vReferencia: Premios Socinfo Digital. Categoría Seguridad
Fecha: 10 de marzo de 2022

Respuesta a un cibertaque en la UCLM

La noche del domingo 18 de abril de 2021 en la UCLM confirmamos que estábamos siendo objeto de un ciberataque. La alarma desencadenada cuando el sitio web de la institución dejó de estar operativo fue el inicio de un frenético proyecto de respuesta al mayor ciberataque sufrido por una universidad pública hasta esa fecha.

Con las infraestructuras críticas de la arquitectura tecnológica de la universidad completamente inoperativas, objeto de un ataque *ransomware*, la institución, a través de la coordinación del Área de Tecnología y Comunicaciones de la universidad, pero con el apoyo de toda la institución y su comunidad universitaria, desarrollaron un proyecto de respuesta que permitió el regreso a la actividad de los servicios digitales de mayor impacto como Campus Virtual en menos de 4 días, tras haber realizado una reconstrucción de las infraestructuras críticas, un rediseño de la red de comunicaciones y, al mismo tiempo, incrementando los niveles de ciberseguridad.

Antecedentes

Nunca en la historia de la UCLM se había sido objeto de un ciberataque. La situación de partida en materia de ciberseguridad en la institución hasta ese momento estaba basada en las recomendaciones y buenas prácticas aplicadas de manera equilibrada en función de los recursos disponibles en este tipo de instituciones. Una política de seguridad aprobada, infraestructuras de seguridad perimetral desplegadas, una política de credenciales exigente, una gestión de activos soportada en cloud y un despliegue progresivo en entornos cloud iniciado hace años eran los puntos de partida con los que se enfrentó la institución a un reto de calibre equivalente al sufrido el año anterior con el inicio de la pandemia y el confinamiento.

Retos

El reto fue de dimensiones antes no abordadas y con impacto multidimensional que se identificó desde el principio.

Reto 1. Regreso a la normalidad. El objetivo estaba claro desde el primer momento: era necesario recuperar los servicios digitales en el menor tiempo posible para facilitar la continuidad de la actividad docente, investigadora y de gestión universitaria.

Reto 2. Nueva normalidad. Si bien la necesidad de recuperar servicios era acuciante, también lo era recuperarlos con niveles de seguridad superiores, que permitiesen evitar una "segunda oleada" de ataques.

Reto 3. Disminución de la superficie de exposición. La nueva normalidad debería basarse en una reducción de la superficie de exposición, externa e interna. Eso implicaba rediseñar la red de comunicaciones, incrementar la granularidad en permisos, mejorar la capacidad de anaálisis y respuesta en dispositivos de usuario y fortalecer la gestión de credenciales.

Reto 4. Comunicación. Desde la noche del ciberataque se tuvo en cuenta la necesidad de informar a la comunidad universitaria de lo que estaba ocurriendo, aportando transparencia al proceso de recuperación.

Fases

1. **Detección**. Realizada a través de los servicios de monitorización 24x7 disponibles en la UCLM. La monitorización continua de la disponibilidad de servicios e infraestructuras críticas en la universidad permitió la detección del incidente durante la noche de un fin de semana, lo que permitió adelantar el inicio de las labores de respuesta
2. **Análisis de situación** en caliente. La detección de indisponibilidad permitió desencadenar los protocolos de análisis que concluyeron en cuestión de minutos que se estaba siendo víctima de un ciberataque.
3. **Contención**. Para evitar la actuación en remoto de los atacantes se procedió a la desconexión de Internet de todas las infraestructuras y servicios digitales de la UCLM. Del mismo modo, para evitar una propagación interna del cifrado se procede al apagado controlado de equipos en el CPD universitario, realizado por in-situ al haberse procedido a la desconexión desde el exterior, por personal técnico funcionario de la UCLM.
4. **Planificación de recuperación**. Supuso, de forma coordinada con el equipo de Gobierno de la universidad, el establecimiento del plan para la recuperación, donde se contó con apoyo externo especializado desde la misma mañana posterior al incidente, asumiendo por parte de la universidad que no se disponían de los medios y el conocimiento especializado suficientes para dar una respuesta eficiente. No obstante, ese apoyo se prestaría en colaboración con un equipo de primera respuesta configurado por personal técnico funcionario especializado en la gestión de las infraestructuras TIC universitarias.
5. **Contratación**. Habiéndose identificado claramente la necesidad de establecer una respuesta basada en la colaboración público-privad, e evaluó la situación desde los servicios jurídicos, que validaron el inicio de un expediente mediante procedimiento de contratación por emergencia ese mismo lunes por la mañana.
6. **Diseño del plan de acción técnico**. Realizado junto a Telefónica Tech, proveedor que respondió de manera proactiva a la situación y con quien se estableció la contratación mediante procedimiento de emergencia. El plan se diseña apra ser ejecutado de forma conjunta con el equipo de respuesta de funcionarios de la UCLM.
7. **Diseño del plan de Comunicación**. Basado en el principio de transparencia, comunicación interna y externa, se materializa en una información diaria redactada por el Gabinete de Comunicación de la universidad en coordinación con la dirección del área TIC de la UCLM. Este plan se comienza a ejecutar desde el día siguiente a la detección del incidente.
8. **Recuperación de infraestructuras críticas**. Habiendo realizado el balance de daños provocados por el cifrado, se establece un proceso de recuperación que requiere de la recuperación inicial de las infraestructuras tecnológicas básicas con un incremento en

el nivel de seguridad, lo que requiere de un rediseño en infraestructuras tan críticas como la red de comunicaciones o los sistemas de autenticación de usuarios. Esta recuperación se realiza en menos de 72h desde la detección del incidente.

9. **Recuperación de los servicios digitales.** El restablecimiento de la conectividad y de las infraestructuras básicas facilita el complejo proceso de recuperación de servicios. Con el alcance tan extensivo del cifrado sufrido, se hace necesaria una priorización para el proceso de restablecimiento. Esta priorización, dado que el alcance de elementos dañados no es homogéneo en todos los servicios, se realiza a las variables de criticidad o impacto y esfuerzo necesario para la recuperación.
10. **Nueva normalidad**. El restablecimiento de servicios no llega acompañado de una situación idéntica a la anterior al incidente. La necesidad de incrementar los niveles de ciberseguridad implica el despliegue de nuevos servicios que inciden no solo en el uso de las redes de comunicaciones en la unviersidad, sino también en la gestión de identidades, la gestión de dispositivos de usuario

Nuevos Servicios

La respuesta al ciberataque desencadenó el desarrollo de proyectos en materia de ciberseguridad ya, en gran parte, estaban diseñados previamente y sobre los que se planteaba un despliegue progresivo habida cuenta del impacto de algunos de ellos en la experiencia de usuario. En general, las mejoras en seguridad y, por tanto, en eficiencia, aportadas por estos servicios han estado vinculadas a la reducción de la superficie de exposición.

1. **Infraestructuras**. El nuevo diseño de la red de comunicaciones, desarrollado en las primeras horas de respuesta al ciberataque, plantea una estricta segmentación externa e interna basada en el criterio Zero Trust. Si bien esa segmentación ya existía en la red previamente, el criterio de confianza cero se establece con un nivel de detalle exhaustivo.
2. **Dispositivos**. La colaboración en el incidente de Microsoft España, así como el alto nivel de adopción de modelos de gestión de dispositivos UCLM en modo cloud , facilitó el en 48h de ampliar 2.000 licencias de antivirus con capacidad EDR en todos los equipos del personal de la UCLM
3. **Identidades**. Identificando la identidad digital como uno de los vectores inicales de ataque más utilizados, se acelera el proyecto existente para el despliegue de doble factor de autenticación en todas las cuentas de usuarios de la UCLM. Este despliegue se realiza en las primeras 72h de trabajo en la respuesta, estableciendo un cambio de contraseña y el uso del doble factor de autenticación como requisito para acceder a cualquiera de los servicios que se restablecieron progresivametne.
4. **Aplicaciones**. El proceso de respuesta supuso también la aceleración de migración de aplicaciones de desarrollo propio a entornos *cloud* nativos. Habiendo identificado que esta migración había implicado un mayor nivel de resiliencia en aplicaciones desplegadas en cloud bajo modalidad no IaaS, no alcanzables mediate los ataques ransomware con objetivo infraestructuras basadas en la existencia de servidores, se han impulsado definitivamente la refactorización de aplicaciones maximizando las capacidades y componentes cloud.

Conclusiones

Si bien la experiencia a lo largo de esa primera semana y las que vinieron después fue de una intensidad y un impacto muy alto para la actividad universitaria, la transparencia en la comunicación y la rápida recuperación progresiva de servicios han generado una situación de mejora en la cultura de ciberseguridad en la institución, facilitando el despliegue de medidas técnicas que han incrementado el nivel de seguridad en la institución. Este proceso ha cambiado la concepción estratégica de la ciberseguridad, evolucionando la visión de la necesidad de abordar la seguridad de manera preventiva para complementarla como un entorno al que enfrentarse necesariamente bajo la visión de la respuesta y recuperación. Ante la certidumbre de ser atacados es necesario adoptar medidas de prevención, pero también disponer de un plan de recuperación adecuado a esta nueva normalidad.

Se aporta como anexo, un artículo publicado en la revista Bit que describe en primera personal las primeras horas del ciberataque: https://bit.coit.es/hola-me-llamo-andres-me-van-a-ciberatacar/