LA RESPUESTA A INCIDENTES EN UN ESCENARIO GLOBAL Y CON PROTAGONISMO DEL *RANSOMWARE*

INCIDENT RESPONSE IN A GLOBAL SCENARIO, WITH A PROTAGONISM OF RANSOMWARE

Autor:

Martiniano Mallavibarrena Martínez de Castro. Telefónica Tech.

martiniano.mallavibarrena@telefonica.com

Resumen:

Este artículo recorre todo el proceso conocido en conjunto como “respuesta a incidentes” y que en el sector de la ciberseguridad se ejecuta cada vez que una organización entiende que un incidente de seguridad ha sobrepasado un nivel de riesgo razonable. Veremos todas las dimensiones de este proceso. En los dos últimos dos años, el escenario predominante ha sido el basado en el *malware* conocido como “*ransomware*”.

Abstract:

This article covers the entire process known collectively as "incident response" and that in the cybersecurity sector is executed every time an organization understands that a security incident has exceeded a reasonable level of risk. We will see all the dimensions of this process. In the last two years, the predominant scenario has been based on malware known as “ransomware”.

Palabras clave:

Ciberseguridad; Respuesta a incidentes; Incidentes de seguridad

Keywords:

Cibersecurity, Incident Response, Malware

INTRODUCCIÓN

Hablar de ciberseguridad al nivel más general a comienzos de 2022 es realmente un desafío. Las sociedades más avanzadas se siguen digitalizando a un ritmo cada vez más alto y es común ahora mismo ver en los medios noticias sobre precios de venta de NFTs (Non Fungible Token), nuevos servicios basados en comunicaciones 5G, avances impresionantes en Inteligencia artificial o el famoso Metaverso. Por otro lado, y como ha ocurrido siempre, cada nuevo avance en el uso de la tecnología abre una ventana de oportunidad para actores maliciosos o su utilización interesada por actores relacionados con la geopolítica (como ocurre ahora con las llamadas *fake news* y la influencia en la ciudadanía).

En lo que se refiere de forma más concreta a incidentes de ciberseguridad, me gustaría comentar brevemente dos documentos de difusión reciente que creo muestran perfectamente esta tendencia:

- El informe del WEF (World Economic Forum), “Global Cybersecurity Outlook 2022”, recalca de forma muy contundente esta nueva generación de incidentes, cada vez más sofisticados. Sin entrar en mayor detalle, el documento explica como aquellas empresas que cotizan en el mercado bursátil NASDAQ suelen perder un 3% de su valor después de un incidente grave y como la mayor preocupación global es a un incidente ransomware. Dentro de este informe podremos obtener algunos indicadores muy relevantes sobre incidentes en seguridad a nivel global, su incremento en 2021, los tiempos medios de ataque, etc.

- Otro informe de interés es el elaborado por la compañía Allianz, “Allianz Risk Barometer 2022”, donde revisando los mayores riesgos este año para las compañías, se destaca a nivel global el de los ciberincidentes como el primero por encima de otros que podríamos entender también críticos como la pandemia causada por la COVID o las interrupciones/afectaciones en las operaciones por causas naturales, conflictos bélicos, etc. En el primer caso, las dos grandes ideas que están en la mente (*top of mind*) de las compañías que han participado

en el estudio son -a partes iguales- los ataques con *ransomware* y las fugas de datos.

Por todo ello y en un mundo donde una emergencia médica global ha enviado a trabajar de forma remota a millones de personas, las oportunidades para la ciberdelincuencia se han multiplicado. Las empresas gravemente afectadas por la pandemia, las infraestructuras no preparadas para un nivel tan alto ni intenso de teletrabajo, el uso incremental de la telefonía móvil (ahora 5G con nuevos servicios) y un largo etcétera, no hacen más que dibujar un entorno de ciberseguridad más frágil donde los ciberataques utilizando *ransomware* consiguen un muy alto resultado en el análisis coste-beneficio. Los modelos de *RaaS* (Ransomware as a Service) permiten a las organizaciones e incluso a los particulares, utilizar *kits* de ataque cada vez más sofisticados sin apenas conocimientos y con ciertas probabilidades de obtener grandes beneficios económicos muy poco trazables por el empleo de ciertas criptomonedas.

En este artículo vamos a revisar de forma completa como entendemos en nuestra compañía el proceso denominado respuesta a incidentes (en inglés se suele utilizar el acrónimo IR) y las distintas técnicas que se suelen utilizar en el mercado para hacer este trabajo útil para las organizaciones que nos contratan: aquellas que desgraciadamente se han visto impactadas por un gran ciber incidente basado en *ransomware*.

EL PROCESO GENERAL IR

En el mundo de la ciberseguridad los marcos que se utilizan nos sirven para organizar las tareas a realizar, la forma de conectar unas con otras y la forma de medirlas, para asegurar su eficacia y el nivel de calidad entregado a los clientes.

Además, existen multitud de organismos y asociaciones que aportan mejores prácticas, guías de implantación, catalogación de diversos elementos de interés (*malware*, actores, vulnerabilidades, etc.)

Por último, tenemos los estándares (los más célebres, pero no los únicos son la serie 27000 de la ISO) y las regulaciones (globales o locales) que nos exigen un cierto nivel de cumplimiento con arquitecturas, controles y procesos.

En lo que se refiere a la gestión de incidentes de seguridad, uno de los marcos más utilizados es el propuesto por el NIST (National Institute of Standards and Technology) agencia de organización de estándares del gobierno federal en Estados Unidos, en su documento “NIST 800-61 r2” y cuyo diagrama general para el proceso IR se muestra debajo.

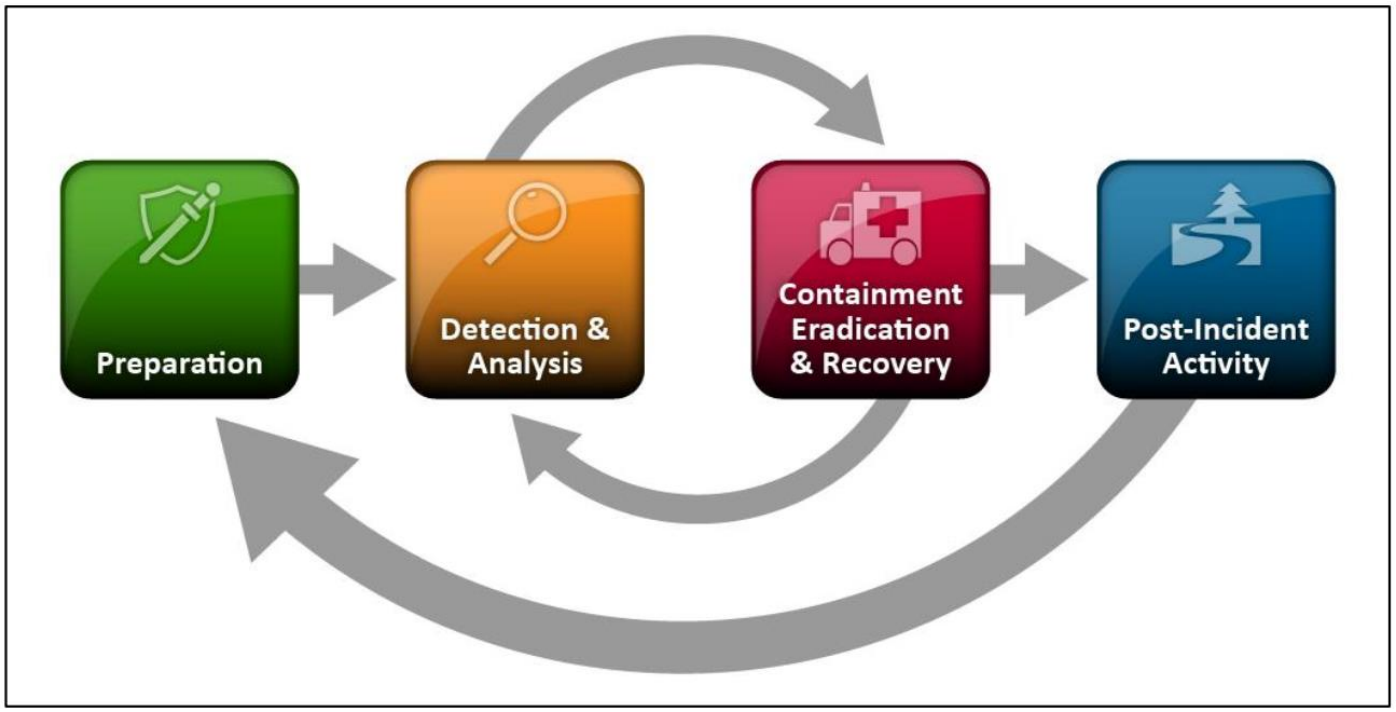

Figura 1
Diagrama general para el proceso IR
Fuente: https://www.cynet.com/incident-response/nist-incident-response/

Este enfoque se suele complementar con una clasificación taxonómica de los incidentes con el fin de utilizar un lenguaje común con nuestros clientes y para poder compartir conocimiento e información con aliados y autoridades.

En muchos casos, para la clasificación de incidentes y algunos detalles concretos de la gestión y comunicación de incidentes se utilizan marcos más “cercanos” como es el caso de ENISA (Agencia Europea de la Ciberseguridad) y del CCN-CERT (Centro Criptológico Nacional en España).

Se debe recordar siendo obvio que ciertos entornos amén de los de tipo militar requerirán un tratamiento distinto por normativa sectorial (caso de banca, por ejemplo) y de la observancia obligatoria de ciertos protocolos de actuación (caso de las administraciones públicas españolas y el llamado ENS – Esquema Nacional de Seguridad).

Al nivel más general y volviendo al proceso general de IR, las fases de mayor interés son, recordando la propuesta del NIST y asumiendo que ya ha sucedido el incidente:

— **Detección y análisis:**

- Si se ha activado ya un proceso de IR, se habrá producido la detección del incidente y posiblemente los efectos (cifrado masivo, caída de servicios, notas de rescate visibles) sean obvios.

- Mientras se comienza de inmediato con la fase de contención, se lanzará una labor de investigación y análisis que acompañará al resto de trabajos hasta su final.

- Los resultados del trabajo de análisis suelen ser guiados por el hilo conductos del trabajo forense que a su vez puede trabajar en distintos ámbitos: análisis de máquinas, análisis de *malware*, revisión de ficheros de *log* diversos, trabajo de investigación con entornos de tipo SIEM o EDR/XDR.

— **Contención:** En esta fase, que se suele iniciar al activarse el proceso de IR y tomar un primer contacto con el escenario, se suelen acordar una serie de medidas muy drásticas que tendrán como objetivo básico evitar una extensión del problema quizás a otras empresas del grupo, países, etc. Estas medidas suelen centrarse en:

- Corte o reducción severa de las comunicaciones con Internet (al menos, los primeros días). A medida que avancemos en el proceso de IR, iremos pasando del corte absoluto a una serie de listas “blancas” (tráfico legítimo como el único permitido) que, en un cierto tiempo (pueden ser semanas), nos devolverá al estado inicial (previo al ataque) de

permisividad en comunicaciones generales con Internet (para todo tipo de usuarios en la organización).

- Corte o limitaciones claras en las comunicaciones internas (tipo WAN, al inicio del proceso de IR). En los primeros momentos y para sustentar tareas de contención, se pueden solo dejar permitido el tráfico de autenticación, el de DNS y el de salida hacia la nube por parte del agente EDR (si se despliega en el proceso de IR que no siempre es necesario).

- Medidas de contención sobre la plataforma de autenticación (muchas veces, se tratará del AD de las plataformas Microsoft Windows): cambios de credenciales, actuaciones concretas sobre ciertas cuentas que utiliza el propio sistema operativo de servicio y lo mismo para aquellos parámetros de configuración que afecta a las relaciones entre dominios AD cuando existe más de uno (habitual en entornos multinacionales, grupos de empresas o en escenarios de fábricas con sus proveedores).

- Posible despliegue (quizás temporal) de plataformas de tipo EDR/XDR o uso intensivo de las actuales si éstas fueran suficientes para obtener telemetría en tiempo real

- Medidas concretas en sistemas o plataformas colaterales, normalmente sistemas propietarios, de tipo Legacy y/o sistemas cuyo sistema de autenticación no esté basado en el directorio activo central de la organización (si éste existiera y hubiera sido como suele el campo de batalla del ataque).

— **Erradicación:** En esta fase se toman medidas para asegurar que el proceso IR expulsa (erradica) la amenaza de nuestra huella tecnológica de forma permanente. Son múltiples las técnicas que un actor puede utilizar (de interés consultar siempre https://attack.mitre.org/tactics/TA0003/) y por ello, esta fase y el trabajo asociado suele requerir de varios días de investigación forense (ello generará indicadores de compromiso y TTPs) con el apoyo lateral de plataformas EDR/XDR por ejemplo, para ayudar a detectar esos indicadores del compromiso y para encontrar esas posibles persistencias en los sistemas

donde el agente esté instalado. Una vez el grupo de trabajo que realiza el proceso de IR va teniendo esa información y se van encontrando situaciones de interés en la planta, se podrá realmente comenzar la erradicación de la amenaza.

— **Recuperación:** El proceso de recuperación es realmente liderado por la organización que ha sido víctima, aunque los proveedores de servicios como nosotros, los acompañemos de forma constante y les vayamos dando soporte en la toma de decisiones. En algunos casos, es necesario prestar temporalmente servicios suplementarios pues la capacidad técnica y operativa puede estar mermada, por ejemplo: la parte del personal de IT con problemas de salud con COVID o confinados luego no pueden desplazarse al *datacenter*. En este grupo de servicios pueden incluirse: trabajo con fabricantes para solucionar problemas concretos en sistemas concretos, personal experto temporal para configurar sistemas de tipo *firewall* o SIEM, personal de soporte IT para instalar de forma masiva sistemas operativos en puestos de trabajo, etc.

Otros aspectos importantes en la fase de recuperación son:

- Realizar una planificación de restauración de sistemas y servicios ordenadas de acuerdo con las prioridades operativas -en algunos casos se utiliza de apoyo el servicio de DRP (Disaster Recovery Plan) o incluso el Plan director de Seguridad (para revisar todos los sistemas críticos y sus dependencias cruzadas con plataformas tecnológicas diversas). Cada una de esas restauraciones deberá seguir un protocolo previamente acordado para asegurar que estamos manteniendo un nivel de seguridad razonable en el proceso.

- Las copias de seguridad (todos los tipos posibles de tecnología) existentes el primer día de trabajo dentro del proceso IR se deberían haber revisado y clasificado para tener una idea clara de cuales serán de utilidad en esta fase. Recordemos que un incidente de *ransomware* tiene varias fases y que, por tanto, el adversario llevará días o semanas dentro de nuestros sistemas. Si restauramos copias del día previo al

ataque, por ejemplo, es muy posible que mantengamos la persistencia del actor o el *malware* y creemos un riesgo de forma inconsciente.

- Los distintos sistemas y servicios básicos de la huella IT de la organización: directorios (AD, LDAP, etc.), la resolución DNS, el servicio DHCP, la conectividad y *routing* general del tráfico IP, etc. Se revisarán de forma completa para asegurar que están en disposición de volver a operar con normalidad sin representar una amenaza o una debilidad.

- Se suelen crear entonces distintos grupos de trabajo entre el proveedor, el cliente y otros terceros para ir trabajando en esta restauración secuencial coordinada. Como veremos después, dentro del gobierno de la crisis, se irán coordinando estos trabajos de forma que se tengan en cuenta las prioridades del negocio y la disponibilidad de servicios primarios que sea necesarios para operar (ejemplos clásicos son la autenticación y el DNS, amén de un nivel básico de comunicaciones):

    - Un grupo habitual es el específico para puestos de trabajo “de oficina” dejando otro independiente para sistemas personales utilizados para teletrabajar (en este caso, los dispositivos suelen no ser siempre propiedad de la organización).
    - Otro grupo se suele ocupar de los sistemas de comunicaciones y servicios colaterales (sobre todo DNS, DHCP y tráfico de gestión IT básico).
    - Los sistemas centrales suelen tener dedicación específica también: ERP, CRM, sistemas de compras o logísticos, etc.
    - Otro grupo de trabajo se puede crear para instalaciones de tipo industrial que puedan tener dispositivos especiales conectados a la red, sistemas de tipo OT o sistemas industriales que se conecten a redes teniendo sistemas operativos especiales embarcados.
    - Otros grupos de trabajo que puede tener sentido crear temporalmente pueden estar relacionados con acceso remoto (entornos tipo Citrix o VPNs), sistemas de virtualización, y

grandes entornos Oracle, Plataformas Legacy (AS/400, Unix, etc).

Como veremos en el apartado siguiente, las fases se van solapando según tenga sentido hacerlo buscando siempre tener una vuelta a las operaciones ágil pero segura. Es por ello posible tener, en algunos casos, algunos sistemas en recuperación ya en las primeras jornadas de trabajo (quizás en una VLAN aislada para comprobaciones previas) y mantener trabajos de las tres fases en paralelo con una cierta planificación.

EL GOBIERNO DE LA CRISIS

Los incidentes de ciberseguridad que utilizan *ransomware* como enfoque, caso de ser exitosos, suelen causar un efecto devastador en las organizaciones que los sufren pues se suma el efecto directo (decenas o cientos de sistemas cifrados con funcionamiento muy degradado y pérdida de acceso a datos de interés) con el colateral automático producido por las propias acciones de contención que se producen en los primeros momentos, bien por mero reflejo y a veces sin mucho sentido, bien por recomendación razonada del proveedor de servicio o del grupo que lidera la respuesta al incidente. Todo ello produce un efecto acumulado que casi siempre conlleva una caída importante o generalizada de servicios con una crisis en las operaciones de la compañía. Es fácil imaginar el terrible impacto que puede causar esta situación en la organización en la que nos encontremos ahora mismo, el efecto suele ser crítico o, al menos, afectar de forma notable a ciertos servicios de la organización.

Cuando se decide activar un procedimiento de respuesta a incidentes se deberá tener muy en cuenta el impacto en las operaciones y organizar un equipo que participe activamente en el proceso (IR) mientras que otras personas deberán dedicar su tiempo a mantener la empresa lo más activa que sea posible, a coordinar las nuevas tareas (comunicación, aspectos legales, activación de métodos de operación alternativos, etc.) mientras dura la crisis.

En las organizaciones de tamaño medio-grande y sobre todo en las multinacionales, un proceso de respuesta a incidentes suele requerir de dos o más semanas para darse por completado cuando la organización entienda que la amenaza se ha contenido de

forma razonable, que se ha erradicado la amenaza y que el proceso de recuperación está muy avanzado y organizado de forma que no sea necesaria la disciplina de crisis que se comenta a continuación. Recordemos que, aunque se necesiten varias semanas para llegar a ese final del proceso IR, algunos sistemas y plataformas quizás se puedan ir recuperando ya (quizás con un nivel de rendimiento degradado) en los primeros días.

En líneas generales, los aspectos a considerar en el gobierno de la crisis en estas situaciones son:

1. Inicio del proceso de IR y creación de equipo de trabajo que siempre incluye roles del “cliente” y del “proveedor”. Adicionalmente y quizás solo en algunos momentos, otras personas fuera de este ámbito participen esporádicamente en reuniones y tareas.
2. Normalmente y de forma temporal, el proveedor de servicios lidera el proceso de IR y por parte del cliente se van tomando las decisiones para ir gobernando juntos la situación.
    a. **Por parte del proveedor** se suele designar un rol de coordinación (coordinador del incidente) para facilitar y agilizar la comunicación entre las partes, la gestión de reuniones, la compartición de información, etc. A lo largo de los trabajos, este role irá incluyendo en las reuniones a otros miembros de los equipos técnicos que apoyan el trabajo: personas expertas en análisis forense o de *malware*, expertos en *log* y comunicaciones, analistas de inteligencia o expertos en técnicas de *Threat Hunting* (búsqueda proactiva de amenazas).
    b. **Por parte del cliente** es muy razonable nombrar a una o dos personas (no es efectivo que sean más de dos) para representar los intereses del cliente, asistir a las reuniones, coordinación interna (pensemos en entornos internacionales con distintas zonas horarias, alternando reuniones en castellano e inglés, involucrando a distintos proveedores de servicios o fabricantes, etc.) y sobre todo tomar decisiones (algunas de gran calado) en la rutina de trabajo constante que se lanzará.
    En función del tamaño de la organización, de su posible distribución geográfica, de la relación con otras empresas del grupo (quizás sean

empresas participadas y tengan cierta independencia a nivel de dirección de tecnología), se suelen involucrar personas responsables de los distintos colectivos de IT que puedan existir: puesto de trabajo, *datacenter*, seguridad lógica, sistemas centrales, etc.

Es importante recordar que no suele ser eficaz involucrar en esta rutina de reuniones a la dirección de la compañía (el conocido como "nivel C") o al menos, mantener reuniones más ejecutivas para ellos, pero en otro calendario diferente al de las reuniones técnicas que serán mas frecuentes y con una agenda técnica detallada.

c. Algunas líneas de trabajo que es mejor gestionar en reuniones independientes son:

- **Aspectos legales y regulatorios** (se comentan posteriormente con más detalle) donde suelen intervenir abogados propios o despachos profesionales especializados, personas con funciones de DPO/DPD y otras personas de ambos equipos que puedan aportar información útil para las gestiones necesarias. En casos de incidentes *ransomware* en España, la práctica totalidad de casos afectan a datos personales de ciudadanos de la UE luego es de aplicación el reglamento UE GDPR y la LOPD (2018) entre otras normas legales. Las organizaciones vinculadas a sectores regulados de forma específica (defensa, espacio, financiero, etc.) y los servicios esenciales que se engloban en las denominadas "infraestructuras críticas" (bajo la supervisión y control del CNPIC) aportarán otras obligaciones ligadas a dichas regulaciones. Ello condicionará tanto la forma de comunicar el incidente como la posible participación de ciertos organismos (caso del CCN-CERT) y la operativa general del proceso de IR.

- **Comunicación en la crisis**: En muchos casos, el impacto del incidente es visible y afecta a los ciudadanos, a clientes de una compañía, a usuarios de un servicio o a alumnos de un organismo con competencias en educación. En esos casos, es totalmente

necesario acordar un plan de comunicación, coordinar el contenido de los distintos comunicados, etc. Este grupo de trabajo estará conectado con el central del proceso IR pero su ritmo de trabajo, calendario y objetivos se deben mantener paralelos por obvias razones de agilidad y eficiencia.

- **Empresas de seguros**: Suelen requerir documentación informativa, notas técnicas periódicas, valoraciones de daños con evidencias, etc. En algunos casos serán necesarias reuniones específicas con los coordinadores del proceso de IR y, al final del proceso, se suele generar un informe específico para cubrir sus necesidades de información.

- **Auditores externos**: En caso de multinacionales, no es extraño tener que colaborar con empresas que realizan funciones de auditoría, supervisión o de "*IT-Advisory*". Se organizará la debida coordinación y compartición de información con estas organizaciones para no afectar al ritmo de trabajo del grupo principal del IR. En algunos casos, esta línea de actividad puede requerir la firma de un NDA específico.

- **Fuerzas y cuerpos policiales**: En función del caso, las organizaciones suelen realizar una denuncia al cuerpo policial cuyas competencias cubran su incidente. Pese a que se suele realizar la denuncia en los primeros días, estos cuerpos necesitan información técnica mas completa del incidente para poder realizar su cometido por lo que la colaboración con estos entes se suele demorar algún tiempo. También se suelen generar informes *ad hoc* para ellos.

- ***Stakeholders*, inversores,** etc.: Algunas empresas de tipo multinacional suelen demandar algunas reuniones informativas con representantes de los principales inversores de la compañía, asesores externos, comité de dirección, etc. Estas reuniones son especialmente delicadas y se deben preparar por personas

específicas tanto del cliente como del proveedor, utilizando algunos materiales de apoyo, informes a medida, etc.

d. La relación con terceros vinculados a la tecnología de la empresa que actúa como "cliente" debe ser orquestada por ellos según sea necesaria su involucración en el proceso de IR. Puede haber conflictos en caso de que los contratos de servicio en vigor no cubran de la forma esperada, por ejemplo, trabajar en 24x7, desplazar personal, etc. Los terceros pueden ser:
    - **Proveedores de hosting o servicios en la nube** (AWS y Azure como dos de los habituales).
    - **Proveedores de servicios de IT, comunicaciones o de seguridad** si no están vinculados al proveedor que lidera el proceso de IR, en este caso, su participación es coordinada internamente. El caso de proveedores de servicios de tecnología o servicios gestionados en ciertas regiones (pero no de forma global) puede representar un reto, amén de cuestiones logísticas de zona horaria e idioma.
    - **Proveedores especializados en mantenimiento de páginas web, de firma electrónica**, etc.
    - **Proveedores de plataformas en modo *SaaS*** (Software as Service) vinculadas con ofimática, ERP, CRM, etc. aun no siendo habitual, en ocasiones hay que pedir su cooperación.
    - **Fabricantes de hardware, software o plataformas mixtas** cuyo funcionamiento esté degradado y requieren de soporte directo especializado (quizás no esté contratado y requiera gestiones urgentes)

El primer día de trabajo del grupo (día cero) se establecerá la rutina de reuniones técnicas más urgentes (pueden celebrarse cada pocas horas, las primeras jornadas) y se presentarán ambos equipos (los roles fundamentales, al menos) y la logística

básica para las reuniones (quizás de forma remota con plataformas de colaboración en la nube) y se realizarán algunas acciones fundamentales:

1. **Demandas de información básica por parte del proveedor** (caso de que no haya conocimiento previo por otros servicios): mapas de red de la organización, direccionamiento público y dominios en Internet utilizados, etc.
2. **Logística básica de reuniones:** plataforma a utilizar, por ejemplo: Slack o Microsoft Teams donde podamos tener las reuniones telemáticas en modo 24x7, albergar y compartir documentos, controlar tareas, etc.
3. **Contactos clave y escalados:** Aunque no siempre suceden incidentes graves, una vez iniciado el proceso de IR, en ocasiones, algunas alertas de SIEM/EDR o situaciones excepcionales, por ejemplo, una inesperada caída de un servicio ya restaurado puede requerir el contacto urgente (fuera de reuniones) entre las partes.
4. **Creación y rutina de trabajo de actividades colaterales:** Antes comentadas, para trabajar en paralelo con mayor agilidad. Se suelen utilizar herramientas ofimáticas habituales (caso de ficheros Excel compartidos, Microsoft Planner, etc.)
5. **Establecer el método de comunicación a dirección:** Se acordará el posible uso de actas breves de reunión, presentaciones ejecutivas para controles específicos, bitácora compartida, etc.

Una vez organizada la dinámica de trabajo, se irán lanzando las distintas actividades con *owners* por cada una de ellas. Las reuniones técnicas servirán para compartir información dentro del equipo, informar de avances o alertas de interés, nuevas medidas de contención/erradicación (normalmente según avance la investigación forense) y en su debido momento, sobre el estado de las tareas de recuperación.

En base a esta disciplina de reuniones, a la participación de distintos roles (algunos fijos, algunos esporádicos) y al plan de trabajo que se describe en este artículo, se irán cubriendo las fases esenciales comentadas, llegando finalmente a un escenario de recuperación básica y una contención/erradicación sólida. En esa fecha, el equipo de trabajo podrá comenzar a discutir el mejor momento para ir completando el proceso de IR y las tareas asociadas.

EL APOYO EN LA CIBERINTELIGENCIA

Empresas como la nuestra, que se dedican a prestar servicios de ciberseguridad, cuentan con plataformas donde gestionar su "inteligencia" y soportar el habitual ciclo que la mantiene útil. También se utilizan otros sistemas más específicos para, normalmente, añadir fuentes de inteligencia exteriores más específicas (utilizando los clásicos STIX, TAXII y demás estándares).

Todo ello se utiliza en muchos servicios de los que ofrecemos, pero también dentro de los procesos de respuesta a incidentes actuales, bien para conocer mejor al adversario, bien para guiar la toma de decisiones como veremos a continuación.

Por otra parte, mientras se realizan los trabajos forenses y de investigación, se suelen cruzar fuentes diversas para obtener información de todo tipo de indicadores de compromiso (IOCs por sus siglas en inglés), sobre todo direcciones IP, dominios utilizados en el ataque y *hashes* de *malware*/artefactos.

— **Conociendo a tu enemigo:** Como si volviéramos a leer "El arte de la guerra" de Tzun Tsú, es obvio que, al disponer normalmente de una nota de rescate o indicación clara de la amenaza persistente avanzada o actor involucrado en el ataque, confrontar fuentes diversas, investigaciones anteriores y referencias públicas nos dará un retrato muy útil de nuestro oponente. En muchos casos podremos conocer cómo suele actuar el actor: como suele realizar sus ataques y, en muchos casos, utilizaremos marcos internacionales comunes como la matriz ATT&CK de MITRE. Para ello, trabajaremos el concepto de TTP (técnicas, tácticas y procedimientos). También podremos conocer si es más habitual que el actor ataque un sector empresarial u otro, intereses geopolíticos si los hubiera (o relación con países concretos) y demás motivaciones. Por otra parte, los aspectos económicos pueden ser de interés: cómo se suele pedir el rescate, si hay baremo conocido para las cantidades, formas de pago típicas, etc.

— **Comportamiento esperado:** La sección de TTPs del actor es muy interesante para ir tomando decisiones en el proceso completo de IR. En muchos casos, nuestros equipos de inteligencia podrán facilitar este tipo de información y ello se utilizará dentro del proceso de respuesta a incidentes de varias formas, todas útiles:

revisando de una en una esas TTPS para ver si lo que vamos encontrando en la investigación forense es compatible y orientar a la vez el trabajo conociendo este comportamiento habitual (no de descartarán otras TTPs pero se pueden utilizar como referencia, caso de aparecer algunos posibles indicios) o ajustando el enfoque en contención y erradicación (fases importantes del proceso IR, explicadas al inicio del artículo) si podemos asumir que lo más probable es que nuestro actor tenga ese comportamiento (vector de entrada, movimientos laterales, escalado de privilegios y exfiltración, esencialmente). Los aspectos de persistencia esperada son interesantes aquí, de cara a poder hacer una erradicación efectiva de la amenaza.

— **Posibles decisiones del ámbito legal y de la comunicación:** En aquellos casos donde sea esperada una exfiltración, subasta de datos, etc. podremos comenzar a planear ya, como organización víctima del ataque, las acciones que tenemos que ir preparando para la comunicación con la agencia de protección de datos correspondiente, salvo que tengamos la certeza de que en los datos cifrados y potencialmente exfiltrados no hay datos personales de ciudadanos de la UE, con nuestro DPD/DPO y con terceros asociados ya que pueden derivarse obligaciones GDPR para comunicar a las personas cuyos datos se han cifrado o exfiltrado, que sus datos han sido comprometidos).Los aspectos de tipo GDPR (en muchos países fuera de la UE existen legislaciones en cierto modo similares a nuestra LOPD y que podrían aplicarse en el caso particular) se pueden ir documentando y preparando, esto nos ayudará en el caso de que se abra un expediente para aclarar el suceso, para agilizar el proceso y tratar de obtener los mejores resultados. El aspecto de comunicación puede ser necesario si, por ejemplo, conocemos que el actor tiene una página de tipo Blog (en el caso de Conti, es muy conocido su blog “Conti news”) luego podemos conjeturar que el nombre de nuestra organización pueda aparecer en dicha página (luego cualquier interesado o agencia especialista lo sabrá ese mismo día) y entonces nuestros empleados, clientes, proveedores y socios (amén de los accionistas y autoridades) lo sabrán también al ser motivo de comentarios en redes sociales, medios y quizás noticias en TV. Este previsible eco mediático, por ejemplo, una cuenta en Twitter considerada como de una persona especializada en la materia puede comentar el

tema y provocar un efecto dominó muy peligroso a raíz de esta noticia, se debe intentar controlar desde el principio como veremos más adelante (ver “daño reputacional”).

— **IOCs y otra información concreta del incidente:** Según avance el trabajo de investigación forense) puede ser contrastada con las fuentes de inteligencia disponibles para comprobar, por ejemplo, si alguno de los indicadores de compromiso, ha sido “visto” de forma reciente en otros incidentes y en cuales, si son ocurrencias cercanas en el tiempo, la misma dirección IP fue utilizada la semana pasada en otro incidente del mismo sector empresarial, por ejemplo. Este tipo de contraste suele ser muy revelador, caso de arrojar resultados positivos. Es importante por tanto contar con fuentes de inteligencia diversas en nuestras plataformas.

— **Inteligencia colateral:** Algunas fuentes adicionales de inteligencia pueden ser de especial interés en muchos escenarios IR y estas vienen relacionadas con, por ejemplo, la venta de credenciales en los llamados *dark markets* (donde esencialmente se puede comprar y vender cualquier producto o servicio al margen de la ley) o la posible actividad en blogs habituales de grupos delictivos, comunidad hacker, etc. En ocasiones, se ha podido trazar la venta en estos entornos de credenciales o datos robados en un incidente sucedido días atrás, lo que puede ayudar a confirmar el vector de entrada si, por ejemplo, el actor accedió directamente a un sistema con credenciales legítimas y se puede trazar venta de credenciales compatible en fechas previas.

EL ANÁLISIS FORENSE Y DE *MALWARE*

Un grupo de actividades que no faltará nunca en un proceso de respuesta a incidentes son las relacionadas tanto con el análisis forense de evidencias como el trabajo con *malware*. En este sentido hay que recordar siempre qué beneficios se deben esperar de este trabajo que nunca debe distraer los trabajos de contención, sobre todo en los primeros momentos. De forma general y sobre todo en el caso de disponer el escenario de una plataforma EDR, los trabajos de este tipo deben intentar apoyar la extracción en software en las utilidades que la plataforma ofrece, para evitar con ello desplazamientos y dedicación de tiempo por parte de la organización afectada.

Los objetivos esenciales del análisis forense serán, en el caso más general:

— Detectar lo antes posible los principales indicadores de compromiso del incidente, sobre todo aquellos que permitan mejorar la fase de contención.

— Intentar confirmar el vector de entrada utilizado por el actor, de forma que las medidas de contención se puedan optimizar al máximo; por ejemplo, en caso haberse utilizado una vulnerabilidad en una VPN.

— Confirmar, en lo posible, qué sistema ha sido el "paciente cero" lo que nos ayudará a comprender mejor la narrativa del ataque.

— Combinando análisis de LOG (quizás de *firewall* o SIEM) y trabajo forense en máquinas concretas, se suele poder trazar comunicaciones con direcciones IP de tipo C2 o con otras direcciones IP utilizadas para descargar herramientas utilizadas en el ataque (*hacktools*) y *malware* (Incluso el *ransomware*).

— Analizando en detalle las evidencias de tipo *malware*, los artefactos y el propio *ransomware* se puede llegar a obtener mucha información y quizás comprender de forma completa cómo funciona el mecanismo de cifrado lo que en algún caso puede ser útil (ejemplo: en algunos casos, el actor utiliza el cifrado standard de Microsoft Windows (Bitlocker) como alternativa y en ese caso, quizás podamos obtener alguna de las claves para descifrar los datos).

Sobre el aspecto concreto de la exfiltración de datos (recordando que no todos los actores, realizan esta medida de presión adicional), debemos tener en mente el enorme impacto que puede llegar a provocar en la organización afectada (se comenta más adelante) y por ello, debemos esforzarnos en intentar confirmar si se ha producido y en ese caso, intentar documentar al máximo los hallazgos asociados. Con frecuencia se puede trazar esta salida de información y en algunos casos, los servidores concretos y/o carpetas origen de los datos. Con esta información, la organización víctima del incidente, tiene más sencillo hacer un cálculo más preciso del contenido de dicha salida de información (podrá ser muy útil para el trabajo legal posterior). En este campo, se debe recordar también que los métodos son muy variados pudiendo utilizarse herramientas de soporte IT habituales como portales de almacenamiento de

datos conocidos. En algunos casos, se ha utilizado el propio almacenamiento de datos en red ofrecido por la empresa a sus usuarios.

EL USO DE PLATAFORMAS EDR

Que no hay dos procesos iguales de respuesta a incidentes es obvio para todos pues cada caso y cada organización tiene peculiaridades. El nivel de éxito del actor también puede cambiar de unos escenarios a otros.

En cualquier caso y en términos generales, para realizar un proceso de este tipo, suele ser del máximo interés contar con telemetría en tiempo real de los *endpoints* de la organización, sobre todo de aquellos sistemas mas importantes (controladores de dominio en concreto) y en la fase de contención y erradicación.

Para esta actividad, se suele comprobar si hay disponible (desplegada y activa) una plataforma de tipo EDR/XDR (detección y respuesta en nodos de red) o si, en su ausencia, el fabricante de antivirus utilizado tiene un módulo de este tipo que se pueda activar en pocas horas y que pueda cubrir las necesidades básicas antes comentadas.

Por ello, es común acordar el despliegue temporal de una solución de este tipo en la infraestructura y priorizando los sistemas de mayor riesgo para seguir con el mayor número de nodos posible (los movimientos laterales y la persistencia puede encontrarse en puestos de trabajo y puede ser necesario aislar estos sistemas de inmediato).

En caso de desplegarse, el proveedor de servicios incluirá temporalmente en el equipo un servicio de gestión de dicho entorno EDR y activará una monitorización de alertas en modo 24x7 para aportar tranquilidad al cliente mientras se va avanzando con el resto de las actividades. Se agregará por tanto este “bloque de actividad” a la rutina de reuniones comentadas en el apartado de “gobierno de la crisis” y la información del grado de despliegue o detecciones “ad hoc” positivas pasarán a ser parte de los puntos de control junto con otras alertas de interés que puedan haber aparecido.

Debemos recordar que la fase de contención se va actualizando a medida que la investigación progresa y se dispone de más información sobre el incidente (Indicadores de compromiso, sobre todo). Por ello, si por ejemplo, un análisis forense

nos entrega un código *hash* asociado a un fichero de *malware* o una dirección IP de tipo C2 (*command and control*), podremos crear una regla de detección en el entorno EDR para ser alertados de inmediato si tuviéramos casos reales de ambos indicadores (existencia del fichero en algún sistema o intento de tráfico con esa dirección IP).

En aquellos casos en que tengamos plataformas demasiado antiguas (EOL, fuera de soporte) o Legacy, es muy posible que el fabricante de la plataforma no disponga de agentes específicos. En esos casos se debe evaluar el nivel de riesgo y tomar medidas específicas como crear VLANs distintas con tráfico restringido o generar reglas a medida en los cortafuegos.

Al final del proceso de IR, la organización cliente decidirá entonces si mantiene este despliegue o se decida realizar un proceso de desinstalación, con apoyo siempre del proveedor de servicios.

EL *THREAT HUNTING* COMO VALOR DIFERENCIAL

No siendo siempre necesarios o posibles, en muchos casos, dentro del proceso de respuesta al incidente, se incluyen algunas actividades de “búsqueda proactiva de amenazas” (*Threat Hunting*, como nombre habitual en el mercado) para, utilizando como centro la plataforma EDR/XDR, realizar tareas de investigación complementarias a las realizadas por el equipo forense.

El punto de vista que ofrece la telemetría, su frescura en tiempo real y las habituales posibilidades que ofrecen las plataformas para hacer búsquedas complejas, crear reglas de detección a medida e incluso de automatizar ciertas actividades (utilizando enfoques SOAR), es realmente útil si, por ejemplo, estamos buscando persistencia, nodos que todavía intentan comunicarse con direcciones IP de tipo C2 o para confirmar el vector entrada y el llamado “paciente 0” del incidente.

Estas actividades se pueden lanzar cuando el escenario lo permita (quizás el despliegue temporal del EDR lleve poco tiempo y no hay nodos interesantes bajo su control) y en muchos casos, por un tiempo limitado. Durante este periodo, este bloque informativo se añadirá a la rutina de reuniones comentada anteriormente.

En casos donde además de EDR/XDR, se dispone de un SIEM con información útil y con la cobertura deseada se pueden combinar ambas fuentes de información e incluso "conectarlas", si ello fuera posible, pudiendo aplicar estos modelos de AI fuentes de datos más diversas y complementarias.

Esta actividad de *Threat Hunting* puede aportar mucho valor al trabajo del equipo y complementa perfectamente el trabajo realizado por el equipo que gestiona y monitoriza alertas en el mismo entorno. La frescura que aporta la telemetría en la investigación y el análisis dinámico basado en comportamiento y no en firmas o movimientos preestablecidos son claramente distintivos en cuanto a su importancia en el proceso.

Recordemos que la mayoría de las muestras de *malware* analizadas en incidentes de este tipo han sido compiladas justo antes del ataque (luego el *hash* no estará indexado en los habituales portales) y el ataque puede ser complejo y multifase, luego la aproximación por comportamiento parece ofrecer las mayores posibilidades de éxito.

ALGUNOS COMENTARIOS A LA LEGALIDAD Y AL DAÑO REPUTACIONAL

Sin duda, si hay dos daños colaterales de interés en los actuales incidentes graves de ciberseguridad son, a nuestro parecer, los daños de tipo "legal" y los relacionados con el impacto relacionado con la reputación de la organización afectada (o terceros relacionados).

En el grupo de daños legales para la organización que sufre el ataque, la rama más habitual (pero no la única) es la relacionada con el célebre Reglamento europeo (GDPR) que en España tuvo su necesario complemento en la nueva LOPD de diciembre de 2018. No era necesaria la transposición, pero la nueva ley orgánica armoniza bien los aspectos a concretar por los estados miembros mientras mantiene el alineamiento y coherencia con otros marcos como el ENS o el propio código penal.

La agencia con autoridad en la materia correspondiente (en España, la AEPD o las que existen en ciertas comunidades autónomas) mantienen el enfoque de considerar vulnerada la privacidad de los datos personales cuando éstos son, por ejemplo, cifrados en un ataque con *ransomware* (si el actor ha llegado a ellos, es obvio que no

se ha asegurado su privacidad) y por ello, la mayoría de los incidentes de este tipo terminan siendo motivos de expedientes en dichas agencias. A nivel internacional se utiliza la expresión PII (Personally Identifiable Information) que, en esencia, se corresponde con la definición de datos personales dada por el famoso reglamento europeo.

Los expedientes relativos con GDPR se inician a veces por el "descuido" de las organizaciones que han sufrido el incidente al notificar (el artículo 33 del Reglamento es claro en este sentido) dicha situación con el previsible objetivo de evadir las sanciones que se podrían derivar. Lamentablemente, es frecuente que los datos (o parte de ellos) cifrados en un ataque de este tipo terminen en algún Blog de TOR y por ello, expertos, medios, aficionados y analistas expertos en ciberseguridad se hagan eco de la noticia. La Agencia también suele estar pendiente de estos escenarios y suele abrir expedientes con claro interés esclarecedor.

En el resto de los casos, algunas organizaciones dejan claro su bajo nivel defensivo, lo relajado de sus políticas de seguridad o la negligencia en el cumplimiento de su propio plan director de seguridad (caso de existir).

Otros daños legales menos habituales pero posibles son los derivados por acuerdos comerciales específicos (quizás protegidos con NDA), denuncias de clientes o socios por lucro cesante o regulaciones sectoriales específicas muy comunes en servicios esenciales y/o infraestructuras críticas. En estos otros casos se han podido "perder" datos financieros, operativos, etc. Se han dado caso también de negligencia en la gestión de la crisis y "contagio" a terceros con consecuencias finales en los tribunales.

En lo concerniente a los daños reputacionales, podemos encontrarnos con varios casos. En todos ellos es importante recordar la importancia de tener un "guion" (*playbook*) de gestión de la crisis, así como un enfoque claro (desde el primer momento) sobre el plan de comunicación (normalmente se podría sugerir algo así como: "*Comunica tú, comunica primero, comunica en positivo la historia como la quieras contar y dale continuidad hasta el final*").

sos de interés:

- Empresas de reputación de cualquier sector que sufren un ataque de pleno impacto con resultados “humillantes” (Ejemplos: fugas graves de datos, periodo largo para recuperar operativa, etc.). Las grandes multinacionales, las entidades financieras (la privacidad es un pilar) o los operadores de energía y transporte son, automáticamente, foco de atención por obvios motivos sociales.

- Empresas que por su cometido albergan datos de especial sensibilidad (en el caso de datos personales de ciudadanos de la UE; los indicados en el artículo 9.1 del reglamento) y que por una “aparente negligencia” terminan expuestos o subastados en algún oscuro lugar de Internet (el régimen sancionador del GDPR se focaliza de alguna manera en estos casos para ser muy punitivo). Casos graves serían ciudadanos que han dado positivo en COVID o tienen enfermedades graves. Otros casos no relacionados con la salud, pero sensibles son “fórmulas secretas” de vacunas, ingeniería espacial o defensa; en este caso, los ataques suelen tener un componente geopolítico y no ser comentados en los medios.

- Organizaciones con mucha presencia en Internet o con modelos de negocio muy digitales con afectación clara en servicios (luego la crisis será obvia desde el primer momento por caída de servicios). Hay páginas web gratuitas para comprobar el estado de un servicio en la red y para comprobar sitios concretos bajo demanda. Las redes sociales se encargarán del resto. El plan de comunicación es el elemento central para gobernar la crisis.

En todos estos casos y en otros que podamos imaginar, las personas clave, directivos, accionistas y en general la “marca” de la organización, sufrirá un daño muy importante que se deberá gestionar desde el primer momento. Las consecuencias de este daño reputacional pueden ser realmente devastadoras en marcas comerciales, en negocios basados en una imagen sólida (¿Me cambiaría de banco si tiene dos incidentes graves de ciberseguridad en un año?), en empresas muy relacionadas con otros terceros (un fabricante de repuestos de automóvil tiene conexión con los propios fabricantes, por ejemplo), etc.

EL CASO CONCRETO DE LOS *DATA LEAKS*

En el mundo de la ciberseguridad se habla de "*data breach*" o "*data leak*" tanto en el caso de exposición accidental de datos con cierta sensibilidad (casi siempre por alguna negligencia en la configuración de la seguridad o métodos de acceso) como en el caso de acceso y exfiltración maliciosa por parte de un actor. En este artículo nos centraremos en el segundo caso, que es el que nos interesa.

Si los datos de nuestra organización terminan expuestos (o en venta/subasta) en Internet, habrá algunos puntos que todos debemos recordar.

1. Que un actor sea capaz de exfiltrar decenas, cientos o miles de gigabytes de datos de nuestra infraestructura es, desde luego, una mala noticia, pero realmente son varias malas noticias en secuencia y de alguna manera, tendremos que responder por todas y cada una de ellas:
    a. De alguna manera, este actor ha conseguido una primera conexión a nuestro entorno (compromiso inicial, múltiples métodos posibles).
    b. Ese actor u otro con el que colabora ha ido realizando acciones para poder moverse a otros sistemas y recopilar información útil para el ataque. Muchas veces, estos movimientos laterales ocurren a nivel internacional.
    c. Con herramientas, técnicas e información recién adquirida, estos atacantes han conseguido escalar sus privilegios. Normalmente utilizan el AD (directorio activo) de la organización, como vehículo. Si hay más de un dominio activo, suelen centrarse en el inicial al que tuvieron acceso.
    d. Cuando están en ese nivel de privilegios, recopilarán información sobre ficheros de interés (miles y miles de ficheros, normalmente, en diversos servidores o subredes) y en función de su patrón de comportamiento, se limitarán a cifrarlos y dejar una nota de rescate o -adicionalmente- los exfiltrarán al exterior utilizando métodos bastante conocidos (como *rclone*).

2. Todos estos pasos, plantean al menos igual número de preguntas por parte de la autoridad de la compañía, auditor o autoridad competente al respecto de las medidas de seguridad existentes y el nivel de vigilancia proactiva existente.
3. El último caso, cuando los datos abandonan nuestro perímetro como organización produce los conocidos como "*data breaches*" o "*data leaks*" (la doctrina en ocasiones matiza un concepto y otro que para este caso aceptamos como análogos) y que comentaremos a continuación.
    a. En función del actor concreto y partiendo de que los datos se han exfiltrado podremos encontramos situaciones diversas:
        - Publicación (parcial o total) en páginas web tipo Mega o similar (en la Internet "superficial") donde podremos tener (la propia organización, su representación legal o la autoridad si hubo denuncia) capacidad de maniobra para pedir de urgencia la retirada de los datos, cierre de la página, etc. En este caso, hay cierta probabilidad de obtener resultados positivos.

        - Referencias explicitas en páginas dentro de la Web Oscura (TOR, sobre todo). Este tipo de páginas, muchas veces se comportan como "Blogs" donde los autores (nuestro actor malicioso o sus patrocinadores, en caso de *Ransomware as a Service*) publicarán el nombre de nuestra organización, una pequeña reseña (pueden copiar la sección "Acerca de" desde nuestra página web corporativa) y en sucesivas ocasiones, quizás una muestra (equivalente a la "prueba de vida" en secuestros de personas) de ficheros robados (suelen buscar por nombres habituales: *"invoice", "order", "payslip",* etc.). Este tipo de páginas web suelen tener nombres explicativos (la presión es incesante) como "*Wall of shame*" (muro de la vergüenza) o "*Happy blog*", entre otros muchos conocidos. En casos de contenido o datos en estas zonas de Internet, las posibilidades de atribución con validez judicial son mínimas o nulas (por su arquitectura específica de túneles y anonimización) luego no debemos esperar resultados positivos aun con la mediación policial y/o judicial.

- Publicación directa o venta/subasta de los datos (parcial o total, para mantener la presión y la esperanza de cobrar el rescate) en entornos dentro de TOR. En estos casos, el actor compartirá (muchas veces de forma pública) multitud de ficheros comprimidos que se corresponderán con nuestra brecha concreta. Ciertos actores anuncian con titulares el contenido y fijan un precio de venta, otros los subastan (dejándole saber a todos que lo están haciendo) y cualquier variante de este tipo de esquemas. En este caso y como el anterior, la atribución con validez judicial es improbable o imposible y con ello terminan las posibilidades de cerrar la página, eliminar el contenido, parar la subasta, etc.

Es común que muchas veces los datos acaben directamente disponibles en estas páginas y cualquiera se los puede descargar. Dejando al margen el escenario legal de bajar datos “robados” en TOR, existen colectivos que bajan de forma regular estos paquetes de información buscando luego obtener beneficios, avisar a otros involucrados para intentar vender servicios de ayuda y un largo etcétera. No es raro que algunas de estas fugas de datos contengan información con la que preparar nuevos ataques, obtener credenciales, cuentas bancarias, etc. El interés para los actores maliciosos es obvio.

En el caso de que se produzca esta fuga de datos una vez se ha producido un incidente hay algunas consideraciones que las organizaciones deberían hacer:

1. **Consecuencias legales**: la más popular pero no necesariamente la más sancionadora es la línea de GDPR, vista en el bloque anterior). Suelen ser necesarias herramientas automáticas para poder analizar cientos de Gigabytes o incluso Terabytes de una fuga, tratando de caracterizar el tipo de datos que tenemos en su interior (lo que centrará el argumentario de la agencia de protección de datos para decidir sobre la sanción).

2. **Daño reputacional:** también comentado anteriormente, es obvio que muchas personas visitan TOR (o lo vigilan con herramientas automáticas) y obtienen beneficios de estas fugas de datos: bien comentándolo en redes sociales, bien

avisando a terceros, descargando los datos y comerciando con ellos, etc. Algunas organizaciones se han visto tentadas de pagar el rescate de un incidente *ransomware*, por ejemplo, solo por evitar esta situación aun teniendo un buen plan de recuperación: el daño reputacional severo y la revelación de secretos, pérdida de confianza de sus principales clientes, etc. Puede ser suficiente motivación. Mas allá de la información sensible que una fuga de datos pueda contener, mucha otra información (incluso ficheros personales de los propios usuarios en cualquier nivel de la organización) puede terminar descargada en cualquier lugar y por cualquier particular o colectivo lo que debe ser tenido en cuenta de nuevo, quizás, para tomar medidas en comunicación, interponer acciones judiciales con terceros, tomar acciones disciplinarias con empleados claramente incompetentes, etc.

Un caso mixto que sucede en ocasiones es aquel en el que la fuga de datos incluye datos de terceras organizaciones luego la fuga relativa a una empresa A impacta negativamente en otras (B, C, D, etc.) lo que de nuevo nos lleva a problemas serios de los dos tipos anteriores.

CONCLUSIONES

Como hemos visto a lo largo del artículo, el gran protagonista de los incidentes de seguridad actuales es el *ransomware*, sobre todo en modelos de colaboración entre actores, *RaaS (*Ransomware as a service*)*, y la utilización de diversas técnicas de intrusión que consiguen tiempos de ataque realmente cortos (no es extraño que sean pocos días los necesarios).

Solo aquellas organizaciones realmente preparadas y con uso eficaz de tecnología de última generación tendrán las mayores posibilidades de salir con un bajo nivel de éxito o impacto. La cultura general de los empleados y usuarios ante aspectos de ciberseguridad sigue siendo igualmente importante.

Un conocimiento completo y actualizado de tus propias infraestructuras tecnológicas, una visión detallada de como tus operaciones/negocio utiliza dicha infraestructura y el apoyo de un gran equipo (personas), disponer de un buen guion o *playbook* (procesos)

y contar con las plataformas mas adecuadas (tecnología) es claramente, la mejor receta para el éxito.

El proceso de respuesta a incidentes debe ser completo, ágil y eficaz de forma que la organización impactada, recupera lo antes posible la normalidad, pero con una garantía mas que razonable de hacerlo en condiciones seguras y permanentes. El uso de tecnología de última generación, el seguimiento de las mejores prácticas con una metodología probada y la implicación de personal experto son las mejores vías para superar con éxito este tipo de incidentes.

"*Mi mensaje para las compañías que creen que no han sido atacadas, es que no han hecho un análisis completo y preciso*" (James Snook, director adjunto de la oficina de ciberseguridad del gobierno británico, abril 2016)

BIBLIOGRAFÍA

- WORD ECONOMIC FORUM. *Global Cybersecurity Outlook 2022*. Disponible en https://www.weforum.org/reports/global-cybersecurity-outlook-2022
- ALLIANZ. *Allianz Risk Barometer 2022.* Disponible en https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html