Coste de la brecha de seguridad en Target y opiniones

Según Target, la brecha de datos costó 252 millones de dólares, de los cuales 90 fueron reembolsados por su seguro y se pudo deducir otros 57 en impuestos (porque sí, las brechas de seguridad son deducibles). De este modo, el coste total para la compañía fue de 105 millones de dólares, el 0,1% de sus ventas.

Sin embargo, este coste podría haber sido inferior, ya que cuando salió por primera vez la norma PCI, Visa y MasterCard la utilizaban para dar a los comerciantes un 'puerto seguro' de sanciones en caso de incumplimiento, cuando el comerciante atacado era compatible con PCI. Pero eliminaron ese 'puerto seguro' justo después de la primera gran brecha. Además, Visa originalmente dijo que los comerciantes, que cumplían con el estándar en el momento en el que sufrieron la fuga de datos confidenciales, estaban exentos de pagar una multa a Visa. Sin embargo, han suavizado la norma indicando que determinarán en cada caso, bajo su opinión, si se imponen multas al comercio afectado. Por ejemplo, Target ha llegado ha un acuerdo con Visa, por el cual se compromete a pagar una multa de hasta 67 millones de dólares dependiendo del número de afectados.

Según Gartner, la norma no se ha mantenido al día con las últimas noticias de ataques y, por ejemplo, ninguna de las aplicaciones anti-malware convencionales que existen en el mercado hoy en día buscan el software malicioso que atacó a Target. Por lo tanto, consideran que es rotundamente equivocado culpar de todo lo sucedido a Target o a cualquier otra entidad que haya sufrido una brecha. Debido a esto, los bancos emisores de tarjetas y la industria de las tarjetas (Visa. MasterCard, Amex, Discover) comparten la responsabilidad por no hacer más para prevenir las debacles que previsiblemente se han producido en los últimos nueve años, cuando comenzaron las primeras grandes brechas.

Venturebeat también añade que los estándares de seguridad de PCI solo consideran el cuidado de los datos en reposo, porque, en 2004, cuando se crearon las normas, el robo de los datos en reposo era el método más fácil y Desde entonces, las aplicaciones de punto de venta y de pago almacenan y abandonan enormes cantidades de registros de datos no cifrados en cada disco duro. Las normas PCI permiten el tratamiento de los datos en texto claro en la RAM de la máquina del punto de venta , así como la transmisión de los datos de las tarjetas sin cifrar a través de las redes locales