Lettre des "Lundi de la cybersécurité" n° 64

Les mots de passe sont-ils obsolètes ?

Les alternatives pour un avenir sécurisé

Les mots de passe sont-ils obsolètes ?

Les alternatives pour un avenir sécurisé

Lorsque vous demandez à utiliser une ressource informatique, vous devez, pour l'obtenir, vous **identifier** puis vous **authentifier**.

Pour l'identification, le nom que vous avez entré est recherché dans une liste de celles ou ceux autorisés à utiliser cette ressource, c'est typiquement votre **login**. Mais êtes-vous bien celle ou celui qui prétend porter ce nom ? Pour le prouver vous devez vous authentifier, vous le faite typiquement par votre **password**. Le mot de passe, un moyen d'authentification fort ? Comme l'a écrit Benjamin Franklin : « *Trois personnes peuvent garder un secret si deux d'entre elles sont mortes. Ou mieux, les trois …* ».

Alors si les mots de passe sont un moyen d'authentification faible, existe-il d'autres moyens de prouver qu'on est bien celle ou celui qu'on prétend être ?

Dans notre monde ultra connecté, alors que nos datas, nos applications surtout en SaaS, nos serveurs migrent vers des Clouds, donc sont gérés par d'autres entités que la nôtre, une gestion sécurisée et centralisée du contrôle d'accès et des identités est devenue une fonctionnalité indispensable. Si les logins et juste les mots de passe n'apportent pas une réponse suffisante, face aux attaques en usurpation d'identité, et aux fuites de données, comment faire ?

Des solutions existent comme les passkeys et le SASE (Secure Access Service Edge), voir le Lundi de la Cybersécurité de juin 2002 sur https://www.arcsi.fr/doc/Lettre-Lundi-Cyber-No50.pdf avec des fonctionnalités telles que le ZTNA, le CASB le SD-WAN, mais je ne veux pas vous bombarder d'acronymes, un des meilleurs experts en cybersécurité nous parlera de ce qui remplacera les simples mots de passe pour une authentification vraiment forte.

Je donne la plume à Renaud Lifchitz

Les mots de passe ont presque tous les inconvénients possibles : trop nombreux, trop complexes, souvent réutilisés, pénibles pour l'utilisateur à utiliser, à renouveler, ou à choisir en fonction de telle ou telle politique de sécurité, ils permettent très souvent pour les attaquants des réutilisations ("password Seraing") et des vols d'identité multiples, un redoutable calvaire pour les utilisateurs…

La biométrie n'est probablement pas une solution, car en plus d'être vulnérable à certaines attaques par rejeu, elle force l'utilisateur qui souhaite utiliser un service anonymement à se dévoiler, et peut être utilisée pour recouper des données depuis plusieurs services en ligne, en plus de n'être aucunement remplaçable en cas de vol de données biométriques. Qui souhaite avoir ses données d'identification compromises à vie ?

Alors la solution repose-t-elle dans **l'authentification à plusieurs facteurs (MFA)** ? **Les "One Time Password" (OTP)** ? **Les authentifications comportementales** ? Est-il encore possible de les envisager sachant que ces solutions n'empêchent nullement les attaques par phishing, et que le phishing est aujourd'hui particulièrement répandu pour le vol d'identité ?

Par ailleurs, qu'apportent **les clés USB** de sécurité ? Les utilisateurs sont-ils prêts à utiliser des solutions matérielles pour s'authentifier partout ? Comment peuvent-ils gérer les pertes et les pannes ?

Que valent les "**passkeys**", ces nouvelles solutions sans mot de passe poussées notamment par Google et Apple ? Est-ce bien raisonnable de donner toutes les clés de notre vie numérique aux GAFAM, même lorsque des services tiers (ou publics) sont utilisés ?

Est-il encore possible d'avoir des solutions d'authentification sûres, respectueuses de la vie privée et indépendantes ? C'est ce que nous aborderons dans cette présentation !

Je reprends la plume

Qui est Renaud Lifchitz ?

Renaud Lifchitz, directeur scientifique de Holiseum, et membre de l'ARCSI (**A**ssociation des **R**éservistes du **C**hiffre et de la **S**écurité de l'**I**nformation) est un expert français reconnu en sécurité informatique ayant une longue expérience d'auditeur et de formateur, principalement dans le secteur bancaire et le secteur télécom. Il s'intéresse tout particulièrement au développement sécurisé, aux protocoles de communication sans fil et à la cryptographie.

Il a été intervenant dans de nombreuses conférences internationales et a formé directement plus de 2000 personnes. Ses travaux de sécurité les plus significatifs portent sur les thèmes : cartes bancaires sans contact, géolocalisation GSM, blockchain, signatures RSA, ZigBee, Sigfox, LoRaWAN, Vigik et calcul quantique

Demande d'inscription pour le Lundi de la cybersécurité du mois de décembre

Lundi 11 décembre, à partir de 18 h 00, en ligne par visio-conférence Zoom.

Cet évènement se fera **en distanciel par Zoom**,

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien personnel vers la visioconférence.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans votre message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements.

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants.

Si vous souhaitez ne plus recevoir les lettres des « Lundi de la cybersécurité » mensuels, une simple demande par mail suffit. Si vous voulez être ajoutés à la liste de distribution, demandez-le nous.

Et bien entendu, si vous vous inscrivez pour assister à notre évènement, soyez connectés, avec votre prénom et votre nom (nous ne demandons pas un password 😊 le **lundi 11 décembre**. Début de l'évènement à 18h00.

Quelques minutes avec une organisation

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une dizaine de minutes la parole à une organisation, qui opère dans l 'écosystème du numérique et dans la sécurité de l'information.

Le nom de l'invité surprise et de son organisation vous seront donnés bientôt.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements sur le web de l'ARCSI, en **https://www.arcsi.fr/.**

Pour le Lundi de la Cybersécurité du mois d'octobre où **la professeure Solange Ghernaouti**, de l'université de Lausanne, nous a parlé de « ***Cybersécurité et intelligence artificielle : perspective transdisciplinaire et sociétale*** », vous trouverez les slides de Solange Ghernaouti et l'excellent compte-rendu de 13 pages, avec les questions – réponses, rédigé par **Clarisse Véron**, étudiante dans le master Cybersécurité et E-santé de l'université Paris Cité en :

https://www.medef92.fr/fr/evenement/lundi-de-la-cybersecurite-23-oct-2023-18h-20h.

Le coin de l'IA générative

Question posée à Chat GPT, et sans livrer, bien sûr, de données confidentielles qui pourraient être exploitées :

« ***Les mots de passe sont-ils obsolètes ?*** »

Réponse reçue :

« Les mots de passe ne sont pas obsolètes, mais il est vrai qu'ils peuvent être vulnérables aux piratages et aux attaques de phishing. De nombreuses entreprises et organisations cherchent des moyens plus sécurisés pour protéger les comptes des utilisateurs, comme l'authentification à deux facteurs, la biométrie ou les clés de sécurité. Il est important de rester vigilant et de choisir des mots de passe forts, uniques et de les changer régulièrement pour protéger ses comptes en ligne. »
Gérard

:

Lundi de la Cybersécurité de janvier

lundi 22 janvier 18h-20h

Bernard Besson – Contrôleur Général honoraire de la police nationale, dirigeant chez Bernard Besson Consulting

Etat stratège et cybersécurité