Comment garantir le retour des équipements sur le réseau en toute sécurité

Dans sa récente intervention, le chef de l'Etat a confirmé que l'intégralité du territoire passait en « zone verte ». Cette nouvelle étape va accélérer la reprise au sortir d'une crise sanitaire qui aura un impact durable sur l'économie française et l'activité mondiale.

Pour les entreprises trop pressées de reprendre leur activité le retour des collaborateurs et de leurs équipements sur le réseau pourrait, sans une préparation suffisante, engendrer une catastrophe en matière de cybersécurité.

Pour l'éviter, les entreprises ne doivent pas confondre vitesse et précipitation, et prendre un certain nombre de dispositions indispensables pour garantir un retour des équipements sur le réseau en toute sécurité.

Recenser les équipements présents sur le réseau

La majorité des entreprises savent quels appareils elles possèdent et ceux qui sont connectés à leurs réseaux. Pourtant, confrontées à l'essor du BYOD et aux mauvaises pratiques de leurs collaborateurs, en particulier durant le confinement, on estime à au moins 30% le taux de dispositifs connectés – smartphones, tablettes, équipements smart desk, etc – qui ne sont pas recensés.

Or tous présentent une même caractéristique : s'ils sont compromis – et la prudence incite à partir du principe qu'ils le sont – ils offrent aux hackers, à l'insu de la direction informatique, une porte dérobée vers le réseau de l'entreprise. Certains seront compromis simplement parce qu'ils ne disposent pas des dernières versions logicielles et de correctifs de sécurité à jour.
Mais au moment même où ils seront réintroduits sur le lieu de travail, ils amplifieront le risque pour l'entreprise.

La première étape consiste, avant même le retour de ses salariés au sein de l'entreprise, à obtenir une visibilité totale sur les appareils présents sur ses réseaux, ce à quoi ils servent et les logiciels qu'ils utilisent.

Des politiques « zero-trust » strictes

A l'image des pays qui ont fermé leurs frontières, ne laissant entrer que des personnes dont ils pouvaient démontrer qu'elles n'avaient pas été exposées au virus, les entreprises doivent établir des exigences minimales de sécurité auxquelles un dispositif doit satisfaire avant d'être autorisé à se connecter au réseau.

La mise en place des politiques « zero-trust », qui ont démontré leur efficacité en terme sanitaire,

peuvent s'appliquer en matière de cybersécurité. Ainsi, tout équipement utilisant un ancien système d'exploitation pour lequel une faille de vulnérabilité est identifiée se verra refuser l'accès au réseau jusqu'à la mise à jour de l'OS ou l'exécution d'un correctif de sécurité.

La segmentation, une clé de voûte de la sécurité

Dans le but de maitriser la propagation d'une maladie contagieuse, les autorités de santé publique ont recours à plusieurs stratégies, parmi lesquelles l'isolement et la quarantaine. Ces deux stratégies sont des pratiques courantes visant à minimiser l'éventualité que les personnes atteintes de maladies infectieuses en contaminent d'autres.

Ces stratégies ne sont pas propres à la virologie et se révèlent particulièrement efficaces en matière de cybersécurité. En cas d'intrusion, la segmentation d'un réseau en différentes parties indépendantes empêche les cybercriminels de s'y déplacer latéralement. Elle permet ainsi à l'entreprise, confrontée à des réseaux de plus en plus grands et complexes à administrer, de contenir la menace et d'éviter qu'elle ne se propage à d'autres zones.

Avant d'être autorisé à rejoindre le réseau, chaque appareil doit être contrôlé. Une fois la segmentation des réseaux mise en œuvre, la direction informatique veillera donc à définir une « zone de décontamination » distincte au sein de laquelle les appareils amenés à se reconnecter seront contrôlés, tout en leur conservant un accès minimum afin de maintenir le bon déroulement des opérations.

Cette approche va de pair avec le dernier pilier d'une approche efficace en matière de cybersécurité post-confinement : le contrôle de l'accès au réseau (NAC).

Surveillance centralisée des accès

Le NAC permet de centraliser la visibilité, la conformité et la segmentation du réseau et garantit que ces éléments individuels soient appliqués de manière cohérente et scrupuleuse sur chaque appareil et sur chaque partie du réseau. Le NAC s'apparente à un centre de commandement de la cyberdéfense grâce auquel les directions informatiques administrent n'importe quel dispositif présent au sein d'un réseau.
Elles surveillent ses activités et interviennent pour révoquer l'accès de tout dispositif au comportement suspect.
Les autorisations d'accès peuvent être gérées et appliquées sur l'ensemble du réseau, ou individuellement pour chaque appareil, et certains de ces processus peuvent même être automatisés. Ces solutions pourraient se révéler indispensables pour mettre en œuvre une protection adéquate face aux cybermenaces imminentes.

La pandémie n'a pas ralenti le rythme des attaques et on anticipe même une hausse des actes malveillants, motivée par l'afflux attendu de dispositifs, nouveaux et existants, sur les réseaux au sortir progressif du confinement. Pour y faire face, les entreprises doivent redoubler de vigilance et agir sans tarder.