Atelier "Cybersécurité"

Animé par Jonathan MONGRENIER de CLOUD SYSTEMS

Visio TEAMS le 24/02/2021 de 18h30 à 20h

Les différents types d'attaques et leur proportionnalité

- Attention ransomware : +255% en 2020 et le plus impactant pour le fonctionnement de l'entreprise (cryptage ordi et serveurs + blocage des SI => travail sans informatique)
- Impacts financiers (image et confiance des tiers, arrêt de production, rançons...)

Exemples et explications d'attaques subies par des organisations locales et à l'international

Les 7 étapes d'une attaque cyber

1. Reconnaissance / préparation (social ingeniering : se renseigner sur la cible te sur 1 personne en particulier à attaquer)
2. Exploration : cartographie du système
3. Accès aux "postes privilèges" pour récupérer les mots de passe admin
4. Exfiltration : voler les données sensibles
5. Attente : patienter le moment propice
6. Assaut : déclenchement de l'attaque
7. Obfuscation : négociation de la rançon sans possibilité de récupérer les données / préconisation ANSSI : ne pas payer pour ne pas financer les hackers

Comment s'en protéger ? Les bonnes pratiques

Pare-feu pour détecter les comportements anormaux

1ère vulnérabilité = humain : surtout en cas de télétravail

- Mise à jour systèmes et applications
- Sauvegardes régulières (tester régulièrement et s'assurer qu'elles soient protégées)
- Gestion des mots de passe (complexes et uniques + coffres forts de stockage des mots de passe comme keepass => https://keepass.fr/)
- Gestion des comptes à privilèges (user et admin)
- Gestion des droits d'accès (accès aux fichiers et au réseau : prévenir en mettant en place des cloisonnements)
- Surveillance des SI (analyse journaux / log)
- Cloisonnement des systèmes pour limiter la propagation
- Restriction d'accès aux périphériques (ports USB)
- Contrôle des accès externes (VPN pour personnels externes et sous-traitants)
- Sensibilisation des utilisateurs et des dirigeants face à la menace

Antivirus recommandés par Jonathan : bitdefender ou kaspersky

⇨ **Ne jamais en utiliser de gratuit pour un usage professionnel**

Comment vérifier si une adresse mail a été victime d'une fuite de données : https://haveibeenpwned.com/

Si sécurité compromise : changer le mot de passe utilisé et d'autant plus s'il est utilisé sur d'autres sites ou appli

Si vous avez des questions : nous vous invitons à contacter Jonathan au 06 37 13 17 45 ou info@cloud-systems.fr