Article
Réseaux et cybermenaces

PSM - N°260 - Juillet 2020

dossier

Réseaux et cybermenaces

Ils sont partout dans nos vies et nous sont devenus indispensables. Le monde de la sécurité n'y échappe pas et il se doit de protéger ses réseaux contre les cybermenaces. Si les choses évoluent dans le bon sens, tout n'est pas encore parfait.

Pour protéger vos réseaux, les solutions existent !

Comme le rappelle la commissaire européenne Mariya Gabriel dans ces colonnes, la cybersécurité est fondamentale pour assurer le respect de notre vie privée ainsi que le bon fonctionnement de nos infrastructures. Protéger les réseaux est donc un impératif vital. Heureusement, la défense s'organise.

En ce qui concerne les cybermenaces, un petit rappel à la loi s'impose. Tout chef d'entreprise est civilement et pénalement responsable des données à caractère personnel liées à son système d'information et de son utilisation par ses collaborateurs. Il doit donc veiller à être en conformité avec les licences de logiciels et contenus soumis à copyright. L'ensemble des postes de travail et de solutions nomades doivent impérativement disposer d'un antivirus et d'un pare-feu. Par ailleurs, il faut que les dirigeants sensibilisent l'ensemble des collaborateurs à la menace, ainsi que leurs prestataires, quelle que soit leur taille.

« On doit rappeler à tous les acteurs de la filière sécurité et à tous ses partenaires, que la dimension cybersécurité de leur métier est primordial, relève de leur responsabilité, insiste Vincent Dupart, président directeur général de STid et du tout nouveau syndicat professionnel Spac (Smart Physical Access Control). *Si nous devons les accompagner dans cette démarche, les aider, ils ne peuvent pas tout attendre de nous et doivent aussi se saisir de la question. »*

Cependant, il ne faut pas désespérer. Les choses évoluent dans le bons sens comme le reconnaît le général Didier Tisseyre, commandant de la cyberdéfense (Comcyber) aux ministère des Armées : *« La prise de conscience est amorcée : les grandes entreprises et administrations ont globalement intégré la culture de cyberdéfense. Néanmoins, les efforts consentis doivent être intensifiés. Et les PME et TPE et les petites structures administratives ou associatives doivent poursuivre leur acculturation. »*

Article
Réseaux et cybermenaces

PSM - N°260 - Juillet 2020

dossier

Réseaux et cybermenaces

© Getty Images

A l'instar du contrôle d'accès

« La création de Spac correspond à cette volonté du monde du contrôle d'accès de porter une démarche commune en matière de sécurité du contrôle d'accès et des réseaux dans lesquels il s'insère, insiste Vincent Dupart. *D'ailleurs, la crise du Coronavirus a agi comme un révélateur : en temps de crise, les entreprises et organisations sont surexposées aux cybermenaces. Par exemple, le port autonome de Marseille et le MED Europe Terminus ont dû faire face à une attaque cyber simultanée. De son côté, pour éviter d'être exposée aux cybermenaces, la CMA CGM a utilisé le support papier pour gérer les conteneurs… Tout cela pour souligner le fait qu'il est plus que jamais nécessaire de pousser des technologies sécurisées et partagées par tous comme le protocole SSCP pour sécuriser les accès et l'IoT que poussent le Spac et déjà adoptées par les principaux industriels français. Enfin, il faut absolument nous organiser, comme nous le faisons au sein du Safe Cluster pour porter les solutions de sécurité françaises… »*

« En temps de crise, les entreprises et les organisations sont surexposées aux cybermenaces. »

VINCENT DUPART, PDG DE STID

Chez ARD, on défend aussi cette approche technologique de la sécurité des réseaux et des solutions de sécurité. *« Certes, certains n'ont toujours pas mesuré le danger représenté par les cybermenaces, la protection de leurs réseaux n'est pas toujours prioritaire. Mais aux fabricants aussi de faire en sorte d'éduquer le marché, de porter la bonne parole, de développer des solutions toujours plus sûres,* martèle Emmanuel Brunet. *Ainsi, en nous appuyant sur les recommandations de l'Anssi, les clés cryptographiques sont renseignées pas l'exploitant lui-même dans des SAM (Secure Access Module), dans lesquelles elles sont impossibles à récupérer… »*

Chez Fichet Group, la collaboration avec l'Anssi est ancienne. *« Nous nous sommes très tôt focalisés sur l'aspect cybersécurité,* explique Dominique Auvray, directeur marketing chez Fichet Group. *Et de plus en plus de fabricants de contrôle d'accès intègrent les prescriptions de l'Anssi. C'est plus du côté de certains utilisateurs et installateurs que le bât blesse car ils ont du mal à appréhender, non seulement, l'intérêt de se protéger contre les cybermenaces, mais aussi, tout simplement, à intégrer les compétences nécessaires au déploiement de ce type de solutions. »*