COLLOQUE SSI MINISTÈRE 19 OCTOBRE 2018

TABLE RONDE " ÇA N'ARRIVE PAS QU'AUX AUTRES ! "

Intervention
Ehpad Cossé-Le-Vivien (Mayenne)

PRÉSENTATION

EHPAD PUBLIC HOSPITALIER AUTONOME

78 RESIDENTS

ZONE RURALE 20KMS LAVAL – 25KMS CHÂTEAU-GONTIER

BUGDET 2,9 M€

ETP 60

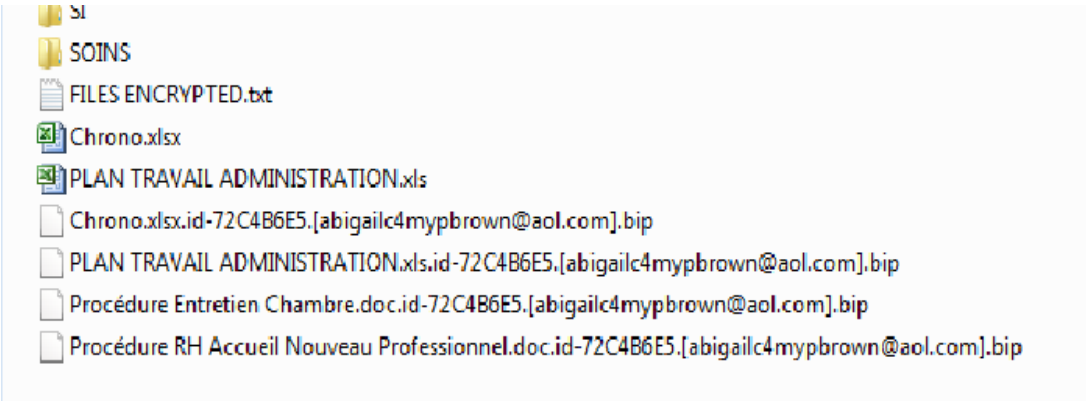
SI

APPLICATIONS METIER : NETSOINS-GEPSS–PLANICIEL+ BUREAUTIQUE + 8 BOITES MAIL
ARCHI : RESEAU FILAIRE + 18 BORNES WIFI + 10 ORDI WINDOWS7
PRESTATAIRE INFORMATIQUE ENTREPRISE MAYENNAISE
SAUVEGARDE : CHAQUE SOIR VERS 22H30 + ITERATION 6 JOURS + BOITIER NAS CONNECTE AU LAN

JAMAIS DEUX SANS TROIS

- 3 mai : 1ere attaque
  - Données bureautique chiffrées
  - Descente de la dernière sauvegarde par le prestataire durée 3 heures
  - Architecture de sauvegarde non modifiée via le lan reconduite par le prestataire
  - Impact : Interruption service administratif pendant 5 heures

- 4 juin : bis repetita
  - 19 juin : lettre de résiliation du contrat de prestation informatique



- 9 juillet : Attaque fatale

3EME ATTAQUE FATALE

- 15 ans de données bureautique perdues
- Sauvegardes chiffrées …. pas de copie hors réseau local
- Transmission à 17h45 par le technicien après échange avec le hacker de la démarche pour le paiement la rançon en bitcoin pour un voyage à Londres et à Vienne la nuit du 9 juillet
- Rôle - Responsabilité Prestataire
  - Mail 10/7/2018 12h au prestataire « J'envisage de ne pas payer sur mes deniers personnels la rançon + 4 500 et un site bitpanda basé à Vienne (n'ayant pas validé mon compte) me le déconseille et ma banque me le déconseille vivement. »
  - Réponse du prestataire « Je profite de votre mail pour vous relancer sur 2 points : Suite à votre courrier de résiliation, qu'attendez-vous de nous ? - Nous vous avons fait parvenir une information par mail concernant la RGPD, notamment au sujet du copieur, mais sans retour de votre part… »

Decoding Files 0.7btc tommorow 0.8btc
pay in Bitcoin (BTC)
translation at the expense of Bitcoin
1PBBzNzPQeAzMoP4dWYkSht9rLEpCrH7BM
Buy Bitcoin here https://localbitcoins.com or
https://www.buybitcoinworldwide.com/find-exchange/ or
https://www.coinbase.com or
https://www.xmlgold.eu or
any other exchanger
or
write to Google how to buy Bitcoin in your country?
in order to guarantee the availability of our key
we can decrypt one file for free
the size of the files <1 mb, doc.docx.xls.xlsx.pdf.jpg.bmp.txt file format
other formats will not be free decryption
after payment you will receive a program
how many computers do you have encrypted ?

3EME ATTAQUE FATALE

- Action
  - Activation service anti-spam par Orange sur les boites mails 10/7
  - Arrêt de branchement de clé USB + boitiers externes aux ordi 10/7
  - Dépôt plainte à la gendarmerie de Craon 11/7
  - Sauvegarde 2 fois par semaine sur 2 boitiers non raccordes au Lan déposés dans le coffre fort depuis fin juillet
  - Gestion de la boite mail principal de l'Ehpad par la secrétaire et fermeture d'une boite
  - Mise en place de code sur le photocopieur par groupe utilisateur
  - Ehpad Meral : sauvegarde hebdomadaire sur boitier externe + harmonisation documentaire entre les 2 Ehpads
- Coût
  - 2000€ non payé à ce jour + 100€ Boitier externe
  - Interruption service 7 jours : service rétablit le 17 juillet facilité par des sauvegardes externalisées des applications métier et architecture reconduite