N&Y MAGAZINE - INFORMATICA A BORDO

http://www.informaticaabordo.com

Informática a Bordo

Nuevas Tecnologías aplicadas en Náutica

CAPITULO 124

TELETRABAJO SEGURO DESDE EL BARCO

Hablar de teletrabajo antes de la pandemia era algo poco habitual. Lo usábamos para conexiones puntuales en viajes, o por urgencias fuera del horario laboral. Se sabía que se trataba de una conexión limitada, para salvar la urgencia y las circunstancias. La pandemia nos aportó otra forma de ver el teletrabajo. Pasó, de repente, a ser una herramienta obligada para todo el mundo, gustase o no. A la mayoría les pilló de sorpresa y con pocos medios para afrontarlo de un día para otro. Y para los usuarios supuso también un cambio repentino y forzado en su forma afrontar su desempeño.

¿Cuáles fueron los retos de las compañías en esos momentos?
Los CIO tenían que tomar decisiones urgentes, balanceando operatividad y productividad con protección y seguridad. No se podía permitir que los empleados se conectaran "a cualquier precio", aunque la urgencia provocó auténticas barbaridades en temas de seguridad. Por ejemplo conexiones desde equipos compartidos con la familia, sin antivirus ni protección ante cualquier ataque.

Para el que estaba preparado, y ya tenía recursos de acceso remoto, fue simplemente un cambio de hábitos al tener que quedarse en casa, pero era un cambio en la forma de trabajo, porque ya tenían entornos que permitían combinar trabajo presencial con trabajo remoto. El que trabajaba remotamente con sistemas seguros no tuvo problemas en adaptarse, pero el que no estaba preparado se enfrentaba a un grave problema.

La pandemia fue tan larga que dio tiempo a securizar los sistemas de acceso y normalizar el teletrabajo. Tanto fue así, que muchas empresas han optado por dar continuidad a ese modelo que apareció forzado, y que nunca se habían planteado internamente.

Cuando pasaron los primeros meses de encierro empezamos un recorrido de dos años de incertidumbre, donde se debatía la necesidad real de seguir teniendo una mesa en las oficinas para todo el personal, o simplemente espacios de trabajo comunes, y "mesas calientes" donde, puntualmente, los trabajadores podrías acudir para reuniones u otras tareas que pudieran requerir la presencialidad. Esto provocó que las compañías se plantearan reducir el espacio de sus instalaciones, las inversiones en infraestructuras internas, y abogasen más por invertir en buenas herramientas para que los empleados puedan trabajar eficientemente, y de forma segura. Desde cualquier ubicación. Buenas herramientas y buenos sistemas iban a ser más necesarias y rentables que crecer internamente con equipamiento fijo.

Antes de la pandemia, los responsables de sistemas de las empresas se preocupaban de tener unas infraestructuras robustas, con seguridad perimetral, protegiendo al máximo las instalaciones y los puestos de trabajo de las oficinas. Su preocupación era el puesto de trabajo dentro de cada sede. Las conexiones remotas eran tratadas como excepciones, y se securizaban para su uso puntual. Con el cambio de escenario, esa preocupación cambió y pasó a ser por cada puesto de trabajo en su ubicación externa, esté donde esté. Si una empresa tenía cien personas en tres sedes, por ejemplo, debía proteger y atender esas tres sedes. Con la pandemia pasó a proteger y atender a cien sedes, una por cada empleado que

teletrabaje. Y esas sedes podían ser pisos, casas, barcos … o cualquier escenario remoto con conexión a internet. Eso no importaba, lo que importaba es que pudiera trabajar, y en la medida de lo posible, de forma segura.

Pero ¿qué pasa con la seguridad si la empresa se diversifica en muchas pequeñas empresas? ¿cómo nos aseguramos de que la información confidencial no corre peligro? ¿cómo sabemos que los orígenes de las conexiones están libres de malware y ciberataques? A esta dispersión y crecimiento exponencial de sedes, hay que sumarle esta preocupación. Lo ataques cibernéticos se han multiplicado exponencialmente en los últimos años, y ya no van dirigidos a las infraestructuras, sino directamente al usuario que accede a estas infraestructuras. Los hackers se han dado cuenta que el usuario ha pasado a ser la parte más vulnerable de las empresas, y son su objetivo principal.

¿Cuál es el escenario óptimo de "teletrabajo seguro"?

El teletrabajo ha llegado para quedarse, sin duda, pero este nuevo escenario tiene que cumplir unos requisitos para mantener la productividad y la seguridad. El mejor escenario remoto será el que más se asemeje al modelo de trabajo presencial, donde las infraestructuras están fortificadas y preparadas para ataques externos.

Un escenario óptimo y seguro debe cumplir estos diez requisitos:

1. Facilidad de establecer la conexión
La forma de establecer la conexión tiene que ser fácil, rápida, sin engorros, con uno o dos pasos como máximo. En algunos casos tenemos que pasar por varios sitios para llegar al acceso al que normalmente llegaríamos en un salto, y perdemos tanto tiempo que se nos hace pesado comenzar a trabajar. Tiene que ser igual de rápido que en el puesto habitual de la oficina.

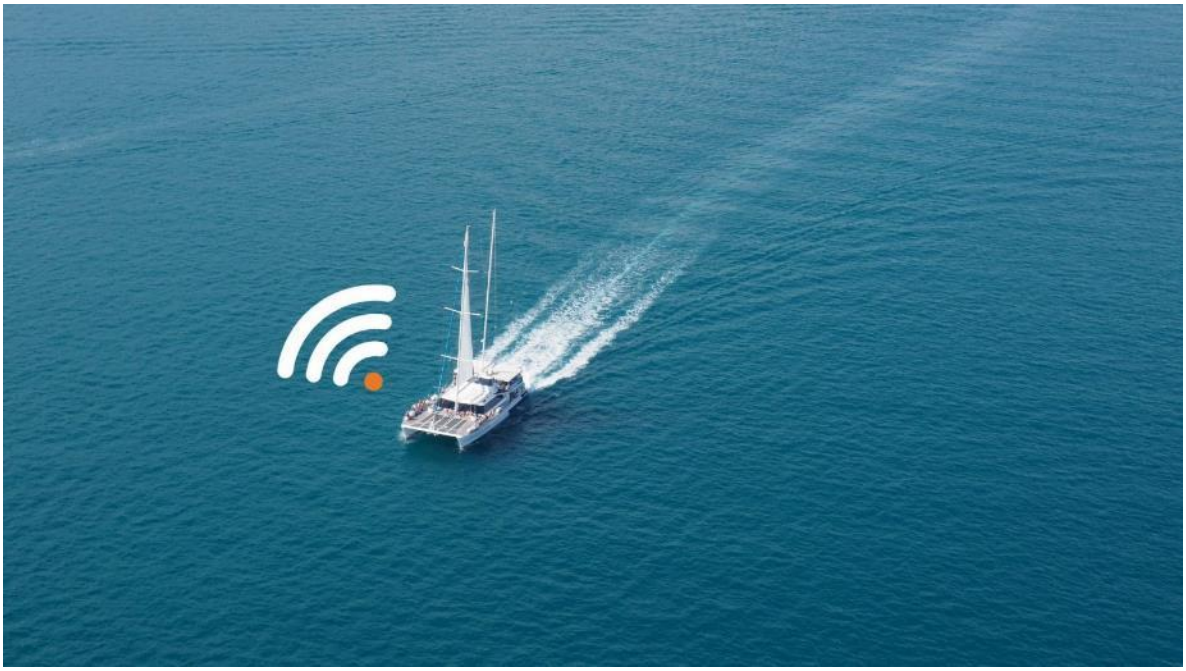
2. Seguridad en la conexión

La conexión debe realizarse con doble factor, MFA (autenticación multifactor). Para por conectarnos, además de la contraseña segura, debemos validarnos con un segundo factor, como en el banco. Una aplicación de autenticación instalada en el móvil es la mejor opción.
Una vez conectados, la transmisión de datos debe ser segura, encriptada, protegida de posibles ataques externos, robo de información, contraseñas, datos bancarios … Aunque pensemos que nuestra información no le importa a nadie, la realidad es que cualquier dato robado hoy en día es un bien preciado para cualquier hacker.

3. Antivirus y antimalware
Todas las empresas tienen sistemas de protección antivirus y antimalware para los equipos que forman parte de su infraestructura. Todos los servidores, ordenadores, portátiles y demás recursos compartidos están protegidos. Pero esta protección se pierde cuando un usuario accede al sistema desde un ordenador ajeno a la organización, de su casa, o de un tercero, sin saber si tiene el antivirus actualizado, o si tiene troyanos u otro malware que se pueden extender sin quererlo al conectarse desde ese equipo a los sistemas de la empresa.
Si nos conectamos a una red WIFI compartida, esa información, si no está encriptada, puede ser capturada por cualquier persona que comparta la conexión.
Un sistema óptimo debe separar y aislar el equipo usado en la conexión, de forma que, aunque dicho equipo pueda estar en riesgo o infectado, no afecte a la seguridad de los sistemas a los que se conecta.

4. Acceso a todos los recursos

Necesitamos tener acceso a todos los recursos, todas las carpetas, aplicaciones, servidores y otros elementos a los que tenemos acceso desde nuestro puesto de trabajo habitual en la oficina.
La situación óptima es la que nos ofrece acceso dichos recursos de la misma forma que lo haríamos en situación normal, y sin notar diferencia por el hecho de estar fuera de la oficina.



5. Alta velocidad de conexión durante toda la sesión de trabajo
Si tenemos acceso a todo, pero la velocidad de conexión es lenta, nuestra productividad bajará de forma proporcional a la baja velocidad, e incluso puede llegar a desesperarnos.
La velocidad de trabajo debe ser la misma independientemente de donde accedamos, e incluso tampoco tiene que depender mucho de la calidad de la línea de acceso que usemos. Existen escenarios, como en el barco, donde la calidad de la conexión no siempre será alta. El sistema de teletrabajo tiene que ser capaz de optimizar al máximo esa conexión y obtener el mejor rendimiento posible.

6. Continuidad en el trabajo
Si estamos teletrabajando, en casa, en el barco, o donde sea, es más posible que tengamos interrupciones por llamadas, tareas u otras obligaciones o requerimientos que nos haga tener que dejar lo que estamos haciendo para continuarlo después. En nuestro puesto habitual dejamos el ordenador en marcha para ir a una reunión, por ejemplo, y al volver seguimos en el punto donde estamos, pero teletrabajando es posible que necesitemos apagar el ordenador o moverlo, y queremos también volver al punto donde lo hemos dejado.
Esta necesidad es una de las más importantes, dar continuidad a lo que estamos haciendo, en cualquier momento, desde cualquier ubicación y sin perder nada.

7. Protección ante cortes eléctricos o de conexión
En las empresas es habitual tener el sistema eléctrico protegido ante desconexiones, pero en el barco es posible que nos quedemos puntualmente sin electricidad, ya sea en el puerto, fondeados, con el generador o un convertidor. Todos sabemos que la electricidad es un bien preciado a bordo, y que su continuidad no es la misma de la que tenemos en el trabajo.
El sistema de teletrabajo ha de estar preparado para fallos eléctricos, micro cortes o cualquier otra desconexión, de forma que podamos volver a conectarnos en el punto donde estábamos, y sin perder nada.

8. Pantalla de acceso exactamente igual
Una de las primeras cosas que se nos viene a la vista cuando nos conectamos desde fuera es eso de "es que en el despacho tengo otros iconos y otros accesos".
El teletrabajo óptimo es el que mantiene el mismo escritorio para el usuario siempre, desde cualquier ubicación.

9. Redimensión de pantalla
Las dimensiones de las pantallas no siempre son las mismas. Es posible que en el trabajo tengamos una pantalla grande, o dos, y que en casa tengamos otra pantalla más pequeña o con otro formato, y a bordo un portátil o un iPad. El sistema debe adaptarse de forma automática a la dimensión de la pantalla o pantallas desde las que nos conectamos, optimizando las aplicaciones e incluso la disposición de los iconos.

10. Sin requerimientos ni instalaciones previas, desde cualquier dispositivo
Y el último de los requisitos es la opción de poder trabajar desde cualquier equipo, sea PC con Windows, Mac, Ipad, e incluso que sea independiente de las prestaciones del equipo. Aunque nos conectemos desde un equipo lento, tenemos que trabajar con los recursos del sistema al que nos conectamos, que siempre serán mejores que los del equipo local.
Un buen sistema de teletrabajo además no requiere que tengamos que preparar previamente el equipo a usar. Ha de ser transparente y debe permitir conectarnos sea cual sea el equipo.

¿Qué sistema cumple estos 10 requerimientos?

Existen muchas formas de teletrabajar. Normalmente nos conectamos por VPN (Virtual Private Network) a la empresa, y tenemos acceso a los documentos, aplicaciones, correo, y otros recursos locales o en la nube.
El entorno de Microsoft 365, sobre todo con Microsoft Teams, por ejemplo, es una muy buena herramienta de teletrabajo colaborativo, con acceso a documentos, correo, reuniones, pero no cumple los diez requerimientos anteriores.
El sistema perfecto es el que cumple los 10 requerimientos, y existe desde hace años. Este escenario se llama "Desktop Virtial" (Escritorio Virtual), y consiste en tener un ordenador virtual en la nube para cada usuario, y que sea siempre el

mismo, independientemente desde donde se conecta, sin distinguir lugar de trabajo, casa o barco, con recursos a medida, alta disponibilidad, y cumpliendo cada uno de los 10 puntos que hemos hablado anteriormente.

Es ideal para usarlo desde el barco, desde cualquier fondeo con poca cobertura, con un ordenador viejo, una tableta o incluso desde el móvil. Y aunque el equipo que usemos no cumpla requisitos de seguridad, no tenga antivirus y esté expuesto a peligros, la conexión mediante el escritorio virtual está totalmente aislada del medio y creará una conexión aislada y segura.

Este entorno consiste en tener toda la infraestructura en un modelo en la nube, incluyendo los ordenadores de cada usuario, los servidores de aplicaciones, servidores de ficheros y cualquier otro recurso. El producto se llama “Arsys Desktop”.

arsys

Con este producto, se consigue que todas las personas de una misma empresa, sea cual sea su localización, ciudad, país o punto de conexión remota, estén trabajando en una misma oficina virtual de dimensiones infinitas, y por tanto también de posibilidades infinitas.

Además, debido a que se eliminan los servidores y equipamientos de las empresas, se produce un ahorro importante en las infraestructuras centrales, entre otras cosas, en mantenimiento, seguridad, electricidad y aire acondicionado.

Como todos los servicios hoy en día, se trata de un pago por uso, es decir, se paga por usuario. El coste aproximado es de 40€/usuario/mes. Y no tiene ni mínimos ni máximos, ni permanencias. Se puede contratar para un solo usuario o para una empresa de miles de usuarios. Los 10 requerimientos se cumplen igual, independientemente de la dimensión contratada.

Más información en https://www.deinfo.es/servicios/teletrabajo-y-escritorio-virtual/

El teletrabajo no seguro es un peligro para el usuario y para la empresa. Recordemos que los hackers generan trampas a los usuarios, más que a las infraestructuras de las empresas. Aunque estemos fondeados y escondidos en una cala perdida, nos encontrarán y nos atacarán si no somos precavidos.

José María Serra Cabrera
www.informaticaabordo.com
Capitán de Yate
Licenciado en Informática
Director General - DEINFO Servicios Informáticos