Oney: respuesta y gestión de ciberincidentes en el sector de medios de pago y financiación

En un proceso de mejora continua de la ciberseguridad resulta imprescindible contar con una buena capacidad de respuesta a incidentes que esté preparada ante cualquier amenaza que ponga en riesgo el negocio y que permita una recuperación rápida del mismo. Una capacidad en la que se conjugue inteligencia, automatización, intercambio de conocimiento y detección de ataques avanzados. Para ello, Oney ha buscado como socio estratégico y especialista en esta área a InnoTec, empresa de ciberseguridad del Grupo Entely.

Javier Allende Astigarraga / Myriam Sánchez González

Oney es una empresa 100% filial del grupo **Auchan**, especialista en medios de pago y financiación, con presencia en 11 países y con más de 8 millones de clientes, de los cuales casi un 13% están en España.

Numerosas empresas como Alcampo, Leroy Merlin, Decathlon, AKI, Simply, ToysRus, Norauto, Verdecora o Midas confían en Oney para la gestión de sus soluciones de pago e impulsar el poder de compra de sus clientes. Tarjetas, préstamos y seguros de todo tipo son los tres ejes que vertebran las soluciones de esta compañía. Unos servicios que, por la criticidad de la información almacenada, son un claro objetivo de los ciberdelincuentes (máxime, teniendo en cuenta que, en su inmensa mayoría, son en línea).

Así pues, para Oney la calidad del servicio y las relaciones a largo plazo con sus clientes son premisas fundamentales en su estrategia. Ambos aspectos están vinculados directamente con una política de seguridad que proteja su modelo de negocio y a sus clientes de una manera proactiva, estableciendo planes directores de seguridad y realizando un proceso de mejora continua. Ello le ha llevado a mejorar su capacidad de respuesta a incidentes de seguridad a través de **InnoTec** (**Grupo Entelgy**) como socio estratégico y especialista en esta área. Una labor de detección, respuesta y recuperación que InnoTec lleva a cabo desde su *SmartSOC,* donde un equipo multidisciplinar trabaja 24x7 con los mejores métodos y herramientas del sector.

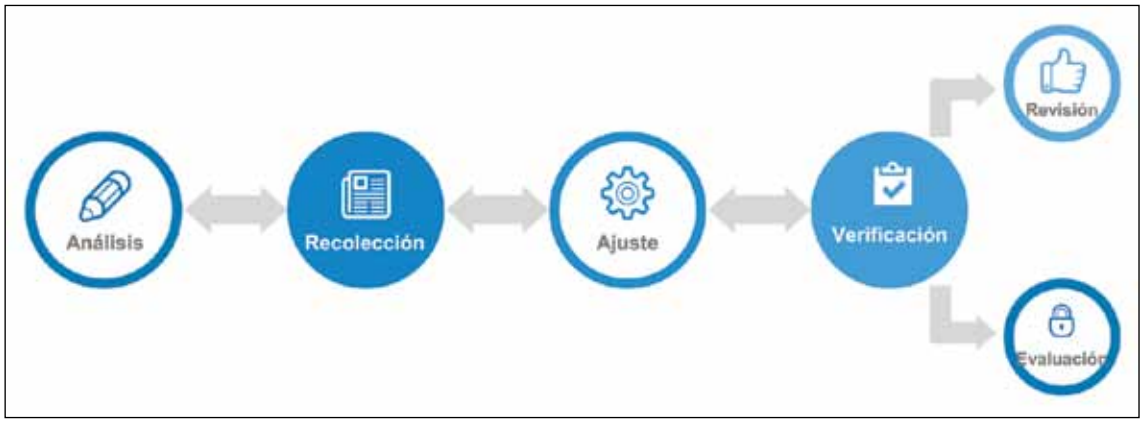

Figura 1.- Proceso de Integración de fuentes de datos.

El objetivo perseguido por Oney para complementar su estrategia de ciberseguridad con un servicio especializado, le ha permitido incrementar su capacidad de respuesta ante incidentes de una manera eficaz, mejorando su visibilidad y conocimiento propio, y adecuar su respuesta ante los riesgos a los que está expuesta por la naturaleza de su actividad.

Primeros pasos

Para comenzar a realizar este servicio era necesario tener una visión completa y rápida de la infraestructura de Oney. Para ello se enviaron las diferentes fuentes de datos hacia el*SmartSOC* de InnoTec en Madrid. Allí se realizó una valoración de los *logs* recogidos para validar los datos obtenidos siguiendo el siguiente proceso:

En este proceso se realiza un análisis completo de la información recogida en el sistema, con el fin de evaluar de un modo efectivo cada uno de los eventos. De este modo, no sólo se integra y se almacena la información, sino que se analizan los eventos de un modo individual (el evento en sí mismo) y de forma colectiva (correlándolo con otros eventos).

En ese sentido es importante tener en cuenta que desde el *SmartSOC* de InnoTec se integran principalmente dos tipos de correlación para la detección de amenazas que pueda poner en riesgo a una organización:

• ***Orientada a las amenazas***. Se correlacionan alertas sobre amenazas conocidas y se actualizan continuamente con la información recogida por los analistas y servicios de inteligencia. Desde el Centro Avanzado de Operaciones de Ciberseguridad de la compañía se recoge información de distintas fuentes (*feeds* de Threat Intel.) propias y de terceros, relacionada con riesgos y amenazas. Estas amenazas se clasifican y, llegado el caso, se transforman en alertas de seguridad para detectar de forma proactiva los riesgos a los que puede estar expuesta la organización. Hay que tener en cuenta que InnoTec es miembro y colaborador de las principales organizaciones y centros de excelencia nacional e internacional donde se comparte este tipo de información (FIRST, TF-CSIRT, CSIRT.es, etc.).

• ***Orientados al negocio de Oney***. Todas los métodos y herramientas empleadas por InnoTec se adecúan a las necesidades de cada cliente; en este caso con Oney se acuerda una serie de casuísticas orientadas a la protección y detección de riesgos en su negocio. Esta labor es fundamental para poder priorizar determinadas alertas y proteger de un modo más eficaz al negocio.

Sobrecarga de datos versus Inteligencia

La aproximación que Oney está llevando a cabo con respecto a la capacidad en la respuesta a incidentes de seguridad se basa fundamentalmente en priorizar dos aspectos:

• Dedicación de los recursos y esfuerzos de la organización a la resolución de los incidentes que tengan un mayor impacto.

• Descripción y realización de las acciones que tienen que llevarse a cabo de manera eficiente en cada caso concreto.

Los servicios de monitorización y gestión de incidentes se enfrentan cada día a una vorágine de datos e información que es preciso transformar en inteligencia para, de este modo, definir y clasificar los incidentes de ciberseguridad que suponen un riesgo real en cada una de las organizaciones. Cada día aparecen nuevas amenazas que deben analizarse y traducirse en una serie de pautas concretas para protegerse frente a todas ellas.

En este proceso de *separación del grano de la paja* es preciso establecer una estrategia eficiente y de rápida respuesta, para lo cual resulta imprescindible, aparte del papel del analista, el desarrollo de ciertos automatismos comunes a ciertas tipologías de incidentes.

Esta estrategia, denominada "***Security Orchestration***", permite definir los puntos clave a la hora de gestionar un incidente, clasificando las acciones según la tipología y la criticidad del mismo (una peligrosidad muy relacionada con la casuística particular de cada cliente) y automatizando las primeras acciones en la investigación de cada uno de ellos.

La orquestación consiste en una primera instancia, en realizar acciones que son necesarias para la investigación del contexto relacionado con el incidente que se está analizando de manera automática. De este modo, la información obtenida se ve enriquecida con la que ya existe de la propia tecnología que tiene desplegada la organización.

Como ejemplo de este tipo de automatismo tenemos la obtención de información de un *hash* detectado como sospechoso a través de la integración con servicios como VirusTotal.

Una vez recogida esta información complementaria, el analista tiene una visión más completa de lo que puede estar sucediendo y si la amenaza es real o es necesario descartarla como un falso positivo. Es importante que este proceso sea ágil para poder tomar decisiones acertadas de una manera más eficiente.

Desde el SmartSOC de InnoTec se proveen una serie de *playbooks* que optimizan este proceso en un amplio porcentaje de incidentes que son gestionados de forma habitual. Estas acciones redundan en una mejora operativa para Oney, al ofrecerle un nivel de precisión muy alto en las detecciones comunicadas. Además, permite un ajuste continuo de las detecciones que suponen una falsa alarma y en las que, por lo tanto, la organización no debe invertir ningún recurso en su resolución.

En una segunda etapa, a través del proceso asociado a cada tipología de incidente, se accionan actividades de mitigación y contención que pueden ser aplicadas de una manera más inmediata, conteniendo así el daño que pueda sufrir la organización ágilmente. Para poder llevar a cabo este proceso es necesario un trabajo previo en el que se haya realizado una comunicación y configuración adecuada del entorno.

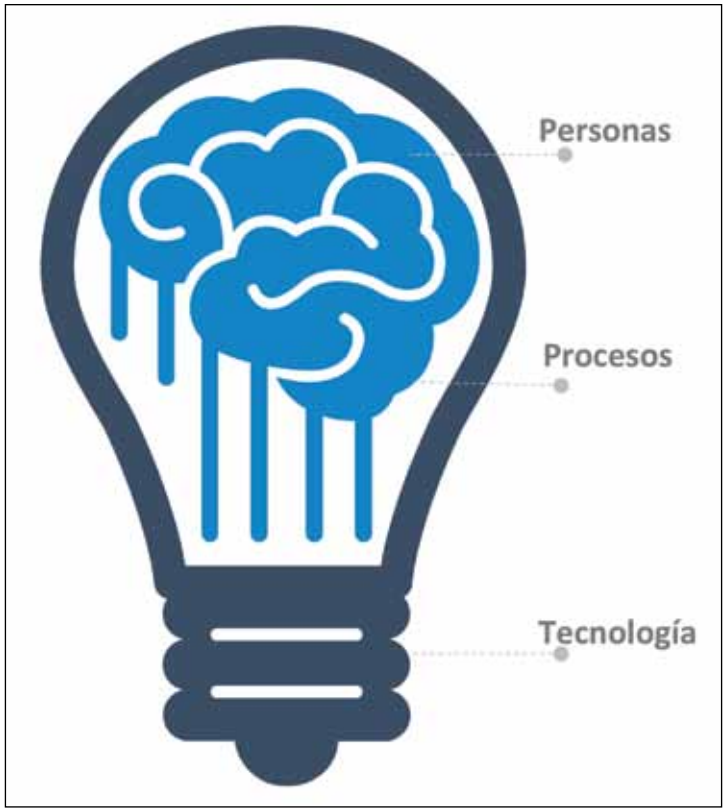

Figura 2.- Método.

Para realizar estas actividades desde el *SmartSOC* se utilizan dos herramientas desarrolladas desde el área de I+D+i de InnoTec: *Incident Manager* (IMA) y *Sonar*. La primera de ellas recoge los eventos correlados desde la plataforma SIEM del cliente, enriquece la información obtenida con otras aplicaciones (por ejemplo con Sonar) y muestra una primera valoración de la amenaza para que el analista tenga los datos suficientes para tomar las acciones que sean necesarias. Por otro lado, *Sonar* aporta los Indicadores de Compromiso (IoC), tanto propios como compartidos con la comunidad, que permiten asociar la detección de un indicador con una amenaza y ofrece una visión más completa en la gestión del incidente.

Para realizar el servicio desde el SmartSOC de InnoTec, se usan dos herramientas desarrolladas desde el área de I+D+i de este prestador: Incident Manager (IMA) y Sonar. La primera de ellas recoge los eventos correlados desde la plataforma SIEM del cliente, enriquece la información obtenida con otras aplicaciones y muestra una primera valoración de la amenaza para que el analista tenga los datos suficientes para tomar las acciones que sean necesarias. Por otro lado, Sonar aporta los Indicadores de Compromiso (IoC).

Así pues, el objetivo perseguido por Oney para complementar su estrategia de ciberseguridad con un servicio especializado le ha permitido incrementar su capacidad de respuesta ante incidentes de una manera eficaz, mejorando su visibilidad y conocimiento propio. Todo ello, adecuando la respuesta ante los riesgos a los que está expuesta por su propia naturaleza como empresa líder en el sector de medios de pago y financiación. ■

Javier Allende Astigarraga
Responsable de Seguridad de la Información
ONEY

Myriam Sánchez González
Responsable de desarrollo de Servicios de Ciberseguridad
INNOTEC – GRUPO ENTELGY