POSITIONING PAPER

Le nouveau paradigme de la cyber sécurité

Auteur : Mathieu Poujol, Head of Infrastructure and Cloud

2018

T · · Systems ·

PAC
A CXP GROUP COMPANY

Sommaire

PREFACE

Dans ce guide, réalisé par PAC, a CXP Group company, vous allez découvrir qu'il est urgent de mettre en place une véritable stratégie de cyber sécurité, en raison du développement du digital qui a rendu les attaques informatiques de plus en plus nombreuses et surtout dévastatrices pour les entreprises.

Les entreprises l'ont bien compris et les investissements dans le domaine se multiplient. Ainsi le marché est en croissance de +9% par an. Mais cet essor est freiné par un manque de compétences sur le marché. En tant que Président du Comité Cybersécurité du Syntec Numérique, j'ai des retours quotidiens des entreprises du numérique sur cette pénurie. Pour répondre à ce double challenge, les entreprises doivent adopter une nouvelle approche de la protection informatique.

Chez T-Systems, nous pensons que la cybersécurité doit être « as a service », centralisée pour proposer des solutions de défense à la pointe de l'innovation pour toutes les entreprises. Les DSI doivent se concentrer sur leur cœur de métier, et non s'occuper de tout sécuriser par elles-mêmes. Les prestataires de service, disposant de milliers d'experts au service des entreprises sont là pour ça. Elles disposent de Security Operating Center (SOC) internationaux et de solutions SIEM pour assurer la défense des systèmes d'information.

Nos offres « as a service » permettent ainsi une implémentation très rapide et répondent aux manques de compétences sur le marché. Nous proposons des plateformes en Europe que nous opérons et nos clients n'ont plus qu'à se concentrer sur les liens entre la cyber sécurité et leur métier.

Avec PAC, nous avons donc souhaité présenter « Le nouveau paradigme de la cybersécurité ». Grâce à leur approche par sujets technologiques et l'expertise dans le Cloud et la Cybersécurité de Mathieu Poujol, nous avons écrit un document résolument pédagogique, instructif et mettant en exergue les priorités actuelles des entreprises pour se défendre des cybermenaces.

Jean-Paul Alibert
Président T-Systems France et Président du Comité Cybersécurité du Syntec Numérique

LE CONTEXTE

Les technologies issues de l'Internet sont en train de révolutionner les usages et les habitudes des consommateurs et des entreprises. Cette transformation digitale est devenue impérative, et comme pour toute évolution rapide, la gestion du changement est primordiale. Les données sont l'énergie de cette transformation et les technologies de l'information en sont les usines. Les entreprises doivent faire face à de nouveaux défis : rapidité, agilité innovation, performance, responsabilité, écosystèmes... Ainsi 55% des entreprises françaises pensent que l'agilité et l'innovation sont leurs principaux défis actuels selon l'enquête PAC CxO 3000 Survey 2017.

50%

des principales entreprises mondiales font de la transformation digitale leur principale priorité

Forbes Insights - 2016

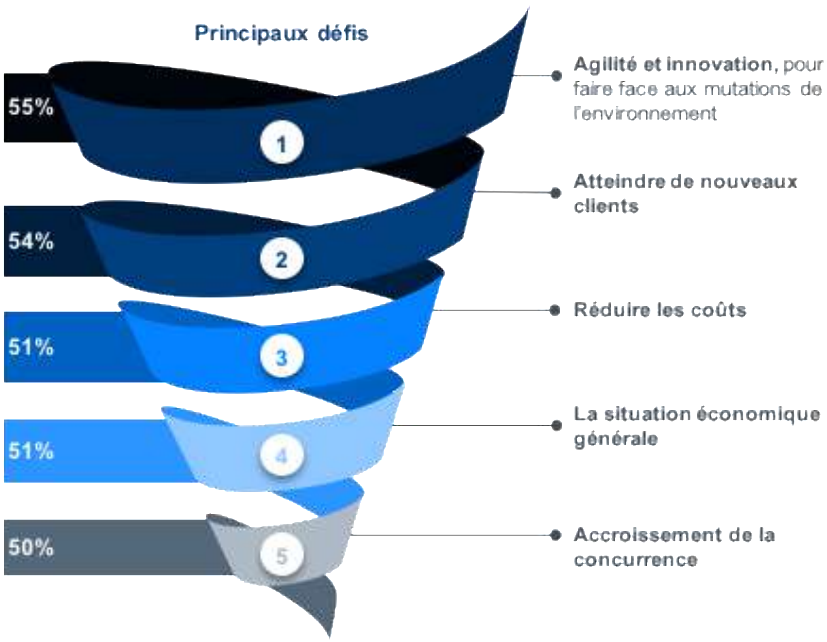


Fig. 1: Principaux défis économiques

Pour réaliser leur transformation Digitale, elles doivent devenir de plus en plus intensives en technologies de l'information et de la communication (TIC). Les TIC sont ainsi devenues omniprésentes dans les entreprises avec une valeur ajoutée de plus en plus forte, tout en étant souvent la principale source d'innovation.

Au sein des TIC, le cloud computing est de facto la norme des nouvelles entreprises numériques et constitue un élément de plus en plus important de l'informatique pour la plupart des entreprises et des administrations. Le cloud computing, Privé et Public a rapidement envahi les frontaux Web puis a fusionné avec les infrastructures existantes, ce qui a abouti à la création de systèmes hybrides. L'intégration et la gestion de ces systèmes hybrides sont devenues de plus en plus difficiles à mesure que les entreprises y migraient de plus en plus de tâches et des tâches de plus en plus complexes à mettre et à gérer dans le Cloud.

Les entreprises cherchent à rendre l'organisation plus agile et innovante et ouvrent de plus en plus leurs écosystèmes aux partenaires, fournisseurs et clients. Cela nécessite une plus grande flexibilité des systèmes informatiques, ce qui explique l'utilisation des services cloud et/ou d'infogérance (liés aux applications ou aux infrastructures).

Ces systèmes ouverts sont aussi hybrides, formés de multiples systèmes interconnectés et interdépendants (effet plat de spaghettis ou intégration Est-Ouest) et constitués de couches multiples (effet mille-feuilles ou intégration Nord-Sud). Il faut connaître, gérer et sécuriser tout cela, car les processus de l'entreprise passent et dépendent de tous ces systèmes et toutes ces couches. Cette complexité du SI est la conséquence la plus sérieuse de la digitalisation pour les entreprises.

Hormis sa gestion, le principal impact de cette complexification du SI est qu'elle accroît la vulnérabilité de l'entreprise aux cyberattaques. Les directions informatiques et les directions générales sont désormais bien conscientes des enjeux et des défis liés à la préservation de la sécurité de leurs systèmes d'information et, en particulier, à la préservation de l'intégrité des données et des processus. Avoir une infrastructure digitale fiable et sécurisée est une priorité pour les Direction des Systèmes d'Information (DSI) en France et dans la plupart des pays, comme le montre notre enquête annuelle CxO 3000. Les DSI ne sont pas les seules directions concernées, car cela affecte l'ensemble des directions de l'entreprise.

Le digital brise les silos entre les métiers, mais aussi entre le développement et la production et il ouvre les SI. Il met sur des processus digitaux de plus en plus de valeur ajoutée. Les architectures hybrides, qui sont donc les architectures de référence de cette mutation digitale ont besoin d'une cyber sécurisation à la hauteur de leur potentiel mais aussi de leur complexité.

41%

des entreprises françaises pensent qu'avoir une informatique fiable et sécurisée est plus difficile d'année en année

Enquête annuelle PAC CxO 3000 - 2017

SECURISER L'ICT EST PLUS CRITIQUE QUE JAMAIS

TOUJOURS PLUS D'ATTAQUES

La transformation digitale a ouvert les économies, les entreprises et les systèmes d'information, les rendant plus vulnérables, alors que le nombre d'attaques se multiplie. Cette situation met en danger la transformation digitale des entreprises, voire les entreprises elles-mêmes. Les statistiques sur le sujet sont éloquentes :

- 4000 attaques pour obtenir des rançons chaque jour, en croissance de 300 % depuis 2015 (FBI – 2017)
- 4500 incidents de cyber sécurité par entreprise et par an en France (PwC - 2017)
- Maerk Shipping évalue à 300 millions US$ les dégâts de l'attaque Petya du printemps 2017 (Maerk Group – 2017)
- 24 000 cyber attaques visant la France ont été bloquées par les dispositifs de cyber sécurité nationaux (Ministère de la défense – 2017)
- 700 Millions d'euros de préjudice en 2016 pour les PME françaises (IRT System X – 2017)
- ...

On pourrait remplir des pages avec des statistiques de ce type, par contre ce qu'il faut en conclure est assez simple : la cyber sécurité, c'est au moins aussi important que la sécurité physique. La sécurité a toujours été une composante essentielle de tout système économique, car plus les économies sont sûres, plus les activités se développent. Il en va de même pour le digital.

De plus, la transformation digitale ne concerne pas seulement les entreprises, elle a aussi un côté obscur... Les pirates et les corsaires (pirates sponsorisés par un Etat) de l'Internet se sont convertis au digital bien plus rapidement que les entreprises. De plus, les cyberattaques sont assez peu sanctionnées par la loi en comparaison de leurs impacts ou gains possibles. Enfin, Internet, en interconnectant le monde a multiplié le nombre de pirates potentiels, puisque les attaques peuvent venir de n'importe quel point du globe, de la Corrèze au Zambèze.

2 fois

plus de cyber attaques en 2016 par rapport à 2015

Enquête France OpinionWay 2017

Le résultat : il y a toujours plus d'attaquants, mais comparativement peu de défenseurs. Ces attaquants utilisent pleinement les capacités du digital pour faire et coordonner toujours plus d'attaques mutantes avec toujours plus de puissance de feu. Ces organisations quasi industrielles sont basées sur des architectures cloud et utilisent ces capacités pour attaquer.

Les motivations des attaquants ont une ou plusieurs de ces trois origines :

- Activisme politique
- Espionnage
- Criminalité

Les impacts sont de plusieurs ordres mais concernent essentiellement le vol de données, la perte de données ou la perturbation d'une activité (service en ligne ou processus physique), avec des effets de plus en plus graves.

LES ATTAQUES AVANCEES PERSISTANTES

Les attaques avancées persistantes sont de loin les formes d'attaque les plus dangereuses et les plus difficiles à détecter. Dans ce type d'attaque, les pirates et corsaires ne frappent généralement pas au hasard, et ce ciblage fait qu'il est difficile d'y résister. Ces menaces sont furtives et continues, car elles exigent un degré élevé de dissimulation sur une longue période de temps. Le but d'une telle attaque est de placer du code malveillant personnalisé sur un ou plusieurs ordinateurs pour effectuer des tâches spécifiques, le plus souvent le vol d'informations, tout en restant inaperçu pendant la plus longue période possible. Ces menaces complexes combinent souvent différents vecteurs et stratégies d'attaques, pouvant utiliser des techniques et failles inconnues.

Mais vu que les moyens pour les construire et les améliorer se démocratisent sur Internet, il est de plus en plus difficile de les prévenir, de s'en protéger et surtout de les détecter. Pour ce faire, il faut avoir accès à des capacités d'analyse, d'intelligence et de retro-ingénierie avancées et puissantes, qui nécessitent de lourds investissements et des ressources humaines très pointues et donc très rares.

Pour ces deux aspects, il est difficile d'être bien protégé et peu d'entreprises sont capables d'y arriver seules, car il faut combiner l'ensemble des aspects que nous avons présentés, tant au niveau de la vision et de la stratégie, que de l'utilisation des technologies de protection les plus avancées. Et il faut surtout beaucoup de capacités de traitement, d'expertises pointues et de ressources, tant matérielles qu'humaines. Ces investissements sont dur à justifier pour beaucoup d'entreprises.

Les attaques persistantes avancées sont les deuxième plus courantes sur le continent

Rapport IOCTA - Europol - 2016

La cyber sécurité qui était une menace plutôt bégnine, est ainsi devenue avec le digital, une problématique majeure.

UNE PRISE DE CONSCIENCE

L'impact des cyber attaques n'est donc plus virtuel, il affecte les comptes de résultats et peut faire des dégâts physiques. Les exemples sont nombreux et il ne se passe pas une semaine sans qu'une cyber attaque ou une vulnérabilité soit signalée.

Les gouvernements, les entreprises et les particuliers ont pris conscience de ces impacts qui pouvaient endommager leur réputation et leur compétitivité, voire les conduire à la faillite.

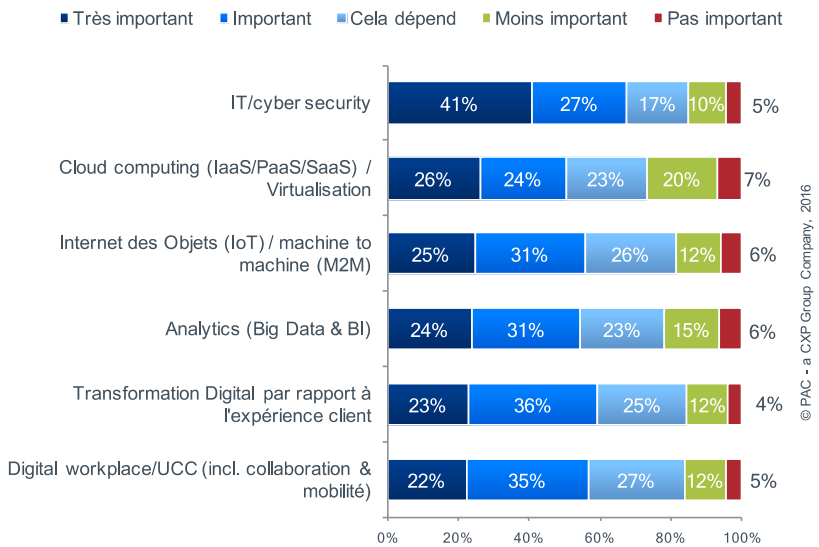
De ce fait, les règlementations se sont durcies, au sein des industries (Bâle III, IATA, etc...), mais aussi au niveau régional (GDPR, NIS) ou national (LPM). Il faut les respecter ou risquer des amendes, qui par exemple, dans les cas des directives européennes, peut aller jusqu'à 4% du chiffre d'affaires annuel.

Les entreprises savent maintenant que la cyber sécurité est un catalyseur clé de la transformation digitale. Les entreprises ont donc entrepris d'investir sur le sujet, pour pouvoir réussir, la cyber sécurité est devenue depuis 3 ans le poste des dépenses informatiques en France où la dépense augmente le plus.

80%

des entreprises françaises sont au courant de leurs obligations règlementaires en matière de cyber sécurité

Étude PAC Cyber Conformité France - 2017



Répartition des réponses des entreprises Monde, exprimée en % (n = 3000)

Fig. 2: CxO 3000 : évolution des budgets Cyber Sécurité

Mais face à la multitude de menaces, la rareté des ressources et à la complexité des métiers et des systèmes informatiques évoqués, les entreprises sont assez désemparées, se demandant comment elles peuvent faire face.

Tous les acteurs du marché (entreprises, fournisseurs, pouvoir publics) se partagent des ressources limitées, ce qui en augmente la rareté et le coût :

- D'une part la formation, même si elle a fait d'importants efforts, peine à suivre la demande.
- D'autre part, la cyber sécurité est un métier où l'expérience est très importante, et donc la demande se focalise plus sur les ressources expérimentées.

C'est pour cela que la cyber sécurité est un marché atypique, en pleine croissance certes, mais comme il est limité fortement par les ressources, il est de plus en plus intensif en services infogérés, des prestations qui caractérisent plutôt les marchés matures. Les services infogérés, voire le Cloud optimisent bien mieux l'utilisation des rares ressources du marché.

Pour faire face, les entreprises doivent mettre en place une vraie stratégie de cyber sécurité basée sur les atouts du digital et ses avantages opérationnels. En un mot, utiliser le digital pour combattre ses effets négatifs. Mais elles doivent aussi se rendre compte qu'elles ne peuvent pas faire tout cela toutes seules.

Selon PAC le marché de la Cyber Sécurité en France a atteint près de 2,5 milliards d'euros en 2017 avec une croissance annuelle moyenne supérieure à 8% d'ici à 2020

Chiffres PAC Étude SITSI Cyber Security France - 2017

COMMENT SECURISER SON SYSTEME A L'HEURE DIGITALE

LA VISION

La cyber sécurité à l'Ere du Digital se doit de changer de paradigme et donc d'être :

- Agile, réactive et adaptable, comme les systèmes qu'elle veut sécuriser, et comme les menaces qu'elle affronte.
- Un facilitateur des activités du digital, qui doit permettre à l'entreprise de gagner en vélocité tout en étant protégée

Cette spécificité de la sécurisation du digital implique des changements important dans la manière dont on se protège. Il faut passer du mode forteresse ou sécurité périmétrique, au mode aéroport : la défense en profondeur des actifs sensibles.

Avant l'ouverture des économies et des systèmes d'information, et leur besoin croissant de vitesse de changement, on pouvait protéger les systèmes d'information comme on protège une forteresse, avec peu d'entrées, et des entrées qui étaient lourdement gardées par des cyber pont levis, barbacanes et herses. Mais comme avec la Renaissance européenne, qui a ouvert les villes, car les ouvrages défensifs gênaient le commerce, les entreprises en mode forteresse peuvent difficilement embrasser la transformation digitale. De plus, ce type de défense est particulièrement vulnérable aux attaques internes.

Il faut dont changer de paradigme, passer de la défense en mode forteresse à la défense en mode aéroport.

La métaphore de l'aéroport, ou défense en profondeur, par contre, repose sur un système ouvert – tout le monde peut entrer dans un aéroport – mais dont la sécurité se durci au fur et à mesure que l'on s'approche du cœur de l'activité de l'aéroport, la gestion des

> Les anciens paradigmes ne sont plus efficaces car la protection ne fonctionne plus si vous regardez seulement votre propre petit monde.
> Pour bien se protéger, il faut aussi regarder loin de vos propres pare-feux
>
> *Nabil Hachem, Consultant Cybersécurité T-Systems - 2017*

passagers et des avions. Ce type de défense en profondeur se focalise sur les actifs les plus critiques de l'entreprise, mais aussi la capacité de réaction et de contre-attaque lors qu'une attaque a été détectée.

Comment traduit-on cela en matière de Cyber Sécurité ?

Tout d'abord, ces deux approches ne sont pas exclusives, il faut toujours de la défense périmétrique - la forteresse - pour arrêter le gros des attaques. Les aéroports sont d'ailleurs des lieux dont le périmètre est fermé. Ensuite, les systèmes doivent plus miser sur la détection des menaces avant et après qu'elles franchissent le périmètre.

La défense en profondeur fonctionne autour du triptyque, protection, détection, résolution alors que la défense périmétrique tend à se focaliser surtout sur la protection. La défense en profondeur part du constat que des attaques vont réussir et qu'il faut donc les détecter au plus tôt, pour s'en protéger, et les résoudre au plus vite pour limiter les dégâts. D'après l'étude PAC Intrusion Detection Protection Europe de 2016, en 2 ans, toutes les entreprises sondées en Europe ont au moins eu une brèche qui a fait des dommages.

Ensuite, il faut mettre en place un zonage dans le système d'information selon l'impact que peuvent avoir les attaques dans chacune de ses zones, en partant des plus critiques au cœur des systèmes et allant jusqu'aux au moins critiques. Ce zonage évite que toute brèche ne devienne un gros risque, et prévient la contagion des attaques de zones en zones. Au début, les cyber défenses sont assez lâches, et peu intrusives pour faciliter les flux métiers, puis progressivement se durcissent au fur et à mesure que l'on atteint des zones sensibles, où l'impact d'une cyber attaque serait très fort. Ce zonage permet en outre de gagner du temps lors d'une attaque ciblée et persistante, tant pour détecter l'attaque que pour la résoudre. Au cœur du système, les défenses sont basées sur des systèmes multiples et redondants, combinés à une authentification forte ainsi qu'un cryptage complexe des données. Ainsi on minimise les impacts de la cyber sécurité sur les métiers tout en gardant un niveau de défense fort. Cette approche est au cœur des préconisations de l'ANSSI (Agence National de la Sécurité des Système d'Information). Cette approche est par ailleurs quasiment obligatoire pour des concepts comme l'IoT.

Cette approche nécessite une vraie stratégie d'entreprise.

Le concept de la défense en profondeur peut s'appliquer à toutes les strates d'un système d'information, du niveau macroscopique aux aspects les plus microscopiques

La défense en profondeur appliquée aux systèmes d'information
Memento - SGDSN - 2004

LA STRATEGIE

La stratégie de cyber sécurité dans le digital ne fait pas table rase du passé, au contraire, elle s'appuie sur la cyber sécurité traditionnelle qu'elle complète et améliore. Il n'est donc pas nécessaire de faire table rase du passé, mais plutôt d'adapter les investissements actuels à la nouvelle donne. Cette stratégie doit s'aligner sur 3 concepts clés :

1. Approche holistique de la cyber sécurité, le système est aussi sûr que son maillon le plus faible. Comme le digital casse les silos, la cyber sécurité du digital doit faire de même et sécuriser tous les systèmes sur toutes les couches.
2. Visibilité, on ne peut protéger que ce que l'on connait et c'est d'autant plus compliqué dans les systèmes digitaux basés sur des écosystèmes et fortement distribués.
3. Une plateforme de contrôle - la tour de contrôle - pour reboucler avec l'allégorie de l'aéroport.

Fig. 3: Les concepts clés de la cyber sécurité

Pour défendre les entreprises dans le digital, il faut pouvoir utiliser les capacités offertes par le digital. La puissance des architectures Cloud, que ce soit au niveau de la capacité de stockage ou de celle de calcul, permet de combiner des capacités analytiques puissantes (le big data basé sur le cloud) et de leur appliquer de l'Intelligence Artificielle (IA). Ce type de défense, réactive, agile et intelligente est parfaitement adapté à la défense en profondeur et s'aligne complètement avec les 3 concepts clés que nous venons de présenter. C'est l'avènement de la cyber sécurité comportementale, contextuelle et auto-apprenante.

Fig. 4: Nouveau paradigme de la cyber sécurité

> La sécurité est l'affaire de tous, à commencer par les cadres dirigeants. L'identification des risques et leur prise en compte au bon niveau est de leur responsabilité.
>
> *Guillaume Poupard- Directeur Général ANSSI - 2015*

LA MISE EN OEUVRE

Premièrement, avant de choisir des outils et services de cyber sécurité, il est impératif de classifier ses données, ses systèmes, ses applications et ses processus selon leur criticité et selon les contraintes métiers qui leur sont afférentes.

Il est de plus en plus important de respecter les fondamentaux de la cyber sécurité : ce n'est pas une question d'outils de sécurité, mais d'organisation et de gestion de la sécurité. Il s'agit d'une approche descendante globale, qui s'oppose aux approches stratifiées et segmentées, dont de nombreux fournisseurs de logiciels de sécurité et certains analystes de marché font l'éloge.

Cette approche se fonde sur 3 cycles interdépendants : le cycle amont, le cycle de gouvernance et le cycle opérationnel.

LE CYCLE AMONT

Fig. 5: Le cycle amont de la cyber sécurité

Le cycle amont de la cyber sécurité est une approche itérative de la cyber sécurité qui vous permet de commencer là où vous allez pouvoir obtenir une visibilité sur toutes les parties constitutives de votre SI (voir partie précédente), puis il va vous permettre de mettre en place votre défense en profondeur et son zonage (voir passage précédent). Ce cycle amont de la cyber sécurité est un enchainement des meilleures pratiques à mettre en place avant de choisir des solutions de cyber sécurité.

55%

des entreprises françaises ont déclenché leur mise en conformité en matière de Cyber Sécurité après une analyse des risques

Etude PAC Cyber Conformité France - 2017

Il est fortement recommandé de se faire aider à ce niveau par un prestataire de service, spécialiste du sujet car si la mise en place de ce cycle est primordiale, c'est une tâche ardue nécessitant une forte expérience et une solide expertise, ainsi qu'une vision extérieure à l'entreprise.

LE CYCLE DE LA GOUVERNANCE

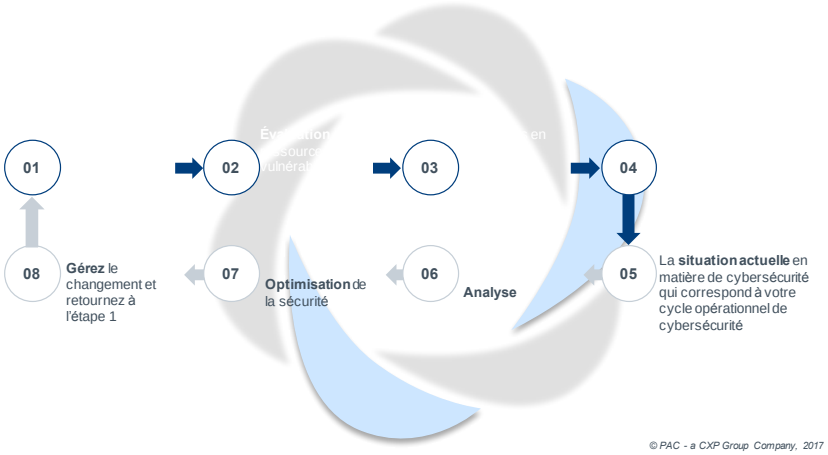


Fig. 6: Le cycle de gouvernance de la cybersécurité

Un fois que le cycle amont a été mis en place, l'étape suivante est de mettre en place le cycle de la gouvernance. Il est basé sur une plateforme globale de gestion de la sécurité ou Security Operation Center ou SOC (voir partie précédente). Ces plateformes sont basées sur des logiciels de SIEM, qui gèrent et corrèlent les évènements de sécurité

Le Security Operating Center désigne une plateforme qui fournit des services de détection, de hiérarchisation et de résolution des incidents de sécurité. Le centre de sécurité va ainsi collecter les événements (sous forme de logs notamment) remontés par les composants de sécurité, les corréler, les analyser, détecter les anomalies et définir des réactions en cas d'émission d'alerte. Les SOCs sont d'autant plus performants qu'ils ont une approche holistique des problématiques, une visibilité globale et des capacités d'analyse et de corrélation puissantes, notamment grâce au Big Data et à l'intelligence artificielle

Pour poursuivre l'allégorie avec l'aéroport, ces tours de contrôle de la cyber sécurité sont elles aussi en plein changement de paradigme, car les technologies actuelles sont limitées pour gérer l'incroyable diversité et plasticité des environnements digitaux. Pour résoudre cette problématique les SOC de nouvelle génération utilisent l'IA et le Big Data (voir partie précédente)

> Le SOC est un dispositif organisationnel nécessaire, au regard des risques et des enjeux actuels pour la sécurité de l'information.
>
> *ANSSI - 2016*

LE CYCLE OPERATIONNEL

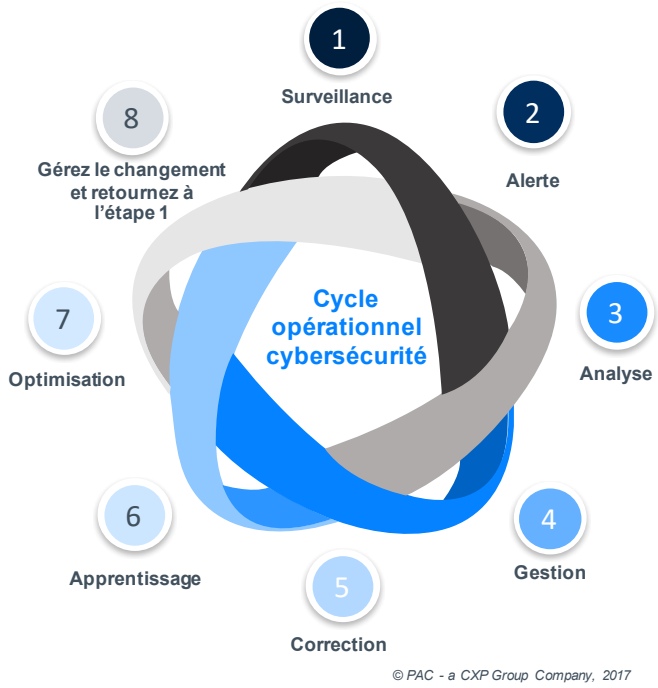


Fig. 7: Le cycle opérationnel de la cybersécurité

Comme les deux autres cycles précédents, le cycle opérationnel de la cyber sécurité est aussi un cycle itératif, qui permet d'améliorer sans cesse son niveau de cyber sécurité. Il se base sur le triptyque protection, détection et résolution, en se focalisant sur les deux derniers points.

La protection des systèmes d'information reste la tâche principale de la cyber sécurité, mais ce n'est plus suffisant. Comme nous l'avons évoqué plus haut, on ne peut pas/plus seulement se protéger derrière les hauts murs d'une forteresse. Il faut doter ses systèmes de cyber sécurité de capacités plus fortes de détection (le SOC en est un des points névralgique) des attaques, avant qu'elles ne se produisent, et une fois qu'elles ont pénétrées le périmètre. Dans le premier cas les entreprises peuvent mieux se préparer aux attaques à venir et dans le deuxième cas, elles peuvent diminuer les risques des attaques, et résoudre au plus vite leurs conséquences. Et pour finir, il ne faut surtout pas négliger la phase résolution des incidents de cyber sécurité, car on en diminue ainsi les impacts.

La sécurité repose sur le triptyque protection, détection, résolution

Étude PAC SITSI Market InSight Intrusion Detection - 2016

ET APRES ?

Une fois que ces cycles sont mis en place, vous pouvez sélectionner vos outils de cyber sécurité et vos prestataires. Il est important de noter qu'en raison de la complexité et de la diversité du cloud et des environnements hérités par de nombreuses entreprises, celles-ci doivent se focaliser en premier lieu sur les fondamentaux de la cyber sécurité, puis sur les autres points clés qui sont développés ultérieurement dans ce document.

Enfin, cette stratégie ne peut être opérée que si l'entreprise se concentre sur ce qu'elle sait faire, sur les points les plus spécifiques, les plus métiers, les plus important de son activité.

Là encore, la métaphore de l'aéroport a du sens. Les entreprises aéroportuaires gèrent et coordonnent les activités des plateformes, en exécutent certaines et en délèguent d'autres. Des entreprises tierces s'occupent des taches industrialisables, très importantes, mais à faible valeur ajoutée, comme le contrôle des passagers, d'autres s'occupent de taches à très forte valeur ajoutée, mais que la plateforme aéroportuaire ne peut maîtriser, comme la maintenance des avions.

Lorsque l'on applique cela à la cyber sécurité, comme les sociétés aéroportuaires, les entreprises ne peuvent maitriser tous les compartiments du jeu. Il faut savoir ce qu'on maitrise, ce que l'on fait et ce que l'on coordonne, car il est crucial d'optimiser ses investissements en cyber sécurité puisque les ressources humaines sont sévèrement limitées. Il est donc nécessaire de faire appel à des partenaires et des sous-traitants, tant pour les parties à faible valeur ajoutée que pour celles qui nécessitent des expertises très pointues. Il est important d'en garder la maîtrise et la gouvernance.

Et bien sûr, la stratégie de cyber sécurité en tant que catalyseur de la transformation digitale doit avoir un soutien au plus haut niveau dans l'entreprise.

Les 6 règles d'or pour les Directions Générales :

1. Identifier, quantifier et prioriser les risques
2. Nommer un Responsable Sécurité Numérique
3. Allouer un Budget à la Cyber Sécurité
4. Intégrer un critère de confiance dans les Achats
5. S'assurer de la prise en compte de la sécurité dans les projets
6. Contrôler régulièrement la sécurité

Syntec Numérique- 2017

LES POINTS CLES DE LA CYBER SECURITE

LES FONDAMENTAUX

La cryptographie et la gestion des identités et des accès sont les bases de la sécurité, qu'elle soit cyber ou pas, et ces bases sont tout aussi importantes dans les environnements digitaux. Ces aspects de la sécurité doivent être adaptés au digital et traités en priorité

Avec l'avènement de la révolution industrielle du digital, les données, qui sont devenues l'énergie de cette transformation digitale, doivent être le but ultime de la cyber sécurité (avec le maintien en conditions opérationnelles). Depuis la nuit des temps, la cryptographie est une mesure simple et efficace de protection des données sensibles.

Un autre aspect fondamental de la cyber sécurité est la gestion des identités et des accès. C'est d'autant plus important à l'heure actuelle, que les identités à privilèges sont une des vulnérabilités les plus utilisées et les plus dommageables, et que le nombre d'identités explose dans l'univers digital, tant pour les humains que pour les machines avec l'IoT. La gestion des accès est elle aussi cruciale, car il faut protéger les points d'entrées au SI, les réseaux et les messageries.

LA PROTECTION DES TERMINAUX

Les terminaux sont les outils d'interaction avec le système d'information, l'interface homme/machine, homme/homme et machine/machine. C'est donc la périphérie du SI et les premières cibles des attaquants. C'est tout particulièrement le cas depuis l'avènement des terminaux mobiles intelligents et ce type d'attaque ne devrait que croitre avec l'IoT. L'inflation des points d'entrée au SI et donc de la surface d'attaque, est une vraie problématique et

73%

des responsables informatiques pensent que l'e-mail est le premier vecteur de menaces

EY Global Information Survey - 2017

comme précisé auparavant la protection périmétrique est toujours un prés requis, même si ce type de protection doit être complété par des approches articulées autour des 3 concepts clés de la cyber sécurité (voir partie précédente).

Les messageries sont le premier vecteur de vulnérabilités, alors qu'elles restent un système incontournable d'échange entre et au sein des entreprises. Il faut donc être capable d'assurer une protection en aval des SI et entre/avec les SI partenaires.

LA PROTECTION DES RESEAUX

Les réseaux sont les systèmes nerveux des écosystèmes digitaux, et leur paralysie peut affecter l'entreprise et/ou l'ensemble de son écosystème. Le Cloud et donc l'économie et les entreprises digitales sont basées sur les réseaux. Le maintien en condition opérationnelles des réseaux de l'entreprise (en interne ou en externe) est donc très important. Les réseaux propagent les attaques, et sont donc le vecteur quasi unique pour les attaques exogènes. De plus, ils sont très sensibles aux attaques affectant leur fonctionnement. Un exemple d'attaque paralysant le réseau est le déni de service ou DDoS. Ce dernier a le vent en poupe, car avec les capacités informatiques du Cloud et l'IoT, c'est relativement devenu facile à faire, tout en restant dur à contrer, si on n'est pas un spécialiste de la gestion des réseaux.

LA SECURITE ET LE CLOUD

Le Cloud est l'architecture de base du digital, que ce soit les projets de transformation qui impliquent une migration vers le Cloud où ceux autour de la mobilité et de l'IoT qui impliquent aussi des plateformes Cloud. Sa protection est essentielle. Il faut donc être capable de :

- Sécuriser dans son SI, ces nouvelles architectures, qui restent par nature assez ouvertes,
- Projeter sa cyber sécurité vers ces systèmes exogènes pour être sûr qu'ils sont sans danger, que ce soit des Cloud Privés ou des Cloud Publics.

Ce dernier point est peut-être le plus difficile à réaliser car les Cloud Publics sont souvent des « boîtes noires » où la sécurité reste une obligation de moyens, mais pas de résultats et qui échappe très largement au contrôle de l'entreprise. Acquérir de la visibilité sur les Cloud public pour intégrer leur gestion dans une plateforme unifiée pour obtenir une vision réellement holistique de ses risques est une gageure...

Cela ne veut aucunement dire que les données et les processus sont plus en danger dans les Cloud Publics. C'est un choix relevant de la gestion de risque et de la confiance en ses fournisseurs que de laisser

> Quelles que soient les ressources dont vous disposez, un fournisseur Cloud en aura toujours plus.
>
> *Richard Norris CIO Reliance Mutual Insurance - 2015*

ces vulnérabilités non couvertes. Les Cloud Privés managés par des tiers sont généralement proches des contrats d'infogérance et offrent des garanties contractuelles. De plus, la dissémination des données et des traitements dans les Cloud Publics, ainsi que la nationalité extra-européenne de certains d'entre eux posent des problèmes de conformité avec les règlementations sectorielles (comme Bâle3), nationale (LPM) et européennes (RGPD, NIS).

À l'inverse, un autre aspect est souvent occulté, c'est le fait que le Cloud peut aussi être un atout pour la sécurité, avec :

- La sécurité venant du Cloud, c'est-à-dire les systèmes de protection tirant parti de la puissance du Cloud en particulier pour faire tourner des systèmes d'IA. Comme présenté plus haut, la partie technologique du nouveau paradigme de la cyber sécurité se base précisément sur ce concept.
- La sécurité dans le Cloud, puisqu'on est généralement plus en sécurité dans les centres de données Cloud que dans ses propres installations. En effet, les investissements en matière de sécurité consentis par la plupart de ces fournisseurs sont assez souvent hors de portée de leurs clients.

> La collaboration est un facteur clé dans la réussite de toute politique de Cyber Sécurité.
>
> *Mark Sayers- Directeur Adjoint - Cyber and government security directive, UK Home Office - 2017*

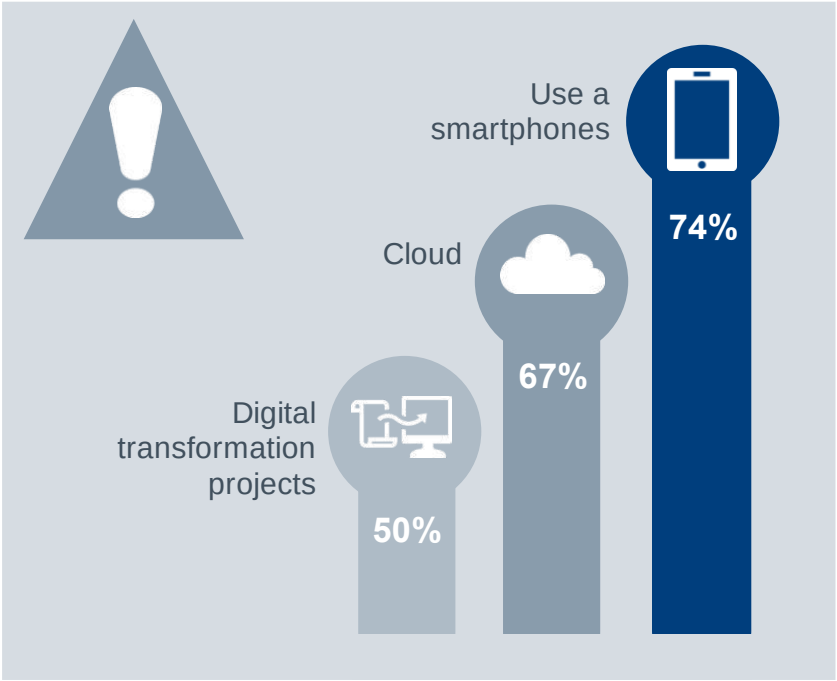


Fig. 8: Les tendances IT qui augmentent les cyber-menaces – Source PAC MSSP 2016

L'HUMAIN

La partie qui concerne l'humain en Cyber Sécurité est primordiale, et concerne principalement trois points : la collaboration, la sensibilisation et les ressources.

LA COLLABORATION

En premier lieu, à l'ère du numérique, la collaboration, activité éminemment humaine, est indispensable, car consubstantielle à la visibilité et à l'approche holistique de la cyber sécurité. Elle est nécessaire à deux niveaux. En interne, puisque vous devrez travailler avec le service IT et les différents départements pour savoir ce qui se passe au sein de vos systèmes, voire découvrir les actifs que vous devez protéger. En externe avec vos pairs, les agences de sécurité nationales/internationales et les prestataires de cyber sécurité. Disposer de plusieurs avis, conseils et prestations autour de la cyber sécurité constitue une autre bonne pratique qui vous permettra de limiter les risques et d'accéder à différents types d'expertises et à davantage d'informations sur les menaces et les meilleures pratiques.

> Les entreprises dépensent des millions de dollars en pare-feu, cryptographie et sécurité d'accès, et c'est de l'argent gaspillé ; aucune de ces mesures n'adresse le maillon le plus faible de la sécurité
> *Kevin Mitnick- Pirate, Consultant & Écrivain - 2005*

LA SENSIBILISATION

Par contre, les meilleures protections techniques ne peuvent garantir une bonne protection si les employés n'agissent pas avec prudence. Par conséquent, l'ensemble des collaborateurs doivent également suivre régulièrement des programmes de sensibilisation, de maîtrise et de formation. C'est tout particulièrement le cas des dirigeants et de certains postes avec de fortes habilitations. Selon les données de PAC, ce type de vulnérabilité interne représente près de la moitié des failles de cyber sécurité depuis 2015. L'impact de ces vulnérabilités humaines est très souvent sous-estimé.

LES RESSOURCES

C'est le principal point noir de la Cyber Sécurité : selon tous les observateurs du marché, une part importante des besoins en ressources humaines en cyber sécurité ne sont pas couverts chaque année. Comme mentionné plus haut dans ce document, les ressources humaines en Cyber Sécurité sont difficiles à former, et très demandées sur le marché, ce qui les rend rares et chères. Les 3 cycles de la Cyber Sécurité montrent clairement que les métiers de la cyber sécurité sont très diversifiés, et leur champ d'applications sont très larges, puisqu'ils couvrent toute l'informatique, des réseaux aux applications, mais aussi et de plus en plus, les métiers. Selon l'étude de l'OPIIEC (observatoire dynamique des métiers du numérique, de l'ingénierie, des études & conseil et de L'événement), la Cyber Sécurité compte 18 métiers et 19

compétences types techniques et fonctionnelles. Et avec la monté en puissance des problématiques métiers, relayées par la règlementation, ces métiers et ces compétences sont de plus en plus spécialisées. C'est donc quasi impossible pour une entreprise de pouvoir avoir tous ces types de profils.

Pour des raisons règlementaires, mais aussi des raisons de proximité, il est assez difficile de délocaliser, en particulier vers les pays à bas coûts extra européens, qui d'ailleurs sont eux aussi confrontés aux mêmes problématiques. La cyber sécurité ne peut pas bien fonctionner sans ces compétences.

Comment les entreprises peuvent-elles maitriser tous ces points clés de la cyber sécurité pour assurer ainsi un niveau de protection acceptable ?

1/4

des besoins de ressources humaines des entreprises françaises en Cyber Sécurité ne sont pas couverts.

Etude ANSSI - 2016

CONCLUSION

LE NOUVEAU PARADIGME DE LA CYBER SECURITE

Un paradigme désigne une représentation du monde, une manière de voir les choses, un modèle cohérent du monde qui repose sur un fondement défini (matrice disciplinaire, modèle théorique, courant de pensée). Avec l'avènement du digital, le paradigme du marché a changé, comme présenté dans ce document, et de ce fait le paradigme qui régissait la cyber sécurité doit lui aussi changer.

Ce nouveau paradigme est nécessaire à la mise œuvre d'une stratégie d'entreprise en matière de cyber sécurité à l'heure digitale, car les vulnérabilités et les menaces sont de plus en plus complexes et nombreuses dans un environnement digital en constante mutation. Tout cela repose sur une plateforme intégrée et globale de sécurité :

- Capable d'assurer une visibilité globale des risques et une protection holistique,
- Et d'opérer les trois cycles itératifs de la cyber sécurité.

La forme la plus aboutie de ces plateformes, ce sont des Security Operation Centers (SOCs) de nouvelle génération, qui intègrent les nouveaux concepts et paradigmes de la cyber sécurité à l'heure du digital, c'est-à-dire les capacités d'analyse contextuelle et comportementale de l'IA couplé aux capacités et à la puissance du Big Data et du Cloud. Véritables tours de contrôle de notre cyber sécurité (architecturée en mode aéroport bien sûr !), ils lui permettent de respecter les concepts clés et les meilleures pratiques de la cyber sécurité.

Point cardinaux de la compliance, ces plateformes doivent être aux normes et permettent de les respecter plus facilement, maintenant et dans le futur. Elles doivent aussi être compatibles avec le Cloud et capables d'être disponibles en mode Cloud. Ce sont les points centraux de l'arsenal de défense de l'entreprise, auxquels se rattachent des offres plus spécialisées telles que :

L'adoption des services mangés de cyber sécurité en Europe est en pleine croissance, car la triple pression de la cyber criminalité, des pénuries de compétences et de la conformité se répercute sur des départements informatiques sous pression et des conseils d'administration qui s'inquiètent de l'impact des violations de données.

Étude PAC Managed Security Services Europe - 2017

- Les bases de toute sécurité informatique, la cryptologie et la gestion des identités et des accès,
- La protection des réseaux,
- La sécurisation des terminaux,
- La protection du Cloud
- La défense contre les attaques avancées et persistantes.

Ces approches intégrées de la Cyber Sécurité, ne sont pas seulement des plateformes destinées aux grands comptes internationaux. Elles concernent aussi leurs partenaires, leurs sous-traitants, leurs clients, en un mot tout leur écosystème, qui peut être source de vulnérabilités. Du fait de leur plus grande fragilité, les entreprises moyennes sont elles aussi fortement concernées.

SA MISE EN PRATIQUE

La mise en pratique d'une approche théorique est toujours compliquée. Dans le cas de ces plateformes critiques, fortement règlementées et dans un environnement où il y a peu de ressources capables de les opérer, c'est très difficile. De plus, les cyber menaces étant en mutation constantes, les systèmes de protection doivent suivre ces mutations, voire les devancer tout en restant alignés avec l'environnement digital hétérogène et mouvant de l'entreprise et de ses partenaires. C'est quasiment la quadrature du cercle...

Pour y arriver les entreprises doivent impérativement optimiser leurs ressources et trouver le meilleur des technologies et des expertises disponibles. Ce n'est possible que de deux manières :

- Utilisation de plates formes industrialisées et automatisées,
- Infogérance, pour mutualiser au maximum les expertises et opérer une bonne partie de ses plates-formes.

Ce nouveau paradigme nécessite le plus souvent des investissements assez lourds, couplés avec une expertise importante et des capacités d'intelligence et d'analyse fortes et novatrices. Ces expertises sont rares voire très rares, et le plus souvent le seul moyen d'y avoir accès à un coût raisonnable, c'est au moyen des ressources mutualisées d'un prestataire de services managés de cyber sécurité. Il est donc nécessaire à ce niveau de faire appel à un ou plusieurs prestataires dont c'est le métier, et qui ont ces capacités d'évolution et de suivi de l'environnement de l'entreprise et de celui des menaces.

PAC prévoit un fort développement de ce type d'offres car sans services managés, il est quasiment impossible aux entreprises de mettre en place ce nouveau paradigme pour faire face aux défis de la cyber sécurité.

42%

des entreprises européennes vont augmenter leur budget dédié aux services managés de sécurité

Étude PAC Managed Security Services Europe - 2017

Les meilleures pratiques dans le domaine des services managés de cyber sécurité, sont des meilleures pratiques classiques lorsque l'on utilise des services managés.

Il faut confier à ses partenaires les taches les plus consommatrices et celles dont la consommation de ressources varie le plus, où leurs capacités d'industrialisation et de mutualisation leur donnent un clair avantage. C'est particulièrement le cas de la gestion des évènements de sécurité au sein des SOC, de la protection des postes clients et de celles du Cloud. La protection contre les attaques en déni de service fait aussi partie de ce groupe, mais sa spécificité fait que le prestataire de services managés doit aussi avoir une forte expertise sur les réseaux.

Le fait que ces prestataires puissent délivrer leurs services en mode Cloud est un avantage indéniable, car le « as a Service » s'adapte bien mieux aux contraintes du digital et les architectures Cloud ont une bonne qualité de plasticité.

Les entreprises doivent aussi évaluer l'utilisation de services externes sur des taches plus spécifiques, comme la gestion des vulnérabilités, qui requièrent une tierce vision pour être effective ou la protection contre les attaques avancées et persistantes qui nécessite une expertise, une expérience et des capacités d'analyse hors de portée de la plupart des entreprises.

Cette approche permet aux entreprises de se concentrer sur les parties les plus proches de leurs métiers, sur la gouvernance de la cyber sécurité, et donc focaliser leur rares ressources sur les points où elles sont le plus utiles.

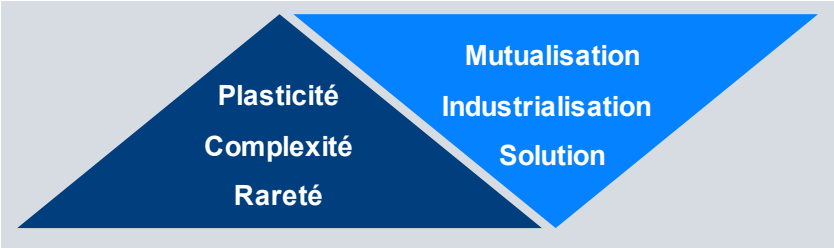


Fig. 9: Meilleures pratiques lors du choix d'un MSSP

La sécurisation des entreprises doit se faire autour du nouveau paradigme de la cyber sécurité. La mise en place de ce paradigme ne peut se faire qu'avec des services managés de cyber sécurité.

« Il suffit d'une vulnérabilité »

Les 33 lois de la Guerre
Robert Greene –
Ecrivain- 2007

ANNEXES

TABLE DES ILLUSTRATIONS

A PROPOS DE T-SYSTEMS, GROUPE DEUTSCHE TELEKOM

T-Systems apporte aux entreprises des plateformes pour porter leurs transformations numériques, back office, front office, connectivité et cyber sécurité. Nos solutions sont disponibles en mode pay per use, et sont disponibles immédiatement en mode opéré (PaaS) principalement, mais aussi en mode IaaS. Nous proposons des solutions de Cloud sur les principales solutions du marché. Nous sécurisons ses plateformes et aussi celles de nos clients en mode "Security as a Service" et leurs objets connectés. Nous concevons ces plateformes dans une approche best-of-breed, agnostique et avec architecture non stop et scalable par éléments.

En utilisant nos solutions, nos clients peuvent donc accélérer et sécuriser leur transformation digitale sur des plateformes mission-critical, agiles, faciles d'usage, hautement sécurisées et hébergées et opérées en Europe.

T-Systems opère plusieurs Security Operation Centers (SOC) pour ses propres besoins et ceux de ses clients.

Notamment :

- T-Systems analyse par jour un milliard d'évènements de sécurité depuis 3000 sources de donnés.
- T-Systems analyse par jour plus de 6 milliards d'enregistrements sur les serveurs DNS Deutsche Telekom pour l'inspection des cyber-attaques et plus de 10 Millions emails arrivant à Deutsche Telekom pour combattre les Spams.
- T-Systems analyse par jour plus que 6 millions attaques de cybersécurité sur son réseau honeypot déployé dans le monde.

T-Systems en chiffres :

- 7,9 milliards € de CA
- 43 700 employés dont 1200 experts sécurité avec plus de 25 années d'expérience dans les solutions et le conseil en sécurité informatique
- 10 500 spécialistes de la transformation des SI
- 140 000 m² de data centers, 20 data centers Twin Core en Europe, Asie, Amérique
- 46 000 systèmes Clouds opérés
- 1,355 million d'environnements de travail opérés à travers le monde

T-Systems France
110 rue Ambroise Croizat
93200 Saint Denis
+33 1 82 30 10 10
Info.france@t-systems.com

A PROPOS DE PAC

Fondé en 1976, Pierre Audoin Consultants (PAC) fait partie du CXP Group, premier cabinet européen indépendant d'analyse et de conseil dans le domaine des logiciels, des services informatiques et de la transformation numérique.

Il offre à ses clients un service complet d'assistance pour l'évaluation, la sélection et l'optimisation de solutions logicielles, l'évaluation et la sélection des ESN et les accompagne dans l'optimisation de leur stratégie de sourcing et dans leurs projets d'investissement. Ainsi, le CXP Group accompagne DSI et directions fonctionnelles dans leur transformation numérique.

Enfin, le Groupe CXP aide les éditeurs et les ESN à optimiser leur stratégie et leur go-to-market à travers des analyses quantitatives et qualitatives ainsi que des prestations de conseil opérationnel et stratégique. Les organisations et les institutions publiques se réfèrent également à nos études pour développer leurs politiques informatiques.

Capitalisant sur 40 ans d'expérience, implanté dans 8 pays (et 17 bureaux dans le monde), fort de 140 collaborateurs, le CXP Group apporte chaque année son expertise à plus de 1 500 DSI et directions fonctionnelles de grands comptes et entreprises du mid-market et à ses fournisseurs. Le CXP Group est composé de 3 filiales : le CXP, BARC (Business Application Research Center) et Pierre Audoin Consultants (PAC).

Pour plus d'informations : www.pac-online.com

Suivez-nous sur Twitter @PAC_FR

A CXP GROUP COMPANY

PAC - CXP Group
8, avenue des ternes
75017 Paris
Tel. : +33 (0)1 53 05 05 53
info-france@pac-online.com
www.pac-online.com

CLAUSE DE NON-RESPONSABILITE, DROITS D'UTILISATION, INDEPENDANCE ET PROTECTION DES DONNEES

Clause de non-responsabilité

Le contenu de cette étude a été élaboré avec le plus grand soin. Cependant, nous déclinons toute responsabilité quant à sa précision. Les analyses et évaluations reflètent l'état actuel de nos connaissances (Novembre-Décembre 2017) et peuvent changer à tout moment. Cela s'applique en particulier, mais pas uniquement, aux déclarations relatives au futur. Les noms et appellations qui apparaissent dans cette étude peuvent être des marques déposées.

Droits d'utilisation

Cette étude est protégée par les droits d'auteur. Toute reproduction ou communication de son contenu à des tiers, même en partie, requiert l'autorisation explicite préalable des sponsors. La publication ou diffusion de tableaux, graphiques, etc. dans d'autres publications requiert également une autorisation préalable.

Indépendance et protection des données

Cette étude est le fruit exclusif de la société Pierre Audoin Consultants (PAC). Les sponsors n'ont eu aucune influence sur l'analyse objective des données et la réalisation de l'étude.

Les participants à l'étude ont été assurés que les informations fournies par leurs soins seraient traitées de manière strictement confidentielle. Aucune déclaration ne permet de tirer des conclusions concernant des entreprises individuelles, et aucune donnée d'enquête individuelle n'a été communiquée aux sponsors ou à d'autres tiers. Les participants à l'étude ont été sélectionnés de manière aléatoire. Il n'existe aucun lien entre la réalisation de l'étude et une éventuelle relation commerciale entre les personnes sondées et les sponsors de l'étude.

A CXP GROUP COMPANY