SERVICE PUBLIC

LA CYBERSÉCURITÉ

DANS UN AVENIR PLACÉ SOUS LE SIGNE DU « TOUT-NUMÉRIQUE »

Document de synthèse réalisé par ORACLE
visant à engager le débat et susciter les réactions

AVANT-PROPOS

La fonction publique a-t-elle les outils et les moyens pour relever les nouveaux défis que l'avenir lui réserve en matière de sécurité informatique ? À l'heure où les administrations, organismes et collectivités sont invités à penser « tout-numérique » et à mettre en ligne de nouveaux canaux d'interaction avec les usagers, la mutation perpétuelle des menaces de cybersécurité engendre de nouveaux risques et de nouveaux enjeux.

La rigueur budgétaire étant toujours de mise, il est essentiel de bien cerner l'évolution de cet environnement pour prendre les bonnes décisions d'investissement en matière de protection et de sécurité informatique. Alors que le coût du cybercrime augmente à une vitesse vertigineuse, les organismes publics doivent respecter une réglementation européenne de plus en plus contraignante en matière de divulgation des violations de sécurité. Certes, l'ANSSI apporte des éléments de réponse sous la forme de guides de bonnes pratiques, mais ces dernières augmentent d'autant le fardeau de la conformité.

Ce document présente l'importance des fondations d'une sécurité véritablement efficace, qui non seulement quadrille le périmètre du réseau, mais permet également la protection de la base de données. La sécurité des bases de données, associée à la validation des identités et à la gestion des accès, assure une défense en profondeur. Elle suit pour cela une approche dite « *inside-out* », qui commence par la protection du principal objet de convoitise des cybercriminels : les données. De fait, toute demande d'accès à ces données est soumise à une authentification et une autorisation rigoureuses. Sans oublier le chiffrement, qui protège les données à tout moment, tant au sein de la base de données que sur le réseau. Il est même possible de les brouiller pour les rendre commercialement inexploitables après une violation de sécurité, accidentelle ou délibérée (utilisateur interne ou administrateur de base de données non autorisé, ou par injection SQL d'un élément extérieur, etc.)

APPROFONDIR LA PROTECTION DES DONNÉES SELON UNE APPROCHE « *INSIDE-OUT* »

Une approche intégrale et approfondie de la cybersécurité dans les services publics non seulement facilite la démarche de conformité, mais assure également d'autres fonctions, comme le partage en toute sécurité des données si nécessaire. Lorsqu'il est bien appliqué, l'étiquetage des données au moyen d'informations juridictionnelles appropriées facilite le partage de ces données avec les autorités étrangères. Dans un même ordre d'idée, le masquage des données, par rédaction et randomisation automatique des informations d'identification personnelle, permet de respecter les réglementations sur la protection des données.

À mesure que les services publics investissent la sphère Internet, la mobilité et les réseaux sociaux, l'évolution permanente des menaces ne cesse de complexifier la sécurité informatique. C'est pourquoi les stratégies de cybersécurité doivent s'adapter en conséquence. Or, la formation et la sensibilisation à la sécurité vont de pair avec les investissements techniques. Cette approche holistique permet aux administrations et collectivités de minimiser les risques, de respecter les réglementations et directives voire, dans le meilleur des cas, …

… de mener une investigation informatique légale et d'identifier les facteurs responsables. La sécurité requiert une attention de tous les instants. De même, il ne suffit plus de se contenter d'un simple dispositif de sécurité périmétrique, autour d'un noyau de personnes réputées fiables. L'heure est à l'adoption de solutions destinées à consolider la sécurité à tous les échelons.

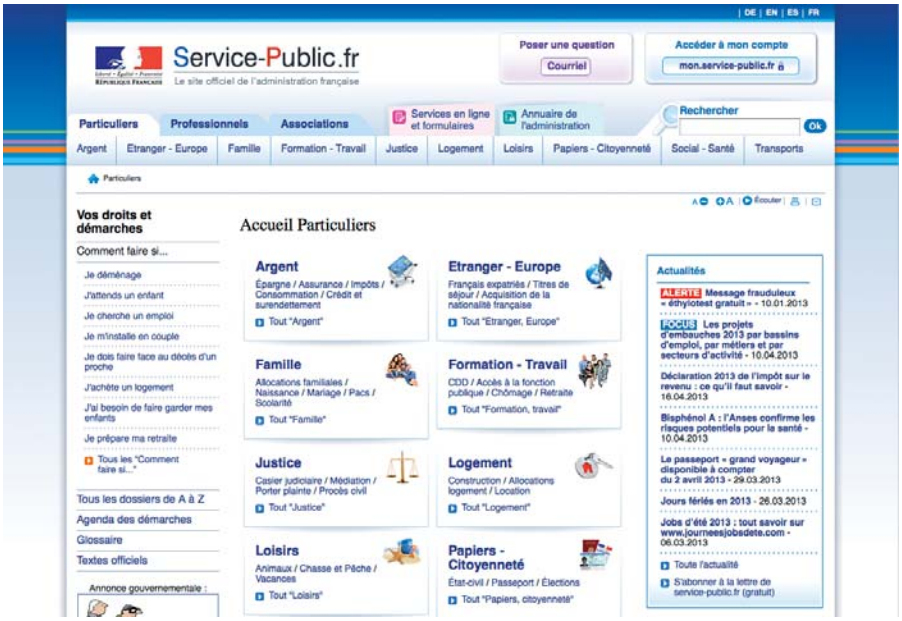
Alors que, sous l'impulsion des technologies Web et mobiles, les organismes publics poursuivent leur transition vers le « *tout-numérique* », ce document dresse un tour d'horizon des considérations, risques et réponses qui leur sont propres. Son objectif : aider les décideurs et responsables à mieux saisir les besoins et les enjeux de la cybersécurité, approfondir la protection des données selon une approche « *inside-out* » et formaliser un cadre de stratégies de sécurité informatique en phase avec les réalités présentes et futures. ■

À l'heure où l'administration et les services publics dépendent de plus en plus de l'informatique, on assiste en parallèle à l'émergence de coûts et de risques qui augmentent la pression sur les spécialistes en sécurité informatique et imposent des investissements urgents dans de nouveaux domaines. Les salariés et les usagers de la fonction publique s'accordent sur une chose : la sécurité des informations est vitale. Toutefois, si le public se préoccupe principalement de ses propres données personnelles, la dimension réelle du problème est bien plus étendue. Face à des menaces externes en perpétuelle mutation, les informaticiens du service public doivent non seulement veiller à la sécurité absolue de leurs environnements, mais aussi faire preuve de la plus grande vigilance face aux risques d'attaques extérieures. Sans compter qu'ils doivent aussi composer avec des budgets de plus en plus restreints et justifier tout investissement informatique, non seulement en termes de faisabilité technique mais aussi de rentabilité. C'est pourquoi ils doivent parfaitement cerner l'ampleur des coûts et des risques en présence, tout en se faisant une idée précise des éléments indispensables à la création de tels environnements sécurisés.

TOUT-NUMÉRIQUE : NOUVEAUX RISQUES, NOUVEAUX COÛTS

Le « *tout-numérique* », tel qu'il transparaît dans des initiatives publiques de type service-public.fr[1], a fait son chemin dans la réflexion des instances publiques autour des TIC. Aujourd'hui, toutes les collectivités locales, territoriales et organismes publics sont incités à faire du Web le point d'interface prioritaire avec les usagers et administrés : cet aspect essentiel de la stratégie des pouvoirs publics a pour but d'assurer un service public à moindre coût et d'optimiser l'usage des TIC dans une optique d'efficacité opérationnelle et budgétaire.

Mais comme toute médaille a son revers, on assiste en parallèle à l'émergence de nouveaux risques et de nouveaux coûts. La cybersécurité se situe au cœur de cette problématique. Dans un pays comme le Royaume-Uni, on estime à 27 milliards de livres Sterling le coût annuel de la fraude pour l'économie[3], dont 2,2 milliards touchent directement les caisses de l'État (la fraude fiscale essentiellement). À 79 £, le coût par enregistrement individuel connaît une hausse de 68 % sur les cinq dernières années, d'après une étude annuelle sur les violations de sécurité au Royaume-Uni[4].



Au niveau de la Commission européenne, la résistance s'organise avec l'ouverture en janvier 2013 d'un nouveau centre baptisé EC3[5] et basé dans les locaux d'Interpol à La Haye.

Les organismes publics doivent faire face aux attaques les plus diverses, qui vont du DDoS (déni de service distribué) aux violations de données. Il va sans dire que l'une comme l'autre est orientée à la hausse. Référence du secteur depuis 2004, le rapport annuel de Verizon sur les violations de données[6] affirme que l'année 2012 fut marquée par davantage d'incidents, issus de sources plus nombreuses et dont l'origine géographique est plus étendue et plus diverse qu'en 2011. Le rapport évoque également des angles souvent négligés de la …

... sécurité informatique. Ainsi, même si la majorité des attaques provient d'agents extérieurs, 4 % sont d'origine interne. De même, 10 % des attaques comprennent un élément physique, contrairement aux attaques exclusivement électroniques par piratage ou malware. Enfin, l'ingénierie sociale fait son apparition avec 7 % des cas de violations.

Pour compliquer le tout, les organismes du service public doivent également se conformer à des réglementations européennes de plus en plus nombreuses en matière de violations de données. Ainsi, l'UE a déjà promulgué une réglementation stricte de divulgation des atteintes à la sécurité, adoptée dans le droit français et applicable tant aux entreprises et organismes du secteur public que privé.

En février 2013, elle a même proposé un renforcement de cette réglementation, avec notamment une obligation de divulgation dans les 24 heures de toute violation de données de clients ou particuliers. Ce resserrement du cadre réglementaire pourrait placer une pression considérable sur les épaules des DSI du secteur public, qui devront non seulement s'assurer que leurs systèmes détectent d'éventuels problèmes, mais aussi en donnent l'alerte rapidement, sous peine de se voir mis à l'amende. Or, le rapport 2012 Verizon constate que 85 % des attaques ne sont découvertes que plus d'une semaine après les faits.

Preuve de l'enjeu croissant que représente la cybersécurité, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a coordonné un exercice d'urgence à grande échelle en octobre 2012, avec la participation de 25 pays et 300 spécialistes de la cybersécurité[7] sur près d'un millier de simulations de cyber-incidents. Objectif : évaluer l'efficacité et les capacités d'action des dispositifs de défense, de communication et de coopération, et identifier les carences et les pistes d'amélioration de ces dispositifs. Les initiatives eGovernment nationales se sont multipliées pour la première fois pour réaliser cet exercice.

D'une manière générale, on ne peut pas dire que les pouvoirs publics ont pris à la légère les questions de sécurité des systèmes d'information. En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est chargée de « *proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées* ». En sa qualité d'autorité nationale, l'ANSSI publie des recommandations et guides de bonnes pratiques dont la vocation dépasse largement le cadre consultatif. En effet, tout directeur informatique faisant preuve de négligences dans la protection des informations des pouvoirs publics ou des citoyens risque non seulement le licenciement, mais également des poursuites judiciaires.

Ironie du sort, c'est l'investissement et la foi des pouvoirs publics dans les avantages opérationnels des TIC qui est à l'origine des risques croissants auxquels ils s'exposent : les innombrables réseaux interconnectés étendent leurs ramifications à l'ensemble de cet environnement organisationnel complexe, non seulement sur le Web, mais aussi sous forme d'une myriade de réseaux internes, de systèmes informatiques partagés et de plates-formes collaboratives.

Le décor est donc planté. Mais qu'en ressort-il concrètement pour les plans TIC et de sécurité informatique dans les services publics ? Et quels sont les types de risques à évaluer pour conjuguer les stratégies de sécurité informatique au présent comme au futur ? ■

1. www.service-public.fr
2. Government ICT Strategy – Strategic Implementation Plan, Cabinet Office
3. Cost of Cyber Crime Report, Cabinet Office/Detica, 2011
4. 2011 Cost of Data Breach Study: UK, Ponemon Institute, mars 2012
5. « European Cybercrime Centre (EC3) opens on 11 January » http://europa eu/rapid/press-release_IP-13-13_en.htm, janvier 2013
6. Data Breach Investigations Report, Verizon, 2012
7. Cyber Europe 2012, organisé par ENISA

LES FONDATIONS D'UNE SÉCURITÉ EFFICACE

Le besoin de sécurité englobe à la fois la confidentialité des données (qui concerne la justification de l'accès d'une personne à des informations) et la cybersécurité (qui porte sur le risque ou la menace que représente l'octroi de cet accès). Entrent ensuite en jeu la sécurisation des données en transit jusqu'au demandeur de l'information, et la protection de ces données dans leur localisation d'origine.

Deux notions techniques fondamentales doivent être mises en place pour minimiser le risque et renforcer les lignes de défense autour de ces différents domaines : la gestion des identités et la gestion des accès. Et seule une stratégie dotée de systèmes et de politiques permettant de gérer ces deux notions peut être considérée comme complète et aboutie.

Gestion des identités et des accès : Qui demande un accès ? Peut-on lui faire confiance ?

GESTION DES IDENTITÉS

Le risque apparaît au moment même où une personne demande un accès à une information. À ce stade, une précaution s'impose : déterminer avec certitude l'identité du demandeur. Ce préalable s'applique tant aux demandeurs internes (agent de la fonction publique) qu'externe (particulier ou collaborateur d'un autre organisme de service public).

Le concept d'« *authentification unique* » (SSO) est désormais considéré comme une approche efficace. Une fois authentifié, l'utilisateur habilité peut accéder à un ensemble de systèmes connexes sans devoir se reconnecter. Cette pratique s'avère particulièrement adaptée aux services publics, pour les agents comme pour les usagers. Ainsi, les utilisateurs de https://mon.service-public.fr/ peuvent unifier leurs comptes au moyen d'un mot de passe unique pour effectuer leurs démarches administratives. Toutefois, cette méthode n'aura jamais l'évolutivité nécessaire pour s'appliquer à tous les domaines administratifs aux niveaux : national, local et territorial, à mesure que de nouveaux services en ligne et de nouveaux modes d'accès apparaissent, notamment via les smartphones et les tablettes.

Chez nos voisins britanniques, l'équipe des services numériques du gouvernement travaille désormais sur un programme ...

… baptisé IDA (Identity Assurance) qui promet un service sécurisé moins restrictif pour permettre aux citoyens de la couronne d'effectuer plus facilement leurs démarches. Au cœur de cette approche, le concept de validation d'identités de confiance, garanties par des entreprises privées qui ont déjà soumis ces identités à des contrôles et évaluations rigoureux sur leurs propres systèmes informatiques. Ainsi, les entreprises d'utilité publique (eau, gaz, électricité) et autres établissements bancaires seront admis au sein du programme dès lors qu'ils pourront démontrer qu'ils ont mis en place les procédures IDA idoines. L'intérêt de cette alliance se situe au niveau des coûts, dans la mesure où elle évitera aux organismes publics de répéter une tâche d'authentification de base déjà effectuée par un partenaire privé de confiance.

Une gestion fiable des identités, garante d'une authentification sûre, est un passage obligé vers l'application de règles d'accès et la sécurisation de la connexion par laquelle les données circuleront.

Enfin, une approche fédérée de l'accès aux technologies passe nécessairement par l'établissement de normes de gestion des accès régissant précisément l'octroi d'autorisations. Il en va de la démocratisation des TIC au service du plus grand nombre et d'un usage efficace et économique des ressources TIC du service public.

GESTION DES ACCÈS

Indexé au risque correspondant, le concept de confiance est essentiel à la gestion des différents types d'informations, et plus particulièrement au prochain maillon de la chaîne qu'est l'autorisation. Cette étape contrôle non pas l'identité d'un utilisateur, mais l'autorisation de cette personne à accéder aux ressources demandées. Pour le secteur public, cette notion est particulièrement importante du fait qu'il doit respecter les directives de l'ANSSI. Toujours de l'autre côté de la Manche, le CESG (équivalent britannique de l'ANSSI) a créé la norme IS1 dans laquelle il définit clairement plusieurs niveaux d'information – des données à niveau d'impact nul (IL0), dont la divulgation publique n'aurait aucun impact, jusqu'aux informations hautement sensibles à niveau d'impact 6 (IL6), qui entraîneraient des conséquences graves si leur confidentialité venait à être compromise. Ce classement va donc des informations publiables sur un site Web public aux données classées « *secret défense* ». Comme on peut l'imaginer, l'accès d'une personne non habilitée aux informations de cette dernière catégorie représente un risque considérable.

QUI DEMANDE UN ACCÈS ? PEUT-ON LUI FAIRE CONFIANCE ?

Au Royaume-Uni, les systèmes d'information de l'Etat ont une obligation légale de mise en place de dispositifs permettant de gérer l'information selon ce classement. Quant aux autres organismes de service public, il leur est recommandé d'en faire de même. De fait, leurs systèmes devront pouvoir déterminer quel type d'information est accessible sur simple identification via la plate-forme IDA. L'usager pourra par exemple régler une contravention de stationnement (information de niveau 1 ou 2) à l'aide d'un seul nom d'utilisateur et mot de passe. Par contre, une preuve d'identité supplémentaire pourra s'avérer nécessaire si cette même personne souhaitait consulter son historique, notamment s'il inclut son adresse, ses coordonnées bancaires ou d'autres informations d'identification personnelle. Ainsi une authentification automatique de base peut être complétée par d'autres vérifications. Pour reprendre un autre exemple, l'envoi d'une demande d'allocation logement peut ne concerner que des données de niveau 1. En revanche, si quelqu'un souhaite consulter l'historique complet de ses prestations sociales et saisir un « *changement de situation* » ou de nouvelles informations de paiement, le …

LES CINQ A DE LA GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

À l'heure où les responsables informatiques du secteur public se penchent sur le cahier des charges de systèmes IAM (Identity & Access Management) plus stricts, les cinq points suivants offrent une piste de réflexion autour des deux grands publics d'utilisateurs : utilisateurs internes (agents de la fonction publique et autres intervenants), et usagers du service public.

Administration

- Comment renforcer le processus d'ajout/modification/suppression des droits d'accès des utilisateurs en fonction de leurs rôles/fonctions opérationnels ou informatiques ?
- Comment ces moyens peuvent-ils améliorer l'efficacité, réduire les coûts et assurer un contrôle centralisé ?

Analytique

- L'ajout/modification/suppression d'un accès est-il conforme aux obligations/politiques/réglementations (internes et externes) de l'organisme ?
- Du point de vue de la conformité et de la gouvernance, quels sont les risques pour notre organisme ?

Authentification

- Une fois les droits d'accès octroyés, comment les utilisateurs accèdent-ils à leurs applications ?
- Leur faut-il uniquement un nom d'utilisateur et mot de passe, une authentification forte basée sur les risques, une authentification unique (SSO, Single Sign-On) leur permettant d'accéder à toutes leurs applications ?

Autorisation

- Une fois connectés, à quoi les utilisateurs sont-ils exactement habilités ?

Audit

- Qui a accès à quoi, pourquoi et avec l'autorisation de qui ?

… risque passe à des informations de niveau 2. La personne devra alors fournir des preuves d'identité supplémentaires ou répondre à des questions de sécurité.
Un contrôle fiable de l'identité ne représente qu'un aspect de la gestion des accès à l'information ou aux applications. D'autres facteurs matériels ou comportementaux peuvent également entrer en ligne de compte pour détecter d'éventuels problèmes de sécurité : nombre de connexions d'un utilisateur, sa localisation géographique, le terminal utilisé, etc.
Ainsi, l'avènement des nouvelles technologies et des services en ligne impose l'adoption, à des degrés divers, de solutions de gestion des identités et des accès dans tous les organismes publics. Ces outils s'érigeront en garants d'un dispositif d'autorisation et d'authentification plus strict, capable d'établir les niveaux de confiance appropriés, et donc de réduire les risques.

SOURCES DE VULNÉRABILITÉ DES DONNÉES

Une approche intégrale de la sécurité des données doit prendre en compte tous les cas de figure : attaques internes ou externes, prévues ou imprévues, pour la gloire ou pour l'appât du gain, etc. Cependant les attaques délibérément malveillantes ne constituent pas le seul risque : les violations de sécurité par accident ou négligence seraient encore plus fréquentes. De fait, les risques d'atteinte à la base de données sont aussi divers que variés :

Exploitation
Perte ou vol de sauvegardes, accès direct au système d'exploitation

Mauvaise utilisation des comptes d'administrateur
Administrateur de bases de données, administrateurs système, utilisateurs internes mal intentionnés, vol d'identifiants

Test et développement
Accès des développeurs aux données réelles (informations d'identification personnelle, données sensibles, etc.) à des fins de test et de développement, dans des environnements non sécurisés

Utilisateurs d'applications
Attaques extérieures par injection SQL et contournement d'application

Sécurité des bases de données : les données sont-elles sécurisées, même lorsqu'elles quittent la base ?
Pour interdire l'accès non autorisé aux données, il ne suffit pas de s'assurer que seuls les utilisateurs habilités bénéficient d'un accès ; il faut aussi veiller à la neutralisation et au blocage des demandes et des individus non autorisés. Cela suppose en particulier d'empêcher tout accès malveillant, vol de données et autres atteintes à la cybersécurité. Mais il s'agit aussi d'éviter qu'un utilisateur interne puisse compromettre l'intégrité ou causer la perte, volontaire ou accidentelle, de données, ou encore d'empêcher que ces données soient envoyées par erreur à une adresse ou une personne non habilitée.
Dépositaire de l'information critique de l'entreprise, la base de données fait l'objet des attaques les plus virulentes. Ainsi, le rapport 2012 de Verizon sur les violations de données[8] révèle que les serveurs de base de données sont la cible de 33 % des atteintes à la sécurité dans les grandes entreprises et représentent 98 % des ressources compromises. Les cybermalfaiteurs sont animés des motivations les plus diverses : appât du gain, révélations de type Wikileaks, « *hacktivistes* » des collectifs LulzSec ou Anonymous, espionnage étatique, crime organisé, etc.
Un rapport récent du cabinet Forrester et de l'association internationale des professionnels de la sécurité (International Association of Security Professionals)[9] estime que les informations d'identification personnelle resteront parmi les cibles les plus visées, sachant qu'elles ont été l'objet de 22 % des attaques perpétrées contre les entreprises au cours des 12 derniers mois.

LES DONNÉES SONT-ELLES SÉCURISÉES, MÊME LORSQU'ELLES QUITTENT LA BASE ?

L'une des méthodes les plus couramment employées est l'injection SQL (SQLi). D'après un autre rapport, les attaques SQLi ont enregistré une hausse de 69 % au cours du premier semestre 2012[10]. Leur principe consiste à saisir des commandes et des requêtes de base de données pernicieuses par l'intermédiaire d'adresses URL ou de champs de texte sur des sites Web mal protégés, généralement à des fins crapuleuses. Le piratage du réseau Playstation de Sony en 2011 en est la parfaite illustration. Le blocage des attaques SQLi fait d'ailleurs l'objet de nombreuses mises en garde et recommandations de la part de l'ANSSI et du CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques).
Pour les entreprises comme pour les organismes publics, la sécurité informatique commence traditionnellement par le pare-feu du réseau. La raison est évidente : interdire à quiconque de pénétrer sur le réseau. Le problème du pare-feu, c'est que lorsqu'un individu accède à un réseau, légitimement ou non, il peut ensuite bénéficier d'une liberté d'action totale. Si un collaborateur mal intentionné représente un risque constant, le risque de violation accidentelle des données n'en est pas moins omniprésent. Au Royaume-Uni, ces violations de sécurité internes seraient d'ailleurs à l'origine du retrait en 2010 de la base de données ContactPoint destinée à la protection des mineurs. La même année, une demande soumise par l'hebdomadaire Computer Weekly au ministère de la justice britannique, dans le cadre de la loi de liberté …

8. Data Breach Investigations Report, Verizon, 2012
9. Forrester, septembre 2012
10. SC Magazine Report, FireHost Survey, juillet 2012
11. Article de Computer Weekly sur la sécurité du service des tribunaux britanniques, 2010

… de l'information (Freedom of Information)[11], a révélé 180 cas de violations internes par les services des tribunaux de Sa Majesté, dont certaines ont été sanctionnées par des licenciements.

Le problème réside dans le fait que les applications elles-mêmes ne sont généralement pas développées dans une perspective de protection de l'information. Par conséquent, lorsque ces applications servent à accéder à des données, le niveau intrinsèque de sécurité est faible. En d'autres termes, il faut appliquer un train de règles capables de protéger efficacement la base de données et son contenu. ■

UNE PROTECTION INTÉGRALE DE LA BASE DE DONNÉES PASSE PAR DIFFÉRENTES MESURES :

Protection de la base de données

La mise en place d'un pare-feu autour de la base de données crée une nouvelle ligne de défense destinée à neutraliser tout accès par des utilisateurs ou requêtes non autorisés. Par cette méthode, les transactions avec la base de données sont bloquées avant même de l'atteindre.

Protection des données

Le chiffrement permet de rendre les données inexploitables ou invisibles en cas d'accès ou de vol par des personnes non autorisées. Il minimise ainsi les risques engendrés par une atteinte aux données, et ce quelle qu'en soit l'origine. Même si un hacker parvient à franchir le pare-feu et à accéder à un flux de données, si un serveur disparaît du datacenter ou si une bande de sauvegarde est égarée pendant son transfert vers un site de stockage extérieur, les données restent à l'abri des regards indiscrets.

Gestion des administrateurs de bases de données

Il est indispensable de bien gérer les droits d'accès d'utilisateurs à forts privilèges.
Car en cas d'excès de privilèges, des brèches s'ouvrent : un administrateur de base de données (BDA) disposant de droits de gestion de l'information peut ainsi posséder des privilèges lui permettant de consulter, voire exporter les données elles-mêmes. Souvent, les DBA disposent par défaut d'un accès administrateur. Or, si leurs droits excèdent le minimum nécessaire pour assurer leurs missions, le risque est bien réel.

Gestion de la destination des données

Dans de nombreux cas, les données doivent être communiquées à des autorités étrangères, notamment les administrations fiscales ou les services de police ou d'immigration. Les informations contenues dans les bases de données des pouvoirs publics sont alors transmises vers l'extérieur, voire accédées directement par des tiers en cas de besoin. Il est donc essentiel d'exercer un contrôle rigoureux sur ses données. Pour ce faire, il existe des outils qui permettent de restreindre les droits de consultation aux seules données de la base dont le tiers à besoin. Outre ces précautions, bon sens et bonne gestion doivent rester de mise. La stricte gestion de l'attribution d'identifiants utilisateur aux nouvelles recrues, et leur annulation en cas de départ, semblent une évidence. Or, des organismes peuvent encore être pris à défaut dans ce domaine. Idem pour les mots de passe partagés entre membres du personnel pour de simples raisons pratiques. Nombreux sont les systèmes qui disposent également de *« portes dérobées »* et de mots de passe *« passe-partout »* qui, s'ils ne sont pas changés régulièrement, peuvent permettre aux intrus d'accéder aux données. C'est pourquoi toutes les vulnérabilités connues des systèmes ou applications qui se connectent à la base de données doivent être recensées et corrigées. Enfin, l'emploi de nombreuses bases de données, souvent issues de divers éditeurs, dans l'ensemble du service public amplifie la difficulté de mise en place de politiques homogènes d'accès aux bases de données, particulièrement lorsque ces dernières sont partagées par plusieurs organismes ou services. Dans ce cas, la centralisation des habilitations est alors vitale.

Gestion de la divulgation intentionnelle des données

Dans certains cas, la sécurité représente une composante essentielle de la divulgation intentionnelle de données. Souvent, la communication externe de données est souhaitable, voire nécessaire. Le partage de dossiers médicaux à des fins de recherche a fait l'objet de débats enflammés outre-Manche, même si selon toute vraisemblance, toutes les informations d'identification personnelle auraient été éliminées ou masquées au moyen d'outils de masquage de données. Dans ce domaine, Oracle propose une solution puissante, capable non seulement de rédiger des informations, mais aussi de randomiser les données numériques telles que les coordonnées bancaires, de les remplacer par des données fictives, de changer les noms de famille, etc., tout en préservant les informations indispensables aux besoins de l'analyse. Ce type d'outil peut être d'une grande utilité pour les développeurs d'applications dans le service public. Ces derniers ont en effet besoin d'informations personnelles aussi réelles et pertinentes que possible pour tester le bon fonctionnement des services avant leur lancement. Toutefois, ces informations doivent être anonymisées et débarrassées de toute information d'identification personnelle pour protéger la vie privée des particuliers. ■

GESTION DU CHANGEMENT

Le développement d'une culture de la sécurité va de pair avec toute nouvelle approche de la cybersécurité : en effet, aucun projet ne peut aboutir sans associer le facteur humain à l'investissement technologique.

En traitant la sécurité selon une démarche dite de « *inside-out* » centrée sur les données, toute restriction des accès peut être perçue par les utilisateurs comme un obstacle, voire une menace, à l'accomplissement de leurs missions. Même le simple fait d'aborder le thème de la sécurité des bases de données peut être vu comme un doigt accusateur en direction des Database Administrators (DBA). Ces DBAs doivent être sensibilisés à la question de la sécurité sous l'angle de leur protection contre toute allégation d'usage mal intentionné de leurs privilèges d'accès. Une sécurisation renforcée peut leur permettre d'administrer les bases de données sans jamais devoir accéder au contenu lui-même, et constitue ainsi une protection active en cas d'investigation informatique légale consécutive à une violation de données.

Il convient également de prendre en compte l'irrésistible montée en puissance des technologies mobiles et sociales. De fait, la généralisation des smartphones et autres tablettes constitue l'une des grandes raisons d'un resserrement des dispositifs de sécurité dans le service public. Comme ils peuvent à la fois stocker des informations et faire office de point d'accès, ces terminaux soulèvent inévitablement la question de leur validation pour un usage professionnel par les agents de la fonction publique – question appelée à gagner de l'importance dans les DSI. Même si la liberté de choix des terminaux (ou politique BYOD, Bring Your Own Device) semble moins d'actualité dans les grandes administrations, les autorités de surveillance des TIC au niveau local et dans de nombreux organismes publics devront gérer cette demande et y apporter des réponses sécurisées. Certaines considérations techniques doivent être prises en compte : le CESG britannique propose par exemple des consignes relatives aux principales plates-formes mobiles[12]. Négligence, perte accidentelle ou laxisme des utilisateurs constituent autant de facteurs de risques pour les mots de passe et les données, car les terminaux mobiles (ordinateurs portables, téléphones, tablettes…) peuvent servir de tête de pont à des activités malveillantes. En ce sens, les politiques de mobilité professionnelle doivent être associées à des programmes de sensibilisation et de formation des utilisateurs, régulièrement actualisés pour rester en phase avec la réalité des menaces. De même, la propagation de l'usage des réseaux sociaux dans le service public comporte également des risques qu'il convient d'intégrer dans le développement d'une culture de sécurité. ■

> AUCUN PROJET NE PEUT ABOUTIR SANS ASSOCIER LE FACTEUR HUMAIN À L'INVESTISSEMENT TECHNOLOGIQUE

12. CESG Smartphone Guidance Overview, 2011

ET EN CAS DE PROBLÈME MAJEUR ?

Que se passe-t-il en cas de violation avérée des données ? Dans le public comme dans le privé, les obligations de détection et de signalement des violations de données ne cessent de se durcir. Cette tendance impose la mise en place de systèmes capables non seulement de prévenir toute intrusion, mais aussi de repérer et de signaler instantanément une infraction en cours. Or, face à l'ingéniosité sans borne des cybercriminels, on peut s'attendre à terme à une poursuite des violations de données, même si le risque sera réduit sur les réseaux les mieux protégés. Le seul remède consiste alors à effectuer un audit précis de toutes les transactions de bases de données, intégré au modèle de sécurité inhérent à la base de données.

Cet audit aboutira à la remontée éventuelle jusqu'au coupable, ou tout du moins à la mise sous surveillance d'un individu soupçonné d'espionnage et de ses transactions avec une base de données. D'après une étude internationale sur le cybercrime menée fin 2011 par PricewaterhouseCoopers[13] dans les secteurs public et privé, plus d'un quart des organisations interrogées s'attendent à être victimes d'une attaque dans l'année. Pourtant, la plupart reconnaissent ne pas disposer des ressources nécessaires à une enquête qui permettrait d'établir d'éventuels méfaits...

L'autre intérêt de l'audit se situe au niveau des obligations de conformité : les auditeurs peuvent en effet exiger des preuves de la mise en place de politiques d'accès, par exemple en vérifiant que seuls les utilisateurs dûment habilités ont pu consulter une feuille d'impôt ou autre information privée. Auparavant, la réponse à une telle demande pouvait passer par de fastidieuses recherches manuelles dans de multiples systèmes. Or, ces modèles conventionnels d'analyse et d'audit périodiques se compliquent encore plus avec l'interconnexion de plus en plus dense des réseaux, les architectures Cloud employées par certains organismes publics et le développement de programmes de mutualisation du Cloud (G-Cloud au Royaume-Uni) pour accroître les synergies et les économies d'échelle dans tous les domaines de l'administration publique. La solution consiste alors à effectuer un reporting automatique et direct à partir de la base de données elle-même. Avec des solutions plus évoluées de sécurité des bases de données, vous pouvez suivre les journaux en temps réel, détecter tout changement ou activité suspecte, et automatiser les alertes pour accélérer les interventions et les mesures correctives. ■

> FACE À L'INGÉNIOSITÉ SANS BORNE DES CYBERCRIMINELS, ON PEUT S'ATTENDRE À TERME À UNE POURSUITE DES VIOLATIONS DE DONNÉES

13. Global Economic Crime Survey, PwC, novembre 2011

A RETENIR

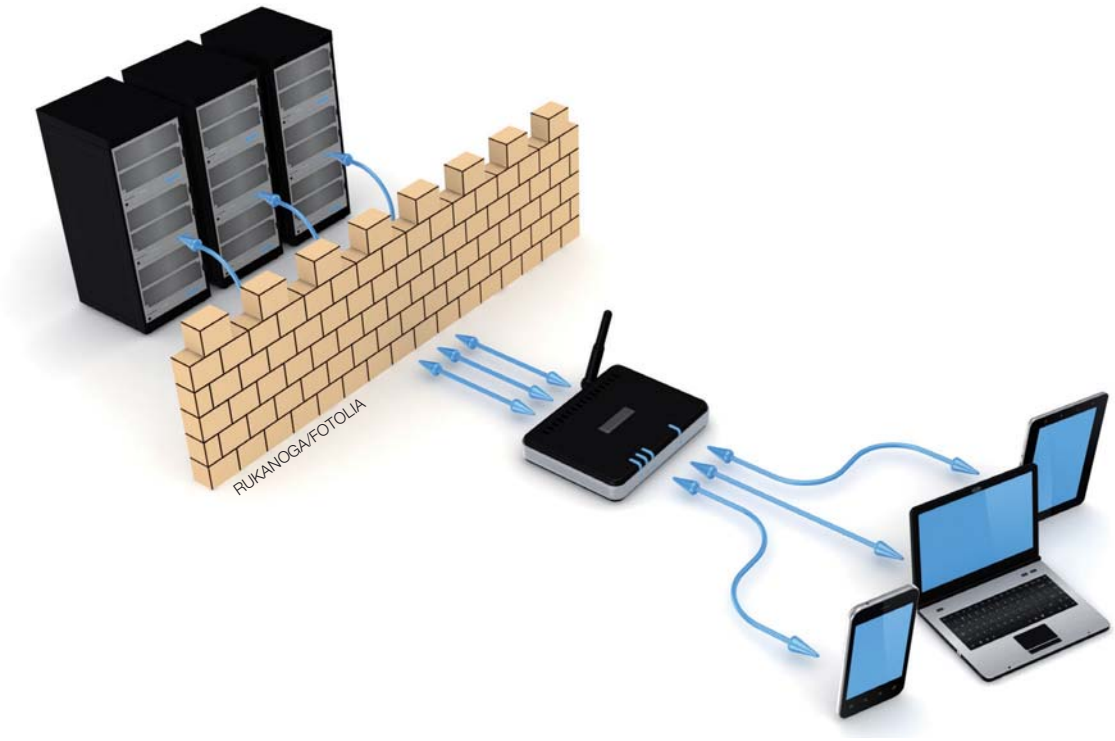
En raison de la nature même des informations qu'elle détient, la fonction publique a bien pris conscience de l'importance d'une sécurité renforcée de ses systèmes.
Or, les risques d'une mauvaise gestion des données des particuliers ou des informations ministérielles les plus sensibles ne cessent d'augmenter, sous les pressions conjuguées des menaces extérieures, de la hausse irrépressible des coûts de la perte de données et des contraintes réglementaires de plus en plus strictes.
Dans ce contexte, des solutions de sécurité efficaces autrefois, se révèlent aujourd'hui dépassées.

La sécurité périmétrique sous la forme d'un pare-feu réseau ne suffit plus à prévenir les violations de données, malveillantes ou accidentelles, d'origine interne. De plus, elle ne protège ni la base de données, ni les données elles-mêmes, ce qui constitue le cœur du problème.

La présence d'un noyau de collaborateurs de confiance ne suffit pas à minimiser les risques : dans la fonction publique, la gestion des accès aux données confidentielles ou aux informations d'identification personnelle, notamment par des utilisateurs à forts privilèges, est tout aussi importante que la gestion des identités et des accès d'utilisateurs lambda externes.

La protection de la base de données et des données proprement dites doit être au cœur d'une politique de cybersécurité efficace. Portant sur les pertes ou intrusions physiques comme électroniques, elle assure une ligne de défense supplémentaire en maquillant les données pour les rendre méconnaissables et inutilisables à des fins politiques ou commerciales en cas d'intrusion.

Il convient également de s'intéresser plus sérieusement à l'enjeu que représente la prévention des atteintes aux données dans la fonction publique, particulièrement à une époque où de plus en plus de services sont accessibles via le Web et d'autres canaux. Quelle que soit l'approche, les impératifs demeurent les mêmes : identification de la personne, autorisation d'accès de niveaux différents, sécurisation des mécanismes d'accès et de transfert des données, et enfin chiffrement des données pour les rendre illisibles en cas d'interception.
Dans un parc informatique public de plus en plus interconnecté et accessible sur le Web, un seul maillon faible peut engendrer de gros problèmes. Pour cela, les structures de plus petite taille pourront se regrouper pour mutualiser leurs investissements en solutions de sécurité, dans une optique de baisse des coûts, de partage des risques et de connexion des systèmes, selon le même principe que les investissements partagés en systèmes back-office. Cette mutualisation leur permettra également de profiter de l'expérience, de l'expertise technique et des solutions des grands fournisseurs informatiques de la place. Les menaces et les risques sont bien connus. Pour y faire face, des éditeurs et constructeurs de premier plan comme Oracle ont mis au point des lignes de défense renforcées, déployées dans les organismes publics du monde entier. Cette expérience peut être mise à votre service. ■



CONTACT
Oracle France,
15 Boulevard Charles de Gaulle,
92715 Colombes Cedex

ORACLE

Téléphone	Renseignements France :	0800 905 805
E-mail	Ventes France :	ic-france_ww@oracle.com
Internet	Site Web France :	www.oracle.com/fr

LES SOLUTIONS DE SÉCURITÉ ORACLE

Oracle Information Security se démarque par une stratégie de « défense en profondeur », avec notamment un chevauchement des contrôles de sécurité de vos ressources informatiques, à travers vos données et vos identités. Les solutions de sécurité Oracle reposent sur deux principes clés : la sécurité des identités et la sécurité de la base de données.

Les solutions Oracle Identity Management

Oracle Identity Management permet aux organisations de gérer avec efficacité le cycle de vie complet des identités utilisateurs à travers toutes les ressources d'entreprise – à l'intérieur du pare-feu, à l'extérieur et dans le Cloud. La plate-forme Oracle Identity Management propose des solutions évolutives de gouvernance des identités, de gestion des accès et de services d'annuaire. Grâce à elles, les organisations peuvent renforcer leur sécurité, simplifier leurs démarches de mise en conformité et exploiter les opportunités émanant de la mobilité et des réseaux sociaux.
Oracle Identity Management est partie intégrante d'Oracle Fusion Middleware, une gamme de produits capables d'améliorer la fiabilité, d'optimiser la prise de décisions et de réduire les coûts et les risques dans les environnements informatiques les plus variés. Les « cinq A » (Administration, Analytique, Authentification, Autorisation et Audit) cités dans l'article sont mis en œuvre via la plate-forme Oracle Identity Management, désormais commercialisée sous la forme de trois suites distinctes en version 11g (Release 2) :

ORACLE IDENTITY GOVERNANCE

Plate-forme d'administration, d'analytique, d'audit, de gestion des mots de passe et de libre-service pour les utilisateurs.

ORACLE ACCESS MANAGEMENT

Plate-forme de signature unique (SSO), de sécurité des services Web, d'authentification et de prévention anti-fraude, d'accès depuis les terminaux mobiles et de centralisation de la gestion et des contrôles d'attribution des droits utilisateurs.

ORACLE DIRECTORY SERVICES

Référentiel central des identités pour l'authentification et l'autorisation.

Les solutions Oracle Database Security

Oracle propose les technologies les plus évoluées pour la protection des données dans leur lieu d'origine : la base de données. Notre gamme complète de solutions de sécurité des bases de données assure la confidentialité des informations, la protection contre les menaces internes et le respect des obligations réglementaires.

ORACLE ADVANCED SECURITY

(En option sur Oracle Database uniquement)

- Protection contre les accès non autorisés au système d'exploitation ou au réseau
- Chiffrement fiable de toutes les données applicatives (sur disque, dans les sauvegardes et sur le réseau)
- Gestion intégrée des clés de chiffrement
- Aucune nécessité de modification des applications
- Certifié sur Oracle Exadata avec l'avantage du chiffrement sans latence

ORACLE DATABASE VAULT

(Oracle uniquement)

- Restreint les pouvoirs des utilisateurs privilégiés et applique la séparation des tâches (SoD)
- Protège les données applicatives et empêche le contournement des applications
- Contrôle qui, où, quand et comment au moyen de règles et de facteurs
- Consolidation sécurisée des données applicatives
- Aucune nécessité de modification des applications
- Certifié sur Oracle Exadata

ORACLE AUDIT VAULT ET DATABASE FIREWALL

(Compatible avec de nombreuses plates-formes de base de données : Oracle, SQL, DB2, Sybase, etc.)

- Consolidation des données d'audit dans un référentiel sécurisé
- Détection et signalement d'activité suspecte
- Reporting de conformité immédiatement opérationnel

(Nombreuses plates-formes de base de données : première ligne de défense)

- Surveille l'activité de la base de données et pare aux attaques et injections SQL
- Établit des listes blanches, listes noires et listes d'exceptions, reposant sur une analyse grammaticale SQL ultra précise
- Blocage et surveillance in-line ou modes de surveillance hors bande

ORACLE DATA MASKING

(Diverses plates-formes de base de données)

- Réduit les besoins d'audit par « désidentification » sur les bases de données hors production
- Préservation de l'intégrité référentielle pour que les applications restent opérationnelles

...

...

- Bibliothèque de modèles et politiques extensibles à des fins d'automatisation

ORACLE LABEL SECURITY

(Contrôle multi-niveaux d'accès aux données)

Oracle Label Security est un outil puissant et ergonomique qui permet de hiérarchiser les données et d'en gérer l'accès en fonction de cette classification. Répondant aux impératifs de la fonction publique en matière de sécurité multi-niveaux et de contrôle obligatoire des accès, Oracle Label Security offre un dispositif flexible d'accès aux données en fonction des rôles et des besoins, dans une optique de protection de la confidentialité et de respect des obligations de conformité réglementaire.

- Dispositif flexible de gestion des accès aux données en fonction des rôles et des besoins
- Restreint l'accès aux seules personnes disposant des habilitations appropriées, en permettant aux administrateurs de hiérarchiser toutes les lignes d'une table pour que l'accès aux données sensibles soit limité aux seuls utilisateurs dûment autorisés
- Respecte les obligations réglementaires grâce à un modèle d'administration basé sur des règles, qui permet aux entreprises d'élaborer des processus personnalisés de hiérarchisation des données dans la perspective d'un accès en fonction des besoins et des rôles
- Les étiquettes peuvent servir de facteurs dans les règles de commande d'Oracle Database Vault pour les politiques d'autorisation multi-facteurs ; elles s'intègrent également à Oracle Identity Management, pour une gestion centralisée des définitions de politiques

ORACLE