DELL Technologies

Lecciones aprendidas de un ataque de ransomware

en la Universitat Autònoma de Barcelona

Gonçal Badenes
Director de TI de la Universitat Autònoma de Barcelona.
Entrevista resumida y editada para facilitar la claridad.

La actuación rápida, la transparencia y un compromiso renovado con la actualización de la ciberseguridad definieron la respuesta de la universidad ante un ataque de ransomware.

Sameer Shah, director de marketing y ciberseguridad de Dell Technologies, habló con el director de TI Gonçal Badenes sobre el incidente.

Shah: Hemos hablado de la necesidad de ayudar a las organizaciones a mejorar gradualmente su madurez en ciberseguridad. Ustedes sufrieron un ciberataque hace algún tiempo. Antes de entrar en más detalles sobre el ataque, ¿puede hablarnos sobre la Universidad y su entorno de TI?

Badenes: La Universitat Autònoma de Barcelona es una de las universidades líderes en España. El departamento de TI supervisa todos los servicios necesarios para el funcionamiento de la universidad.

Justo antes del ataque, teníamos un plan completo para mejorar nuestro estado en cuanto a la ciberseguridad. Habíamos implementado la autenticación multifactor (MFA), pero no en todos los servicios y usuarios. Los alumnos y todo el personal de TI ya tenían MFA, pero solo en la plataforma Microsoft 365. Otros servicios no estaban protegidos. La falta de una MFA universal fue importante, como veremos más adelante.

¿Cuándo ocurrió el ataque y de qué tipo fue?

Fue un ataque de ransomware que sucedió durante un puente, como suele ocurrir. Alrededor de las cuatro de la mañana, recibí una llamada de mi equipo diciendo que los servicios estaban cayendo como fichas de dominó. Dieron la voz de alarma e inmediatamente reunimos al equipo de respuesta que habíamos previsto para estos casos.

¿Cómo supo que se trataba de un ataque de ransomware? ¿Había una nota de rescate?

Había notas de rescate en los sistemas afectados. Pero también llevaron a cabo un ataque menor ejecutando una secuencia de comandos para cifrar los ordenadores que estaban en línea durante el fin de semana. El impacto de esto fue limitado y el objetivo principal probablemente era asegurarse de que el personal y los alumnos se enteraran del ataque, no solo el equipo de TI.

¿Su organización se planteó en algún momento pagar el rescate?

No.

¿Por qué no?

No podíamos hacerlo desde un punto de vista ético. Afortunadamente, teníamos copias de seguridad: dos copias en dos centros de datos diferentes en el campus y una tercera en cinta fuera del perímetro de la organización.

Y para que quede claro, estas copias de seguridad no eran un almacén de datos, ¿verdad?

No, en ese momento no. No teníamos un almacén. Era una prioridad futura en la hoja de ruta. Pero luego, por supuesto, le dimos prioridad [tras el ataque].

Las comunicaciones pueden ser críticas en estas situaciones. Parece que se enfrentó al ataque comunicándose de forma clara y transparente, incluso con los medios de comunicación, ¿no es así?

Sí, desde el primer día. Teníamos que ser perfectamente transparentes y lo más abiertos posible, explicando lo que había sucedido. Nos aseguramos de que otras personas pudieran prepararse y aprender de nuestra experiencia. Supongo que parte de la prensa leyó la nota de rescate y se puso en contacto con los atacantes porque nosotros nunca lo hicimos. El grupo de atacantes se identificó como el grupo PISA (Protect Your System, Amigo).

Muchas veces las organizaciones prefieren el secretismo para evitar exponer sus puntos débiles o sus tácticas de corrección. ¿Eso les preocupaba?

Son preocupaciones muy válidas, pero estoy seguro de que todos sabemos que somos vulnerables. Cuando tratamos de proteger nuestra casa, sabemos que incluso si compramos la mejor puerta posible, si los ladrones realmente quieren entrar, encontrarán la manera de romperla o encontrarán otra forma de entrar. Esto es exactamente lo mismo.

No nos avergüenza el hecho de que haber sido atacados ni de que tuviéramos vulnerabilidades. Es importante compartir con la gente el hecho de que teníamos una hoja de ruta muy clara para la protección y, a pesar de eso, nos atacaron. Aunque tuviéramos una protección muy buena, seguíamos teniendo vulnerabilidades que podían ser atacadas. Al implementar pasos adicionales, tu posición puede ser mucho más fuerte.

Cuéntenos qué hizo inmediatamente para empezar a solucionar el problema.

Desconectamos la red, todos los sistemas. Nos pusimos en contacto con la policía y la agencia regional de protección de datos, que son cosas que tenemos que hacer legalmente. Inmediatamente pusimos en marcha dos equipos: el forense y el de recuperación. Llamamos a Dell y el asunto se elevó inmediatamente a la máxima prioridad, y tenemos un equipo increíble trabajando en ello sin parar. Lograron recuperar completamente todos los datos en el segundo Data Domain.

Entonces, ¿los análisis forenses comenzaron durante el proceso de recuperación?

Para algunos de los procesos de recuperación, tuvimos que esperar un poco. Por eso digo que los forenses empezaron primero. Todo se puso en cuarentena porque tienes que entender que ha pasado. Tuvimos que configurar otro sistema para poder empezar a restaurarlo todo. Decidimos que, aunque tardáramos un poco más, todos los sistemas que se conectaran tendrían que estar a la altura de los mejores estándares de seguridad.

"Creo que lo más importante a tener en cuenta es que existe una gran probabilidad de que tarde o temprano todos suframos un ciberataque y, por lo tanto, debemos tener un plan detallado de mitigación y recuperación".

Ha mencionado que la MFA solo estaba en Microsoft 365, lo que, en parte, permitió el ataque. Entonces, ¿disponen ahora de MFA en todos los ámbitos?

El vector de ataque era un usuario con credenciales comprometidas que estaba en un equipo que ya tenía MFA en Microsoft, pero cuando el atacante intentó acceder al correo electrónico y vio que no podía acceder a él debido a la MFA, siguió buscando. Y descubrieron que teníamos una VPN, que no estaba protegida por MFA. Una vez que obtuvieron acceso a través de VPN, pudieron comenzar a inspeccionar la red.

En una red tan grande como la nuestra, encontraron un sistema que tenía una vulnerabilidad y comenzaron a realizar movimientos laterales. Una vez que empezamos a recuperar los sistemas, decidimos que no se conectaría nada hasta que estuviera protegido con MFA.

Si le diera a sus compañeros UNA recomendación o consejo fundamental para evitar un ataque de ransomware, ¿cuál sería?

Es muy difícil dar un solo consejo, pero creo que lo más importante a tener en cuenta es que existe una gran probabilidad de que tarde o temprano todos suframos un ciberataque y, por lo tanto, necesitamos tener un plan detallado de mitigación y recuperación.

Por ejemplo, es muy importante tener a mano los contactos de socios clave en análisis forense y recuperación, para tener un mapa detallado y priorizado de los servicios con un cronograma para la recuperación y una estrategia bien alineada con las unidades de negocio clave, incluida la comunicación (tanto interna como externa). Y, por supuesto, es muy importante mantener a los usuarios alerta y formados sobre las técnicas utilizadas por los atacantes.

¿Cree que el refuerzo de la capacidad de ciberseguridad en la universidad ha aumentado la confianza para continuar con la misión y realizar su gran labor?

Sin duda. Antes del ataque, una de las percepciones era que cualquier nueva medida para proteger el sistema era recibida con muchas preguntas y preocupaciones sobre si realmente la necesitábamos. El hecho es que la protección es absolutamente necesaria, porque de lo contrario pones en peligro toda tu empresa. Y, por supuesto, algunas personas todavía creen que estas medidas obstaculizan su trabajo. No obstante, la mayoría cree que los sistemas están mucho mejor protegidos.

Gracias. Su franqueza y transparencia son beneficiosos para todos los que trabajan para avanzar en la madurez de su ciberseguridad.