43° RAPPORT ANNUEL DE LA CNIL (2022)

QU'EST-IL ARRIVÉ CETTE ANNÉE Á ORTHORISQ ET AUX ORTHORISQUEURS

- Avons-nous été attaqués ou menacés?
- Et cela malgré toutes nos précautions (bof n°90 novembre 2021)

DE NOMBREUX « HAMEÇONNAGES »

- Sur des messageries non sécurisées personnelles
- Type: appel au secours d'une connaissance
- Ne jamais répondre (vous donnez au moins votre localisation…)
- Bloquer ou marquer comme spam ou comme hameçonnage

DES ATTAQUES NÉCESSITANT L'INTERVENTION DE L'ANSSI

- 12 cyber attaques d'établissements de santé par Ranconware
- Groupe russe Lockbit3 ou Vice Society
- E-mail avec pièce jointe piégée, envoyé à une adresse rattachée à l'établissement de soin
- Fonctionnement dégradé (parfois un an) car nécessité d'isolement des systèmes d'informations pour éviter la propagation des attaques
- Cout: généralement deux fois le montant de la rançon demandée

DES ATTAQUES « SIMPLES » DE MESSAGERIES SÉCURISÉES PROFESSIONNELLES

- Toute attaque d'une messagerie (ou d'un site) professionnelle sécurisée doit faire l'objet
  - D'une déclaration à « cybermalveillance.gouv.fr »
  - D'une plainte à la CNIL
  - Doit faire prendre des mesures correctives et préventives

TENTATIVE D'EXTORSION DE FOND DONT ORTHORISQ A ÉTÉ VICTIME

- Vous avez reçu un e-mail de votre propre compte mail
- J'ai accès par un cheval de Troie à tous vos courriels, liste de contacts, caméra et microphone
- Je vais diffuser à vos contacts une vidéo pornographique vous mettant en cause
- Payez..en bitcoins sur l'adresse portefeuille bitcoin…dans les 48 heures. Sinon…
- Ne partagez pas cet e-mail; je le saurai immédiatement et diffuserai la vidéo

SI VOUS TRAVAILLEZ EN RÉSEAU

- DÉBRANCHEZ LE CABLE RÉSEAU ET LE WI-FI
- DANS TOUS LES CAS N'ÉTEIGNEZ PAS L'ORDINATEUR (cela risque d'effacer des éléments de preuve situés dans la mémoire)

ALERTEZ IMMEDIATEMENT VOTRE INFORMATICIEN

- C'EST LUI QUI SCANNERA LE SYSTÈME
- RELANCER VOS ANTI-VIRUS RISQUE DE SUPPRIMER DES TRACES DE L'ATTAQUE

PRÉVENIR TOUS LES COLLABORATEURS DE L'ATTAQUE EN COURS

PLUS AUCUNE MANIPULATION

RÉFLÉCHIR

- QUELS FICHIERS SEMBLENT VISÉS
- PAR QUELLE VOIE D'ACCÉS? Une pièce jointe avec un malware non détecté?
- A PRIORI: courriel non chiffré émis à partir d'une messagerie non sécurisée
- VERIFIER L'ABSENCE D'UTILISATION RÉCENTE DU MODE ADMINISTRATEUR

PRÉVENIR LES PERSONNES DONT LES DONNÉES PERSONNELLES SONT MENACÉES ET LES METTRE EN GARDE CONTRE UNE UTILISATION FRAUDULEUSE

SIGNALEMENT
ET
PLAINTE Á LA CNIL

- 72 HEURES
- DÉCRIRE L'AGRESSION
- PRÉCISER LES MESURES PRISES: CURATIVES ET PRÉVENTIVES

RENSEIGNER LE REGISTRE DE NOTIFICATION DES VIOLATIONS DE DONNÉES

DÉPOSER UNE PLAINTE AU COMMISSARIAT DE POLICE OU A LA GENDARMERIE

- NE PAS OUBLIER « cybermalveillance.gouv.fr »

DE NOMBREUSES VIOLATIONS DE DONNÉES

- Vol de données (pour les revendre)
- Utilisation illicite de données
- La CNIL a reçu 4088 signalements de violations de données (tout confondu en 2022)

LES PROBLÈMES POSÉS PAR CES VIOLATIONS

- Licéité et finalisation de l'accès aux données sensibles
- Qualité du requèteur (il doit être missionné)
- Contenu des fichiers: principe de minimisation des données conservées
- Accord des personnes dont les données sont transmises
- Information sur les droits des personnes dont les données sont concernées
- Garanties de sécurité pour les données communiquées
- Enoncé clair de la date à laquelle les données seront détruites

PRINCIPES DU RGPD

CHAPITRE II articles 5 et 6

CONDUITE A TENIR: la même que pour une tentative d'extorsion de fonds

SITE ORTHORISQ

- ACTUALITES DU RGPD ET CYBERSÉCURITÉ
- VEILLE JURIDICO TECHNIQUE
- TRUCS ET ASTUCES

- MERCI DE NOUS RACONTER VOS AVENTURES PERSONNELLES…. PARTAGEABLES