



Evaluación de la madurez en materia de seguridad y buenas prácticas en organizaciones del sector

INTRODUCCIÓN

Dirigir una empresa en el siglo XXI se parece mucho a nadar entre tiburones. El peligro es evidente: los cibercriminales se vuelven más poderosos, organizados y colaborativos con cada día que pasa. Aun así, las organizaciones se ven obligadas a nadar en el océano de la transformación digital, lo cual se está convirtiendo en una inquietud vital para los CEO de hoy en día. Sin embargo, esto implica adentrarse todavía más en aguas infestadas de tiburones.

Las tecnologías de la transformación digital (Big Data/análisis de datos, computación en la nube, movilidad y social business) dejan a las aplicaciones corporativas fuera de la seguridad de los controles perimetrales existentes en los terminales y en la red. Para los profesionales de la seguridad, esto supone una pérdida de visibilidad y control. Ya no es solo que estemos nadando en aguas turbias, sino que la puerta de esa jaula a prueba de tiburones que antes solía protegernos se ha abierto ahora de par en par.

Evitar la transformación digital no es una opción. Tan solo hay que mirar ejemplos de empresas como Blockbusters y Borders, que no han sido capaces de adaptarse a la nueva realidad y ser conscientes de sus implicaciones. Más bien, es preciso un cambio radical tanto en el enfoque tecnológico como en la mentalidad estratégica. Este informe tiene como objetivo descubrir las buenas prácticas de las que hacen gala las empresas del sector que tienen un enfoque más maduro en materia de seguridad. A fin de poder nadar entre tiburones, y tal vez incluso ser capaz de devolver los ataques, es preciso adoptar una nueva perspectiva.

UTILIZACIÓN DE ESTE INFORME

Este informe pretende ayudarle a comprender las características y la progresión de la madurez en materia de seguridad. En él se identifican ejemplos de buenas prácticas que puede seguir para mejorar su madurez en el ámbito de seguridad. Asimismo, se destacan los aceleradores de la innovación que influyen de manera particularmente notable en el aumento de los niveles de madurez. Por último, se ofrecen recomendaciones sobre cómo mejorar la posición de su empresa con respecto al resto de organizaciones del mismo sector. Estas reflexiones provienen de una encuesta, realizada en el verano de 2016, a 500 altos ejecutivos del sector de la seguridad en Francia, Alemania, Italia, España y Reino Unido.

PERFIL DE MADUREZ DE LAS EMPRESAS DEL SECTOR

De acuerdo a nuestra encuesta a 500 altos ejecutivos del sector de la seguridad, IDC ha dividido el mercado en cinco categorías de madurez. De menos a más, las categorías son las siguientes:

- ad-hoc**
- oportunista**
- repetible**
- gestionada**
- optimizada**

Las empresas se distribuyen, como suele ser lo normal, en una clásica "curva de campana", como puede apreciarse en la Figura 1

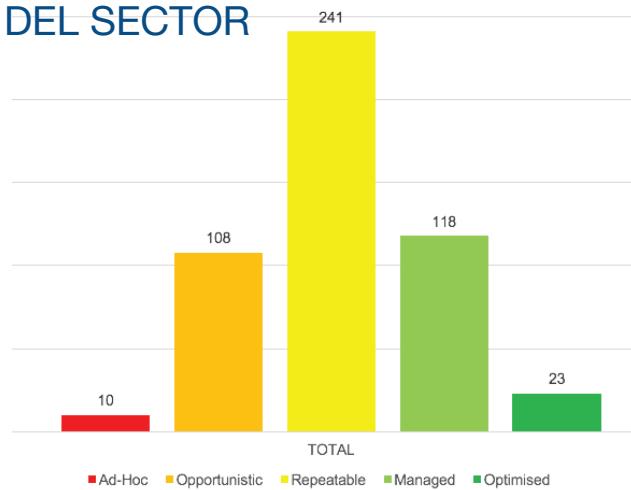


Figure 1

Fuente: IDC, 2016

En lo que respecta al enfoque sobre seguridad, hay muy pocas organizaciones de este sector que estén situadas en el extremo inferior, al igual que ocurre en el extremo superior. En cambio, la mayoría de empresas del sector se encuentran en un término medio. Si su empresa pretende nadar entre tiburones sin llevarse un escarmiento, debe aspirar a superar a las empresas de su mismo sector y adoptar buenas prácticas lo antes posible. La siguiente sección de este informe da una indicación de cuáles esas prácticas en materia de seguridad.

BUENAS PRÁCTICAS EN EL ÁMBITO DE LA SEGURIDAD

Tradicionalmente, el objetivo de la tecnología de seguridad ha sido el de proteger a las empresas frente a las amenazas conocidas. Al situar a los dispositivos, las aplicaciones y los datos detrás de la red de seguridad del cortafuego, los controles perimetrales existentes a nivel de dispositivo y red podían mantener a raya esas amenazas conocidas. Sin embargo, existen dos tendencias que están haciendo que estos modelos preventivos de seguridad sean insuficientes como enfoque independiente:

- Digital transformation is taking corporate applications and data beyond the perimeter, and outside the visibility and control of in-house security teams.
- La magnitud de las amenazas no tiene precedentes. Cada día aparecen más de un millón de nuevas variantes de software malicioso, y es sencillamente imposible generar firmas a un ritmo lo suficientemente rápido como para mantener las defensas tradicionales que tratan de bloquear nuevas amenazas.

Es evidente que hacen falta nuevos enfoques que ayuden a las empresas a identificar amenazas desconocidas y responder ante ellas, así como a bloquear las conocidas. La seguridad debe hacerse proactivamente y buscar indicadores potenciales de amenaza que se puedan corregir, en lugar de esperar a que un ataque se vuelva evidente. Sin embargo, para ello hace falta adoptar una nueva mentalidad en la estrategia de seguridad. En la Figura 2 puede apreciarse un análisis muy ilustrativo de los factores que se considera que limitan la eficacia de la seguridad en función de los niveles de madurez.

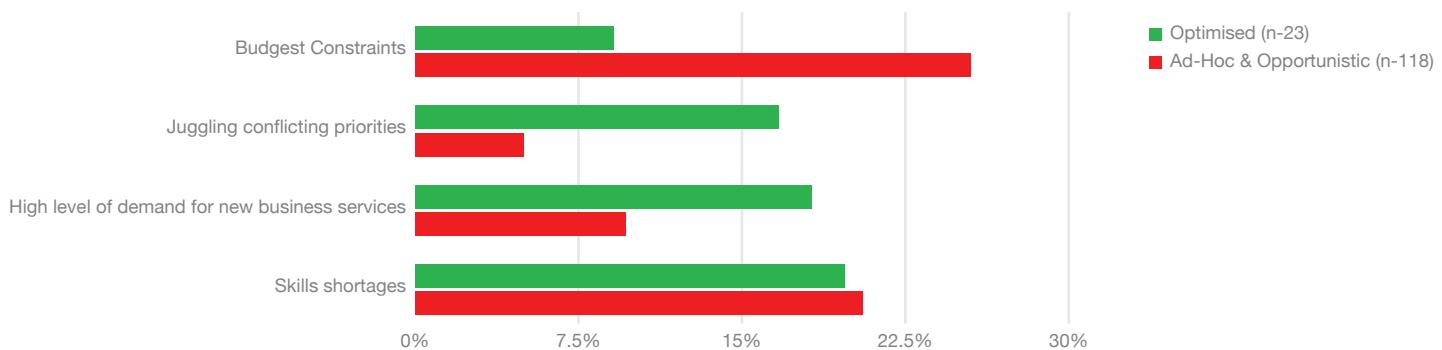


Figure 2

Fuente: IDC, 2016

Hay ciertos aspectos comunes que se aplican a todos los niveles de madurez. Concretamente, las principales limitaciones son el coste y la falta de talento. Esto no es ninguna sorpresa dada la escasez generalizada de talento que se da en el mercado de la seguridad. Sin embargo, es el grado de atención que se le preste al resto de preocupaciones lo que hace aflorar la comprensión sobre buenas prácticas.

En los niveles más bajos de madurez, las presiones en cuanto a costes y la falta de talento son las principales preocupaciones. Pero a niveles más altos, existe un mayor equilibrio entre estas áreas y cuestiones como la gestión de conflictos entre prioridades y el respaldo a la demanda de nuevos servicios comerciales. Esto pone de relieve un cambio drástico de mentalidad: en lo que respecta a la seguridad, una buena práctica es tener en cuenta las necesidades de la empresa.

Una vez asumido este cambio, las empresas deben valorar lo que ello significa desde el punto de vista de los enfoques en materia de seguridad práctica. En particular, es preciso alejarse de los modelos de seguridad reactiva y dirigirse hacia una seguridad proactiva. De hecho, como se muestra en la Figura 3, hay dos tendencias claras en función de las técnicas de madurez. Cuanto más madura es una empresa, es menos probable que no esté utilizando técnicas de seguridad proactivas, y es más probable que ya las esté planificando o utilizando.

Adopción de seguridad proactiva por nivel de madurez

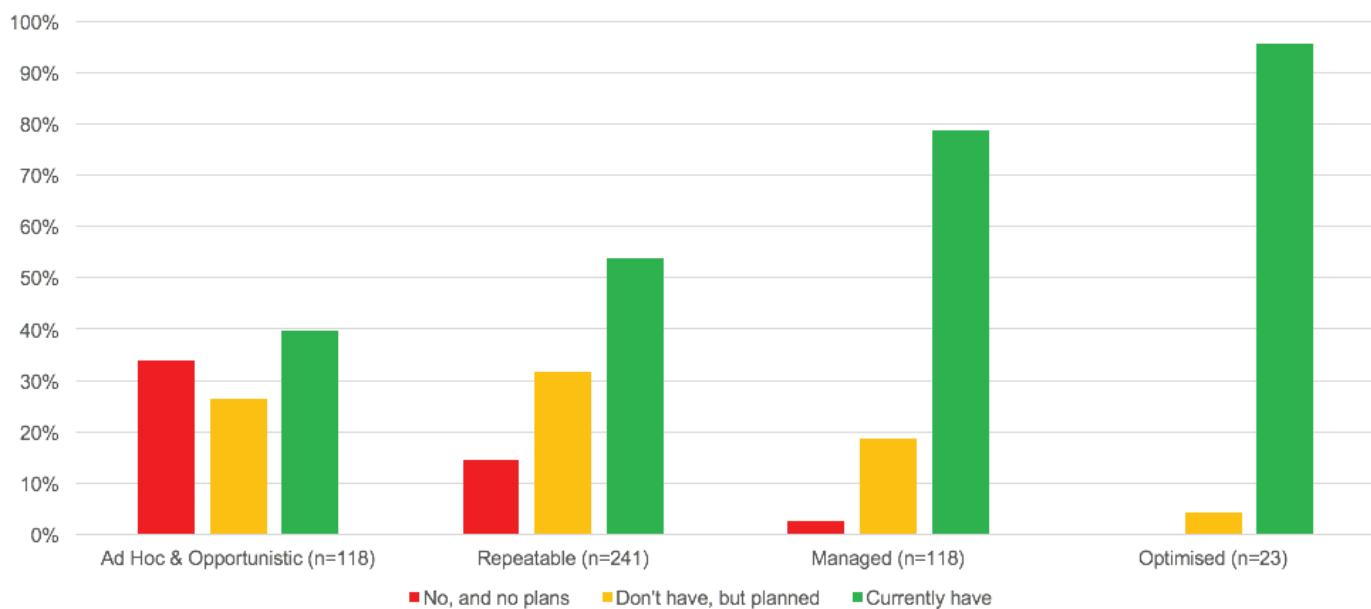


Figure 3

Fuente: IDC, 2016

Según nuestra encuesta, las principales tecnologías de seguridad que las empresas pueden adoptar para facilitar estos enfoques más proactivos son las siguientes: información sobre amenazas, inteligencia artificial y análisis heurístico del comportamiento del usuario. Como ocurre con las tecnologías proactivas, cuanto más maduro sea el enfoque de una empresa en cuestión de seguridad, más probable es que utilice soluciones como inteligencia artificial y análisis heurístico.

Aunque los enfoques proactivos sobre seguridad suponen una oportunidad para avanzar en la escala de madurez en materia de seguridad, también traen consigo sus propios desafíos. Por ejemplo, las técnicas proactivas requieren de la recopilación y supervisión de registros operacionales y de comportamiento en una escala mucho mayor. Dadas la presión a la que están sometidos los equipos de seguridad en lo que respecta a los recursos financieros, es preciso llevar a cabo un profundo análisis de las técnicas que contribuyan a aliviar las tensiones sobre los recursos internos. Las buenas prácticas muestran dos opciones posibles.

OUTSOURCING

Aunque la seguridad empresarial es compleja, la tónica general es mantener el control de la misma a nivel interno. Hay una serie de factores que contribuyen a ello. Para empezar, se considera que la seguridad es una actividad vital y cualquier externalización amenaza con reducir la visibilidad y el control que los equipos internos mantienen con respecto a la seguridad. Los proveedores de servicios de seguridad gestionados (PSSG) han hecho grandes promesas en el pasado, pero estas no siempre se han hecho realidad. Por último, los equipos internos pueden llegar a considerar el recurrir a tercera empresas como una admisión del fracaso y la constatación de que no son capaces de hacer el trabajo por sí solos.

Sin embargo, en un mundo interconectado, ninguna empresa por sí sola puede hacer frente a las amenazas. Esto es especialmente cierto cuando las empresas europeas poseen limitados recursos en cuestión de seguridad, y además existen otras empresas que cada vez están mejor posicionadas para prestar asistencia gracias a, por ejemplo, sus negocios a escala mundial, sus modelos de suministro industrializados y un mejor acceso a personal cualificado. Por lo tanto, para aquellas empresas que aspiran a adoptar buenas prácticas en materia de seguridad, los SSG son un factor importante a tener en cuenta.

Aunque los SSG pueden ser una herramienta útil para aliviar la presión a la que se someten los recursos internos, no puede ser la única respuesta. Un estudio de IDC indica que, en lugar de recurrir al outsourcing integral, la mejor opción reside en encontrar un equilibrio entre la prestación de servicios interna y los SSG, de modo que se atiendan tanto los objetivos empresariales como la disposición de la empresa al riesgo. Preservar las capacidades internas de las operaciones en materia de seguridad es importante para entender el impacto estratégico de las decisiones empresariales en cuestiones de seguridad, y viceversa. Dado que la seguridad está cada vez más orientada a la gestión de riesgos y constituye una preocupación que afecta a la organización en su conjunto, esta es una característica fundamental de las buenas prácticas en el ámbito de la gestión empresarial, cuanto más de las prácticas de seguridad.

AUTOMATIZACIÓN

Además de los SSG, otro instrumento clave para que las empresas puedan afrontar la presión sobre los recursos y el desequilibrio entre la transformación digital y el panorama cambiante de las amenazas es la automatización. La automatización hace posible que se pueda llevar a cabo la gestión, e incluso la ejecución, de las operaciones de seguridad mediante productos de tecnología. La participación del personal interno ayuda a mantener la visibilidad y el control sobre la seguridad.

Esto tendrá consecuencias para la aparición de la inteligencia artificial y la computación cognitiva en el ámbito de la seguridad, que tiene como objetivo ceder la toma de decisiones a las máquinas para aliviar aún más la presión sobre los recursos. Sin embargo, está claro que las buenas prácticas (al menos por el momento) supondrán mantener un cierto grado de supervisión humana para asegurar el buen funcionamiento de las máquinas, o evitar que las decisiones más críticas las tomen robots.