Entretien

Salwa Harif : *La cybersécurité est désormais une préoccupation partagée au Maroc*

Ingénieure cybersécurité ayant acquis une grande expérience chez des groupes internationaux de renom, Salwa Harif est la fondatrice et directrice d'ISSROAD, une société de conseil et d'intégration de solutions cybersécurité. Dans cet entretien, elle nous livre ses impressions.

Libé : Vous êtes à l'initiative de la première édition de l'événement «Cybersecurity Awareness Month» qui s'est tenue en octobre dernier à Casablanca. Quel en était l'objectif ?

Salwa Harif : Le but est simple : éveiller les consciences sur les nouvelles règles de sécurité numérique à l'heure où nous passons en moyenne plus de 6 heures par jour devant des écrans, selon un rapport d'Electronics Hub.

Cet événement, organisé en partenariat entre ISSROAD, le Technopark, CSPF et Elysec, vise à démocratiser le sujet pour qu'il ne reste pas l'apanage des experts.

A travers plusieurs webinaires et discussions, nous cherchons à encourager le dialogue autour des bonnes pratiques et des nouvelles menaces en ligne. L'initiative s'inspire d'un mouvement international lancé en 2004 par la National Cybersecurity Alliance et le Department of Homeland Security aux Etats-Unis, et elle est aujourd'hui adoptée par de nombreux pays.

Rendez-vous donc en 2025, pour la deuxième édition !

Les participants à cet événement étaient majoritairement jeunes, avec une forte présence de femmes. Y voyez-vous une explication ?

Cet événement a attiré un public jeune, dont beaucoup de femmes, avec des participants venant de Casablanca, Tanger, Nador et d'autres villes. La cybersécurité est désormais une préoccupation partagée : chacun perçoit le risque et cherche à comprendre les bases pour se protéger. Ce dynamisme des jeunes est inspirant; ils veulent apprendre des experts et affichent un enthousiasme débordant !

Concernant la mixité, j'attache une importance particulière à garantir la parité parmi les experts et lors de nos recrutements. Même si l'IT reste majoritairement masculin, nous veillons à ce que les femmes aient une place égale dans ces échanges.

Quatre thèmes ont ponctué cette rencontre. Pourquoi avoir choisi de mettre l'accent sur ces volets ?

Les quatre thèmes principaux de la rencontre étaient :

Atelier 1 : Salwa Harif – Prévenir les cyberattaques : Vous êtes la première ligne de défense

Atelier 2 : Ilham Ikbal – Comprendre et contrer les ransomwares : Se préparer pour survivre

Atelier 3 : Jamal Jessour – Démystification de l'ingénierie sociale : les attaques psychologiques.

Atelier 4 : Samy Rifky – Confidentialité des données en entreprise : vos données, vos règles.

Ces thèmes répondent aux menaces récurrentes identifiées dans le rapport Interpol de 2023 sur les tendances des cybermenaces en Afrique. L'objectif était d'aborder les risques concrets auxquels le Maroc et l'Afrique sont confrontés.

D'autres menaces, comme les trojans bancaires ou les attaques ransomware contre les industriels, ont été couvertes par ISSROAD lors de webinaires organisés dans les semaines suivantes, et qu'on peut trouver sur la chaîne YouTube.

A votre avis, quels sont les secteurs les plus touchés par la cybercriminalité au Maroc et pour quelle raison ?

La cybercriminalité poursuit deux grandes motivations : le gain financier et l'activisme.

Pour l'argent, les criminels ciblent les secteurs capables de payer des rançons élevées, comme la finance, l'industrie et la santé. Ils utilisent souvent des ransomwares pour bloquer les systèmes industriels ou menacent de divulguer des données sensibles, notamment dans le secteur bancaire.

Pour des raisons politiques ou idéologiques, les hacktivistes visent plutôt les institutions publiques, modifient les sites officiels (défaçage) ou exposent gratuitement des données sur le dark web.

Une enquête menée par Trend Micro au Maroc révèle que le pays est le plus touché en Afrique par les trojans bancaires. Pouvez-vous nous éclairer sur ce type de menaces et d'autres menaces courantes?

Le trojan, ou en français « cheval de troie », est un type de logiciel malveillant (malware) qui se fait passer pour un logiciel légitime tout en cachant du code malveillant. Il a comme spécificités de s'installer avec des logiciels qu'on pense légitimes :

Via des logiciels crackés

Via des applications dans le play store

Via des jeux ou autre application téléchargés en ligne

Ils sont souvent très difficiles à détecter par les utilisateurs car leur objectif est de rester cachés au maximum. Ils peuvent cependant être détectés par les logiciels antivirus bien classés et régulièrement mis à jour.

Les trojans bancaires sont spécialisés dans le vol des identifiants bancaires, l'interception des codes de vérification SMS et le remplacement des pages de connexion bancaires légitimes.

L'attaquant ayant réussi à infecter un appareil (ordinateur ou mobile) a souvent le contrôle total sur celui-ci, il peut lancer des commandes à distance et récupérer les données.

D'après le rapport de Trend Micro, le Maroc devance largement les autres pays d'Afrique en termes d'infections de trojans bancaires.

Les Marocains utilisent de plus en plus d'applications "craquées". Un mot sur ce phénomène et les risques encourus ?

Les applications crackées font partie du quotidien des Marocains, habitués à se fournir dans des marchés comme Derb Ghallef en licences crackées. Ces logiciels crackés sont des versions modifiées des logiciels originaux, permettant à ceux qui les utilisent de bypasser le système de licences ou de le remplacer par un système de génération de clés de licences qu'ils maîtrisent.

Les licences originales étant parfois coûteuses, beaucoup préfèrent cette solution peu onéreuse pour accéder aux fonctionnalités. Cependant, le problème devient sérieux lorsqu'il n'y a pas de frontières claires entre un système vulnérable (un appareil non protégé avec des applications crackées installées) et un autre qui doit être sécurisé (comme un site web bancaire, des dossiers clients ou une comptabilité interne).

Enfin, lors des audits, les éditeurs de logiciels peuvent identifier les sociétés utilisant des licences non conformes (crackées), lesquelles risquent alors des amendes et des poursuites pour violation des lois sur la propriété intellectuelle et les droits d'auteur.

Le facteur humain est au cœur de la sécurité, disiez-vous lors de votre exposé. Au Maroc, est-on suffisamment conscient des risques numériques ?

En deux mots : Absolument pas ! La prise de conscience des risques numériques est encore trop faible au Maroc, et le plan Digital Maroc 2030 accorde malheureusement peu d'attention à la sécurité numérique.

Dans l'univers numérique, il y a trois piliers : la technique, l'humain et l'organisation. Pour illustrer, imaginons une voiture :

La technique représente la voiture elle-même : des outils performants, installés intelligemment pour qu'elle soit fiable.

L'organisation, ce sont les règles et les lois, comme le code de la route et les procédures à suivre en cas d'accident.

L'humain, c'est le conducteur qui doit être formé, sensibilisé aux risques et aux responsabilités pour utiliser le véhicule en toute sécurité.

Pour réussir la transformation digitale, il ne suffit pas d'avoir les bons outils ou des règles bien définies. La formation et la sensibilisation de chacun aux risques numériques sont indispensables, tout comme le fait d'apprendre à conduire.

Quels sont aujourd'hui les gestes de base à adopter pour se prémunir, ne serait-ce qu'un peu, des risques de la cybercriminalité ?

La règle d'or en cybersécurité : «Je réfléchis avant de cliquer !». Les clics impulsifs et la confiance aveugle sont souvent la porte d'entrée des cyberattaques.

Propos recueillis par
Alain Bouithy

Le Maroc devance les autres pays d'Afrique en termes d'infections de trojans bancaires

La cause, extrait de la déclaration officielle de la DGSSI : «Tout d'abord, il convient de souligner que les banques marocaines sont des leaders en Afrique en matière de digitalisation, ce qui les rend plus exposées aux cyberattaques. En plus, il est important de noter qu'une détection de cyberattaque ne signifie pas nécessairement qu'une attaque a réussi, car toutes les banques marocaines disposent de systèmes de supervision et de détection avancés, ainsi que de plans de gestion d'incidents bien établis. Enfin, la Direction de la supervision bancaire de Bank Al-Maghrib collabore étroitement avec la Direction générale de la sécurité des systèmes d'information (DGSSI) pour garantir le respect strict de la réglementation en vigueur. En outre, la DGSSI effectue régulièrement des audits à la suite de chaque incident de cybersécurité». La cybersécurité dans le secteur bancaire | DGSSI

Voici les mesures simples mais essentielles pour réduire les risques :

Installer un antivirus de qualité : Un bon antivirus bloque l'installation de logiciels malveillants avant même qu'ils ne deviennent un problème. Utiliser un coffre-fort de mots de passe : Un gestionnaire de mots de passe permet de créer des mots de passe complexes et uniques pour chaque application. Il existe des coffres-forts open-sources comme keepass pour les PCs.

Activer l'authentification multifacteurs (MFA) : Même si un mot de passe est compromis, le MFA rend l'accès à vos comptes plus difficile pour les hackers.

Mettre à jour ses applications et systèmes

Les mises à jour corrigent des failles de sécurité. Ignorer ces mises à jour revient à laisser des portes ouvertes aux intrusions.

Eviter les applications crackées : Elles contiennent souvent des malwares et ne sont pas mises à jour, ce qui les rend vulnérables.

Faire des sauvegardes régulières : En cas d'attaque, les sauvegardes sont essentielles pour restaurer rapidement vos données. Pour les systèmes critiques, n'hésitez pas à simuler des restaurations pour vérifier l'efficacité des sauvegardes.