Una opinión personal sobre el estándar PCI DSS

Una vez realizados todos los posts anteriores, ya tengo una idea más amplia de lo que el estándar PCI DSS (*Payment Card Industry Data Security Standard*) propone y también he observado casos en los que el estar certificado con PCI DSS no ha evitado que ocurran acciones fraudulentas en una empresa. Todo esto me ha hecho pensar en lo que pasa cada vez que hago una compra online y, además, en el estado de las empresas con mayor facturación online en España. Por todo esto, me gustaría centrar este post en una opinión personal (basada en datos reales) sobre lo que ocurre en las compras del día a día.

Con la evolución del internet para poder comprar online casi todo lo que queremos, han surgido diferentes empresas dedicadas casi en exclusiva al comercio online y otras empresas que han evolucionado para vender online lo que ofrecen físicamente en tienda. Mirando diferentes artículos en internet, he encontrado uno que mostraba las empresas con mayor facturación online en España[1].

Encabezando la lista tenemos a Amazon liderando el *ecommerce* con unas cifras abrumadoras de 1.301 millones de euros facturados en el año 2017. Si bien es verdad que se han encontrado publicaciones[2] en las que se especifica que el servicio *Amazon Web* Services es PCI DSS compilant, no he llegado a encontrar ninguna publicación que asegure que la página de *ecommerce* lo sea. Aun así, existe un FAQ[3] en el que afirman que sí es PCI compilant aunque únicamente en los servicios que ofrecen.

En segundo lugar nos encontramos el *eccomerce* de El Corte Inglés con ventas por el valor de 684 millones de euros facturados en el año 2017. Haciendo una búsqueda rápida se

puede verificar que esta empresa cumple con el estándar gracias a la pasarela de pago ConexFlow que utilizan[4]. Si bien esos datos fueron recogidos en el año 2007, podemos seguir observando en diferentes páginas actualizadas de la empresa[5] que cumplen con el estándar PCI DSS y, además, con el estándar PA DSS (*Payment Application Data Security Standard)*.

En tercer lugar tenemos PC Componentes, con una facturación de 301 millones de euros en el año 2017. Con un vistazo rápido en su web[6], ha sido fácil encontrar que cumplen con el estándar PCI DSS.

En cuarto lugar tenemos la empresa Mediamarkt, con una facturación de 227 millones de euros en el año 2017. Al igual que ha pasado con la empresa anterior, con una simple búsqueda en su página web[7] ha sido suficiente para encontrar que cumplen con el estándar.

Una vez observados estos datos, he cambiado de misión, me he puesto a buscar empresas de cualquier lugar del mundo que han tenido vulnerabilidades. Si es de esperar que estas empresas a nivel nacional cumplan con el estándar, es de esperar que empresas conocidas mundialmente lo sean y, en mi opinión, deberían tener aún más cuidado que empresas nacionales en lo que al *ecomerce* se refiere.

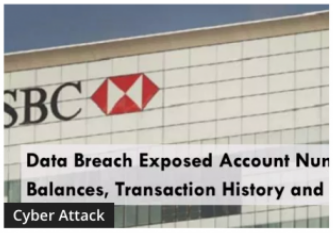
Echando un vistazo en la página gbhackers[8], ha sido muy fácil encontrar diferentes ejemplos de este problema, ¿cómo he dado con esta página? Muy sencillo, soy una persona a la que le gusta comprar maquillaje, una de las empresas americanas en las que suelo comprar es Tarte. Me he puesto a buscar fallos de esta empresa y, tras encontrarlos[9] he podido observar que este sitio guarda aun más noticias relacionadas con el estándar PCI DSS.

Amazon Suffered Data Breach – Customers Name & Email Addresses Exposed

Most Important Steps to Prevent Your Organization From Identity Theft – Detailed Explanation

Nearly 700,000 Plaintext Records of American Express India Customers Personal Info Exposed Online

How To Stop Cyber Criminals to Spy & Track Your Smartphone



HSBC Bank Data Breach Exposed Account Numbers, Balances, Transaction History and Other Details

Radisson Hotel Group Data Breach Exposed Customer's Personal Data

Actualmente, no existe ninguna ley que regule los pagos realizados en *ecommerces* y, se puede observar que los problemas que ocurren cuando se implementan mal estas transferencias (o, directamente, no aplicar ningún tipo de control) hace 'quebrantar' leyes sobre la protección de los datos de los clientes. Vivimos en un mundo en el que las ventas online incrementan todos los años de manera continuada[9] y en el que el robo de datos está a la orden del día. Estamos en el momento propicio para crear leyes que regulen las compras (y el tráfico en general) online. Hay demasiados antecedentes en este sector como para que se empiecen a tomar medidas inmediatamente.

Si bien es verdad que 'los malos' siempre van a existir, ¿no es hora de que 'los buenos' les pongan el trabajo aun más difícil? ¿No es hora de empezar a imponer leyes y acciones para proteger los datos de los ciudadanos de este mundo? ¿No es hora de empezar a controlar el tráfico online de una manera más exhaustiva? Yo creo que sí, yo creo que ya va siendo hora de empezar a tomar cartas en el asunto. Desde mi punto de vista, es hora de coger el estándar PCI DSS y redactar una ley (o las que hagan falta) sobre el mismo y obligar a las

empresas a que la apliquen como es debido. Es hora de crear sanciones para todas aquellas empresas que apliquen mal el estándar y, aún más severamente, de sancionar a todas aquellas empresas que no acojan las leyes creadas.

Referencias:

[1] <<Las cinco tiendas online que más facturan en España>>, Statista, 24 de Noviembre de 2018, https://es.statista.com/grafico/15551/tiendas-online-con-mayor-facturacion-en-espana/

[2] <<Introducción a Amazon Web Services>>, Deloitte, 24 de Noviembre de 2018, https://www2.deloitte.com/es/es/pages/technology/articles/introduccion-a-amazon-web-services.html

[3] <<Is Amazon.com PCI compilant?>>, Quora, 24 de Noviembre de 2018, https://www.quora.com/Is-Amazon-com-PCI-compliant

[4] << Informática El Corte Inglés, primera empresa española en obtener la máxima certificación internacional de seguridad en el pago con tarjetas de crédito>>, El Corte Inglés, 24 de Noviembre de 2018, https://www.elcorteingles.es/informacioncorporativa/es/comunicacion/notas-de-prensa/informatica-el-corte-ingles-primera-empresa-espanola-en-obtener-la-maxima-certificacion-internacional-de-seguridad-en-el-pago-con-tarjetas-de-credito.html

[5] Informática El Corte Inglés, El Corte Inglés, 24 de noviembre de 2018, https://www.iecisa.com/es/que-hacemos/soluciones/Enhanced-Commerce/

[6] <<Condiciones de tarjetas vinculadas>>, PC Componentes, 24 de noviembre de

2018, https://www.pccomponentes.com/condiciones-paytpv

[7] Atención al cliente, MediaMarkt, 24 de noviembre de 2018, https://specials.mediamarkt.es/atencion-al-cliente

[8] GBHackers on security, GBhackers, 24 de noviembre de 2018, https://gbhackers.com/

[9] <<E-Commerce In 2018: Here’s what the experts are predicting>>, Forbes, 24 de noviembre de 2018, https://www.forbes.com/sites/tompopomaronis/2017/12/15/e-commerce-in-2018-heres-what-the-experts-are-predicting/#1552ddf06deb