El actual Marco de Ciberseguridad del Uruguay, no contempla la protección de los datos en uso.

La seguridad de los datos, tal como se establece en el área PR.SD de la sección 4.2 Función: Proteger (PR) del capítulo 4 Marco de Ciberseguridad (Páginas 21 y 22) del actual Marco de Ciberseguridad del Uruguay, publicado por AGESIC, refiere a la protección de la confidencialidad, integridad y disponibilidad de la información pero tiene una carencia grave.

La subcategoría PR.SD-1 refiere a la protección de datos inactivos o en reposo y la subcategoría PR.SD-2 refiere a la protección de los datos en tránsito, la grave carencia detectada es que no existe una subcategoría que refiera a la protección de la información en uso, y este problema no es siquiera considerado en el borrador de la definición de una estrategia nacional de ciberseguridad.

Al igual que el agua puede encontrarse en la naturaleza en cualquiera de sus tres estados (Sólida en el hielo, líquida en el agua que bebemos y gaseosa en el vapor), los datos en el mundo cibernético se pueden encontrar en cualquiera de sus tres estados (En reposo aquellos datas almacenados para un uso posterior, en tránsito los datos que se envían de un punto a otro y en uso aquellos datos que se encuentran siendo utilizados, creados, modificados o eliminados).

Si ni siquiera se considera la protección de los datos en uso, no habrá forma de evitar que esa información sea robada en una vulneración de la seguridad de acceso a ella.

La inmensa mayoría de la información personal robada mediante ciberataques es justamente información en uso que no está protegida.

Se debe agregar al Marco de Ciberseguridad la protección de los datos en uso mediante el uso de criptografía que asegure su confidencialidad.

Mientras que la protección de los datos en reposo y en tránsito se basa en el uso de criptografía, donde se encripta la totalidad de los datos a proteger (Los datos en reposo en archivos de protegen cifrando la totalidad de cada archivo individual y con los datos en tránsito se procede de manera similar, cifrando cada paquete de datos que se envía de un punto a otro), con los datos en uso se debe proceder de una forma diferente. No es viable cifrar la totalidad de una base de datos y utilizarla en forma cifrada, además de no ser necesario. Lo que se debe encriptar es esa porción de los datos que permite saber a quién pertenecen y refieren el resto de los datos. ¿De qué sirve saber, por ejemplo, que una cuenta bancaria tiene un determinado saldo si no se sabe a quién pertenece esa cuenta? Sin saber a quién pertenece esa cuenta no es posible extorsionar ni al banco ni al propietario con hacer público ese saldo y tampoco es posible disponer de ese saldo al no poder suplantar al propietario.

Una Estrategia Nacional en Ciberseguridad que no solucione esa carencia del Marco de Ciberseguridad actual, tendrá esas mismas limitaciones.

Por Julián Murguía Hughes
julian.murguia@omegakrypto.com