| Questions | Réponses |
|---|---|
| les systèmes linux ont ils été touchés ? Ou que windows ? | Que Windows dans notre cas. |
| | |
| Suivi en temps réel en décembre : ? / nuit et we | Suivi en temps réel au fur et à mesure du rétablissement des services et des postes. En différé la nuit après avoir pris les précautions d'usage le soir. |
| | |
| Quelle solution de sauvegarde utilisez vous ? Avez vous des sauvegardes déconnectées ? Principe du 321 de la sauvegarde ? | Au moment de l'attaque, nous disposions de deux systémes de sauvegarde et d'un systéme de réplication :<br>1. Sauvegarde sur bande<br>2. Script maison assurant un export ovf des vms sur le NAS avec rétention sur 4 semaines.<br>3. Réplication des exports sur le site de backup |
| | |
| Vous avuez des sauvegardes des postes ? | Nous avons des masters par service + un systéme de distribution des packages si besoin (Zenworks) |
| | |
| question: avez vous tout re installer serveur et PC from scratch | Non.<br>Pour les postes de travail, moins de 10 % ont été touchés au point de ne plus fonctionner. Les autres disfonctionnements ont été corrigés à distance par des mises à jour.<br>Pour les serveurs, nous avons du reinstaller la grande majorité. |
| | |
| Concernant le futur SOC, quel prestataire, quel tarif pour quel périmètre? | Société ITRust. Tarifs suivant périmétre de couverture. |
| | |
| Je n'ai pas bien compris la prestation externalisée mise en place pour une supervision "securité | SOC : Security Operation Center. Supervision par une plateforme distante de votre infra : détection des failles de sécurité et des tentatives d'attaque. |
| | |
| L'alerte initiale de la part du FAI, qui a entrainé la nécessité de la mise à jour: sur quel type d'équipement: Firewall, Anti virus??? | Information malheureusement confidentielle à ce stade de l'enquête. |
| | |
| J'ai compris que le pra a été d'une grande aide. Votre pra est-il communicable ? | Non, pas en l'état. Mais je peux communiquer en revanche sur sa structure et notre approche du sujet. |
| | |
| Et concernant le SOC, qui surveille le comportement réseau, sur quel type de solution? Basée sur de l'IA type Dark Trace? | https://www.itrust.fr |
| | |
| Vous parlez bien de PRA et non de PRI ? | A partir du moment où les locaux, les alimentations électriques ... n'étaient pas touchés, PRA = PRI. A noter que nous avons dû rappatrier nos serveurs du site de PRA. |
| | |
| La DSI c'est combien de personnes mobilisées ? Tous les sites sont interconnectés entre eux pour se partager le virus ? | 13 personnes mobilisées à plein temps pendant 10 jours y compris le week-end et très tard le soir.<br>70 sites interconnectés physiquement mais une segmentation en VLAN. |
| | |
| Votre PRA était sur un seul site ou à été dupliquer sur un autre site ? Le virus n'a pas été propager sur le site de PRA ? Concernant le PCA avez-vous pu ou pas reprendre l'ancien système fax, poste non connecté ou envisager la reprise des sauvegardes sur un nouveau serveur ? En tout cas Bravo pour votre réactivité. | Le virus n'a pas attaqué le site de PRA du fait des VLANs mis en place et des technologies utilisées (Baies Netapp en mirroring).<br>Pas de PCA au niveau des services. Nous devons travailler sur ce sujet. |
| | |
| sauvegardes épargnées pourquoi d'après toi ? | Baies Netapp protégées par une protection virale dédiée + Technologie Netapp (ce n'est pas du Windows) + Mirroring Asynchone + Snapshots + Droits d'accés limités<br>Le serveur de sauvegarde (Windows) a quant à lui été complétement détruit. |