine (interne ou externe, volontaire ou non) ou technique) pourrait menacer la vie de l'entreprise mais ils n'agissent pas en conséquence.

La menace à venir : le déferlement des objets connectés ; ils sont vus aujourd'hui comme des gadgets mais ils seront demain au cœur de la santé, de la banque, des transports, de l'assurance. Or, ils sont très faciles à hacker, ne disposent souvent pas des dernières versions des logiciels, etc. : ils sont déjà au cœur de réseaux de botnets, mais demain seront au cœur d'attaques de grande ampleur.

Annonces :

- Livre « 2017 : 100 idées pour une France numérique »
- The digital transformation manager : 1er juillet à VIVATECH
- 4 octobre 2016 prix du Hub Forum Start up et Scale up innovantes

Associatif :

- Présentation par Nacira Salvan du Cefcys, le Cercle des femmes de la cybersécurité http://cefcys.com/ , pour promouvoir la diversité dans le monde de la sécurité informatique. Association en création, plus jeune que Duchess France (Women in Tech http://www.duchess-france.org/ ) et plus spécialisée.

### Guillaume Poupard, Directeur de l'ANSSI

La prise de conscience progresse mais il faut aider les entreprises à sécuriser leurs données.
3 messages de l'ANSSI :

1/ La menace est réelle et multiforme. Il y a de nombreuses cibles et de nombreux types d'attaque, du petit vol à la destruction du système vital de la nation : escroquerie, revendications, guerre de destruction, pillage discret de données et renseignements commerciaux, stratégiques peuvent être des objectifs. Ce peut être de petits graffitis numériques mais avec de gros dégâts à la clé s'ils sont visibles de la planète.

Les attaques sont souvent discrètes, l'attaquant fait tout pour être discret le plus longtemps possible : ne pas constater d'anomalie visible dans son système n'est donc en aucun cas une garantie sécurité effective.
L'objectif d'un certain nombre d'assaillants souvent de piller les données, les boîtes mails des dirigeants (il n'est pas si difficile d'accéder même aux smartphones quand les réseaux sont corrompus ; des données techniques (fabrication), commerciales (réponse appel d'offre), financières (ex : annonces boursières, délit d'initié), etc. Mais l'attaquant n'est pas infaillible. Il faut faire l'effort de le repérer. Quand on détecte les attaques, on voit que souvent (grâce aux logs) que l'attaquant est rentré dans le système d'information depuis plusieurs mois.
Des attaques comme le sabotage de TV5 augmenteront. Les gens disent : « je ne suis pas une cible, personne ne m'en veut ». Mais si TV5 a été attaqué, tout le monde peut être visé ; quelle entreprise n'a pas de données sensibles (données des collaborateurs a minima) ?
La pire attaque serait à des fins terroristes. Nier la menace est grave.

2/ Une fois qu'on a pris conscience de cette menace, il faut se protéger. Ce n'est pas facile, et c'est coûteux. Il y a un impact sur collaborateurs dans leur ensemble ; tout le monde doit s'impliquer. La doctrine est de :

a) concevoir les systèmes en intégrant la cyber-sécurité ; avant, la sécurité était traitée après, pas à la conception ; ça ne marche plus ;
b) la menace étant humaine (vengeance...), l'entreprise n'est pas infaillible ; on communique avec l'extérieur ; l'entreprise a les portes et fenêtres ouvertes… ; il faut pouvoir détecter et réagir dans l'heure ou dans la journée (l'attaquant de TV5 était là depuis 2 mois….) ; prévention et détection se complètent
c) les PDG veulent de la sécurité sans payer trop cher… ; mais si l'exemple ne vient pas d'en haut, on pourra difficilement l'imposer aux autres.

Il faut aller plus loin. Les impacts sont si grands que le conseil ne suffit pas ; il faut imposer certaines mesures, tant pour l'administration publique que pour certains opérateurs publiques sensibles. Cf la loi de programmation militaire de 2013 (OIV : organisation importance vitale). Quand un attaquant est détecté, voir s'il n'y a pas le même problème ailleurs. Partager les traces des attaques permet à chacun de vérifier si un système sain en apparence a été testé ou même infiltré, avant l'exploitation des failles. Instaurer des contrôles est de plus en plus nécessaire. En cas de crise majeure, consignes gouvernementales strictes pour éviter la contagion. La démarche française est efficace, en avance par rapport aux alliés. Elle repose toutefois en partie sur des arrêtés d'application en cours de signature.

3/ Les questions de cyber-sécurité n'ont de sens que si les acteurs travaillent ensemble ; il faut être capable de travailler avec les victimes potentielles ; on a donc besoin d'une industrie forte, de professionnels pour des produits efficaces et de confiance, mais aussi de services et de prestataires efficaces : les boîtes noires ne font pas tout. Comment choisir un prestataire de cloud ? Le plus cher n'est pas une garantie, le plus sympa non plus… C'est pourquoi on a une démarche de qualification. Rôle de l'État établir des listes blanches ; éviter de perdre du temps dans discussion. C'est à ce prix que l'ANSSI peut apporter une garantie.

Les points clés sont donc :

- **PREVENIR**. La protection n'est pas « facile », certainement pas sans coût ni impact. Pas uniquement quelques experts, mais tout le monde. Il ne sert à rien d'être seulement réactif, mieux vaut développer la Protection *by design*.
- **DETECTER, REAGIR.** Des failles vont exister car les systèmes ne sont pas clos : les outils de communication, les personnes même dans la forteresse sont autant de points de vulnérabilité potentiels. Il faut savoir détecter et réagir
- **SENSIBILISER**. Ex. du PDG qui veut imposer la sécurité, mais s'affranchit lui-même des contraintes que cela peut impliquer en termes d'outils ou de comportement. Il faut expliquer les contraintes et leurs motivations.

En réponse à une question de la salle sur l'open-source, il s'agit de considérer le concept global de l'IT d'une société, pas le statut du code de telle ou telle application, qui n'est souvent ni une garantie de qualité ni au contraire de fragilité par rapport à des cyber-attaques.

### Table Ronde : Retours d'expérience animée par Florence Puybareau , journaliste indépendante

- Olivier Vallet , CEO Solutions et CyberSécurité SopraSteria
- Frédéric Valette, responsable du Pôle SSI de la DGA
- Yves Bigot , Directeur général TV5Monde
- Thierry Olivier, RSSI Société Générale
- Gil Delille, directeur SSI Groupe Credit Agricole

**Olivier Vallet, CEO Solutions et CyberSecurité SopraSteria**
+ 51% d'attaques par an
Il y a une vraie prise de conscience ; la cyber-sécurité devient un sujet de Comex voire de Conseil de surveillance, mais ce n'est pas suffisant.
Il faut accepter le coût et sanctuariser les budgets.
Un problème : le nombre de personnes compétentes correspond à 25% des besoins, manque 75% de professionnels compétents.

**Frédéric Valette**, responsable du Pôle SSI de la **DGA**
Plaide pour la *security by design*, dès la table à dessin : prévoir les attaques d'interception, créer des réseaux robustes en interne, avec des verrous dans l'architecture pour limiter une propagation d'atteinte. Les systèmes sont forcément interconnectés, on demande aujourd'hui des architectures ouvertes mais maîtrisées…
Le hacking a remplacé l'écoute des transmissions.
Tout que ce qui rentre et sort d'Internet doit être contrôlé.
Exemple : risque d'attaque d'un bateau en mer ; il y a un accès Internet pour que les marins consultent leurs mails ou des AIS (échange entre bateaux). Au cas où on ne peut éviter l'intrusion, il faut empêcher qu'il y ait propagation dans le reste du système.
C'est une question d'anticipation (estimer le niveau de la menace). Or, les attaques sont toujours plus évoluées et la menace s'accélère. Exemple d'un piratage de système de gestion de conteneurs qui aurait pu déboucher sur une prise de contrôle du navire.
Si l'attaquant met les moyens, il peut y arriver ; il faut donc réagir.

**Yves Bigot, Directeur général TV5Monde**
Récit de l'attaque :
8 avril 2015, jour de Conseil d'administration et le même jour, on lance une nouvelle chaîne. Tout le monde est là (ministres, 200 journalistes…).
Lors du dîner : alertes : les 12 chaînes présentent en écran noir (« par terre »), avec un message au nom du « cybercalifat » qui se revendique de l'EI.

TV5 appelle le ministère de l'Intérieur qui contacte l'ANSSI.
À 5h du matin, on a pu restaurer un programme unique sur toutes les chaînes. À 11h, restauration des chaînes. À 18h : on reprend la production (le JT francophone).
On a compris plus tard ce qui c'était passé mais le plus urgent était de reprendre l'activité ; une entreprise peut arrêter et redémarrer 3 mois plus tard ; une télé ne peut pas, c'est une question d'heures.
On avait un système de protection mais insuffisant (qualifié de moyen par l'Anssi).
Pendant un mois, on ressort les fax et les crayons ; on travaille sans mails, sans Skype, avec îlots pour se connecter, en faisant très attention de ne raccorder les téléphones ou ordi à aucune machine et beaucoup de problèmes pendant 6 mois.
Pour le coût de l'attaque, on paie encore. En 2015 : 4,7€ et 3,9 en 2016, etc. ; 3,5 M€ en vitesse de croisière. Et le coût n'est pas que financier. La souffrance du personnel est importante car il y a un retour à un fonctionnement normal qui n'est pas une route linéaire : le déploiement d'une infrastructure plus sécurisée en doublon du fonctionnement courant 24/24 s'accompagne d'arrêts temporaires de réseaux, de régression de fonctionnalités, etc. qui génèrent un stress important.
Conclusion : nous avons été sauvés par miracle : les équipes DSIT étaient restées à cause du lancement de la nouvelle chaîne. La déconnexion d'Internet a permis d'interrompre l'attaque. 4 à 5 h plus tard, il ne serait rien resté (nous avons 32 ans d'archives…)
L'attaque était destinée à nous détruire, pas à voler des données. On était assuré pour la destruction physique de matériel et pour le vol de données (cf Sony) avec class actions (2-3 milliards de $ à la clé) mais pas pour ce type d'attaque. J'ai trouvé un assureur français pour construire quelque chose.

**Thierry Olivier, RSSI Société Générale**
Il y a des gens malveillants qui ont compris que l'argent n'est plus dans les coffres forts mais dans les systèmes d'information. Les hackeurs se professionnalisent : la récupération d'information permettant de préparer des accès non autorisés et leur exploitation sont séparés. Le hacking est plus lucratif que le trafic de drogue, et on fait ça tranquille depuis chez soi, sans arme, et vu la possibilité de se couvrir par des rebonds internationaux, souvent en toute impunité. Il y a des spécialisations en fonction de la revente des données.
On peut remonter certaines étapes de l'attaque mais en cas de rebond, on perd la trace. Il peut devenir plus intéressant pour des experts techniques d'analyser les méthodes en laissant rentrer un peu, ou dans un système factice, pour voir les méthodes et saturer de fausses informations…
Il y a aussi les tentatives pour entrer par des moyens légitimes (ex : par le compte de collaborateurs qui accédaient à SWIFT).
On sensibilise les collaborateurs contre la fraude au président ou le *phishing*, mais le nombre de clics sur les spams (vous avez gagné…) est impressionnant…
La centralisation des données autant que possible dans des zones géographiques sûres est importantes, elle permet de couper les flux si nécessaire.

**Gil Delille, directeur SSI Groupe Crédit Agricole**
Questions financières et humaines. L'achat adéquat de solutions est un point important dans la qualité des SI.
Il faut aussi revoir la question des compétences : quand on recherche un administrateur de base de données, on lui demande un esprit de synthèse, pas de connaître la sécurité…
Quel dirigeant a déjà donné un objectif de sécurité à un directeur informatique ? Aujourd'hui, trop souvent la sécurité n'est pas dans les fiches de postes IT
Il y a une transformation profonde à opérer dans l'entreprise : c'est une course face aux attaquants.
Il faut recruter des ingénieurs mais les plus compétents veulent aller travailler chez Google… Autrement dit l'un des axes de développement est la reconversion ou la montée en compétence des IT existants.
Autre problème : vous êtes sécurisé mais votre prestataire ne l'est pas…. (ex : Airbus où 60% de la *supply chain* est externalisée).
Recruter des hackeurs éthiques.
La sensibilisation commence à l'école maternelle. Constituer des équipes SSI d'élite c'est bien, mais il faut faire bouger le système entier.

On sait que le risque ne peut être nul, mais on peut retarder l'incident, en limiter l'ampleur et accélérer la remédiation.
Il commence à exister quelques assurances américaines contre la destruction physique de matériel ou le vol de données, mais l'impact d'image ou le traumatisme humain est important, on l'a vu pour TV5.

### Table Ronde : Solutions du Futur, animée par Laurent Charreyron , Directeur Cybersécurité CXP Group

- Jérôme Chappe , Directeur Général The Greenbow
- Jacques Sebag , CEO Deny All
- Fabien Lecoq , CTO Cybersécurité SopraSteria
- Christophe Pagézy CEO Prove and Run
- Jacques Pantin , Fondateur Dictao

**Laurent Charreyron, Directeur Cyber Sécurité CXP Group**
L'industrie de la cyber-sécurité se développe (2,5 milliards d'€).
Il s'agit plus de comportements (hygiène) que de questions d'infrastructure : sécurité des identités, de la traçabilité, de la compliance. Sortir du cliché « la cyber-sécurité, c'est un truc de techniciens ».

Nous avons une grande technicité en France, avec un vivier d'entreprises d'excellence mondiale ; on ne peut dépendre de la technologie américaine.
Cf le concept d'homéostasie (système du corps humain pour survie en milieu hostile) ; il nous faut un système immunitaire.
Difficile d'imposer la sécurité, d'empêcher les gens de cliquer sur un *phishing* ; il faut inclure la cyber-sécurité dans les systèmes, développer la Security by design.

**Jérôme Chappe, Directeur Général The Greenbow**
Il faut masquer la sécurité pour l'imposer discrètement. La contrainte peut marcher dans un environnement militaire, mais pas quand c'est tout le monde qui est concerné. C'est impossible de demander un mot de passe à chaque geste ; ce sera contourné.
Il faut « enfouir la sécurité »,.

**Jacques Sebag, CEO Deny All**
Une partie de l'informatique est à l'extérieur ; nos solutions détectent et bloquent les failles (une adresse Ip inhabituelle, plusieurs connexions proches dans lieux différents…).
Le budget de la cyber-sécurité est de 12% du budget informatique en Corée et Israël ; ailleurs, c'est 2-3%...
Importance de la double vérification via l'envoi d'un SMS lors d'un virement (pour authentifier).
Il faut retrouver le trouver le bon équilibre entre le produit de sécurité et son utilisation, anticiper les comportements de l'utilisateur pour accroître la difficulté d'une utilisation de mot de passe frauduleuse.

**Fabien Lecoq, CTO CyberSecurity SopraSteria**
Il faut accompagner la montée en compétence des collaborateurs, des clients….
On peut s'appuyer sur une approche « intelligence artificielle » avec la classification des données, des algorithmes pour identifier des comportements déviants. Par contre la surface d'attaque des entreprises s'est nettement étendue : géographiquement, techniquement, humainement (nb et accès collaboratif)…
Existe maintenant la solution de souscription à des systèmes extérieurs : entreprises spécialisées dans le management des pare-feux applicatifs. Le Cloud Access Security Brokerage devient un nouvel objectif de l'infogérance, qui loue de la puissance machine et se concentre sur la sécurité.

Le Shadow IT, pour lancer des outils à des coûts faibles et avec une technologie raisonnable, est une réalité qui comporte des risques.

**Christophe Pagézy CEO Prove and Run**

Les objets connectés sont liés aux systèmes embarqués (voitures, avions, systèmes d'énergie….). Toutes les voitures sont hackables.

Les hackers raisonnent de façon économique : l'investissement initial est lourd, mais réutilisable. Le hackeur cherche la défaillance des systèmes opératoires ; le bug est la matière première du hackeur, or la sécurité de plate-forme est aujourd'hui sans espoir à partir de systèmes complexes comme les smartphones. Il faut des systèmes d'exploitation (OS) plus résistants, voire formellement prouvés, c'est le stade ultime de la sécurité *by design*, ou du moins on augmente de plusieurs ordres de grandeur la difficulté de l'attaque. L'homme est encore le maillon faible, d'où l'importance de la biométrie. Le comportemental est un point essentiel : banques, réseaux sociaux aussi. Le reste doit suivre. L'intervention après coup ne marche plus.

**Jacques Pantin , Fondateur Dictao**

Le monde est rentré dans une phase mobile ; tout sera dans le mobile.

Avec le risque d'usurpation d'identité.

La réponse est dans le comportemental. Les réseaux sociaux investissent là-dessus. On a déjà des algorithmes pour voir les comportements déviants.

Tous les systèmes sont dans le cloud ; il faut s'assurer que les données ne sont pas exploitables par d'autres (pare-feu applicatifs en amont, nouveau métier CAS pour *cloud access security*, etc.).

Le problème n'est pas technologique : sensibilisation > prise de conscience > passage à l'acte (décision de DG). C'est comme une assurance : acheter porte blindée avant ou après cambriolage ?

**Laurent Charreyron**

La cyber-sécurité comme facilitateur du business plutôt que comme remédiation.

Pour les utilisateurs, la sécurité n'est pas un bénéfice, mais c'est un des éléments qui permettent la confiance (et pour cela, il peut être utile d'avoir un service fourni par une marque reconnue). Avec la blockchain, le réseau est lui-même le tiers de confiance, hors des acteurs étatiques ou établis. Quelle que soit la technologie, il faut de toute façon un tiers certificateur de la qualité des intervenants.

### Conclusion par Laurent Giovachini, Directeur Général Délégué SopraSteria

La prise de conscience est insuffisante, car la question est trop complexe.

Un décideur préfère nier un risque qu'il comprend mal.

Il est aujourd'hui plus facile d'attaquer que de se défendre.