Data Centers: tendencias y seguridad

PRINCIPALMENTE SE BUSCA CONVERGER, UNIFICAR, TODOS LOS SERVICIOS, EN UN LUGAR DETERMINADO, ELIMINANDO ELEMENTOS, AHORA INNECESARIOS

Jonathan González Fernández

CONSULTOR SENIOR EN UNIDAD DE INTELIGENCIA

Homeland Security / Sistemas de Defensa y Seguridad
Indra Sistemas S.A.

Los Data Centers, o CPD (en español, Centros de Proceso de Datos) en muchas organizaciones son el activo más importante, representando incluso, para algunas de ellas, la razón de la existencia de la organización en sí misma. Por esta razón, las organizaciones necesitan estar al día en cuanto a las tecnologías que hacen de su Data Center un lugar "vivo y seguro". Tendencias y seguridad no tienen que ser enemigas y el artículo que se acompaña podría ofrecer algunos detalles a simple modo de ejemplo.

Tendencias

Tradicionalmente los Data Centers, o centro de procesamiento de datos, eran grandes salas repletas de racks (armarios) con servidores y grandes equipos de almacenamiento y comunicaciones. Gracias al avance tecnológico las proporciones físicas externas se han ido reduciendo a la vez que la capacidad de almacenamiento se ha ido incrementando. Podríamos decir, no siendo del todo exactos, que ha habido una relación de inversa proporcional entre espacio ocupado y capacidad de almacenamiento.

> El concepto de virtualización, además, está jugando un papel muy importante en el campo del almacenamiento y procesamiento de información

Las plataformas de próxima generación están siendo diseñadas teniendo en cuenta la simplicidad, seguridad, rapidez y fiabilidad de respuesta ante las necesidades cambiantes del negocio en el mundo actual.

El concepto de virtualización, además, está jugando un papel muy importante en el campo del almacenamiento y procesamiento de información. Representa el ejemplo de transición necesario para que las organizaciones reduzcan costes (TCO) pero sigan siendo lo suficientemente flexibles y ágiles como para afrontar las necesidades cambiantes del negocio. De esta manera, el concepto de virtualización se está asociando a la mejora de la productividad en muchas organizaciones.

¿Cuáles son las principales líneas de actuación, con las nuevas tendencias aplicables a Data Centers?

Principalmente se busca converger, unificar, todos los servicios, en un lugar determinado, eliminando elementos, ahora innecesarios. Las principales líneas de actuación se están centrando en:

Simplificación de las arquitecturas de los Data Centers.
(Re)Diseño de la infraestructura IP.
Incorporación del *switching* virtual (conmutación de datos).
Virtualización de sistemas.
Virtualización de la seguridad.

Este último punto ha cobrado especial relevancia en el sector, con defensores y detractores por igual, en el tema de la seguridad, ¿se ha de ir hacia la tendencia?

Seguridad

Si bien las tendencias cambian, la tecnología mejora y las organizaciones deciden nuevas líneas de actuación, la

seguridad es un proceso que ha de desarrollarse de forma constante y paralela, porqué no, conforme a las tendencias. Existen tendencias para todo lo que representa la parte "hardware/software" de los Data Centers, pero, ¿y qué ocurre con las partes física y humana de un Data Center? ¿Hay tendencias? ¿Y la seguridad? ¿Sigue aplicándose o hay que tener en cuenta algo que se nos haya escapado a priori? Hagamos un rápido repaso.

Siguiendo un modelo de seguridad de "Defensa en Profundidad" (en inglés, Defense in Depth) rápidamente se puede apreciar que la seguridad física es el vector de amenaza más vulnerable y fácil de explotar.

La penetración física ofrece al potencial atacante acceso a información sensible sin tener que salvar grandes medidas de seguridad tecnológicas, y por lo tanto no es necesario poseer un gran *background* técnico, ni ser un gran "hacker". Por la naturaleza de como se desarrolla un ataque físico, podríamos decir que es uno de los más difíciles de prevenir, detectar y cuantificar, y uno de los más tentadores en lo que al atacante se refiere, dado el potencial volumen de información al que se puede acceder en un tiempo relativamente corto.

Cuando se trata el tema de los CPD y su seguridad, generalmente se tiende a eliminar de la escena al ser humano. ¡Craso error! Las personas también son un vector de amenaza a tener en cuenta. La ingeniería social, el acceso a equipos de forma incontrolada, por personal no imprescindible, entre otros, representan factores de riesgo que se han de evaluar y medir para poder mitigar.

> ¿Qué medidas de seguridad deberían de tenerse en cuenta en el planeamiento, ubicación, construcción, y operación/explotación de un CPD?

Pero, ¿qué medidas de seguridad deberían de tenerse en cuenta en el planeamiento, ubicación, construcción, y operación/explotación de un CPD? ¿Qué medidas de seguridad son la línea base de partida? Las siguientes son las más importantes:

Ubicación y Construcción

Ubicación física del lugar de emplazamiento: evaluación ante posibles desastres naturales, desastres producidos por el hombre, infraestructuras necesarias para su servicio (principalmente acometidas eléctricas), utilización de las zonas aledañas…

Perímetro del lugar de emplazamiento: seguridad del perímetro en la zona de ubicación del Data Center, vigilancia, razones de diseño constructivo del edificio, puntos de acceso y evacuación…

Centros de cálculo: infraestructuras de control y vigilancia en el acceso a salas, seguridad ambiental (temperatura, humedad, prevención de incendios), zonas comunes y zonas

compartidas, dársenas de carga y descarga de materiales…

Equipamiento del edificio y mantenimiento: sistemas de frío y calor, acometidas eléctricas, sistemas de destrucción de información en soporte físico (papel, CDs, etc.), sistemas de monitorización para vigilancia en el NOC (Network Operation Center, en español, Centro de Operaciones de Red).

Personas

Personal externo: controles aplicados al servicio de vigilancia, servicio de limpiezas, ingenieros y visitantes.

Personal interno: concienciación en materia de seguridad, involucración del personal en la seguridad del edificio y en sus planes de seguridad y de recuperación ante desastres (que cada profesional sepa lo que tiene que hacer en caso de urgencia o emergencia) y diseminación de las políticas corporativas de seguridad, hasta su arraigo corporativo.

Plan de Prevención, Continuidad y Recuperación ante Desastres

RA, Risk Assessment, o Evaluación de Riesgos

BCP, Business Continuity Plan, o Plan de Continuidad de Negocio (porque las cosas pueden suceder…)

DR, Disaster Recovery, o Plan de Recuperación ante desastres (… y hay que tener planeado como salir de la situación).

Importante: RA+BCP+DR… ¡¡¡Ha de ser un proceso continuo!!!

Referencias

Para aquellos que deseen profundizar un poco más en el tema de tendencias sobre Data Centers y sobre la seguridad, a continuación se proveen unas referencias que seguro serán de su interés:

(1) **Virtualization, Consolidation and Security – Special Report:**
http://gcn.com/microsites/virtualization-consolidation/virtualization-index.aspx

(2) **Intelligence community to start using virtual worlds:**
http://www.networkworld.com/news/2008/032108-intelligence-community-to-start-using.html

(3) **Best practices in planning data centers and their networking:**
http://www.level3.com/downloads/Data%20Center%20Networking%20For%20FS.pdf

(4) **Data center physical security:**
http://www.sans.org/reading_room/whitepapers/awareness/data_center_physical_security_checklist_416

(5) **Guidelines for specifying data center criticality and tier levels:**
http://www.apcmedia.com/salestools/VAVR-6PHPBU_R0_EN.pdf