Brexit: el impacto en identidades con privilegios

Mientras el Reino Unido y el resto de Europa se preparan para el *brexit* (la salida de Gran Bretaña de la Unión Europea), los expertos en seguridad informática se preguntan qué significará este hecho para los procesos de gestión de seguridad y riesgos que se han establecido en el pasado y cómo deben ajustarlos a la realidad emergente. En este documento, se debate el impacto del *brexit* en la gestión de accesos con privilegios y qué pueden considerar los profesionales de la seguridad de la información como soluciones inmediatas para mitigar riesgos.

Brexit: ¿qué pasa después?

Con la notificación formal de la primera ministra Theresa May de que el Reino Unido abandona la Unión Europea, se ha iniciado el proceso oficial de separación. Ahora, se inicia un periodo de 24 meses en los que ambas partes deben crear un marco para trabajar juntas. El proceso se describe en el siguiente diagrama.

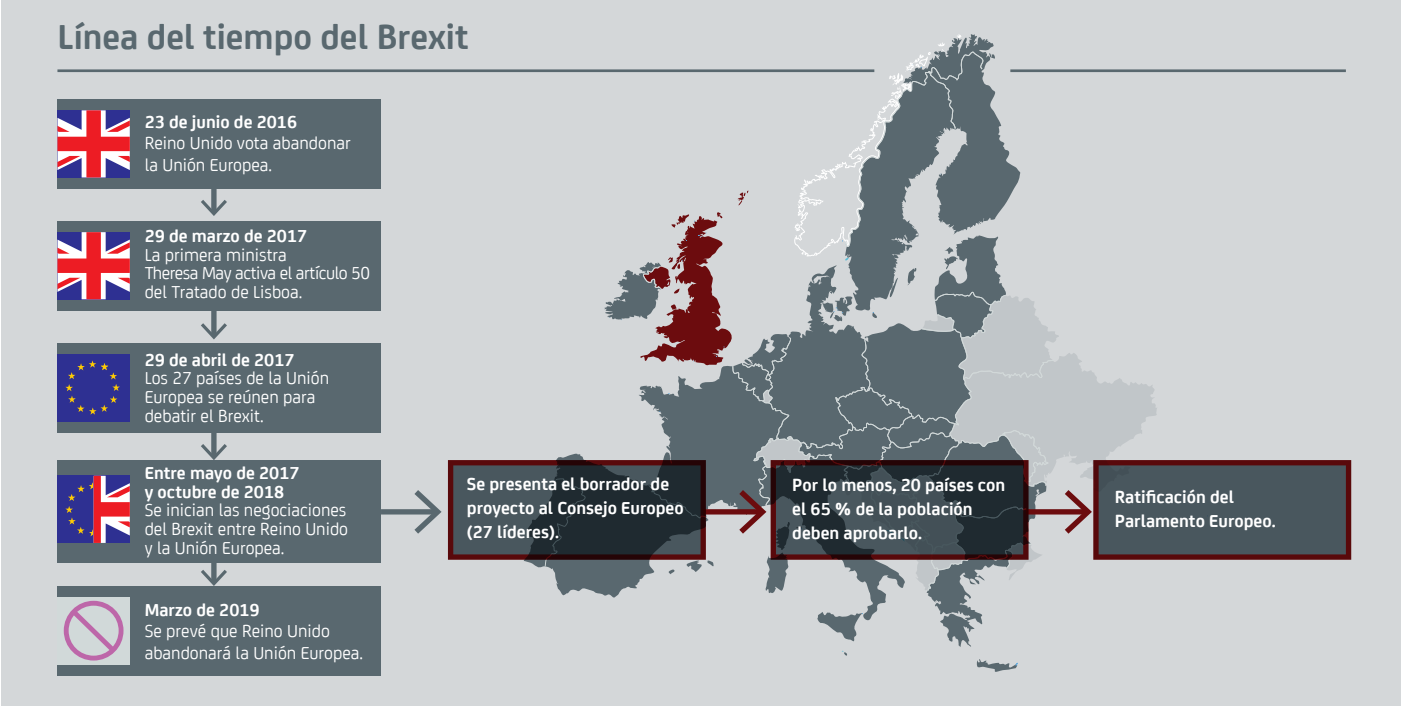

Ilustración A. Calendario del *brexit* (cortesía de APA y DW)

Durante los próximos 24 meses, la Unión Europea y el Reino Unido deben ponerse de acuerdo en los términos de su relación posteiror a la separación. Entretanto, varias organizaciones, tanto públicas como privadas, de ambos lados han empezado a idear formas de coordinar unas transacciones comerciales fluidas. Este proceso está plagado de riesgos y callejones sin salida. Después de todo, los que se ven involucrados, directa e indirectamente, se mueven por territorio desconocido, lo que requiere un programa de gestión de riesgos bien planeado.

Posible impacto económico

Se han creado muchos modelos del impacto macroeconómico del *brexit* en el Reino Unido. Muchos de ellos sugieren lo siguiente:

- Disminución del PIB a largo plazo
- Caída de la inversión extranjera directa (IED)
- Disminución de la inmigración

De forma colectiva, significa que muchas organizaciones tendrán que buscar modos en los que puedan mantener la competitividad y seguir ofreciendo servicios en sus respectivos mercados. Con el fin de garantizar el mínimo impacto en la dirección que tome el negocio, las organizaciones están creando un marco de trabajo de cara al futuro en el que, a menudo, contemplan la peor situación. "Para fines planificadores, debemos considerar un *brexit* 'duro' en el que el Reino Unido pierde su capacidad de abrirse camino en la Unión Europea", escribió James Cowles, el director ejecutivo europeo de Citigroup, en un memorando para el personal. Otras instituciones financieras se han embarcado en planes similares, pero no son las únicas. Se debe considerar el impacto en ambos lados de la ruptura. Por ejemplo, Vauxhall se está planteando externalizar toda su cadena de suministros para el Reino Unido dentro de dicho país, mientras que BMW busca una nueva ubicación en Europa continental para su Mini. Sin embargo, cualquier decisión empresarial racional que influye en el trabajo (por ejemplo, un movimiento para mejorar la productividad dentro del Reino Unido con el fin de alcanzar el nivel de otros países de la Unión Europea o cambios en la demanda internacional) corre el riesgo de colgarse la etiqueta de víctima del *brexit*.

Impacto en los trabajos

Uno de los ámbitos de preocupación será el impacto del *brexit* en los trabajos. Varias organizaciones han insinuado el movimiento de los trabajos más allá de las fronteras; por ejemplo, la decisión de Nestlé de trasladar la fabricación de las barritas de chocolate Blue Riband del Reino Unido a Polonia se puede correlacionar con la eliminación de 300 puestos de trabajo en Reino Unido. Esto puede deberse a los cambios en el entorno de inmigración (la restricción de la normativa relativa a los visados o el mayor escrutinio) o a los aranceles comerciales, así como la incertidumbre que los rodea. La contratación en el sector privado del Reino Unido ha caído a su nivel más bajo en tres años debido a las incertidumbres en torno al *brexit*, de acuerdo con una de las empresas de contratación más grandes del mundo. Tal desplazamiento de puestos de trabajo no solo tiene un impacto considerable en la economía general, sino que también representa una amenaza en cuanto a la seguridad de la información muy alta.

Exposición a los riesgos

Como hemos visto hasta el momento, se aprecian abundantes pruebas de que existen importantes riesgos que las organizaciones deben gestionar como parte del *brexit*. Junto con los drásticos cambios tecnológicos que experimentamos en la actualidad, la gestión de riesgos de TI ha adquirido una importancia significante. Una parte primordial de esto engloba los riesgos en cuanto a la seguridad de la información. Se ha demostrado ampliamente que los mayores riesgos financieros y comerciales para los activos de seguridad de la información residen en el aprovechamiento de los accesos de usuarios con privilegios. Este riesgo ha aumentado a medida que las organizaciones han adoptado entornos tanto en la nube como virtuales de cara al crecimiento empresarial y la transformación digital.

Cómo abordar los riesgos de la gestión de accesos con privilegios

Puesto que las organizaciones estudian sus opciones para abordar los retos que presenta el *brexit*, sobre todo, el desplazamiento de empleados, deben contemplar el riesgo de las amenazas internas. Cualquier incertidumbre, como posibles cambios en la situación laboral o transferencia de responsabilidades, puede dar lugar a comportamientos inseguros por parte de los empleados internos. Asimismo, presenta una oportunidad para que personas externas malintencionadas aprovechen posibles vulnerabilidades. Además, la transferencia de responsabilidades, como la contratación de un distribuidor externo para determinadas funciones empresariales, puede causar una mayor exposición y requerirá la supervisión y visibilidad adecuadas. De forma colectiva, estos problemas exigen la implementación de una estrategia eficaz de mitigación de riesgos relativos al acceso con privilegios. De hecho, la protección de información confidencial y propiedad intelectual adquiere una importancia relevante.

Consideraciones para mitigar los riesgos relativos al acceso con privilegios

Se deben contemplar los siguientes aspectos para mitigar riesgos derivados de los peligros e infracciones de accesos con privilegios durante la incertidumbre.

1. **Escala:** superficie de exposición
    a. Terminales o dispositivos: no se limita a datos almacenados de forma local, sino que también abarca activos virtuales y basados en la nube.
    b. Identidades: no solo se limita a los usuarios administrativos, también incluye cuentas y scripts de aplicación a aplicación.

2. **Alcance:** estrategia futura
    a. Transformación digital: si existe un programa de transformación digital, cualquier cliente, distribuidor o partner involucrado se convierte en factor.
    b. Programas del Internet de las cosas (IoT): tenga en cuenta todos los dispositivos que puedan disponer de acceso a información con privilegios.
3. **Automatización:** aprendizaje automatizado y grabación de sesiones
    a. Aprendizaje automatizado: mediante análisis del comportamiento de los usuarios (UBA) para detectar anomalías con el fin de reducir el tiempo que se tarda en detectar y mitigar la exposición.
    b. Grabación de sesiones: sirve para evitar el rechazo y cumplir la normativa.
4. **Recursos:** presupuesto y talento
    a. Presupuesto: dada la incertidumbre geopolítica, probablemente, los presupuestos se verán limitados durante las negociaciones del *brexit*.
    b. Talento: con los inminentes cambios en cuanto a la inmigración y la migración del talento, resultará fundamental garantizar que la necesidad de habilidades concretas no impida el despliegue.

Conclusión

La gestión de accesos con privilegios, como la que ofrecen las soluciones de CA Technologies, serán primordiales para asegurar que los activos importantes se protegen de forma adecuada durante esta fase de cambio geopolítico. Aunque puede resultar tentador empezar por la funcionalidad básica, como el almacenamiento de contraseñas, para mitigar riesgos, es vital enfrentarse al problema desde un punto de vista holístico. El *brexit*tiene una planificación fija. Probablemente, el ritmo de la actividad se acelere, de manera que los profesionales de la seguridad de la información dispondrán de un tiempo reducido para reaccionar. Resultará fundamental plantearse el coste total de propiedad (TCO) de una solución, junto con el alcance y la escala de la compatibilidad funcional, antes de embarcase en este viaje. Planifique cómo enfrentarse a lo desconocido, por ejemplo, problemas relativos a la separación de funciones, así como a la supervisión de datos, durante el proceso. Por último, contemple una solución que no solo proporcione, escala, alcance y automatización, sino que también actúe como fundamento de una gestión de accesos con privilegios segura, junto con análisis basados en el aprendizaje automatizado. Este cambio influye tanto en el Reino Unido como en cualquier partner comercial importante del Reino Unido y de la Unión Europea.

CS200-277092_0617