**Sécurisation des accès réseaux, un enjeu majeur pour les entreprises**

Les entreprises d’aujourd’hui sont confrontées à une croissance exponentielle du nombre d’équipements interconnectés au sein de leurs réseaux informatiques : Téléphone IP, switches, routeurs, PC de bureau, ordinateurs portables, photocopieurs, caméras IP, des objets IoT (l'Internet des objets), équipements de visioconférences, ainsi qu’une multitude de mode d’accès à leurs réseaux internes qu’il faudra sécuriser, allant de la connexion des utilisateurs de l’entreprise à Internet, aux accès distants via des connexions VPN des employés itinérants (commerciaux) ou autres collaborateurs qui font du Télétravail.

# Les risques de réseau pas assez ou non sécurisés

Nous avons assisté l’année dernière en France à de nombreuses attaques de ransomwares ciblant différents organismes d’état ou privé : parmi eux, [Go Sport et Courir](https://www.lemondeinformatique.fr/actualites/lire-go-sport-et-courir-victimes-d-un-ransomware-77403.html), victimes d’un ransomware en octobre 2019 causant la fermeture de leurs magasins. D’autres entreprises ont aussi essuyé des attaques via des crypto-locker (ransomware) ; Altran, CHU de Rouen, Fleury Michon, Picoty SA, le Centre hospitalier d'Issoudun, l'agglomération du Grand Cognac qui elle aussi a fait les frais d’un ransomware, logé dans les serveurs de fichiers. Ces serveurs ont été infectés et chiffrés, les rendant inutilisables.

D’autres organismes comme le groupe Riveira Beach n’ont pas eu le choix que de payer une rançon qui s’élevait à 600 000 dollars (65 bitcoins) pour récupérer l’utilisation de leur système d’information. (***Attention tout de même, il n'existe aucune garantie de voir ses fichiers décryptés, malgré le paiement de la rançon exigée par les pirates)***

**N**ous devons nous attendre à une recrudescence de ces ransomwares et surtout à un ciblage plus affiné des cibles potentielles qui touchera beaucoup moins le grand public mais qui visera des organismes beaucoup plus rémunérateurs tels que les aéroports, les Hôpitaux, les grandes entreprises et les organismes d’états – aussi, la sécurisation des accès devient critique, surtout avec de nouveaux challenges comme le « BYOD »

# Bring Your Own Device

Nous assistons par ailleurs à un nouveau phénomène appelé BYOD (Bring Your Own Device) : des utilisateurs qui accèdent aux ressources de l’entreprise via leurs propres équipements (Tablettes, Smartphones…), venant ainsi complexifier la tâche des équipes informatiques. Elles doivent prendre en charge la multiplication de ces nouveaux appareils et la nécessité de les authentifier et de les sécuriser avant de leur donner un accès au réseau. Ceci afin de protéger le système d’information contre les menaces croissantes des virus et malwares qui peuvent compromettre la sécurité des accès aux données de l’entreprise.

Il est donc primordial que les entreprises intègrent dans leurs politiques de sécurité ces nouveaux terminaux pour qu’ils soient conformes aux règles préétablies. Les entreprises devront systématiquement vérifier les applications installées sur ces appareils, interdire celles potentiellement dangereuses, pouvoir aussi effacer les données à distance en cas de perte ou de vol d’un terminal.

**Il s’agit-là de la première étape** intervenant au niveau de la phase d'authentification, avant que d'éventuels programmes malveillants puissent endommager le système d’information de l’entreprise.

**Dans une seconde étape** : la sécurité du réseau requiert la vérification de la conformité des

terminaux avec des politiques de sécurité. Ces politiques dépendent du type d'utilisateur,

d'équipements utilisés ainsi que du système d'exploitation.

En cas de non-conformité, des actions peuvent être appliquées tel qu’un refus d’accès et une mise en quarantaine suivi d’une remédiation.

Dans un vlan de quarantaine, un utilisateur peut se voir accorder un accès très limité au réseau. Dans le cas où la base de données antivirale de l’utilisateur est obsolète, le vlan va lui permettre de procéder à sa mise à jour avant toute autorisation d’accès au réseau de votre entreprise.

Pour faire face à ces menaces, il devient plus que nécessaire de bien contrôler et sécuriser les accès aux réseaux en se dotant de solutions éprouvées sur le marché de la sécurité.

**En conclusion** :

Comme nous l'avons vu tout au long de cet article, les solutions de NAC (Network Access Control) vous permettent de surveiller, d’identifier et de gérer les périphériques réseau de manière centralisée. Elles disposent d’un contrôle total sur l'ensemble des périphériques et utilisateurs d'un réseau en temps réel. Ces solutions contribuent à renforcer et à améliorer la sécurité réseau des entreprises grâce au déploiement de stratégies de sécurité. Elles empêchent les virus et les malwares d’infecter vos systèmes, évitent les fuites d’informations de votre entreprise et de vos clients et renforcent ainsi les directives de protection des données énoncées dans le cadre de la loi sur le RGPD (Règlement général sur la protection des données).

Le marché des outils de contrôle est riche, avec des solutions opensource (OpenNAC), des solutions de grands noms de la sécurité et du réseau (ARUBA Networks, Fortinet/FortiNac, Cisco ISE, Extreme Networks/ExtremeControl)) et des spécialistes du sujet (PortNox, Impulse Safeconnect…) – ces solutions peuvent être onpremise ou hébergées sur le cloud en mode Saas pour plus de flexibilité, mais nécessitent de l’expertise pour bien fonctionner. C’est pourquoi, iDNA peut vous accompagner dans votre choix de solutions correspondant au mieux à vos besoins.