DANIEL LARGACHA

Director del Centro de Ciberseguridad de ISMS Forum
Head of CCG-CERT MAPFRE

Daniel Largacha Lamela es Global Control Center Assistant Director en MAPFRE, puesto en el que confluyen en el plano operativo los ámbitos tradicionales de seguridad física y seguridad de la información. Asímismo Daniel colabora en los subgrupos de Cyber-riesgos del CROF (Chief Risk Officer Forum de entidades aseguradoras europeas) y de transformación digital del EFR (European Financial Services Round Table).

La carrera de Largacha ha estado siempre vinculada a las Tecnologías de Información principalmente en el ámbito de la Seguridad, actividades que ha desarrollado en grandes empresas como Telefónica, Deloitte, y Azertia. Largacha es Ingeniero Superior en Informática por la Universidad Politécnica de Madrid y Máster en Dirección Aseguradora por el ICEA (Investigación Cooperativa de Entidades Aseguradoras y Fondos de Pensiones).

El estado de la ciberseguridad en España

La base del estado del bienestar en la sociedad actual está arraigada en pilares como la sanidad, la educación y la satisfacción de las necesidades básicas, pero además está también ligado necesariamente a algunos aspectos más básicos como el agua corriente, el suministro eléctrico que por lo esencial de su naturaleza (en la sociedad actual) pasan inadvertidas. Con la ciberseguridad, nos ocurre algo parecido, es una cuestión que está intrínsecamente relacionada con la tecnología, aunque a diferencia de lo comentado anteriormente, es completamente intangible y su ausencia puede pasar desapercibida o no apreciada hasta que realmente se hace evidente y necesaria.

Lo cierto es que, gracias a la adopción de la tecnología por parte de los individuos en los años 90

El concepto de seguro no existe y no es algo propio de la tecnología

con la aparición de Internet en los hogares, los ordenadores personales tomaron un nuevo hueco, motivando la primera burbuja tecnológica. En el ámbito de la ciberseguridad, la rápida expansión de la tecnología tuvo efectos negativos, debido a que el objetivo de la entrega primó sobre otros requisitos frente a la ciberseguridad. Algunos fabricantes atendiendo al riesgo potencial en el que nos encontrábamos inmersos, decidieron entonces cambiar sus estrategias de desarrollo de productos limitando su expansión y elevando el peso de los requisitos de ciberseguridad.

En la situación actual, el número de ordenadores ha aumentado geométricamente con la introducción de los smartphones, tablets, dispositivos IoT (que entran dentro de lo que se entiende por un ordenador), hasta el punto de que en los países desarrollados se ha pasado de uno por hogar a más de uno por persona. Esta tendencia ha despertado el interés de todos los sectores, cuestión que podemos ver en la "smartización" de bienes de consumo no vinculados históricamente con la informática, como por ejemplo los electrodomésticos (neveras, lavadoras…), automóviles, etc.

Sin embargo, en el ámbito de la ciberseguridad, aunque también se ha despertado cierto interés, mejorando en términos relativos, el crecimiento no ha seguido la misma proporción, y su evolución no ha ido necesariamente en la misma medida que la tecnología. Para ayudarnos a entender bien el escenario vamos a exponer cuales son los principales factores que influyen sobre este:

- **El concepto de seguro no existe y no es algo propio de la tecnología.** En muchos ámbitos no hablamos de ignífugo o impermeable sino realmente de resistente al fuego o resistente al agua. En la tecnología hay que partir de la base que el software es imperfecto per se, por lo que nunca podemos asegurar con certeza que un sistema es seguro.
- **Mayor exposición:** la aparición y conexión a una red global de miles de millones de nuevos dispositivos cuyo funcionamiento está basado en software (imperfecto) aumenta la posibilidad de éxito que tendría un potencial atacante.
- **La falta de equilibrio que existe en escenarios de proteger versus atacar.** La globalización y la conexión desde cualquier punto del mundo muestra un escenario desigual a la hora definir estrategias o medidas de protección frente a posibles ataques.
- **Aumento de tamaño de la amenaza, debido principalmente a dos factores.** El aumento de los "actores" que destinan sus esfuerzos a atacar y la mayor sofisticación de estos ataques.

A todos estos factores además hay que añadirle el más importante, y es la dependencia actual que tenemos tanto la sociedad en su conjunto, como

DOLPHINATTACK, O LOS FALLOS DE SEGURIDAD DE SIRI, ALEXA O GOOGLE NOW

Se trata de susurrar, de hablar tan bajito que el oído humano no lo detecte, pero sí los micrófonos de los dispositivos móviles. Se trata de hablar por debajo de los 20kHz. Después de esto basta con decir "activar modo avión" para que el usuario quede desconectado de la red; o susurrar la dirección de una página web para acceder a una que pudiera ser maliciosa. Por ahora es un estudio, una prueba de concepto, pero quién sabe.

La aparición y conexión a una red global de miles de millones de nuevos dispositivos cuyo funcionamiento está basado en software aumenta la posibilidad de éxito que tendría un potencial atacante

las personas de manera individual sobre las tecnologías de información. La tecnología juega hoy un rol crítico en todo lo que hacemos en nuestro día a día, y nadie es ajeno a ello. Desde que nos levantamos y encendemos la luz del dormitorio, hasta que bebemos el último vaso de agua. Tanto gobiernos como empresas son conscientes de la sensibilidad del escenario actual, y desde ambos frentes se trata de mejorar lo máximo posible este escenario, que pasa inexorablemente por sensibilizar a los principales grupos de interés (ciudadanos, accionistas, consumidor, empleados… etc.).

La situación actual requiere el compromiso por todas las partes, gobiernos, empresas y la sociedad. La comprensión y aceptación de la situación es uno de los factores críticos de éxito. El otro es el consenso de los compromisos en seguridad que sean necesarios acometer. Un elemento catalizador que puede favorecer la aparición y persistencia de estos factores críticos de éxito es el papel que juegan las asociaciones como el ISMS, ya que pueden acercar las posturas de éstos, así como facilitar recursos, actividades, o capacidades desde una posición más neutra que facilite el entorno de colaboración.

La rápida expansión de la tecnología tuvo efectos negativos, debido a que el objetivo de la entrega primó sobre otros requisitos frente a la ciberseguridad

Existen tres pilares sobre los que los que se puede cimentar una mejora sostenible del escenario actual:

- **La mejora de la capacidad de las organizaciones: aumentando la capacidad de detección y prevención ante un ataque para una entidad, es un aspecto crítico que puede permitir el bloqueo o minimización del ataque.** Para este punto la colaboración entre entidades en la compartición de información de eventos que puedan ser dañinos posibilita que el resto de entidades puedan estar preparadas ante eventos similares.
  Otro factor que afecta directamente a la capacidad de reacción de las organizaciones tiene que ver con los planes de respuesta y gestión de crisis ante incidentes de seguridad. Estas situaciones requieren de la toma de decisión de alto calado, en periodos de tiempo críticas, una buena preparación de estos escenarios minimiza los impactos que pueden tener los incidentes de seguridad en las organizaciones.
- **El fomento de la seguridad: tanto en la sociedad en su conjunto, tanto a individuos como organizaciones empresariales.** La creación de escenarios de colaboración a través de los cuales las organizaciones puedan compartir sus experiencias y necesidades con otras organizaciones, de forma que se optimicen esfuerzos tanto internos como externos, potenciando su capacidad de influencia en la sociedad.
- **La capacitación y especialización de profesionales: enfocados en la seguridad de la tecnología.** Tanto universidades, como entidades privadas deben de facilitar a la sociedad la creación de perfiles con capacidad suficiente, que abarquen todos los ámbitos, desde los perfiles más técnicos, pasando por perfiles de especialistas en procesos y gestión, hasta perfiles directivos.

Enlaces de interés...

- ISMS Fórum
- Incibe