Ciberseguridad aplicada a la Estrategia de Ciberseguridad Nacional (ECN)

Según un estudio de Lloyds sobre riesgos corporativos, el ciber riesgo se sitúa en el podio en la agenda de las cosas que más preocupan a los consejos de administración, solo por detrás de la pérdida de clientes y de la subida de impuestos. El crecimiento cualitativo y cuantitativo de los ciberataques en los últimos meses, y su eco en los medios de comunicación generalistas, está provocando una alarma social que poco a poco se está trasladando a las administraciones públicas.

DAVÍD FERNÁNDEZ
Responsable de desarrollo de negocio de Ciberseguridad de Symantec

JOSÉ LUIS LAGUNA
Systems Engineer Manager de Fortinet

La reacción gubernamental ha sido notable mediante la publicación y ejecución de la Estrategia de Ciber: INCIBE-CNPIC, CCN y MCCD. Sin embargo, el resto de la administración pública, salvo excepciones, no refleja en sus licitaciones la importancia de la realidad que nos ocupa, ya que a menudo se pretende resolver la problemática a base soluciones tecnológicas de nicho, olvidando las personas y los procesos necesarios para acometer el reto con ciertas garantías de éxito.

Symntec, en colaboración con Fortinet, propone una aproximación programática que contribuya de forma continuada a la mejora de la postura de seguridad de las administraciones públicas, reduciendo el ciber riesgo y redundando en definitiva en una mejora de la disponibilidad y calidad de los servicios públicos que se prestan a los ciudadanos. Para ello, Symantec ha adoptado como suyo el reto de la ECN, alineando todas sus soluciones de valor en ciberseguridad al objetivo global de la estrategia: Lograr que ESPAÑA haga uso seguro de los Sistemas de Información y Telecomunicaciones fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. (FIGURA 2)

Las capacidades a las que contribuimos desde Symantec deben entenderse como un ciclo de mejora continua ya que la prevención contribuye a la defensa, ésta a la detección y finalmente a la respuesta, para finalmente cerrar el círculo realimentando a la prevención de nuevo. La aproximación programática propuesta se basa en la realización de un análisis de las capacidades actuales, definición de un estado deseado realizable e identificación de un plan de actuación basado en "quick wins", entendiendo bajo este concepto aquello que puedo realizar en menos de tres meses.

Contribución a la Capacidad de Prevención

Todos los Gobiernos de los países más desarrollados han identificado la ausencia de profesionales "ciber" capaces de satisfacer las necesidades, tanto en calidad como en cantidad, que el mercado laboral está demandando y demandará en los próximos años.

El profesional "ciber" es eminentemente tecnológico, multidisciplinar y con visión integradora, desde los sistemas operativos y redes hasta el mundo de las aplicaciones y la criptografía. Además, el cambiante panorama de amenazas, técnicas de hacking y rápida evolución de la sociedad de la información con muchos más canales de acceso a la misma, hace que no sea suficiente con una formación estática y se hace necesaria la formación y aprendizaje continuo. Symantec contribuye a este reto mediante su plataforma de simulación (FIGURA 3) que bajo el prisma de una competición basado en casos reales, permite a los participantes el despliegue de un role play en el que desarrollarán su actividad e incrementarán sus conocimientos a lo largo de las diferentes fases de un ciber ataque. Bajo el lema de "conoce a tu enemigo" permite al participante la adquisición de conocimiento de ataque para mejorar la defensa.

Por otro lado, a nivel de prevención hay muchas actividades menos atractivas que se deben realizar como es identificar los activos de TI que dan soporte a los servicios públicos, así como evaluar la postura de seguridad de dichos activos de acuerdo a las mejores prácticas (configuración, vulnerabilidades conocidas, controles compensatorios aplicados) o guías de configuración recomendadas, entre otros, por el CCN. Básicamente se trata de evitar instalar una puerta blindada colgando la llave en el pomo de la puerta, así como iden-

FIGURA 1.Los cinco mayores riesgos

FIGURA 2.Estudio de Lloyd sobre riesgos corporativos

FIGURA 3. Plataforma de simulación de Symantec

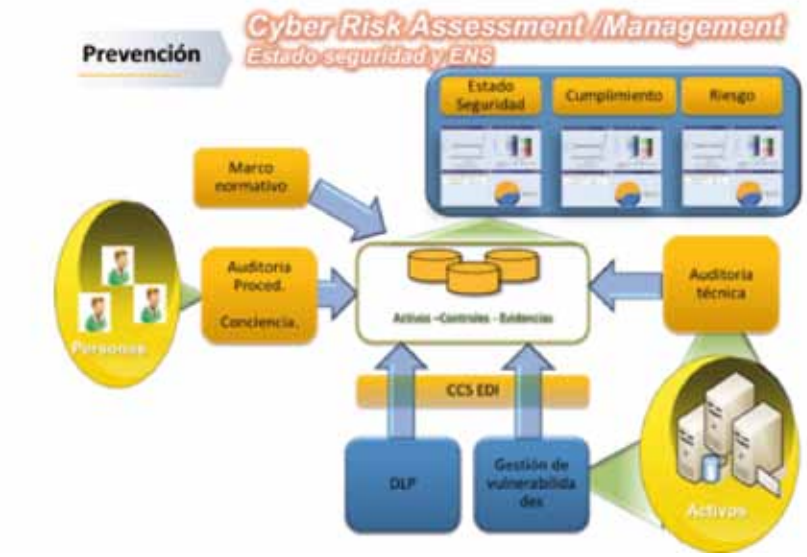

FIGURA 4. Esquema de la plataforma *Cybermaganement*

tificar ventanas abiertas u otras puertas además de la principal. Symantec propone para ser capaz de abordarlo su plataforma de *CyberManagement*. (FIGURA 4)

Cuando hablamos de ciberseguridad, se nos vienen a la cabeza palabrotas como Dragonfly, Turla, Careto, Cryptolocker,... que aparentemente son cosas nuevas, pero que la realidad es que son evoluciones de las existentes y ya conocidas. Entonces, ¿qué podemos hacer para anticiparnos a la siguiente evolución? Symantec propone de dotarse de Inteligencia de Seguridad que permita adquirir un conocimiento de las campañas, actores, mecanismos y, finalmente, tecnologías empleadas por estos APT (Advance Persistent Threats) para ver su aplicabilidad o afectación a nuestro entorno. Nuestra propuesta proporciona inteligencia de seguridad accionable (FIGURA 5), es decir, información de valor que permite la actuación por parte de la administración pública en sus capacidades de defensa, detección y respuesta.

Otra aplicación clave de la Inteligencia de seguridad de Symantec es la del consumo por parte de máquinas, fundamentalmente SIEMs o IDSs de los feeds reputacionales de IPs y URLs que proporciona contexto indispensable de lo que ocurre en el ciberespacio con el fin de mejorar la detección de lo conocido y desconocido por comportamiento.

Por otro lado, en la capacidad de prevención es recomendable identificar la información crítica para la administración pública, especialmente aquella que tenga que ver con LOPD. El falso mito en el que estamos instalados es aceptar que la información crítica reside donde se pensó en su día que debería residir. Sin embargo, la realidad es bien distinta y es recomendable realizar periódicamente un proceso de descubrimiento de la

misma, tanto a nivel estático (donde duerme) como dinámico (como se mueve), sobre la información estructurada (bases de datos) como no estructurada (ficheros en NAS, servidores de ficheros, buzones de usuarios...). Para ello Symantec propone su solución de *DLP/insight*. (FIGURA 6)

Finalmente, y como guinda a la capacidad de prevención, una buena práctica es la compartición de la información de forma que compensemos en cierta medida la "guerra" asimétrica en la que estamos inmersos. Además de la misión que en este aspecto tienen los CERTs gubernamentales, Symantec incorpora a todas sus soluciones una capacidad opcional que permite, de forma anónima y con determinados campos tokenizados, poner en conocimiento a los suscriptores de esta solución lo que a una entidad le esté pasando, nuevamente bajo el concepto de información accionable, como por ejemplo los IoC (indicadores de compromiso) que bajo la supervisión de la entidad que los recibe, de forma automática puedan ser implementados en las soluciones de Symantec que la entidad receptora tenga. Con esto pretendemos provocar un fenómeno viral positivo que beneficiará a todos los actores implicados.

Capacidad de Defensa

Esta es la capacidad más tradicional donde se han ido haciendo fuertes inversiones a lo largo del tiempo en soluciones tecnológicas más o menos avanzadas. Nuestra visión es ir ofreciendo progresivamente "Security Defence as a Service", involucrándonos junto con nuestras alianzas estratégicas en la defensa, más allá de suministrar una caja u otra. Desde el punto de vista de defensa avanzada, destacar que hay dos vectores de ataque frecuentes de los que hay que preocuparse actualmente y ante

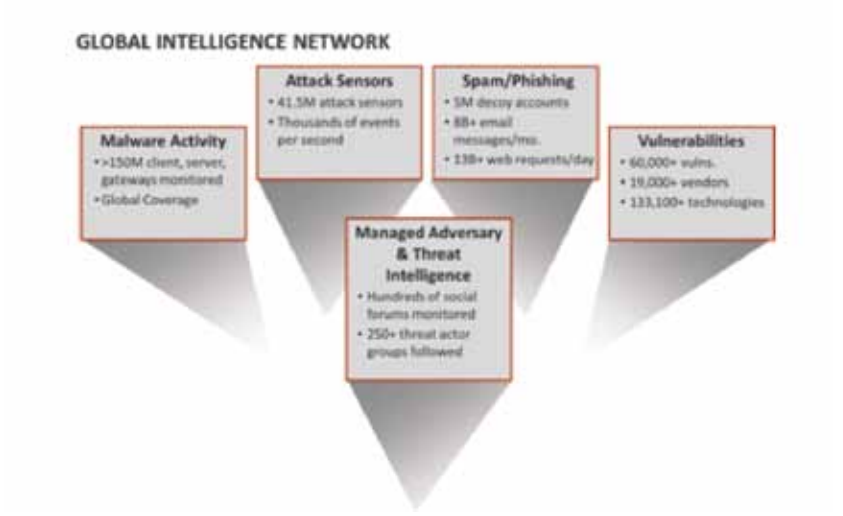

FIGURA 5. Inteligencia de seguridad accionable

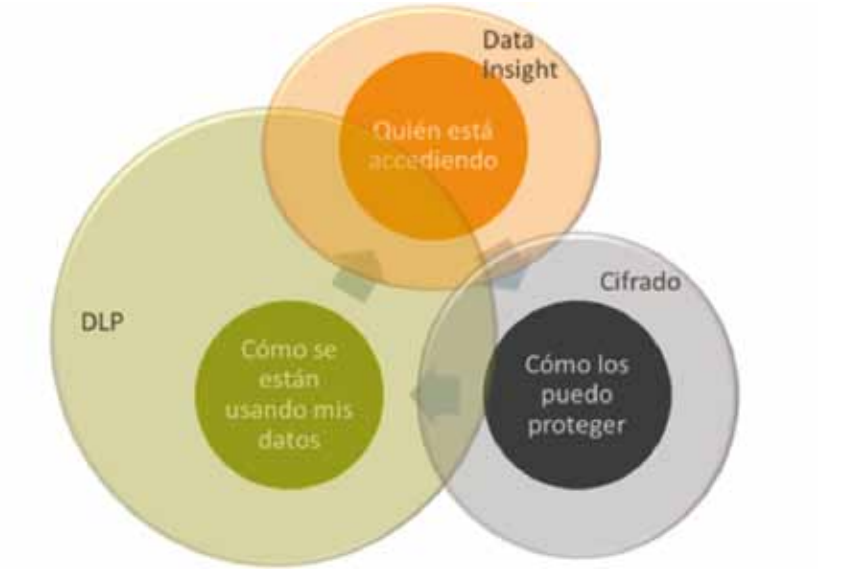

FIGURA 6. Solución de DLP/insight

FIGURA 7. Datacenter Security Server Advance

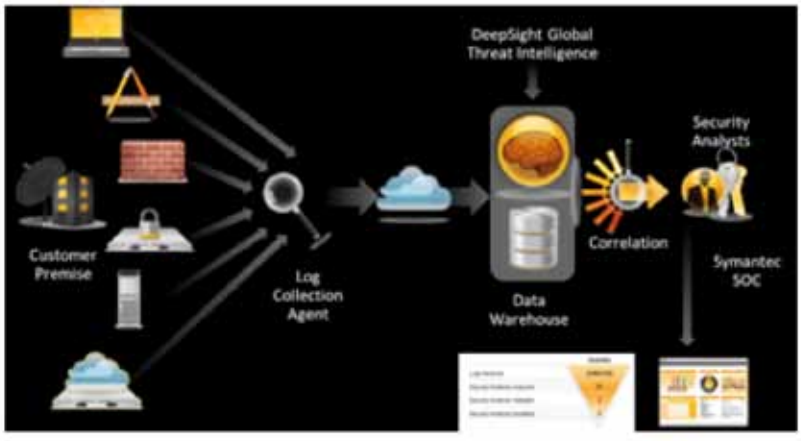

FIGURA 8. Solución integradora de Monitorización Avanzada

los cuales las soluciones de defensa tradicional (basados en firmas y otros mecanismos básicos) se manifiestan insuficientes: Usuarios y DMZ.

Comenzaremos por el segundo de ellos. La DMZ hoy en día es un elemento clave que hace realidad la administración electrónica, y por lo tanto la prestación de servicios a los ciudadanos, ahorrando costes y modernizando dichos servicios. Garantizar la disponibilidad de dichos servicios es clave y hasta ahora la replicación de datacenters, balanceos de carga y soluciones de copia de seguridad eran suficientes. Las ciberamenzas obligan a implementar mecanismos de defensa avanzada que impidan el sabotaje remoto de estos servicios, precisamente en la zona más expuesta al ciber espacio. Los desarrollos realizados basados en middleware (JBOSS, J2EE, .NET, JAVA) que están sometidos a nuevas vulnerabilidades, un mes sí y otro también y que no pueden ser parcheadas por diversas razones, hace que se

tengan que adoptar soluciones avanzadas de seguridad como *Datacenter Security Server Advance* (FIGURA 7). Esta solución proporciona parcheo virtual de escalado de privilegios y otros elementos de protección a nivel de servidor que permiten elevar el nivel de resiliencia muy por encima del existente actualmente sin afectar al rendimiento.

Continuando con el vector de ataque de usuarios, en el escenario actual de la ciberseguridad, donde aquello que no se detecta, es susceptible de provocar daños; proliferan los ataques dirigidos y adaptados que logran, cada vez más, eludir las defensas tradicionales de seguridad camuflándose como archivos inocuos que se intercambian constantemente en el día a día de una organización.

Para luchar contra estas amenazas avanzadas, los principales fabricantes de seguridad, entre los que se encuentra FORTINET, han desarrollado sistemas de Sandbox para la detección de brechas de seguridad. Estos sistemas deben permitir el escaneo de múltiples tipos de archivos, incluyendo Microsoft Office, archivos PDF, Internet Explorer, URLs, carpetas de archivos compartidos e incluso descomprimir y escanear archivos guardados. De esta manera, los departamentos de TI están protegidos contra los códigos maliciosos sin importar dónde se oculten.

Es importante que estos sistemas de *sandbox* se integren con las diferentes plataformas de seguridad perimetral, pero mucho más aún en el caso del correo electrónico, pues este es el vector más explotado en los ciberataques afectando a usuarios.

No todos los clientes pueden permitirse un sistema de *Sandbox* en su propio data center, por este motivo es muy conveniente que los fabricantes ofrezcan también soluciones de *Sanboxing* en la nube, que tienen un menor impacto para los clientes con menos recursos económicos.

Hasta ahora hemos mencionado soluciones en el vector DMZ orientadas a la defensa de la infraestructura. En cuanto a la protección de la información Symantec cuenta con las soluciones bien conocidas como DLP y PGP (cifrado).

Capacidad de Detección

Si una solución es apropiada defendiendo, también lo debe ser detectando haciendo buena la máxima de "no se puede controlar aquello que no se puede medir". Por lo tanto, todo lo desarrollado en la capacidad de defensa, aplica en este apartado. Sin embargo, la dificultad de obtener valor a nivel de detección cuando se mezclan tecnologías muy heterogéneas a nivel de red, puesto, servidores, etc. y el esfuerzo en personal e inteligencia que requiere, hace que tenga sentido la solución integradora de Monitorización Avanzada de Symantec (Symantec MSS) (FIGURA 8). Se trata de un servicio SIEM nube que se encarga de la recolección y custodia de los logs de seguridad, su análisis en tiempo real añadiendo el contexto de seguridad necesario en función de las ciberamenazas actuales, orientado a la identificación de incidentes de seguridad, momento en el que son escalados al cliente mediante analistas de seguridad de Symantec proponiendo un plan de remediación al mismo.

Capacidad de Respuesta

Entregada a través de las alianzas estratégicas de la compañía, haciendo uso de los equipos de respuesta a incidentes distribuidos globalmente y que han contribuido en la erradicación parcial y/o total de campañas como dragonfly, ramnit, etc. así como de las soluciones de las capacidades anteriores. Con estas, Symantec contribuye de forma significativa a fortalecer las capacidades existentes en los ámbitos de prevención, defensa, detección y respuesta, orientando sus soluciones a "Security as a Service" que permiten una aplicación efectiva y eficaz en la administración pública. ✱

El profesional "ciber" es eminentemente tecnológico, multidisciplinar y con visión integradora, desde los sistemas operativos y redes hasta el mundo de las aplicaciones y la criptografía.