Table ronde : « Tous connectés, tous accompagnés, tous protégés ! »

Colloque TRIP d'automne 2021 de l'Avicca

Intervention de Loïc GUÉZO - Secrétaire général du Clusif

CLUSIF

Le Clusif est l'association de référence de la sécurité du numérique en France à travers ses conférences thématiques et les publications de ses groupes de travail.

Il réunit en parfaite équité au sein de deux collèges, offreurs et utilisateurs, tous les secteurs d'activité autour de la cybersécurité et de la confiance numérique.

Le Clusif, c'est aussi :

- Le Panorama de la cybercriminalité - #Panocrim
- L'étude Menaces informatiques et pratiques de sécurité en France - #MIPS
- L'exercice de cybercrise ECRANS
- GT Systèmes industriels (IoT)
- GT CoTer

L'ANIMATEUR DU GROUPE

Damien ALEXANDRE
SOLURIS

LE CO-ANIMATEUR DU GROUPE

Arnaud FILEUX
CONSEIL DEPARTEMENTAL DE L'ESSONNE

ESPACE COTER

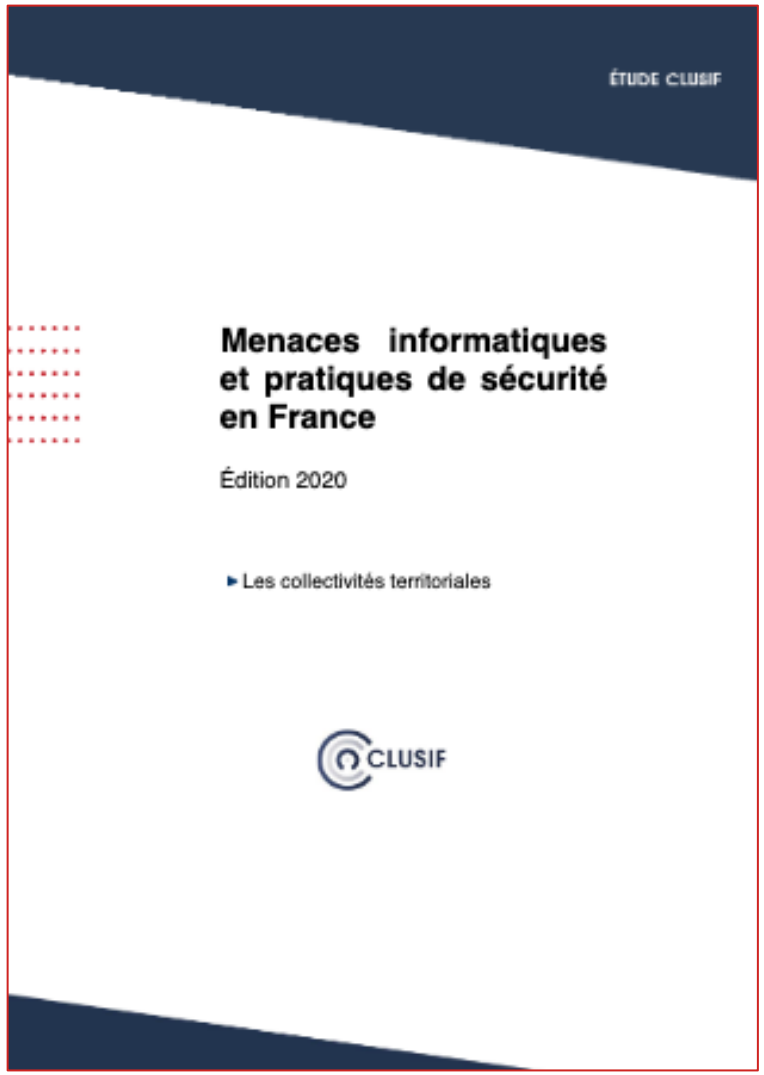
L'Espace CoTer, un lieu d'échange indispensable pour les collectivités territoriales

L'Espace CoTer du Clusif est un espace de travail réservé aux référents sécurité, responsables de la sécurité informatique (RSI) ou encore responsables de la sécurité des systèmes d'information (RSSI) œuvrant au sein des Collectivités territoriales adhérentes de l'association. L'objectif de cet Espace est fondamentalement de **favoriser l'échange de savoir-faire et de retours d'expériences** entre ses membres mais aussi de proposer des synergies avec d'autres Espaces ou Groupes de Travail du Clusif traitant ponctuellement des collectivités territoriales.

Les rencontres organisées par l'Espace CoTer se tiennent trois fois par an et sont accessibles en visioconférence.

Vous souhaitez participer ? Rejoignez-nous !

MIPS 2020



Collectivités territoriales : une amélioration à géométrie variable, mais encore insuffisante

Pour la troisième fois, le Clusif s'intéresse à la façon dont les collectivités territoriales intègrent la cybersécurité dans leur fonctionnement. Pour cela un sondage a été réalisé auprès de 202 collectivités en début d'année 2020. Les résultats ainsi obtenus ont été redressés afin de correspondre à la réalité de la répartition des collectivités. Ces derniers ont ensuite été analysés par des experts provenant de différents horizons professionnels, mais aussi des collectivités territoriales françaises.

Il en ressort que les collectivités, avec l'appui de 70 % des directions générales ont progressé dans la formalisation de leur PSI ; cependant, cette dernière a encore du mal à sortir de la sphère DSI.

Corollaire de la PSI, la fonction de RSSI est présente dans la majorité des collectivités, mais il reste difficile pour beaucoup de la dédier à un poste à plein temps, ce qui a pour conséquence de placer le RSSI dans une position de juge et partie qui ne permet pas une réelle liberté de parole ou une évaluation correcte des enjeux par les dirigeants.

Bien qu'en amélioration, la SSI n'est pas encore l'affaire de tous et les moyens tant humains que financiers ne sont pas la plupart du temps à la hauteur des enjeux. Bien que le sentiment de dépendance au SI soit fort, le budget alloué à la cybersécurité reste la variable d'ajustement des DSI avec l'absence de budget dédié et/ou pérenne. Cependant, ce dernier est en augmentation par rapport à la précédente étude.

Du côté des ressources humaines (RH), la mise en place de chartes d'usage des SI continue de progresser même si les communautés de commune restent à la traîne. Il reste malgré tout difficile de gérer les départs ou les changements de poste. Un point remarquable concerne la mise en œuvre de programmes de sensibilisation pour les différentes populations, mais malheureusement sans pour autant en évaluer l'impact réel.

CLUSIF

ACTUALITÉ

Isère : une mairie paralysée par une attaque informatique "ransomware"

3 FÉVRIER 2020 A 16:40 PAR FLORENT DELIGIA

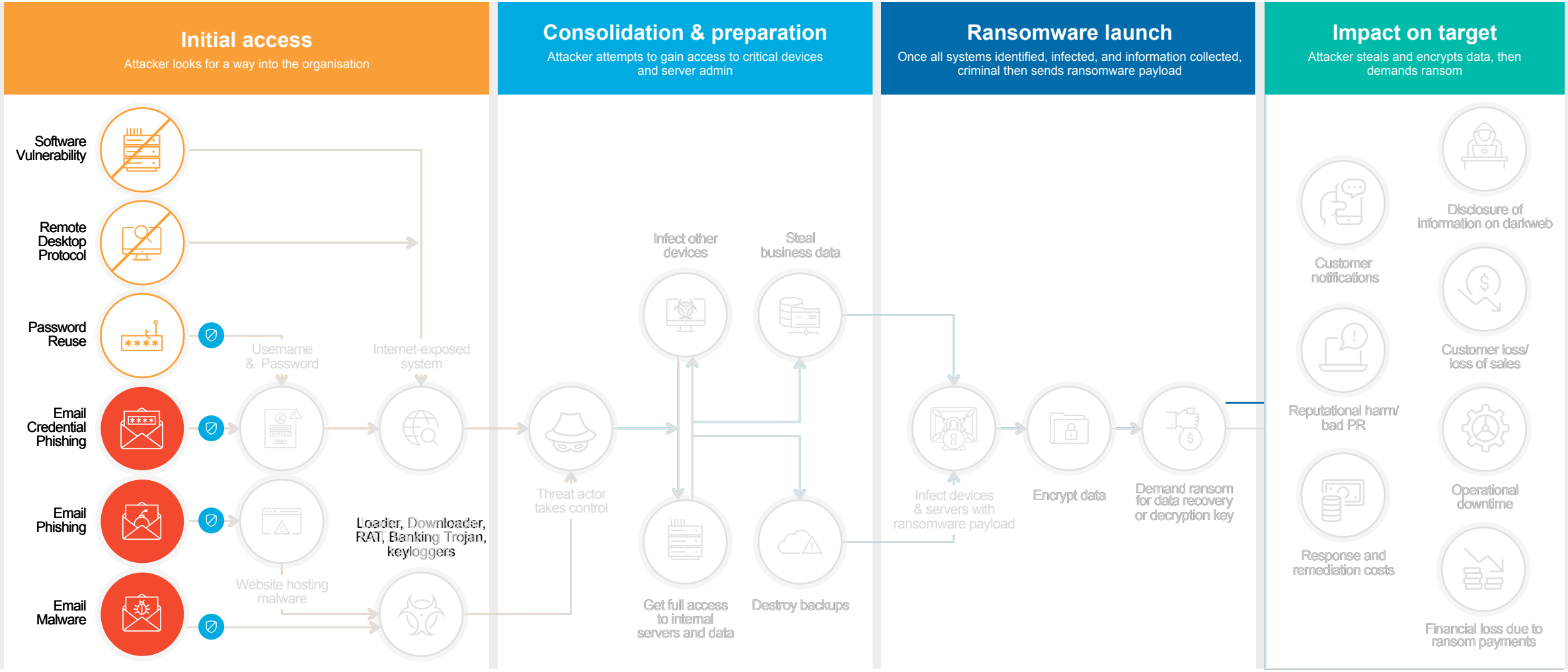
La mairie de Tullins dans l'Isère a été la cible d'une attaque informatique de type "ransomware" ou "rançongiciel".

Les attaques de type "*ransomware*" ou "*rançongiciel*" sont assez courantes. Les escrocs du web envoient un mail avec une pièce jointe qui contient un virus informatique chargé de chiffrer les données. Une fois que la cible lance le logiciel, elle ne peut plus accéder à certains fichiers sur l'ordinateur. Les escrocs demandent alors le paiement d'une rançon pour débloquer l'accès à ces fichiers chiffrés (sans aucune garantie que cela sera le cas au final).

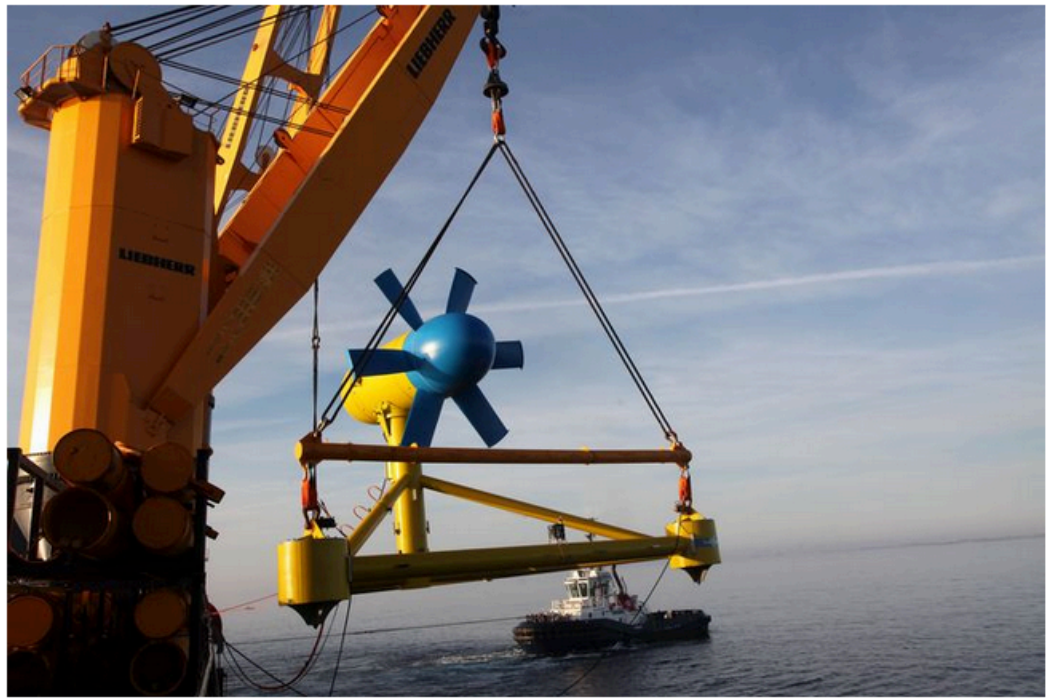
La ville de Tullins dans l'Isère vient d'être la cible d'une attaque de ce type, selon *Le Dauphiné*. Les données auraient été chiffrées dans la nuit du jeudi 30 au vendredi 31 selon la mairie. Agents et élus n'ont plus accès à leurs fichiers tandis que la ville a fait savoir qu'elle ne payerait pas de rançon. Une enquête a été ouverte par la gendarmerie.

CLUSIF

Quid des rançongiciels ?



proofpoint.



Même immergée à 55 mètres de profondeur, une hydrolienne n'est pas à l'abri des pirates. En octobre 2015, des hackers se sont attaqués à l'ordinateur qui permettait la connexion satellitaire entre l'hydrolienne de Sabella D10, installée au large d'Ouessant (Finistère), et Quimper. *"On s'est rendu compte que l'un des serveurs était crypté, un message était inscrit sur l'écran",* raconte Jean-François Daviau, PDG de la PME quimpéroise.

— TECH —

États-Unis : des pirates ont tenté d'empoisonner l'eau potable d'une ville de 15.000 habitants !

ACTUALITÉ

Classé sous : CYBERGUERRE , TRAITEMENT DE L'EAU , STATION D'ÉPURATION

Louis Neveu
Journaliste

Publié le 09/02/2021

Une cyberattaque suspectée de causer un black-out en Ukraine

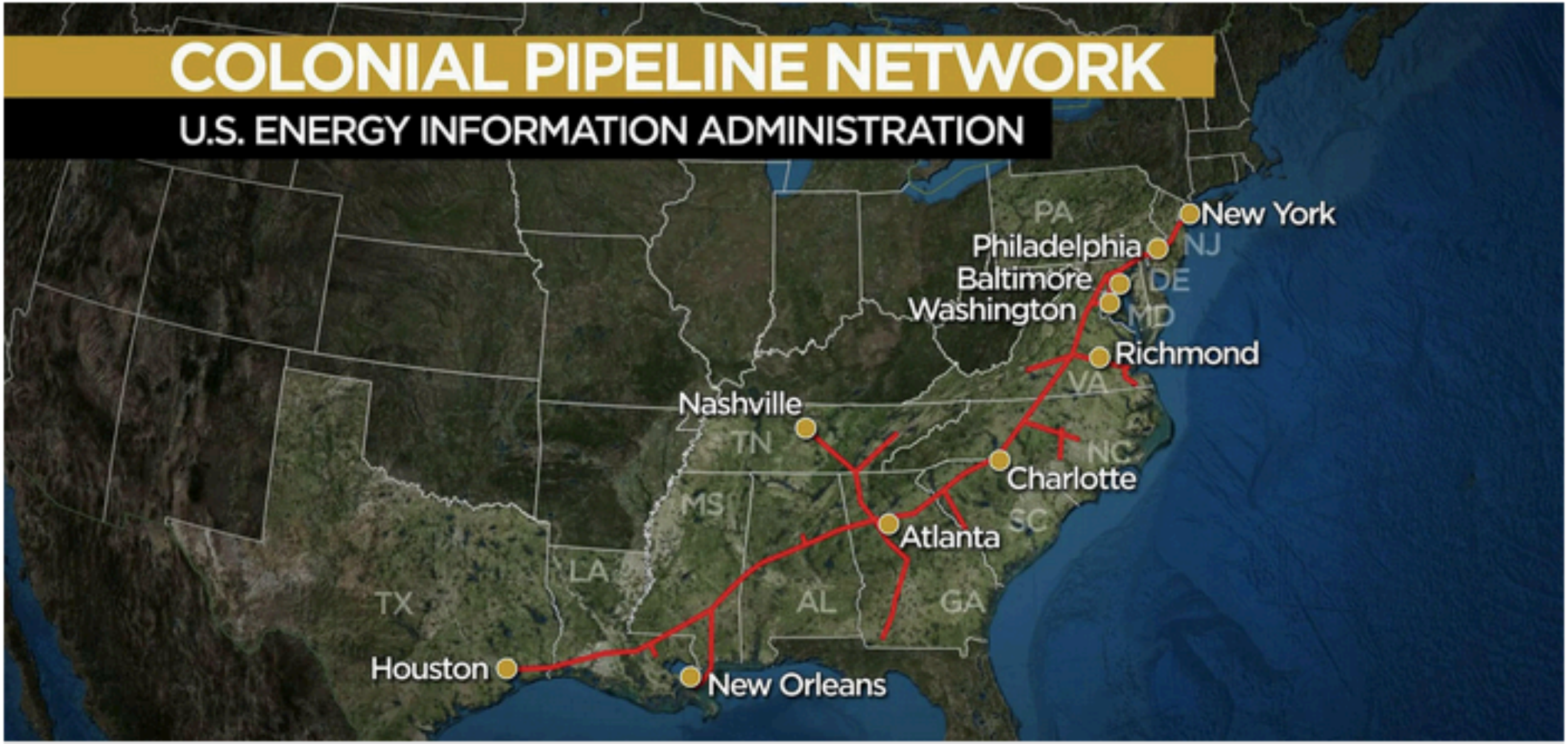
Lucian Constantin, IDG NS (adaptation SL) , publié le 20 Décembre 2016

Suite à une nouvelle panne de courant, la compagnie nationale d'électricité de l'Ukraine enquête pour savoir si une attaque de cyberpirates est à l'origine du problème.

Des cyberhackers pourraient être à l'origine de la nouvelle panne qui a touché le réseau électrique de l'Ukraine le week-end dernier. (Crédit D.R.)

Les ingénieurs d'Ukrenergo, la compagnie d'électricité ukrainienne, ont commuté l'équipement de commande en mode manuel et commencé à rétablir la puissance par palier de 30 minutes, a dit Vsevolod Kovalchuk, directeur d'Ukrenergo, dans un billet posté sur Facebook. Il a fallu 75 minutes pour restaurer toute la puissance électrique dans les zones touchées de la région, où les températures descendent jusqu'à -9 en ce moment. Une des causes suspectées est « une interférence externe à travers le réseau de données » a déclaré sans plus de précision Vsevolod Kovalchuk. Les experts en cybersécurité de la société étudient la question et publieront très bientôt un rapport.

CLUSIF



Le colonial pipeline traverse les États-Unis à travers les États du sud et du sud-est de Linden dans l'État de New-York jusqu'à Houston dans l'État du Texas (Source : WSLS.com).

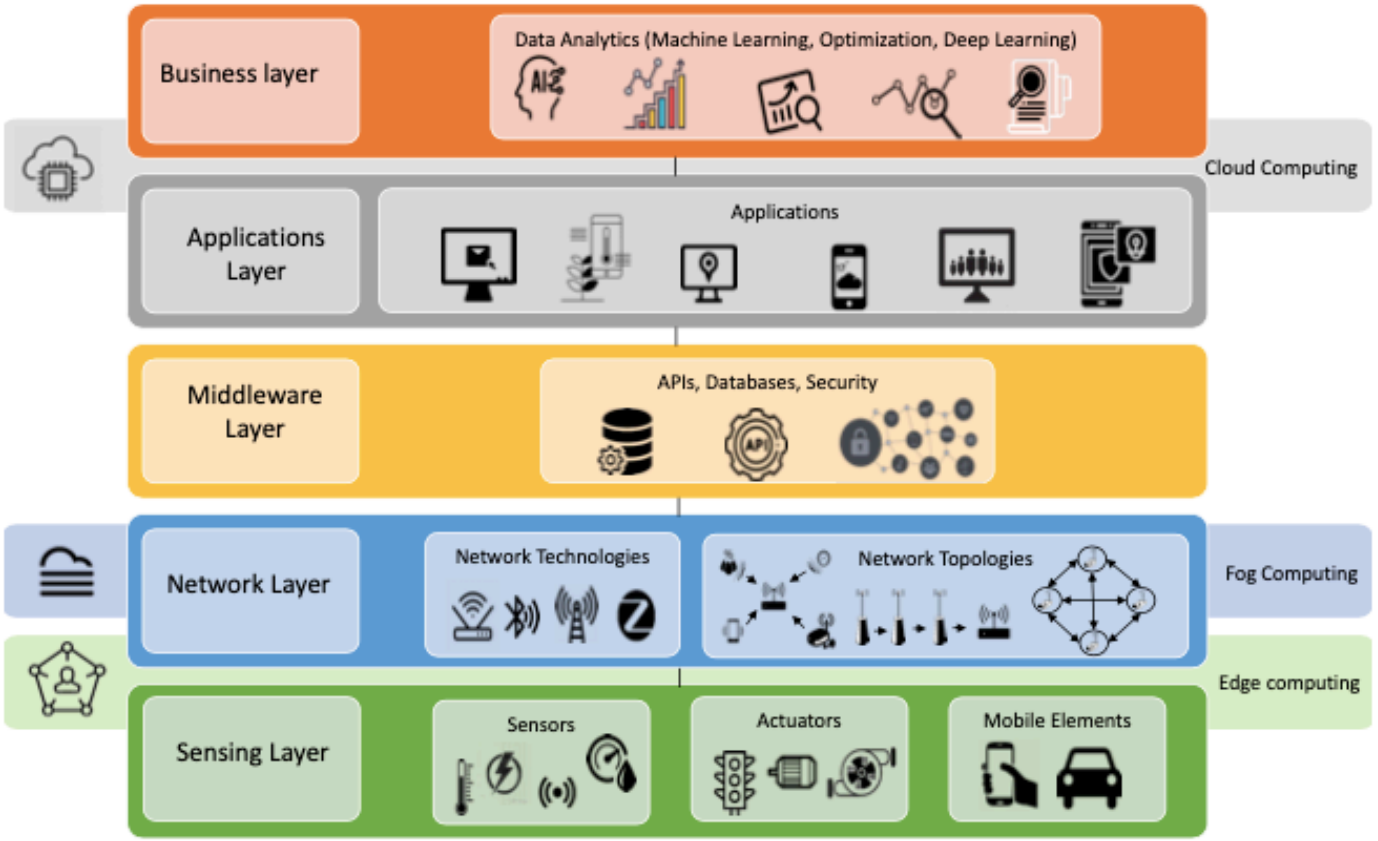


Figure 3. IoT Architecture.

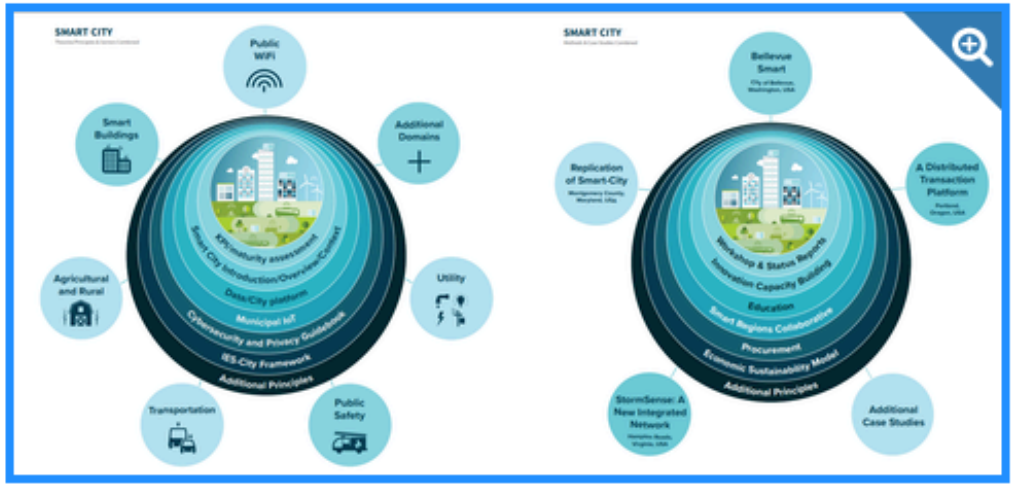
https://www.mdpi.com/2624-6511/4/2/24

CLUSIF

CYBER-PHYSICAL SYSTEMS

NIST Smart Cities and Communities Framework Series

Background: When considering smart technologies, cities and communities seek best practices for achieving standards-based solutions that are replicable, scalable and readily adoptable.



Smart Cities and Communities Framework Structure

Goal: The NIST Smart Cities and Communities Framework (SCCF) series will provide cities and communities with best practices and technical guidelines for the planning, developing and implementing smart solutions. Industry stakeholders and the research community can use the NIST SCCF as a reference to further their innovation and product development goals, and to improve the quality of service. The target audience includes city and community officials, technology innovators, researchers, project planners and managers, and other implementers.

Figure 4. Challenges for IoT in Smart Cities.

https://www.mdpi.com/2624-6511/4/2/24

CLUSIF

Table ronde : « Tous connectés, tous accompagnés, tous protégés ! »

Colloque TRIP d'automne 2021 de l'Avicca

Contact : Loïc GUÉZO - Secrétaire général du Clusif

loic.guezo@clusif.fr