CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 16 – Juin / Juillet 2015

CyberÉdito

Quelles sont les méthodes de cyberattaques à la mode ? De nombreux témoignages publiés dans la presse placent le *phishing* comme la méthode préférée des attaquants pour pénétrer un SI. Effectivement, un simple lien dans un e-mail permet d'introduire au sein du réseau interne un code malveillant contrôlé depuis l'extérieur par un pirate. Cette attaque rend le pare-feu périmétrique inefficace, puisque, pour lui, le flux de contrôle provient de l'intérieur et usurpe un flux légitime autorisé.

Face à cette évolution de la menace, dont l'utilisateur est le complice involontaire, est-il encore utile de réaliser des analyses pour lutter contre des attaques frontales depuis Internet ? Les tests d'intrusion simulant des attaques directes ont-ils encore un intérêt ?
Si une maturité suffisante des dispositifs et processus est aujourd'hui souvent atteinte pour protéger le périmètre des entreprises et éviter la prise de contrôle du réseau interne, le *phishing* n'est pas le seul moyen de contourner les pare-feux. Un simple oubli laissant un port réseau non sécurisé sur un serveur suffit à permettre une intrusion sur le réseau interne. Dernièrement, une prestation de test d'intrusion nous a conduit à prendre le contrôle total d'un SI interne en exploitant une passerelle SIP (voix sur IP) mal sécurisée et accessible sur Internet.
En outre, une intrusion au sein du réseau interne n'est pas toujours le moyen le plus simple pour causer des dommages critiques à sa cible. L'ouverture des SI aux partenaires ou clients entraine en effet un développement de la publication sur Internet de *web services* destinés à permettre un accès contrôlé à des données métier. Or, une faille dans les couches applicatives, par exemple de type injection SQL, peut permettre de contourner les contrôles et d'accéder à de grandes quantités d'informations sensibles.

Les tests d'intrusion visant les infrastructures Internet et les sites ou applications web restent donc plus que jamais nécessaires.

Vincent Maret — Responsable de l'offre cybersécurité CGI Business Consulting

Parole d'un CyberExpert

Comment lutter contre des attaques de plus en plus sophistiquées sans entraver le métier ?

Nous avons constaté les échecs répétés d'organisations qui se lancent tête baissée dans l'achat et le déploiement de solutions de SIEM (*Security Information and Events Management*). Revenons à la dure réalité : l'outillage ne fait pas tout !

Le RSSI pragmatique s'attachera d'abord à définir la verbosité des traces, les informations de supervision utiles à leur enrichissement (à l'aide des annuaires, télé-inventaires, veille, etc.) ainsi qu'à leur centralisation. Puis, il organisera un *Security Operations Center* (SOC) dont il assurera l'intégration transverse dans l'organisation afin de disposer d'une capacité centrale d'analyse et de qualification des évènements de sécurité. Enfin, il organisera la réaction avec une intégration au processus de gestion d'incidents.
L'accent doit être mis sur la définition des scénarios à détecter, sur les compétences du SOC, éventuellement organisées en plusieurs niveaux d'expertise, et la disponibilité de ses équipes (Top 10 des stratégies SOC).
Vient ensuite l'implémentation du SIEM pour outiller le SOC : vérifier la maturité minimum dont notamment le processus de traitement des incidents, définir pour chaque type d'équipement les scénarios à détecter (Indicateurs d'incidents de sécurité - ETSI), mettre à disposition les flux de traces nécessaires (Stratégies de SIEM et log management – SANS Institute), choisir l'outil, réaliser un *Proof Of Concept* (POC) et industrialiser la solution.

La principale clé de réussite est d'adopter une démarche d'amélioration continue à long terme en rodant (2 à 3 mois) le dispositif sur des périmètres réduits. Il s'agit ensuite d'étendre progressivement ces périmètres et les capacités de détection.

La mise en place d'un SIEM/SOC est un chantier à haut risque d'échec. Le succès de son intégration est conditionné à l'adoption d'une approche itérative, réaliste et opérationnelle.
Il implique une triple compétence de DSI, d'analystes experts en sécurité et d'exploitants ou le recours à des prestataires qualifiés (PDIS).

Mouloud Aït-Kaci — Consultant CGI Business Consulting

CyberMenaces

Coup de tonnerre sur la mutualisation dans le *Cloud*

Une faille 0-day baptisée Venom a récemment été découverte. Cette faille permet d'accéder, à partir d'une machine virtuelle infectée, à toutes celles installées sur un serveur. Mauvaise nouvelle, Venom affecte un module de QEMU, logiciel open source largement utilisé par de nombreuses solutions telles que Xen, KVM ou Virtualbox.
Lire

BIOS : toujours pas corrigé

Deux chercheurs en sécurité informatique ont développé un outil permettant d'exploiter automatiquement les failles présentent sur le BIOS de la plupart des cartes mères du marché, le tout en un temps record de deux minutes. Il faudra néanmoins un accès physique à la machine pour la compromettre.
Lire
L'ANSSI donne des éléments de réponse pour configurer les BIOS et UEFI.
Lire

TV5 Monde : une attaque qui a fait du bruit …

Le 9 avril, une attaque initiée par un groupe de pirates a mis TV5 Monde sous le feu des projecteurs. Tout le monde en a entendu parler ! Passés le stress et l'excitation du moment, revenons sur cette attaque avec un peu de recul.
Lire

… mais pas si complexe qu'il n'y parait

Cette attaque, bien que finement orchestrée, a pour origine une simple campagne de *phishing* réalisée deux mois auparavant. Suite à quoi, plusieurs machines furent infectées, dont le système de transmission des programmes de la chaine.
Lire

Plus de 2/3 des attaques utilisent de « vieilles » méthodes

Verizon a publié son étude annuelle de 2015 sur les fuites de données. Bien que les cyberattaques deviennent de plus en plus sophistiquées, 70% d'entre elles utilisent d'anciennes techniques ou des failles connues qui ne sont pas corrigées.
Lire

Réponses aux CyberMenaces

Vous saurez tout sur le DDOS

DDOS par réflexion ? DDOS par amplification DNS ? par amplification NTP ? Ce guide de l'ANSSI ne déroge pas à la qualité habituelle des publications de l'agence. Il détaille plusieurs types d'attaques DDOS et apporte les clés pour s'en protéger.
Lire

Le DAF : nouvel acteur de la protection du SI

Le directeur administratif et financier est amené à être partie prenante dans la protection du système d'information de son entreprise. De par son rôle stratégique, il peut être un bon moyen de vendre la sécurité auprès du Président.
Lire

Évaluer votre prestataire *Cloud* en quelques clics, par l'ENISA

L'ENISA a publié un guide de sécurité ainsi qu'un outil en ligne pour vous aider dans le choix des prestataires de services *Cloud*. Ces outils mettent en évidence les opportunités de sécurité et les risques à prendre en compte pour évaluer les services *Cloud*. L'outil vous permet même de générer en quelques clics votre questionnaire de sécurité à adresser à vos prestataires.
Lire

IETF : bonnes pratiques SSL/TLS

Suite aux récentes découvertes de failles sur le protocole SSL/TLS telles que Heartbleed et POODLE, l'Internet Engineering Task Force (IETF) a publié des « recommandations pour sécuriser l'utilisation des protocoles Transport Layer Security (TLS) et Datagram Transport Layer Security (DTLS) »
Lire

CyberRèglementation

Les données personnelles des Russes resteront en Russie

À compter du 1er septembre 2016, les sociétés étrangères devront créer leurs propres centres de traitement de données sur le territoire russe ou louer des serveurs à des entreprises russes. D'autres pays vont-ils suivre le pas ?
Lire

La collecte d'adresses IP : un traitement de données à caractère personnel ?

La Cour d'appel de Rennes a récemment rendu un arrêt qui considère la conservation d'adresses IP en vue de la découverte ultérieure d'auteurs de pénétrations non autorisées, ne constitue pas un traitement de données à caractère personnel.
Lire

Attention à vos contrats avec les hébergeurs

Récemment, un hébergeur a gagné face à son client, société de santé à domicile. Ce dernier lui reprochait de ne pas disposer de l'agrément d'hébergeur de données de santé. Et pour cause, rien dans le contrat ne mentionnait le type de données qui allait être hébergé !
Lire

CyberBrèves

Les fichiers robots.txt

Un chercheur en sécurité a démontré que les fichiers robots.txt, destinés aux robots d'indexation des moteurs de recherche, peuvent être utilisés pour récolter des informations précieuses comme des arborescences supposées inaccessibles et des documents sensibles.
Lire

Des *malware* Linux qui envoient du spam. Comment les faire taire ?

Les *malware* Mumblehard sont restés sous les radars pendant cinq ans. Découvrez leur fonctionnement et comment s'en protéger.
Lire

Publication du décret relatif à l'habilitation et l'assermentation des agents de l'ANSSI

Le décret N° 2015-349 du 27 mars 2015 offre désormais un cadre légal aux agents de l'ANSSI pour interroger les opérateurs de communications électroniques afin d'obtenir les coordonnées des victimes menacées ou attaquées puis de les alerter sur la vulnérabilité ou la compromission de leur système.
Lire

Même des experts en sécurité se font pirater !

Thales, spécialiste français de la sécurité informatique, aurait subi une attaque : les pirates se seraient infiltrés dans le système d'information américain du groupe et auraient propagé l'attaque dans les autres SI.
Lire

Ransomware as a service

Les services n'en finissent pas de fleurir sur le *deep web*. Le dernier en date : la possibilité pour tout un chacun de commander son *ransomware* personnalisé.
Lire

206

C'est le nombre de jours pendant lequel un attaquant arrive à rester infiltré dans un système d'information.
Lire

Chez CGI Business Consulting

Qualification PASSI : CGI sur le site de l'ENISA

Un processus français reconnu par la communauté européenne ! L'ENISA référence le lien vers la procédure de qualification PASSI de l'ANSSI. CGI Business Consulting fait bien entendu partie des sociétés en cours de qualification. Le processus devrait aboutir dans les prochaines semaines.
Lire

Recrutement

CGI Business Consulting fait face à une forte croissance de son activité sécurité. 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 Jean Olive
Comité de rédaction Mouloud Aït-Kaci, Geoffroy Andrieu, Rémi Kouby, Jean Olive, Miriam Paiola
Contact jean.olive@cgi.com