White Paper
Vulnerabilidad del centro de datos

En los últimos meses se ha dado más énfasis a la seguridad de los datos, considerando la rápida expansión del "Internet de las cosas" (IoT). Esto, a su vez, ha planteado el tema de la vulnerabilidad de la instalación que soporta o almacena esos datos.

Se han publicado dos estudios en los últimos 18 meses que respaldan esto. El primero, relacionado con dispositivos habilitados para PoE, pronostica que el mercado crecerá en más del 19% y alcanzará ventas superiores a $ 1 mil millones en 2021. La segunda encuesta estimó que habrá 36 mil millones de dispositivos conectados a IoT para 2021, llegando a 75.5 mil millones para 2025 Con esta tasa de crecimiento, la seguridad que rodea el almacenamiento de los datos es crítica.

Si bien se publica mucho sobre la importancia de la seguridad cibernética, con bastante razón, ha habido muy poca cobertura con respecto a las otras vulnerabilidades que rodean a los centros de datos. Hay dos áreas clave que debemos considerar que podrían afectar el desempeño continuo del DC.

Limpieza interna

Lo primero se relaciona con lo que yo llamo "Limpieza".

La buena limpieza es esencial y también se puede dividir en dos partes, la primera relacionada con la infraestructura. Si bien el diseño inicial puede haber sido "apto para el propósito" cuando se construyó por primera vez, pronto puede verse abrumado si la complacencia se arrastra. Con demasiada frecuencia veo cables que quedan "in situ" porque la organización de la conectividad no se mantiene correctamente. Esto luego lleva al "Factor de miedo". Si un miembro del personal no sabe a qué cable está conectado o es demasiado difícil de quitar, se queda y sacan un nuevo latiguillo de la bolsa y lo instalan. Esto pronto pasa a estar fuera de control y la infraestructura se desborda con cables redundantes.

Esto lleva a que ocurra una de dos cosas, ejemplos, los cuales puedo extraer de la experiencia personal. Para el primer escenario (no puedo mencionar nombres, todo lo que puedo decir es que fue un DC operado por uno de los principales supermercados) fui llamado al lugar para revisar parte de la instalación de cableado existente y hacer algunas recomendaciones sobre la expansión del centro de datos, ya que querían agregar más armarios. Cuando entré por primera vez en la habitación, me sorprendió el ruido de las unidades CRAC en las paredes, que estaban trabajando a una capacidad casi máxima. La habitación no estaba demasiado caliente, sin embargo, el problema era el diseño. En este DC, todos los cables, tanto de alimentación como de datos, se colocaron debajo del falso suelo. Este espacio también era un espacio de tratamiento de aire, con el suministro de aire frío. No se canalizaron cables por la parte de arriba. Al levantar algunas de las baldosas, el culpable era obvio; se habían sometido a una serie de actualizaciones en los equipos a lo largo de los años, pero nunca habían eliminado ninguno de los cables redundantes viejos, ya que no tenían un registro lo suficientemente bueno como para comprender qué cables no se utilizaron y cuáles eran críticos para el rendimiento de DC.

Si bien este DC no falló en última instancia, resultó en un plan de transición muy costoso, que implicó el alquiler de una sala de datos externa, mientras que ésta fue completamente rediseñada y reconstruida. Fue un proceso muy largo y costoso que tardó más de un año en completarse. Cabe señalar que el DC original se diseñó y construyó por primera vez a mediados de la década de los 90, cuando el equipo informático y la conectividad eran totalmente diferentes y durante el tiempo continuaron instalado más equipamiento.

El segundo ejemplo está relacionado con una compañía financiera, donde tuvieron que documentar y replicar un parcheo y cableado redundante completo dentro de una de sus salas de datos antes de pasar uno de sus sistemas de cableado existentes al tercero, con trabajo nocturno y luego rectificar, etiquetar y documentar correctamente el sistema erróneo antes de volver a ponerlo en servicio, quitando el sistema redundante original. Este trabajo tardó más de 3 meses en completarse y costó más de £ 250,000.

El segundo elemento con respecto a la buena limpieza se reduce a la limpieza. Con todos los entornos de DC, es esencial mantener el mayor nivel de limpieza. Veo demasiados DC, especialmente aquellos utilizados por organizaciones más pequeñas, donde abundan las malas prácticas. Desafortunadamente, hay dos grupos diferentes que trabajan en la sala de datos; tienen "personas de IT" y "personas de cableado" operando en conjunto y nunca los dos entenderán el problema del otro.

Muchas veces veo una sala de datos o una sala de comunicaciones principal que se utiliza como otro armario de almacenamiento para equipos y embalajes antiguos. Con todo esto viene el polvo, uno de los mayores enemigos del

funcionamiento eficiente de una infraestructura de fibra. La investigación de Fluke afirma que el 85% de todos los errores de fibra se derivan de la contaminación del extremo. NTT indica que más del 80%,

Por lo tanto, este es el problema número UNO con la conectividad de fibra.

La mejor práctica dicta que todo el empaquetado debe dejarse fuera y nunca llevarse a la sala de datos.

Seguridad física

No solo debemos preocuparnos de la amenaza de los ciberataques, sino también la seguridad física de la infraestructura que está amenazada. Los organismos de normalización no han tardado en reaccionar. Cenelec publicó EN 50600-2-5 en 2016, Tecnología de la información - Instalaciones e infraestructuras del centro de datos - Sistemas de seguridad. El ISO / IEC 22237-6, basado en el contenido del estándar Cenelec, se publicó en 2018.

Paralelamente a esta actividad en 2016, se publicó el ANSI / TIA- 5017 - Estándar de seguridad de redes físicas de telecomunicaciones. Esto no solo se centra en los centros de datos, sino que cubre toda la infraestructura física.

Existen varias diferencias clave entre los estándares Cenelec / ISO y ANSI / TIA. Por lo tanto, en 2018 ISO / IEC JTC1 / SC25 / WG3 acordó proponer una versión internacional de este último. El borrador del comité de ISO / IEC CD 24383 se publicó en 2019 y ahora está fuera para comentario final.

ANSI / TIA-5017 describe tres niveles de seguridad de la siguiente manera:

- **SL1 - instalación de seguridad básica:** linstalaciones que siguen las pautas de la familia de estándares de infraestructura de cableado TIA TR-42 con niveles mínimos de seguridad y protección adicionales. Esto se usa típicamente en todas las instalaciones donde existe el deseo de construir una infraestructura de red segura y proteger el cableado de seguridad y el tráfico de red del acceso no autorizado o la interrupción.
- **SL2 - Instalación a prueba de manipulaciones:** instalaciones que reducen la posibilidad de manipulaciones o daños en las instalaciones donde hay un riesgo adicional, vulnerabilidad y la necesidad de una mayor seguridad para proteger la infraestructura y el tráfico de la red.
- **SL3 - instalación de seguridad crítica:** instalaciones destinadas a alcanzar un nivel de seguridad donde el nivel de riesgo se considera alto y se requieren las mejores prácticas de protección. Esto generalmente cubre instalaciones donde la seguridad de la infraestructura de red y la información es crítica.

Si bien ISO / IEC TS 22237-6 (para centros de datos) especifica cuatro clases de protección como se muestra a continuación, pero toda la infraestructura de telecomunicaciones debe estar en espacios que cumplan con sus requisitos de protección de clase 3 (con requisitos de monitorización para vías que no están en espacios de clase 3)

	Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Protection against unauthorised access	Public or semi-public area	Area that is accessible to all autorised personnel (employees and visitors)	Area restricted to specified employees and visitors (other personnel with access to Class 2 shall be accompanied by personnel autorised to access Class 3 areas).	Area restricted to specified employees who have an identified need to have access (other personnel with access to Class 2 or 3 areas shall be accompanied by personnel authorised to access Class 4 areas).
Protection against internal fire	No special protection applied	The area requires to be protected against fire by a detection and suppression system which maintains the function of that area during a fire in that area or one in a Class 1 area	The area requires to be protected against fire by a detection and suppression system which maintains the function of that area during a fire in that area or one in a Class 1 or Class 2 area.	The area requires to be protected against fire by a detection and suppression system which enables critical data centre function to be secured during a fire in that area or one elsewhere in the data centre.
Protection against other internal environmental events	No special protection applied		Mitigation applied	
Protection against unauthorised access	No special protection applied		Mitigation applied	

Esto demuestra una sutil diferencia de enfoque ya que la ISO / IEC TS 22237-6 describe quién puede acceder a los espacios (antes de definir las soluciones de seguridad de dichos espacios) y qué protección contra incendios se aplica, mientras que ANSI / TIA-5017 describe las soluciones de instalación de la infraestructura de telecomunicaciones en cualquier espacio.

Propuesta para el desarrollo del ISO / IEC CD 24383

Con respecto al sistema SL en ANSI / TIA-5017, la diferenciación de los niveles implica una redacción vaga como “alto”, “más alto”, “agregado” en relación con el riesgo y “mejor” en relación con las prácticas. Todas estas son palabras que Cenelec e ISO / IEC intentan evitar.

La alternativa es considerar las soluciones primero como se muestra en la siguiente tabla:

Topic		Security Grade 1	Security Grade 2	Security Grade 3
Pathways	Access control	x	✓	✓
	Intrusion resistance	x	✓	✓
	Monitoring	x	x	✓
Spaces	Access control	x	✓	✓
	Intrusion resistance	x	x	✓
	Monitoring	x	x	✓

En resumen, ANSI / TIA-5017 tiene tres niveles de seguridad en relación con las prácticas. ISO / IEC TS 22237-6 por otro lado tiene cuatro clases de protección con más detalle. Por lo tanto, se adoptó un enfoque alternativo que (a) acerca los dos estándares y (b) evita declaraciones vagas de riesgo y soluciones, para adoptar tres clases de seguridad con más claridad en ISO / IEC CD 24383.

Se está dando más énfasis a la colaboración continua para mantener y actualizar el estándar como 5G. IoT continúa acelerando sus implementaciones. Con todo el arduo trabajo que se ha dedicado al desarrollo de estándares, es importante que no solo los operadores de DC los conozcan, sino también todos los administradores de infraestructura.

European Headquarters
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
England

T: +44 (0) 121 326 7557
E: sales@excel-networking.com

Mayflex MEA DMCC
Office 22A/B
AU (Gold) Tower
Cluster I
Jumeirah Lake Towers (JLT)
Dubai
United Arab Emirates
PO Box 293695

T: +971 4 421 4352
E: mesales@mayflex.com

www.excel-networking.com