CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 18 – Mars / Avril 2016

CyberÉdito

La période étant propice aux rétrospectives, le CLUSIF a présenté le 14 janvier 2016 son 15e panorama sur la cybercriminalité.
L'année 2015 a été riche en évènements en tout genre :

- en marge des attentas de janvier 2015, 1550 dégradations de sites et attaques DDoS en 10 jours et aucune en novembre ;
- une propagation ciblée en France du malware Dridex, mais sans grande ampleur ;
- l'attaque de TV5 Monde où l'on constate pour la première fois une volonté claire de détruire l'entreprise ;
- plus d'un million d'empreintes digitales dérobées dans l'affaire OPM aux États-Unis ;
- la divulgation des données personnelles des abonnés d'Ashley Madison, avec une conséquence finalement inattendue en France puisque le nombre d'abonnements aurait augmenté !
- enfin, les risques liés à l'usage des IoT bien que les attaques restent à ce jour à l'état de preuve de concept : la possibilité de prendre la main à distance sur une voiture, sur une lunette de visée d'arme militaire ou sur des équipements médicaux.

Aucun système n'est épargné, mais on ne note finalement pas de grandes innovations, en dehors de l'ampleur des attaques. On assiste toutefois à une professionnalisation de la menace illustrée en 2015 par le marché des 0-day : un million d'euros pour des failles sur iOS 9, la levée de fonds de 25 millions d'euros par une place de marché de bug bounty (HackerOne) et le développement de grossistes spécialisés tels que Zerodium (ex Vupen). Il y a tout de même de bonnes nouvelles : les OIV (français) n'ont pas (encore) subi d'attaques aux conséquences dramatiques que l'on peut imaginer. La France a-t-elle réagi à temps ou est-ce l'attaquant qui n'a pas encore les moyens ?

À la lumière de ces éléments, il parait hasardeux de faire des projections sur ce qui nous attend en 2016. Seule certitude : un renforcement de la loi est à prévoir. Le facteur de risque pourrait donc provenir du législateur. Désormais, en 2016, le défi est de préparer le SI face aux risques liés au nouveau Data Privacy Shield, aux sanctions d'un million d'euros susceptibles de peser sur les contrevenants à la LPM ou encore à celles prévues pour les entreprises qui ne respecteraient pas le règlement européen sur les données à caractère personnel, jusqu'à 4% du CA. Ces évolutions nécessiteront des transformations des SI parfois significatives, dans un climat de forte pression économique.

Jean Olive – Manager CGI Business Consulting

Parole d'un CyberExpert

La sécurité des architectures à base de conteneurs

Exit le SOA. Bienvenue dans le monde des architectures microservices. Bienvenue à la solution phare de containerisation qui va avec : Docker. Longtemps considéré comme une technologie *hype* pour quelques développeurs de la Silicon Valley, ce nouveau paradigme atteint sa maturité depuis peu et sera généralisé. Plusieurs entreprises l'utilisent déjà en production : Netflix, Spotify ou encore Shopify.

En simplifiant à l'extrême le déploiement, Docker ouvre la possibilité d'une meilleure prise en charge des problèmes de sécurité : plus besoin de redéployer l'application à chaque modification.

Cependant, ces bénéfices s'accompagnent également de nouveaux risques : comment établir la confiance entre plusieurs microservices qui échangent des données ? Les conteneurs sont-ils réellement isolés ? Être administrateur dans un conteneur, c'est être administrateur sur l'hôte ou uniquement sur une partie ? Pourquoi transférer tant de pratiques de sécurité à des développeurs alors que les exploitants faisaient le travail ?

La virtualisation a nécessité une organisation et des pratiques de sécurité dédiées. Il en sera de même avec les microservices containerisés : renforcement des machines hôtes, utilisation d'outils spécifiques de gestion (équivalents aux hyperviseurs), formation des développeurs et exploitants, etc.

Avant d'autoriser ces déploiements dans vos organisations, interrogez-vous et assurez-vous d'appliquer des mesures de sécurité adaptées. Des guides vous y assistent déjà, afin d'éviter une catastrophe qui réduirait la confiance dans une technologie qui est sur le point de devenir incontournable.

Rémi Kouby — Consultant CGI Business Consulting

CyberMenaces

IE 8, 9 et 10 ne sont plus supportés. Migrez !

Passée beaucoup plus silencieusement que la fin du support de Windows XP, celle des anciennes versions d'Internet Explorer n'en est pas moins inquiétante. De nombreuses entreprises utilisent encore IE 9 ou 10 avec Windows 7. Sachant que IE a été l'un des composants les plus concernés par des alertes de sécurité, notre conseil : migrez avant la prochaine faille critique !
Lire

Un réseau électrique protégé car cloisonné. Pas si sûr …

C'est désormais une quasi-certitude : la panne du réseau électrique ukrainien est due à une opération malveillante, organisée et multiforme (malware, DDOS, etc.). C'est une première mondiale. L'attaquant reste pour le moment inconnu.
Lire

Sécurisez-vous assez les PC reliés à des lecteurs de code-barres ?

Pas besoin, on ne peut pas y accéder ! En êtes-vous certains ?. Comme le présente ce chercheur, les scanneurs étant reconnus comme des claviers par les PC, il est possible d'envoyer des codes de frappes clavier qui seront ensuite interprétés par Windows.
Lire

La fin du SHA-1 : l'heure est arrivée

L'algorithme de hachage SHA-1 est vulnérable. Depuis le premier janvier 2016, les autorités de certification ne délivrent plus de certificats utilisant cet algorithme. De plus, les principaux navigateurs (Chrome, Firefox et Internet Explorer) ont annoncé leur plan de dépréciation, de juillet 2016 jusqu'à janvier 2017.
Autre chose à prévoir : des incompatibilités logicielles avec les certificats SHA-2 existent. C'est par exemple le cas de Windows XP SP2 ou Apache 1 qui ne supportent pas les certificats SHA-2.
Lire

Réponses aux CyberMenaces

Les guides de l'ENISA

Évaluation de la maturité d'un CERT, bonnes pratiques pour la sécurisation des systèmes de transport intelligents ou encore état de l'art des technologies d'intégration de la sécurité à la chaine de valeur « Big Data », voici quelques-uns des guides récemment publiés par l'ENISA.
Lire

Du chiffrement dans les ministères

L'ANSSI signe un contrat de licence globale avec PrimX, une société française spécialisée dans le chiffrement. La licence prévoit 3 solutions de chiffrement (Cryhod, Zed et ZoneCentral) à déployer au sein des ministères et des administrations.
Lire

Data Privacy Shield : le nouveau Safe Harbor

Alors que le Safe Harbor vient d'être invalidé en octobre, les instances européennes ont trouvé un premier accord pour le remplacer. Il renforce les obligations vis-à-vis des entreprises américaines pour la protection des données personnelles des Européens.
Lire

CyberRèglementation

Règlement européen sur les données personnelles : les pays de l'Union arrivent enfin à s'entendre

Les trois instances européennes ont trouvé un accord le 15 décembre sur un texte du règlement. Dans l'attente d'une validation en séance plénière au Parlement, prévue au printemps 2016, ce texte devrait entrer en vigueur au plus tôt en 2018.
Lire

Un accord sur la future directive européenne NIS

Le parlement européen et les États membres sont arrivés à un accord sur la future directive NIS. Cette règlementation prévoit des obligations en matière de signalement d'incidents de sécurité pour les entreprises et plateformes de services numériques. En particulier seront concernés les moteurs de recherche, les sites e-commerce et les fournisseurs Cloud ainsi que tous les acteurs de l'énergie, du transport et de la santé (une LPM à l'européenne).
Lire

Optical Center épinglé pour mauvaise gestion des données personnelles

Un consommateur porte plainte contre le fait qu'Optical Center lui a communiqué son mot de passe par téléphone. La CNIL enquête sur la gestion par l'entreprise des données personnelles. Résultat : Optical Center a écopé d'une amende « record » de 50.000 euros.
Lire

La CNIL verra-t-elle son pouvoir renforcé par la loi numérique

Cela reste encore à valider par les passages devant toutes les chambres, mais le pouvoir de la CNIL pourrait bien se voir renforcé par la nouvelle loi Lemaire. Les amendes pourraient aller jusqu'à 20 millions d'euros contre 150000 aujourd'hui.
Lire

CyberBrèves

Objets connectés : l'ANSSI craint le pire

Lors du Forum International de la Cybercriminalité 2016, l'ANSSI s'est montrée alarmiste au sujet de la sécurité des objets connectés. Guillaume Poupard, directeur général de l'ANSSI, a notamment mis l'accent sur les failles de sécurité touchant les dispositifs médicaux dont l'exploitation pourrait causer des décès de patients.
Lire

Des directeurs des services secrets américains victimes de piratages

Le directeur de la CIA a été victime d'un piratage de boite mail privée (vers laquelle il avait bien sûr transféré des documents confidentiels !). L'attaque a réussi grâce à des méthodes d'ingénierie sociale. Le pirate qui a réalisé l'attaque a décrit son mode opératoire.
Lire
L'auteur a également piraté les accès aux comptes téléphoniques et Internet du directeur du renseignement américain.
Lire

SCADA+, des failles 0-day à prix discount

La société russe Gleg, spécialisée dans la recherche et la revente de failles 0-day, propose un module complémentaire au logiciel de test d'intrusion Immunity Canvas. Cet *add-on*, nommé SCADA+, renferme un ensemble de vulnérabilités et failles 0-day spécifiques aux systèmes industriels. La surprise est que vous pouvez vous offrir ces moyens opérationnels d'attaque pour seulement $8100.
Lire

25%

C'est la proportion du secteur de la santé dans les fuites d'information identifiées depuis 10 ans.

Lire

Chez CGI Business Consulting

Thierry Jardin, Vice-Président sécurité et gestion des risques de CGI Business Consulting, a été reçu par Xerfi Canal TV

Il revient en détail sur les menaces qui pèsent aujourd'hui sur les entreprises et les moyens de se défendre.
Regardez l'interview

Une question sur la méthode EBIOS ?

Les membres de CGI Business Consulting, adhérent au Club EBIOS, apportent des réponses via la FAQ du Club EBIOS. Transmettez vos questions et suggestions à jean.olive@cgi.com pour enrichir les débats !
Lire la FAQ

Recrutement

CGI Business Consulting fait face à une très forte croissance de son activité sécurité. Nous recrutons des consultants sécurité de tout niveau. Envoyez votre candidature.

Pour de l'information en temps réel, @CGIsecurite est sur Twitter

CGI Business Consulting fait partie du groupe CGI inc, 5e plus importante entreprise indépendante de services en technologie de l'information et en gestion des processus d'affaire au monde.

CGI Business Consulting dispose notamment d'une équipe d'experts spécialisée dans le conseil aux entreprises et aux organismes publics pour les assister à lutter efficacement et globalement contre toutes les formes de cybercriminalité.

Directeur de la rédaction Rémi Kouby
Comité de rédaction Geoffroy Andrieu, Rémi Kouby, Jean Olive, Miriam Paiola
Contact remi.kouby@cgi.com