Cuando el punto flaco de tu estrategia de ciberseguridad es tu proveedor

Una de las vulnerabilidades más importantes de las estrategias de ciberseguridad de las empresas se encuentra en su cadena de suministro. Si nuestros proveedores no están debidamente protegidos, pueden hacer de puerta para los delincuentes a nuestra información y nuestros sistemas .

"Solamente hay dos tipos de empresas: aquellas que han sido hackeadas y aquellas que lo serán". Así de tajante se muestra Robert Mueller, director del FBI entre 2001 y 2013, a la hora de expresar que, dentro de la economía digital, nadie está a salvo de convertirse en la víctima de un ciberdelito.

Un reciente estudio de la aseguradora Hiscox, realizado entre empresas de Estados Unidos y de varios países europeos incluyendo España, pone en evidencia que la proporción de compañías que ha denunciado haber sufrido ciberincidentes ha subido del 45% del año pasado al 61% de 2019. Por otra parte, el porcentaje de las

mismas que, de acuerdo con el modelo de Hiscox, presentan un nivel de experto en el diseño y la aplicación de su ciberestrategia es tan solo del 10%.

Los ciberriesgos no respetan el tamaño. Tradicionalmente, el objetivo de los *hackers* eran las grandes corporaciones, pero, gradualmente, el problema se ha extendido a todo el tejido empresarial. La proporción de empresas medianas (entre 50 y 249 empleados) que han reportado problemas en este sentido ha crecido este año del 36% al 63%; en el caso de las más pequeñas (menos de 50 trabajadores), la cifra ha variado del 33% al 47%.

Como es natural, los ciberataques suponen cuantiosas pérdidas monetarias para los negocios. El informe de Hiscox establece un crecimiento interanual del 61%, de 229 000 dólares en 2018 a 365 000 este año.

Los incidentes de ciberseguridad que están cobrando cada vez más protagonismo son los relacionados con la cadena de suministro de las compañías. El pasado año, casi dos tercios de las empresas tuvieron problemas en este sentido por culpa de sus proveedores. De hecho, el 75% de las empresas de tecnología, comunicación, servicios de telecomunicaciones y transporte, fueron atacadas.

Si nos centramos en España, la cifra sube: hasta el 72% de las firmas ha sufrido un ciberataque a través de su cadena de suministro. Esta proporción solamente es superada por Bélgica (73%), dentro de los países estudiados por el informe.

Otro estudio, esta vez promovido por LEET Security, destaca que el 80% de las empresas españolas está muy preocupado por su ciberseguridad, y entre los aspectos que más inquietud despiertan está la protección de los datos de los clientes.

No obstante, la consideración de los riesgos de la cadena de suministro es un tema pendiente de la empresa española. Tan solo un 40% de las organizaciones reconoce que evalúa a todos sus proveedores, mientras que el 31% lo hace solamente con aquellos tecnológicos, y el 29% únicamente con los calificados como “críticos”.

Riesgos en la cadena de valor

Un ataque a la cadena de suministro tiene lugar cuando alguien se infiltra en los sistemas informáticos de una empresa y accede a sus datos a través de uno de sus socios o proveedores. En el mundo empresarial actual, la externalización de funciones y servicios es algo natural, por lo que en el terreno de la informática y las telecomunicaciones es normal que exista una gestión por parte de terceros. Esto implica que personas ajenas a la empresa pueden entrar en sus sistemas para mantener equipos y aplicaciones, o administrar las redes de forma remota, entre muchas otras acciones. Igualmente, existe otro tipo de proveedores que, aunque no están conectados digitalmente a la empresa, disponen de información sensible de esta. Los consultores y auditores son ejemplos de ello.

Un ciberataque que llegue a través de la cadena de valor puede suponer, desde la pérdida de información de valor para la compañía o de propiedad intelectual, hasta el robo de información personal y financiera, e incluso, la sustracción de fondos. Y, de acuerdo con el INCIBE, el 63% de los ataques se producen a través de los proveedores.

La cadena norteamericana de almacenes Target sufrió en 2014 el robo de los datos de 70 millones de clientes y de 40 millones de tarjetas de débito y crédito. Los ladrones utilizaron las credenciales de un proveedor de material de climatización de la empresa, Fazio Mechanical Services, que obtuvieron infectando con *malware* su web. A partir de allí, los hackers pudieron acceder a la zona de proveedores de la web de Target.

Igualmente, en 2017 la empresa de informática Equifax descubrió una brecha de seguridad en sus sistemas por culpa de una aplicación web de terceros, que dejó expuestos los datos personales de 143 millones de estadounidenses.

En 2015, fue *hackeada* la operadora de telecomunicaciones Verizon a través de una empresa proveedora de servicios de analítica web y quedaron desprotegidos los datos de seis millones de clientes.

Gestionar el riesgo de terceros

Los ciberriesgos asociados a los proveedores de la empresa hacen necesario mitigar, en la medida posible, las amenazas que se plantean. Esto es lo que se conoce como gestión de la cadena de suministro, en inglés *vendor risk management* (VRM).

Gartner define el VRM como el proceso de asegurar que la utilización de proveedores de servicios y suministradores de tecnología informática no genera un inaceptable potencial para la disrupción del negocio o el impacto negativo en la actividad comercial.

Un programa de gestión del riesgo de la cadena de valor debe contemplar todas las amenazas posibles, no solo las relacionadas con la ciberseguridad, sino también otras, como, por ejemplo, la probabilidad de quiebra que puede tener un proveedor determinado y la posibilidad de que acarree un impacto reputacional para la empresa.

Igualmente, debe establecer concretamente la responsabilidad de todos los procesos que puedan verse afectados por un incidente, y contar con un equipo multidisciplinar integrado por miembros de los departamentos correspondientes.

Como es lógico, el programa VRM de la compañía tiene que conocer a fondo la relación de proveedores, algo más difícil cuanto mayor es su tamaño, y determinar cuáles son los más sensibles, para dedicarles más recursos. Por otro lado, no vale con evaluar el riesgo una vez y olvidarse; la monitorización de las posibles amenazas a la cadena debe ser una tarea continua en el tiempo.

¿Cuál es el peligro real?

Hasta ahora hemos hablado de ciberriesgos y de cadenas de valor, pero conviene describir cuáles pueden ser los efectos de un ciberataque en la actividad de la empresa. En este sentido, podemos destacar los que siguen:

Aquellos que causan un daño *directo*, como son el robo de datos personales, de contraseñas, de know-how, las extorsiones, el infectar equipos y redes, o el tirar abajo servidores, entre muchos otros.

Aquellos que tienen un impacto negativo *indirecto* en la actividad de la organización, como pueden ser los que obligan a paralizar la actividad e implican el incumplimiento de contratos, los que implican pérdida de mercados o de imagen de marca, los que suponen sanciones regulatorias o los que obligan a pagar indemnizaciones por daños a terceros.

En cualquier caso, cualquier ciberincidente puede generarle a la compañía responsabilidad civil frente a terceros o usuarios, responsabilidad laboral, respecto a sus empleados que puedan haber sufrido perjuicios por el ataque, responsabilidad penal, para los cuadros de mando por las acciones indebidas de un tercero en las redes, responsabilidad administrativa, por incumplimiento de normativas, responsabilidad contractual, al no poder responder a las obligaciones establecidas e, incluso, responsabilidad extracontractual, en el caso de

que haya terceras personas afectadas -sin relación con los servicios de la empresa- por los efectos del ciberataque.

Resiliencia de la cadena de suministro

Relacionado con la gestión de riesgos de la cadena de suministro, aparece el concepto de resiliencia. Se trata de un término muy de moda actualmente en el mundo del *coaching*, que, como se puede comprobar, puede aplicarse a numerosas áreas y actividades.

La resiliencia es la capacidad de un sistema para volver a su estado original (o deseado) después de haber sido perturbado. Si hablamos de ciberseguridad, sería la habilidad de la cadena de suministro de la empresa para enfrentarse a trastornos inesperados. O, en otros términos: la capacidad de la organización para continuar llevando a cabo el negocio, aunque su acceso a los servicios de internet haya sido cortado o dañado.

Desde esta perspectiva, la ciberresiliencia va más allá que establecer medidas de seguridad informática, puesto que implica a la gestión de los riesgos del negocio en sí misma, y a la gestión de la cadena de proveedores. Dado que los ataques se dirigen contra la información de la empresa, así como de los soportes de almacenaje y de los canales de transmisión, el objetivo último que tiene la resiliencia es precisamente proteger esa información diseminada por la cadena de valor.

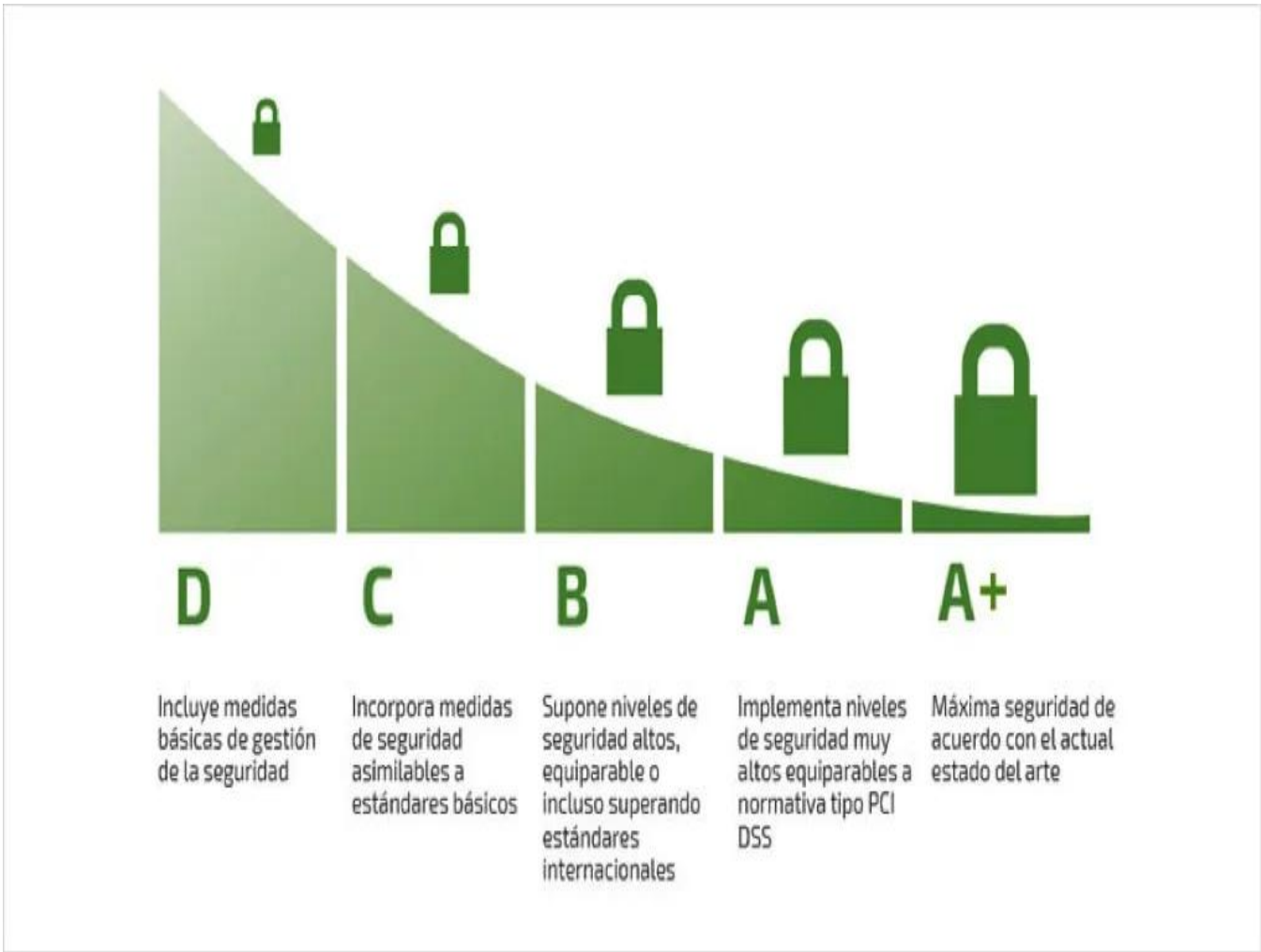
Gestionar como propio el riesgo de los proveedores

La gestión de los ciberriesgos de la cadena de valor no es sino asumir como propio el riesgo de sufrir un ataque al que pueden estar expuestos nuestros proveedores. Ello implica llevar un control y establecer un nivel de exigencias en materia de seguridad equivalentes a los que se imponen a las distintas áreas internas de la compañía.

La estrategia de ciberseguridad lanzada por la Comisión Europea en 2013 ya planteaba el desarrollo de estándares que certifiquen el grado de desempeño de las empresas en el campo de la ciberseguridad. Se trata de etiquetas que garantizan que los sistemas y aplicaciones de un determinado proveedor cumplen con un nivel de protección requerido.

Existen estándares, como ISO/IEC 27001, cuyo fin es establecer los requisitos necesarios para crear, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información. Sin embargo, la empresa LEET Security ha ido más allá, y en 2010 creó el *sello LEET*, que evalúa y califica el nivel de ciberseguridad que implementa un proveedor en el servicio calificado que lo exhibe. Se trata de un sistema que está reconocido por la European Agency for Network and Information Security y que está inscrito como mecanismo de confianza en el Instituto Nacional de Ciberseguridad (INCIBE).

La puntuación que otorga LEET tiene tres dimensiones: confidencialidad, integridad y disponibilidad. Cada uno de estos aspectos recibe una letra que equivale a un determinado nivel de seguridad, como aparece reflejado en el gráfico siguiente:



Fuente: LEET Security. *https://www.leetsecurity.com/niveles-calificacion/*

De esta forma, una compañía puede establecer unos niveles mínimos de ciberseguridad (no tiene por qué ser A+ en los tres conceptos) a los suministradores de su cadena de valor, gestionando de esta forma el riesgo y minimizando, en la medida de lo posible, las vulnerabilidades que estos pueden presentar.

Ciberseguros, una forma de transferir el riesgo

De acuerdo con el Instituto Nacional de Ciberseguridad (INCIBE), existen cuatro formas de tratar un ciberriesgo: evitarlo, mitigarlo, aceptarlo o transferirlo. Los ciberseguros, una figura cada vez más en boga, corresponden a la cuarta categoría. Son definidos por la firma de ciberseguridad Eleven Paths como *la última línea de defensa*, que es complementaria – pero no sustituye- a las políticas de protección de la información y los sistemas llevadas a cabo por la empresa.

Como en otros tipos de seguros, una póliza que cubre ciberriesgos vincula y obliga legalmente a pagar a una empresa aseguradora ante la ocurrencia de una serie de eventos previamente definidos contractualmente, que hayan causado daños o pérdidas al asegurado.

La cobertura de un ciberseguro típico suele incluir conceptos como:

- Responsabilidades ante terceros: procedimientos regulatorios, defensa, perjuicios, multas regulatorias…
- Daños propios que impliquen pérdidas económicas para el asegurado.

- Servicios de crisis, es decir, gastos pagados a expertos por servicios como gestión de crisis y publicidad, asesoramiento legal, investigación forense y respuesta a afectados.

A pesar de que el mercado actual de ciberseguros se concentra en Estados Unidos, se espera que esta práctica se extienda por Europa a lo largo de la próxima década y que, incluso, pueda llegar a ser obligatorio, como sugirió recientemente Gabriel Bernardino, presidente de la autoridad europea de los seguros, Eiopa. Se calcula que las primas en todo el mundo podrían alcanzar el valor de 20.000 millones de dólares en 2025.

Fotografía de Pixabay en Pexels

Davis, A. (2015) "Building Cyber-Resilience into Supply Chains" en *Technology Innovation Management Review*, pag. 23. Disponible en: https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=28

European Commission (2013) "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". Disponible en: Http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206225%202013%20INIT

Hiscox (2019) "Hiscox Cyber Readiness Report 2019".

INCIBE (2017) "Gestionar el riesgo de los proveedores como propio" en *Incibe-cert*. Disponible en: https://www.incibe-cert.es/blog/gestionar-el-riesgo-los-proveedores-propio

Instituto de auditores internos de España (2016) "Ciberseguridad. Una guía de supervisión". Disponible en: https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

Korolov, M. (2019) "What is a supply chain attack? Why you should be wary of third-party providers" en *CSO*. Disponible en: https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html

LEET Security (2019) "II Estudio Empresas y Ciberseguridad. La otra cara de la digitalización: ¿es segura nuestra cadena de valor?"

Olasvrud, T. (2014) "11 steps attackers took to crack Target" en *CSO*. Disponible en: https://www.csoonline.com/article/2601021/11-steps-attackers-took-to-crack-target.html

Ponce de León, M. (2019) "El supervisor europeo abre la puerta a la obligatoriedad de los ciberseguros" en *Expansión*. Disponible en: http://www.expansion.com/empresas/banca/2019/03/07/5c80277122601d7b6b8b45e8.html

PwC (2015) "Insurance 2020 & beyond: Reaping the dividends of cyber resilience". Disponible en: https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

Ragan, S. (2017) "Equifax says website vulnerability exposed 143 million US consumers" en *CSO*. Disponible en: https://www.csoonline.com/article/3223229/equifax-says-website-vulnerability-exposed-143-million-us-consum

ers.html

Signaturit (2018) “Ciberseguros: protección y defensa en el tratamiento de datos”. Disponible en: https://blog.signaturit.com/es/ciberseguros-ante-las-exigencias-del-reglamento-general-proteccion-datos

Thiber (2016) “Ciberseguros. la transferencia del ciberriesgo en España”. Disponible en: https://www.elevenpaths.com/wp-content/uploads/2016/04/Informe_Ciberseguros_Thiber_ElevenPaths.pdf