CGI BUSINESS CONSULTING

vQice of CGI

LA LETTRE
CYBERSÉCURITÉ
Octobre 2019
n°24

La fin des mots de passe, **ce n'est pas pour demain !**

édito

Les mots de passe, premier vecteur de cyber-attaques

À l'heure où l'on fournit de plus en plus d'informations aux sites web (nom, prénom, adresse, e-mail, données bancaires, etc.), et parce que les utilisateurs ne se préoccupent que faiblement de la complexité de leurs mots de passe, les pirates et les fraudeurs trouvent de nouvelles manières d'accéder à nos données de connexion. Vous avez certainement entendu parler du *credential stuffing*. Les pirates se procurent des listes d'identifiants volées sur le *darknet* puis les chargent sur un botnet qui envoie des milliers de tentatives de connexion sur les applications web. Les bons identifiants/mots de passe permettent alors au pirate d'effectuer de nombreuses actions frauduleuses : vol de données, usurpation d'identité des clients, etc. Les contrôles de sécurité standards (blocage IP, limitation de débit, tests JavaScript et empreinte de navigateur) ne suffisent plus pour arrêter ces attaques. En effet, les bots utilisés pour le *credential stuffing* et la fraude sur le web comptent parmi les techniques les plus sophistiquées. Lorsqu'on sait qu'un compte piraté aurait 17 fois plus de valeur qu'un numéro de carte de crédit volé, on comprend mieux pourquoi certains souhaitent la disparition de l'authentification par simple mot de passe.

WebAuthn : une alternative aux mots de passe

En partant de ce postulat, les géants high-tech (Google, Mozilla, PayPal, Visa, Mastercard, Samsung et Microsoft) se sont penchés sur le problème et ont formalisé l'API Web Authentication plus connu sous le nom de WebAuthn : un moyen de faciliter l'authentification de l'utilisateur tout en répondant aux problématiques de sécurité.
Sans se perdre dans les détails techniques (que vous pouvez trouver **ici**), WebAuthn, lors de l'enregistrement de l'utilisateur, associe le compte utilisateur à une clé publique. Pour s'authentifier, il suffit alors de résoudre un challenge de l'application : signer un message avec la clé privée.
L'authentificateur peut être tout élément permettant de stocker une clé privée, ou de déchiffrer une clé privée stockée à un autre endroit, de manière chiffrée : clés FIDO, smartphone, etc.
Après plusieurs années de test et de succès auprès des utilisateurs initiés, l'information est rendue publique le 4 mars 2019 : le World Wide Web Consortium (W3C), organisme international qui gère les standards web, et l'Alliance FIDO (Fast Identity Online), une association d'entreprises qui œuvrent à la sécurisation le web, ont annoncé l'adoption de WebAuthn comme un standard web officiel. Cette standardisation met le système Fido2 à disposition de tous les sites web et répond aux exigences d'aujourd'hui : délivrer une sécurité renforcée, tout en facilitant le quotidien de l'utilisateur grâce à l'éviction du mot de passe.

Alors, allons-nous vers la fin des mots de passe ? Non.

La spécification Web Authn devrait être de plus en plus utilisée. Le développement de moyens alternatifs risque certainement, à terme, de marginaliser la pratique du mot de passe.
Mais nous partageons l'analyse de Troy Hunt : malgré toutes les évolutions technologiques et en dépits des défauts qu'ils peuvent comporter, les mots de passe ne disparaitront pas de si tôt, principalement parce que tout le monde comprend facilement comment cela fonctionne. Tout le monde sait utiliser les mots de passe. Les générations à venir ne connaitront peut être pas le concept de mots de passe mais pour l'heure, supprimer les mots de passe sur l'ensemble de nos systèmes d'authentification ne parait pas envisageable. On observe plutôt la mise en place de système appelés «Risk based authentication» qui permettent d'adapter la force de l'authentification demandée en fonction de la sensibilité de ce qui est accédé.
Vous devrez toujours maintenir la sensibilisation et faire évoluer les moyens techniques autour des mots de passe. Pour cela, le document du NIST 800-63B donne des indications à jour sur le sujet : privilégier des mots de passe long, ne pas bloquer la fonction « copie » du mot de passe, interdire le choix de mots de passe sur des dictionnaires et des règles (cf. algorithme zxcvbn) plutôt que sur des règles de composition, parmi plein d'autres.
Vous pouvez également tester si vos mots de passe se sont retrouvés dans la nature en utilisant les outils du site web **have i been powned** ou le plus récent **Firefox Monitor**. Et si tel est le cas, n'oubliez pas de changer vos mots de passe bien sûr !

Estelle de Monchy

Consultante cybersécurité
CGI Business Consulting

LES ÉVÈNEMENTS CYBER À VENIR...

Cybermoi/s
Le mois européen de la cybersécurité

Octobre est le mois européen de la cybersécurité. Des conférences sont organisées dans plusieurs sites et institutions en France et en Europe.

Les Cyberdays en Corse
8 OCT. 2019

La première édition du CyberDay Corsica se tiendra le 8 octobre 2019 au **Palais des Congrès d'Ajaccio** en partenariat avec la CCI d'Ajaccio et de la Corse du Sud, durant le mois européen de la cybersécurité.

Les Assises de la Sécurité et des systèmes d'information
9,10,11 OCT. 2019

Les Assises de la Sécurité et des systèmes d'information du 9 au 11 octobre à **Monaco.**

Le 7è RP cyber
7 NOV. 2019

Le CyberCercle conçoit et organise chaque année depuis 2013, un grand rendez-vous à **Paris** sur la cybersécurité. Il se tiendra le 7 novembre au **ministère de l'Intérieur.**

Conférence AEGE
12 NOV. 2019

Conférence AEGE sur la gestions de crise Cyber 12 novembre , Amphithéâtre.

196 rue de Grenelle, 75007 Paris

REVUE DE PRESSE
LA COURSE AUX FAILLES

LE BUG BOUNTY À UN MILLION DE DOLLARS

Apple a récemment augmenté les montants offerts pour la trouvaille de vulnérabilités sur ses produits iOS, macOS, watchOS et même Apple TV. Mieux encore, le programme de *bug bounty* est ouvert à tous les chercheurs en cybersécurité intéressés. La récompense la plus intéressante monte jusqu'à un million de dollars, une des plus importantes jamais offertes par une grande société dans le domaine. Elle reviendra au chercheur capable de réaliser une prise de contrôle à distance sans intervention de l'utilisateur, dit *« zero click »*, sur le cœur iOS d'un iPhone.
En janvier, Zerodium avait annoncé offrir jusqu'à deux millions pour le même type de faille.

UN OUTIL DÉSORMAIS DISPONIBLE POUR EXPLOITER BLUEKEEP

Renseignée sous la CVE-2019-070, cette faille est considérée aussi virulente qu'EternalBlue, la vulnérabilité responsable de WannaCry et permettant d'exécuter du code arbitraire à distance. Depuis le 5 septembre 2019, un module d'exploitation a été rendu public par l'entreprise rapide, responsable du célèbre framework de sécurité offensive metasploit. La publication de cet outil est un fait majeur car il facilite grandement l'exploitation de la vulnérabilité. Pour information, les derniers scans de masse trouvent près d'un million de périphériques non patchés face à cette menace.
Des correctifs sont disponibles pour supprimer ce risque, assurez-vous de mettre le vôtre à jour !

AT&T, LE PLUS GRAND FOURNISSEUR DE SERVICES TÉLÉPHONIQUES AMERICAIN, INFILTRÉ !

Extradés de Hong Kong vers les États-Unis, les deux pirates présumés sont accusés par la justice américaine d'avoir piraté deux millions de téléphones portables achetés avec l'aide des employés AT&T. Ils sont également soupçonnés d'avoir versé jusqu'à 420 000 dollars à des employés travaillant dans un centre d'appels de Boswell, dans l'État de Washington. Au départ, la mission des malfaiteurs a été de demander aux employés de déverrouiller des téléphones bloqués sur le réseau AT&T et ce sont les clients qui payaient le déblocage. Mais la fraude ne s'est pas arrêtée là. Les pirates auraient demandé aux salariés d'AT&T d'installer des logiciels malveillants dans les ordinateurs de l'entreprise afin d'étudier le fonctionnement des processus internes du leader des télécommunications. Ensuite, ils ont créé un outil qui automatisait les accès aux différents ordinateurs afin de pouvoir déverrouiller eux-mêmes les smartphones. Et pour finir, ils ont rémunéré les employés pour installer du matériel d'espionnage, des routeurs malveillants et des points d'accès Wi-Fi non autorisés dans le bâtiment, permettant ainsi un accès supplémentaire à des ordinateurs qui étaient initialement protégés. Cette attaque de grande ampleur aurait coûté des millions de dollars à l'entreprise américaine. On ne le dira jamais assez mais le collaborateur, malveillant ou non, est un des vecteurs d'attaque les plus vraisemblables dans les entreprises.

ALEXA, QUE FAIS-TU AVEC LES DONNEES DE MES ENFANTS ?

Une enquête du CCFC (Campaign for a Commercial-Free Childhood) a permis de montrer qu'Alexa, l'assistante virtuelle d'Amazon, conservait les données issues des enfants même après une demande de suppression de la part de leurs parents.
L'appareil incriminé est en réalité un dérivé d'Alexa pour enfants, « Echo Dot Kids », et est placé la plupart du temps directement dans les chambres des enfants dans le but de les éduquer et de les divertir. Les données collectées concernent principalement des enregistrements vocaux et les films, livres, et habits qu'ils achètent ou consultent. Au-delà de poser un réel problème en matière de vie privée dans le foyer familial, on peut se demander s'il est judicieux de laisser les GAFA s'initier dans l'éducation de nos enfants.

REVUE DE PRESSE
LA COURSE AUX FAILLES

LA GENDARMERIE INNOVE DANS SA LUTTE CONTRE LA CYBERCRIMINALITÉ

Les cybergendarmes français ont signé une première mondiale en innovant leur manière de traiter un botnet composé de 850 000 machines de particuliers et d'entreprises. Depuis trois ans, le serveur des pirates permettait de prendre le contrôle de machines « zombies » et de les commander à distance pour commettre des attaques d'ampleur ou miner de la cryptomonnaie. Habituellement, la solution choisie pour bloquer un botnet est de neutraliser le serveur de commandement. Ici, les gendarmes français ont dupliqué et modifié le serveur afin qu'il envoie du code aux machines victimes lorsqu'elles essayent de se connecter. Ce code bloque tous les services vulnérables directement sur la machine et supprime toutes les versions du virus Retadup, utilisé pour constituer ce botnet.

> Lire l'article

« L'ARNAQUE AU PRESIDENT », ENCORE ET TOUJOURS UN RISQUE MAJEUR POUR LES ENTREPRISES

Lors de la sortie du baromètre 2019 du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), l'arnaque au président, aussi appelée « fraude au président », été catégorisée comme le 2e type d'attaque la plus constatée. Pour rappel, elle consiste en un attaquant qui entre en contact avec l'un des employés de l'entreprise, usurpe l'identité d'un directeur et ordonne d'effectuer un virement bancaire, prétextant souvent un rachat d'entreprise. Ce type d'approche nécessite une préparation de la part des criminels afin de cartographier l'entreprise, identifier les collaborateurs ayant accès aux comptes et mettre en place des techniques d'ingénierie sociale. Pour exemple, en mars 2018, le groupe de cinéma Pathé en a été la victime. Les fraudeurs vantaient une prétendue acquisition à Dubaï. Le montant total du préjudice s'élevait à plus de 19 millions d'euros.
En cette rentrée 2019, ce type d'attaque semble avoir évolué de façon significative. En effet, les faussaires ont cette fois-ci simulé la voix du P.-D.G. grâce à une intelligence artificielle, aussi appelé « deep fake », l'imitant quasi-parfaitement. 220 000 euros ont ainsi été extorqués à l'entreprise. Cette mutation des moyens d'attaque n'est en réalité pas nouvelle et existe depuis plusieurs années. Menace toujours très présente au sein de nos entreprises, elle doit nous encourager à rester d'autant plus vigilant et continuer à sensibiliser nos collaborateurs.

DES FAILLES DANS LES VPN, UNE PORTE OUVERTE VERS VOTRE RÉSEAU

Certaines solutions de VPN, outils fréquemment utilisés dans les entreprises pour sécuriser les connexions à distance et véritables portes d'entrées dans les entreprises, ont présenté des vulnérabilités facilement exploitables par un attaquant. Plusieurs VPN largement répandus sont concernés, dont ceux de Palo Alto, Fortinet et Pulse, qui ont rapidement mis à disposition des correctifs de sécurité. Il a été prouvé que toutes les versions GlobalProtect de Palo Alto antérieures à juillet 2018 étaient vulnérables. Uber et Twitter ont été les deux premières entreprises ayant communiqué sur une attaque de leurs serveurs par ce biais. Les VPN, souvent présentés comme une mesure ultime pour sécuriser l'entrée sur votre réseau, pourraient être un peu moins sûrs que l'on ne pense. Des audits techniques sur ces équipements se justifient désormais d'autant plus.

LE CHIFFRE

120

C'est le nombre d'établissements de santé affectés par la **cyberattaque** qui a touché le groupe privé Ramsay Générale de Santé au mois d'août en France.

REVUE DE PRESSE
LE RGPD DANS TOUS SES ÉTATS

PAYS-BAS : LES APPLICATIONS MICROSOFT OFFICE BANNIES PAR LE GOUVERNEMENT

L'utilisation des applications Microsoft Office, en ligne et mobile, ne permettrait pas de respecter le RGPD ? C'est ce que semble déclarer le ministère de la justice néerlandais qui met en garde les institutions du pays. Les applications mobiles Office ne devraient plus être utilisées par les employés, et plus particulièrement par les services douaniers, judiciaires ou encore policiers. Voici la raison de cette mise à l'écart : « Dans au moins trois des applications mobiles sur iOS, les données relatives à l'utilisation des applications sont envoyées à une société de marketing américaine spécialisée dans le profilage prédictif » peut-on lire dans le rapport du ministère.

ROYAUME-UNI - RGPD : UNE PORTE OUVERTE À L'INGÉNIERIE SOCIALE ?

Le RGPD confère à toute personne un droit d'accès à ses données et l'entreprise qui les détient ne peut pas lui refuser, sous peine de recevoir une amende. Il a été démontré lors de la conférence Black Hat 2019 que le processus de vérification des entreprises était insuffisant. Pour arriver à ce constat, l'expert qui a réalisé cette enquête s'est fait passer pour sa fiancée, complice et co-auteure de l'étude. Il a envoyé un courrier à 150 entreprises dans lequel il demande en retour, une copie de toutes les données qu'elles détiennent sur elle. Sur les 108 qui ont répondu, environ un quart a directement envoyé les données sans établir de vérification.

Parmi les entreprises ayant demandé une vérification, 16 % ont obtempéré après avoir reçu une faible preuve d'identité, facile à voler ou falsifier : un identifiant technique, une déclaration sur l'honneur, une réponse à une question de sécurité, une facture d'électricité, etc. Seules 39 % des entreprises ont demandé une preuve d'identité d'un niveau correct, comme la connexion par un formulaire en ligne ou l'envoi d'un message depuis l'adresse e-mail référencée chez le fournisseur. Certains Certains sont cependant allés trop loin, en réclamant l'envoi d'une copie de passeport ou d'une carte d'identité. Grâce à cette étude d'ingénierie sociale, James Pavur a réussi, en seulement deux mois, à récupérer 60 types de données personnelles concernant sa fiancée. Certains d'entre eux étaient plutôt sensibles comme l'adresse, le numéro de téléphone, le numéro de sécurité sociale ou le numéro de carte bancaire. Une entreprise a même envoyé le login et le mot de passe de son compte d'utilisatrice. Finalement, le résultat de cette enquête n'est pas étonnant. En effet, le RGPD ne dit pas comment les fournisseurs doivent vérifier l'identité d'un utilisateur. Le préambule du règlement stipule seulement que « le responsable du traitement devrait prendre toutes les mesures raisonnables » pour y parvenir, sans plus de précision (considérant n°64). L'expérience a prouvé que les grandes entreprises ont plutôt bien géré les différentes demandes d'accès. Cependant, les PME et les associations représentent une cible facile pour ce type d'attaque. En tant qu'utilisateur, il est presque impossible d'éviter de tels vols sur ses propres données. La meilleure solution reste de se renseigner auprès des fournisseurs sur d'éventuelles demandes d'accès qui auraient été faites par le passé. Et d'inciter les entreprises à renforcer leurs procédures.

ROYAUME-UNI : LES AMENDES DE L'ICO

L'Information Commissioner's Office (ICO), l'équivalent britannique de la CNIL, a annoncé mi-juillet son intention d'imposer deux sanctions d'un montant record, à l'égard de deux groupes internationaux dans l'hôtellerie et dans le transport. Marriott et British Airways devront respectivement faire face à des amendes de plus 111 millions et de 200 millions d'euros, ce qui correspond à 1,5% de leur chiffre d'affaires. Toutes deux victimes de fuites de leurs données clients, au cours du dernier semestre 2018, ces entreprises ont notifié ces incidents à l'ICO. Les informations personnelles sensibles dérobées (numéros de passeports, informations bancaires, etc.) concerneraient plus de 500 000 victimes. Ainsi, malgré leur coopération avec les enquêteurs de l'ICO et leurs efforts d'amélioration de leur système de sécurité, l'autorité britannique a décidé d'imposer ces lourdes amendes pour manquement à leurs obligations de protection des données, prévues par le RGPD. En raison de la dimension européenne de ces affaires, l'ICO a déclaré qu'elle tiendrait compte des recommandations des autres autorités nationales affectées à la protection des données.

LA BIBLIOTHÈQUE

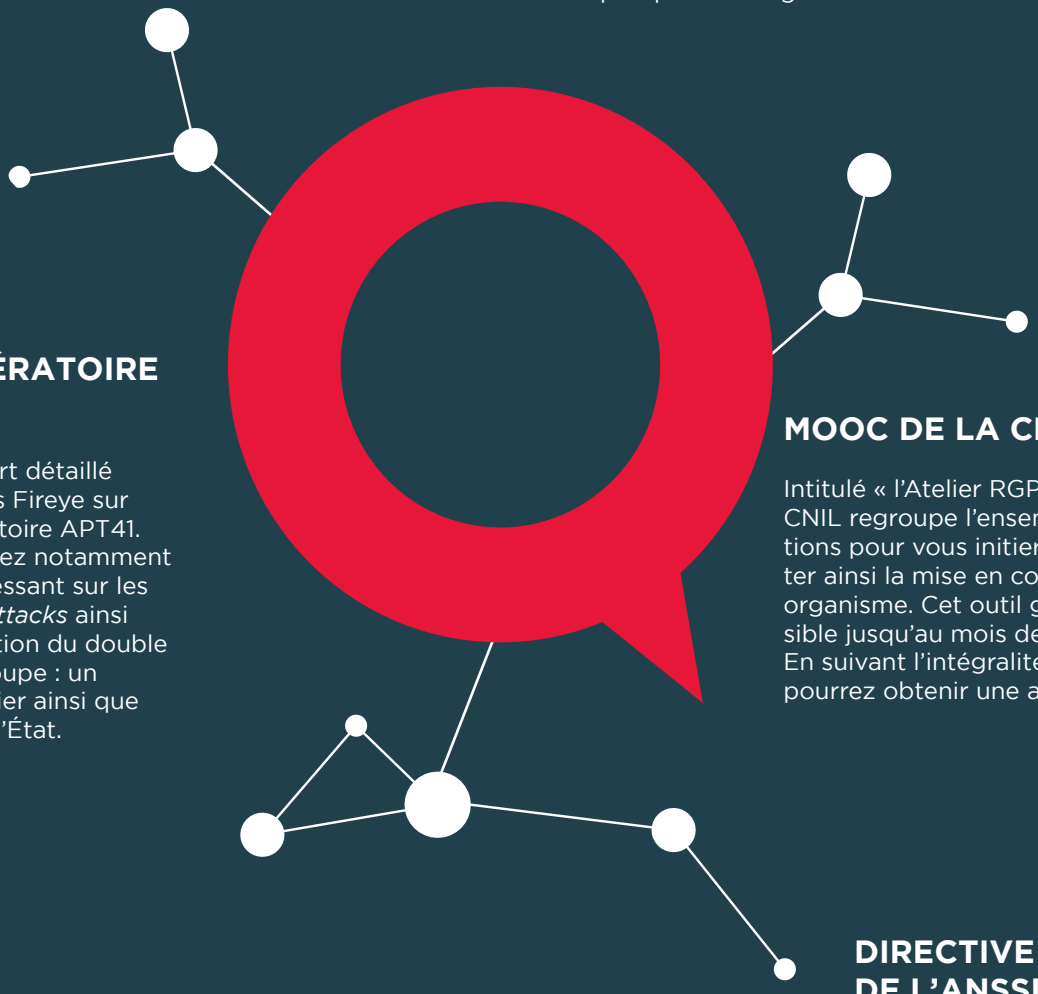
GUIDE SÉCURITÉ D'IOS

Vous cherchez en détail comment est sécurisé un des mécanismes d'iOS (12.1).

> C'est ici !

SUPPORTS DE FORMATION EBIOS RISK MANAGER

L'ANSSI publie un support de formation à la méthode Ebios RiskManager. Vous trouverez un support de formation pour le formateur et des exercices pratiques pour le stagiaire.



MODE OPÉRATOIRE APT41

Voici un rapport détaillé des recherches Fireye sur le mode opératoire APT41. Vous y trouverez notamment un focus intéressant sur les *supply chain attacks* ainsi que la description du double objectif du groupe : un objectif financier ainsi que des objectifs d'État.

> C'est ici !

MOOC DE LA CNIL

Intitulé « l'Atelier RGPD », le MOOC de la CNIL regroupe l'ensemble des informations pour vous initier au RGPD et débuter ainsi la mise en conformité de votre organisme. Cet outil gratuit est accessible jusqu'au mois de septembre 2021. En suivant l'intégralité de ce MOOC, vous pourrez obtenir une attestation.

DIRECTIVE MOBILITÉ DE L'ANSSI

> Découvrir

À PROPOS DE CGI

CGI BUSINESS CONSULTING

Chez **CGI Business Consulting**, cabinet de conseil majeur en France, nous sommes audacieux par nature. Grâce à son intimité sectorielle et à sa capacité à mobiliser des expertises diverses, **CGI Business Consulting** apporte aux entreprises et aux organisations des solutions de conseil audacieuses et sur mesure, pour une réussite stratégique et opérationnelle de leurs projets de transformation.

Nos 1 000 consultants accompagnent nos clients dans la conduite et la mise en oeuvre de leurs projets de transformation, dans une relation franche et de confiance, pour leur permettre de prendre les bonnes décisions.

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

Fondée en 1976, **CGI** figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Elle aide ses clients à atteindre leurs objectifs, notamment à devenir des organisations numériques axées sur le client.

www.cgi.fr

Directeur de publication
Rémi Kouby

Rédactrice en chef
Estelle de Monchy

Rédacteurs
Antonin Deneux, Florent Naliato et Jérôme Freani

vQice of innovation

transformer,
accélérer,
performer