harmonie technologie

8eme FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ

DATA SECURITY & PRIVACY

25 & 26 JANVIER 2016 | LILLE GRAND PALAIS

LIVRE BLANC

EXTERNALISATION DES DONNÉES, PANORAMA DE MENACES ET ORIENTATIONS 2016

Réalisé par Harmonie Technologie

En partenariat avec ARXAN oodrive Trusted Cloud Solutions

Pour la 8ème édition du Forum International de la Cybersécurité (FIC) dont le thème est Data Security & Privacy, Harmonie Technologie a choisi d'animer une table ronde sur les menaces et les orientations liées à l'externalisation des données des systèmes d'information. Rassemblant des acteurs de référence dans ce domaine : régulateurs, éditeurs/offreurs de services et responsables de la sécurité du SI de grands comptes, cette table ronde a été l'occasion de mettre en perspective cette problématique à travers des points de vue complémentaires.

Dans la continuité de cette prise de parole, ce livre blanc a pour objectif de compléter les échanges de la table ronde résumés en 1ère partie avec des éclairages sur les solutions de sécurité actuelles.

FIC Forum International de la Cybersécurité

Le Forum International de la Cybersécurité (FIC) est un salon annuel organisé conjointement par la Région Hauts-de-France, la Gendarmerie nationale et la société de conseil CEIS. Il s'inscrit dans une démarche de réflexions et d'échanges visant à promouvoir une vision européenne de la cybersécurité. Avec la participation de 5450 visiteurs, 240 exposants et 250 intervenants en 2016, le FIC est devenu l'évènement européen de référence réunissant l'ensemble des acteurs de la confiance numérique.

Plus d'infos sur www.forum-fic.com

EDITO

Pour les entreprises, l'externalisation des données se matérialise par :
- l'extension de leurs SI à des services tiers offerts par des spécialistes d'applications métiers (ERP, CRM, etc.) et de sécurité (antivirus, log management, confiance numérique, etc.) ;
- la multiplication des applications mobiles permettant d'accéder à ces nouveaux services comme à ceux mis en œuvre au sein des entreprises.

Ce nouveau paradigme de l'externalisation intervient dans un contexte complexe pour les entreprises, confrontées simultanément à une augmentation exponentielle du volume de données, à un renforcement des réglementations et à une multiplication des cyberattaques.
Face à ce constat, il est nécessaire d'adapter les plans d'investissement pour absorber ce changement en répondant aux enjeux des informations externalisées.
Pour y arriver, il s'agit d'identifier, de la manière la plus objective possible, les opportunités et les menaces liées à l'externalisation des données pour conduire des projets.

Dans ce contexte, les équipes sécurité ont un rôle majeur à jouer vis-à-vis des décideurs. Au-delà de la mise en exergue des risques associés aux nouveaux services (localisation géographique des données, capacité à respecter les exigences des régulateurs, etc.), ils doivent pouvoir mettre en avant les apports de ces services pour encadrer les nouveaux usages de manière sécurisée.

Le présent livre blanc synthétise les échanges avec les représentants de l'ANSSI, de Crédit Agricole, de Natixis, d'Oodrive et d'Arxan lors de cette 8ème édition du FIC. Il aspire également à approfondir la thématique à travers des avis d'experts pour permettre aux lecteurs de disposer d'une vision à date des possibilités de cohabitation de la sécurité et de l'externalisation des données.

Christophe Guéguen,
Responsable de la practice Data & Cyber Security
Harmonie Technologie

SOMMAIRE

PARTIE 1

RESTITUTION DE LA TABLE RONDE

EXTERNALISATION DES DONNÉES, PANORAMA DE MENACES ET ORIENTATIONS 2016

Quels sont les risques associés au Cloud et à la Mobilité ? Quelles opportunités métier et sécurité représentent-ils ? Quelles solutions déployer pour recourir à l'externalisation en confiance ? Invités par Harmonie Technologie dans le cadre du Forum International de la Cybersécurité (FIC) 2016, plusieurs experts – régulateurs, offreurs de services et Responsables de la Sécurité du SI de grands groupes – ont proposé un panorama des menaces et des orientations 2016 de l'externalisation des données.

EXTERNALISATION DES DONNÉES : QUELLES MENACES ?

L'externalisation des services et des données dans le Cloud est une réalité pour les entreprises qui souhaitent se concentrer sur leur coeur de métier et étendre les usages mobiles. Ce changement fait apparaitre une maturité hétérogène de l'écosystème en termes de maîtrise des risques et présente des risques potentiels qu'il est impératif de connaître, d'anticiper et de mieux maîtriser. Les experts invités à la table ronde d'Harmonie Technologie en dressent un premier tour d'horizon.

A quelles menaces les entreprises font-elles face lorsqu'elles externalisent leurs données dans le Cloud ? *« Lorsque vous externalisez vos données sur l'infrastructure d'un tiers, en somme vous les transférez sur l'ordinateur d'un autre »* : cette remarque de Charles-Henri Schulz, chargé de mission à l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), pose bien le problème. Dans une telle configuration, certaines menaces relèvent purement de question de sécurité quand d'autres sont essentiellement une question de confiance dans le prestataire du service. Charles-Henri Schulz identifie ainsi une première série de problématiques :

- juridique : quelle législation s'applique aux données externalisées ?
- de sécurité physique : où est situé le data center ? comment est-il protégé ?
- de sécurité logicielle : quelles mesures sont prises par le prestataire ? quel chiffrement utilise-t-il ?

L'UTILISATEUR, UNE MENACE ?

Pour Federico Garcia, RSSI adjoint du Groupe Crédit Agricole, s'ajoute une autre source de menace potentielle : l'utilisateur et sa façon d'utiliser le Cloud. *« Les services Cloud sont de plus en plus simples à utiliser et échappent à la DSI. Or il faudrait en recadrer les usages, en les sécurisant »*. Une attention d'autant plus nécessaire que l'intensification de la réglementation contraint les entreprises à se professionnaliser encore davantage en matière de sécurité. *« Il faut mettre en place des processus plus stricts de détection, de réaction et de sécurisation, tout en permettant au business de se développer dans le même temps, en optimisant le recours aux solutions de type Cloud »*, estime-t-il.

> **« Il faut intégrer la sécurité le plus en amont possible du circuit. »**
>
> *Brice Hauser Kauffmann, Responsable solutions de sécurité de continuité de NATIXIS*

ANTICIPER ET VÉRIFIER

Alors comment anticiper ces menaces bien identifiées ? D'abord *« en intégrant la sécurité le plus en amont possible du circuit »*, indique Brice Hauser Kauffmann, Responsable solutions de sécurité et de continuité de Natixis. La contractualisation constitue selon lui un premier rempart à la menace, mais nécessite de bien sensibiliser les équipes achats des entreprises à la problématique. Pour plus d'efficacité, Brice Hauser Kauffmann juge lui aussi impératif de réaliser un inventaire des données non-structurées et de les classifier, *« c'est un chantier indispensable pour les années à venir »*.

ATTENTION À LA SÉCURITÉ DES APPLICATIONS

Comme le précise Olivier Acoulon, Manager Southern Europe chez Arxan, il ne faut pas négliger la protection des applications, notamment mobiles. *« A l'heure de l'Internet des Objets, elles sont partout et constituent une cible de choix pour les pirates. Avec des systèmes aussi sensibles que la HCE (Host Card Emulation) pour le paiement mobile, la gestion des droits numériques et la voiture connectée, les applications doivent être protégées »*. Or comme le regrette Brice Hauser Kauffmann *« seule une niche de développeurs ont la sécurité dans le sang, elle n'est pas une préoccupation pour beaucoup d'entre eux »*. Selon lui, l'une des solutions est la formation : *« Nous devons mettre en place des formations en sécurité pour les développeurs, et internaliser des compétences spécifiques »*. Les audits de sécurité démontrent bien trop souvent une absence de prise en compte de la notion de sécurité dans le développement, en particulier pour les applications mobiles. Les autres experts réunis confirment ce constat. Selon Olivier

Acoulon, *« il ne faut pas faire confiance car au-delà du fait que les développeurs ne sont pas des experts en sécurité, on ne peut pas contrôler tous les réseaux et tous les devices. C'est pourquoi la philosophie d'Arxan est de « sceller » le binaire des applications mobiles avant de les publier sur un portail, quel qu'il soit, de sorte qu'aucun hacker ne puisse venir les modifier ».*

> « A l'heure de l'Internet des Objets, les vulnérabilités sont partout et constituent une cible de choix pour les pirates. »
>
> *Olivier Acoulon, Manager Southern Europe, ARXAN TECHNOLOGIES*

LE CLOUD, SOLUTION DE SÉCURITÉ ?

Incontestablement, le Cloud est une opportunité business. Peut-il aussi être une opportunité pour la sécurité ? Federico Garcia et Edouard de Remur le pensent. Explications.

Oui, le Cloud peut être une solution de sécurisation de la donnée pour les entreprises. Edouard de Remur, Cofondateur d'OODRIVE, dont le métier est précisément de proposer des solutions de partage de fichiers dans le Cloud, expose le constat suivant : *« Nos clients ont deux contraintes, la simplicité et la sécurité. L'une des forces du Cloud est sa simplicité d'utilisation. Il y a 15 ans, pour qu'une solution soit sécurisée, les entreprises voulaient absolument la maîtriser en interne. Elles savent aujourd'hui que sécuriser des données coûte cher et se sont rendu compte que le Cloud permet aussi de mutualiser les coûts. Elles viennent donc nous voir pour trouver des solutions plus sécurisées que celles qu'elles pourraient elles-mêmes mettre en place ».* Particulièrement vrai pour les petites entreprises, l'argument vaut aussi pour les plus grandes, lorsqu'elles ne souhaitent pas partager certains documents sur les réseaux internes : *« Le Cloud permet d'offrir un niveau de sécurité supplémentaire pour des documents sensibles : définition de la stratégie commerciale, prise de décisions financières ou organisationnelles, suivi des investissements, gestion des crises, etc. ».*

DES POINTS DE VIGILANCE

Pour que le Cloud soit une opportunité de sécurité, Federico Garcia souligne pour sa part plusieurs points de vigilance. D'abord, rester en alerte constante : *« Une veille permanente est essentielle. Les offres de services évoluent très vite, il faut anticiper ».* Ce qui implique que les DSI, acteurs centraux en matière de sécurité, se modernisent, en assurant eux-mêmes cette veille permanente et soient force de proposition.
Ensuite, savoir mobiliser toutes les personnes concernées par la sécurité *« il faut sensibiliser les cibles (sociétés, maîtres d'ouvrage, lignes métier) et les embarquer le plus tôt possible »*, car eux aussi ont des devoirs en matière de sécurité. Il ajoute : *« il faut envisager que des mesures de sécurité puissent être à la main de l'utilisateur »*, c'est-à-dire de l'entreprise. Pouvoir chiffrer et anonymiser les données, gérer les identités, s'assurer que les données dans le Cloud sont bien sécurisées, etc. sont autant de besoins exprimés par les entreprises.

> « Le Cloud a mis en exergue que sécurité et simplicité n'étaient pas contradictoires. »
>
> *Edouard de Remur, Co-fondateur de OODRIVE*

> « Il faut envisager que les mesures de sécurité puissent être à la main de l'utilisateur. »
>
> *Federico Garcia, RSSI Adjoint du Groupe CREDIT AGRICOLE SA*

Enfin, muscler le juridique : *« il faut être exigeant sur le contrat et s'assurer que les clauses, de réversibilité, par exemple, pourront s'appliquer ».* Le sujet des contrats et des juridictions compétentes est un enjeu clé. *« Savoir quelle législation s'applique est en effet un véritable problème »* souligne Charles-Henri Schulz. *« L'ANSSI préconise que le droit du contrat régissant la relation entre le fournisseur de Cloud et son client soit d'une part un droit unique et d'autre part un droit européen. L'ANSSI préconise également que les fournisseurs soient transparents sur la localisation réelle des données ».* D'ailleurs, les big players (Amazon, Microsoft) se laissent-ils auditer pour que leurs clients puissent vérifier le respect des exigences et les mesures de sécurité en place ? *« Les grands acteurs comme Microsoft indiquent dédier du personnel à l'accueil de leurs clients dans leurs data centers.»* précise Brice Hauser Kauffmann. Federico Garcia ajoute *« Une part de lobbying reste à accomplir pour obtenir le respect de plus grandes exigences. Les entreprises ont intérêt à se regrouper pour cela, par exemple au sein du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) ».*

Conclusion, pour faire du Cloud une opportunité de sécurité, les mots clés sont veille et exigences contractuelles vis-à-vis des fournisseurs. Encore faut-il avoir affaire aux *« bons »* fournisseurs de solutions Cloud. Charles-Henri Schulz est rassurant sur ce point, tout au moins pour les éditeurs français : *« nous avons des acteurs d'excellence dans le Cloud en France, qui sont des acteurs de confiance et des spécialistes de la sécurité ».*

PEUT-ON FAIRE CONFIANCE ET COMMENT ?

Externaliser les données, oui, mais pas avec n'importe qui. Comment bien choisir son prestataire ? Comment lui faire confiance ? Une solution : la certification !

Comment permettre au marché et aux entreprises de juger de la confiance d'un service Cloud ? A cette question centrale dans le débat sur l'externalisation des données, l'ANSSI répond par l'élaboration d'un référentiel d'exigences à destination des prestataires de service Cloud, actuellement en cours d'expérimentation. Ces exigences, qui seront vérifiées via un audit du prestataire, couvrent la sécurité physique, la contractualisation, le chiffrement, le contrôle des accès, la gestion des identités, etc. *« Grâce à ce référentiel d'exigences », indique Charles-Henri Schulz, les entreprises seront en capacité de mieux juger de la qualité des acteurs du marché (…) pour l'ANSSI, c'est une réponse crédible à la question de la confiance ».*

> « Le référentiel d'exigences est une réponse crédible à la question de la confiance. »
>
> *Charles-Henri Schulz, Chargé de mission de l'ANSSI*

CERTIFIER POUR RASSURER LE CLIENT

Les prestataires et leurs clients sont favorables à l'émergence de référentiels et de certifications qui sont efficaces pour juger de la qualité d'un service. Pour Edouard de Remur, *« les certifications et référentiels ont une vraie valeur ajoutée, à la fois pour les éditeurs et pour les utilisateurs. Ils permettent d'inciter et d'aider les éditeurs Cloud à atteindre les bons standards en termes de sécurité d'une part, et de clarifier et simplifier la relation de confiance entre les éditeurs et leurs clients d'autre part. Chez Oodrive, nous préconisons une politique de certification, pour rassurer les clients et leur permettre de simplifier leur prise de décision ».* L'entreprise est certifiée RGS (Référentiel Général de Sécurité), Cloud Confidence, ISO 27001 : 2013, Label France CyberSecurity et joue le rôle de pilote pour la certification *« Secure Cloud Plus »* de l'ANSSI.

S'INFORMER ET CONTRÔLER

Federico Garcia soulève une limite à la démarche : *« la certification est une bonne voie, mais il faut en connaître la profondeur et les modalités. De plus, les offres Cloud évoluant très rapidement, un audit régulier reste nécessaire, au-delà de la certification ».* Il cite ainsi

l'exemple des Security Operating Center (SOC) : *« comment être certains qu'ils soient réellement efficaces contre de nouvelles attaques ? La certification le permettra-t-elle ? Une veille permanente est absolument nécessaire pour atteindre un niveau de sécurité satisfaisant pour une banque ».*

EXTERNALISATION & DONNÉES SENSIBLES ?

Des programmes de classification de l'information dite non structurée sont nécessaires. Les entreprises externalisent tous types de données, d'où l'importance de la classification. *« Bien que la contractualisation soit certainement le premier levier à utiliser, encore faut-il connaître ses données afin de savoir quelles sont les données à confiner dans le Cloud »,* souligne Brice Hauser Kauffmann. *« Dans ce cadre, des programmes de classification de l'information dite non-structurée (documents bureautiques) sont indispensables »,* ajoute-il. Ces programmes sont encore difficiles à mettre en oeuvre. Federico Garcia et Brice Hauser Kauffmann se rejoignent sur ce point : *« Ne vous lancez pas dans des classifications complexes, appuyez-vous sur des approches pragmatiques et dynamiques. Il ne faut pas oublier non plus la problématique du big data. Certaines données non sensibles prises individuellement le deviennent une fois agrégées ».* Enfin, Charles-Henri Schulz précise : *« la classification doit se faire chez le client et non chez le fournisseur de Cloud ».* Il ajoute : *« il faut aussi faire attention aux comportements : ne mettez pas vos informations ultra-sensibles et vos informations plus usuelles sur le même nuage ! ».*

PARTIE 2

AVIS D'EXPERT

Par Christophe Guéguen

Responsable de la practice Data & Cyber Security, Harmonie Technologie

EXTERNALISATION DES DONNÉES DANS LE CLOUD : PASSAGE INCONTOURNABLE DANS LE CADRE DE LA MUTATION VERS L'ENTREPRISE DIGITALE ET MOBILE

CLOUD & ENTREPRISE DIGITALE

Externalisation des données dans le Cloud, passage incontournable dans le cadre de la mutation vers l'entreprise digitale ?

Les avis sont partagés au sein des entreprises, des plus sceptiques qui essayent de freiner l'engouement, aux plus enthousiastes qui s'interrogent sur le comment nous avons pu faire sans. Sans aller dans un extrême ou un autre, peut-on réellement exposer ses données sensibles en toute confiance dans le Cloud ? Est-il possible de maitriser les risques vis-à-vis du patrimoine informationnel dans les environnements externalisés ? En cas de compromission des données, qui sont les responsables et quels sont les recours ?
Nombre de points clés auxquels il faut pouvoir répondre afin de mieux appréhender les enjeux de cette transformation. L'externalisation dans le Cloud est souvent perçue comme un moyen *« simple »* et *« rapide »* d'offrir des services en procédant à des économies d'échelle sur les budgets informatiques.

Pour les métiers, l'externalisation dans le Cloud permet :

- **Une plus grande agilité :** meilleure gestion de la capacité, meilleure évolutivité / adéquation des besoins, capacité accrue de disponibilité ;
- **Une meilleure accessibilité :** exposition d'applications métiers ou bureautiques sur Internet, accessibilité simplifiée pour des *« devices »* gérés ou non - BYOD ;
- **Une capacité à diminuer le CAPEX** pour se limiter à des coûts d'OPEX.

L'externalisation dans le Cloud est également perçue comme une plus grande exposition des données d'entreprise et de facto aux risques cyber associés.

Ce point de vue est légitime eu égard à la variété des services offerts, parmi lesquels il est possible de citer :

- La gestion déportée d'applications métiers historiques ou non (CRM, ERP, Support, Etc.) ;
- Le déport de la gestion de certaines fonctions de sécurité (Sécurisation de l'infrastructure Cloud, SIEM/SOC, Cert) ;
- La gestion des développements d'applications en cycle court, en particulier pour les applications mobiles.

ENJEUX DE L'EXTERNALISATION DES DONNÉES EN CONFIANCE

Comment concilier ces deux vérités et « s'engager » sur la route de l'externalisation dans le Cloud sans risquer de mettre en péril son patrimoine informationnel ?

Par nature, le Cloud étend le périmètre du SI et remet en question les principes de sécurité périmétriques, fondement historique de la sécurité des entreprises.
Sa mise en oeuvre nécessite donc de déterminer une stratégie d'externalisation en commençant par définir le périmètre à adresser : Quelles données ? Quelles applications ? Quels services ?

GESTION DES RISQUES

Cette stratégie doit être accompagnée d'une analyse de risques pour permettre aux décideurs de disposer des éléments pour juger si le niveau de risque est acceptable pour les informations concernées. Il s'agit bien de mesurer l'évolution des risques actuels dans ce nouveau contexte et de recenser les nouveaux risques spécifiques au Cloud.
La décision n'est pas à sous-estimer, car comme évoqué lors de la table ronde, externaliser ses données sur l'infrastructure d'un tiers revient à *« les transférer sur l'ordinateur d'un autre ».*

Cette image permet d'illustrer simplement la criticité du mandat confié aux différents prestataires de Cloud par les entreprises et les questions qu'elles doivent se poser :

- Quelle confiance peut-on / doit-on accorder aux prestataires choisis ?
- Est-ce que le prestataire sera en mesure de prévenir les risques et de réagir correctement le cas échéant ?
- Comment traduire les engagements d'une entreprise vis-à-vis des clients et des régulateurs (LPM, CNIL, PCI DSS, ISO 27001, BALE III, SOLVENCY II, etc.) dans les contrats ?
- Quelles sont les garanties associées et les clauses d'exclusion ?

- Qui est responsable en cas d'incident en général et de compromission des données en particulier ?
- Où sont stockées les données et quelles sont les juridictions compétentes ?
- Est-il possible de changer de fournisseur et dans quelles conditions ?

COMPROMISSION DES DONNÉES ET GESTION DE CRISE

Il convient de ne pas être naïf. Des compromissions peuvent arriver. Les derniers référentiels de conformité (LPM, PCI DSS pour ne citer qu'eux) rappellent ce risque et exigent le renforcement des moyens de détection des incidents de sécurité ainsi que la capacité de les traiter afin de s'inscrire dans une stratégie globale de cyber résilience.

La stratégie de sécurisation du Cloud doit donc également prévoir ce volet de gestion de crise cyber en s'assurant :

1. de la mise en oeuvre d'une organisation conjointe de traitement de la crise ;
2. de la capacité du fournisseur à détecter une compromission de données et à assurer cette organisation en cas de compromission de plusieurs autres clients.

Le choix des mécanismes de sécurité et leur niveau d'implémentation doit être en adéquation avec les enjeux des informations. Cela implique qu'à minima les données sensibles soient classifiées. Il est donc nécessaire de définir une stratégie en la matière avec dans la mesure du possible un outillage et une automatisation ne se basant pas uniquement sur les utilisateurs.

PROTECTION DES DONNÉES : ANONYMISATION, ACCÈS, ...

Dans ce cadre, la fonction du responsable sécurité évolue également. Le passage dans le Cloud l'oblige à se focaliser sur la donnée et les engagements de protection offerts par le fournisseur. Il doit également se positionner sur certains axes clés pour se prémunir des écueils auxquels il est confronté en interne.

- **Anonymisation / désensibilisation des données :** Tous les services externes ne nécessitent pas de disposer des données de production brutes. A titre d'exemple, il n'est généralement pas nécessaire d'exposer en dehors du SI les numéros de CB. Une partie du numéro est suffisant. De même, en cas d'externalisation des développements des applications mobiles, des données anonymisées sont suffisantes. L'expérience démontre qu'il en va de même pour de nombreux cas d'usage métier.
- **Gestion des permissions et des accès :** A l'instar des applications internes, il est nécessaire de s'assurer que les services Cloud bénéficient des mécanismes IAM de l'entreprise que ce soit en termes d'affectation / retrait des droits et de recertification. Les éditeurs de solution IAM l'ont bien compris et proposent pour la plupart la possibilité d'intégrer des services Cloud couvrant la Gouvernance des Identités et des Accès aux services (IAG) comme aux Données non-structurées (DAG).
- **Mise en place de DLP :** Confidentielles jusqu'à il y a peu, les initiatives autour des solutions de DLP se sont multipliées du fait de la multiplication des cas de fuites de données et de la mutation vers l'entreprise digitale. Les solutions ont atteint un niveau certain de maturité pour traiter les différents cas d'usage, en interne ou dans le Cloud. Les gestionnaires de ces solutions ont également appris à en tirer le meilleur profit pour :
  - Sensibiliser les utilisateurs et prévenir les fuites *« sans mauvaise intention »* ;
  - Bloquer les principaux canaux de fuites ;
  - Obliger les fraudeurs à utiliser des biais non traditionnels pour exfiltrer les données et ainsi pouvoir être repérés par les systèmes de détection comportementale.

Ces exemples et ceux partagés lors de la table ronde démontrent que des solutions existent et permettent de couvrir une partie des risques. Tous ces mécanismes doivent être agencés et mis en oeuvre dans le cadre d'une gouvernance adaptée et éprouvée qui seule permettra de limiter la survenance d'une compromission de données.

EN CONCLUSION

La mise en place de service Cloud avec externalisation des données pour accompagner le développement des entreprises peut évidemment être compatible avec la sécurité. Toutefois, elle impose de disposer d'une vision 360° de la sécurité et d'accepter une délégation de la gestion, notamment des composants d'infrastructure sous-jacents au service.

L'externalisation constitue une réelle opportunité de s'interroger sur les informations qui ont réellement de la valeur au sein de l'entreprise. L'exemple le plus probant est l'externalisation dans le Cloud de données non structurées. Elle pourrait être comparée à un *« déménagement »*, qui obligerait à ne conserver que les données réellement utilisées et archiver les autres.

Enfin, l'analyse de risques lors du choix du service doit s'interroger sur la capacité à ré-internaliser le service ou le transférer chez un autre opérateur. Deux questions de fond doivent se poser :

- **La réversibilité :** est-il possible de récupérer ses informations de manière exploitable ?
- **La destruction des informations :** quel est le niveau d'engagement du fournisseur du service quant à la suppression des informations une fois le service rompu.

Ce dernier point impose de pouvoir disposer d'informations du fournisseur sur les moyens de suppression des données de production, mais également des données résiduelles dans des environnements hors production.

Cette question du changement de fournisseur n'est pas encore pleinement au coeur des préoccupations des entreprises. Beaucoup d'entre elles sont au stade de la consolidation de leur stratégie digitale en intégrant l'utilisation de services tiers. Toutefois, il est probable que les prochaines années vont voir apparaitre la volonté de pouvoir changer de fournisseur simplement en conservant le même niveau de maitrise sur les données.

À PROPOS DE ...

harmonie technologie

Nationalité du siège social :
France

Lieux d'implantation de la société :
Paris et Lyon

Site internet :
www.harmonie-technologie.com

Présentation de la société :
Harmonie Technologie est un cabinet de conseil indépendant, spécialiste de la Gestion des Risques et de la Sécurité du Système d'Information (SSI). Partenaire sécurité des grands comptes depuis 2005, le cabinet intervient auprès des filières risques, sécurité de l'information et des directions informatiques.

Harmonie Technologie cultive une double compétence fonctionnelle et technique pour accompagner ses clients grands comptes sur les thématiques de sécurité du SI :

- Gestion des risques et gouvernance de la SSI ;
- Gestion des identités et des accès ;
- Sécurité des données sensibles et des applications ;
- Cyber sécurité : audit & surveillance.

PARTIE 3

FOCUS OODRIVE

Interview Edouard de Remur

CHEZ OODRIVE, LA CONFIANCE DE NOS CLIENTS DANS NOS SOLUTIONS EST DÉTERMINANTE

Depuis 2001, le Groupe Oodrive propose aux professionnels des solutions de partage de données, de sauvegarde en ligne et de confiance numérique à forte valeur ajoutée. Elles séduisent, à ce jour, un million d'utilisateurs et près de 15 000 entreprises dans plus de 90 pays. Oodrive place son expertise en matière de sécurité, d'ergonomie et d'innovation au coeur de ses solutions. Fort de cette stratégie, de son expérience et de son engagement quotidien dans la promotion du Cloud, Oodrive est devenu un acteur majeur du Cloud européen et se positionne au 29e rang des éditeurs de logiciel français. Rencontre avec Edouard de Remur qui nous présente plus en détail la stratégie d'Oodrive en matière de sécurité et de protection des données.

Comment garantissez-vous la sécurité des solutions de partage de données à vos clients ?

EDR : Chez Oodrive, la confiance de nos clients dans nos solutions est déterminante. Deux types d'outils sont d'ailleurs fréquemment utilisés par les clients pour s'assurer du niveau de sécurité des solutions : les questionnaires de sécurité et les Audits. Malheureusement, les questionnaires de sécurité reposent sur du *« déclaratif »* et les audits sont très coûteux. Alors, pour simplifier le processus de décision de nos clients et pour renforcer la relation de confiance que nous mettons en place avec eux, nous avons décidé d'investir dans une politique de certification.

De quelles certifications disposez-vous à ce jour et que garantissent-elles pour vos clients ?

Les différentes certifications et qualifications obtenues par Oodrive garantissent un niveau de sécurité élevé de nos solutions :

- **RGS :** pour assurer la confiance dans les échanges électroniques (Certificats Electroniques, Signature électroniques…).
- **Cloud confidence :** protection des données personnelles et transparence dans la chaine de sous-traitance (CNIL).
- **ISO 27001:2013 :** Référentiel pour améliorer la sécurité des infrastructures.
- **Label France CyberSecurity :** garantie pour les utilisateurs que les produits et services sont français et qu'ils possèdent un niveau de qualité vérifié par un jury indépendant.
- **Secure Cloud + (en cours) :** Référentiel de l'ANSSI pour améliorer la sécurité et la confiance dans le Cloud.

Comment procédez-vous pour satisfaire les problématiques de souveraineté et de confidentialité des données des entreprises ?

EDR : Toujours pour des questions de sécurité, Oodrive héberge les données de ses clients dans des datacenters Tier III certifiés ISO 27001. Par ailleurs, cet hébergement est proposé en local (France, Belgique, Allemagne, Suisse ou Brésil). De ce fait, la réglementation appliquée est celle du pays concerné. Une protection légale qui a son importance car toutes les législations n'offrent pas les mêmes garanties en termes de protection des données. Enfin, selon les besoins de nos clients, nos solutions sont disponibles en mode SaaS mutualisé, Cloud dédié ou licence.

Focus Mode Cloud Dédié : le mode Cloud dédié répond aux exigences de sécurité les plus poussées en offrant une infrastructure dédiée au client au sein des Datacenters Oodrive. Ce mode est d'ailleurs un prérequis obligatoire pour obtenir la qualification Secure Cloud Plus de l'ANSSI. Il est particulièrement recommandé aux OIV (Organismes d'Intérêts Vitaux).

Quels outils mettez-vous en place pour sécuriser l'accès, le transfert et le stockage des données de vos solutions de partage ?

EDR : Le chiffrement des données, la signature électronique, l'authentification forte, la navigation web déportée sur serveur, les boitiers HSM, la détection des attaques par force brute, les certificats

numériques, les applications dédiées aux usages mobiles et tablettes… sont autant d'outils mis en place pour garantir la sécurité optimale de nos solutions de partage de fichiers.

Vous évoquez les boîtiers HSM (Hardware Security Module), comment fonctionne ce dispositif ? Quel est son avantage pour vos clients en matière de protection des données sensibles ?

EDR : Nous proposons la mise en place d'un HSM pour permettre de renforcer la sécurité du serveur en chiffrant les données qu'il héberge à l'aide d'une clé maîtresse. Pour la générer, on réunit plusieurs personnes appelées «porteurs» (le client, le prestataire Cloud, etc.), chacune étant munie d'une carte à puce, le *« secret »*. Après avoir contrôlé l'identité des personnes présentes, on leur demande d'insérer leurs cartes dans le module matériel de sécurité. Celui-ci crée alors la clé maîtresse dont on définit le périmètre d'action et la durée de validité.
Cette clé permet ensuite de chiffrer toutes les données stockées sur le serveur, garantissant au client qu'elles ne seront ni consultées ni modifiées par des tiers non autorisés. Tout accès ultérieur au HSM pour effectuer des modifications nécessite en effet la présence des porteurs munis de leurs cartes respectives.

Selon vous, quels sont les métiers qui ont des besoins en matière de sécurité des échanges dans les entreprises ?

EDR : Plus que le métier, c'est le type de données échangées qui justifie d'un besoin de sécurité important. Au sein des entreprises, chaque métier est donc amené à sécuriser ses échanges de fichiers.

La sécurité des échanges de fichiers est devenue centrale. Pouvez-vous illustrer un besoin rencontré chez vos clients ?

La sécurité du partage de données en entreprise est un besoin d'autant plus important lorsqu'il s'agit d'informations échangées dans le cadre des Conseils d'Administration, Comités de Direction et Conseils de Surveillance. En effet, on y partage des informations déterminantes, qui influent tant sur les axes de développement de la société que sur les équipes : définition de la stratégie commerciale ou marketing, prise de décisions financières ou organisationnelles, suivi des investissements, gestion des crises, etc. Il est donc primordial de s'assurer que les propos tenus dans le cadre privé des réunions de gouvernance ne seront pas divulgués au reste de la société et à l'externe. Par ailleurs, il est également indispensable de permettre aux membres de ces réunions d'intervenir et de favoriser leur participation malgré les agendas chargés et la distance géographique qui, parfois, sépare chacun.

Dans ce cadre des Conseils d'Administration, Comités de Direction et Conseils de Surveillance, quelles solutions proposez-vous pour faciliter le partage de données sensibles en confiance ?

Oodrive a conçu une solution, BoardNox, pour accompagner tout le cycle de vie des réunions et les faire gagner en efficacité. Ergonomique et intuitive, elle facilite la préparation en amont en limitant les échanges d'e-mails et de documents papier. Elles offrent par ailleurs un cadre sécurisé où il est possible d'échanger des fichiers et des messages sans risque d'interception par un tiers, depuis l'établissement d'un ordre du jour jusqu'à la mise à disposition du compte-rendu.

À PROPOS DE ...

oodrive
Trusted Cloud Solutions

Nationalité du siège social : France

Lieux d'implantation de la société :
France, Allemagne, Belgique, Suisse, Espagne, Brésil et Hong Kong

Site internet : www.oodrive.fr

Autour des moyens humains et techniques :
Le groupe compte plus de 310 collaborateurs et son centre R&D basé à Paris emploie 120 ingénieurs développant des solutions multilingues dont la fiabilité est régulièrement évaluée par des audits externes et attestée par des certifications.
Pour satisfaire aux problématiques de souveraineté et de sécurité des entreprises, les données des clients sont hébergées, selon leur choix, dans l'un des 8 pays d'implantation d'Oodrive. Ses Datacenters, certifiés ISO 27001 et conformes Tiers III respectent les normes les plus élevées du secteur.

Offre de services :
Le Groupe Oodrive, éditeur de logiciels en mode SaaS, propose aux professionnels des solutions à forte valeur ajoutée adaptées aux problématiques métiers. Spécialisé dans le partage de données, la sauvegarde en ligne et la confiance numérique, Oodrive se porte garant des performances de ses solutions et fournit à ses clients un service de haut niveau assurant le succès de leurs projets et la confidentialité de leurs données. Oodrive propose ses solutions en mode SaaS avec une infrastructure mutualisée ou dédiée ainsi qu'en licence. Les technologies d'accélération de flux permettent quant à elles de garantir une expérience utilisateur internationale optimale.

Document de présentation disponibles sur le site web d'OODRIVE :
Solution BoardNox : https://www.oodrive.fr/saas/ebook-boardnox

PARTIE 3

FOCUS ARXAN

Interview Olivier Acoulon

ARXAN : PROTECTION DES APPLICATIONS MOBILES SENSIBLES, CONTRE LA FRAUDE, LA COPIE, LE PIRATAGE

ARXAN propose des solutions pour protéger les applications contre les attaques de type MATE (Man At The End) sur des environnements distribués et non de confiance. Ces solutions protègent et sécurisent le code au niveau des binaires (applications) contre les tentatives de « Reverse Engineering », les modifications, altérations du code afin de lutter efficacement contre le piratage, copie, vol de propriété intellectuelle (IP), fraude. Rencontre avec Olivier Acoulon, Regional Manager France chez ARXAN, pour nous présenter plus en détail les solutions proposées par l'éditeur.

ARXAN est un éditeur de solutions spécialisées dans la sécurité des applications, pouvez-vous nous en dire un peu plus ?

OA : Les solutions d'ARXAN sont déployées sur plus de 500 millions de périphériques et instances applicatives dans le monde. Nous proposons un solution complète, multi-environnements (Ios, Android, Windows, Linux, Mac, Multi langage de développement Java, Microsoft. net) la plus répandue dans le monde et protégeons les clefs de chiffrements AES, RSA et ECC. La protection est assurée par maillage de « Guards » et il n'y a pas de modification du code source.

Quelles sont les menaces auxquelles les entreprises doivent faire face ?

OA : Un des risques majeurs pour une société est d'apprendre que son système d'informations (y compris son ou ses applications mobiles) a été hacké.
Les tentatives de reverse engineering, de fraude, de piratage de données, ou encore des tentatives d'accès non autorisés à des services représentent de véritables menaces pour les entreprises. La plupart de nos clients ont conscience de ces menaces. Leur préoccupation n'est pas de savoir quand une attaque peut survenir mais plutôt *« sommes-nous prêt à réagir »* efficacement ? Nous apportons à nos clients une véritable réponse face à ces nouvelles menaces avec une solution unique et facile à intégrer.

Que ce soit dans un contexte interne ou en environnement Cloud, les applications mobiles sont autant de nouveaux points d'accès sur les SI. Vous avez partagé un constat plutôt pessimiste sur leur niveau de sécurité lors de la table ronde, pourquoi ?

OA : Les applications mobiles sont devenues la pierre angulaire du monde connecté ou du monde digital. On assiste aujourd'hui à leur explosion dans toutes les industries (e-commerce, e-santé, m-paiement) et que ce soit pour un usage interne (BtoB) ou un usage externe (BtoC). La DSI ne peut pas ignorer les risques de confidentialité et d'intégrité liés à l'usage de ces dernières. Ces applications mobiles, déployées au travers de store public ou privé accèdent aux SI des entreprises, qu'il faut également contrôler.

Comment peut-on savoir si des applications sont vulnérables à des attaques au niveau du binaire ?

OA : On peut facilement identifier si une application est vulnérable au niveau du binaire. Il existe en effet un certain nombre d'outils, (gratuits ou payants) disponibles sur Internet.
Voici 4 cas qui permettent de le savoir : d'abord, s'il est possible de déchiffrer le code de l'application à l'aide d'outil automatisé ; ensuite, s'il est possible de visualiser le flux de contrôle et le pseudo-code de l'application ; également, s'il est possible de modifier la couche de présentation de l'application et exécuter du code modifié ; enfin, s'il est possible de modifier l'exécutable binaire de l'application via un éditeur hexadécimal pour contourner un contrôle de sécurité.

Selon vous, quels sont les métiers qui ont des besoins en matière de sécurité de leurs applications ?

OA : La transformation digitale est en marche et les métiers veulent un *« time to market »* de plus en plus court en matière de *« delivery »* de leur application mobile. Que ce soit dans le domaine de la finance pour les applications de paiement (HCE Host Card Emulation), dans le domaine du jeu ou encore dans l'industrie du DRM (Digital Right Management) et du véhicule connecté, les équipes en charge de l'innovation associée aux équipes de la sécurité sont concernées et convaincues par ce besoin de protection de l'application.

Quels outils mettez-vous en place pour sécuriser les applications mobiles et leur contenu contre ces menaces ?

OA : Comme on ne peut pas contrôler tous les réseaux et tous les périphériques mobiles, nous proposons d'intégrer la sécurité directement au niveau de l'application mobile. ARXAN a développé une technologie logicielle qui consiste à injecter des « Guards » de défense, de détection et de réaction directement dans l'application pendant la phase de compilation. L'application mobile est ainsi capable de s'auto-protéger et capable de reagir selon le type d'attaque détectée. Par cette approche, nous ne modifions pas le code source de l'application.

Pouvez-vous nous apporter plus de précisions sur votre approche ?

OA : Nous intégrons la sécurité directement au niveau du binaire des applications à partir de technologies robustes, éprouvées et sans impacts sur la chaine de valeur du cycle de développement. Par conséquent la sécurité de l'application est toujours présente quel que soit le support (Mobile, PC, tablette, Smartphone, etc..) à partir duquel elle est exécutée. Grace à des agents de surveillance à plusieurs niveaux (les guards s'auto surveillent), notre approche fournit une sécurité durable, résistante, qui a fait ses preuves pour résister aux attaques persistantes et sophistiquées des pirates. L'un des avantages de notre offre est l'industrialisation du processus de protection pour les différentes plateformes mobiles (iOS, Android/Java, Windows Phone, Linux, Mac) ou plateformes IoT (Véhicules connectées). Enfin, avec notre approche, la politique de sécurité est appliquée au niveau du binaire et seulement connue par quelques personnes en charge de la sécurité des applications.

Quels sont les besoins de sécurité couverts par votre offre ?

OA : Nous proposons une offre unique et évolutive articulée autour de *« Guards »* de Défenses, Détections et Réactions.
GuardIT pour la protection des applications sur des architectures X86 (Intel) et EnsureIT pour les applications mobiles (architecture ARM). Pour se défendre et empêcher le reverse engineering d'un code source natif, géré ou les deux, les agents *« Guard »* utilisent les techniques d'offuscation au niveau du binaire, les techniques de chiffrement pour sécuriser la chaine du code et les techniques d'anti-debug. Concernant la détection, notre solution vérifie l'intégrité du code par la technique de Checksum et empêche la falsification et l'altération du code. La solution permet également de contrôler les routines d'authentification des composants et détecte la fonction de *« débogueur »*. Cet arsenal prévoit aussi des fonctionnalités de dommages potentiels, visant à empêcher l'exécution de l'exploit lorsque l'application est attaquée.
Enfin, afin de réagir lorsqu'une attaque est détectée, les agents *« Guards »* peuvent être programmés de différentes manières, telles que l'autoréparation du code modifié, communiquer avec d'autres composants logiciels, fermer le programme, émettre un appel en collectant des informations ou tout simplement mettre fin à l'exécution. Toutes ces techniques font parties des *« policy »* des agents (Guards) en matière de réaction.

À PROPOS DE ...

Nationalité du siège social :
USA

Lieux d'implantation de la société :
USA Europe UK- France, Allemagne, Asie, Japon

Site internet :
www.arxan.com

Contact France :
ACOULON Olivier - Régional Manager France - oacoulon@arxan.com -Tel : +336 70 160 962

Solutions :

- **GuardIT et EnsureIT*:** Protection du binaire. Préserver l'intégrité de vos codes binaires. GuardIT for Windows, GuardIT for Linux, GuardIT for Mac OS X, GuardIT for Microsoft .NET Framework, GuardIT for Java, GuardIT for Android/Intel, GuardIT for Windows/ARM, GuardIT for Windows/Embedded, and GuardIT for Flexnet® Publisher Architectures x64 et x86
- **TransformIT :** Protège les clefs de chiffrement utilisées et supporte les principaux algorithmes RSA, AES, ECC.
  Menaces : Altération, Reverse Engineering, Accès Non Autorisé.
  Bénéfices : Protection de la propriété intellectuelle, brevets, prévention contre la copie illicite, images, revenus, données ou contenus.

Références :

- **Institutions financières :** Dans une approche de protection des applications dites *« transactionnelles »* mobiles et autres à destination de leurs clients et employés - 6 importantes institutions bancaires européennes utilisent les technologies ARXAN.
- **Fournisseurs de « contenus numériques » :** En vue de protéger la gestion des droits (DRM) - Les 10 plus importants fournisseurs de contenu utilisent les technologies ARXAN
- **Editeurs de software :** Pour protéger leurs sources et leurs revenus.
- **Acteurs de la e-santé (Hôpitaux, Editeurs spécialisées) :** Pour assurer de manière sécurisée les soins à distance aux patients et garantir intégrité, confidentialité des données.
- **Editeurs de jeux :** Le top 10 de l'industrie du jeu utilise les technologies ARXAN.

Vidéos de présentation disponibles sur le site web d'ARXAN :
https://fr.arxan.com/how-to-hack-a-mobile-application/
https://www.arxan.com/products/api-protection/

*EnsureIT couvre les applications mobiles plateforme ARM.

REMERCIEMENTS

Harmonie Technologie tient à remercier tout particulièrement :

- *La société CEIS pour l'organisation du FIC et l'accompagnement dans la réalisation de la table ronde et du livre blanc ;*
- *Charles-Henri Schulz, Chargé de mission de l'ANSSI, pour son éclairage sur les référentiels et la nouvelle certification Secure Cloud ;*
- *Federico Garcia, RSSI Adjoint du Groupe CREDIT AGRICOLE SA et Brice Hauser Kauffmann, Responsable solutions de sécurité de continuité de NATIXIS, pour leurs témoignages ;*
- *Edouard de Remur, Co-fondateur de OODRIVE et Olivier Acoulon, Manager Southern Europe, ARXAN TECHNOLOGIES pour la présentation de leurs solutions ;*
- *Ronan Bertin-Hugault, Data Security Practice Manager chez HARMONIE TECHNOLOGIE, pour son implication dans la rédaction de ce livre blanc.*

Harmonie Technologie

Harmonie Technologie est un cabinet de conseil et d'expertise technique spécialiste de la gestion des risques et de la sécurité du système d'information (SSI). Partenaire sécurité des grands comptes, Harmonie Technologie assiste ses clients pour conduire des chantiers de réflexion stratégique, de transformation des organisations et d'évolution des dispositifs de sécurité.

Plus d'infos sur www.harmonie-technologie.com

Livre Blanc - FIC 2016

Réalisation par HARMONIE TECHNOLOGIE
en partenariat avec ARXAN et OODRIVE

Contacts communication

Harmonie Technologie - Gabrielle Pavia
Oodrive - Charlène Chatel
Arxan - Olivier Acoulon
CEIS - Melodie Reynaud