

# ECSM - Semaine 2

1

ECSM 2019, du 1er au 31 Octobre, l'European Federation of Cyber Security Experts met à disposition des contenus de tout type pour zoomer sur la cybersécurité et susciter des interrogations / réflexions sur l'évolution du cyber espace.

Au démarrage de cette 2<sup>ème</sup> semaine, l'EFCSE poursuit sa démarche de sensibilisation à la cybersécurité dans l'Union Européenne.

Après le zoom de la 1<sup>ère</sup> semaine sur l'importance de l'information, nous poursuivons sur la base de la curiosité, telle une clef pour plonger plus profondément dans le cyber espace.



Be secure,  
Be curious

En préambule, notons que la nouvelle Présidente de la Commission Européenne, **Ursula von der LEYEN**, a déclaré il y a à peine un mois (10 septembre 2019) :

2

“Nous devons adapter notre marché unique à l'ère numérique, nous devons tirer le meilleur parti de l'intelligence artificielle et du Big Data, nous devons améliorer la **cybersécurité** et nous devons travailler dur pour notre souveraineté technologique.”

Cette déclaration semble présenter de belles opportunités pour l'Union européenne, même si un nouveau cyberspace est en cours de préparation.

Pour suivre de telles évolutions, regarder les choses autrement peut permettre un accès au niveau supérieur de la compréhension de la cybersécurité, non seulement en restant informé, mais en faisant appel à sa curiosité pour aller plus loin.

Au-delà de l'information, il s'agit de rechercher activement les prochaines grandes nouveautés en matière de cybersécurité, les prochaines pratiques optimales ou les meilleures solutions pour contrer les dernières cybermenaces.

L'étape suivante de cette démarche consiste à utiliser toute source d'information y compris ce formidable outil qu'est le Web, pour en extraire les bonnes informations au bon moment, en étant proactif et non simple « récepteur passif ». Attention, être curieux ne veut pas dire être crédule, votre sens critique doit rester en éveil, mais nous évoquerons ce sujet la semaine prochaine.

De nombreux facteurs doivent être pris en compte lors de la gestion de cybermenaces et de suites d'attaques, être informé est important mais pas suffisant, il ne s'agit pas d'être en position « patient zéro ». Il est nécessaire d'aller plus loin dans sa compréhension du cyberspace et de son fonctionnement, d'être curieux et organisé dans sa recherche.

Pour alimenter cette curiosité, l'EFCSE a prévu un programme intégrant différents sujets et questions qui, nous le souhaitons, sauront maintenir votre intérêt tout au long de ce mois d'octobre, et plus...

L'une des principales classifications des cybermenaces est l'ingénierie sociale, conçue pour tromper et exploiter les individus. Dans un contexte de sécurité de l'information, il s'agit bien de pratiques clairement malveillantes, basées sur la manipulation psychologique, personne n'est vraiment à l'abri.

Les cybercriminels s'adaptent en permanence, ils augmentent les volumes d'attaques et « tirent » sur toutes cibles, entreprises de toutes tailles, de tout statut, gouvernements, particuliers, professions réglementées, etc. ... les attaques sont évolutives, il s'agit donc bien d'observer sous des angles variés pour essayer de comprendre quel comportement adopter ou quelle(s) habitude(s) changer.

Être curieux, faire preuve d'imagination et être inventif peuvent aider à déjouer des cyber menaces.

Lorsqu'on parle par exemple de chatbot malicieux, alimentés par l'intelligence artificielle et capables de nous inciter à divulguer des informations sensibles, avons-nous une curiosité assez créative pour en imaginer les conséquences et le coup d'après ?

Adopter de nouveaux objets connectés dans son quotidien, intégrer de nouvelles formes de travail collaboratif dans l'entreprise, ou encore fournir « quelques » informations personnelles sur un site marchand, sont autant d'exemples d'accès potentiel à des informations intéressantes pour un cyber criminel.

Il ne s'agit pas d'être alarmiste mais tout simplement de déclencher l'étincelle de questionnement sur l'usage que chacun peut faire des toutes ces nouvelles tendances technologiques attractives.

Be secure,  
Be curious

Désir de comprendre, envie d'enrichir une expérience, capacité à pousser plus loin et à regarder autrement, la **CURIOSITE** est un moteur puissant pour l'humain.

C'est aussi un facteur de motivation et un stimulant pour l'innovation.

En matière de cybersécurité envisager les choses sous des aspects différents et donc faire preuve de curiosité, peut contribuer à détecter des failles ou à ajuster des usages.

- Regardez autrement ce que l'on appelle la sécurité des données.
- Que signifie concrètement : assurer la confidentialité des données ?
- Posez-vous la question de votre usage des réseaux sociaux ou des objets connectés.
- Demandez-vous ce que signifie une cyber criminalité plus forte et plus efficace (l'actualité l'évoque en permanence).
- Qu'est-ce que L'intelligence artificielle vient faire dans la cybersécurité ? Comment cela se traduit-il dans notre quotidien, tant personnel que professionnel ?

Autant de questionnements qui contribuent, peut-être, à modifier nos mauvaises cyber-habitudes face à de mauvaises cyber-intentions !

EFCSE vous invite à aborder les sujets sous divers angles, en suivant une sorte de guide de réflexion, selon des thèmes différents chaque semaine.

Nous avons planifié des publications journalières,

Du lundi au vendredi,

Selon des formats variés :

Actualité, outil, dossier de fond, quiz, ...

