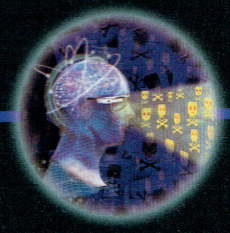


Ciberdefensa inteligente: confianza y reciprocidad

En la gestión de la ciberseguridad, la información lo es todo. Sin embargo, el cómo tratar la ingente cantidad de información generada acaba siendo crítico a la hora de realizar una defensa eficiente. La automatización de esta defensa es importante pero, en los ataques más complejos, queda sobrepasada por los atacantes. De ahí que la clave se encuentre en el factor humano, que es el que tiene la última palabra para interpretar y filtrar la información, para confiar o no en ciertos referentes y para compartir o no sus pesquisas.

Javier Candau

La sofisticación creciente de los ataques registrados es un hecho palpable que, sin lugar a dudas, nos obliga a replantearnos el quién y el cómo de la ciberseguridad en nuestras organizaciones. La complejidad de las técnicas usadas y el nivel de conocimientos técnicos de ciertos atacantes, la disponibilidad de nuevas o renovadas herramientas (incluyendo la prestación de servicios delictivos *on demand*) y la pulcritud en la perpetración de tales acciones, constituyen una preocupación creciente. Del mismo modo, la interacción que viene observándose entre los distintos atacantes, también dificulta todas las labores de seguridad. Así, los ataques dirigidos o APTs, que siguen representando la amenaza más significativa para las empresas y los organismos públicos de todo el mundo, están empezando a ser realizados también por los ciberdelincuentes, lo que incrementa su peligrosidad y eficacia.

Ante este panorama, cuando una organización se plantea adaptarse y mejorar el conocimiento de la amenaza, surge una problemática común: gestionar una cantidad ingente de información. Así, por ejemplo, la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, recibe diariamente más de dos millones y medio de eventos susceptibles de convertirse en un ciberincidente. De hecho, sólo una ínfima parte (alrededor de 75 al día), se convierten en tales. Pasar de una catalogación a otra (de evento a ciberincidente) no es baladí. Tan pronto como los incidentes y las vulnerabilidades son detectadas se inicia un proceso de gestión en el que se genera un volumen de información muy elevado que es necesario conocer y procesar en el mínimo tiempo posible. En una decisión en la que intervienen tanto factores humanos como técnicos que deben tratar la información proveniente de múltiples fuentes, propias o facilitadas por otras organizaciones, públicas o privadas; con todo tipo de acciones, datos y lenguajes y expuesta a la interpretación subjetiva de la persona o grupo de gestión de incidentes que la recibe.

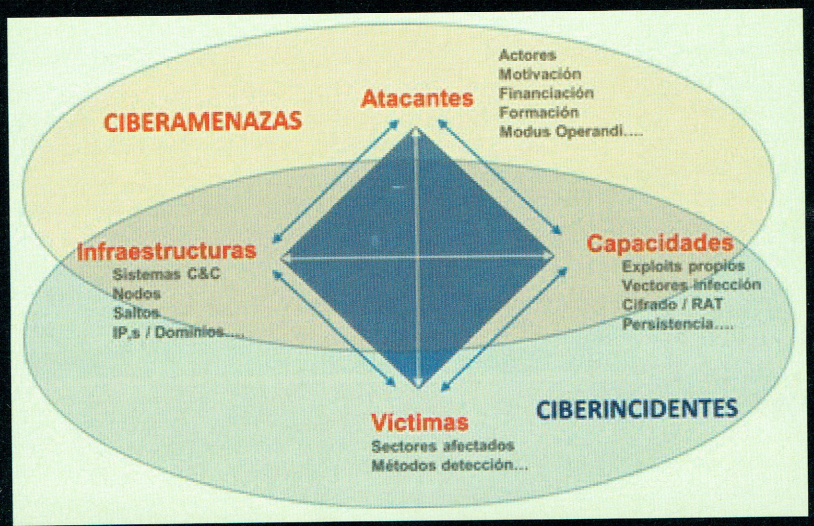


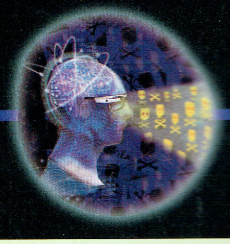
Figura 1.- Ciberamenazas y ciberincidentes constituyen las dos principales áreas de compartición de información.

El papel del analista

Ha quedado claro que es necesario realizar un primer filtro de modo automático. Conviene, por tanto, desplegar herramientas capaces de monitorizar y consolidar los registros de actividad de las diferentes tecnologías, del tráfico de red, de los usuarios remotos, de las contraseñas de administración, etc. Sin embargo, y sobre todo en ataques complejos, esta automatización es sobrepasada por el atacante, de ahí la importancia, y podríamos decir, la criticidad del equipo de seguridad con el que cuente la organización. La Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, como antes se ha señalado, recibe diariamente más de dos millones y medio de eventos susceptibles de convertirse en un ciberincidente.

Es el analista el que, tras acceder a toda la información, debe investigar los eventos y las alarmas, detectar falsos positivos, realizar análisis en profundidad, notificar ciberincidentes y, posteriormente, realizar un seguimiento de su estado y de su correcta resolución (o no). A tiempo, tendrá que generar nuevas reglas de detección (o refinar las ya existentes) y, por último, elaborar el correspondiente informe en el que se recoja toda la investigación que el incidente ha generado. Resulta de gran ayuda para esta labor, el empleo de herramientas que permitan el estudio y la correlación de eventos, basadas en la minería de datos del tráfico de red de la organización.

La Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, recibe diariamente más de dos millones y medio de eventos susceptibles de convertirse en ciberincidentes.



En líneas generales, el equipo de seguridad de una organización debería ser mixto (con personal externo e interno) y, llegado el caso, traspasar el ciberincidente a organismos superiores con una mejor perspectiva del conjunto y una mayor capacidad de actuación. En cuanto a la seguridad preventiva, que actúa como primer dique de contención, el decálogo de ciberseguridad del CCN-CERT [1] está plenamente vigente. Muchas de estas medidas apuntan a que la defensa tradicional [2] sigue estando vigente y las configuraciones de seguridad, la segmentación de redes, el control de los privilegios administrativos y la reducción del perímetro de exposición son principios que dificultan el ataque y en su caso la progresión del mismo en la red corporativa.

Compartición de información [3]

Tal y como hemos reseñado, es innegable que la constante monitorización de los sistemas y aplicaciones de una red permite la detección temprana de las amenazas, propiciando una respuesta rápida y eficaz y, en su consecuencia, limitando el daño. No obstante, tal monitorización constituye un trabajo intensivo y de alto coste, por lo que muchas organizaciones, públicas o privadas, no disponen de los recursos necesarios para implementar estas soluciones. Para hacer más eficiente este trabajo se hace necesaria la compartición de información y el uso de herramientas comunes o compartidas. Sobre todo, teniendo en cuenta que, aunque los atacantes van evolucionando, en muchos casos se observan aspectos recurrentes: mismos modus operandi, señales que indican el mismo origen, etc.

Principales estándares de compartición de información
OpenIOC
STIX , Structured Threat Information Expression
IDMEF, Intrusion Detection Message Exchange Format
MAEC, Malware Attribute Enumeration and Characterization
IOC, Indicators of Compromise
IODEF, The Incident Object Description Exchange Format
TAXII, Trusted Automated eXchange of Indicator Information
VERIS, Vocabulary for Event Recording and Incident Sharing
YARA
CybOX, Cyber Observable eXpression
CAPEC, Common Attack Pattern Enumeration and Classification
CVE, Common Vulnerabilities and Exposures
CWSS, Common Weakness Scoring System
CWE, Common Weakness Enumeration
WVE, Wireless Vulnerabilities and Exploits
CVSS, Common Vulnerability Scoring System
CCE, Common Configuration Enumeration
CVRF, Common Vulnerability Reporting Framework
CRF, Common Reporting Format
SCAP, Security Content Automation Protocol
OVAL, Open Vulnerability and Assessment Language
CWAF, Common Weakness risk Analysis Framework
XCCDF, Extensible Configuration Checklist Description Format

Figura 2.- Estándares de intercambio de información.

En cuanto a la materia a compartir, existen dos grandes áreas: ciberamenazas y ciberincidentes que permiten cubrir los vértices del modelo de diamante (**Figura 1**) y determinar las tácticas, técnicas y procedimientos (TTPs) del atacante. Con respecto a la primera, encontramos una mayor concienciación y voluntad de intercambiar por parte de las organizaciones y proveedores de servicio. En este sentido, nos encontramos con el problema del lenguaje utilizado a la hora de compartir la información: formatos inconexos (cada fuente elige su propia manera de expresar diversas características de la ciberamenaza), diversos tipos de protocolos o mecanismos de compartición de información, etc.

Existen estándares de intercambio lo suficientemente sólidos para que se avance con prontitud en este aspecto –**Figura 2**– (una gran parte de estos estándares son recogidos en la herramienta REYES [4] del CCN-CERT). En algunos casos, incluso, se podría hablar de fiebre en proporcionar herramientas de ciberinteligencia que buscan actividades sospechosas en redes sociales. Esta tendencia, consideramos que no se ajusta a la amenaza actual, pues normalmente consigue el seguimiento de atacantes que se mueven en este medio como el fenómeno *hacktivista* y, parcialmente, algunos relacionados con el ciberdelito, pero que no justifica el gasto y la necesidad de mantenimiento de las mismas por la necesaria migración para adaptarse a las APIs y las restricciones que van imponiendo las diferentes redes sociales.

Otra tendencia muy fuerte es la de vender información de interés sobre ciberamenazas. Nuestra experiencia es que pocas fuentes privadas que proporcionan este tipo de información justifican los precios que solicitan por tales servicios. Sobre todo cuando están muy industrializadas y no se adaptan a las necesidades de los clientes. Todas estas propuestas, sin embargo, no resuelven el punto clave: la confianza necesaria entre los participantes para que, por un lado vean beneficio en invertir tiempo y dinero en foros y sistemas de intercambio y, por otro, sea una actuación recíproca, en la que la información aportada es paralela a la obtenida para optimizar sus defensas.

Respecto a los ciberincidentes, la disposición a intercambiar entre organismos se ve reducida por el posible impacto que estos causan en las víctimas (compromiso de información, pérdida de propiedad intelectual, daños en la imagen o pérdida de contratos/

Conviene desplegar herramientas capaces de monitorizar y consolidar los registros de actividad de las diferentes tecnologías, del tráfico de red, de los usuarios remotos, de las contraseñas de administración… Sin embargo, y sobre todo en ataques complejos, esta automatización es sobrepasada por el atacante. De ahí la importancia, y podríamos decir, la criticidad del equipo de seguridad con el que cuente la organización.

negocio) y es necesario un mayor nivel de confianza. Este escenario se ha complicado con la aparición de diferente normativa que obliga al intercambio de información de ciberincidentes:

- RD 3/2010 que regula el Esquema Nacional de Seguridad (ENS). En su artículo 36 se habla de la notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados (esta actividad se puede automatizar con el empleo de la herramienta LUCIA [5] de gestión de ciberincidentes).
- Instrucciones de la Secretaria de Estado para la Seguridad en el caso de las Infraestructuras Críticas.
- Nuevo Reglamento Europeo de Protección de Datos.
- Nueva Directiva NIS.

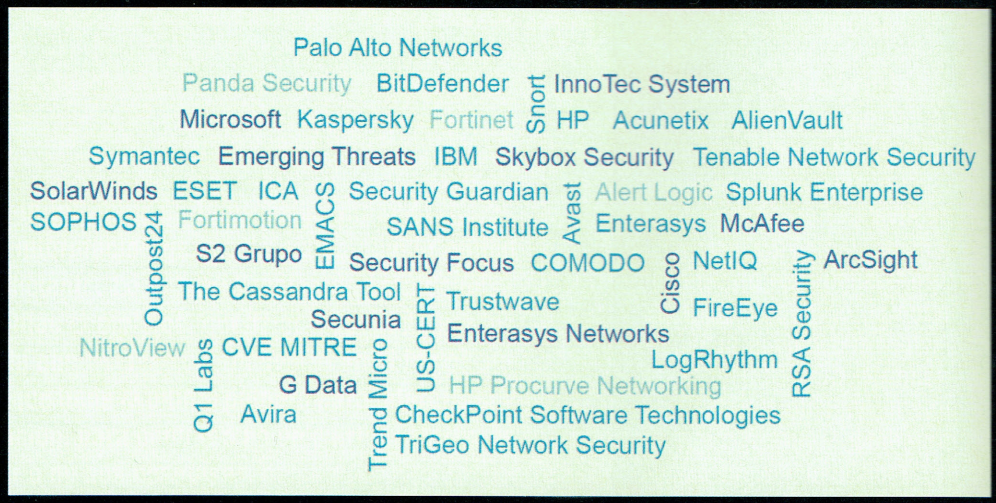


Figura 3.- Principales empresas que distribuyen Feeds entre su oferta de servicios (inteligencia, SIEM, IDS, antivirus y vulnerabilidades).

La industria de ciberseguridad nacional (sobre todo la de servicios) debe actuar como catalizador de la compartición de información de valor, dando especial énfasis al factor humano y a la formación de un buen equipo de analistas e investigadores, que aporten conocimiento y sean capaces de interpretar la ingente cantidad de datos.

No obstante, el intercambio de información tanto de ciberamenazas como de ciberincidentes siempre es más efectivo a través de la confianza entre las partes, no por imposición normativa. Por ello, los responsables de recibir estas notificaciones tienen que implementar sistemas que proporcionen valor añadido, tanto a la hora de aportar información agregada y sanitizada, que complemente la información remitida en los ciberincidentes notificados, como proporcionando información que mejore la detección o proponiendo medidas que optimicen las defensas de todas las organizaciones implicadas. Por otro lado, cualquier notificación se debería realizar una vez por lo que la coordinación en la recepción de estas notificaciones es clave.

Para que este modelo funcione las aportaciones respecto a ciberamenazas y ciberincidentes deben estar compensadas pues es necesaria tanto la información del atacante (sus capacidades e infraestructuras) como de la víctima (procedimiento de ataque, impacto sufrido y técnicas de detección/resolución que han tenido éxito) y así poder cubrir todos los vértices del modelo de diamante y poder conocer las TTPs del atacante.

La industria de ciberseguridad nacional (sobre todo la de servicios) debe actuar como catalizador de esta compartición de información de valor, dando especial énfasis al factor humano, a la formación de un buen equipo de analistas e investigadores, que aporten conocimiento y sean capaces de interpretar la ingente información. Es esta la labor que se debe esperar de ellos, más que la de proporcionar información de ciberamenazas en la que pueden estar compitiendo con otra empresa que proporcione los mismos servicios. ■

Hay una tendencia fuerte a vender información de interés sobre ciberamenazas. Nuestra experiencia es que pocas fuentes privadas que proporcionan este tipo de información justifican los precios que solicitan por tales servicios.

Javier Candau
Jefe del Departamento de Ciberseguridad
CENTRO CRIPTOLÓGICO NACIONAL-CCN

REFERENCIAS

(1) https://www.ccn-cert.cni.es/documentos-publicos/1153-decalogo-de-ciberseguridad/file.html

(2) Conocida como INFOSEC o STIC (Seguridad de las Tecnologías de información y comunicaciones)

(3) El CCN cuenta con dos Guías CCN-STIC: CCN-STIC-423 Indicadores de Compromiso y CCN-STIC-424 Intercambio de Información de Ciberamenazas. STIX-TAXII. Pueden consultarse en la parte pública del portal del CCN-CERT: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias-generales.html

(4) REYES (REpositorio común Y EStructurado de amenazas y código dañino) es una herramienta desarrollada por el CCN-CERT para automatizar el intercambio de información y conocimiento sobre ciberamenazas: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/reyes.html

(5) LUCIA es una herramienta desarrollada por el CCN-CERT para gestionar ciberincidentes y cumplir con el Esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/herramientas-deciberseguridad/lucia.html