La prueba del viernes

José de la Peña Muñoz
Director
jpm@codasic.com

Un amigo y experto en ciberseguridad me aseguraba hace tiempo que para mostrar al mundo el poder del cifrado estaban haciendo más los delincuentes con el Ransomware que todos los criptólogos de bien juntos.

No es fácil discutir semejante aseveración a la vista de la notoriedad alcanzada por el ciberataque ejecutado con el "bicho", que ha significado para la sociedad internacional algo así como un plan intensivo y masivo de concienciación: la que más o el que menos ya tiene una idea de que se pueden adueñar de la información que tiene en el ordenador de casa (y lo que ello comporta) y de que para tener opciones de recuperarla, o dispone de copias de seguridad actualizadas o criptoapoquina. (En este caso, y en un primera derivada, en eso consiste el negocio primario de la delincuencia, que saca petróleo del mercado de vulnerabilidades –algunos estados sacan ventajas frente a otros–, de la falta de diligencia profesional de muchos y de la ingeniería social).

El asunto se magnifica cuando el escenario es un centro de trabajo interconectado con otros (empresa o administración pública), como bien hemos podido comprobar. Además de ir cayendo una máquina tras otra y tener que parar servicios (por necesidad unos y por si acaso otros), algunas personas remitieron por mensajería móvil unas magníficas fotos del ya célebre pantallazo, y archivos de audio y video, calentando de paso las redes sociales. Es evidente: el hecho constituyó una de las supremas expresiones del *gardneriano* Shadow IT, y la puesta en marcha de un eficiente sistema viral de propagación de alarma, que dejó en precario los planes corporativos de gestión de crisis de más de una organización, antes incluso de activarse. (No sé si funcionaron los sistemas de contacto interpersonal entre CIOs, CISOs, CERTs y SOCs de proveedores en el contexto de sistema de Ciberseguridad Nacional; el caso es que ese día andaba todo el mundo… ¡comunicando!).

Con la notoriedad del incidente, su amplitud, la divulgación casi en tiempo real, y la presión mediática, no me imagino que las altas direcciones y los consejos de administración se hayan quedado fríos. Como mínimo, habrán sentido la curiosidad propia de los buenos gobernantes por saber qué ha pasado dentro y fuera de su organización, y si internamente los deberes estaban hechos. Por lo que vamos sabiendo, no está claro que el ciberataque se manifestara un viernes con finalidades recaudatorias. Ateniéndonos a sus efectos conocidos, más pareció provocado para concienciar de lo que se nos puede venir encima por no parchear, por no haber diseñado bien las redes y por la mala custodia de algunos arsenales de vulnerabilidades. ¡Qué será cuando vayan calando las infraestructuras "inteligentes" sin ciberseguridad o avance unos cuantos puntos la "IoTificación" a fuerza de ocurrencias molonas!

> "Con la notoriedad del incidente, la divulgación casi en tiempo real por las redes sociales y la presión mediática, no me imagino que las altas direcciones y los consejos se hayan quedado fríos. Como mínimo, sus miembros habrán sentido la curiosidad propia de los buenos gobernantes por saber qué ha pasado dentro y fuera de su "casa", y si internamente se habían puesto los medios necesarios para tener los deberes hechos."

Como dice un excelente colaborador de SIC, conviene prepararse para evitar que nos secuestren los ascensores de un edificio, las cerraduras de un complejo hotelero, el sistema de gestión de rutas y flotas de un consorcio de transportes… Si sucede, estaremos hablando de seguridad de las personas, de continuidad de negocio, de exposición a demandas, de deterioro del valor de la marca, de castigo en los mercados y de la responsabilidad de las altas direcciones.

El episodio vivido da para una enciclopedia. Mientras que alguien la termina (antes del próximo incidente), traigo a esta sección el vaticinio para 2017 que hizo en el número 123 de esta publicación un excelente profesional. Decía: "…Veremos también el primer ciberincidente en España en entorno industrial (o en algún operador de Infraestructura Crítica) con impacto en el ciudadano". ¿Nos apostamos algo? ●