DELL Technologies

# Leçons à tirer de l'attaque par ransomware

## sur l'Universitat Autònoma de Barcelona

***Gonçal Badenes***
*DSI, Universitat Autònoma de Barcelona.*
*Interview condensée et modifiée pour plus de clarté.*

**La réponse de l'université à une attaque par ransomware s'est composée d'une action rapide, de transparence et d'un engagement renouvelé en faveur de la mise à jour de leur cybersécurité.**

**Sameer Shah, Dell Technologies Cybersecurity Marketing, a parlé de l'incident avec le DSI Gonçal Badenes.**

**Sameer Shah : Nous parlions de la nécessité d'aider les organisations à améliorer progressivement leur maturité en matière de cybersécurité. Vous avez subi une cyberattaque il y a quelque temps. Avant d'aborder plus en détail l'attaque, pouvez-vous nous en dire un peu plus sur l'Université et son environnement IT ?**

**Gonçal Badenes :** L'Universitat Autònoma de Barcelona est l'une des principales universités d'Espagne. Son IT supervise tous les services nécessaires au fonctionnement de l'Université.

Avant même que l'attaque ne se produise, nous avions déjà élaboré un plan détaillé visant à améliorer notre posture de cybersécurité. Nous avions déployé l'authentification multifacteur (MFA), mais pas pour tous les services et utilisateurs. Les étudiants et tout le personnel IT avaient déjà l'authentification multifacteur, mais seulement sur la plateforme Microsoft 365. Les autres services n'étaient pas protégés. L'absence de généralisation de la MFA était importante, comme nous le verrons plus loin.

**À quel moment l'attaque s'est-elle produite et de quel type s'agissait-il ?**

Il s'agissait d'une attaque par ransomware qui s'est produite au cours d'un long week-end, comme c'est généralement le cas. Vers quatre heures du matin, j'ai reçu un appel de mon équipe disant que des services tombaient en panne comme des dominos. Ils ont lancé l'alerte et nous avons immédiatement mis en place l'équipe d'intervention que nous avions prévue pour les cas comme celui-ci.

**Comment saviez-vous qu'il s'agissait d'une attaque par ransomware ? Y avait-il une note de rançon ?**

Des notes de rançon ont été envoyées sur les systèmes concernés. Mais ils ont également mené une attaque mineure en exécutant un script pour chiffrer les ordinateurs qui étaient en ligne pendant le week-end. L'impact de cette attaque était limité, et l'objectif principal était probablement de s'assurer que le personnel et les étudiants, pas seulement l'équipe IT, étaient au courant de l'attaque.

**Votre organisation a-t-elle envisagé de payer la rançon à un quelconque moment ?**

Non.

**Pour quelle raison ?**

D'un point de vue éthique, nous ne pouvions pas le faire. Heureusement, nous avions mis en place des sauvegardes, deux copies dans deux datacenters différents sur le campus et une troisième sur bande en dehors du périmètre de l'organisation.

**Pour être clair, ces sauvegardes n'étaient pas un coffre-fort de données, n'est-ce pas ?**

Non, pas à ce moment-là, nous n'avions pas de coffre-fort. C'était prévu, mais plus loin sur notre feuille de route. Bien sûr, nous en avons depuis fait une priorité [après l'attaque].

**La communication peut être essentielle dans ces situations. Il semble que vous ayez fait face à l'attaque en communiquant de manière claire et transparente, y compris avec les médias ?**

Oui, dès le premier jour. Nous devions être parfaitement transparents et aussi ouverts que possible, en expliquant ce qui s'était passé. Nous nous sommes assurés que d'autres puissent apprendre de notre expérience et se préparer. Je pense que certains journalistes ont lu la note de rançon, puis ont pris l'initiative d'entrer en contact avec les attaquants. Nous ne l'avons de notre côté fait à aucun moment. Le groupe d'attaquants s'est identifié comme le groupe PISA (Protect Your System, Amigo).

**Souvent, les organisations préfèrent le secret pour éviter d'exposer leurs faiblesses ou leurs tactiques correctives. Était-ce une préoccupation ?**

Ce sont des préoccupations très valables. Mais je suis sûr que nous savons tous que nous sommes vulnérables. Lorsque nous essayons de sécuriser notre maison, nous savons que même si nous achetons la meilleure porte possible, si des voleurs veulent vraiment entrer, ils trouveront comment la forcer ou un autre moyen d'entrer. C'est exactement la même chose.

Il n'y a pas de honte à se faire attaquer et avoir des vulnérabilités. Nous avions une feuille de route de protection très claire et nous avons quand même été touchés. C'est important de le dire. Même si nous disposions d'une très bonne protection, nous avions malgré tout des failles de sécurité qui pouvaient être attaquées. En mettant en œuvre des étapes supplémentaires, vous pouvez énormément renforcer votre position.

**Dites-nous ce que vous avez fait immédiatement pour commencer à résoudre le problème.**

Nous avons arrêté le réseau, tous les systèmes. Nous avons contacté la police et l'agence régionale de protection des données, ce qui est légalement obligatoire de faire. Et nous avons immédiatement constitué deux équipes : une d'investigation et une de récupération. Nous avons appelé Dell, qui a immédiatement escaladé l'incident comme priorité absolue, et une équipe vraiment incroyable s'est mise au travail non-stop. Elle a réussi à restaurer complètement toutes les données sur le deuxième domaine de données.

**L'investigation a donc commencé pendant le processus de récupération ?**

Pour certains processus de récupération, nous avons dû attendre un peu. L'investigation a donc commencé en premier. Tout a été mis en quarantaine parce que vous devez comprendre ce qui s'est passé. Nous avons dû mettre en place un autre système pour pouvoir remettre les choses en service. Nous avons décidé que, même si cela prenait un peu plus de temps, tous les systèmes qui seraient mis en ligne devraient répondre aux normes de sécurité les plus strictes.

**« Je pense que le plus important est qu'il y a une forte probabilité de subir une cyberattaque tôt ou tard, il est donc important de mettre en place un plan détaillé d'atténuation et de récupération. »**

**La MFA était uniquement mise en place sur Microsoft 365, ce qui a contribuer à permettre l'attaque. La MFA est-elle désormais en place à tous les niveaux ?**

Le vecteur d'attaque était un utilisateur avec des identifiants compromis qui faisait partie d'une équipe ayant déjà l'authentification multifacteur sur Microsoft. Mais lorsque l'attaquant a essayé d'accéder à l'e-mail et s'est rendu compte qu'il ne pouvait pas du fait de la MFA, il a poursuivi sa recherche. Et ils ont découvert que nous avions un VPN, qui n'était pas protégé par la MFA. Une fois qu'ils ont accédé au réseau via VPN, ils ont pu commencer à le surveiller.

Dans un réseau très vaste comme le nôtre, ils ont trouvé un système qui avait une vulnérabilité et ont commencé à effectuer des mouvements latéraux. Une fois que nous avons commencé à récupérer les systèmes, nous avons décidé que rien ne serait mis en ligne sans protection MFA.

**Si vous aviez UNE recommandation ou un conseil pour éviter à vos pairs une attaque par ransomware, que serait-ce ?**

Il est très difficile de donner un seul conseil, mais je pense que le plus important est qu'il y a une forte probabilité de subir une cyberattaque tôt ou tard, il est donc important de mettre en place un plan détaillé d'atténuation et de récupération.

Par exemple, il est très important d'avoir à portée de main les contacts des partenaires clés en matière d'investigation et de récupération, d'avoir une carte détaillée et hiérarchisée des services avec un calendrier de récupération et une stratégie bien alignée avec les divisions opérationnelles clés, y compris la communication (interne et externe). Et, bien sûr, il est très important de garder les utilisateurs vigilants et de les informer sur les techniques utilisées par les pirates.

**Avez-vous le sentiment que le renforcement des capacités de cybersécurité de l'Université a renforcé la confiance dans la poursuite de votre mission et de toutes vos grandes réalisations ?**

Absolument. Avant l'attaque, nous avions l'impression que toutes les nouvelles mesures visant à protéger le système entraînaient de nombreuses questions, notamment sur leur réelle nécessité. La protection est absolument nécessaire, car sinon vous mettez toute votre entreprise en danger. Il y a bien sûr toujours certaines personnes qui pensent que ces mesures entravent leur travail. Mais la plupart estiment que les systèmes sont bien mieux protégés.

**Merci. Votre honnêteté et votre clarté sont utiles pour tout ceux qui travaillent à améliorer la maturité de leur cybersécurité.**