Dossier de Presse

Forensic: Identifier l'incident ? C'est bien. Le résoudre ? C'est mieux

Atelier, Assises de la Sécurité et des Systèmes d'Information
Mercredi 2 Octobre 2013 à 16h00

Conférenciers
Laurent CHARVERIAT – CTO & Cofounder, I-TRACING
Alexis JANUSKIEWICZ – Manager Security Solutions Integration, I-TRACING
Pierre GRANGER – Manager, BOUYGUES TELECOM

I-TRACING

Tour Chantecoq
5 rue Chantecoq - 92800 PUTEAUX
tél : +33 (0)1 70 94 69 70
fax : +33 (0)1 70 94 69 71

Sommaire

Pour tout renseignement complémentaire :
Migé Gauchet - mige.gauchet@free.fr - Portable : + 33 (0)6 84 77 31 74
Théodore-Michel Vrangos - tmvrangos@i-tracing.com - Tél. : + 33 (0)1 41 02 50 71

I-TRACING en bref

Fondée en 2005 à Paris, I-TRACING est une société de conseil technique, d'ingénierie et de services opérés, spécialisée dans le domaine de la traçabilité des informations, de l'impact des mises en conformité légale sur les systèmes d'information, de la sécurité des systèmes d'information et des réseaux et de la valorisation des preuves et des traces numériques.

Carte d’identité

Fondateurs et Dirigeants	Théodore-Michel Vrangos, Président Laurent Charvériat, Directeur Général et Directeur Technique
Directeur Ingénierie	Michel Vujicic, Directeur Conseil et Ingénierie de Solutions
Directeur Audit/Forensic	Laurent Besset, Directeur Audit et Forensic
Forme juridique	SAS au capital de 183 000 €
Adresse	Tour Chantecoq - 5 rue Chante Coq à Puteaux (92800) Tél. : +33 (0)1 70 94 69 70 Fax : +33 (0)1 70 94 69 71
Site internet	www.i-tracing.com

Chiffres-clés

C.A.	7 M€ en 2012 Prévisions 2013 : 10 M€
Croissance C.A.	30% (2012 vs 2011)
Résultat net 2012	800 300 € Prévisions 2013: 750 000€
Effectifs	+45 ingénieurs et consultants
Recrutements	20 ingénieurs dans l’année

Historique

Novembre 2005 Création.

2006
Lancement et premiers projets de traçabilité de la fraude dans la banque et les télcos, offre de log management.
Partenariat avec Qosmos dans le domaine du DPI (Deep Packet Inspection) et la valorisation des traces pour la traçabilité des accès aux données personnelles et la lutte contre la fraude.

2007
Lancement de l'offre de mise en conformité Sarbanes-Oxley.
I-Tracing signe ses premiers partenariats techniques (RSA, Imperva, LogLogic…).
Lancement de l'activité Managed Services (services opérées de traçabilité et sécurité du SI.)
Partenariat avec Compuware dans le domaine de la mesure QoS et temps de réponse applicative.

2008
Lancement de l'offre de sécurité et collecte de preuves pour la lutte contre les fraudes, clients télécoms.
Lancement du « Service Notarial Dépôt électronique de la Chambre des Notaires ».
Lancement du pôle d'expertise sécurité des applications et des bases de données. Projets de développement d'applications sécurisées.
Partenariats ingénierie : RSA, SpectorSoft, LogLogic, etc.
Lancement du SOC de I-TRACING et croissance des activités de type Support et MSSP.

2009
Lancement de l'offre « Audit et mise en conformité PCI-DSS ».
Fort développement des projets de conformité légale (LSF, Bâle 2, LOPSSI 2 /LSQ,…) basés sur la gestion de logs.
Croissance importante des projets de mise en conformité des opérateurs télécom (suivant les exigences « Paquet télécom ») et des projets de traçabilité en environnement banque-finance (traçabilité et authentification des opérations et utilisateurs, etc.)

2010
Offre de conformité ARJEL (jeux et paris en ligne).
Nouvelle offre « Audit Sécurité et Cartographie des Données Personnelles ».
Partenariat avec des éditeurs (Cryptolog, RSA…) pour le développement d'applications sécurisées telles que des workflow métier, des coffres-forts, des SIM/SIEM… incorporant des fonctions de signature, d'horodatage…

2011
I-TRACING est retenue parmi les 15 sociétés dont la croissance est rentable, dans le classement Journal du Net et Bureau Van Dijk.
Nouveaux partenariats d'intégration : Balabit, ObserveIT, Wallix, Qualys, Sourcefire.
Emménagement dans de nouveaux locaux.

2012
I-TRACING rentre au capital de la société de conseil et d'ingénierie APALIA, spécialiste du Cloud Computing. Offre de service de sécurité des infra virtualisées.
I-TRACING figure pour la 2de fois consécutive au classement des entreprises à forte croissance Deloitte Technology Fast 500 EMEA à la 88ème place.

2013
Ouverture d'I-TRACING Ltd à Londres.
Lancement d'un nouveau data center hautement sécurisé en Région Parisienne.
Partenariats d'intégration avec de nouveaux éditeurs comme Cyber Ark, FireEye, Varonis,…

Compétences et expériences

Totalement indépendante, I-TRACING est une entreprise française en forte croissance.

I-TRACING est une société de conseil et d'ingénierie en sécurité - sécurité Internet, sécurité des systèmes d'information, traçabilité des informations et des opérations, impact des lois et règlements sur la conformité du SI, valorisation des preuves et des traces numériques, analyse forensique… Sa mission repose sur le besoin fondamental qu'a toute société de connaître, identifier, suivre, tracer, protéger et, le cas échéant, valoriser l'accès et la manipulation de ses données sensibles et de celles de ses clients (données personnelles, juridiques, commerciales, de savoir-faire, etc.). Ce besoin est en très forte hausse avec le développement d'Internet et de la dématérialisation. Il est accentué par l'impact des mises en conformité légales telles que CNIL, Sarbanes-Oxley, LSF, Loppsi, Bâle, ANSSI, PCI-DSS, « Paquet télécoms », ARJEL, etc.

I-TRACING se distingue par la forte expertise de ses équipes qui combinent la compréhension et l'anticipation des besoins fonctionnels spécifiques à chaque environnement métier avec des connaissances technologiques « avancées ».

Une forte expertise technologique

La société est avant tout constituée d'ingénieurs, dotés d'une forte culture technique et d'une forte culture Internet. Consciente de l'importance stratégique de l'information pour ses clients, I-TRACING a formé des équipes d'ingénieurs réseaux et sécurité et de spécialistes en développement applicatif sécurisé et bases de données.

Animée par le respect des engagements et de la délivrance des projets clé en main, I-TRACING combine la compréhension et l'anticipation des besoins fonctionnels, spécifiques à chaque environnement métier, avec une forte expertise technologique des protocoles et solutions IP sécurisés, de mobilité et de télécommunications. Les ingénieurs d'I-TRACING possèdent les compétences qui leur permettent de maîtriser les solutions les plus pertinentes du marché de la sécurité. Leur secret : être en veille permanente et rester à l'affût de l'apparition de nouvelles technologies pour toujours garder une longueur d'avance.

Des hommes d'expérience

Dotés d'un réel esprit entrepreneurial, les fondateurs d'I-TRACING n'en sont pas à leur coup essai. Ils comptent plusieurs succès sur le marché de la sécurité et de la traçabilité depuis plus de deux décennies. Ces hommes d'expérience savent insuffler l'élan nécessaire pour relever les défis et satisfaire des enjeux. Ils conduisent les opérations et les changements avec le sens de l'anticipation, prenant ainsi un avantage concurrentiel et des parts de marché. Ces résultats sont obtenus grâce au savoir-faire qu'ils savent entretenir dans leurs équipes.

Objectif d'I-TRACING : développer désormais son activité en Europe. Une première filiale, I-TRACING Ltd., a été ouverte à Londres cette année pour accompagner sa croissance internationale.

Des clients, entreprises leaders

I-TRACING fournit des services à haute valeur technologique aux grandes entreprises, leaders dans leur secteur. Elle leur apporte son expertise et son expérience pour mettre en œuvre des solutions clé en mains et les accompagne techniquement et fonctionnellement pour faire vivre et évoluer les solutions déployées.

La traçabilité d'un produit ou d'une information est un enjeu fondamental tant économique, qu'éthique et sécuritaire. Universelle en raison de la forte pénétration des nouvelles technologies, d'Internet et de la mobilité dans la vie de tous les jours, la sécurité de l'information se révèle nécessaire pour protéger le patrimoine des entreprises qui repose, de plus en plus, sur des données dématérialisées. De nombreuses entreprises et les administrations sont aujourd'hui confrontées à des menaces d'un nouveau type. Il leur faut déjouer les attaques ciblées, DDoS, 0-days, APT…

Riche d’une palette de compétences très variées, I-TRACING est en mesure d’apporter une réponse complète aux nouveaux enjeux de la sécurité Internet, de la traçabilité des informations et des impacts liés aux conformités légales. Cette large compétence est complétée par des expertises technologiques pointues, dans certains secteurs d’activités tels que les télécoms avec la sécurité IMS ou la convergence all-IP, la traçabilité fine des opérations financières et l’extraction des faisceaux de preuves. Cette approche globale s’appuie sur une expertise technique continuellement enrichie par de nouveaux projets et une veille technologique permanente.

Activités

Conseil, audit de sécurité, analyse de code, gouvernance SI et SSI, élaboration d’architectures, ingénierie et intégration, développement sécurisé, managed services, formation… dans le domaine de la traçabilité et de la sécurité de l’information, I-TRACING répond aux besoins de :

- Traçabilité des accès aux données,
- Traçabilité des interventions et des opérations des infogérants, mainteneurs et sous-traitants,
- Optimisation de l'exploitation, de la production informatique et du traitement des incidents,
- Forensic, analyses post-mortem,
- Mise en conformité avec les règlements et les lois,
- Préparation et accompagnement pour une certification réglementaire (PCI-DSS, CNIL, ARJEL, ISO27001, SOX,…),
- Obtention de preuves à partir du système d'information sécurisé,
- e-discovery,
- Valorisation de l’information à partir de la connaissance précise de son usage (Information Data Usage),
- Mieux cibler sa clientèle ou ses consommateurs pour mieux vendre ses produits et services,
- Protection du patrimoine informationnel de l’entreprise contre les attaques (DDoS, APT, 0-Day…)
- Sécurité du cloud et des infrastructures virtualisées,
- Etc.

Offre

Traçabilité des informations et des opérations

Contrôle des accès des utilisateurs à privilèges ; solutions d’accès à rebond ; traçabilité des opérations des infogérants, des mainteneurs ou du call center… ; traçabilité des accès aux données personnelles ; coffres-forts de mots de passe ; enregistrement de sessions…

Sécurité des applications et des bases de données

Développement d’applications sécurisées ; signature électronique, SSO, authentification forte, Identity & Access Management ; dématérialisation sécurisée de processus ; Database Activity Monitoring, mesure QoS et SLA d’applications…

Conformité

Respect des obligations légales propres à chaque métier et accompagnement pour la certification ARJEL, PCI-DSS, LSF, LOPPSI, Sarbanes-Oxley, Mifid, Bâle, Solvency, CNIL, ISO 27000… ; extraction de preuves du SI à caractère légal et e-discovery…

Sécurisation de l’information et de l’infrastructure

Spécification d’architectures de sécurité SI et télécoms ; virtualisation sécurisée des infrastructures, cloud computing… ; ingéniérie et mise en production de solutions ; exploitation et MCO des infrastructures de sécurité et de traçabilité (SOC/NOC)…,

Log Management & SIEM

Collecte, archivage et valorisation des logs ; extraction et analyse des traces d’infrastructure (deep packet inspection) SEM, SIM, SIEM ; gouvernance sécurité et tableaux de bord SSI ; archivage des traces et logs, coffres-forts électroniques, politiques de rétention…

Traçabilité de la fraude

Forensic, audit de sécurité du SI, audit de code… ; protection du patrimoine informationnel, DLP, classification des données, accès illicite aux données critiques ; détection et prévention contre le piratage, le plagiat et la contrefaçon, E-DRM (gestion des droits numériques)…,

Managed services des infrastructures de sécurité et traçabilité

I-TRACING possède un SOC/NOC (Security & Network Operations Center) hautement sécurisé et animé par une équipe d'ingénieurs dédiée.

Ingénierie des solutions

I-TRACING a bâti des partenariats d'intégration avec des éditeurs spécialisés tels que LogLogic, VMware, Imperva, Palo Alto Networks, Qosmos, Fortinet, SpectorSoft, RSA, Compuware, Click&DECIDE, Sourcefire, ArcSight, Cisco, Cryptolog, RSA, Balabit, ObserveIT, Wallix, Qualys, Sourcefire, Cyber Ark, FireEye, Splunk, etc.

Pour communiquer ses compétences techniques à ses clients, I-TRACING propose un catalogue complet de formations intra-entreprise dans les domaines de la sécurité et de la traçabilité : solutions à rebond, coffres-forts de mots de passe, enregistrements de sessions…, log management, SIEM, certifications PCI DSS, Arjel, CNIL…, sécurité des infrastructures cloud et virtualisées, etc.

Références

La clientèle d’I-TRACING est essentiellement composée de grands comptes et d’administrations. Ce sont de grandes entités françaises et internationales telles que Aéroports de Paris, AG2R La Mondiale, Allianz, Bolloré, Bouygues, Banque Palatine, Carrefour, CEGEDIM, Chambre des Notaires de Paris, Crédit Agricole, Euler Hermès, France Télévisions, Groupama, Groupe Crédit Agricole, KBL Banque, Lafarge, Macif, Ministère des Affaires Etrangères, Orange, La Poste, PMU, RATP, Sanofi, Servier, SFR, Société Générale, Systra, Total, Vodafone, Yves Rocher.

I-TRACING intervient régulièrement depuis sa filiale de Londres auprès de grands groupes internationaux et des filiales d'entreprises françaises en Allemagne, USA, Qatar, Arabie Saoudite, Singapour, Royaume-Uni, Bulgarie, Suisse, etc.

Équipe dirigeante

Théodore-Michel Vrangos et **Laurent Charvériat** ont créé et dirigent I-TRACING. Ils s'appuient sur leurs valeurs communes et leur complémentarité. Les décisions se prennent à deux, stratégiquement comme quotidiennement.

Un parcours professionnel à deux

Ils n'en sont pas à leur coup d'essai. En décembre 1995, Théodore-Michel Vrangos et Laurent Charvériat, fondaient ensemble leur première entreprise, Cyber Networks. (Cette société de sécurisation des systèmes d'information et de l'Internet a été intégrée, en décembre 2004, au Groupe NET2S, lui-même racheté en 2008 par BT France).

En 2005, forts d'une expérience de près de 10 années dans la sécurité du système d'information, ils poursuivent ensemble leur parcours d'entrepreneurs et lancent I-TRACING, spécialiste de la sécurité et de la traçabilité de l'information. Laurent Charvériat et Théodore-Michel Vrangos aiment à rappeler que, s'ils ont bâti une entreprise comme beaucoup, en s'appuyant sur leur complémentarité, leur amitié les a conduits à une réelle complicité dans la direction de leur projet.

« Nous entendons devenir un acteur majeur de ce marché qui va très fortement croître dans les dix prochaines années », déclaraient-ils alors.

Ils vont très tôt acquérir une vision d'Internet qui va révolutionner les systèmes d'informations des entreprises. Mais, ils comprennent cependant que le passage du monde client/serveur fermé vers un monde ouvert où le client devient l'internaute va poser d'innombrables problèmes de sécurité. Le tout était de savoir comment la migration allait s'opérer. Pour Laurent Charvériat et Théodore-Michel Vrangos, la Sécurité et la Traçabilité de l'information sont la déclinaison d'une démarche globale au niveau des applications (une application, c'est ce qu'on utilise chaque jour lorsque l'on va à la banque, lorsqu'on achète un billet de train…) et au niveau des tuyaux, de l'infrastructure. Il convient donc de sécuriser l'ensemble - la partie visible que sont les applications et la partie cachée que sont les infrastructures, le back office - et de 'tracer' l'information.

Théodore-Michel Vrangos et Laurent Charvériat.

Théodore-Michel VRANGOS

Master of Science en IT Management de « University of Manchester Institute of Science and Technology » (UMIST) et diplômé de l'Ecole Supérieure de Technologie Electrique (Groupe ESIEE). Ancien Président de CYBER NETWORKS (aujourd'hui BT France) qu'il a fondée avec Laurent Charvériat, il est aussi ancien co-fondateur de la société de conseil en télécommunications DataStaff - Noméa, devenue Dimension Data France.

Après un stage de Master of Science chez Coopers & Lybrand (UK), Théodore-Michel Vrangos a démarré sa carrière comme ingénieur d'affaires au sein du Groupe Générale des Eaux (Vivendi) à Paris.

Laurent CHARVERIAT

Ingénieur ENTPE, Laurent Charvériat est Directeur Général et CTO d'I-TRACING, entreprise qu'il a cofondée avec Théodore-Michel Vrangos en 2005. Auparavant Directeur Général et CTO de la société Cyber Networks, entreprise qu'il avait cofondée avec T-M Vrangos et intégrée depuis à BT France, et préalablement responsable réseau au Ministère de l'Equipement, il évolue depuis 20 ans dans le domaine de la Sécurité des Systèmes d'Informations.

Il possède une parfaite connaissance des problématiques, des méthodologies et des solutions de sécurité SI, télécoms et applicatives et des problématiques de traçabilité et de gestion des preuves. Il intervient régulièrement auprès des grands comptes français et internationaux et des administrations pour les accompagner dans leur démarche de sécurisation de leurs systèmes d'informations et de leurs données sensibles. Il participe aussi en tant que conférencier à de nombreux séminaires et manifestations dans le domaine de la sécurité.

« L'information dématérialisée se trouve au cœur de la création de valeur de toute entreprise. La maîtriser n'est donc plus une démarche optionnelle ou opportuniste. Il s'agit d'un enjeu-clé que toute entreprise se doit d'intégrer »

Les pages suivantes regroupent quelques points de vue d'auteurs, associés chez I-TRACING.

Point de vue

Cyber-espionnage

Espionnage et fuite de données, légende ou réalité ?

Par Théodore-Michel Vrangos, président et cofondateur d'I-TRACING

Durant 4 mois, les 53 employés de la rédaction du New York Times ont été piratés par des hackers. L'attaque, en provenance de Chine, coïncide ou plutôt débute le 25 octobre 2012 lors de la publication par le journal d'une série d'articles sur l'enrichissement illicite des hauts membres du comité central du parti communiste chinois.

Non, ce n'est pas un mythe : la guerre de l'information a bien lieu. On assiste chaque jour à la perturbation des réseaux et des infrastructures numériques. Et le phénomène s'amplifie, à la mesure de l'importance de la révolution numérique. Des délinquants pénètrent sur les réseaux pour récupérer les informations qui y circulent ou qui sont stockées sur le système d'information. Piratage de données personnelles, cybercriminalité, espionnage, intrusions, vol d'informations stratégiques, APT, manifestations et revendications d'hacktivistes… l'inquiétude grandit au sein des directions informatiques. Les délits commis sur les systèmes d'information et les réseaux informatiques menacent les entreprises françaises et affectent le fonctionnement de l'économie et des institutions. Les cyber-territoires deviendraient-ils les champs de bataille des temps modernes au même titre que les airs et l'espace ?

Cyberguerre ou simple délinquance ?

La frontière entre les deux est très mince. La cyber-attaque est un art parfaitement maîtrisé par les organisations criminelles, les hacktivistes et les états. Cette réalité revêt de multiples formes. Il s'agit aussi bien d'une escroquerie comme le vol de numéros de cartes bancaires par une organisation mafieuse qu'une agression lancée contre un pays, comme ce fut le cas, en 2007, de l'Estonie, particulièrement en pointe dans l'usage quotidien des techniques numériques ou encore un déni de service visant des établissements financiers comme l'attaque récente de plusieurs banques américaines. Personne n'est épargné. Plusieurs ministères ont été victimes de vols massifs de données sensibles, des ONG et des entreprises ont été espionnées. Aujourd'hui, les entreprises sont aussi le théâtre d'opérations de la guerre du Net. L'été dernier, le quotidien Le Monde rapportait qu'une cinquantaine d'entreprises, appartenant au secteur de la défense et de l'industrie chimique, avaient été victimes d'une série d'intrusions informatiques. Ces intrusions étaient coordonnées : les ordinateurs des dites sociétés auraient été infectés par un programme malveillant, utilisé pour dérober des informations. Les informations volées étaient protégées par la propriété intellectuelle. L'espionnage industriel semble bien être le mobile de cette vaste attaque.

Vers un cyber-espionnage généralisé ?

Dans une économie de l'immatériel, les biens numériques acquièrent de la valeur. Certains sont convoités pour leur valeur informative (invention, plan stratégique…), d'autres pour leur valeur commerciale (certaines bases de données se revendent). Pour s'en emparer, certains rémunèrent les services des pirates informatiques. La dématérialisation permet d'agir à distance, souvent depuis un pays où la législation est moins répressive, et sans les risques que comporte la délinquance physique, grâce à l'anonymat des auteurs. Il est même facile d'usurper une identité pour "pénétrer" dans des zones interdites comme des bases de données confidentielles ou des centres de paiement.

Dans son rapport "*La cyberdéfense : un enjeu mondial, une priorité nationale*", le sénateur Jean-Marie Bockel s'inquiète de l'ampleur de l'espionnage industriel qui se traduit par des pertes économiques atteignant de 3 à 5 milliards d'euros par an. Pour lui, nul doute, la cyberdéfense est devenue une priorité stratégique absolue.

L'augmentation des attaques ciblées envers les entreprises et les institutions est plus que préoccupante. Cette tendance ne devrait pas s'inverser dans les prochaines années en raison des gains potentiels pour les cybercriminels. Le spectre des attaques s'élargit même. Les cibles jusque-là privilégiées des grandes entreprises sont rejointes par de plus petites structures. Les auteurs utilisent de nouveaux vecteurs d'attaques. La tendance irréversible du BOYD facilite les intrusions. L'infection d'appareils mobiles privés comme les tablettes, les smartphones ou les MP3 permet de s'introduire dans les entreprises. Il n'est plus nécessaire d'être un expert en informatique pour fomenter une attaque. Des kits d'exploits prêts à l'emploi sont vendus en ligne !

Il est très inquiétant et déconcertant d'observer avec quelle facilité on peut entrer dans un système d'information pour y voler des informations ! Les entreprises assistent, impuissantes, à la fuite de leurs données ou plutôt, dans nombre de cas, se rendent compte du cambriolage quelques temps après qu'il ait été effectué. Qui commandite ces vols ? Quels moyens n'hésitent pas à employer certains acteurs pour espionner leurs concurrents ?

Les APT, un type nouveau de menace

APT. Trois lettres qui donnent des sueurs froides aux Responsables Informatiques. Les *Advanced Persistent Threats*, couramment appelées APT, font parties des pires menaces actuelles. Pour les experts, il ne s'agit pas d'un mythe. Bien réelles, les APT concernent aussi bien les états que les entreprises et les organisations. Chacun doit être conscient du savoir-faire de certains cybercriminels, prêts à s'introduire dans le système d'information de l'entreprise pour voler des informations sensibles. RSA, Sony, Google - et bien d'autres encore - ont été victimes d'attaques informatiques très ciblées, compromettant leurs données stratégiques. Mais aujourd'hui, encore trop peu d'entreprises et d'administrations sont véritablement préparées à contrer ces menaces 'intelligentes'.

La patiente stratégie des espions

Complexes et très sophistiquées, les menaces persistantes avancées ciblent les actifs de valeur de l'entreprise que sont les informations stratégiques. Invisibles, elles peuvent se dérouler sur une période assez longue. Une APT est une attaque ciblée qui s'appuie sur un logiciel malveillant, taillé sur mesure et capable de contourner les dispositifs de sécurité en place. Elle relève d'une association de malfaiteurs - et non plus d'un pirate isolé - qui s'infiltre dans une entreprise pour l'espionner. Une APT se termine toujours par le vol de données sensibles.

Les auteurs d'APT déploient des efforts considérables pour que leurs actions restent inaperçues. Ils passent furtivement d'un hôte compromis à un autre, sans générer de trafic réseau. Certains hackers font muter le code utilisé, déjouant ainsi les solutions de sécurité en place pour demeurer indétectable. Il est courant qu'une entreprise attaquée ne s'en rende compte que tardivement. Lockheed Martin détecte une intrusion qui a permis de détourner des données liées à la conception du nouvel avion de chasse F-35 Lightning II, en 2009. Les systèmes informatiques impliqués dans la fuite d'informations auraient été infiltrés quelque 2 ans auparavant. Les pirates-espions sont entrés grâce aux vulnérabilités de réseaux d'entreprises sous-traitantes. En chiffrant les données volées, ils ont brouillé les pistes et rendu difficile l'identification du butin et des auteurs.

Une APT est très souvent commanditée car son exécution demande des compétences informatiques sérieuses. Les exécutants sont parfaitement organisés. Ils sont financés par ceux à qui profite le crime. Pour arriver à leurs fins, ils utilisent un cocktail de moyens très bien dosé : cheval de Troie, par exemple, involontairement installé par un utilisateur imprudent, exploitation des vulnérabilités d'un logiciel ou d'un programme, mise en place d'outils divers pour des opérations ultérieures, etc.

Portait-robot d'une APT

Le mode opératoire est sensiblement le même d'une attaque à l'autre. Dans un premier temps, les utilisateurs de l'entreprise constituent la cible principale des pirates car ils serviront de point d'entrée. L'APT s'appuie sur l'ingénierie sociale. Le hacker se renseigne discrètement sur sa cible pour bien la connaître. Il lui sera alors plus facile de la convaincre de cliquer sur un lien ou d'ouvrir une pièce jointe. Une fois l'accès obtenu, le pirate essaie d'accroître ses privilèges. Il bénéficie au minimum des droits d'accès accordés à l'utilisateur légitime de la machine qu'il occupe à son insu. Des programmes d'exfiltration, des outils de chiffrement, des proxys… sont

introduits. L'attaquant explore le réseau pour atteindre les serveurs de données. Il utilise des vulnérabilités applicatives, des informations du poste compromis et tous les mécanismes qui lui permettront d'accéder à de nouvelles machines disposant de droits d'accès plus importants et contenant les informations sensibles qu'il recherche. L'exfiltration des données pourra ensuite commencer. Lorsque le hacker quitte le champ d'opérations, il efface les traces de son passage pour toujours demeurer parfaitement invisible.

En résumé, l'espionnage s'opère en sept phases plus ou moins longues, selon les obstacles rencontrés par le hacker.

1. Approche de la victime par ingénierie sociale ou autre moyen (par exemple keylogger installé à travers le flux web http, ou à travers un courrier de type spear-phishing - email de phishing particulièrement ciblé, etc.),
2. Infiltration furtive des systèmes cibles,
3. Mise en place d'un backdoor après pénétration sur le réseau,
4. Obtention des droits d'accès vers d'autres systèmes internes,
5. Installation d'un ensemble d'outils nécessaires à la clandestinité et à l'exfiltration de données,
6. Obtention de privilèges plus importants,
7. Exfiltration discrète et régulière des données.

La sécurité est un voyage pas une destination

Nous l'avons déjà dit, les entreprises rencontrent des difficultés à déceler les APT. Or, la virulence de telles attaques voudrait qu'elles soient détectées le plus tôt possible. Cela permettrait de minimiser les dégâts. Comment une entreprise peut-elle alors se défendre contre ce fléau ? Tout d'abord, il faut rappeler que même si toutes les entreprises ne sont pas équipées, la plupart des grands comptes disposent de protections efficaces pour défendre leurs biens les plus chers, les données sensibles. Mais, croire qu'il suffit d'acheter des pare-feu, des anti-malwares, des firewalls pour les bases de données, et toutes sortes de solutions pour que le système d'information soit entièrement sécurisé, est une grave erreur. Il est utopique d'imaginer que seule une panoplie d'outils technologiques constitue la parade infaillible à l'insécurité. Les équipements de sécurité - même les plus sophistiqués - doivent s'accompagner d'un certain nombre de règles et d'actions humaines de la part d'experts, qu'il faut impérativement respecter, d'une analyse des risques auxquels l'entreprise est exposée et d'un processus permanant de contrôle et de surveillance.

C'est ce que nous appelons un SOC (Security Operations Center) propre à l'entreprise ou externalisé chez un prestataire de services de sécurité, capable d'avoir à la fois la vision d'ensemble du système d'information et la connaissance du détail des flux de données. Un SOC est composé d'experts et d'analystes qui surveillent et scrutent les signaux en provenance des équipements de sécurité et du système d'information en général.

A travers un processus de SOC, la traçabilité de l'information est un moyen efficace pour dépister une attaque APT. La corrélation des logs, l'analyse des événements de sécurité, la prise en compte des incidents, l'examen des nombreuses informations disponibles souvent en temps réel, la surveillance des actions et connexions des comptes à privilèges… fournissent de précieuses indications et permettent de savoir s'il y a danger.

La requête d'un domaine avec lequel l'entreprise n'a pas de relation, l'accès anormal à certaines ressources ou la transmission de fichiers chiffrés vers des hôtes externes en dehors des processus de transmission de données classiques sont quelques exemples d'opérations pointées par la traçabilité de l'information, qui doivent retenir toute l'attention pour éviter le pire.

Informer ses propres troupes du danger

D'une part, les entreprises se sont dotées de solutions de sécurité pertinentes, d'autre part, les APT perdurent. On est en droit de se demander où est le maillon faible.

Le facteur humain joue un rôle essentiel dans la lutte contre les menaces. Rien ne sert de mettre en place une politique de sécurité si les règles ne sont pas respectées. Très peu d'entreprises disposent aujourd'hui de procédures formalisées par écrit, à appliquer en cas de vulnérabilité. C'est pourquoi, il n'est pas rare d'observer des réactions confuses et un manque de réactivité de l'administrateur lorsqu'un risque se déclare.

Les APT exploitent souvent des vulnérabilités connues. Or, des patchs sont régulièrement publiés par les éditeurs pour remédier aux vulnérabilités. Mais, les cyber-attaquants savent qu'ils ne sont pas toujours

déployés. Aussi continuent-ils de mener leurs attaques en exploitant de vieilles vulnérabilités connues. Pour y remédier, il n'existe qu'un moyen : informer les utilisateurs des risques et des dangers.

En France l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) réalise un travail important de sensibilisation et d'information. Mais, les entreprises ne mesurent souvent qu'après le sinistre, l'étendue des dégâts. Une investigation complète de type forensics (analyse post-mortem de l'incident, évaluation des compromissions, définition de plans d'actions, etc.) et surtout la mise en conformité des systèmes après l'incident, ont des coûts non négligeables.

Une APT débute souvent parce qu'un salarié mord à l'hameçon. Sensibilisé aux problèmes de sécurité, le salarié devient plus vigilent. Sa prudence lui permet de déjouer les pièges tendus par les cybercriminels qui veulent l'amener à ouvrir la porte du système. L'attaque de RSA d'EMC où des données sensibles ont été dérobées, a été déclenchée par un employé qui a ouvert un fichier Excel malveillant, reçu par courrier électronique et qui exploitait une faille inconnue de Flash. S'il avait été informé du danger, ce salarié aurait probablement fait preuve de plus de discernement.

La menace nous concerne tous

Sur le plan technique les APT ne sont pas particulièrement « avancées ». Elles utilisent les mêmes outils que d'autres types d'attaque. Mais, sur le plan « business », il s'agit d'un fléau sans commune mesure. Ce sont actuellement les cyber-menaces les plus virulentes. Elles plongent le monde dans une insécurité permanente où chacun doit se préparer aux crises qui en résultent. Bien réelles, les menaces persistantes avancées visent tous les secteurs économiques et touchent toutes les entreprises, de la PME au grand groupe. Les directions générales, les DSI et les responsables de la gestion des risques doivent de toute urgence évaluer leur exposition face aux APT pour prendre des mesures préventives et correctives.

La lutte contre la fuite des données illustre le paradoxe de notre société de l'information qui est devenue une société du risque. Depuis des années les spécialistes alertent les pouvoirs publics sur l'ampleur de l'espionnage dont sont victimes les entreprises françaises et sur la nécessité de renforcer leur protection. Une loi sera-t-elle suffisante pour faire baisser le cyber-espionnage industriel, comme semble le penser le Gouvernement ? L'avenir proche nous le dira.

Point de vue

Les comptes à privilèges, talon d’Achille de la sécurité des systèmes d’information ?

Par Michel Vujicic, Directeur Associé d’I-Tracing.

La traçabilité des accès et des opérations des utilisateurs à privilèges au service de la détection des cyber-attaques et du combat contre les menaces internes.

Les attaques auxquelles nous assistons actuellement confirment l’importance de la gestion des identités des utilisateurs privilégiés. L’authentification des utilisateurs et la traçabilité des accès et des opérations réalisées demeurent, sans aucun doute, le point faible d’un système d’information de plus en plus ouvert au monde extérieur.

Conserver le contrôle du système d’information

Avec la pratique incontrôlée du BYOD (Bring your own device), l’externalisation des maintenances et l’infogérance ou la généralisation des pratiques de Cloud Computing - sujets très discutés et controversés lors des dernières Assises de la Sécurité - la gestion des identités se trouve au cœur du débat. Les programmes de sécurité informatique détectent et empêchent les violations de données. Pourtant, il ne se passe pas un jour sans que de grandes entreprises, appartenant à tous les secteurs de l’économie, soient victimes d’intrusions, de piratages ou de vols d’informations. Les données sensibles sont souvent consultées, voire dérobées, à l’insu de leur propriétaire !

Pour accéder aux données sensibles, il faut entrer. Les attaques et les fuites de données prouvent, s’il est besoin de le faire, que la gestion des identités et des accès reste une faiblesse importante du système d’information. Que la violation des données soit le fruit de l’attaque ciblée d’un cybercriminel ou résulte de l’‘*erreur*’ d’un utilisateur privilégié, l’impact est désastreux et peut prendre rapidement des proportions insoupçonnées.

La préoccupation majeure des Responsables de la Sécurité demeure bien évidemment le maintien de la capacité opérationnelle du système d’information. Ils doivent tout mettre en œuvre pour conserver un niveau de sécurité élevé. Mais, c’est une mission impossible si la surveillance des accès au système et aux ressources et plus particulièrement, des accès des comptes à privilèges, est négligée. Pour mieux communiquer entre collaborateurs, partenaires et clients, les applications se sont multipliées, renforçant la place du réseau au cœur de l’entreprise mais fragilisant son système d’information. Le contrôle des accès permet d’identifier qui est présent sur le réseau - c’est l’authentification - et connaître les ressources utilisées par chaque personne connectée.

Menaces externes ou menaces internes ?

Quelle que soit la source, il faut les combattre et veiller à ce que les données sensibles soient protégées. D’ailleurs, lorsqu’un pirate obtient l’accès à un compte utilisateur interne comment distinguer son comportement d’une activité légitime ?

La majorité des grands comptes sous-traitent la gestion de la totalité ou d’une partie de l’administration et de la supervision du système d’information. Déléguer des opérations techniques sur le système d’information, pôle stratégique de l’entreprise, à des intervenants externes comporte des risques. Interdire les opérations qui pourraient se révéler dangereuses et conserver la trace de toutes les interventions est indispensable. Par ailleurs, l’entreprise doit pouvoir prouver sa conformité aux normes et obligations réglementaires (ISO 27001, CNIL, Sarbanes-Oxley, PCI-DSS, conformité Bâle 2, « Paquet Télécom », …). La surveillance de l’intégrité des fichiers est un facteur-clé pour assurer la conformité aux normes de sécurité informatique des données.

Certaines menaces internes sont malveillantes, d’autres non. Dans le second cas, les systèmes et les données stratégiques sont involontairement exposés, par erreur ou par manque de discernement. Il s’agit d’un courrier électronique ou d’une application mal utilisée, d’un ordinateur portable ou d’un smartphone perdu ou volé…

Les dangers qui en découlent restent toutefois une réelle préoccupation. Dictées par le gain, la rancœur contre l'employeur ou toute autre motivation, les menaces internes malveillantes risquent d'engendrer d'importants dommages. On constate malheureusement que les infractions les plus graves sont souvent causées par des utilisateurs disposant de privilèges élevés. On constate aussi que les salariés bénéficient souvent de plus de privilèges qu'ils n'en ont besoin pour effectuer leur travail.

Les comptes à privilèges, sources d'insécurité

Nous devons prendre conscience que les comptes à privilèges, parce qu'ils sont anonymes et ont tous les droits, font courir de grands risques à l'entreprise ! Rien n'empêche un utilisateur mal intentionné de prendre le contrôle du système et d'accéder à l'ensemble des informations. Il peut même effacer ses traces, comme on le voit dans de nombreuses affaires de piratage.

Le « 2010 Data Breach Investigations Report » de Verizon Business, effectué en collaboration avec les services secrets américains, souligne que 48 % des violations de données sont internes ; ce qui représente - ce n'est pas négligeable - une augmentation de 26% par rapport à 2008 ! Dans la plupart des infractions, des privilèges importants avaient été accordés à des membres du personnel ! Une autre enquête, réalisée par B2B International en juillet 2012, révèle que 33% des entreprises accordent à leur personnel un accès sans restriction à leurs ressources à partir de leur smartphone !

Il est normal d'octroyer des pouvoirs à ceux qui en ont besoin. Mais, il est capital de conserver la maîtrise et le contrôle des opérations effectuées sur le système d'information. Prenons l'exemple des comptes administrateur. Ces comptes à privilèges sont utilisés pour exécuter des tâches d'administration comme modifier la configuration d'un équipement. Une mauvaise manipulation pourrait causer une interruption de service. L'entreprise serait alors sévèrement sanctionnée. La baisse de la qualité du service est dommageable à son image, à sa notoriété et se révèle souvent coûteuse.

Tracer et contrôler les interventions sur le S.I.

Si l'utilisation des comptes à privilèges est indispensable, quelles précautions prendre pour protéger les données sensibles ? Dans le cas où l'administration et la supervision du système d'information sont déléguées à une société externe, le périmètre d'intervention autorisé doit être défini. En aucun cas, le personnel du prestataire ne doit avoir accès à l'ensemble du système d'information, pas plus qu'il ne doit connaître les mots de passe des comptes à privilèges dont il dispose pour exécuter les tâches qui lui sont confiées. Des autorisations d'accès temporaire au système permettront aux sous-traitants de travailler. Toutefois, des dispositions particulières seront prises lorsque des tâches sont externalisées chez un fournisseur, installé dans un pays reconnu à risques en matière de protection des données personnelles (cf. la liste des pays à risques établie par la CNIL).

En cas d'incident, retracer ce qu'il s'est passé est essentiel ; en particulier, lorsque les intervenants sur un même serveur ou une même application critique sont nombreux. Qui a fait quoi ? Sur quel équipement ? A quel moment ? Des solutions, appelées solutions d'*accès à rebond* garantissent la sécurité et assurent le contrôle et la traçabilité des opérations. La conservation des traces des actions effectuées sur le système permet de savoir quelles opérations ont été exécutées par les utilisateurs à privilèges. L'activité étant enregistrée (en vidéo dans certains cas), des recherches *post-mortem* par mots-clés sont possibles. La traçabilité totale des opérations facilite le diagnostic des incidents critiques. La maîtrise de la gestion des partenaires et des salariés devient alors aisée. Et ce, dans le respect du cadre légal.

Quelle solution à rebond choisir ?

Le *rebond* est une machine dont l'accès est limité aux personnes, individuellement autorisées à le faire. Il a pour vocation de permettre comme point de passage obligé, les connexions aux équipements informatiques. Les solutions à rebond centralisent les accès des utilisateurs en un point unique afin de maîtriser, contrôler et auditer l'utilisation des comptes à pouvoir. Elles mettent en œuvre tout ou partie des fonctions de sécurité telles que l'authentification, la gestion des habilitations par périmètre et la traçabilité. Certaines incluent la protection des secrets en permettant à un administrateur de se connecter à un équipement sans en connaître le mot de passe. Il convient évidemment de choisir la solution à rebond qui s'adapte à l'environnement technique du système d'information, qui s'interface notamment avec les fonctions de sécurité existantes comme la gestion des identités, des profils, la PKI ou la détection d'incidents de sécurité et qui prend également en compte les contraintes opérationnelles des exploitants.

Il existe plusieurs types de solutions. Une solution en mode *bastion* dispose d'une double connexion pour contrôler la session finale par les opérations sur le rebond. Une solution en mode *proxy* fournit l'analyse « transparente » des flux réseau pour contrôler la session système cible. On peut adopter une solution avec *agent de traçabilité* ou un *rebond packagé*. Il est aussi possible de choisir un *coffre-fort* de mots de passe si besoin. Les mots de passe des comptes à pouvoirs sont des secrets critiques. Certaines solutions permettent de limiter la communication de ces secrets - l'utilisateur n'ayant pas besoin de connaître le mot de passe du système pour se connecter - voire intègrent la gestion du renouvellement de ces secrets sur les systèmes.

Enfin, la solution doit tenir compte des protocoles en vigueur au sein de l'entreprise. Les solutions supportent les principaux protocoles - y compris ceux qui utilisent des mécanismes de chiffrement comme RDP et SSH. Elles intègrent plus ou moins efficacement d'autres protocoles comme ICA, Vmware View, Telnet, VNC et http selon les technologies mises en œuvre dans l'entreprise.
Les transferts de fichiers et les clients lourds nécessitent une attention particulière.

Facile à mettre en place, une solution d'accès à rebond maintient la sécurité du Système d'Information à un niveau élevé. Les autorisations d'accès sont centralisées et les accès directs anonymes avec les comptes administrateur sur l'équipement-cible supprimés. La traçabilité des opérations permet de combattre les menaces internes et détecter plus rapidement les attaques qui malheureusement se multiplient.

Point de vue

Cyber-délinquance

Les applications et les bases de données sont des portes dérobées pour cambrioler l'entreprise en toute discrétion

Par Laurent Besset, Directeur Associé chez I-Tracing

Les données représentent un enjeu majeur pour les entreprises. Leur valeur les rend attrayantes aux yeux des pirates mais aussi des utilisateurs internes peu scrupuleux. Les différentes réglementations (Sarbanes-Oxley, PCI-DSS, CNIL…) obligent les firmes à mettre en place des dispositifs de protection et d'audit des données. La sécurité de l'information et le respect des bonnes pratiques s'avèrent d'autant plus indispensables que le système d'information s'ouvre et qu'Internet accroît les risques. La fuite de données a un impact sur tout l'écosystème de l'entreprise. Collaborateurs, clients, partenaires et fournisseurs se trouvent affectés. Un vol de données se traduit aussi par d'importantes pertes financières. Toute entreprise, quelle que soit sa taille, doit contrôler les conditions d'utilisation de ses données et mettre en œuvre une protection adaptée à ses systèmes d'information et aux nouveaux usages en entreprise afin de se défendre au mieux contre le pillage, le vol et les comportements malveillants internes.

Facilement accessibles, les applications web sont devenues les cibles favorites des cyber-voleurs qui les transforment en un point d'entrée pour accéder aux données sensibles. Les entreprises et les administrations, dont l'activité repose de plus en plus sur les technologies et les applications web, veulent protéger leur site internet contre les menaces environnantes, sans affecter les performances et la disponibilité des applications. Lutter contre une attaque par DDoS ou combattre une APT (*Advance Persistent Threat*, menace invisible mais permanente), commence par l'adoption des bonnes pratiques durant le développement et le cycle de vie des applications. C'est un élément capital de la maîtrise des risques.

Anticiper les failles applicatives

La sécurité applicative recouvre la sécurité des composantes transverses, c'est-à-dire du serveur web et du serveur d'applications qui permettent à l'application de fonctionner, mais recouvre aussi la sécurité des développements logiciels spécifiques, sans oublier les processus de création, de gestion des profils, les fonctions d'authentification, de gestion d'identités, etc.

Les serveurs possèdent leurs propres failles. Les pirates les exploitent pour prendre la main sur le système d'information. Mais le danger le plus grave peut provenir de failles directement ou indirectement liées aux négligences de sécurité dans le développement même de l'application. Un traitement dont les paramètres ne sont pas vérifiés produit obligatoirement des failles, permettant un passage aussi facile qu'une porte sans serrure. Par exemple, la légitimité des demandes de l'utilisateur doit être établie. Sinon, rien ne l'empêche d'outrepasser ses droits et d'accéder - directement ou non - à des données auxquelles il ne devrait pas accéder. Le Cross Site Scripting et tous les types d'injection (SQL, java script…) peuvent mettre en péril les données de l'entreprise. Les pirates savent très bien utiliser les failles d'injection pour dérober des données. C'est ce qu'il s'est passé, par exemple, lors de l'attaque du réseau PlayStation qui s'est terminée par un vol de données chez Sony. Les requêtes ont été directement envoyées à partir de l'application dans… la base de données ! Nombre d'applications web et d'applications sur mobile révèlent des vulnérabilités comme l'absence de contrôles ou la non-conformité avec la réglementation. La sécurité applicative est avant tout une affaire de bon sens. Le maillon faible reste une fois encore le facteur humain.

Détecter les comportements anormaux

Dans le monde web, la connexion au réseau n'est pas continue. Chaque page est transmise par une connexion séparée. Il est donc impossible que le serveur détecte si une séquence de requêtes provient du même client. Sur le plan applicatif, des éléments tiers comme les cookies sont utilisés dans les échanges entre le client et le serveur pour maintenir la session.

Tout utilisateur doit s'identifier. Et ce, afin d'éviter qu'un utilisateur "mal intentionné" accède à des données sensibles ou simplement… « plante » le système. Une bonne sécurité des accès prévient les usurpations d'identité et les attaques DoS et DDoS de l'infrastructure. Mais il existe aussi des risques liés aux dénis de service applicatifs comme en témoigne l'exemple suivant. Une compagnie d'assurance fournissant des devis en ligne pourrait se retrouver « noyée » sous le nombre de demandes, si l'application ne tient pas compte des éventuels comportements dangereux. Recevoir 50 ou 100 demandes de devis à la minute est tout à fait anormal ! Cette avalanche de requêtes ne peut provenir que de robots ! L'application doit reconnaître et bloquer les demandes de scanners et d'automates. En bref, une application doit prévoir tout ce qu'il faut autoriser et tout ce qu'il faut interdire ! En d'autres termes, lors de la conception de l'application, on doit projeter et anticiper les situations et les comportements anormaux qui pourraient se présenter et incorporer les outils pour les contrer.

Comment remédier aux failles ?

S'il s'agit de failles du serveur web ou du serveur d'applications, il est notamment indispensable d'*exécuter chaque mise à jour*. Les éditeurs fournissent des correctifs, quelques jours après la découverte d'une faille. Pour les failles applicatives, il convient de *sensibiliser et former les développeurs* afin qu'ils prennent toutes les précautions sécuritaires. Ils devront tenir compte des éventuels abus et des comportements anormaux possibles lorsqu'ils concevront l'application afin d'éviter les dénis de service applicatifs. Il est essentiel de mettre en place un cycle de développement sécurisé, d'auditer et tester le code puis de vérifier le fonctionnement de l'application.

Par ailleurs, une nouvelle génération de pare-feu, les Waf (Web Application Firewall) compensent les failles applicatives en bloquant les requêtes dangereuses des attaquants qui exploitent les vulnérabilités des applications pour voler des données par déni de service.

Ils sont complétés par des fonctions de type DAM (Database Activity Monitoring) de plus en plus nécessaires pour le monitoring et la sécurisation des bases de données.

Eliminer les attaques automatisées

Pour éviter les demandes piégées, des composants complémentaires s'intègrent et s'ajoutent aux firewalls, garantissant que la requête n'est pas exécutée par un robot depuis un poste piraté, mais émane d'un internaute. Imaginons qu'un pirate cherche à pénétrer dans une banque via une application. Sans mot de passe qui lui permettrait de s'identifier, il va exploiter une faille applicative pour accéder aux données. Il essaie - c'est ce qu'on appelle une APT (Advanced Persistent Threat) - à partir du poste de Monsieur X et à son insu, d'atteindre l'application. Parce que le poste de Monsieur X est compromis par un virus ou un backdoor, il accède directement à l'application en récupérant les éléments voulus. Pour éviter cette situation, l'intégration de composants complémentaires comme Captcha s'il s'agit, par exemple, d'un formulaire à remplir, est nécessaire dans l'application. Ces composants permettent d'assurer que les demandes faites à partir du poste de Monsieur X proviennent bien d'une personne, en l'occurrence de Monsieur X.

Réputation des adresses IP

La localisation des adresses IP source est possible. Une cartographie existe. Prenons l'exemple d'une billetterie qui reçoit des demandes de réservation pour un concert qui a lieu le soir même à Paris. Plusieurs demandes de réservation émanent du Japon. De toute évidence, ces requêtes paraissent suspectes ! Comment se rendre aussi rapidement d'un pays à l'autre ?

Les adresses IP des postes zombies sont connues. A l'origine de spams, de phishing…, elles sont répertoriées. Grâce à la gestion dynamique des adresses IP, les demandes émanant de pays à risques peuvent être éliminées. Il suffit de le prévoir lors de la conception de l'application.

Protection des données des bases de données

La sécurité de la base de données commence par une réflexion sur les usages, les utilisateurs et la manière dont s'effectuent les accès. Les bases de données sont souvent critiques pour l'entreprise. L'ouverture du système d'information accroît les risques. Respecter les bonnes pratiques s'avère indispensable. Suivre les patches évite que les failles du serveur de bases de données soient exploitées par un cybercriminel qui cherche à prendre la main sur le système.

La sécurité des données de la base de données repose sur la sécurité du serveur de bases de données (Oracle, SQL Server…). Les données sensibles, les informations financières, les fichiers des ressources humaines et les données personnelles des clients se trouvent dans les bases de données de l'entreprise. Il faut donc s'assurer de la légitimité des requêtes et des accès des applications pour éviter qu'une attaque cible l'entreprise,

affectant son activité, la déstabilisant, dégradant son image et mettant en cause la responsabilité de son dirigeant. La valeur des données contenues dans la base de données la transforme en une proie évidente. D'où l'importance, encore une fois de la sécurité applicative. Cependant, des applications différentes accèdent à un même serveur de base de données. Au niveau du serveur d'applications, l'accès aux données de la base est global.

Outre la protection contre les attaques, la sécurité de la base de données inclut la traçabilité, l'intégrité et la confidentialité des données. Chiffrer les données sensibles est impératif. Or celles-ci apparaissent souvent en clair dans la base de données ; ce qui représente un risque important car toute personne qui accède à la base de données, peut les lire ! Afin d'éviter tout accès illicite de l'administrateur (qui possède un compte à privilèges lui donnant un droit d'accès à toutes les données de la base de données), il existe plusieurs solutions comme les firewalls de base de données et les audits de traçabilité des comptes à privilèges. Le *firewalling* de la base de données - global ou spécifique - s'applique à l'ensemble des accès des administrateurs qui sont tracés et *loggés*. La vérification des requêtes est alors effectuée.

Détecter les données sensibles de la base de données

Certaines solutions permettent d'inventorier les données sensibles. Leur emplacement et leur type (n° SS, n° carte bancaire…) sont repérés en scannant la base de données. Une des règles fondamentales de sécurité exige de n'utiliser aucune donnée réelle de production lors du développement, de la validation ou de l'homologation. Les données employées doivent être anonymes ou totalement imaginées. L'observation de cette consigne élimine le risque d'utiliser des données personnelles.

En résumé, la sécurité doit être conçue pour l'ensemble des éléments du système d'information. Une base de données fait partie d'un projet global. Elle doit être protégée. Mais, si l'outil utilisé pour s'y connecter est vulnérable, il ouvre la porte du système d'information. La sécurité de la base de données repose d'abord sur celle du serveur de base de données. Mais, il faut aussi prévoir une sécurité applicative, regroupant la sécurité de toutes les composantes qui permettent à l'application de fonctionner, c'est-à-dire la sécurité du serveur web, des serveurs d'applications et des développements spécifiques. Par ailleurs, les serveurs peuvent avoir leurs propres failles. Certains se sont illustrés de manière célèbre. Un exploit lié à une faille du serveur web peut potentiellement permettre de prendre la main sur le serveur.

La solution retenue devra évaluer les risques inhérents à l'utilisation des données, vérifier leur conformité et permettre la mise en place d'une politique de sécurité appropriée.

Pour tout renseignement complémentaire :
Migé Gauchet - mige.gauchet@free.fr - Portable : + 33 (0)6 84 77 31 74
Théodore-Michel Vrangos - tmvrangos@i-tracing.com - Tél. : + 33 (0)1 41 02 50 71