White Paper
La vulnérabilité des Data Centers

Au cours des derniers mois, l'accent a été mis sur la sécurité des données, compte tenu de l'expansion rapide de l'Internet des objets (Iot). Cela a soulevé la question de la vulnérabilité de l'installation qui détient ou stocke ces données.

Deux études ont été publiées au cours des 18 derniers. La première, qui porte sur les appareils compatibles avec le POE, prévoit une croissance du marché de plus de 19 % et des ventes de plus de 1 milliard de dollars en 2021. La deuxième enquête a estimé qu'il y aura 36 Milliards d'appareils connectés d'ici 2021, atteignant 75,5 Milliards d'ici 2025. Avec ce taux de croissance, la sécurité entourant le stockage des données est critique.

Bien qu'il y ait beaucoup de publications sur l'importance de la cybersécurité, à juste titre, on a très peu parlé des autres vulnérabilités entourant les centres de données (DC). Il y a deux aspects clés dont nous devons tenir compte et qui pourraient influer sur le rendement continu des DC.

L'entretien quotidien

Le premier aspect porte sur ce que j'appelle la « gestion interne ».

Un bon entretien est essentiel et peut également être divisé en deux parties, la première concernant le confinement. Bien que la conception initiale puisse avoir été « adaptée à l'usage » au moment de sa construction, elle peut bientôt être dépassée si la complaisance s'installe. Trop souvent, je vois des câbles laissés sur place parce que les dossiers VDI ne sont pas tenus correctement. Cela mène ensuite au « facteur de peur ». Si un membre du personnel ne sait pas à quel câble il est raccordé ou s'il est trop difficile à enlever, il le laisse et il prend un nouveau cordon de raccordement et l'installe. Cela devient rapidement incontrôlable et le site déborde de câbles redondants.

Deux choses peuvent se produire. En voici des exemples tires de mon expérience personnelle.

Premier scénario (je ne peux pas citer de noms, tout ce que je peux dire, c'est qu'il s'agissait d'un DC exploité par l'un des grands supermarchés de la rue) J'ai été appelé sur place pour examiner une partie de l'installation de câblage existante et faire des recommandations concernant l'agrandissement de la salle des données parce qu'on voulait ajouter des armoires. Quand je suis entrée dans la pièce, j'ai été frappée par le bruit des unités du CRAC sur les murs - elles fonctionnaient presque à pleine capacité. La pièce n'était pas trop chaude mais le problème était dans la conception elle-même. Dans cette CRAC, tous les câbles, alimentation et données – étaient acheminés sous le faux plancher. Cet espace était également un espace de traitement d'air avec l'alimentation en air froid. Aucun câble n'était acheminé par le haut. En soulevant certaines des dalles l'erreur était flagrante : ils avaient eu de nombreuses mises à niveau de l'équipement au fil des ans, mais ils n'avaient jamais retiré les câbles précédents et ils n'avaient pas suffisamment d'information pour comprendre quels câbles étaient inutilisés et essentiels à la performance du courant continu. Bien que ce DC fonctionnait, il y à eu un plan de transition très couteux qui a nécessité la location d'une salle externe pour que celle-ci puisse être entièrement remaniée et reconstruite. C'était un processus très long et coûteux qui a pris plus d'un an. Il convient de noter que la VDI d'origine avait été conçue et construite au milieu des années 1990, alors que l'équipement informatique et la connectivité étaient plus récent et qu'on essayait tout simplement d'installer plus d'équipement.

Le deuxième exemple est lié à une organisation financière. Ils ont dû documenter et recâbler l'une de leurs salles de données avant de faire la transition d'un de leurs systèmes de câblage existants vers une nouvelle salle : travail de nuit, recherche d'erreur pour rectification, ré étiqueter correctement le système avant de le remettre en service et de supprimer le système redondant original. Ce travail a pris plus de 3 mois et a coûté plus de £250,000.

Le deuxième élément concernant la bonne tenue des locaux se résume à la propreté. Dans tous les environnements DC, il est essentiel que le plus haut niveau de propreté soit maintenu. Je vois trop de DC, surtout ceux qui sont utilisés par de plus petites organisations, où la pratique est mauvaise. Malheureusement, il y a deux groupes différents qui travaillent dans la salle de données; il y a des « gens de l'IT » et des « gens du câblage » qui travaillent en tandem et jamais les deux ne comprendront le problème de l'autre.

Trop souvent, je vois une salle de données ou une salle de communication principale utilisée comme une autre armoire de rangement pour les vieux équipements et les emballages. Avec tout cela vient la poussière, l'un des plus grands ennemis à l'exploitation efficace d'une infrastructure de fibre. Les recherches de Fluke indiquent que 85% de toutes les défaillances des fibres proviennent de la contamination en bout de ligne. NTT affirme que c'est plus de 80%. C'est donc le

problème numéro UN de la connectivité par fibre optique.

Les règles de l'art veulent que tous les emballages soient enlevés à l'extérieur et ne soient jamais introduits dans la salle de données elle-même.

La sécurité physique

Ce n'est pas seulement la menace de cyberattaques qui doit nous préoccuper, c'est aussi la sécurité physique de l'infrastructure qui est menacée. Les organismes de normalisation n'ont pas tardé à réagir. Cenelec a publié la norme EN 50600-2-5 en 2016, Technologies de l'information – Installations et infrastructures de centres de données – Systèmes de sécurité. La norme ISO/CEI 22237-6, basée sur le contenu de la norme Cenelec, a été publiée en 2018.

Parallèlement à cela en 2016, la norme ANSI/TIA- 5017 - Télécommunications Physical Network Security Standard a été publiée. Il ne s'agit pas seulement des DC, mais de toute l'infrastructure matérielle.

Il existe plusieurs différences clés entre les normes Cenelec/ISO et ANSI/TIA. Par conséquent, en 2018, l'ISO/IEC JTC1/SC25/WG3 a accepté de proposer une version internationale. La version préliminaire de la DC ISO/CEI 24383 a été publiée en 2019 et est maintenant disponible.

ANSI/TIA-5017 décrit trois niveaux de sécurité comme suit :

- **SL1 - Installation de sécurité de base :** Installations qui suivent les lignes directrices de la famille de normes d'infrastructure de câblage TIA TR-42 avec un minimum de niveaux de sécurité et de protection supplémentaires. Cette fonction est généralement utilisée dans toutes les installations où l'on souhaite construire une infrastructure réseau sécurisée et protéger le câblage de sécurité et le trafic réseau contre tout accès ou interruption non autorisé.
- **SL2 - Installation résistante à l'altération:** Installations qui réduisent la possibilité d'altération ou d'endommagement du site où il y a un risque supplémentaire, la vulnérabilité et la nécessité d'une sécurité plus élevée pour protéger l'infrastructure et le trafic réseau.
- **SL3 - Installation de sécurité critique:** Installations destinées à atteindre un niveau de sécurité où le niveau de risque est considéré comme élevé et où les meilleures pratiques de protection sont requises. Il s'agit généralement d'installations où la sécurité de l'infrastructure et de l'information du réseau est essentielle.

Alors que l'ISO/IEC TS 22237-6 (pour les centres de données) spécifie quatre classes de protection comme indiqué ci-dessous mais que toutes les infrastructures de télécommunications doivent être dans des locaux conformes à ses exigences pour la classe de protection 3 (avec les exigences de surveillance pour les voies qui ne sont pas dans les espaces de classe 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		

Ceci démontre une différence subtile dans l'approche puisque le ISO/IEC TS 22237-6 décrit qui peut accéder aux espaces (avant de définir les solutions de sécurité de ces espaces) et quelle protection contre le feu est appliquée, alors que l'ANSI/TIA-5017 décrit les solutions d'installation de l'infrastructure de télécommunication dans n'importe quel espace.

Proposition pour l'élaboration de la DC ISO/CEI 24383

En ce qui concerne le système SL dans l'ANSI/TIA-5017, la différenciation des niveaux implique des formulations vagues comme « élevé », « supérieur », « ajouté » par rapport au risque et « meilleur » par rapport aux pratiques. Ce sont tous des mots que Cenelec et ISO/IEC essaient d'éviter.

l'alternative consiste à examiner les solutions d'abord, comme le montre le tableau suivant :

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 résumé, l'ANSI/TIA-5017 a trois niveaux de sécurité par rapport aux pratiques. ISO/IEC TS 22237-6, par contre, elle a quatre classes de protection avec plus de détails. Par conséquent, une approche alternative qui (a) rapproche les deux normes et (b) évite les déclarations vagues de risque et de solutions, a été adoptée pour adopter trois classes de sécurité avec plus de clarté dans la ISO/IEC CD 24383.

La collaboration continue met davantage l'accent sur le maintien et la mise à jour de la norme 5G. L'Iot continue d'accélérer son déploiement. Avec tout le travail acharné qui a été fait pour élaborer des normes, il est important que non seulement les exploitants de DC en soient conscients, mais tous les gestionnaires de l'infrastructure.

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