La Cadena de Suministros y la Ciberseguridad

1. INTRODUCCIÓN

La Fundación ESYS organizó con fecha 28 de Mayo un seminario virtual para reflexionar sobre los distintos aspectos que relacionan la cadena de suministros en las empresas y la ciberseguridad y explorar las implicaciones en este debate de la regulación existente, las certificaciones necesarias y las buenas prácticas.

Se trata de un debate de gran actualidad, debido a la **vulnerabilidad creciente para la continuidad de negocio de las empresas, derivada de la dependencia de una cadena de suministros global** y "just in time", y a la existencia de una **regulación compleja**, de diferente aplicación en cada país y que, ante la ausencia de certificaciones, carga la responsabilidad de forma asimétrica en las empresas usuarias respecto de sus proveedores.

El seminario contó con la participación de ponentes y expertos que abordaron la Cadena de suministros y la Ciberseguridad desde diferentes perspectivas:

- Rosa Kariger, Global CISO de Iberdrola
- Karen Gaines, Global Head of Cybersecurity Defense de Siemens
- Luis Jiménez, Subdirector General del Centro Criptológico Nacional (CCN)
- Álvaro Garrido, Group Chief Security Officer & Group CISO de BBVA

2. IDEAS PLANTEADAS

- Dificultad para gestionar la seguridad en la cadena de suministro y los daños tanto reputacionales como económicos que ocasionan en las empresas
- Incremento de los incidentes, suponiendo ya para algunas grandes empresas el porcentaje mayoritario de sus brechas de seguridad
- Necesidad de que exista una corresponsabilidad, intensificar la inversión y realizar una labor de concienciación

- Dificultad para regular y armonizar la legislación en un problema tan complejo y que afecta de forma importante a múltiples sectores
- Importancia de las buenas prácticas y el análisis de riesgos en las compañías, adicionalmente a los posibles estándares o certificaciones que se implementen
- Se espera, aunque no sea la solución definitiva, contar en los próximos años con las certificaciones europeas de ciberseguridad de servicios, aplicaciones y productos

3. RESUMEN DEL SEMINARIO

• Introducción

La Gestión de los Riesgos de Ciberseguridad que provienen de la cadena de Suministros es actualmente un tema de preocupación para muchas empresas y Gobiernos para el que no existen soluciones ni respuestas sencillas.

La digitalización de las empresas ha experimentado un salto cualitativo desde el inicio de la pandemia y con ello se ha incrementado la superficie ataque y los riesgos de ciberseguridad.

Nos estamos volviendo cada vez más dependiente de la tecnología y el número de posibles puntos de fallo, así como la complejidad de las interdependencias con terceros está creciendo de forma exponencial.

La cadena de suministros compuesta por proveedores de equipos, materias primas o servicios se está complicando con la aparición de proveedores de servicios en la nube, programas de software que se escalan a los equipos, etc. y se extiende incluso a los componentes como los chips.

Toda esta red de compañías complejas que son necesarias para que las empresas puedan llevar a cabo sus operaciones, cada vez más digitales, es lo que denominamos cadena de suministros y sus relaciones se basan en aspectos comerciales, pero también de confianza en el cumplimiento de, por ejemplo, los estándares de calidad comprometidos, los plazos y en las mejores prácticas en materia de ciberseguridad. Se trata de confianza porque actualmente en este último punto no tienen ninguna obligatoriedad más allá de la estipulada por las empresas en los contratos.

En la Unión Europea y en otros países se está trabajando en el tema pero actualmente no existen certificados de Ciberseguridad que puedan ofrecer las garantías suficientes y la regulación que existe en esta materia no es de aplicación, solo es aplicable a aquellas empresas que suministran servicios esenciales, pero no así a la cadena de suministros.

A las consecuencias económicas derivadas de la existencia de un incidente para las empresas se suman los daños reputacionales por los ciberincidentes que probablemente quedarían excluidos de las pólizas de seguros tradicionales.

La situación se agrava si consideramos el componente económico porque al no ser un requisito obligatorio muchos proveedores rebajan los precios de la ciberseguridad y las empresas no siempre tienen una comprensión suficiente de los riesgos que están asumiendo por el ahorro de costes.

La conclusión es que la ciberseguridad se está "subastando" en las mesas de compras".

Teniendo en cuanta este planteamiento, es una cuestión de responsabilidad compartida pero en un ámbito donde no están claramente definidos los roles y responsabilidades que se complica ante la dificultad de comprender adecuadamente las interrelaciones y los riesgos asociados.

La complejidad de la situación está siendo aprovechada por los atacantes que obtienen más rentabilidad comprometiendo a un solo proveedor de múltiples empresas que a cada una de ellas individualmente. Y en este punto radica el potencial de los ataques a la cadena de suministros, ya que pueden comprometer a todos los clientes de un proveedor, y en el caso de grandes proveedores puede llegar a suponer un verdadero riesgo sistémico para un país o incluso a nivel internacional.

Los riesgos en la cadena de suministros es un problema difícil de abordar porque al final la ciberseguridad en las compañías depende del eslabón más débil y con esta creciente complejidad y ante un tipo de ataques cada vez más sofisticados y habituales, este eslabón podría estar en cualquier lugar. La cuestión es si es posible identificar dónde está ese punto más débil y si se tiene la capacidad para gestionar ese riesgo.

- INTERVENCIONES

Perspectiva de las empresas

La digitalización ha supuesto un doble reto para las empresas no solo por la seguridad sino por el nacimiento de nuevos negocios asociados al mundo online y cuyos clientes esperan el mismo servicio que en los formatos más tradicionales. A esto hay que sumar la emergencia en los últimos años del tema de la privacidad y la legislación asociada.

Hasta ahora resultaba más fácil proteger la cadena de suministro y esta situación ha cambiado por completo suponiendo actualmente un importante reto para las empresas.

Se está creando una disparidad entre las empresas que tienen más potencial inversor, experiencia o volumen para detectar los ataques a la cadena de suministro frente a otras empresas que quizá no tienen esa tradición o capacidad económica.

No suelen producirse riesgos con los grandes proveedores como Microsoft, Google, Amazon, etc., pero sí con otros proveedores en la cadena de suministros que tienen muy poca capacidad inversora.

El sistema de las cláusulas en los contratos con proveedores no se ha mostrado muy eficaz o es muy caro y por ello se están tomando iniciativas de control más sofisticadas tanto a nivel interno como de sensibilización a los proveedores para el trabajo en entornos protegidos de la propia compañía.

En el sector financiero se ha puesto en marcha la iniciativa Pinakes que puede marcar una tendencia, una asociación de 24 empresas con un formato donde las empresas proveedoras se puedan certificar en cuestiones que afectan a la ciberseguridad como la integridad, disponibilidad y confidencialidad, estableciendo una escala de clasificación.

Perspectiva de los Proveedores

El rol de los proveedores como integrantes de la cadena de suministros a la hora de asegurar la ciberseguridad debería seguir un enfoque integral para proteger los productos, soluciones y servicios, incluyendo la propia infraestructura interna de la compañía.
Entre las medidas existe una monitorización de los componentes de software proporcionados y se hacen públicos los avisos de seguridad para los clientes en los propios productos.

Los principales desafíos para los proveedores son la integridad, la interoperabilidad y la transparencia en la cadena de suministro que requieren los componentes de software que utiliza un producto (SBOM), sin embargo, rara vez se encuentra para productos en funcionamiento.
La integridad apunta realmente a la relación de confianza, por ejemplo, cómo un componente realiza el trabajo para el que está destinado. Así los controles de integridad están destinados a garantizarlo tanto a nivel técnico como organizativo.

Destacan iniciativas como “Charter of trust” en la que participan varias empresas para tratar de garantizar los requisitos en la seguridad digital: protección de datos, control de accesos, monitorización, proceso para productos auténticos e identificables e implementar más concienciación y formación para empleados.

Perspectiva de la Administración y reguladores

El papel de las administraciones y las agencias gubernamentales para ayudar a las empresas a mitigar los riesgos es muy importante en relación a la seguridad en la cadena de suministros. Se trata de un problema que no es nuevo pero es actual, y se viene abordando desde hace años.
Las organizaciones han ido madurando a la hora de implementar políticas y medidas de seguridad en sus sistemas de comunicaciones y fruto de esa madurez, se ha detectado la presencia de elementos y proveedores externos que suponen elementos de riesgos y vulnerabilidad.

El problema de la seguridad en la cadena de suministros se aborda con prácticas y metodologías muy tradicionales en el ámbito de la ciberseguridad que pasa en primer lugar por el análisis y la gestión de los riesgos.

La vulnerabilidad en los componentes y servicios externos debe formar parte de la gestión de riesgos integral de la empresa.

Existen tres principios básicos contemplados en todas las normas y estándares sobre ciberseguridad: nodo autoprotegido, mínimo privilegio y defensa en profundidad.

Nodo autoprotegido es considerar cualquier cosa que vas a instalar en tus sistemas o red como algo no confiable; mínimo privilegio afecta a el personal que gestiona los sistemas desde el exterior y cuenta con unas credenciales que permiten intervenir dentro del sistema de información y defensa en profundidad disponiendo de distintas medidas de seguridad en las diferentes capas a nivel de cada componente que permita detectar las vulnerabilidades y recuperarlas lo antes posible.

Las Administraciones públicas están trabajando en que la tecnología no sea vulnerable, evaluación y certificación de dicha tecnología y exigencia de las mejores prácticas en las empresas, principalmente a las que proporcionan servicios esenciales o digitales transponiendo la directiva NIS. Quedaría pendiente crear las condiciones adecuadas para que la colaboración público-privada en el tema de la cadena de suministros se pueda producir y en el conocimiento de los incidentes de las organizaciones que se debería intercambiar. Para que dicha información que es muy delicada se pueda compartir, ya que puede perjudicar reputacional y económicamente a las empresas o a las Administraciones públicas, se debe compartir en unos foros adecuados con unas reglas claras y donde prime la confianza de todos los participantes.

• CUESTIONES PLANTEADAS

- Teniendo en cuenta que en muchos casos las pequeñas y medianas empresas no disponen de suficientes recursos especializados para gestionar sus propios riesgos de ciberseguridad, ¿qué consejos claves se pueden dar para abordar los de su cadena de suministros?
    - Intentar trabajar en el factor humano y sensibilización (material de INCIBE)
    - Mantenimiento tecnológico (backups, servidores, etc.)
    - Plantear el mantenimiento tecnológico a través de proveedores de servicios o en la nube

- ¿Una regulación adicional o de otro tipo podría ayudar a abordar adecuadamente los riesgos de terceros? ¿Y en qué medida los certificados podrían contribuir a solucionar este problema?
    - La fuerte regulación en sectores como Salud o infraestructuras críticas siguen presentando problemas con componentes de seguridad de terceros
    - Existe regulación que afecta a las empresas (no a todas) partiendo de la Directiva NIS traspuesta a la legislación española, se establecen requisitos mínimos de intercambio de información de incidentes. También hay regulaciones sectoriales, por ejemplo, en el sector bancario, energéticos bastante completas o derivadas de la Ley de Infraestructuras Críticas. La PYME no tiene regulación o exigencias en relación con la ciberseguridad, se basa en buenas prácticas
    - La Directiva de la Unión Europa que crea el marco de Certificación Europea sobre la Ciberseguridad está por desarrollar, se encuentra en proceso (esquemas de seguridad en la Nube (ya existente), 5G (en proceso), seguridad del automóvil (en un futuro)…). Está en marcha también la Certificación del IOT (Internet de las cosas).
- Teniendo en cuenta la cantidad de proveedores que tenemos las empresas y la creciente complejidad de las interdependencias, ¿cómo podemos priorizar adecuadamente nuestros esfuerzos en este ámbito?
    - Criterio de volumetría de los datos, proveedores que puedan afectar a acciones de fraude o protección de datos
- Desde que se inició la crisis de la pandemia, la digitalización de las empresas se ha acelerado significativamente, en la mayoría de los casos soportada por servicios de terceros en la nube, herramientas de colaboración, videoconferencias, etc. ¿Qué pueden hacer las empresas para evitar los riesgos de una alteración o incluso interrupción de sus operaciones en esta situación de elevada dependencia de estos servicios?

- Crear transparencia y estructuras los riesgos reales para la mitigación y realizar las inversiones necesarias
- Contratar un seguro de Ciberseguridad con los riesgos residuales
- Estrategia de múltiples proveedores para evitar bloqueos y dependencia e interoperabilidad

- Determinadas empresas no son consideradas esenciales, pero al ser proveedores de multitud de empresas, si son atacadas, podrían ocasionar una disrupción relevante. Ejemplo Solardwinds. ¿Si se hubiesen aplicado todos los principios tradicionales de ciberseguridad, se podría haber evitado?

  - El problema del software o hardware con malware embebido es un problema con el que se tendrá que convivir mientras no se produzca una evolución en los estándares de desarrollo.
  - Gestionar los elementos más críticos en la red se permite detectar y mitigar el problema
  - Impulso de la colaboración público-privada desde nodos centrales

- *REFLEXIONES PLANTEADAS EN EL DEBATE*

  - Fondos de recuperación europeos como un vector de inversión potencial (en pymes, ciudadanos y Administraciones Públicas)
  - Mala calidad del software que se está comprando por aumento de vulnerabilidades, ¿cuál es la responsabilidad del proveedor? Incidir en la corresponsabilidad y mayores garantías
  - Exigir responsabilidad a operadores pero también a proveedores
  - Balancear despliegue tecnologías y sociedad de la información con la ciberseguridad

- Explorar modelos regulatorios no sancionadores sino que incentiven la ciberseguridad que se están aplicando en otros países y discriminadora de la calidad
- Revisar los procesos de contratación y los requisitos de ciberseguridad como un factor diferenciador pero que supone un aumento de costes
- Ciberseguridad como un factor de rating que empieza a ser diferenciador para las empresas y que en un futuro puede ser un modelo obligatorio
- Regulación en Europa y España muy sectorizada (banca, energía, etc.) que dificulta tener unos requisitos de cumplimiento definidos con claridad. Complejidad de compartir esquemas en todos los sectores. Esfuerzo por parte de ISO y los organismos de estandarización europeos, por ejemplo, en la tecnología 5G
- Impulsar la cultura de la Ciberseguridad a nivel social y profundizar en la concienciación de los riesgos
- Dificultad de cuantificar el riesgo para los Seguros de Ciberseguridad
- Importancia de la figura del CISO en la estructura de una empresa y colaboración necesaria con el departamento de compras

RESUMEN CONCLUSIONES

- Aplicar las mejores prácticas
- Trabajar con entornos protegidos tratando de mantener los proveedores aislados
- Importancia de la inversión y de los fondos europeos para tratar de elevar el nivel
- Análisis de riesgos como elemento fundamental para tener una buena visibilidad de los riesgos de la cadena de suministros, las dependencias y los daños colaterales asociados
- Cooperación de las empresas, proveedores y Administraciones públicas
- Incremento de colaboración público-privada en el intercambio de información