Recomendaciones para acceso remoto seguro a información sensible preservando seguridad y productividad

Abstract: incrementar la productividad y la movilidad de los usuarios, que requieren del acceso a información sensible, ya sea desde la red corporativa de una organización, sedes remotas, filiales o sucursales necesita de un conjunto de recomendaciones y mejores prácticas. La aplicación de estas medidas incrementará la protección frente a accesos no autorizados, a la vez que mejorará la productividad permitiendo un acceso controlado, seguro y vigilado.

Contenido:

1. INTRODUCCIÓN 1
2. ESCENARIO TECNOLÓGICO 2
2.1 Segregación y confinamiento de la información 2
2.2 Acceso remoto seguro 3
2.3 Análisis de riegos y perfiles de seguridad 4
3. EJEMPLO DE ARQUITECTURA 4
4. REFERENCIAS 4
ANEXO A. ARQUITECTURA DE REFERENCIA 6

1. INTRODUCCIÓN

Cualquier organización que maneje información sensible es consciente de las dificultades a las que se enfrenta para permitir el acceso a este tipo de información, sin poner en riesgo el sistema que maneja la información, pero a su vez, incrementando la productividad y la movilidad de los usuarios.

Las organizaciones buscan mejores resultados en sus operaciones, que en muchos casos pasa por incrementar los niveles de movilidad de sus usuarios y permitir el acceso a la información en cualquier lugar y dispositivo. Sin embargo, la búsqueda de mejores resultados no debe en ningún caso poner en riesgo la información en sí misma. Es por ello, por lo que, en muchas ocasiones, habrá que establecer un equilibrio adecuado entre productividad y seguridad.

Si a esto se le suma la necesidad de cumplir con diversas normativas o legislaciones y los requisitos de seguridad que el sistema debe cumplir, entonces la toma de decisiones se puede complicar en gran medida.

Es por ello por lo que los Directores de Tecnología y responsables de seguridad deben de diseñar arquitecturas seguras de servicios para manejar información sensible pero también productivas cuando se enfrentan a escenarios del tipo comentado.

2. ESCENARIO TECNOLÓGICO

El escenario tecnológico (Anexo A) que se plantea en este documento es únicamente una muestra o ejemplo de cómo se podrían combinar los requisitos de seguridad y las necesidades de acceso a la información.

Pueden existir otros escenarios similares que contemplen todos o parte de los elementos aquí mostrados, pero a grandes rasgos, éste puede ser un modelo de partida para implementar sistemas con características similares.

2.1 Segregación y confinamiento de la información

Como es conocido, a mayor grado de sensibilidad de la información, mayores son las exigencias de las medidas de seguridad a implementar, incluyendo medidas físicas de acceso a los centros de datos y puestos de procesamiento de dicha información.

Según el caso, se puede limitar mucho las capacidades de acceso remoto a la información, ya que será necesario cumplir, entre otros aspectos, con zonas de acceso restringido (ZAR), regulaciones de emanaciones electromagnéticas y requisitos de interconexión.

En este sentido, es recomendable hacer una segregación de la información, aislando el grado de menor sensibilidad del resto, para dotar al sistema de una mayor flexibilidad, mejorando así la productividad en el consumo y manejo de dicha información.

De acuerdo al grado de sensibilidad de la información no se requiere de determinadas medidas físicas y de emanaciones electromagnéticas, por lo tanto, existe una mayor flexibilidad a la hora de utilizar distintos tipos de clientes y dispositivos para el acceso a la información.

Por otro lado, se puede proveer de acceso remoto seguro a la información sensible, siempre que se cumplan una serie de condiciones de seguridad:

a. La segregación de la información sensible debe contemplar la implementación de un sistema dedicado para su manejo.
b. En el caso de arquitecturas virtuales:
    i. Se podrán considerar arquitecturas virtuales que unifiquen diferentes grados de sensibilidad de la información, siempre y cuando se cumplan las medidas de seguridad relativas a aislamiento y segregación.
    ii. A todos los efectos, los sistemas que residan en una misma arquitectura de virtualización deberán ser considerados sistemas independientes entre sí, cumpliendo el conjunto de requisitos de seguridad específicos tanto para el ámbito como para el grado de sensibilidad de la información que manejen.

c. Dependiendo de los casos y las medidas de seguridad implementadas, se podrá habilitar un flujo unidireccional de información (fundamentalmente correo electrónico) desde el sistema de menor grado de sensibilidad hacia el sistema de grado superior, pero nunca, al contrario.

2.2 Acceso remoto seguro

En aquellos casos en donde se requiere disponer de acceso remoto a la información sensible, dado que se dispone de sistemas dedicados para su manejo, se deberá segregar también este tipo de accesos ya sea hacia un sistema u otro, con las medidas de seguridad adecuadas a cada uno de ellos, así como el uso corporativo del puesto de trabajo para otros fines.

A continuación, se indican las principales directrices generales que se deberían tener en cuenta a la hora de diseñar una arquitectura de acceso remoto seguro.

a. El acceso remoto al sistema que maneja información sensible necesitará implementar medidas complementarias de vigilancia.

b. La arquitectura de los puestos de trabajo para el acceso remoto a la información sensible deberá cumplir con alguno de los casos de uso indicados en la Guía de Seguridad "*CCN-STIC 498A Arquitectura multidominio de Puesto de Trabajo (End Point) seguro. Caso de Uso: Difusión Limitada - Sin Clasificar*" o, en su defecto, con los casos de uso indicados en el Abstract "*Casos de acceso a tratamiento de información sensible*".

c. Los usuarios podrán acceder al sistema que maneja información sensible desde sus estaciones de trabajo localizadas en la red corporativa de propósito general de acuerdo al análisis de riesgos preceptivo.

d. El acceso remoto al sistema que maneja información de grado superior deberá seguir cumpliendo con todos los requisitos de seguridad expuestos en las distintas normas e instrucciones de seguridad, incluyendo los mecanismos de interconexión si los hubiere.

Dado que habitualmente existe un mayor volumen de información de menor grado de sensibilidad, si la arquitectura que se va a diseñar garantiza que este tipo de información estará segregada del resto y se aplican las medidas complementarias de vigilancia y control en accesos remotos, se podrá conseguir una infraestructura lo suficientemente segura para cumplir con las distintas normas e instrucciones técnicas de seguridad, pero a la vez lo suficientemente flexible como para permitir que la mayoría de los usuarios puedan trabajar en remoto o desde sus equipos corporativos y por lo tanto se pueda mejorar la productividad de la organización.

2.3 Análisis de riegos y perfiles de seguridad

Otro de los elementos básicos para definir la arquitectura y sobre todo las medidas de seguridad requeridas a implementar es la realización de un análisis de riesgos preceptivo, que permita determinar una declaración de aplicabilidad adaptada al ecosistema en cuestión.

El análisis de riesgos permitirá conocer el punto de partida en materia de riesgos y amenazas en el que se encuentra el sistema. A partir de ello, se deberán incorporar al sistema las salvaguardas necesarias para minimizar la probabilidad de materializarse la amenaza sobre el mismo.

Por otro lado, el análisis de riesgos permitirá elaborar un perfilado de seguridad adaptado al contexto y tendencias de la amenaza, las carencias del sistema y mala praxis habitual detectada en el uso.

3. EJEMPLO DE ARQUITECTURA

En este sentido, se puede elaborar una arquitectura (Anexo A) a modo de ejemplo, con el objetivo de dar cumplimiento a las necesidades y requisitos planteados. La idea es identificar una arquitectura básica de acceso remoto seguro a la información, no siendo ésta la única opción y pudiendo existir otras arquitecturas con un mayor grado de complejidad que se adapten mejor a las necesidades de cada organización.

En este caso, los accesos remotos a la información sensible de grado inferior se realizan mediante túneles VPN con autenticación de doble factor, mientras que el acceso remoto a la información de mayor grado se realiza mediante el uso de cifradores hardware directamente de ZAR a ZAR. De esta forma se logra segregar tanto el acceso a la información como la administración, pero a la vez dotar de flexibilidad a aquellos usuarios que mayoritariamente hacen uso de información de menor grado de sensibilidad.

4. REFERENCIAS

Se han tomado como referencia los siguientes documentos publicados por el Centro Criptológico Nacional:

- Norma de seguridad CCN-STIC-220 - Arquitecturas Virtuales: https://www.ccn-cert.cni.es/ultimas-guias/5192-ccn-stic-220-arquitecturas-virtuales/file.html
- Instrucción Técnica de Seguridad CCN-STIC 301 - Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/9409-nueva-guia-ccn-stic-a-implementar-en-sistemas-clasificados.html

- Instrucción Técnica de Seguridad CCN-STIC 302 – Interconexión de CIS: https://www.ccn-cert.cni.es/series-ccn-stic/300-instrucciones-tecnicas/57-ccn-stic-302-interconexion-de-cis/file.html
- Guía de seguridad CCN-STIC 498A - Arquitectura multidominio de Puesto de Trabajo (End Point) seguro Caso de Uso: Difusión Limitada – Sin Clasificar: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/5156-ccn-stic-498a-arquitectura-multidominio-de-puesto-de-trabajo-end-point-seguro-caso-de-uso-difusion-limitada-sin-clasificar/file.html
- Abstract - Casos de acceso a tratamiento de información sensible: https://www.ccn-cert.cni.es/informes/abstracts/5422-casos-de-acceso-a-tratamiento-de-informacion-sensible/file.html
- Abstract - Orientaciones para el manejo de información clasificada (DIFUSIÓN LIMITADA o equivalente) en entornos ajenos a la organización (teletrabajo): https://www.ccn-cert.cni.es/informes/abstracts/5467-orientaciones-para-el-manejo-de-informacion-clasificada-difusion-limitada-o-equivalente-en-entornos-ajenos-a-la-organizacion-teletrabajo/file.html

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.10.03 00:37:42 +02'00'

ANEXO A. ARQUITECTURA DE REFERENCIA