Estrategia Nacional de Ciberseguridad del Uruguay, una buena idea que nacerá renga.

Una Estrategia Nacional de Ciberseguridad que no incluya una estrategia para la protección de la privacidad de la información cuyo acceso busca proteger, es una estrategia que será renga, incompleta, ya que no podrá prevenir el daño causado por el mal uso de información sustraída mediante un ciberataque exitoso o una filtración de datos.

La palabra "Ciberseguridad" no existe en el diccionario de la Real Academia, es una traducción de la palabra "Cybersecurity" del idioma inglés, cuyo significado, según el diccionario Merrian-Webster es: "*Medidas adoptadas para proteger una computadora o un sistema informático (como en Internet) contra accesos no autorizados o ataques*." El mayor problema de la ciberseguridad es que sólo se enfoca en proteger y controlar el acceso a los sistemas y a la información, dejando totalmente de lado la protección del contenido de dicha información de miradas indiscretas.

De manera esquemática podríamos equiparar la ciberseguridad a una guardia perimetral que controla y limita el acceso a un lugar donde se guarda algo que se considera valioso, y trataremos de explicar este concepto mediante un ejemplo práctico.

Vayamos atrás en el tiempo, bastante antes de que existieran las computadoras, vayamos 500 o 1000 años atrás. Aquellos que poseían riqueza protegían su riqueza y su propia integridad construyendo castillos y fortalezas, con gruesos muros y guardias armados que evitasen el ingreso de enemigos. Con el correr del tiempo, los muros se hicieron cada vez más gruesos y más altos, se agregaron fosos y puentes levadizos y se mejoró la técnica y el armamento de los guardias, porque se sabía que si el enemigo conseguía vulnerar las defensas, el daño y el saqueo eran inevitables.

Ya entrado el siglo 21, con la universalización de la informática e internet, la información se transformó en un nuevo petróleo, con su valor superando ampliamente al mismo petróleo y a los metales preciosos. La seguridad física evolucionó a ciberseguridad, construyendo muros virtuales cada vez más altos y gruesos, con fosos cada vez más anchos y profundos (Firewalls) y mejorando la técnica y el armamento de los guardias que controlan los accesos (Autenticación).

Pero, al igual que 500 o 1000 años atrás, cuando el enemigo consigue vulnerar las defensas, el daño y el saqueo siguen siendo inevitables.

El concepto o término más común en los documentos relacionados a la ciberseguridad es "*Mitigación*", la acción e efecto de mitigar, moderar, aplacar, disminuir o suavizar algo riguroso o áspero, tanto cuando se habla de mitigar el riesgo de sufrir un ciberataque como cuando se habla de mitigar el daño causado por un ciberataque.

Por Julián Murguía Hughes
julian.murguia@omegakrypto.com

Es posible mitigar los daños causados por un ataque de ransomware que encripte los archivos de una computadora o un sistema si se disponen de los respaldos de datos adecuados y se puede instalar rápidamente equipamiento nuevo, pero, ***¿cómo se mitiga el daño causado por el mal uso de información robada o filtrada?*** Una vez que información confidencial ha sido sustraída, esa sustracción no puede revertirse, el atacante ya dispone de ella y aunque luego de pagar un rescate extorsivo la información sustraída pudiese ser recuperada, el atacante seguirá disponiendo de ella y podrá utilizarla como mejor sirva a sus intereses.

También debemos tener en cuenta que cualquiera que haya sido víctima de un ciberataque exitoso, volverá a ser atacado nuevamente, sea porque la información robada le sirva al atacante o porque la víctima haya cedido a la extorsión, el atacante sabe que podrá obtener nuevos beneficios de la misma víctima.

No existe la ciberseguridad inviolable, es un hecho que fue claramente demostrado cuando la Agencia Nacional de Seguridad de los Estados Unidos (NSA) fuera hackeada y sus herramientas de espionaje cibernético ofrecidas en subasta pública en la Deep Web unos años atrás.

La mejor ciberseguridad del mundo tampoco puede evitar la acción de un empleado infiel o un infiltrado que robe, extraiga o filtre información sensible que pueda ser utilizada para causar daño.

Pongamos un ejemplo bien uruguayo, la constante filtración y divulgación de información reservada de fiscalía de casos de alto perfil que se encuentran en proceso. Esa información no ha sido obtenida mediante ciberataques sino mediante la acción de empleados infieles que han divulgado información que estaban obligados a preservar y mantener secreta. Si la justicia dispusiese de las herramientas criptográficas necesarias que le permitiesen asegurar la privacidad y confidencialidad de la información digital que poseen, la filtración y divulgación de información reservada podría evitarse.

Una Estrategia Nacional de Ciberseguridad por más moderna y avanzada que sea, será siempre insuficiente a menos que sea sólo un pie para una verdadera ***Estrategia Nacional de Protección de Datos*** cuyo otro pie sea la protección del contenido de la información mediante el uso de criptografía segura, de forma que su contenido no pueda ser leído, comprendido o utilizado por las personas equivocadas. Si se intenta caminar con un solo pie, cualquier tropiezo llevará inevitablemente a una estrepitosa caída.

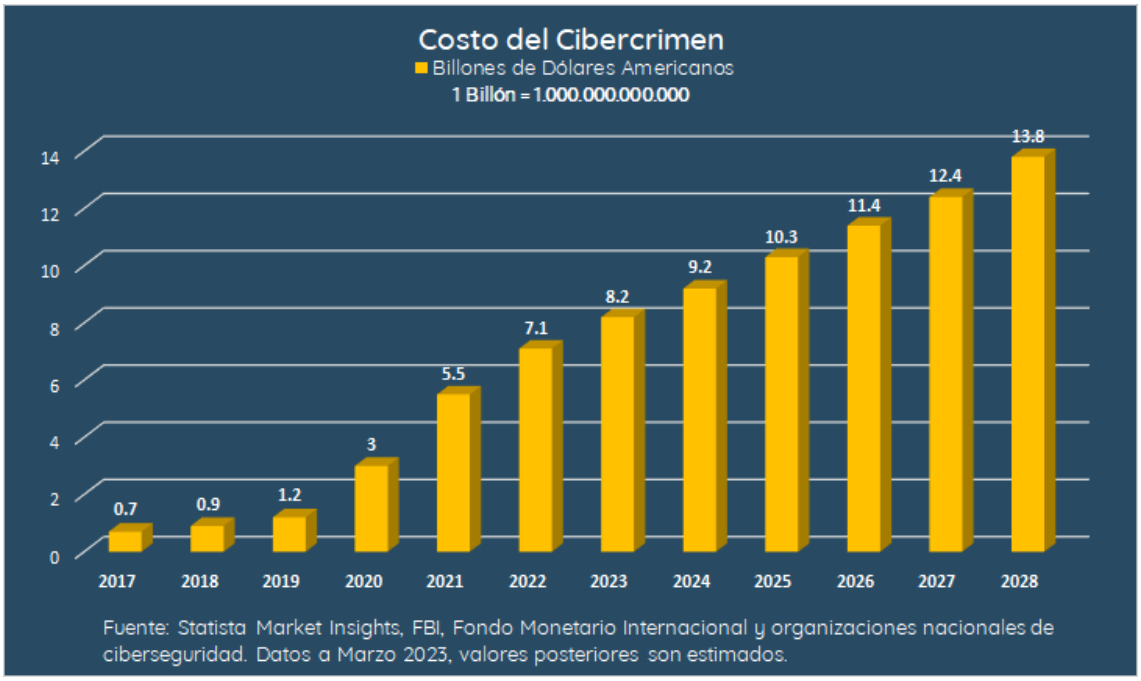
El cibercrimen cuenta con el tiempo y los recursos para invertir en mutaciones cada vez más agresivas de los ciberataques, mientras las empresas y gobiernos del mundo no pueden competir con su inversión en ciberdefensa con la que pueden realizar los cibercriminales para sus ataques. Tal como expresara, en un reciente artículo publicado en el diario El País, Nicolás Correa, gerente del Centro de Operaciones de Seguridad (SOC) de Agesic: **"Siempre corremos de atrás por la velocidad con la que mutan los ataques"**.

Por Julián Murguía Hughes
julian.murguia@omegakrypto.com

En el borrador presentado de esta nueva Estrategia Nacional de Ciberseguridad del Uruguay no se plantea ninguna medida que apunte a dejar de correr de atrás al cibercrimen y tomar la delantera con medidas preventivas que protejan el contenido de la información de forma tal que su robo, sustracción o filtración no permita que esta sea utilizada para causar daño ni otorgue a los atacantes ninguna ventaja que les permita extorsionar con la divulgación de la misma.

A todo esto se suma el daño económico que produce el cibercrimen, representado por el costo de los daños causados. Según analistas expertos, el cibercrimen le costó al mundo aproximadamente ocho billones de dólares estadounidenses en 2023. Eso equivale a un ocho seguido de doce ceros. Un monto que representa más de cien veces el PBI total del Uruguay en 2023.

El costo del cibercrimen crece año a año y se espera que supere los diez billones y medio en 2025, lo que convertiría al cibercrimen en la tercera economía del mundo, solo detrás de Estados Unidos y China.



Los montos expresados no se refieren al daño causado a los computadores y sistemas o al costo de su substitución, el cual es equivalente a los costos causados por una falla de hardware, sino al daño causado por el mal uso de la información robada, sustraída o filtrada y el perjuicio económico que ese mal uso provoca.

Dado que Uruguay, como la inmensa mayoría de los países del mundo, está lejos de poseer el poder económico del cibercrimen para invertir en ciberdefensa, la única opción que nos queda para defendernos es utilizar nuestra inteligencia al máximo para proteger el contenido de la información aún después de que un ciberataque haya tenido éxito, como forma de prevenir el daño que pueda provocar el mal uso de la información robada.

Por Julián Murguía Hughes
julian.murguia@omegakrypto.com

¿Qué pasaría si la información robada o filtrada no pudiese ser leída o utilizada?

Si la información obtenida mediante un ciberataque, un infiltrado o un empleado infiel estuviese protegida mediante una criptografía segura que no pudiese ser vulnerada por el atacante, esa información le sería inútil ya que no podría utilizarla para causar daño, no podría venderla ya que nadie le compraría algo que no puede utilizar, no podría extorsionar con divulgarla, y al final, todo el tiempo, esfuerzo y dinero invertidos en su obtención habrían sido estériles, una pérdida total y absoluta.

Un ciberataque que vulnerase la ciberseguridad pero no pudiese sustraer información utilizable, sería el equivalente a una simple falla de hardware para la víctima y una pérdida de esfuerzo, tiempo y dinero para los atacantes, lo que a su vez tendría efectos disuasivos de futuros ataques.

Hay un viejo aforismo que dice que "*Demencia es seguir haciendo lo mismo y esperar resultados diferentes*". Establecer una estrategia de ciberseguridad sin agregarle ciberprivacidad, es una solución renga, es seguir haciendo lo mismo y si seguimos haciendo lo mismo, jamás podremos obtener resultados diferentes.

Veamos algunos ejemplos prácticos de agregar ciberprivacidad a la cibersguridad:

- Si un ciberataque exitoso a una institución bancaria le permitiese a los atacantes obtener un listado de cuentas bancarias con sus saldos pero los datos personales de los dueños de esas cuentas estuviesen encriptados, al no disponer de las identidades de los dueños de las cuentas, no podrían extorsionar al banco con hacer pública la información robada ni podrían suplantar la identidad de ninguna persona para acceder al dinero en su cuenta.
- Si una empresa tuviese los controles remotos de sus procesos de producción protegidos mediante una criptografía segura, un ciberataque exitoso que permitiese acceder a esos controles, no podría alterar los procesos ni provocar daño a los mismos.
- Si las embajadas uruguayas dispusiesen de las herramientas criptográficas adecuadas, sus comunicaciones no podrían ser intervenidas por otros países tal como documentara un artículo publicado hace un tiempo en el diario El País.
- Si se agregase una capa de privacidad criptográfica a las comunicaciones de las fuerzas policiales, las mismas no podrían ser intervenidas ni escuchadas por los criminales.
- Si la justicia dispusiese de las herramientas criptográficas adecuadas para proteger la privacidad de la información digital sobre los casos que investiga, se limitarían radicalmente las filtraciones.
- Si se agregase una capa de privacidad criptográfica a las infraestructuras críticas, se podrían prevenir los daños causados por futuros ciberataques en lugar de intentar mitigar los daños después de ser víctima de ellos.
- Si se agregase una capa de privacidad criptográfica a la información en uso, un robo de datos no daría margen al mal uso de los mismos y evitaría el daño que ese mal uso podría causar.

Por Julián Murguía Hughes
julian.murguia@omegakrypto.com