ENERO 2021

AUTOR: ANA LÓPEZ POLINARIO

Nº 383

FICHA TÉCNICA

Título: El estado de la ciberseguridad en España. Digitalización, teletrabajo y ciberataques en tiempos de pandemia

Año: 2020

Fuente: Deloitte

Nº de páginas: 42

Acceso/coste: Gratuito

Localización: Disponible en el siguiente link

CONCLUSIÓN PRINCIPAL

La pandemia del **Coronavirus** ha hecho necesaria la **aceleración de la digitalización de muchos servicios y la generalización del teletrabajo**.
Esto ha planteado importantes **retos y desafíos**, sobre todo en torno a la ciberseguridad, ya que **otro de los efectos inmediatos provocado por el Covid-19 ha sido el incremento de los ciberataques**, que han llegado, incluso, a triplicarse. Ejemplo de ello ha sido la virulenta y cuantiosa campaña de **ataques informáticos contra el sector farmacéutico y los laboratorios de investigación** para acceder a información confidencial y datos relevantes sobre las vacunas antes de su puesta en marcha.

En cuanto al teletrabajo, los ciberdelincuentes aprovechan la **fragilidad de las redes domésticas y dispositivos personales** para acceder a los sistemas de información corporativos. Lo que ha puesto de manifiesto la **vulnerabilidad de muchas empresas**. De hecho, el informe expone que el **76% de las empresas españolas han sufrido entre uno y dos ataques al año,** sobre todo en sectores como el de la administración, el de la salud y el de los seguros. Consecuentemente, surge la apremiante **necesidad de proteger los equipos digitales y la formación profesional en ciberseguridad** para mitigar el riesgo de esos ataques cibernéticos. Un dato que lo corrobora es que **el 91% de las empresas encuestadas cuenta con un Comité de Seguridad.**

Este estudio puede resultar de gran utilidad para conocer el estado de la ciberseguridad corporativa en España y, sobre todo, porque constituye **un estándar de seguridad informática** que permite obtener una referencia externa para aquellas empresas que deseen y necesiten **definir una estrategia de seguridad.**

AUTORÍA

El informe "El estado de la ciberseguridad en España. Digitalización, teletrabajo y ciberataques en tiempos de pandemia" ha sido elaborado por Cyber Strategy Transformation and Assessment, un equipo de trabajo especializado en ciberseguridad de Deloitte, una de las empresas de servicios profesionales más importantes del mundo, considerada de las llamadas "Cuatro Grandes Auditorías", que tiene presencia en 150 países.

La compañía ofrece servicios que giran en torno a cinco ámbitos funcionales: consultoría, asesoría jurídica, impuestos, asesoría financiera y auditoría. Además de la elaboración y publicación de informes.

DESCRIPCIÓN Y CONTENIDO

El informe se propone dar respuesta y resolver algunas de las dudas y preocupaciones de los llamados CISOs (Chief Information Security Officer) o directores de seguridad, en un contexto como el actual de incremento de la digitalización, el teletrabajo y las compras online, en términos de ciberseguridad.

Para ello se ha recogido una muestra de más de 60 compañías españolas, teniendo en cuenta la facturación, el número de empleados y el sector de actividad en el que operan. Posteriormente, se han analizado cada una de las siguientes dimensiones: el tamaño de los equipos dedicados a la ciberseguridad; presupuesto y servicios; inversión; modelo de gobierno adecuado; certificaciones, marco de actuación y formación; entornos cloud; revisión de la seguridad y de las nuevas tendencias; entorno regulatorio; incidentes de seguridad; preocupaciones del CISO; el CISO y la pandemia del Covid 19.

Con este estudio, Cyber Strategy Transformation and Assessment (Deloitte) trata de captar una imagen de la situación actual en la seguridad digital empresarial y, paralelamente, servir a las empresas españolas, como una referencia externa sobre las tendencias y la actuación seguidas por el resto de competidores en materia de ciberseguridad.

ESTRUCTURA DEL INFORME

1. Introducción

2. Contenido

3. Muestra tomada para el estudio

4. Principales conclusiones del estudio

OTRAS CONCLUSIONES

La "forzada" digitalización, consecuencia del confinamiento llevado a cabo para contener la pandemia, **ha supuesto un gran quebradero de cabeza para los CISOs**, pues ha cambiado el contexto empresarial y hace **necesario replantear los modelos de ciberseguridad** ante esta nueva realidad.

Del informe, cabe destacar que **el 70% de las organizaciones** encuestadas **contaban con menos de 10 empleados especializados en ciberseguridad en 2019** (menos del 10% de la plantilla), lo que indica que probablemente **hay una externalización de estos servicios.** Asimismo, **una de cada cuatro empresas no realizó ningún tipo de formación.** Sin embargo, **con la pandemia se ha producido un incremento en la formación de los empleados.**

En lo referente al **Comité de seguridad, sólo un 69% de las compañías participan en él.** Además, algunas cuestiones como la privacidad o la seguridad física quedan fuera de las competencias de los CISOs.
Respecto a las certificaciones de seguridad, si bien es cierto que incrementan el valor de los servicios y los productos de las empresas, todavía son percibidas como un factor prescindible. De hecho, **el 60% de las empresas no posee ninguna certificación en ciberseguridad.** Por otra parte, la regulación cobra más importancia cada año, aunque **el 25% de las empresas consideró que la legislación que les afecta es necesaria** y tan sólo el 11% la vio eficaz.

En cuanto a las nuevas tecnologías, **el 96% de las empresas trabajan en entornos cloud**, sobre todo en sectores como el de la Energía, y **el 87% cuenta con dispositivos relacionados con el Internet de las cosas**, especialmente en sectores relacionados con la fabricación.

En relación a los incidentes de seguridad, **en 2019 los sectores de la Administración, la Salud y los Seguros han sido los que reportaron un mayor número de incidentes.** Entre las principales amenazas, destacan el **malware** (software malicioso), **el phishing** (engaño para acceder a información) **y el ransomware** (secuestro de datos que requiere un pago). La pandemia y la generalización del teletrabajo ha complicado la labor de los CISOs. **El 62% de las empresas reconoce que ha sufrido más ataques de los que cabría esperar.** No obstante, **el 79% se sentía preparada para afrontar esos riesgos.**

En cuanto a la inversión, las compañías españolas invierten cada vez más en ciberseguridad. **En 2019, se destinó de media un 9% del presupuesto**, 0,5 puntos más que el año anterior. Sin embargo, **la crisis económica desencadenada por la Covid-19 ha afectado al presupuesto en ciberseguridad, reduciéndose la inversión en el 57% de las empresas estudiadas**, lo cual implicará un serio riesgo en el futuro.