CHEOPS TECHNOLOGY

The Cloud Customized For You !

CLUB ETI NOUVELLE-AQUITAINE
ENTREPRISES DE TAILLE INTERMÉDIAIRE

Club ETI Nouvelle-Aquitaine

Cybersécurité, cybersabotage-cyberattaque, guerre économique et numérique…

Sommaire

CHEOPS TECHNOLOGY
The Cloud Customized For You !

Une attaque pas à pas …

Etat de l'art & conclusion

Une attaque pas à pas …

CHEOPS TECHNOLOGY
The Cloud Customized For You !

Cas d'une administration avec plusieurs centaines de VM sur site

Etat de l'art du SI, périmètre de sécurité en place, Firewall, Antivirus, solution de gestion des correctifs, inventaire du parc

Chronologie de l'attaque

Samedi matin : applications métiers à l'arrêt, plus de messagerie, accès distant impossible

- 9h signalement du problème....par un client : 80% VM avec le message du Ransomware à l'ouverture de session.
- 10h mise en place d'une cellule de crise par le DSI : acceptation du problème, décision de couper tous les accès réseaux interne & externe. Constat, un certain volume de donnée est chiffrée par un ransomware... et les sauvegardes aussi
- 12h arrivé des équipes techniques sur site pour évaluation du plan d'action …
- 14h : Intervention d'un prestataire de réponse sur incident en support des équipes de la DSI & signalement auprès de l'ANSSI

Une attaque pas à pas … J+1

CHEOPS TECHNOLOGY
The Cloud Customized For You !

Recherche du patient zéro

- La cellule de crise avance difficilement car l'inventaire des serveurs compromis prend du temps et ne permet pas d'élaborer un plan d'action
- Les indicateurs de compromission ont été supprimés par les premières actions des équipes techniques, l'équipe de réponse sur incident a du mal à identifier l'attaquant
- l'ANSSI qui amène des indices sur la source

Fin de journée

- Premier contact avec les rançonneurs, partie légale gérée par la police. Et la question sensible: Payer ou ne pas payer ?
- La DSI s'occupe de la communication avec l'ANSSI afin d'éviter la panique, rassurer les clients et calmer les médias
- C'est confirmé par l'équipe technique, une partie des sauvegardes sont chiffrées

Une attaque pas à pas … les semaines défilent

CHEOPS TECHNOLOGY
The Cloud Customized For You !

Avec l'aide de 5 prestataires pendant 4 semaines dont une en 24/24

- Pas de perte de données car duplication : multiples sauvegardes logiques et physiques
- Restaurations des sauvegardes sur systèmes neufs
- Les serveurs se trouvant dans un réseau protégé sont non touchés. Importance de la segmentation des réseaux et du micro cloisonnement

Saisi du parquet

- Fichiers retrouvés sur Internet. 20Go publiés quelques mois plus tard

95% services rétablis après 4 mois

- Délai médian car ce type d'attaque enclenche plusieurs projets de sécurisation du SI: audit de l'annuaire d'entreprise, audit technique, refonte réseau, isolation des actifs sensibles, révision de la stratégie de sauvegarde, campagne de patch, …

Etat de l'art & conclusion

CHEOPS TECHNOLOGY
The Cloud Customized For You !

1. Préparer votre résilience

- Avoir dans son carnet d'adresse les contacts des instances étatiques : ANSSI, DIPJ, DGSI.
- Maillage avec le tissu associatif : CLUSIR AQUITAINE, CESIN, OSSIR.
- Préparer des contrats « prêt à l'emploi » avec des prestataires de réponses sur incidents
- Evaluer la résilience de vos équipes en simulant un exercice de cybercrise
- Surveillance à 360 de votre SI. Ne pas négliger les signaux faibles [connexion HNO, activités anormales,…]. Le vecteur d'attaque est souvent la messagerie.

2. La cybersécurité est vecteur de confiance dans les enjeux du numérique

- Gage de confiance pour les investisseurs et pour vos clients
- En interne, l'équipe sécurité en sort grandie, plus écoutée. Intégrer la sécurité dans la phase build des projets
- Instaurer le « Zero Trust » au sein de votre SI [segmentation, isolation des systèmes obsolètes] mais aussi avec les partenaires
- Envisager la souscription à des services externes [SOC] et des solutions techniques plus en adéquation avec ces nouvelles attaques [EDR]

Etat de l'art & conclusion

CHEOPS TECHNOLOGY
The Cloud Customized For You !

Sources

- ANSSI : Olivier Grall - olivier.grall@ssi.gouv.fr
- DIPJ : cybermenaces-bordeaux@interieur.gouv.fr
- DGSI : securite-eco-bordeaux@interieur.gouv.fr

- https://www.ssi.gouv.fr/entreprise/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/
- https://clusif.fr/publications/livre-blanc-la-cybersecurite-a-lusage-des-dirigeants/
- https://www.ssi.gouv.fr/particulier/guide/agilite-et-securite-numeriques-methode-et-outils-a-lusage-des-equipes-projet/
- https://www.ssi.gouv.fr/entreprise/guide/organiser-un-exercice-de-gestion-de-crise-cyber/
- https://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/
- https://clusif.fr/replay/202101-panocrim/
- http://www.departement-information-medicale.com/blog/2021/02/19/jetais-tranquille-jetais-penard/

Merci de votre attention !

CHEOPS TECHNOLOGY

The Cloud Customized For You !