Date :01/11/2020 | Votre interlocuteur : Service sécurité | Mail : contact@espace-technologie.com | # 01

Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

LES NOUVELLES MENACES DE LA PROCHAINE DECENNIE

COMPÉTENCES - TRANSPARENCE - CONFIANCE

GENERALITES

Au cours de la prochaine décennie, les risques liés à la cyber sécurité deviendront plus difficiles à évaluer en raison de la complexité croissante du paysage des menaces, de l'écosystème des attaquants et de l'expansion de la surface d'attaque des entreprises.

L'Agence européenne pour la cyber sécurité (ENISA), avec le soutien de la Commission européenne, vient de publier son 8e rapport annuel sur l'état de la menace cyber. Intitulé ENISA Threat Landscape 2020,

l'ENISA entérine le fait que l'irruption de la pandémie en début d'année constitue une nouvelle frontière entre l'ancien et le nouveau en matière de menaces cyber. « En raison de la pandémie actuelle de Covid-19, nous entamons la décennie avec une nouvelle norme et de profonds changements dans le monde physique et le cyberespace. Avec la distanciation ou le confinement, le public aura tendance à utiliser l'espace virtuel pour communiquer, établir des relations et se socialiser. Cette nouvelle norme introduira de nouveaux défis dans toute la chaîne de valeur numérique et, en particulier, dans le secteur de la cyber sécurité », résume le rapport.

LES DIX DEFIS DANS LA PROCHAINE DECENNIE

1- FAIRE FACE AUX RISQUES SYSTEMIQUES ET COMPLEXES

Le risque cyber se caractérise par la vitesse et l'ampleur de sa propagation ainsi que par l'intention potentielle des acteurs de la menace. L'interconnexion des différents systèmes et réseaux permet aux attaques de se propager rapidement et largement, ce qui rend les risques plus difficiles à évaluer et à atténuer.

2- GENERALISATION DE LA DETECTION DE L'IA ANTAGONISTE

La détection des menaces exploitant l'IA (Intelligence Artificielle) pour lancer une attaque ou éviter la détection constituera un défi majeur pour l'avenir des systèmes de cyberdéfense.

3- AUGMENTATION DES ERREURS INVOLONTAIRES

Avec le nombre croissant de systèmes et de dispositifs connectés au réseau, les erreurs involontaires continuent à être l'une des vulnérabilités les plus exploitées dans les incidents de cyber sécurité.

4- MENACES LIEES A LA CHAINE D'APPROVISIONNEMENT ET AUX TIERS

La chaîne d'approvisionnement diversifiée qui caractérise aujourd'hui l'industrie technologique offre de nouvelles possibilités aux acteurs de la menace pour tirer profit de ces systèmes complexes et exploiter les multiples vulnérabilités introduites par un écosystème hétérogène de fournisseurs tiers.

5- ORCHESTRATION DE LA SECURITE ET AUTOMATISATION

Le renseignement sur les menaces cyber et l'analyse comportementale deviendront de plus en plus importants avec l'automatisation des processus et de l'analyse.

6- REDUCTION DES FAUX POSITIFS

Cette promesse longtemps attendue est essentielle pour l'avenir de l'industrie de la cyber sécurité et pour lutter contre la lassitude des fausses alarmes qui se multiplient.

7- STRATEGIES DE SECURITE ZERO-CONFIANCE

Face à la pression croissante exercée sur les systèmes informatiques par les nouvelles exigences des entreprises,

tels que le travail à distance, la numérisation du modèle économique et l'étalement des données, la stratégie zéro-confiance est considérée par de nombreux décideurs comme la solution de facto pour sécuriser les actifs des entreprises.

8- ERREURS DE CONFIGURATION DU CLOUD D'ENTREPRISE

De nombreuses entreprises migrant leurs données vers des solutions basées sur le cloud, le nombre d'erreurs de configuration va augmenter, exposant les données à une brèche potentielle.

9- MENACES HYBRIDES

Les cybercriminels adoptent de nouveaux modes opératoires augmentant les menaces du monde virtuel et physique. La diffusion de la désinformation ou de fausses nouvelles, par exemple, sont des éléments clés du paysage des menaces hybrides.

10- L'ATTRAIT DU CLOUD

L'infrastructure comme cible va accroître la menace. La dépendance croissante à l'égard des infrastructures du cloud public augmentera le risque de pannes. La mauvaise configuration des ressources du cloud reste la cause principale des attaques dans le cloud, mais les attaques visant directement les fournisseurs de services dans le cloud sont de plus en plus populaires parmi les pirates.

Jérôme, Notre expert en Cyber Sécurité est à votre disposition pour vous assister dans votre plan de prévention des risques CYBER..