INFORME JUSTIFICATIVO DE LA CONTRATACIÓN POR EMERGENCIA DEL CONTRATO MIXTO DE SERVICIO DE CONSULTORÍA PARA HACER FRENTE AL CIBERATAQUE SUFRIDO POR EL AJUNTAMENT DE CALVIÀ EN FECHA 13 DE ENERO DE 2.024 Y DE SUMINISTRO DE LICENCIAS DE USO DE DIFERENTES SOLUCIONES DE SOFTWARE.

En la madrugada del pasado 13 de enero de 2024 el Ajuntament de Calvià fue víctima de un ciberataque que afectó a la disponibilidad de los sistemas.

En concreto, a las 3 a.m de dicho día, se produjo una elevación de la actividad de los servidores, detectando a las 8 a.m por parte de los servicios de la Policía Local un funcionamiento anómalo de los sistemas de información poniendo los hechos en conocimiento de los servicios de informática del Ajuntament que procedieron a la desconexión de los servidores y backups, así como de la red de internet. También se revisaron los equipos (PCs) cerrando y desconectando de las red eléctrica los que estaban en funcionamiento.

Inicialmente se detectó que era un ciberataque provocado mediante ransomware que encriptó parte de los servidores. En concreto resultaron encriptados cinco servidores y diez ordenadores personales. Asimismo se detectaron más ordenadores que contenían el fichero sin haberse ejecutado.

Esta situación provocó la interrupción de la prestación de los servicios públicos municipales por cuanto se bloquearon los servidores en los que se aloja la información municipal, se aisló el sistema (bloqueando su acceso a internet) y la imposibilidad de poner en marcha los ordenadores personales por cuanto podían suponer riesgos a la seguridad del sistema.

Entre los servicios afectados se encontraban algunos de carácter esencial para la población y para garantizar la seguridad pública como son Servicios Sociales o Policía Local y Protección Civil.

Asimismo provocó la suspensión del funcionamiento de la página web municipal, nuestra sede electrónica, las bases de datos de los servicios y los registros de entrada y de salida. También provocó problemas de comunicación por cuanto parte de las líneas de teléfono municipales van por internet.

Para poder reiniciar el sistema y poder prestar servicios esenciales para la Comunidad del modo más inmediato posible fue necesario la realización de una serie de actuaciones de emergencia.

Con el objetivo de restablecer los sistemas y la red corporativos y de dotarlos de un mayor nivel de seguridad, se tuvieron que llevar a cabo determinadas actuaciones, algunas de las cuales requirieron la adquisición de dispositivos y/o servicios de empresas externas.

En primer lugar se tuvo que realizar el diagnóstico de los daños provocados al sistema. Este diagnóstico permitió adoptar a continuación las medidas necesarias para afrontar la situación.

A continuación, se tuvo que realizar -y de forma inmediata- la restauración de todo el sistema de forma segura. En este sentido, se debían configurar nuevamente todos los sistemas dotados de un nivel mayor de seguridad para evitar un nuevo ataque y solventar los problemas detectados como consecuencia de este. Estas medidas se tuvieron que adoptar especialmente en aquellos servicios y sistemas que están en contacto con internet.

[redacted]
FRANCISCO JAVIER MIR JAUME
22/05/2024

[redacted]
MARIA DEL CARMEN OLIVER PAYAROLS
22/05/2024

Para poder garantizar dicha seguridad en la red se tuvieron que incorporar unas herramientas de monitorización al sistema (para detectar con mayor antelación las brechas). Se activaron nuevos módulos (Threat Intelligence, Threat Hunting y Machine Learning) a la herramienta MONSE que el Ajuntament ya tenía contratada con la empresa. Cabe destacar que esta solución forma parte del CCN-STIC 105 (CPSTIC) en la familia de Sistemas de gestión de eventos de seguridad, como Producto Cualificado, verificando los requisitos de seguridad exigidos para el manejo de información sensible en el ENS en categoría ALTA. El Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) tiene como finalidad ofrecer a los organismos de la Administración un conjunto de productos o servicios STIC de referencia cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas.

Ante un incidente de la envergadura del sufrido en el Ajuntament de Calvià, desde los primeros minutos se requiere de servicios especializados de un Equipo de Respuesta Inmediata ante Emergencias Informáticos (CSIRT). En este caso se optó por encomendar estas funciones a la empresa que lleva prestando los servicios de asesoramiento en materia de protección de datos y seguridad de la información, así como adecuación al Esquema Nacional de Seguridad desde hace más de una década.

Al tener esta empresa sólidos conocimientos sobre la infraestructura de seguridad del Ajuntament, estar dentro del objeto del contrato con el que prestan sus servicios al Ajuntament el asesoramiento en materia de ciberseguridad y ofrecer dentro de su portfolio de servicios precisamente servicios de CSIRT, se estimó que era la empresa que estaba en condiciones de poder colaborar con los servicios municipales en las fases de contención, análisis forense, comunicación y colaboración con las autoridades competentes, recuperación, formación y propuestas de mejora en estos momentos tan complicados.

A mayor abundamiento, se debe señalar que son servicios que se necesitaban de modo inmediato y la decisión se tuvo que adoptar un sábado a primera hora de la mañana, momento en que es difícil realizar una consulta al mercado (más careciendo de acceso a los sistemas de información municipal).

Además de los servicios de coordinación del incidente (CSIRT), también se ocuparon de las actuaciones legales con autoridadesd de control. Se evidenció la gestión diligente del incidente de seguridad con las autoridades de control en materia de protección de datos (AEPD), Centro Criptológico Nacional (CCN) y Fuerzas y Cuerpos de Seguridad del Estado. Se llevó a cabo el desarrollo del informe de brecha, análisis forense y denuncia con FFCCSS, así como asistencia en comunicados externos.

Fruto de estos servicios se pudieron identificar puntos que suponían un grave riesgo en términos de seguridad, por lo que se sugirieron una serie de herramientas y soluciones para incrementar el nivel de seguridad tanto a nivel de microinformática, como de servidores y de red. La implantación de estas medidas era imprescindible para el restablecimiento de la operatividad de la infraestructura informática municipal con garantías.

En el caso de licenciamiento de soluciones software, se adquirieron subscripciones de 12 meses, con el objetivo de cubrir el servicio y de que el Ajuntament publique un procedimiento de contratación para cubrir estas necesidades a largo plazo. Estas licencias eran necesarias para poder restablecer los sistemas de modo seguro y serán objeto de licitación para los años sucesivos en que se tengan que mantener.

Se tuvieron que implantar nuevos programas de antivirus. El Ajuntament hasta la fecha hacía uso de un antivirus basado en firmas (EPP), tecnología que se ha demostrado obsoleta a día de hoy. Por ello se ha implantado una solución MDR. La detección y respuesta administradas (MDR) es un servicio gestionado 24x7, que incluye monitorización, detección y respuesta a amenazas. El objetivo de MDR es ayudar en la respuesta a incidentes (IR). El servicio incluye tecnologías automatizadas que se pueden implementar tanto en la capa de red como en la de host. MDR emplea inteligencia de amenazas y análisis avanzados en combinación con expertos en investigación y respuesta a incidentes derivados del riesgo humano. En concreto, se han adquirido 650 licencias de uso de la solución CYNET.

También se adquirieron licencias de Tenable IO para poder controlar la superficie de exposición mediante una auditoría continua. Se trata de una solución de gestión de vulnerabilidades local que proporciona visibilidad de su superficie de ataque para gestionar y medir el ciberriesgo. A través de análisis avanzados, paneles/informes personalizables y flujos de trabajo permite identificar los puntos débiles en los activos conectados a la red, identificando todas las vulnerabilidades, las configuraciones erróneas y el malware en ellos. Esta solución proporciona una cobertura de vulnerabilidades completa, con evaluación continua y en tiempo real de la red y sus activos, permitiendo identificar, investigar y priorizar las vulnerabilidades existentes. La solución ofrece diversos paneles de seguridad, con múltiples indicadores que permitirán realizar un seguimiento del nivel de riesgo existente en la organización, sus elementos más vulnerables, cómo estos se van solucionando y, en consecuencia, el nivel de riesgo se va rebajando.

Adicionalmente, también se cubre la protección del Directorio Activo con Tenable AD, que es una solución de protección del dominio que permita la gestión de los mecanismos de defensa (prevención, detección y reacción) ante ataques dirigidos o que puedan afectar al Directorio Activo. La solución permite la identificación y evaluación de las principales vulnerabilidades inherentes a la versión del software de directorio activo o a la configuración de este, genera recomendaciones destinadas a eliminar o reducir vulnerabilidades a través de la modificación de los parámetros de configuración del directorio activo, permite la protección del directorio activo frente ataques como escalado de privilegios, suplantación de identidad, fuerza bruta, DCShadow, Password Spraying y DCSync entre otras y recopila evidencias que puedan servir de base para un análisis forense tras la materialización de una amenaza que haya impactado contra el directorio activo.

También se evidenció la necesidad de proteger la navegación complementando la protección existente en firewalls perimetrales y proteger los equipos en movilidad mediante la solución de Cisco Umbrella. Esta solución permitirá aumentar las capacidades de protección de la navegación de los usuarios, tanto si están en la red corporativa como si se encuentran en una red externa, asegurando en todo momento que no se realicen conexiones a sitios web malintencionados o se utilicen aplicaciones de riesgo.

Entre los servicios contratados también se incluyeron unas jornadas formativas con el objetivo de comunicar la situación sucedida en relación con el incidente, así como unos servicios asistencia en la recuperación de la cabina de almacenamiento.

La tramitación de emergencia del presente expediente ha sido absolutamente necesaria para remediar los efectos de los perjuicios provocados por el ciberataque. Al estar completamente paralizada la actuación de la Administración se tuvo que acudir a dicho procedimiento por cuanto los restantes procedimientos de contratación no permitían dar la respuesta inmediata que se necesitaba.

Hay que señalar, asimismo, que las actuaciones se han ceñido exclusivamente a la contratación de los servicios indispensables para satisfacer la necesidad sobrevenida objeto de la presente actuación.

Las medidas y protocolos que se han adoptado para hacer frente a la restauración de los sistemas y el reforzamiento de las medidas de seguridad de los mismos son las establecidas por el Centro Criptológico Nacional tanto para prevención como de reacción frente a un ciberataque.

El presupuesto base de licitación asciende a 152.081,36 (IVA incluido), que se desglosa en los siguientes conceptos:

Tenable AD: 43.923 €

Solución MDR CYNET: 42.842,56 €

Tenable IO: 18.125,80 €

Cisco Umbrella: 12.342 €

Servicios: 34.848 €

Lo que se informa a los efectos oportunos.

Calvià, a

Jefe de Servicio de Informática e Innovación
Fdo.: Francisco Javier Mir Jaume

VºBº
Directora Gral de Servicios Generales
Carmen Oliver Payarols