IoT et télétravail : s'adapter à la nouvelle normalité pour assurer sa cybersécurité

Selon une Ã©tude de Statista , il y aura 75 ,4 milliards d'objets connectÃ©s dans le monde d'ici 2025. Ils sont en effet arrivÃ©s massivement dans les foyers ces derniÃ¨res annÃ©es, pour faciliter le quotidien de leurs utilisateurs via l'automatisation. Cependant, ces innovations reprÃ©sentent une vÃ©ritable porte d'entrÃ©e vers le rÃ©seau domestique. Avec la gÃ©nÃ©ralisation du tÃ©lÃ©travail, les objets connectÃ©s sont ainsi devenus des cibles privilÃ©giÃ©es des cybercriminels, qui profitent de leur niveau sÃ©curitÃ© gÃ©nÃ©ralement faible pour accÃ©der aux informations sensibles des entreprises.

D'aprÃ¨s une rÃ©cente Ã©tude rÃ©alisÃ©e par HP, 70 % des appareils intelligents sont vulnÃ©rables. Les exemples d'attaques rÃ©ussies exploitant l'IoT ne manquent donc pas : les machines Ã cafÃ©, les thermostats, les tÃ©lÃ©viseurs, ou encore les babyphones, peuvent Ãªtre hackÃ©s pour espionner leurs propriÃ©taires, collecter leurs donnÃ©es ou exiger de l'argent - des cybercriminels ont par le passÃ© menacÃ© d'augmenter le chauffage, et donc la facture Ã©nergÃ©tique, de foyers si une demande de ranÃ§on n'Ã©tait pas payÃ©e. Bien souvent, ces compromissions sont facilitÃ©es par le fait que les utilisateurs ne changent pas les identifiants par dÃ©faut de leurs appareils intelligents.

Mode de travail hybride, la voie royale pour les cybercriminels

En parallÃ¨le de cette adoption massive et des vulnÃ©rabilitÃ©s certaines, nous avons Ã©tÃ© frappÃ©s par pandÃ©mie du Covid-19. Cette crise a conduit le gouvernement franÃ§ais Ã demander aux organisations de favoriser le tÃ©lÃ©travail, voire de l'imposer, au cours de l'annÃ©e. De nombreux employÃ©s se sont donc connectÃ©s aux rÃ©seaux de leur entreprise depuis leurs rÃ©seaux domestiques, peu, voire pas, sÃ©curisÃ©s. Cela reprÃ©sente un danger significatif pour leur employeur en cas de manquement aux principes de base de cybersÃ©curitÃ©. L'utilisation de plus en plus frÃ©quente d'objets connectÃ©s offre en effet davantage de possibilitÃ©s aux cyberattaquants, en mesure de compromettre facilement un appareil du foyer mal sÃ©curisÃ© puis, via le rÃ©seau domestique, et par rebond, de tirer profit de l'appareil professionnel du tÃ©lÃ©travailleur.

En situation de travail Ã distance, les employÃ©s doivent prendre toutes les mesures nÃ©cessaires pour assurer et amÃ©liorer la sÃ©curitÃ© des objets connectÃ©s, en renforÃ§ant notamment leur authentification de connexion. Ils doivent accorder une attention particuliÃ¨re aux identifiants. En effet, il est important de modifier les informations de connexion par dÃ©faut et de choisir un mot de passe fort. En omettant de le faire, les utilisateurs ouvre la voie royale aux pirates informatiques. En plus de la sÃ©curisation de l'IoT, il est important que les tÃ©lÃ©travailleurs sÃ©curisent leur poste de travail, au moyen d'une double authentification, qui consiste Ã prÃ©senter deux preuves d'identitÃ© distinctes pour obtenir l'accÃ¨s. Il est Ã©galement essentiel de redoubler de vigilance sur la protection des ordinateurs professionnels dans le cadre de l'activitÃ© en ligne : de nombreuses violations sont le fruit d'erreurs humaines, les utilisateurs cliquant notamment sur des liens malveillants, ou installant des malwares en pensant qu'ils sont sÃ»rs.

Des outils disponibles, au-delÃ des bonnes pratiques

Au-delÃ des salariÃ©s, les employeurs ont Ã©galement la responsabilitÃ© de mettre en place des procÃ©dures destinÃ©es Ã sÃ©curiser les donnÃ©es qui circulent entre les rÃ©seaux domestiques et professionnels. Une solution simple consiste en un rÃ©seau privÃ© virtuel (VPN), soit un lien chiffrÃ© entre l'ordinateur d'un utilisateur et le serveur de l'entreprise. Un VPN empÃªche toute personne d'accÃ©der Ã des donnÃ©es sensibles pendant leur transit. Il peut Ã©galement offrir un environnement sÃ»r si un tÃ©lÃ©travailleur est amenÃ© Ã utiliser un Wi-Fi public. MÃªme si un pirate crÃ©e un faux spot Wi-Fi pour essayer d'intercepter les donnÃ©es, il ne serait pas en mesure de les traduire.

Par ailleurs, la plupart des routeurs domestiques portent un nom standard qui, s'il n'est pas modifiÃ©, peut indiquer aux pirates informatiques que l'utilisateur n'est pas rigoureux en matiÃ¨re de sÃ©curitÃ©. En modifiant le Service Set Identifier (SSID), et en utilisant un mot de passe long et complexe, les particuliers et les entreprises rÃ©duisent considÃ©rablement les menaces. Il s'agit d'une modification rapide, mais qui pourrait empÃªcher un foyer de se retrouver victime d'une attaque gÃ©nÃ©ralisÃ©e.

La division du rÃ©seau domestique en deux est par ailleurs un moyen efficace de renforcer la sÃ©curitÃ© de son systÃ¨me informatique. Dans cette configuration, les utilisateurs peuvent se servir des appareils qui prÃ©sentent des donnÃ©es sensibles, tels qu'un ordinateur professionnel, sur un rÃ©seau diffÃ©rent de celui qui supportent les objets connectÃ©s pour la maison. En recourant Ã cette mÃ©thode, mÃªme s'il obtient l'accÃ¨s Ã l'un des appareils intelligent du foyer, un cybercriminel ne peut pas accÃ©der directement Ã l'ordinateur professionnel s'il est utilisÃ© via le rÃ©seau qui est isolÃ© et donc protÃ©gÃ©. Le rÃ©seau utilisÃ© pour les objets connectÃ©s qui ne gÃ¨rent pas de donnÃ©es critiques peut aussi Ãªtre utilisÃ© pour les invitÃ©s, protÃ©geant ainsi les appareils sensibles, si leur comportement inappropriÃ© en matiÃ¨re de navigation pose un problÃ¨me de sÃ©curitÃ©.

Ainsi, Ã mesure que les tÃ©lÃ©travailleurs s'habituent Ã la Â« nouvelle normalitÃ© Â», la protection des objets connectÃ©s doit faire partie intÃ©grante de leur vie quotidienne. S'ils sont mal sÃ©curisÃ©s, ils peuvent rapidement devenir des fardeaux aux consÃ©quences dramatiques. Quelle que soit la maniÃ¨re dont une faille entraine une compromission, aucun utilisateur ne souhaite que ses appareils intelligents se retournent contre lui. Quant aux entreprises, leur stratÃ©gie de cybersÃ©curitÃ© est Ã adapter aux nouveaux usages, et il est crucial de mettre en place les outils et procÃ©dures adÃ©quates pour soutenir les tÃ©lÃ©travailleurs. En effet, la vigilance en matiÃ¨re de cybersÃ©curitÃ© est plus que jamais une nÃ©cessitÃ©, tant du cÃ´tÃ© des collaborateurs en tÃ©lÃ©travail que des entreprises.