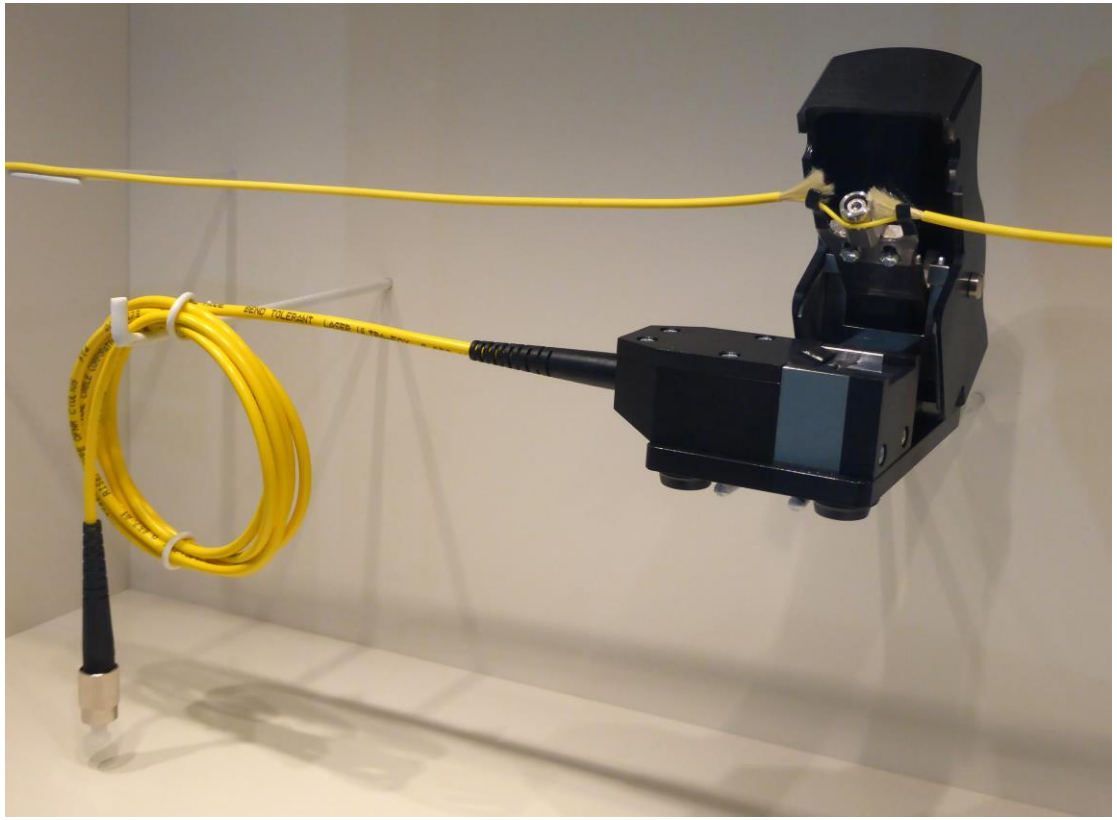
Pouvez-vous détecter un accès non autorisé à votre câble de données?

CONNECTCOM

Situation initiale

Les entreprises investissent beaucoup d'argent pour des concepts de cybersécurité, c'est-à-dire: afin d'empêcher toute pénétration dans la partie active de leurs réseaux.
L'infrastructure physique des réseaux est ici souvent oubliée, c'est-à-dire les câbles en fibres de verre et en cuivre qui transportent les données critiques. Si elle n'est pas prise en compte dans le concept de sécurité, l'infrastructure de communication **représente un point faible bien trop négligé.**

Selon les statistiques, 75% de tous les câbles de réseau se trouvent dans des espaces publiquement accessibles, où ils peuvent facilement être écoutés à l'aide de coupleurs à cintrage. Cela les rend à la fois fragiles et faciles d'accès.



Source: Wikipedia «Biegekoppler_an_einem_Glasfaserkabel»

CONNECTCOM

Questions

- Comment l’infrastructure de communication optique passive peut-elle être protégée de façon complète et judicieuse sans que des mesures constructives d’importance soient nécessaires?
- Quel mécanisme de sécurité automatisé reconnaît en temps réel des manipulations sous forme d’écoutes, de mise hors service ou d’endommagement physique?

CONNECTCOM

Solution

VANGUARD CS™ est une solution de cybersécurité pour les infrastructures de réseau (layer-1) destinée à défendre et à protéger les réseaux critiques contre les attaques physiques. En recourant à des technologies brevetées, **VANGUARD CS™** assure l'intégrité et la disponibité de données de réseau en surveillant les fibres libres dans des câbles optiques. Cette surveillance en continu 24h/24 7j/7, elle permet au système de détecter et de signaler immédiatement même les **manipulations** mêmes les tentatives d'infraction les plus subtiles aux fins du **vol de données** (écoute) ou de **denial-of-Service** (mise hors service).

Source: Illustration de produit «VANGUARD CS™»

CONNECTCOM

Avantages

- La pose d’infrastructure de communication dans les zones protégées devient inutile
- L’infrastructure existante peut être facilement et rapidement protégée 7/24/365
- La technologie Smart-Filtering™ élimine les fausses alarmes en apprenant et en filtrant les activités quotidiennes normales dans l’environnement
- Pas de goulets d’étranglement de largeurs de bandes ni d’atteinte à la performant du réseau
- Alarme en temps réel

Des questions?

L’équipe de Connect Com se tient à votre disposition!

Andreas Haupt
Développement du secteur d’activité
+41 79 333 91 35
andreas.haupt@ccm.ch

David Stoller
Développement du secteur d’activité
+41 79 333 91 31
david.stoller@ccm.ch

CONNECTCOM

Sites de la société

Connect Com AG
Rothenburg, Suisse

Connect Com SA
Gland, Suisse romande

Connect Com GmbH
Nürtingen, Allemagne

CONNECTCOM

Connecting the dots