Orange Cyberdefense

Retour sur les conséquences de la cyberattaque du quotidien régional Ouest France.

Interview de Guy Sauvage RSSI du groupe Sipa Ouest France

Qui est Ouest France ?

Ouest France fait partie du groupe Sipa Ouest-France qui comprend plusieurs médias d'informations papier, radios, télés et numériques.
C'est le **1er quotidien francophone** au monde avec **580 000 abonnements** numériques et journal papier. Son site Internet ouest-france.fr se place parmi les premiers sites d'information avec une moyenne de 150 à 190 millions de visites mensuelles.

Ce journal, appartenant à une association à but non lucratif, défend des valeurs de démocratie humaniste, et analyse les actualités du monde entier mais aussi et surtout la vie des communes de l'ouest. Il s'emploie à informer et relier les habitants des territoires et se veut le plus transparent possible pour ses lecteurs.

«C'est la raison pour laquelle notre direction a décider d'informer nos partenaires puis nos lecteurs quand nous avons été victime d'une cyberattaque en novembre dernier, explique **Guy sauvage** Responsable de la sécurité des systèmes d'information pour le groupe ».

Contexte de la cyberattaque

Alors que les équipes de production sont en pleine impression de son quotidien, elles découvrent des messages de type « Egregor » sur leurs imprimantes.

Ces équipes, sensibilisées à ce type d'attaques, contactent immédiatement le service IT d'astreinte afin de connaître la procédure à suivre.

La décision est prise : Il faut continuer la production des titres prévus pour le samedi tant que les rotatives fonctionnent encore.
Mais l'alimentation en bobines de papier commencent à avoir des problèmes et le calage se termine manuellement ce qui engendre du retard.

« Nous avons très vite compris que nous étions face à une cyberattaque importante, explique Guy Sauvage. Notre direction consciente de son ampleur nous déclare en état de crise. ».

Orange Cyberdefense : un partenaire très réactif

« Nous avons pris l'initiative de couper tous les liens internet et les accès aux messageries et mis en place 3 cellules pour éviter que l'attaque se répande d'avantage :
Une cellule de reconstruction-reprise d''activité, de remédiation et d'investigation.
Ces cellules étaient coordonnées par une équipe spécifique afin d'assurer une bonne communication entre ces acteurs tant en interne qu'en externe».

« Face à l'étendu des dégâts nous avons déclaré l'incident à l'ANSSI et contacté notre ingénieur commercial chez Orange Cyberdefense. Nous étions en contact avec lui car nous avions le projet d'acquisition d'une solution de détection des menaces sur les EndPoints (EDR). Bien que nous ne soyons pas encore client, les équipes CSIRT d'OCD ont réagi très rapidement et sont intervenues dès l'aube pour nous aider à contenir l'attaque.

Ces équipes faisaient face à de nombreuses cyberattaques dans la région et n'avaient plus de personnel disponible pour nous aider dans la phase d'investigation. Nos interlocuteurs nous ont conseillé de prendre contact avec ON-X »,

Grâce à la mobilisation des tous nos interlocuteurs, techniques et métiers l'attaque a pu être contenu. Les experts d'Orange Cyberdefense ont déployé une solution MicroSOC EDR immédiatement en en s'alignant sur les étapes du plan de reprise de l'activité.
Cela nous a permis d'isoler les équipements infectés et d'éviter que l'attaque se propage d'avantage sur l'ensemble de nos équipements. Nous avons pu ainsi ouvrir nos liens internet dès le dimanche matin et assurer la continuité de notre activité » poursuit Monsieur Sauvage

Les leçons à en retirer !

Renforcer son niveau de sécurité !

« Cette crise nous a contraint de renforcer notre niveau de sécurité et a accéléré le déploiement de solutions qui n'étaient pas prioritaire. Je pense qu'il est désormais primordial d'avoir une solution EDR afin d'endiguer les menaces au plus tôt. La solution Micro SOC EDR Cortex proposée par Orange Cyberdefense répond pleinement à ce besoin, car elle nous a permis de détecter des attaques ces dernières semaines et donc à protéger notre activité. Elle permet de les contenir au plut tôt

S'entrainer à la gestion de crise !

Il me paraît important de s'entrainer en simulant des cyberattaque pour mieux se protéger. Plus vous êtes entrainés, mieux vous réagissez. Il ne faut pas paniquer.

Eduquer ses utilisateurs

Vous ne renforcez pas votre niveau de sécurité, si vos utilisateurs n'ont pas acquis les bons gestes d'hygiène Cyber. C'est pourquoi nous organisons régulièrement des sessions de sensibilisation afin d'informer nos utilisateurs aux cyber risques, conclut Guy sauvage »

.