CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 20 – Octobre / Novembre 2016

CyberÉdito – La *blockchain* changera le monde, avec ou sans vous

Internet a changé le monde. La *blockchain*, en devenant un registre général partagé, révolutionne le concept de confiance. Initialement utilisée uniquement en support des échanges de crypto-monnaies, cette technologie est aujourd'hui le cœur de plateformes, comme Ethereum, qui étendent les usages bien au-delà du pur aspect monétaire.

En particulier, la *blockchain* et le caractère indélébile de ses échanges, au moins à moyen terme, permettent d'instaurer la confiance pour tout échange entre deux pairs, sans intermédiaire. Les autorités de confiance sont aujourd'hui autodéclarées : vous êtes obligés de faire confiance à une multitude d'autorités, des institutions ou des entreprises, dans lesquels vous n'avez pas forcément une confiance absolue (Paypal, Google, Facebook, etc.). Demain, ces autorités de confiance seront remplacées par des communautés, soutenues par des moyens technologiques partagés, prouvés et sécurisés.

Comment devez-vous, en tant que RSSI ou DSI, réagir à cette nouvelle révolution ? Le plus important est la maitrise de la technologie et la mise en place de *proof of concepts*. S'informer. Recruter. Se faire accompagner. Expérimenter. Notre savoir-faire et notre expérience nous prouvent qu'il est possible de trouver des usages dans lesquels des bénéfices concrets sont atteignables. Les utilisations innovantes de la *blockchain* ne demandent qu'à être découvertes et développées. Elles doivent également être encadrées. Rien de tel qu'une nouvelle technologie et une nouvelle usine logicielle dans l'entreprise pour voir les failles se multiplier, surtout dans un monde où toutes les transactions sont publiques. Les démarches d'intégration de la sécurité doivent être adaptées à cette nouvelle technologie qui amènera de nouveaux processus de développement et d'exploitation.

Mais avant tout, brisons deux mythes :

- **« Il faut d'excellentes connaissances cryptographiques pour *utiliser* la technologie. »** C'est faux. L'utilisation de la *blockchain* requiert l'apprentissage de langages et de bibliothèques spécifiques et de son fonctionnement mais la cryptographie intervient principalement dans le fait d'assurer la confiance entre les échanges et cela peut être considéré comme un prédicat.
- **« La *blockchain*, ce n'est pas sécurisé. De nombreuses attaques ont réussi ! »** C'est également faux. La plupart des attaques visent des intermédiaires qui interagissent avec une *blockchain*, et notamment des places de marchés (MT. Gox, Bitfinex, etc.). La technologie elle-même n'est pas vulnérable à ce jour.

Vous doutez encore ? C'est normal. En 1994, le rapport Thery écrivait : « Internet et son mode de fonctionnement coopératif n'est pas conçu pour offrir des services commerciaux. Sa large ouverture à tous types d'utilisateurs et de services fait apparaitre ses limites, notamment son inaptitude à offrir des services de qualité en temps réel de voix ou d'images ». La même année, Amazon était créé aux États-Unis. Au début des années 2000, le streaming et le protocole Bit Torrent ont fait leur apparition. Les usages d'une technologie se développent souvent bien plus que prévu initialement.

Rémi Kouby – Consultant sécurité et gestion des risques

Parole d'un CyberExpert

DevOps : comment ne pas rater le train déjà en marche

Adopter une culture DevOps consiste à abstraire l'infrastructure par le code, orchestrer, versionner les développements, intégrer les tests fonctionnels et unitaires, industrialiser les *builds* et déployer les livraisons à un rythme soutenu. L'automatisation de ces étapes au sein d'un *pipeline* DevOps crée de nouveaux risques qu'il faut identifier et apprécier.

Comment éviter l'erreur de script se propageant à tous les serveurs orchestrés ou le déploiement automatique de code vulnérable en production ? Comment cloisonner les environnements de production ? Comment tester en recette sans données cohérentes ? Comment protéger le pipeline lui-même ?

Une stratégie efficace : anticiper les vulnérabilités dans les scripts d'administration et d'exploitation en sensibilisant les opérationnels/développeurs, comme des développeurs classiques. Les équipes projet doivent également être formées à exprimer leurs besoins de sécurité. Pour répondre aux enjeux de rapidité, les analyses de risques doivent être adaptées, notamment en capitalisant sur l'étude des fonctionnalités, des technologies, des risques et des exigences.

L'autre volet consiste à répondre aux enjeux d'industrialisation de l'ISP :

- cataloguer les solutions de sécurité existantes et les proposer efficacement, idéalement via des APIs ;
- créer un catalogue de tests de sécurité en s'appuyant sur le déroulement des tests fonctionnels et unitaires ;
- définir les critères et seuils d'acceptation lors du recours à des outils d'analyse automatique ;
- fournir l'anonymisation en *data as a service* ;
- se fondre dans les méthodes Agiles en intégrant par exemple un coach sécurité dans une équipe pratiquant le *pair programming*.

Notre conviction est qu'il faut replacer l'humain au centre de l'attention en apportant la compétence SSI directement au sein des équipes, tout en industrialisant les activités sécurité via un catalogue de services sécurité projets adapté.

Mouloud Aït-Kaci — Consultant sécurité et gestion des risques

CyberMenaces

Encore une attaque bitcoin ?

Non. Le réseau bitcoin a démontré depuis longtemps sa résilience. Ici, c'est encore une fois l'attaque d'un des plus gros mandataires qui détenait, pour le compte de tiers, leurs clés privées permettant de leur associer des bitcoins. 120000 bitcoins ont été dérobés, l'équivalent de 59 millions d'euros.
Lire

Des professionnels à l'attaque

Ces deux exemples de l'année vont vous convaincre : la banque centrale du Bangladesh a été victime d'un détournement de fonds qui aurait pu atteindre le milliard de dollars, sur fond de complicité interne et exploitation d'une vulnérabilité d'un logiciel de virement interbancaire. Deuxième attaque : des retraits coordonnés dans plusieurs centaines de banques japonaises à l'aide de fausses cartes bleues créées suite à une fuite de données d'une banque sud-africaine, quelques mois auparavant.
Lire et Lire

Retour d'expérience : l'auteur de l'attaque de Hacking Team vous dit tout

Et ce n'est pas rien : s'attaquer à une entreprise vendant de la sécurité et donc supposée prudente. L'attaque reste toutefois classique : trouver une ressource exposée sur internet, trouver un 0day sur cet équipement, rentrer sur le réseau, installer un *backdoor* et progresser.
Lire

L'iPhone protégé des malwares : pas si sûr !

Installer un malware exploitant plusieurs 0day iOS pour espionner un iPhone via un simple lien web ? C'est le tour de force qu'un groupe de pirates israélien a réalisé. Détectée récemment, cette faille concerne plus de 80% des iPhones en circulation. Elle permet d'intercepter l'intégralité des communications de l'iPhone, sms, appels, GPS, e-mails… Une seule solution : la mise à jour.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 20 – Octobre / Novembre 2016

Réponses aux CyberMenaces

Votre mot de passe se trouve-t-il dans le *deep web* ?

Vous entendez régulièrement des fuites d'information de nombreux sites (récemment Yahoo, LinkedIn, Ashley Madison, Dropbox, Badoo, etc.). Mais votre adresse e-mail fait-elle partie de la base qui a fuité ? Votre mot de passe est-il connu et à vendre sur le *deep web* ? Le site https://haveibeenpwned.com/ vous permet de le savoir.
Lire

Rapport annuel de l'ANSSI : une année charnière

L'ANSSI revient en détail sur l'ensemble de ses actions dans son tout premier rapport annuel : lancement de la stratégie nationale pour la sécurité du numérique, intervention opérationnelle auprès de TV5Monde, définition du dispositif sur la cybersécurité des opérateurs d'importance vitale, déploiement en région des référents ANSSI, etc.
Lire

Publication des spécifications techniques de l'eIDAS

L'ANSSI et son homologue allemand, le BSI, ont publié les spécifications techniques préliminaires d'un jeton eIDAS compatible avec les objectifs de la proposition de règlement européen.
Lire

CyberBrèves

Le ransomware 2.0 ?

C'est le mal de l'année et cela va encore durer. D'ores et déjà, les fabricants de ransomware redoublent d'inventivité pour assurer la pérennité de leur business juteux. La nouveauté réside dans les sauvegardes et pour cela deux façons de faire : développer la capacité d'attaquer directement les sauvegardes en les chiffrant ou attendre d'être sauvegardé avant de se déclencher. Dans ce dernier cas, la restauration entrainera une nouvelle infection.
Lire

La presse française perd ses abonnés pendant plusieurs semaines

GLI, le prestataire principal de gestion des abonnements des éditeurs de presse en France, a subi en juin dernier une défaillance majeure de son système d'information. *Le Figaro, L'Express* et d'autres journaux, ne possédant pas de sauvegarde, ont dû attendre plusieurs jours avant l'intervention des équipes IBM pour pouvoir à nouveau accéder à leur base d'abonnés.
Lien

Ransomware sur thermostat connecté : la température augmente tant que la rançon n'est pas payée

L'internet des objets n'est désormais plus à l'abri des *ransomware*. Lors de la conférence DEFCON, deux chercheurs en cybersécurité ont présenté la prise de contrôle d'un thermostat. Cette vulnérabilité exploitée pose à nouveau la question de l'avenir de l'IoT et de sa sécurisation.
Lire

Vos employés sont plus enclins à connecter des clés USB inconnues que ce que vous imaginez

Un chercheur américain a disséminé 300 clés USB sur un campus. Les résultats sont impressionnants : 98% des clés ont été récupérées. Près d'une sur deux a été branchée et les documents, qui pointaient vers un serveur externe, ont été exécutés.
Lire

Enfin des PC portables avec filtre de confidentialité intégré !

Si vous utilisez des filtres de confidentialité pour vos employés, HP les propose en option, directement intégré à l'écran pour certains de ses modèles.
Lire

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

CyberRèglementation

OIV : les décrets d'application sont publiés

Après une première vague en juillet (eau, santé et alimentation), de nouveaux arrêtés sont publiés pour les secteurs de l'énergie et du transport. Ce sont les premiers secteurs concernés par les décrets d'application sortis en juin afin de se mettre en conformité avec l'article 22 de la Loi de Programmation Militaire (LPM).
Lire

CNIL : 100 000 euros d'amende pour Google

Google refuse le déréférencement des liens du moteur de recherche pour les domaines non européens. La présidente de la CNIL avait mis en demeure Google en mai 2015, qui avait alors proposé un filtrage selon le pays de l'utilisateur. Cette solution n'a pas convaincu la formation restreinte de la CNIL.
Lire

Vous déployez des solutions d'IDS, IPS ou DLP ? Pensez à demander l'autorisation de la CNIL

Le but des IDS et IPS est d'empêcher les intrusions sur vos systèmes d'information et de tracer toute tentative de pénétration. Il s'agit cependant ni plus ni moins de collecter des données à caractère personnel concernant des infractions pénales… Exactement le type de traitement de DCP qui doit être couvert par une demande d'autorisation à la CNIL.
Lire

28000

C'est l'estimation du nombre de DPO nécessaires suite au règlement européen sur la protection des données personnelles

Lire

Chez CGI Business Consulting

CGI Business Consulting et l'AFNOR vous invitent à un atelier en région bordelaise

Comment sécuriser votre système d'information dans un contexte de transformation digitale ? Hervé Ysnel, associé chez CGI Business Consulting, apportera son témoignage et retour d'expérience sur l'implémentation des démarches ISO 27001 et ISO 20000-1. L'atelier se déroule en Gironde, au Haillan, le mardi 11 octobre. La participation est gratuite, mais l'inscription est obligatoire.
Inscrivez-vous !

CGI Business Consulting est qualifié pour les besoins de la Sécurité nationale

CGI Business Consulting est qualifié depuis le 30 juin 2016 par l'ANSSI pour contrôler le niveau de sécurité et le respect des règles de sécurité applicables aux SIV des opérateurs d'importance vitale. Cette qualification est valable jusqu'à juillet 2017.

En quoi cette qualification est-elle différente de la qualification PASSI ?
Pour être auditeur OIV, il est nécessaire de respecter les règles applicables aux PASSI mais également d'être en capacité de travailler pour la Défense nationale. Après étude du dossier par l'ANSSI et en attendant le schéma de qualification prévu spécifiquement pour cette qualification, l'ANSSI délivre temporairement cette qualification aux sociétés répondant à certains critères de qualité et de confiance.

CGI Business Consulting est présent aux Assises de la sécurité à partir du 5 octobre

Hervé Ysnel et Emmanuel Petit de CGI Business Consulting présenteront notre vision de la prise en compte de la sécurité dans les projets à l'heure des méthodes agiles et des pratiques DevOps. Cette présentation sera illustrée d'un retour d'expérience en compagnie de Brice Hauser-Kauffmann, responsable projet SSI-CA de Natixis.

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 20 – Octobre / Novembre 2016

CyberLab++

Pour son 20e numéro, la lettre cybersécurité et cybercriminalité évolue. Elle s'accompagne désormais de « Cyberlab++ », une section dédiée, alimentée par notre équipe d'experts du laboratoire de sécurité. Cette page met en avant des sujets d'actualité et de veille dans les domaines de l'audit technique, la détection et la réponse à incident. Elle est destinée principalement aux RSSI opérationnels, responsables de SOC et ingénieurs sécurité. Utilisez-la pour structurer la veille technique de vos équipes !

CyberAttaques

Identifiants Windows : 13 secondes pour tout perdre

Il ne faut que 13 secondes à Rob « Mubbix » Fuller, célèbre ingénieur en sécurité, pour récupérer votre login et le hash de votre mot de passe Windows (ou Mac OS X). Il utilise pour cela un micro PC de la taille d'une clé USB qui simule une nouvelle carte réseau se paramètrant automatiquement en *gateway* prioritaire pour tout le trafic réseau à l'aide d'une requête DHCP. L'outil Responder, installé sur le micro PC, intercepte ensuite les données d'authentification. Cela fonctionne même avec l'écran verrouillé. Il ne reste plus qu'à cracker le hash du mot de passe…
Lire

Comment créer un micro PC USB qui ressemble vraiment à une clé ?

En résonance directe à ce qui est décrit ci-dessus, on découvre au détour de cet article, qui recense les attaques classiques à l'aide d'une « clé USB » récupérée et branchée par une victime, des détails sur la création d'un micro PC USB qui ressemble vraiment à une clé et pas à un circuit imprimé.
Lire

Apprenez le *reverse engineering* avancé sur Android

Bernhard Muellern, expert sécurité, propose un guide pour apprendre le *reverse engineering* avancé sur Android à travers l'étude d'applications de génération de *token* comme RSA SecurID ou Vasco DIGIPASS.
Lire

Umbreon : un *rootkit* particulièrement discret

Les Pokémons n'ont pas fini de faire parler d'eux ! Umbreon (Noctali) est le pokémon qui se cache dans le noir, tout comme ce *rootkit* éponyme qui cible les systèmes Linux sur des processeurs x86 ou ARM. Particulièrement sophistiqué, il est très difficile à détecter, car il n'installe aucun composant et force la bibliothèque C à utiliser ses propres fonctions.
Lire

Tests d'intrusion sur un serveur Citrix

Cet article détaille les étapes clés d'un test d'intrusion d'un serveur Citrix.
Lire

CyberRecherche

Un *backdoor* Mac OS X passé au microscope

Nous le savons depuis un moment maintenant, Mac OS X n'est plus intouchable. Le système d'exploitation d'Apple est maintenant une cible de choix pour les malwares. Stefan Ortloff propose l'analyse du fonctionnement du *backdoor* multiplateforme `Backdoor.OSX.Mokes.a` sous Mac OS X.
Lire
Et pour une vision plus générale des malwares existants sur l'OS de « la marque à la pomme », retrouvez une liste bien fournie ici.

L'internet est-il en danger ?

Les systèmes vitaux de l'infrastructure du réseau Internet seraient depuis plusieurs mois victimes d'attaques de plus en plus nombreuses et sophistiquées. C'est en tout cas ce que révèlent les recherches de Bruce Schneier, qu'il expose dans un article publié sur son blog. D'après l'ampleur des attaques, un État semble être à l'origine du mouvement. Le réseau tiendra-t-il le coup ?
Lire

CyberVulnérabilités

Phishing or not phishing ?

Lenny Zeltser nous propose une revue des bonnes pratiques pour envoyer des e-mails à ses clients et ses collaborateurs qui ne risqueront pas d'être considérés comme du *phishing*. De bons conseils à suivre pour une campagne de *phishing* simulée en interne.
Lire

HTTP2 : Quatre vulnérabilités en détail

Dernière version en date du protocole (mai 2015, première version de la RFC), HTTP2 est implémenté au sein des serveurs web les plus répandus (Apache2, Nginx, etc.). Cependant, les recherches sur la sécurité du protocole ne font que débuter. Imperva délivre une analyse détaillée de quatre vulnérabilités et leurs implémentations.
Lire

18000

C'est le nombre de serveurs Redis accessibles sans contrôle d'accès sur Internet et potentiellement vulnérables

Lire

CyberOutils

Bloodhound vous dit ce que vous ne savez pas sur les droits de vos utilisateurs

Présenté cet été à la Black Hat et à la DEFCON, *BloodHound* est un outil d'escalade de privilèges au sein d'un Active Directory. Basé sur la théorie des graphes, l'outil permet d'identifier des utilisateurs involontairement privilégiés.
Lire

ANSSI : un outil d'extraction d'image du cache RDP

Sur son dépôt Github, l'ANSSI propose un outil développé en python permettant d'extraire différentes informations du cache des connexions Remote Desktop Protocol (RDP). La réussite de l'exploitation des fichiers pourrait « permettre de récupérer des fragments de ce que voyait l'utilisateur lors de la session RDP ».
Lire
Le CERT-FR a également publié un bulletin d'actualité qui décrit comment le Bitmap Cache de RDP peut être exploité.
Lire

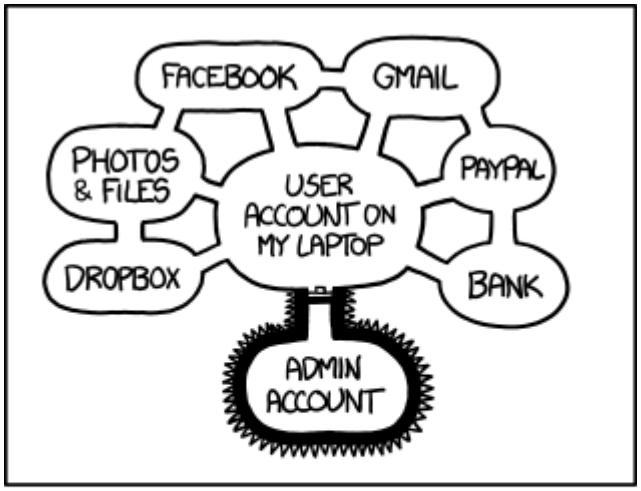
Les règles Outlook : un attaquant peut en abuser et prendre le contrôle d'un poste de travail

Sensepost montre comment, à l'aide du login et mot de passe d'un compte Exchange, exploiter les règles Outlook et les bibliothèques MAPI pour prendre le contrôle du PC d'un utilisateur. Le tout, à distance. Pour éviter cela, il est nécessaire de bien encadrer et surveiller l'utilisation des services MAPI, notamment à distance.
Lire

Effacer efficacement votre historique bash

Vous connaissez `history -c` pour effacer votre historique bash. Mais cela ne fonctionne pas tout le temps. Si une autre session est ouverte, c'est son fichier `.bash_history` qui sera conservé et l'effacement n'aura pas fonctionné. Préférez un « bon vieux » `cat /dev/null > ~/.bash_history`.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 20 – Octobre / Novembre 2016



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS, BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

CGI | Business Consulting

Fondée en 1976, CGI est l'une des plus importantes entreprises de services en technologie de l'information et en gestion des processus d'affaires au monde et offre des services-conseils en management ainsi que des services d'intégration de systèmes et de gestion déléguée de grande qualité.

CGI Business Consulting, qui fait partie du groupe CGI, 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.

CGI Business Consulting et son laboratoire de sécurité sont qualifiés « Prestataire d'audit de la sécurité des systèmes d'information » (PASSI) par l'ANSSI.

Cette qualification atteste du haut niveau de qualité et d'expertise de nos prestations, ainsi que du traitement hautement sécurisé des informations de nos clients collectées lors des audits.

À ce titre, CGI Business Consulting est un partenaire de choix pour réaliser les contrôles de sécurité dans tous les organismes publics ainsi que les opérateurs d'importance vitale, rendus obligatoires par la loi de programmation militaire et dont les arrêtés sectoriels ont récemment été publiés.

CGI Business Consulting
Immeuble CB16
17 place des Reflets, 92400 Courbevoie

Directeur de la rédaction Rémi Kouby
Comité de rédaction Mouloud Aït-Kaci, Geoffroy Andrieu, Florent Cottey, Paul Mars, Rémi Kouby, Jean Olive, Emmanuel Petit, Thomas Tabary
Contact remi.kouby@cgi.com