Willis Towers Watson

Ciber-riesgo y acceso remoto seguro

Contenido

05

¿Es posible asegurar un acceso remoto 100% seguro?

06

La ciber-póliza e incidentes relacionados con el acceso remoto

07

¿Y si se produce un incidente de ciberseguridad?

08

Conclusiones

01

Capacidades de acceso remoto seguro

El estado de alarma decretado en España persigue reducir el avance de la pandemia producida por el COVID-19. Estas dos circunstancias han provocado que muchas organizaciones hayan decidido facilitar a sus empleados la posibilidad de realizar teletrabajo. Esta forma (remota) de trabajar puede aportar importantes ventajas a las organizaciones en una situación tan anómala como la que estamos viviendo: por ejemplo, la de mantener umbrales mínimos de productividad o la de ayudar a conciliar nuestra vida personal y profesional, sobre todo si en casa se encuentran niños o tenemos que atender a personas contagiadas.

El teletrabajo no es siempre posible. Esto que parece obvio, requiere de una mínima reflexión. Si mis procesos y actividades esenciales siguen apoyándose en papel, mi organización no utiliza de forma masiva sistemas de información o habitualmente no utilizo ningún tipo de herramienta colaborativa, ¿puedo teletrabajar? Probablemente la respuesta sea no. Y en este caso, ¿para qué tengo que desplegar un sistema de conexión a través de una red privada virtual (Virtual Private Network) a los pocos sistemas que utilizo? No todas las tecnologías “habituales” son útiles para todas las organizaciones.

Si por el tipo de actividades que la organización realiza, puede teletrabajarse, lo primero que hay que definir son las capacidades que necesitan los colaboradores:

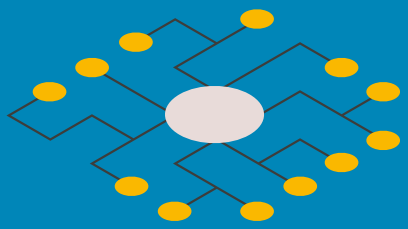
- Capacidad de que interactúen y se coordinen entre ellos. Adicionalmente que también lo hagan con clientes y proveedores clave.
- Capacidad de acceder a sistemas de información corporativos y otros recursos (datos, aplicaciones, servicios) que sean esenciales (desplegados on-premise o prestados como servicio).
- Capacidad de compartir y/o editar información de forma colaborativa. Aquí puede incluirse desde la posibilidad de compartir un calendario, a escribir un documento entre varios colaboradores o desarrollar lo entregables de un proyecto.

Una vez que se han definido estas capacidades, es necesario identificar qué sistemas y tecnologías las facilitan, comunicar a los usuarios de su existencia y definir el conjunto de procedimientos y estándares que les guíen en cómo utilizarlos de forma adecuada y segura. Si se han llevado a cabo acciones formativas, este proceso será más sencillo. En caso contrario, la realización de píldoras formativas (a través de entradas de infografías, blog, podcast, videos) puede ser una de las primeras medidas a adoptar.

Dado que no todos los colaboradores necesitan disponer de las mismas capacidades, es recomendable definir roles o grupos e identificar para cada uno de ellos las más adecuadas.

02

Cada Organización es diferente



Es difícil proporcionar recomendaciones genéricas para el acceso remoto seguro. El sector, el tipo de actividad, el tamaño, la madurez tecnológica, son tan sólo algunos factores que deben considerarse a la hora de desplegar sistemas, diseñar procedimientos y realizar formaciones sobre cómo acceder de forma remota segura.

Hace unos años (muy pocos, por cierto), el acceso remoto seguro se restringía básicamente a configurar correctamente un servidor de acceso remoto (o de salto), a través de una VPN (*Virtual Private Network)* que permitiera acceder a los sistemas desplegados on-premise y a los recursos propietarios que la organización tenía accesibles en su LAN (*Local Area Network*). Para aquellas organizaciones que tienen la mayoría de los sistemas de información desplegados de esta manera *(on-premise*), y/o almacenan información y documentación en sistemas tipo *NAS* o similares, nuestra recomendación es que sigan las mejores prácticas que propone el NIST en la SP 800-46 rev.2 *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device* (BYOD) Security. En la sección 3 del documento, se habla de forma explícita del Remote Access Solution Security y se enumeran entre otras las siguientes recomendaciones:

- Utilizar un servidor de acceso remoto seguro (o de salto) exclusivo, en el que no se instalen otras aplicaciones y servicios.
- Integrar el servidor de acceso remoto seguro con las soluciones que permiten la identificación, autenticación, autorización y traza de usuarios (habitualmente en estos casos el Active Directory).
- Desplegar dicho servidor en zonas desmilitarizadas.
- Dependiendo de cada perfil o grupo de usuarios, establecer los factores de autenticación necesarios. No para todos los grupos o para el acceso a todos los recursos, es siempre necesario el doble factor de autenticación.
- Cifrar la conexión realizada de forma remota, así como todos los datos que transiten.
- Asegurar que los equipos que acceden desde el exterior están configurados con los privilegios adecuados, están actualizados y parcheados y disponen de las medidas de protección antimalware, cifrado de datos, firma digital, uso de certificados, etc.

Hoy en día, muchas organizaciones están abandonando (o combinando) el modelo tradicional de despliegue propietario de sistemas de información por el modelo basado en el consumo de servicios proporcionado por un proveedor Cloud en cualquier de sus tres modalidades básicas (IaaS, PaaS o SaaS). En estos casos, el acceso remoto se hace siempre. Se accede a los servicios de forma ubicua, desde la oficina, desde casa, desde el aeropuerto. ¿Pero se hace de forma segura?

Depende. Cuando una organización decide consumir servicios Cloud (normalmente varios de diferente naturaleza), la seguridad se gestiona bajo un modelo de responsabilidad compartida. El proveedor Cloud asume mayor o menor responsabilidad sobre la seguridad de las redes, el almacenamiento, los servidores, las políticas de virtualización, los sistemas operativos, el middleware, la ejecución de procesos, los datos y las aplicaciones, dependiendo del tipo de modalidad. El proveedor de SaaS, asume casi toda la responsabilidad de la seguridad, mientras que el proveedor de IaaS, asume normalmente sólo la seguridad relacionada con las redes, el almacenamiento y la gestión de servidores y la virtualización. Sea como sea, el acceso remoto, ubicuo a este tipo de servicios, también debe hacerse de forma segura. La gran diferencia con respecto al acceso a recursos *on-premise*, es que el acceso no se hace a una red local o a unos activos propietarios, sino a unos recursos y servicios que proporciona un tercero. La organización debe habilitar mecanismos que permitan identificar a cada uno de los usuarios que quieren acceder a los recursos Cloud, a facilitar su acceso utilizando para ello diferentes factores de autenticación o basándose en el contexto, a autorizar y a dar privilegios según el perfil o al grupo de usuarios que corresponda y a trazar toda la actividad que el usuario realice mientras accede a estos recursos. En muchas ocasiones, los proveedores Cloud no proporcionan este tipo de funcionalidades y si lo hacen obliga a la organización a disponer para cada uno de ellos de diferentes mecanismos de acceso.

Es por ello, que, en los últimos años, han surgido soluciones denominadas *PAM (Privileged Access Management) o CASB (Cloud Access Security Management*), que normalmente se integran por delante de los diferentes servicios que proporcionan los distintos proveedores Cloud que una organización puede utilizar y que aseguran que las políticas de IAAA (Identificación, Autenticación, Autorización y Auditabilidad) se lleven a cabo correctamente. Es decir, que el acceso a recursos no propietarios (en este caso siempre remoto), se lleve a cabo de forma segura.

Siguiendo con la casuística (cada organización es diferente), dependiendo de si la organización facilita dispositivos corporativos a los empleados o no (se utilizan los dispositivos particulares), será necesario realizar unas medidas u otras. En el primer caso, habitualmente ya estarán preconfigurados con los privilegios adecuados para cada usuario y con las medidas habituales para evitar posibles incidentes de ciberseguridad (antimalware, desactivación de puerto USB, etc.). Si por el contrario se trata de dispositivos personales, será necesario verificar que siguen y cumplen las medidas que la organización estime oportunas. Por ejemplo, que el sistema operativo está actualizado, que dispone de una solución antimalware, que tiene instaladas las aplicaciones necesarias en caso de que los recursos sean propietarios, que la red doméstica tiene las configuraciones mínimas de seguridad, etc.

Las soluciones PAM (Privileged Access Management) o CASB (Cloud Access Security Management) facilitan el acceso remoto seguro a servicios Cloud consumidos por una organización

03

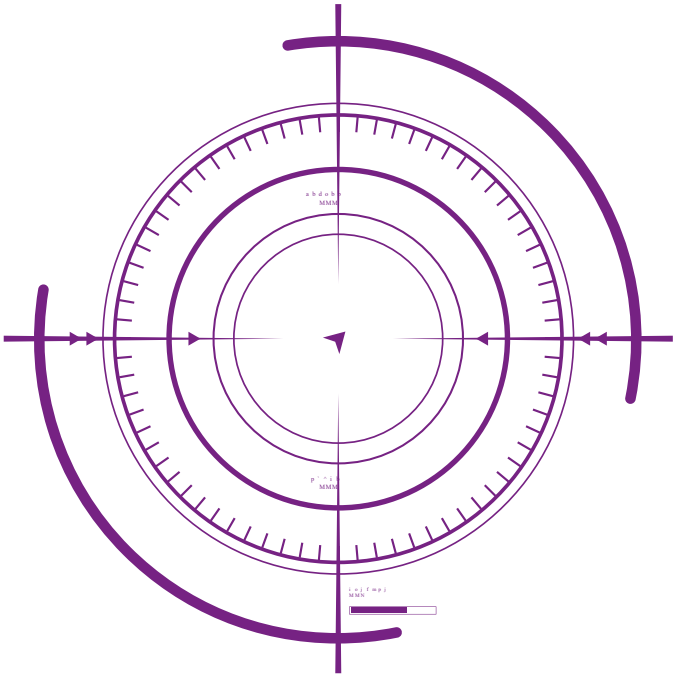
El ciber-riesgo y el acceso remoto seguro

¿Pueden materializarse nuevas amenazas por el hecho de que los colaboradores de una organización teletrabajen de forma masiva? Sí. En primer lugar, se está incrementando la superficie de exposición al tener que habilitar conexiones de forma remota. Esto a su vez, hace que las medidas tomadas para defender en profundidad se flexibilicen. Y, por último, el principio de mínimo privilegio, seguramente ha tenido que ser modificado para permitir un tipo de acceso que antes no era necesario.

La concurrencia masiva de usuarios puede ser aprovechada para robar credenciales y llevar a cabo escalado de privilegios. Una vez que se han robado credenciales, una eventual denegación de servicio, la infección por *ransomware* o por otro tipo de malware (tipo *cryptojacking*, por ejemplo) puede producirse con más facilidad.

Adicionalmente, si se utilizan servicios para la realización de teleconferencias y en estas se comparte información, esta puede ser interceptada o “escuchada” si el sistema de videoconferencia no asegura que las comunicaciones multipunto estén cifradas (normalmente la realización de sistemas de video-conferencia punto a punto suelen incorporar por defecto el cifrado en sus comunicaciones).

Probablemente, todas estas amenazas hayan sido identificadas previamente, pero lo que ocurre es que, en estas circunstancias, tanto su probabilidad de ocurrencia como su impacto (las pérdidas que puede generar en la organización) han incrementado.



04

¿Cómo evaluar y gestionar el ciber-riesgo que surge del uso masivo de sistemas de teletrabajo?

Como decíamos anteriormente, cada empresa es diferente. Nada tiene que ver la probabilidad y el impacto de que una amenaza se materialice por el uso masivo de sistemas que facilitan el teletrabajo en una organización que fabrica cohetes o una que maneja información de pacientes u otra que procesa datos bancarios. Para evaluar el ciber-riesgo asociado al uso masivo de sistemas de teletrabajo,

- En **primer lugar**, es necesario identificar qué procesos y servicios son esenciales para el trabajo de la organización.
- En **segundo lugar**, se debe realizar un sencillo modelo de amenazas, que permita identificar como podrían verse afectados dichos procesos y servicios esenciales si no es posible acceder de forma remota a ellos o si se accede a ellos de forma fraudulenta.
- En **tercer lugar,** es preciso analizar con qué probabilidad podrían producirse estos hechos (para cada una de las amenazas) y cuantificar las pérdidas que supondría para la organización.

Esta información, es clave para entender hasta qué punto y con qué extensión las recomendaciones antes mencionadas (tanto para sistemas on-premise como para los sistemas Cloud) deben ser llevadas a cabo. Todo este proceso estaría integrado en lo que se conoce como una evaluación estratégica del ciber-riesgo.

05

¿Es posible asegurar un acceso remoto 100% seguro?

Creemos que a nadie se le escapa, que actualmente, la respuesta a esta pregunta es no. Podemos y debemos llevar a cabo las recomendaciones arriba descritas con el objetivo de mitigar la probabilidad y el impacto de que las amenazas existentes sean provocadas por agentes maliciosos. Sin embargo, siempre existe un riesgo residual (habitualmente aquel que se produce con baja probabilidad y alto impacto) que debe ser transferido.

Para transferirlo, las organizaciones tienen a su disposición la contratación de una **ciber-póliza** que les cubra ante las pérdidas producidas por un incidente de ciberseguridad causado por el uso (o mal uso) de los sistemas de acceso remoto. O como lo que está ocurriendo actualmente, cubrir las pérdidas producidas porque se producen fallos en los sistemas debido a la falta de personas que los gestionen presencialmente (el equipo de IT y/o ciberseguridad también tiene que teletrabajar a causa del COVID-19)

06

La ciber-póliza e incidentes relacionados con el acceso remoto

Como ya hemos explicado en alguna publicación anterior, la ciber-póliza es un producto que combina coberturas por responsabilidad civil y daños propios e incluyen coberturas ante tres grandes costes/pérdidas: primera respuesta y gestión de crisis; daños y perjuicios ante autoridades y/o terceros; e interrupción del negocio (o pérdida de beneficio). Teniendo en cuenta el alcance de este tipo de productos, estas son algunas preguntas que podríamos hacernos antes de contratar una ciber-póliza, para saber hasta qué punto esta forma de seguir mitigando el ciber-riesgo es efectiva para mi organización.

¿Quedarían cubiertas las pérdidas de beneficio si los sistemas de información sufren un fallo de sistema porque los administradores de dichos sistemas no están presentes o el sistema de acceso remoto no les permite actualizarlos o parchearlos? En condiciones normales, siempre y cuando no exista una exclusión de mantenimiento tecnológico, las pérdidas de beneficio (transcurrido el periodo de espera) deberían ser cubiertas.

1

En segundo lugar, también podríamos plantearnos esta situación. Ahora que todo mi equipo de sistemas y ciberseguridad está trabajando de forma remota y que no puede atender óptimamente mi infraestructura, si se produce un fallo de seguridad (brecha de datos, denegación de servicio, infección por ransomware), ¿cubriría la ciber-póliza de forma estándar las pérdidas producidas? Sí, a no ser que existan exclusiones explícitas, la ciber-póliza se activaría con normalidad.

2

07

¿Y si se produce un incidente de ciberseguridad?

Si se produce un incidente de ciberseguridad en estas circunstancias, en las que la mayoría de los colaboradores están trabajando de forma remota (incluyendo los responsables de sistemas y/o ciberseguridad) es clave disponer de un Plan de Respuesta ante Incidentes (PRI).

El principal objetivo de un Plan de Respuesta ante Incidentes (PRI) es minimizar el impacto (pérdidas) que la ocurrencia de un incidente de ciberseguridad puede causar en una organización. Para ello, es necesario poder responder de una forma estándar, homogénea, sistemática y estructurada. Con este propósito se diseñan los PRI.

Otra ventaja importante que proporciona el diseño de un PRI es que ayudará a recopilar información sobre por qué, quién, cómo, dónde, cuándo se ha producido el incidente, definir acciones aprendidas y poder estar prevenidos en caso de que se produzcan incidentes futuros.

Si la organización no dispone de este tipo de plan, ahora sin duda es excelente momento para diseñarlo, de manera que, ante un incidente de ciberseguridad, la organización esté preparada para detectar, analizar, contener y erradicar un eventual incidente, recuperar el normal funcionamiento de los sistemas en el menor tiempo posible, documentar lo ocurrido como lecciones aprendidas e informar a quien corresponda de todo lo acontecido.

Si por el contrario ya dispone de él, es clave actualizarlo y revisarlo. Habrá que considerar que el teletrabajo masivo hará que aparezcan nuevos incidentes que antes no estaban contemplados y habrá que adecuarlo a esta nueva situación en la que existirán menos recursos disponibles para llevar a cabo todas las etapas básicas del PRI antes mencionadas.

08

Y para concluir

1. Cada organización debe proporcionar capacidades de acceso remoto seguro, teniendo en cuenta su idiosincrasia, su madurez tecnológica y teniendo en cuenta que no todas las personas requieren del mismo nivel de privilegios

2. Los sistemas, procedimientos y la formación relacionada con el acceso remoto seguro serán diferentes, dependiendo de si la organización gestiona recursos propietarios o consume servicios a través de proveedores Cloud.

3. Pueden materializarse nuevas amenazas por el hecho de que los colaboradores teletrabajen de forma masiva. Se incrementa la superficie de exposición, se modifican los principios de mínimo privilegio y se flexibilizan las estrategias de defensa en profundidad. Además, su probabilidad de ocurrencia y su impacto se han elevado ¿Serías capaz de cuantificar hasta qué punto la materialización de estas amenazas pueden afectar a tu cuenta de resultados?

4. La mitigación no siempre es suficiente. La ciber-póliza ayuda a cubrirte ante esos casos en los que a pesar de haber llevado a cabo buenas prácticas para permitir un acceso remoto seguro, el incidente de ciberseguridad ocurre.

5. El Plan de Respuesta ante Incidentes (PRI) te va a ayudar a minimizar el impacto (pérdidas) que la ocurrencia de un incidente de ciberseguridad puede causar en una organización. No hay mejor trigger que este para ponerlo en marcha.

Fernando Sevillano Ph.D.
Head of Cyber Risk Consulting
Iberia

Willis Towers Watson
Paseo de la Castellana, 36-38, 6ª Planta | 28046
Madrid (Spain)
Mobile: +34 654 519 235
ernando.sevillano@willistowerswatson.com

Carolina Daantje Santana
Directora de Ciber Riesgos e infidelidad de empleados
Cyber Champion de España

Willis Towers Watson
Pº Castellana, 36-38 6ª Planta, 28046 Madrid
Directo: (34) 91 154 9025 Ext. 3443025
Movil: (34) 608220419
carolina.daantjeS@willistowerswatson.com

Sobre Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW), empresa líder en consultoría global, broking y soluciones, ayuda a los clientes de todo el mundo a convertir el riesgo en un camino hacia el crecimiento. Con una historia que se remonta a 1828, Willis Towers Watson cuenta hoy con 45.000 empleados en más de 140 países y mercados. Diseña y ofrece soluciones que gestionan el riesgo, optimizan los beneficios, desarrollan el talento y potencian la capacidad del capital, para proteger y fortalecer a instituciones y particulares. Su punto de vista le permite conocer la conexión entre el talento, la experiencia y el conocimiento – una fórmula dinámica que potencia los resultados y el futuro crecimiento del negocio.

willistowerswatson.com

Willis Towers Watson