Servicios en la nube en tiempos de guerra:
El caso de ucrania

Imágen: Wikipedia U.S. Navy photo by Photographer's Mate 2nd Class Greg Roberts

Recuerdo que cuando comenzó la guerra, la mayoría de medios de comunicación señalaron que uno de los principales retos a los que ucrania se iba a tener que enfrentar era al fallo de sus sistemas de información.

Dejando de lado la clarísima superioridad del ejército ruso, el miedo no solo estaba en tierra, sino en el impacto que tendría el sabotaje y la ciberguerra a la hora de que el ciudadano de a pie pudiera acceder a servicios digitales; y ojo, que no hablamos únicamente de estar bien informados, sino de poder estar comunicados, y de que toda la tecnología que está a nuestro alrededor funcione al menos con un mínimo de solvencia para que, por ejemplo, no deje sin luz y/o sin calefacción a millones de ciudadanos.

Obviamente, en los primeros compases de la guerra todo parecía estar en contra de ucrania. más tarde empezaría a llegar la ayuda exterior, y lo demás, como se dice, es historia.

El caso es que de toda la barbarie que nos llega cada vez más dosificado del frente, hay algo que ha quedado palpable: ucrania no ha perdido acceso a la red global, y sus servicios públicos siguen funcionando… ¡pese a que las bombas siguen cayendo!

¿cómo es posible?

Todo ese esperable colapso tecnológico que, salvados muy contados casos, no llegó ni tan siquiera a materializarse. tanto que incluso el presidente de ucrania se ha permitido negar al bueno de Elon Musk su supuesta ayuda con la red satelital, que al comienzo parecía ser el único salvavidas (para los medios, al menos) que tenía el país.

Así pues, hechas las presentaciones, conviene plantearse qué demonios ha pasado para que, en efecto, la hecatombe no haya salpicado a los sufridos ucranianos.

Y la respuesta es sencilla: la nube.

Sistemas en la nube en tiempos de guerra

Ya antes de comenzar la guerra, y sin tantos aspavientos mediáticos como los que llevó a cabo Elon, Amazon comenzó a suministrar al país diferentes kits de "primeros auxilios" para prepararse ante la inminente guerra, y entre esos kits estaban unos dispositivos llamados snowball edge, que básicamente eran maletas cargaditas de discos duros para almacenar de forma segura información y sistemas de infraestructura crítica.

El mismo día que empezó la invasión, amazon, junto con el gobierno ucraniano, pactaron rescatar buena parte de los sistemas críticos del país (sistema bancario, sistema de impuestos, bases de datos de la administración pública…) para alojarla en sus amazon web services.

Parte de ella, directamente subida desde ucrania. otra parte descargada en estos dispositivos, que ofrecen 80 terabytes de datos cifrados cada uno, y transportada en todoterrenos hacia europa, para ya ser subida desde conexiones menos comprometidas.

Y ojo, que no hablamos de un movimiento precisamente sencillo de ejecutar:

"Estamos ante la guerra tecnológica más avanzada de la historia de la humanidad. una guerra que no solo se realiza con armas, sino con datos. amazon web services nos ha ayudado a salvar la economía y el gobierno de ucrania".

Quien dijo este no ha sido cualquier papanatas, sino Mykhailo Fedorov, el vice primer ministro y ministro de transformación digital del país.

En total hablamos de 10 millones de gigabytes portados en tiempo récord en medio de una invasión militar, que se dice pronto. todo el core de la infraestructura que mantenía, y ha seguido manteniendo, el gobierno de Zelensky funcionando. Todo esto por dos motivos principales que conviene recordar.

Asegurar la accesibilidad y escalabilidad de los sistemas

Una vez migrados a AWS, el acceso a servicios ciudadanos y de la administración pública fue asegurado en todo el país. obviamente, sigues necesitando una red operativa para acceder, pero al menos los servidores, al estar en la nube, seguirán funcionando, y como cada vez más dependemos de conexiones satelitales (una tecnología que requiere menor presencia de repetidores en tierra), hay menor exposición a los riesgos clásicos de una guerra (destrucción de infraestructura básica de conectividad).

Ergo, es posible seguir operando en el país ahí donde la infraestructura física puede haber sido destruída. Es decir, se asegura la accesibilidad y la escalabilidad de los sistemas, habida cuenta de que, como es normal, algunos recibirán muchísimas más peticiones que en tiempos normales.

Hacer imposible el robo y/o destrucción

Siempre pongo el mismo ejemplo, pero no está de más recordarlo cada poco:

En 1936 en Holanda se realizó un censo que, además de incluir los típicos datos censales, pidieron además las preferencias religiosas de sus ciudadanos. El objetivo no era otro que el poder destinar de una manera más exacta los recursos económicos para cada religión según el número de adeptos que tuviera.

¿Cuál es el problema de esto?

Pues no hubiera habido ninguno… sino fuera por pocos años más tarde la alemania nazi invadió el país. Cuando llegaron los nazis, ya tenían todo el trabajo hecho.

Solo daré un dato: el 90% de los judíos holandeses murieron en el holocausto.

Sin embargo, cuando rusia irrumpió en ucrania, sus datos y sus sistemas ya no estaban en ucrania, sino en algún otro país (o más bien, en muchos otros países).

De esta manera, no han podido destruir la información, o peor aún, usarla para hacer aún más daño: la nube ha servido para evitar el colapso.

Fíjate tú, lo mismo que ocurrió no hace mucho con la salida forzosa de afganistán por parte del ejército estadounidense, y el abandono de sistemas de identificación biométrica de colaboradores ahora en manos de los talibanes.

¿Y qué hay de la soberanía de los datos?

Llegamos al quid de la cuestión, y es que por si a alguien se le ha pasado por la cabeza, en efecto, con la invasión se tuvo que cambiar la regulación de ucrania para permitir que los datos estatales estuvieran fuera del territorio nacional.

Obviamente, se trata de una medida transitoria y de extrema urgencia. A ningún país (o empresa, o ya puesto, ¿usuario?) le debería gustar que sea un tercero quien tiene control de su información, pero estamos hablando de una guerra, y como pasó por buena parte del mundo en época covid, para tiempos desesperados, medidas desesperadas.

Esta es una de las principales reticencias a abrazar la nube. Que pasamos a delegar la responsabilidad del tratamiento de los datos en uno o varios terceros. para lo bueno (ya no depende de nosotros asegurar su accesibilidad, y no pasa "nada" si en el CDP de mi empresa cae una bomba), pero también para lo malo (ucrania ha tenido que confiar en que amazon, una empresa norteamericana, proteja bien todos sus activos digitales, y no esté por detrás suministrándole información al gobierno de turno y/o pueda cerrarle el grifo y dejarle sin infraestructura mañana).

Por supuesto, la decisión, a la vista de los resultados estos últimos meses, ha sido todo un acierto.

Es probablemente la guerra que mayor cobertura ha tenido de la historia, y parte de los motivos está en el hecho de que sigue llegando sin problemas información de primera línea.

Y la realidad es que lo mismo pasa con todas las empresas que apuestan por migrar sus activos a la nube. tras un periodo de transición, el cambio es a mejor siempre.

Pero claro, hay que tener vocación para realizarlo. o, como ha sido el caso, estar, lamentablemente, obligados a ello…

Autor: Pablo Iglesias

Se describe como un apasionado de la tecnología-Consultor de Presencia Digital y Reputación Online, presidente de la Consultora de Reputación Online CyberBrainers, y fundador, co-fundador, vocal y vicepresidente de varias startups y asociaciones relacionadas con el mundo de la ciberseguridad, la transformación digital y el marketing.

Con más de una década escribiendo a diario en www.pabloyglesias.com, es uno de los mayores referentes en materia de nuevas tecnologías y seguridad de la información de habla hispana.

Desarrolla labores pedagógicas (online y presencial) sobre Presencia Digital y Seguridad de la Información, intentando concientizar a la sociedad sobre los riesgos y oportunidades del tercer entorno.

Actualmente asesora a profesionales, PYMES y grandes empresas sobre cómo obtener valor de la información que circula a su alrededor. El punto medio necesario entre marketing, comunicación y seguridad de la información.