CONCOURS EXTERNE / INTERNE D'INGÉNIEUR EN CHEF TERRITORIAL

SESSION 2023

Note de synthèse et de propositions visant à faire l'analyse du dossier remis au candidat portant sur un sujet technique

Option : Systèmes d'information et de communication

ÉPREUVES N° 5 & 10

Durée : 5 h
Coefficient : 5

SUJET :

Il y a à peine un mois, vous avez été recruté(e) comme directeur(trice) du numérique et des systèmes d'information (DNSI) pour la communauté d'agglomération de Saint-Pont l'Argone. La DNSI est mutualisée entre la ville et l'Établissement Public de Coopération Intercommunale (400 000 habitants).

Samedi matin (il y a 2 jours), les employés des services ouverts au public ne peuvent plus se connecter à leurs ordinateurs. Un message de demande de rançon s'affiche au démarrage de plus de 80 % des 3 500 PC de la collectivité.

L'équipe d'astreinte informatique vous a rapidement prévenu(e) et a mis en sécurité le système d'information. L'Agence Nationale de la Sécurité des Systèmes d'information a été prévenue et vous avez informé votre hiérarchie.

La situation qui vous est remontée est :

- la collectivité ne dispose ni d'un Plan de Reprise d'Activité, ni d'un Plan de Secours Informatique ;
- les principaux systèmes sont atteints et les documents sont chiffrés ;
- des sauvegardes régulières sont réalisées et non affectées par l'attaque ;
- la majorité des serveurs informatiques sont hors-service et seuls quelques systèmes sont épargnés ou sont encore à diagnostiquer (voir cartographie du système d'information et des zones « contaminées »),
- le système d'information « Smart City » qui contrôle les objets connectés et capteurs divers n'est pas géré par la DNSI *(réseaux basse consommation - LPWAN, Edge Computing, réseaux de capteurs sans fil – WSN)* mais par un opérateur extérieur. Ce système n'a pas été impacté par l'attaque.

Dans une première partie, vous rédigerez une note de synthèse à l'attention de Madame la Maire-Présidente et de son cabinet pour les informer de la situation et apporter quelques « éléments de langage » pour la communication externe.

Dans une seconde partie, vous rédigerez un dossier à l'attention du directeur général qui souhaite « connaître le plan de route des prochains mois, les moyens que vous allez mobiliser et l'organisation que vous allez mettre en place. ». Il souhaiterait aussi savoir comment la remise en état du Système d'information pourrait engager une démarche de Numérique Responsable.

Barème de notation :

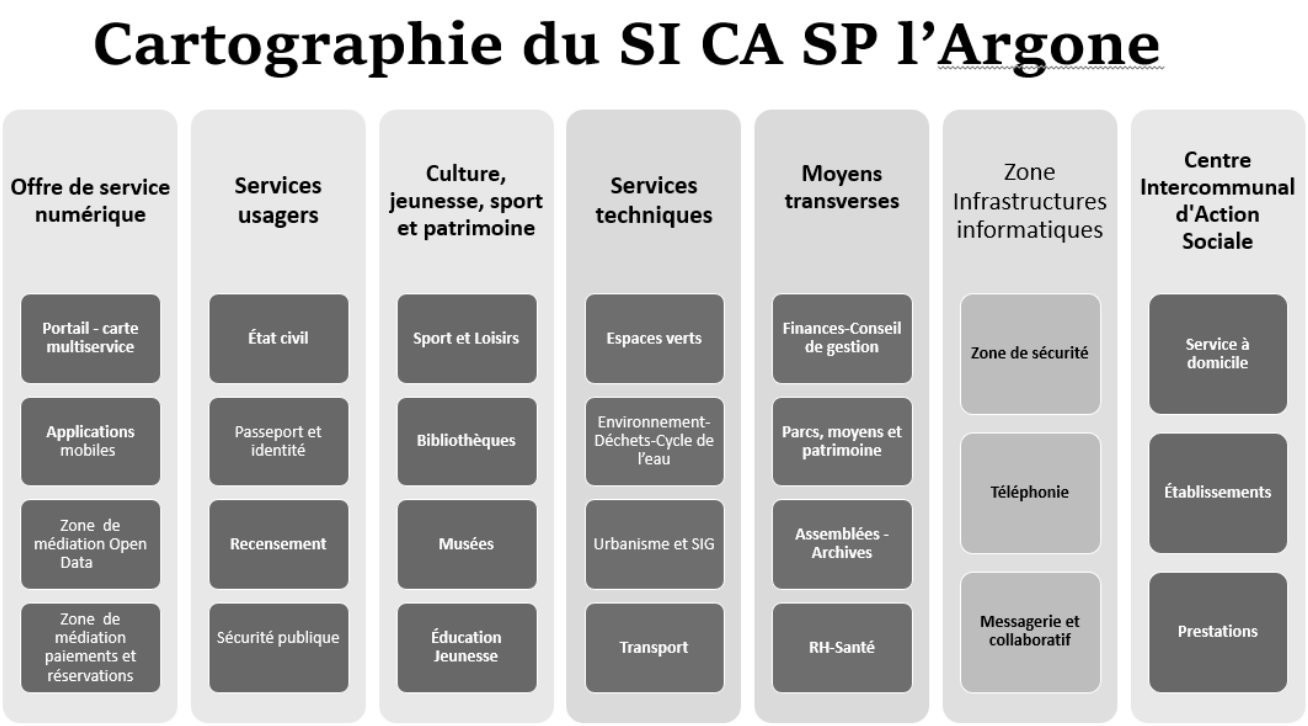
Note de synthèse : 10 points
Proposition pour un plan d'action : 10 points

DOCUMENTS JOINTS

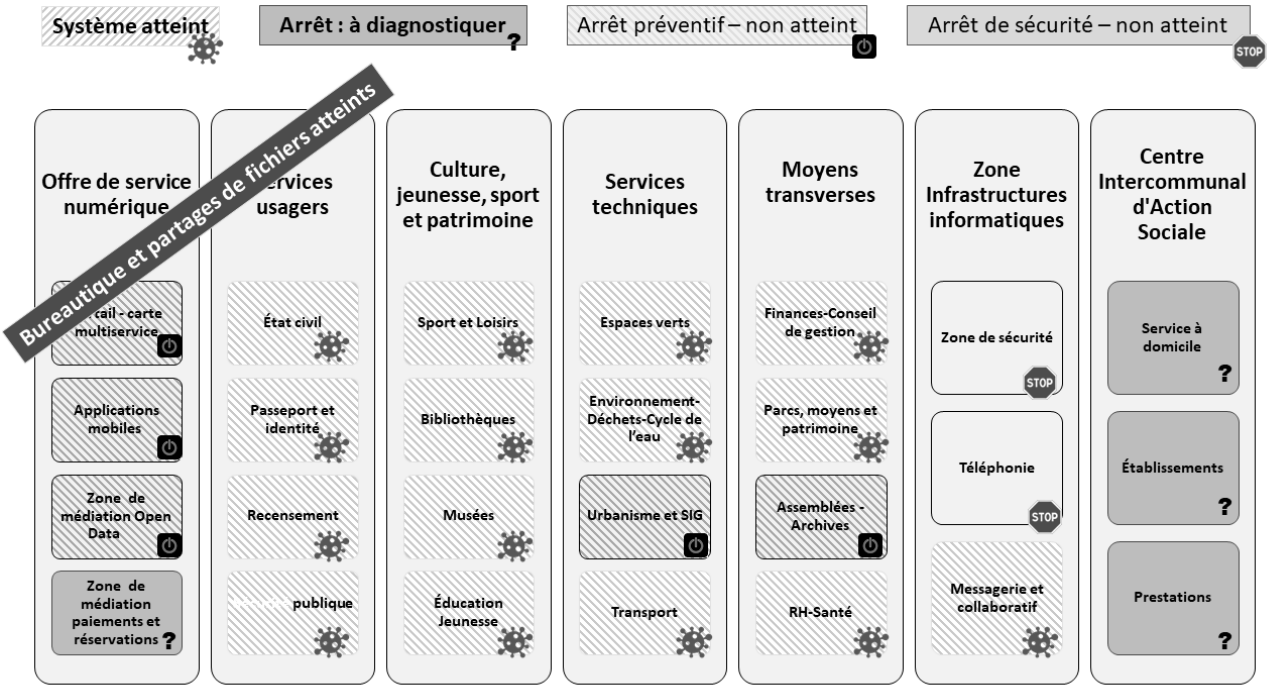
NOTA :

- 2 points seront retirés au total de la note sur 20 si la copie contient plus de 10 fautes d'orthographe ou de syntaxe.
- **Les candidats ne doivent porter aucun signe distinctif sur les copies** : pas de signature ou nom, grade, même fictifs.
- Les épreuves sont d'une durée limitée. Aucun brouillon ne sera accepté, la gestion du temps faisant partie intégrante des épreuves.
- Lorsque les renvois et annotations en bas d'une page ou à la fin d'un document ne sont pas joints au sujet, c'est qu'ils ne sont pas indispensables.

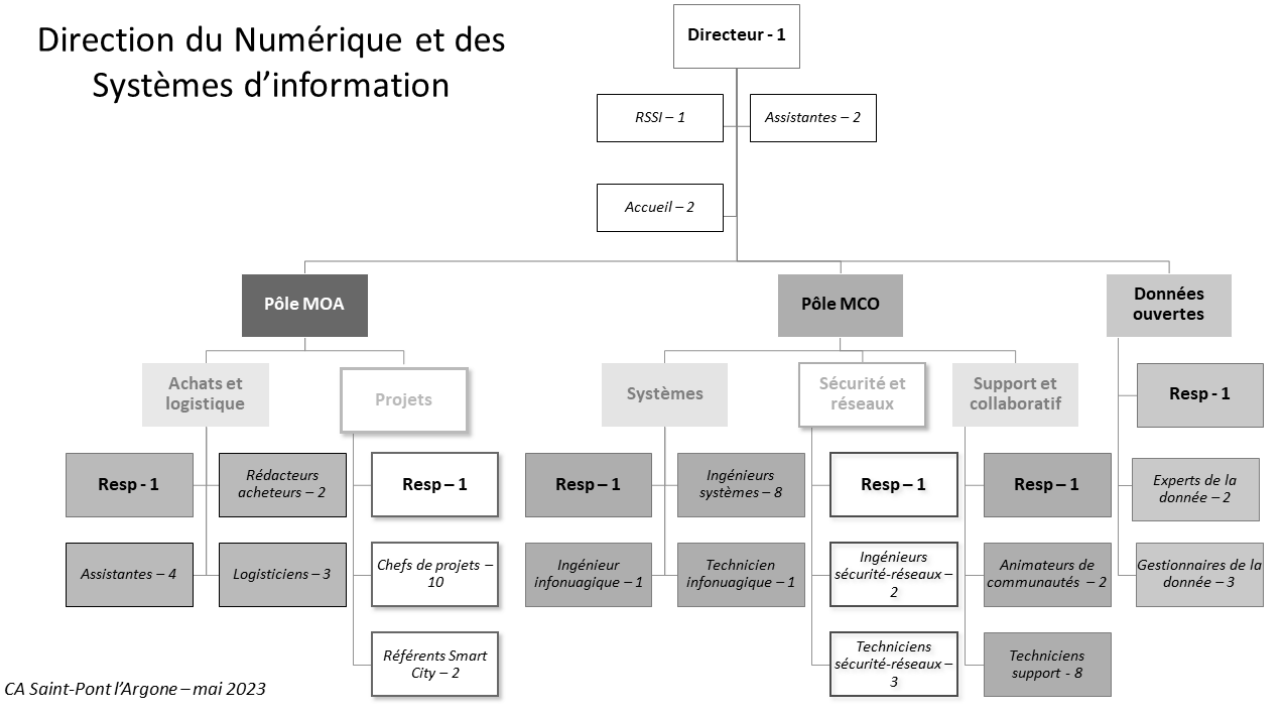
Document 1 : Cartographie simplifiée du système d'information de la collectivité.



Document 2 : Cartographie avec impacts après la cyberattaque.



Document 3 : Organigramme de la Direction du Numérique et des Systèmes d'information



Document 4 : Lemagit.fr – 1re partie – Construire un plan de sécurité (…)

22 mars 2017

Comment construire un plan de cybersécurité pour son entreprise

Le plan d'action de cybersécurité est un élément crucial de l'état de préparation à la cybersécurité. L'expert Peter Sullivan explique ce qui entre dans ces plans et comment en commencer un.

Être préparé à répondre aux incidents de sécurité est un état que chaque entreprise doit s'efforcer d'atteindre. Dans la première partie de cette série sur la préparation à la cybersécurité, un ensemble de sept objectifs fondamentaux a été détaillé. Cet article traite du premier élément de cette liste : le plan de cybersécurité.

Les objectifs du plan de cybersécurité

Pour atteindre un objectif quel qu'il soit, il est essentiel d'élaborer un plan d'orientation. La cybersécurité n'est pas différente de tout autre effort à cet égard. Dans ce contexte, la préparation à la cybersécurité est le but et un plan de cybersécurité est le premier de plusieurs objectifs.

Un plan de cybersécurité devrait décrire clairement ce qu'une organisation veut atteindre par rapport à la cybersécurité. Lorsque l'on se penche sur les types de problèmes informatiques et de sécurité réseau qui sont signalés chaque jour, certains éléments de planification de la sécurité apparaissent évidents. Voici des exemples d'objectifs de planification de la cybersécurité qui appuient la préparation à la cybersécurité :

1. Protéger la propriété intellectuelle, qui concentre la valeur et la force de différenciation de l'entreprise sur le marché, contre le vol par des acteurs malveillants internes ou externes à l'entreprise.
2. Protéger les informations personnelles des clients et des employés, ainsi que les informations régulées, contre le vol par des acteurs malveillants internes ou externes à l'entreprise.
3. Être capable de voir et de comprendre le contexte de sécurité de chaque paquet entrant et sortant du réseau d'entreprise. Être capable de surveiller et de comprendre quelles informations circulent, sortent du réseau et y transitent, et de savoir si ce flux d'information est souhaité ou indésirable, et approprié ou inapproprié.
4. Disposer d'un système de messagerie électronique offrant un niveau élevé de confidentialité, même en cas de vol de messages.

Sélectionner des objectifs

Chacun de ces quatre objectifs du plan d'action pour la cybersécurité pourrait et devrait être traité comme un projet avec un calendrier, des jalons, des mesures et des indicateurs. Les premier et deuxième objectifs partageront vraisemblablement plusieurs des mêmes contrôles et pratiques de sécurité. Le troisième objectif sera discuté en profondeur dans un prochain qui traite de l'architecture de sécurité et de la surveillance du réseau.

Dans cet article, la réalisation d'un système de courrier électronique confidentiel est développée comme un exemple d'un objectif pour un plan de cybersécurité. Il comprend l'identification de certains obstacles et des exemples d'indicateurs qui peuvent être utilisés pour mesurer les progrès accomplis dans la réalisation de l'objectif.

Messagerie confidentielle

L'objectif de la messagerie électronique confidentielle est réalisable grâce à l'utilisation du chiffrement des e-mails. Cette technologie existe depuis des décennies. Pourquoi alors, des emails volés de grandes sociétés, d'organismes gouvernementaux et de partis politiques sont-ils régulièrement divulgués sur WikiLeaks et sur des sites similaires ?

Le chiffrement, en particulier la cryptographie des infrastructures à clés publiques (PKI), n'est pas bien compris par les administrateurs systèmes. Il peut être difficile à mettre en œuvre correctement. Un effort d'administration très élevé peut être à fournir, et l'ensemble peut s'avérer coûteux. Si un système de chiffrement est mal géré, de grandes quantités d'informations peuvent être perdues. Ce sont là quelques-unes des raisons qui militent contre son utilisation.

Une préoccupation particulière de la PKI est que si toutes les personnes qui ont besoin de recevoir des emails chiffrés ne disposent pas de leur propre paire de clés, elles ne peuvent pas participer à des conversations sécurisées par courrier électronique. Pour les grandes organisations où la majorité du courrier électronique est échangée entre membres de l'organisation, ainsi que dans les organismes gouvernementaux, militaires et de renseignement, les coûts associés à la PKI peuvent en valoir la peine. Pour ces organisations, l'avantage de chiffrer automatiquement, déchiffrer et stocker en toute sécurité chaque message électronique est un avantage.

Il existe d'autres outils disponibles, moins coûteux et plus faciles à administrer, surtout si ce ne sont pas tous les messages qui doivent être chiffrés. Ces autres options sont essentiellement des services de messagerie Web où le destinataire d'un message crypté peut avoir besoin de se connecter à un portail de messagerie sécurisé pour lire le courrier électronique chiffré qui lui a été adressé. Les destinataires peuvent avoir besoin de s'inscrire sur ce portail et de configurer les informations d'authentification, mais aucune paire de clés de PKI n'est requise. Les problèmes liés au courrier électronique sécurisé incluent le fait de garantir que le courrier est chiffré au repos sur le serveur et non pas seulement dans le transport, que le fournisseur de messagerie chiffrée déchiffre ou non votre courrier électronique. Mais il faut aussi compter avec la complexité à introduire dans l'organisation un nouveau système de messagerie électronique que les utilisateurs devront adopter. Et qui les conduira à choisir quoi chiffrer et quoi ne pas chiffrer…

Il existe des systèmes de passerelle de courrier électronique qui peuvent analyser du courrier électronique non chiffré avant l'envoi, rechercher des mots clés et des motifs spécifiques - tels que des numéros de sécurité sociale et des informations de carte de crédit - et envoyer des courriels alors identifiés comme sensibles à un système de messagerie sécurisé. Ce système a l'avantage de fonctionner avec n'importe quel système de messagerie électronique. Mais il induit une surcharge administrative liée à la création des règles de filtrage de contenu. Dans ce système, seuls les e-mails identifiés par les filtres de contenu seront sécurisés et rien ne garantit que chaque e-mail qui doit être sécurisé le sera bien.

Il existe également des systèmes de chiffrement de courrier électronique plus simples utilisant des extensions de messagerie électronique et des clés de secret partagées symétriques, où la même clé est utilisée pour le chiffrement et le déchiffrement. Là encore, l'utilisateur doit décider quels messages électroniques doivent être chiffrés et il y a également le problème d'échange et de gestion de la clé secrète partagée. Dans le passé, l'échange de clés secrètes était l'un des problèmes que la cryptographie à clé publique devait résoudre. De nos jours, il peut être tout aussi facile de partager une clé secrète par SMS ou tout autre méthode utilisant un canal de communication secondaire.

Mesures et indicateurs

Une fois qu'un plan de sécurité approprié est établi pour le courrier électronique, une façon d’évaluer l'efficacité du produit ou du service utilisé doit être déterminée. De toute évidence, cela ne pas se faire sur la base de la quantité d'informations non perdues grâce au système de sécurité retenu. Mais il existe des moyens simples de montrer les progrès par rapport à l'objectif de confidentialité du courrier électronique.

Un indicateur simple peut être par exemple le volume total des courriels envoyés par jour, semaine ou mois. Un indicateur montrant les progrès accomplis dans la réalisation de l'objectif de cybersécurité montrerait la quantité de courrier électronique envoyé crypté, en pourcentage de tous les courriers électroniques envoyés.

Document 5 : Lemagit.fr – 2e partie – Construire une architecture de sécurité (…)

31 mars 2017

Construire une architecture de sécurité de l'information pas à pas

La préparation à la cybersécurité nécessite une architecture de sécurité robuste. L'expert Peter Sullivan explique quelles briques de base sont essentielles à cela.

Être préparé à répondre aux incidents de sécurité est un état que chaque entreprise doit s'efforcer d'atteindre. Dans la première partie de cette série sur la préparation à la cybersécurité, un ensemble de sept objectifs fondamentaux a été détaillé. La seconde partie a été consacrée au premier élément de cette liste : le plan de cybersécurité.

Précédemment, l'architecture de sécurité de l'information a été décrite comme une architecture de sécurité permettant de contrôler le réseau supportant les communications locales, étendues et distantes, d'en comprendre le fonctionnement, et d'en assurer la surveillance.

L'architecture est la façon dont les composants d'une chose s'organisent. S'agissant d'un système d'information en réseau, l'objectif est d'organiser et d'exploiter ce système de manière à pouvoir le contrôler le système et à détecter des activités inattendues, indésirables et malveillantes.

Passerelle sécurisée

Si le trafic qui s'écoule dans, hors et au travers d'un réseau ne peut pas être vu, il ne peut pas être surveillé. Pour éviter cela, le trafic doit traverser un environnement de passerelle maîtrisé. Les grandes entreprises peuvent ne pas avoir une bonne gestion du nombre de points d'accès à Internet utilisés. La direction générale fédérale américaine a par exemple identifié plus de 8 000 connexions à Internet parmi ses différentes agences - dont la plupart n'ont pas été surveillées par un centre opérationnel réseau ou sécurité. Ce qui représente une vulnérabilité majeure pour le l'administration américaine. La situation idéale est d'avoir une seule passerelle pour concentrer et surveiller le trafic.

La passerelle Internet sécurisée devrait fournir les services suivants :

- Pare-feu pour fournir inspection des paquets et contrôle d'accès ;
- Système de détection/prévention d'intrusion (IDS/IPS) ;
- Service proxy applicatif pour les protocoles http/https, smtp, ftp, etc. ;
- Filtrage du spam ;
- Filtrage antivirus et logiciels malveillant ;
- et Analyse du trafic réseau.

Pare-feu

Si recommander l'utilisation d'un pare-feu peut paraître dépassé et trop évident, rappelez-vous ceci : le Sony PlayStation Network et les services de jeux en ligne Sony Online Entertainment ont été compromis en 2011, perdant les données personnelles de plus de 100 millions d'utilisateurs. Les réseaux affectés n'étaient pas protégés par des pare-feu.

Du point de vue de l'architecture de la sécurité de l'information, un pare-feu peut être considéré comme un périphérique qui assure l'implémentation de la politique de sécurité, et

en particulier la politique d'accès. La présupposition est qu'une politique de contrôle d'accès périmétrique - si c'est là qu'est placé le pare-feu - a été définie et documentée. Sans une politique de contrôle d'accès définie qui sert de guide pour la configuration du pare-feu, l'implémentation du pare-feu risque de ne pas fournir le niveau de service de sécurité requis par l'organisation.

Détection et prévention des intrusions

Disposer d'un IDS ou d'un IPS est essentiel dans une architecture de passerelle sécurisée. Généralement, l'IDS/IPS s'appuie sur une base de données de signatures pour détecter les intrusions potentielles ou les violations de la politique de sécurité, comme l'utilisation de protocoles non autorisés. La base de données de signatures dans un IDS est comparable à celle utilisée dans un système de détection de virus, notamment en cela qu'il ne produira aucune alerte pour une signature d'intrusion absente de sa base de données. Celle-ci doit donc être mise à jour régulièrement, tout comme avec un système de détection de logiciels malveillants.

À chaque service, son proxy

Tous les protocoles applicatifs qui traversent la passerelle doivent passer par un service de proxy bidirectionnel complet afin d'être surveillés efficacement. Cela commence par le courrier électronique (Smtp, Imap, Pop) et les protocoles Web (HTTP, HTTPS). La majorité du trafic réseau devrait être couverte. Une analyse de bande passante permettra d'identifier d'autres protocoles applicatifs utilisés dans l'organisation, tels que FTP et SSH. Faire transiter ces protocoles via un service proxy bidirectionnel complet fournira une visibilité supplémentaire et la possibilité de surveiller les informations et les fichiers entrant et sortant du réseau. Ces services proxy incluent :

Proxy de messagerie

Les appliances proxy de messagerie peuvent filtrer le spam, effectuer des recherches de virus et contrôler les pièces jointes et les liens HTML. Le contenu actif et le code mobile peuvent également être filtrés par un service proxy. Le courrier électronique peut également être analysé dans une perspective de prévention des fuites de données.

Proxy Web

Un service de proxy Web devrait fournir un filtrage bidirectionnel pour les protocoles http et https en fonction de l'adresse IP et/ou de l'URL, y compris le filtrage des liens et du code actif intégrés dans les pages Web. Le filtrage de contenu et de mots clés devrait également être utilisé dans le cadre d'un service proxy Web. L'accès à un courrier électronique externe via une interface Web - une option de choix pour l'exfiltration de données - peut être surveillé ou bloqué.

Antivirus, antimalware et blocage de spam

Si elle n'est pas fournie ailleurs, dans le cadre d'un serveur proxy par exemple, la détection des virus et des logiciels malveillants, et le blocage des courriers indésirables, doivent être fournis dans la passerelle sécurisée. Bien qu'il soit possible d'effectuer une analyse antivirus et un blocage des courriers indésirables sur les postes de travail, identifier ces menaces aussi tôt que possible avant leur entrée dans l'environnement de confiance est préférable.

Analyse du trafic réseau

L'analyse du trafic du réseau informatique repose sur la collecte et l'analyse des flux IP. Cette analyse est extrêmement utile pour comprendre le comportement du réseau : l'adresse source permet de comprendre qui produit le trafic ; l'adresse de destination indique qui reçoit le trafic ; les ports donnent des indications sur l'application liée au trafic ; la classe de service examine la priorité du trafic, etc.

À l'aide de ces informations, il est possible de déterminer des profils comportementaux qu'il sera possible de considérer comme normaux, pour ensuite identifier les comportements inattendus ou indésirables, y compris les comportements malveillants. Par exemple, si un utilisateur commence à transférer de grandes quantités de données par courrier électronique vers l'extérieur l'entreprise, il serait possible de détecter ce comportement avec l'analyse du trafic réseau.

Document 6 : Agence Nationale de la Sécurité des Systèmes d'Information – infographie

Les collectivités face aux enjeux de cybersécurité – Cadre réglementaire applicable.

Avril 2021

Les rançongiciels (*ransomware* en anglais) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.
Source : ***www.cybermalveillance.gouv.fr***

QUELS SONT LES IMPACTS ?

DIRECTS

Vol de données, chiffrement des données, interruption des services administratifs durant plusieurs jours voire plusieurs semaines.

INDIRECTS

Coûts financiers de rétablissement des services numériques, atteinte à la réputation, conséquences juridiques, etc.

QUE FAUT-IL PROTÉGER ?

DES DONNÉES

Données d'état civil, données personnelles liées aux prestations sociales, données financières, etc.

DES SERVICES

Services en ligne de paiement de contravention, de déclaration d'imposition, de cantine scolaire, d'inscription scolaire, etc.

DES SYSTÈMES & DES INFRASTRUCTURES

Systèmes d'information et de communication, réseaux d'énergie, etc.

En 2020, les signalements d'attaques par rançongiciel ont été multipliés par 3,5 par rapport à 2019. Toutes les collectivités sont concernées, quelle que soit leur taille.
Source : ANSSI

ÉVOLUTION DU CADRE RÉGLEMENTAIRE

MAI 2010 *(revisé en 2014)*

Le référentiel général de sécurité (RGS) fixe le premier cadre français de la confiance numérique pour les téléservices et au sein de l'administration.

DÉCEMBRE 2013

La loi de programmation militaire (LPM) garantit la protection des activités d'importance vitale.

AVRIL 2016 (entré en vigueur le 25 mai 2018)

Le Règlement général sur la protection des données (RGPD) responsabilise les acteurs publics et privés quant à la protection des données personnelles.

JUILLET 2016

La directive *Network and Information Security* (NIS) garantit la protection des services essentiels au sein de l'Union européenne.

OCTOBRE 2016

La loi pour une République numérique (LRN) introduit de nouvelles dispositions relatives à l'*Open data* et confirme les dispositions du RGPD en matière de protection des données personnelles.

QUELS SONT LES OBJECTIFS DE CES RÉGLEMENTATIONS ?

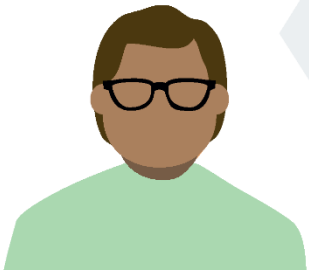
Renforcer la confiance des usagers dans les services numériques.

Garantir la protection des données personnelles et des infrastructures qui les hébergent.

Renforcer la sécurité des activités d'importance vitale et des services essentiels.

SAISISSEZ-VOUS DE L'ENJEU CYBER !

Les collectivités territoriales sont responsables de la sécurité des données qu'elles traitent et de leurs services numériques vis-à-vis des autorités et des citoyens.



Les normes de cybersécurité et de protection des données instaurent une **logique de prévention des risques**. Elles impliquent une mise en conformité permanente et dynamique. Les collectivités doivent donc démontrer qu'elles offrent un niveau optimal de protection.

QUELLES SONT LES MESURES GÉNÉRALES À METTRE EN PLACE ?

À SÉCURISER : TÉLÉSERVICES
TEXTE RÉGLEMENTAIRE ASSOCIÉ : RGS

- ✓ Analyse de risques et définition des mesures de sécurité adaptées aux enjeux et aux menaces
- ✓ Homologation de sécurité du téléservice
- ✓ Suivi opérationnel et amélioration continue

À SÉCURISER : DONNÉES PERSONNELLES
TEXTE RÉGLEMENTAIRE ASSOCIÉ : RGPD

- ✓ Nomination d'un délégué à la protection des données
- ✓ Établissement d'un registre de traitement
- ✓ Analyse d'impact lorsqu'un traitement peut impliquer un risque élevé pour les droits et les libertés des personnes concernées
- ✓ Mise en place des clauses relatives à la protection des données personnelles avec ses fournisseurs et ses sous-traitants
- ✓ Notification des violations de données personnelles

À SÉCURISER : SYSTÈMES D'INFORMATION D'IMPORTANCE VITALE OU ESSENTIELS
TEXTES RÉGLEMENTAIRES ASSOCIÉS : LPM & DIRECTIVE NIS

- ✓ Définition d'une politique de sécurité des systèmes d'information
- ✓ Cartographie des systèmes d'information
- ✓ Analyse de risques des activités d'importance vitale ou des services essentiels
- ✓ Homologation des systèmes d'information
- ✓ Audit de sécurité

Des services et des produits qualifiés par l'ANSSI permettent de répondre à certaines exigences règlementaires comme celles du RGS : ***www.ssi.gouv.fr/administration/visa-de-securite***

LES FONDAMENTAUX POUR PROTÉGER SES SERVICES NUMÉRIQUES

SOCLE DE SÉCURITÉ
« MESURES D'HYGIÈNE INFORMATIQUE »

Exemples : sauvegardes régulières, gestion des droits d'accès, gestion des mots de passe, dispositifs de chiffrement, cloisonnement des réseaux, application des correctifs et des mises à jour et détection des incidents.

POUR FAIRE LA DIFFÉRENCE

- Nommer un responsable de la sécurité numérique
- Organiser des formations régulières au bénéfice des agents
- S'entraîner à la gestion d'incidents de type rançongiciel

- Mettre en place des clauses de sécurité avec ses fournisseurs et ses sous-traitants
- Mettre en place un dispositif de gestion de crise et de continuité d'activité en cas de sinistre
- Adhérer à un dispositif de supervision et de réponse à incident

POUR ALLER PLUS LOIN

- *Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation,* ANSSI, 2020.
- Kit de sensibilisation, **www.cybermalveillance.gouv.fr**
- *Cybersécurité : toutes les communes et intercommunalités sont concernées,* Association des maires de France et des présidents d'intercommunalités, 2020.
- *Guide de sensibilisation au RGPD pour les collectivités territoriales,* CNIL, 2019.
- *Attaques par rançongiciels, tous concernés,* ANSSI, 2020.
- Prestataires de sécurité : le label ExpertCyber, **www.cybermalveillance.gouv.fr**
- *Guide pratique pour une collectivité et un territoire numérique de confiance,* Banque des territoires, 2020

Version 1.0 - Avril 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 007 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr

Document 7 : Le Journal du Net – Comment les architectures cloud se protègent-elles (…)

16 juin 2021

Comment les architectures cloud se protègent-elles contre la vague de cyberattaques ?

À mesure que nous nous dirigeons vers un monde post pandémique, de plus en plus d'entreprises investissent dans le renforcement de leur cyber résilience. En effet, l'année 2020 a été marquée par un nombre record d'attaques par déni de service distribué (DDoS) et de ransomwares. Des chiffres qui devraient continuer de croitre jusqu'à la fin de la décennie.

Le cloud et les architectures natives du cloud peuvent contribuer à la résilience grâce à trois attributs clés. Premièrement, les applications et services distribués : si les applications tirent parti d'un modèle de distribution, par exemple des services basés sur le cloud tels que les réseaux de diffusion de contenu (CDN), les entreprises sont moins exposées aux attaques DDoS. En effet, ces attaques fonctionnent mieux lorsqu'elles concentrent leur puissance dans une seule direction. Dans un second temps, lorsque les applications utilisent des solutions qui ne modifient pas les enregistrements, mais qui les ajoutent à l'écriture, cela rend l'ensemble des données immuable. De fait, les organisations ont moins à se soucier des attaques visant l'intégralité de ces données car il est alors plus facile de les détecter et de les remonter. On retrouve pour finir les charges de travail éphémères. Pour les entreprises ayant recours à des applications éphémères par nature, il n'y a plus de risque que les attaquants établissent une résistance et se déplacent latéralement. De plus, la valeur des informations confidentielles est réduite, car ces actifs sont simplement mis hors service et de nouveaux sont instanciés dans un laps de temps réduit.

En exploitant les architectures cloud native modernes qui sont distribuées, immuables et éphémères, les entreprises peuvent venir à bout des problèmes de confidentialité, d'intégrité et de disponibilité qui sont à la base de la trilogie de la cybersécurité. Comment les organisations mettent-elles ces attributs en évidence dans leurs applications ? Les architectures cloud modernes passent de modèles monolithiques à plusieurs niveaux à des architectures distribuées basées sur des microservices, où chacun peut évoluer indépendamment, dans une région géographique ou entre régions. Par ailleurs, chaque microservice dispose de son propre stockage et de sa propre base de données optimisés pour fonctionner sans état (ou, plus précisément, en utilisant un modèle d'état partagé dans lequel ce dernier est partagé entre les instances en cours d'exécution via la couche de stockage/base de données). Ainsi, ces services peuvent devenir véritablement éphémères et distribués.

Le concept « Pets vs. Cattle »

On en arrive à un concept qui a déjà fait l'objet de nombreuses discussions dans le domaine du cloud computing : Pets vs. Cattle. D'un côté les animaux domestiques (pets) ont de beaux prénoms et peuvent être reconnus individuellement. Lorsqu'ils tombent malades, leurs propriétaires les emmènent chez le vétérinaire. Les propriétaires s'occupent de leurs animaux toute leur vie et veillent à ce qu'ils vivent en bonne santé le plus longtemps possible. On peut comparer les applications traditionnelles à des animaux de compagnie. Chaque instance est unique. Si l'application est infectée, elle est emmenée chez le cyber-vétérinaire. Mettre en place une procédure de correctif est courant avec les applications traditionnelles,

ce qui rend ces instances uniques. Le travail des équipes IT consiste à maintenir les applications en état de marche le plus longtemps possible.

De l'autre côté, le bétail (cattle) quant à lui n'a pas de nom, mais il est identifié par des numéros. En général, il n'est pas possible de distinguer les bovins d'un troupeau et il n'est pas possible de nouer des relations avec ces derniers. En cas de maladie ou d'infection, c'est tout le troupeau qu'il faut abattre. Les applications modernes sont comme le bétail. Les services sont créés sous forme d'un grand nombre d'instances en cours d'exécution, et chacune est indiscernable des autres. On ne fait jamais de correctifs sur place, c'est-à-dire qu'on ne personnalise jamais les instances. Il incombe aux équipes IT de rendre les instances éphémères, en les détruisant rapidement pour en créer de nouvelles. Ce faisant, ils construisent des systèmes résilients et non des systèmes fragiles.

Les avantages du cloud computing

Le cloud offre de nombreux outils permettant de construire des systèmes qui suivent ce paradigme. Par exemple, Amazon a annoncé en fin d'année dernière une "ingénierie du chaos" as-a-service, qui permet aux organisations d'introduire des éléments perturbateurs dans leurs charges de travail de production, comme l'arrêt d'instances en cours d'exécution. Ceci garantit que les performances globales ne sont pas affectées et que les charges de travail deviennent, au fil du temps, résilientes face à ce type de perturbations opérationnelles.

Arriver à ce stade constitue un long voyage et les entreprises doivent adopter plusieurs mesures pour y parvenir. Par exemple, faire passer ses applications physiques au cloud sans modifier de manière significative l'architecture des applications, n'est qu'une étape. Le terme courant pour désigner cette opération est "lift and shift". Une fois que ces applications sont dans le cloud et que les entreprises ont commencé à se familiariser avec les outils cloud native, elles peuvent s'atteler à la réarchitecture de ces applications dans des architectures modernes, distribuées, immuables et éphémères. En d'autres termes, elles peuvent passer du statut d'animaux domestiques au sein du cloud à celui de bétail dans le cloud. Une fois arrivé à ce stade, les organisations doivent veiller à ne pas faire marche arrière et éviter de mettre en place des correctifs ou de maintenir des instances en fonctionnement plus longtemps que nécessaire.

Document 8 : actu.fr - Bondy : la facture s'élève à 1,5 million d'euros

12 juillet 2022

Bondy : la facture s'élève à 1,5 million d'euros pour la Ville

Après la cyberattaque de novembre 2020, la Ville de Bondy (Seine-Saint-Denis) estime que le préjudice s'élève à 1,5 million d'euros. Elle doit encore rattraper des factures.

La facture est salée. Un an et demi après la cyberattaque qui a touché les serveurs de la Ville de Bondy **(Seine-Saint-Denis),** les effets s'en font toujours ressentir. Dans un entretien accordé au *Parisien,* le maire, Stephen Hervé (LR), révèle que l'attaque a coûté au total 1,5 million d'euros à la Ville.

Pas de retour à la normale avant 2023

Pour remettre sur pied la municipalité de 1 600 agents, la Ville a dû renouveler l'ensemble de son matériel informatique, reconstituer l'ensemble des données dérobées et installer de nouveaux logiciels. Le coût total de l'opération est évalué à 1,5 million d'euros.

Les effets se font aussi ressentir sur la gestion des ressources de la Ville. Pendant plusieurs mois, les salaires ont été versés avec quelques jours de retard. Aujourd'hui encore, la Ville doit rattraper les factures de la cantine et du périscolaire des mois précédents. Dans un courrier adressé aux parents d'élèves, elle annonce qu'elles seront envoyées au rythme « d'une toutes les trois semaines » afin d'effectuer le rattrapage. Elle espère un retour à la normale d'ici 2023.

Document 9 : usine-digitale.fr – Assurance : un projet de loi (…)

07 septembre 2022

Assurance : un projet de loi clarifie le cadre de l'indemnisation des rançons en cas de cyberattaque

La Direction générale du Trésor a rendu son rapport sur la couverture assurantielle du risque cyber au ministre de l'Économie, qui a donné son feu vert au remboursement des rançons par les assureurs. Un projet de loi du ministère de l'Intérieur obligeant les entreprises à porter plainte pour pouvoir en bénéficier est présenté ce mercredi en conseil des ministres.

Comme nous l'expliquions il y a peu dans nos colonnes, une grande partie des assureurs continuent de rembourser les rançons, dans le cadre de sinistres résultant d'une cyberattaque par rançongiciel, si les entreprises respectent certaines conditions. Mais il manquait une clarification du cadre juridique, qui pouvait en rebuter certains, comme Axa France et Generali.

Le retour du projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) – un premier texte avait été présenté en mars sous l'ancienne mandature -, en conseil des ministres ce mercredi 7 septembre, devrait y remédier. Il intègre une mesure dédiée aux cyber-rançons, imposant aux entreprises de déposer plainte sous 48 heures pour pouvoir être indemnisées. Ce qui valide du même coup la légalité du remboursement de la rançon.

D'après une étude de France Assureurs réalisée en 2022, sept assureurs sur dix proposent le remboursement des rançons dans leurs contrats d'assurance cyber dédiés aux TPE/PME.

Le trésor présente un plan d'action pour l'assurance cyber

Cette mesure est issue des travaux de la direction générale du Trésor, qui a mis en place à la demande du ministre de l'Économie Bruno Le Maire, en juin 2021, un groupe de travail sur le développement de la couverture assurantielle des risques cyber. Le Trésor a remis son rapport aujourd'hui.

Celui-ci présente un plan d'action pour améliorer la couverture des entreprises contre les cyberattaques. Si 84% des grandes entreprises sont assurées contre ce risque, moins le 0,3% des PME le sont en France selon l'Association pour le management des risques et des assurances de l'entreprise (Amrae), alors que 54% des entreprises françaises auraient fait l'objet d'une cyberattaque en 2021 d'après le baromètre de la cybersécurité en entreprise CESIN 2022. Les cotisations de ces polices d'assurance ne représentent que 3% des cotisations en assurance dommage des professionnels.

Une task force mise en place fin septembre

Le plan d'action de la DGT recommande notamment de clarifier les clauses de ces contrats, de retenir le principe d'inassurabilité des sanctions administratives, de créer à moyen terme une branche cyber dans le Code des assurances (pour mieux piloter statistiquement et budgétairement l'activité), et de créer une plateforme public-privée de partage de données anonymisées sur les incidents cyber, afin de disposer de davantage de données sur ce risque pour que les assureurs puissent mieux le mesurer, et de faciliter les enquêtes judiciaires. Ces données pourraient être issues entre autres des dépôts de plainte des entreprises.

La DGT précise dans un communiqué qu'un "task force dédiée à l'assurance du risque cyber, associant les acteurs concernés, sera mise en place d'ici la fin du mois de septembre".

Bercy souhaite une mise en œuvre rapide

"Ce rapport propose des actions concrètes et crédibles pour développer un marché de solutions assurantielles, tout en renforçant la prévention du risque cyber. Il est issu d'une

large concertation avec l’ensemble des acteurs concernés : fédérations d’entreprises, assureurs, experts du monde académique et superviseurs. Je souhaite que ces orientations soient mises en oeuvre le plus rapidement possible", commente Bruno Le Maire dans un communiqué.

Selon les données de la police et de la gendarmerie citées par le rapport du Trésor, la valeur médiane des rançons atteignait 6375 euros en France en 2020 (+50% par rapport à 2016). Retenir la valeur médiane est intéressant, car la valeur moyenne est faussée par les grandes disparités des rançons réclamées, qui peuvent atteindre plusieurs millions d'euros.

Document 10 : Le Journal du Net - L'architecture Zero Trust

16 juin 2021

L'architecture Zero Trust : bouclier de la sécurité des entreprises

Cette technologie figure parmi les plus explorées par les équipes IT et constitue l'alternative aux anciennes approches centrées sur la sécurité périmétrique indique Philippe Alcoy, de Netscout.

Selon le dernier rapport sur les priorités de sécurité conduit par la société Foundry, le Zero Trust est de plus en plus plébiscité par les entreprises, pour lutter contre les cybermenaces. Cette technologie figure parmi les plus explorées par les équipes IT et constitue l'alternative aux anciennes approches centrées sur la sécurité périmétrique. Il ressort ainsi qu'un tiers des organisations ont un modèle Zero Trust en place ; l'intention d'en déployer est passée à 21 % en 2022 contre 13 % en 2021. Face à des vecteurs d'attaques toujours plus variés et plus nombreux, les équipes IT doivent absolument renforcer la sécurité de leurs structures.

Selon l'ANSSI, « le Zero Trust est une approche architecturale selon laquelle la confiance inhérente au réseau est supprimée, le réseau est supposé hostile et chaque demande est vérifiée sur la base d'une politique d'accès ». Cette approche consiste au contraire à réduire la « confiance implicite » accordée aux utilisateurs et aux activités menées par le biais des équipements d'une entité donnée. Divers facteurs sont nécessaires pour qu'une demande soit considérée comme digne de confiance, notamment l'autorisation, l'accès à des données sensibles, l'authentification forte et le bon état de l'appareil.

Qu'est-ce que le modèle Zero Trust ?

Les principes de conception du Zero Trust qui ont été intégrés par l'ANSSI constituent une nouvelle approche pour résoudre un problème auquel les entreprises sont confrontées de longue date : la sécurisation des informations et des réseaux. Ainsi, les entreprises d'un large éventail de secteurs reconsidèrent leur approche de la sécurité et intègrent des éléments de type Zero Trust dans leur architecture, leurs processus et leurs procédures de sécurité.

L'authentification multi-factorielle (MFA) est un exemple de principe Zero Trust. En exigeant l'application de facteurs supplémentaires pour prouver l'identité des utilisateurs avant qu'ils ne puissent accéder à une ressource – par exemple, le contrôle de leur empreinte digitale ou la confirmation d'un code PIN envoyé à leur appareil mobile – la MFA ajoute une couche supplémentaire de sécurité aux réseaux et aux systèmes. Du point de vue du Zero Trust, la MFA est utilisée pour vérifier les mesures de sécurité d'une organisation, afin de s'assurer que les personnes ayant accès au réseau sont bien celles qu'elles prétendent être. Ce niveau de sécurité réduit considérablement les possibilités pour les cybercriminels d'utiliser des informations d'identification compromises afin d'accéder aux données, dispositifs, réseaux et systèmes d'une entreprise.

Construire un domaine sûr et sécurisé

Le modèle Zero Trust peut être envisagé comme un groupe de piliers qui représentent différents aspects de la sécurité, des dispositifs aux réseaux, en passant par les applications et les utilisateurs. Cependant, sous ces piliers se trouvent les éléments fondamentaux d'une architecture Zero Trust : l'analyse, l'automatisation, la gouvernance et la visibilité.

Par ailleurs, le processus du modèle Zero Trust est réputé comme continu et régulier. Au départ, les entreprises affinent généralement leurs architectures, en veillant à ce que leurs solutions soient presque totalement intégrées dans les piliers susmentionnés. Cela leur

permet de prendre des décisions plus rapidement et plus efficacement au regard de la mise en œuvre des politiques.

Bien que l'installation et la construction d'un modèle Zero Trust soient chronophages, la mise à niveau des politiques, des processus et des outils se révèle très positive pour l'architecture, à condition qu'elle bénéficie d'une vérification et d'un audit permanents. Ces actions sont indispensables pour garantir la solidité et l'efficacité des mesures de sécurité en place.

Surveiller pour mieux protéger

Le modèle Zero Trust ne s'accompagne d'aucun faux sentiment de sécurité : il s'agit d'une sécurité « sans périmètre ». Elle est très différente des architectures traditionnelles périmétriques, où tout ce qui se passe à l'intérieur du réseau est considéré comme digne de confiance, sur le principe que pour se trouver dans le réseau, les utilisateurs doivent avoir franchi avec succès l'étape de l'authentification et sont donc autorisés à s'y trouver. Or, ce modèle considère que les initiés ne représentent aucune menace potentielle pour l'organisation et que la sécurité du périmètre est irréprochable. À l'inverse, l'architecture Zero Trust met l'accent sur la protection contre les éventuelles menaces internes, empêchant ainsi les cybercriminels d'accéder au système en utilisant des informations d'identification compromises.

Assurer une visibilité réseau de bout en bout

Dès lors qu'une entreprise décide de mettre en œuvre un modèle Zero Trust, afin d'en garantir l'efficacité, elles doivent intégrer plusieurs caractéristiques essentielles : une visibilité complète de l'ensemble du réseau, des TAP réseaux capables de reproduire le trafic à partir du flux, ainsi qu'un outil à même de répliquer et de distribuer les paquets aux applications de surveillance de la cybersécurité préexistantes.

Une visibilité à grande échelle permettra en effet aux organisations de repérer la moindre activité inhabituelle, d'identifier les menaces éventuelles, de suivre les dispositifs interconnectés, d'observer l'historique des utilisations et d'orchestrer les mesures d'atténuation par l'intermédiaire d'interfaces de programmation d'applications (API). Elles devraient également être en mesure d'utiliser des groupes de protection afin de classer les réseaux, les serveurs et les services en fonction du degré potentiel de dommages qu'ils pourraient subir. Les organisations seront ainsi en position de force pour adopter rapidement un modèle Zero Trust.

En somme, quelle que soit l'étape à laquelle se trouve une organisation dans son parcours de mise en œuvre de cette approche – qu'elle soit en phase de lancement ou déjà bien avancée – il est impératif de veiller à ce que l'analyse et la visibilité fassent partie intégrante de la détection et de la validation de la conception qui sous-tend l'architecture Zero Trust. Dans une conjoncture où les entreprises sont en friction constante face aux cybermenaces, des stratégies de renforcement de la sécurité du réseau sont cruciales.

Document 11 : La Gazette des communes - Lille, la crise informatique s'installe après la cyberattaque

24 mars 2023

À Lille, la crise informatique s'installe après la cyberattaque

La ville de Lille a déploré une fuite de données après l'attaque informatique dont elle a été victime à la fin février, et quatre agents ont même reçu des demandes de rançon. Une cyberattaque qui se traduit toujours par un travail en mode dégradé.

Trois semaines après l'intrusion informatique repérée à la fin février, la crise s'installe en mairie de Lille. Alors que la collectivité estimait dans un premier temps "ne pas avoir constaté de difficultés sur les données hébergées" sur ses serveurs, la piste d'une fuite de données a finalement été confirmée en fin de semaine dernière. La collectivité a en effet déploré l'exfiltration de données, dont certaines à caractère personnel.

Une très mauvaise nouvelle : avec le chiffrement de données, le vol de données est le sinistre le plus redouté par les organisations victimes d'une intrusion informatique. On ne connaît pas le volume des données volées lors de cette attaque, toujours pas revendiquée, ni leur nature exacte, le diagnostic technique de l'attaque étant toujours en cours.

Prudence informatique

"C'est une forte attaque informatique, on ne peut pas le nier", résume toutefois auprès de La Gazette des communes le député (Nupes) Roger Vicot, ancien maire de Lomme, commune associée à Lille également touchée par la cyberattaque. Ce qui oblige donc les services de la ville à reprendre étape par étape leur informatique pour repartir sur des bases saines. À titre de comparaison, l'agglomération et la ville de Caen, victimes d'une intrusion informatique à la fin septembre, avaient mis quatre mois pour rétablir la majorité de ses services en ligne.

Quatre salariés de la ville ont également reçu sur leur messagerie personnelle un message de demande de rançon. On ignore là aussi les montants demandés, ainsi que les modalités précises de la tentative d'extorsion.

Un dernier point, rassure Roger Vicot, qui n'a pas suscité "de craintes particulières" chez les agents de la collectivité à ce sujet.

L'attaque informatique a par contre contrarié brutalement les habitudes de travail, observe le député. "L'informatique et internet ont pris une place prédominante dans le travail quotidien", rappelle-t-il. Alors que les adresses de messagerie des élus et des agents sont toujours désactivées, il faut donc apprendre à travailler autrement.

Services dégradés

Cette remise en cause des habitudes et des facilités du numérique vaut aussi pour les usagers. L'envoi de documents par mail est toujours impossible, la collectivité appelant à déposer au guichet des dossiers papier ou à appeler les services concernés.

Autre conséquence de la cyberattaque : la billetterie est toujours sévèrement entravée. La carte bancaire restant proscrite, faute d'informatique, la mairie a désormais limité les moyens de paiement pour accéder aux équipements municipaux, des musées aux piscines, aux espèces et au chèque bancaire.

Enfin, si la mairie a rétabli l’accès à des services essentiels tels que l’état-civil ou la demande de papiers d’identités, moyennant des procédures revenues au papier-crayon, les services des bibliothèques sont toujours très perturbés. Certes, les prêts viennent tout juste d’être rétablis. Mais les retours, réservations et inscriptions sont toujours suspendus, tout comme l’accès à la bibliothèque numérique. Pour emprunter le prochain ebook, il va falloir s’armer de patience.

Document 12 : radiologie.fr- Cyberattaques : le cloud = solution ou

risque 20 janvier 2023

Cyberattaques : le cloud est-il une solution ou un risque ?

La cybersécurité est importante pour les données de santé car ces données sont particulièrement sensibles et peuvent être utilisées à des fins malveillantes comme pour des escroqueries financières, de la discrimination dans le cadre d'une assurance ou d'un emploi, et même pour des actes de terrorisme. Les attaques informatiques peuvent également entraîner des perturbations importantes pour les soins médicaux, en perturbant l'accès aux données médicales et en causant des retards dans la prise en charge des patients (cf. article précédent sur les cyberattaques en milieu hospitalier).

Les organisations hospitalières peuvent être exposées à de nombreuses failles de cybersécurité, qu'il y ait ou non des outils cloud utilisés. Citons les plus courantes :

- **Les systèmes d'exploitation et les logiciels non mis à jour** : Les systèmes d'exploitation et les logiciels obsolètes ne bénéficient plus des dernières mises à jour de sécurité, ce qui les rend vulnérables aux attaques.
- **Les mots de passe faibles ou partagés** : Les mots de passe faibles ou partagés facilitent la tâche des cybercriminels pour accéder aux systèmes.
- **Le manque de contrôle d'accès** : Les systèmes de contrôle d'accès mal configurés ou inadéquats permettent à des personnes non autorisées d'accéder aux données sensibles.
- **La perte ou le vol d'équipements** : Les ordinateurs portables, les téléphones mobiles et les autres appareils contenant des données sensibles peuvent être volés ou perdus, exposant ainsi les données à des risques de fuites.
- **Les réseaux mal configurés** : Les réseaux mal configurés peuvent permettre aux cybercriminels d'accéder aux systèmes et aux données sensibles.
- **Les attaques de phishing et de rançongiciels** : Les employés d'une organisation hospitalière peuvent être victimes d'attaques de phishing ou de rançongiciels, qui peuvent entraîner des fuites de données ou des perturbations des systèmes.

De plus en plus d'outils en Imagerie médicale, que ce soit des PACS, des plateformes de données de santé ou des outils de post traitements en Imagerie **utilisent des solutions cloud** et nous sont proposés sous cette forme.

Le cloud computing peut être utilisé comme une solution pour se protéger contre les cyber-attaques, mais il peut également être considéré comme un risque si les mesures de sécurité appropriées ne sont pas mises en place.

Les avantages de l'utilisation de la technologie cloud pour les hôpitaux et les utilisateurs sont nombreux, notamment la flexibilité, la scalabilité et l'accès aux données depuis n'importe où. Cependant, il est important de **veiller à ce que les données soient correctement protégées** lorsqu'elles sont stockées sur des serveurs cloud externes.

Il est essentiel de choisir **un fournisseur de cloud sécurisé adaptée à la législation du pays d'où proviennent les données** (question de gouvernance sur les données en santé) et de s'assurer que les données sont chiffrées lors de la transmission et du stockage. Il est également important de mettre en place des politiques et des procédures de sécurité appropriées pour protéger les données contre les cyberattaques.

En outre, les hôpitaux doivent s'assurer que **les fournisseurs de cloud respectent les normes de conformité,** telles que le RGPD pour les données médicales en Europe, et de l'HIPAA aux États-Unis.

Il est donc possible d'utiliser des outils cloud pour les hôpitaux tout en garantissant un bon niveau de sécurité. Il est important de mettre en place une **stratégie de cybersécurité efficace pour minimiser les risques pour les données sensibles des patient**s.

Nous avons rencontré Thomas SALNOT directeur Système Informatique Olea, et Mathieu JEANDRON (Amazon Web Service AWS) qui travaillent ensemble pour proposer aux utilisateurs radiologues français notamment, un accès cloud des solutions Olea, la suite de cet article se rapporte à notre entretien ainsi qu'à un travail de synthèse sur la question du cloud et de cybersécurité.

Les fournisseurs de cloud, tels qu'AWS, mettent en place de **nombreuses protections pour protéger les données de santé stockées sur leurs plateformes**. Ces points peuvent être une aide pour la cybersécurité :

- **Chiffrement** : les fournisseurs cloud offrent des options de chiffrement pour protéger les données stockées sur ses serveurs, ainsi que pour les données en transit. Les données sont chiffrées à l'aide de clés de chiffrement gérées par le client ou gérées par AWS.
- **Contrôle d'accès** : ils utilisent un système de contrôle d'accès pour garantir que seules les personnes autorisées puissent accéder aux données de santé. Il permet de gérer les utilisateurs, les groupes et les autorisations.
- **Audit et conformité** : Ils fournissent des outils pour aider les clients à se conformer aux normes de conformité, telles que HIPAA aux États-Unis, et RGPD en Europe. Ils permettent de surveiller les activités sur les comptes, pouvant noter des activités inhabituelles à risque et lancer une procédure de sécurisation en cas d'attaque suspectée.
- **Protection contre les attaques** : les fournisseurs cloud utilisent une série de mesures pour protéger les données de santé contre les attaques, notamment les pare-feu, les systèmes de détection et de prévention des intrusions (IDS/IPS), et la protection contre les DDoS.
- **Sauvegarde et récupération** : Ils proposent des options de sauvegarde et de récupération pour les données de santé, y compris la sauvegarde automatique des données, ainsi que des options de récupération après sinistre pour les données critiques.

Inconvénients :

- **Les mécanismes de protection des données dans le cloud sont d'une nature différente de celle sur site**, et il est important que le fournisseur de systèmes de santé dans le cloud mette en œuvre les pratiques à l'état de l'art en termes de protection contre les attaques extérieures.
- Si les données sont stockées dans le cloud par des prestataires étrangers, il est important de vérifier si ces derniers **respectent les réglementations et les normes de confidentialité et de sécurité applicable à votre pays**.

- Si les utilisateurs ne prennent pas les mesures de sécurité appropriées pour protéger leurs comptes et leurs informations d'identification, ils peuvent devenir des cibles de cyber attaque. Il faut donc un **travail en lien avec le département des services informatiques** pour mettre en place un environnement sécurisé, également lors de l'utilisation de solutions cloud.

En résumé, le cloud computing peut être une solution pour se protéger contre les cyber-attaques si les mesures de sécurité appropriées sont mises en place. Il est donc important de bien sélectionner son fournisseur de cloud, de s'assurer que les données sont protégées conformément aux normes de sécurité et de confidentialité et de mettre en place une stratégie de cybersécurité efficace pour minimiser les risques pour les données sensibles, impliquant une somme de mesures à mettre en place en lien avec le département des services informatiques.

Myriam EDJLALI-GOUJON, pour la SFR

Document 13 : Mega.com- La contribution de l'Architecture d'entreprise

durable 25 juin 2022

La contribution de l'Architecture d'entreprise durable

Qu'est-ce que la durabilité ?

La définition écologique de la durabilité provient du rapport Brundtland rédigé en 1987 et décrit le développement durable comme un mode de développement qui répond aux besoins du présent sans compromettre les capacités des générations futures à répondre aux leurs. Une entreprise durable est robuste, capable de résister aux forces disruptives d'un monde changeant, sans pour autant mettre en péril les ressources, humaines et matérielles, nécessaires pour survivre.

La santé durable de l'entreprise n'est pas limitée à son unique résilience et optimisation. Elle consiste à adopter un point de vue holistique qui instaure un équilibre pérenne avec son environnement, en constante évolution. Au-delà de la performance financière, de la gestion des risques et de la conformité réglementaire, la durabilité implique d'adopter les standards éthiques les plus élevés et de démontrer son intégrité au regard de la société, de l'économie et de l'environnement.

Comment l'architecture d'entreprise contribue-t-elle au développement durable ?

Pour débuter, nous allons enfoncer quelques portes ouvertes en mettant en exergue que l'application de fondamentaux d'architecture d'entreprise, comme la gestion des processus et l'Architecture IT, dynamise la progression vers l'installation d'une entreprise durable. Une entreprise responsable qui s'appuie sur une architecture durable intègre les critères de **Responsabilité Sociale d'Entreprise** (RSE) **à chaque niveau architectural** : stratégie et prise de décision, processus organisationnels, y compris la logistique et les environnements de travail, gestion de portefeuille informatique et conception/évolution du système d'information.

La pratique de l'architecture d'entreprise accompagne la transformation économique et numérique des organisations en apportant la visibilité requise du fonctionnement de l'entreprise : quelle organisation, avec quel système d'information, avec quels objectifs, etc. Elle permet aussi d'identifier les opportunités d'amélioration et de formaliser les initiatives de transformation ayant un impact positif dans la durée.

Vers une architecture métier durable

Le point de départ de la gestion d'entreprise est la **réalisation d'une carte des capacités centrée sur la valeur métier**. Celle-ci a pour vocation de mettre en exergue les différents objectifs de l'organisation et les résultats attendus pour les clients. Cela ne signifie pas ajouter une capacité « durabilité » pour autant mais que chaque objectif en tient compte de manière transversale. Les chaînes de valeur des opérations et le système d'information servent cette stratégie d'entreprise. Avec pour finalité d'installer des comportements durables dans la culture d'entreprise.

Une absence de vision « durable » génère du gaspillage, de mauvaises pratiques et des échecs éventuels. La gouvernance, les processus et les politiques internes sont utilisés pour communiquer sur les meilleures méthodes et peuvent être consignés dans un rapport de développement durable. Sont par exemple concernés : la due diligence, la gestion du cycle de vie des matériaux, l'approvisionnement, la sécurité informatique, les procédures de

dénonciation et l'optimisation du stockage des données. Réaliser la cartographie de la chaîne de valeur permet de visualiser le cycle de vie d'un produit. Une illustration serait par exemple de considérer le décommissionnement de machines dans un processus de clôture (offboarding) d'un projet.

Pour une gestion durable du portefeuille informatique

Comment rationaliser nos ressources informatiques et par conséquent notre impact sur la planète ? L'optimisation du système d'information passe par une prise de conscience de l'état des déploiements et des usages existants, via l'inventaire. En ce qui concerne l'évaluation du portefeuille informatique, elle peut non seulement reposer sur des critères de coûts ou de fiabilité technologique, mais aussi sur la valeur métier, une couverture fonctionnelle optimisée, ainsi que des données d'investissements Environnementaux, Sociaux et de Gouvernance (ESG).

Lors de l'intégration des risques associés à la prise de décision, l'entreprise prend en compte non seulement les éléments de RSE, mais aussi les notations de durabilité des fournisseurs via un score Ecovadis par exemple. Cela passe aussi par l'impact environnemental des technologies et le déploiement de solutions « cloud » reposant de plus en plus sur l'utilisation d'énergies propres.

Pourquoi une architecture applicative durable ?

C'est sur l'informatique que reposent aujourd'hui nombre de nos activités humaines. Intégrer la sobriété dans les projets informatiques et le design des produits est un engagement important pour contribuer à préserver la planète. Selon The Shift Project : « La consommation d'énergie du numérique est aujourd'hui en hausse de 9 % par an. Il est possible de la ramener à 1,5 % par an en adoptant la « Sobriété numérique » comme principe d'action. » Les démarches d'éco-conception et de « Green IT » permettent de réduire l'impact sur l'environnement. Selon l'AFNOR, « l'éco-conception consiste à intégrer l'environnement dès la conception d'un produit ou service, et lors de toutes les étapes de son cycle de vie ».

Cela permet de rationaliser et moderniser le SI de manière vertueuse, de sa création à son exploitation à travers 3 principes clés :

1. **Se focaliser sur la valeur client** : Tout ce qui n'apporte pas de valeur métier réelle ne doit être ni développé, ni livré. Cela s'applique à la fois à l'interface visible par l'utilisateur et au noyau technique de la plate-forme. Plusieurs études - Cast Software and Standish Group - montrent que **70% des fonctionnalités demandées par les utilisateurs ne sont pas essentielles et que 45% ne sont jamais utilisées.** Un environnement de planification et de collaboration en mode agile permet de cerner les exigences métier, de se concentrer sur les besoins primaires et d'éviter de développer des fonctionnalités superflues.
2. **Définir des principes de design sobre** pour une meilleure optimisation des ressources et de la performance du code.
3. **Passer à des architectures d'applica**tion consommant moins d'énergie et d'espace. Ce qui signifie mettre en place des solutions permettant des approches modulaires pour mutualiser les infrastructures. Utiliser les API Web permet d'échanger uniquement les informations nécessaires.

Les entreprises florissantes de demain pratiquent l’architecture d'entreprise durable aujourd’hui

Construire un avenir meilleur bâti sur des normes écologiques nécessite de s'adapter, de repenser nos habitudes et de moderniser nos méthodes et nos technologies. **L'architecture d'entreprise aide à développer les capacités d'apprentissage d'une organisation pour la faire évoluer avec son environnement.** L'architecture d'entreprise soutient les initiatives de transformation RSE en cassant les silos pour rassembler les parties-prenantes autour d'objectifs communs - dont le développement durable. Ce qui recouvre des fonctions aussi différentes que les gestionnaires des risques, les architectes, les chefs de projet, les propriétaires d'applications, les équipes qualité et d'amélioration des processus, ainsi que les équipes dirigeantes.

La RSE peut être un fil conducteur pour la mise en place d’une stratégie de gestion qui tienne compte de **la rentabilité, des risques et de l’impact** de l’entreprise. Les entreprises durables qui réussissent établissent une feuille de route qui assure un équilibre entre ce qui est bon pour les clients, pour l'entreprise et pour l'avenir de tous sur la planète.

Ces entreprises envisagent leur transformation vers un écosystème durable comme une source de vitalité, d'innovation et d'inspiration. Elles bénéficient en plus d'une efficacité accrue, de produits et de services de qualité améliorée et d'une meilleure image auprès de leurs clients et collaborateurs.

Leslie ROBINET - MEGA International

Document 14 : La gazette des Communes - Numérique responsable : comment verdir les collectivités ?

14 décembre 2022

Numérique responsable : comment verdir les collectivités ?

L'association les Interconnectés a fait halte pour son intercoTour à Rouen, mardi 13 décembre. L'occasion de faire le point sur le numérique responsable et sur les ingrédients à réunir pour une transformation numérique réussie.

« Le numérique responsable fait partie des priorités fixées par les engagements métropolitains », a rappelé Nicolas Mayer-Rossignol, maire PS de Rouen et président de la Métropole Rouen Normandie, à l'occasion d'une journée de l'Intercotour à Rouen, organisée par les Interconnectés mardi 13 décembre.

Les actions engagées par la collectivité sont déjà nombreuses : signature de la charte numérique responsable, formation des agents, en liaison avec le CNFPT, structuration de la filière Reboot pour reconditionner et réutiliser les ordinateurs de la collectivité, et une labellisation « numérique responsable » visée pour l'an prochain. « L'impact du numérique sur le réchauffement climatique est parfois sous-estimé, tout comme la fracture numérique sur l'accès aux services publics. Il faut qu'on arrive à en faire ensemble l'un des moteurs un des enjeux principaux du changement de société qu'on est en train d'impulser », a-t-il déclaré.

Et ce chantier s'insère dans une réalité sous tension car marquée ces derniers mois par des cyberattaques à de multiples échelles : « le CHU de Rouen en 2019, Caen en septembre, le département de Seine-Maritime dans lequel des agents ne peuvent toujours pas travailler, et la région depuis quelques jours », a contextualisé Jonas Haddad, conseiller régionale délégué au numérique à la région Normandie, qui a assuré : « nous allons faire de ces crises des opportunités pour avoir une vraie filière de cybersécurité », assurant que la collectivité souhaite devenir pilote en matière de politique de cybersécurité.

Un haut comité pour accélérer le verdissement du numérique

Du côté de l'État, Pierre Colle, chef de projet numérique responsable à l'ANCT, a pu apporter plusieurs éclairages sur les chantiers en cours. Le 14 novembre dernier, les ministères de l'environnement et du numérique ont créé le haut comité au numérique écoresponsable, marquant la « volonté de l'État d'accélérer et de donner du sens aux initiatives réduisant l'impact environnemental du numérique », a-t-il déclaré En effet, les acteurs sont nombreux (Dinum, Ademe, Cerema, ANCT, Arcep, collectivités, entreprises) et les chantiers multiples : les nouvelles obligations imposées par la loi REEN, telle que l'élaboration d'une stratégie numérique responsable, sur laquelle les Interconnectés travaille avec l'Institut du numérique responsable et l'ANCT à la rédaction d'un guide, la feuille de route numérique et environnement, la stratégie d'accélération pour le verdissement du numérique actuellement en préparation. Plusieurs groupes de travail ont été mis en place, autour des terminaux afin d'en réduire l'impact environnemental (80% de l'empreinte des équipements venant de leur production), des data center et du cloud, de la sobriété et des usages, des réseaux.

Le but est de lancer début 2023 un appel à manifestation d'intérêt lié à la stratégie d'accélération pour le verdissement du numérique, une formalisation des engagements pris par les différentes parties d'ici mars, la publication en avril d'une feuille de route de décarbonation du secteur, avant un premier point d'étape en juin.

Deux expérimentations pilotes

De plus, l'ANCT a également lancé une expérimentation avec 6 collectivités pilotes, entre novembre et janvier prochain, pour définir leurs stratégies numériques responsables. « Le but est aussi de voir si un accompagnement plus vaste, à l'échelle nationale, est nécessaire pour généraliser la rédaction de ces stratégies dans les collectivités », a précisé Pierre Colle. Les collectivités pilotes sont : Valence, Evry-Courcouronnes, Saint Quentin, la CA du Pays ajaccien, la CA du Grand Chambery, et la CA de Niort.

Enfin, avec ces 6 collectivités et 4 autres collectivités supplémentaires qui restent à déterminer, une deuxième expérimentation sera lancée début janvier pour 6 mois dans le cadre d'un partenariat entre l'ANCT et le Cerema sur une méthodologie d'audit des cas d'usages autour des territoires connectés et durables. « L'objectif sera de mettre cette démarche à disposition en accès libre sur la plateforme de l'ANCT pour que chacun puisse s'en emparer et ait un meilleur impact environnemental et un meilleur rendement en matière de numérique », a précisé Pierre Colle.

Focus - Modernisation et inclusion

Sur le volet du déploiement du numérique en interne et en externe, les retours d'expérience ont aussi été éclairants sur l'ampleur et la transversalité du sujet : « aujourd'hui à la ville de Rouen, 16 000 comptes ont été créés, on compte environ 35 000 foyers, donc au moins un tiers, voire la moitié des habitants ont créé un compte sur le site de la ville. Cela passe souvent par les écoles, l'inscription à la cantine, aux activités périscolaires. Cela reflète combien ce n'est pas un détail ou un gadget, mais un élément essentiel de fonctionnement », a déclaré Matthieu de Montchalin, adjoint au maire de Rouen. Qui a dans ce cadre rappelé la responsabilité de la mairie de « ne jamais oublier ceux qui ne peuvent pas, ne savent pas, n'ont pas les moyens, pour se connecter. Une des difficultés est de pousser le numérique sans jamais oublier ceux qui en sont exclus », a-t-il insisté.

Lors d'une autre table-ronde, Marie Blondel, directrice de la délégation Normandie au CNFPT mais précédemment en poste à la ville de Rouen pour moderniser la relations usagers et la simplification des démarches, a elle aussi rappelé qu' « on aurait tort de sous-estimer la nécessité de conserver une relation humaine en service public. » Ce que la collectivité a tenu à faire en créant un guichet unique physique, en organisant la montée en compétence de ses agents sur la polyvalence de leurs prestations. « On n'a jamais supprimé de postes en guichets, il est important de le rappeler, on sortait d'une période de restriction des effectifs de l'Etat dans ses accueils et d'un transfert de charge vers les collectivités », a-t-elle souligné.Les porteurs de projets sont sensibilisés sur la démarche écoresponsable et le rôle des architectes est clé, notamment afin de promouvoir la réutilisation de ressources existantes dans les nouveaux projets. « L'architecte a une vue plus globale sur le système d'information : il va voir comment ces différents projets se mettent en place, comment ceux-ci vont pouvoir utiliser des capacités identiques, même si, bien entendu, chaque projet doit être personnalisé. Il ne faut pas réinventer la roue à chaque fois et réutiliser un maximum de choses existantes. Et par rapport à cette approche, s'appuyer sur la modularisation, la réutilisation et le décommissionnement sont des axes sur lesquels nous agissons pour diminuer l'empreinte carbone du groupe. »