Nobody Maxime MONTOURO Alexandre PICOULET-SONDER

Notes :

Qui : Jessica Haworth journaliste

Quand : 28 july 2021

ou : site internet the daily swig UK !!! Cybersecurity News and Views

Theme : Cyber attaque durant le onfinement dut au télétravail

point de vue :/

idees secondaires :

- 60 % des failles sur les employees ont été détecté sur des employés à la maison

- l utilisation d une ia a été un franc sucès pour réduire les failles et préserver plusd’ $1.5 million

- presque la moitié du data volé représente du perso

- les milieus les plus attaqué sont la finznce et le pharmaceutique qui représente plus de $10 million de pertes uivi de l’hopital milieux a risque surtout pendant cette période

Compte Rendu :

Cet article de presse britanique pour le Daily Swig, rédigée par la journaliste Jessica Hamworth, relate de la montée exponentielle des cyber-attaques depuis le premier confinement.

En effet, dans cet article, la journaliste évoque le problème qu’a entrainé le télétravail  car plus de 60 % des failles de sécurité ont été détecté directement chez les employés (source IBM). Ajouter à cela, les données volées représentent des données personnelles (de l’email en passant par les mots de passe) et représente une perte concidérable pour les entreprises.

Pour contrer ces failles, la mise à jour des systèmes s’est avérée necessaire mais aussi l’adoption de l’IA dans l’analyse de risque. Ce fût d’ailleurs un franc succès, cette dernière permit de préserver plus $1.5 million par entreprise.

De plus, durant la crise, les attaquants ciblés des milieux à risque. En effet, plus de $10 million de perte sont représentés par le domaine de la finance et de l’inustrie pharmaceutique, suivi de près par les hôpitaux.

Pour conclure, la crise du COVID-19 a permi de centrer la sécurité des services informatique au coeur même des entreprises. Aujourd’hui, des personnes travaillent à plein temps pour corriger, mettre à jour et maintenir les differents services afin de mieux garentir la sécurité et la privatisation de données personnelles. Mais jusqu’ou allons nous, avec des hackeurs toujours plus performants et des failles de toute taille ?

Email :

Dear Madam Smith,

Thank you for your contact,

You contacted me to have some ideas about system’s security since the COVID-19. I know that a lot of employees are in remote working, and we work in a critical domain.

The problem is clear, we are impact each days by cyber-attacks and in 90 % it is a humain breach (phishing for exemple).

We have 2 possibilities to patch cyber breaches. First, be carefull with emails. Secondly, we can use, for our system, an IA who can search breaches. I know that, pay a good IA is a lot of money but I repeat, we work on a critical domain. Since 2 weeks, good AI perform on the market and I think, we can follow it and watch to use this IA in the future.

So, it’s really important to have a stable system.

Thank you for your consideration,

Best regards,

Maxime MONTOURO Ex White Hat – Consulting in Cyber Security