Les grands piliers dâ□□une cybersÃ©curitÃ© dÃ©diÃ©s aux TPE et PME

SÃ©curitÃ©

PostÃ© par : JulieM
PubliÃ©e le : 9/2/2022 13:00:00

Peu importe leur taille ou leur secteur dâ□□activitÃ©, toutes les entreprises sont concernÃ©es et font face aux mÃªmes besoins : se protÃ©ger des risques cyber, sÃ©curiser lâ□□ensemble du parc informatique et dâ□□objets connectÃ©s et respecter les rÃ©glementations lÃ©gales en vigueur.

Les TPE/PME sont peu ou mal protÃ©gÃ©es face aux cybermenaces et ne disposent pas dâ□□Ã©quipes dÃ©diÃ©es Ã la sÃ©curitÃ©. Elles reprÃ©sentent une cible plus vulnÃ©rable pour les cyberattaquants. En ce sens, elles doivent veiller Ã mettre en place un environnement de confiance permettant Ã leurs Ã©quipes, partenaires et clients de travailler dans les meilleures conditions.

Pour autant, une telle approche nâ□□est pas forcÃ©ment aisÃ©e pour les petites structures. Il convient donc de les accompagner au mieux et de leur proposer des dispositifs adaptÃ©s Ã leurs spÃ©cificitÃ©s. Mais par quoi les TPE/PME doivent-elles commencer ? Quels sont les fondamentaux Ã prendre en considÃ©ration pour une cybersÃ©curitÃ© optimale dans leurs entreprises ?

Accompagner les chefs d'entreprise et les collaborateurs dans une utilisation responsable et sÃ©curisÃ©e d'Internet

Devant les interrogations et inquiÃ©tudes des dirigeants pour lutter contre les risques cyber, il est nÃ©cessaire dâ□□offrir des rÃ©ponses simples et intuitives pour les accompagner dans la sÃ©curisation, lâ□□administration et lâ□□optimisation de lâ□□ensemble du rÃ©seau informatique et des accÃ¨s Internet.

Pour quâ□□une solution soit utilisÃ©e, il ne faut pas dÃ©laisser les interfaces de gestion : interaction et fluiditÃ© sont les maÃ®tres mots. Une visualisation graphique et synthÃ©tique des donnÃ©es est le meilleur alliÃ© pour que tout un chacun se sente Ã lâ□□aise, sans complexe, pour prendre facilement en main lâ□□outil. Afin de sensibiliser tout lâ□□Ã©cosystÃ¨me de la sociÃ©tÃ©, il est important de le guider dans lâ□□adoption de bons rÃ©flexes pour la sÃ©curitÃ© informatique de lâ□□entreprise.

Proposer des outils de cybersÃ©curitÃ© puissants

La plupart des TPE/PME possÃ¨de un antivirus ou un pare-feu. DÃ©sormais ce nâ□□est plus suffisant pour se protÃ©ger et contrer les attaques. Pour Ãªtre efficace, une cyberdÃ©fense doit reposer sur des bases de sÃ©curitÃ© solides, telles que la technologie de pointe et des personnes ressources formÃ©es.

Les dispositifs doivent intÃ©grer tous les outils indispensables Ã une bonne sÃ©curisation du systÃ¨me dâ□□information : dÃ©tection et visualisation en temps rÃ©el de 100 % des Ã©quipements connectÃ©s sur le rÃ©seau de lâ□□entreprise (IoT), analyse et traitement de 100 % des flux entrants et sortants du rÃ©seau de lâ□□entreprise, alerte automatique en temps rÃ©el des actions numÃ©riques Ã risque et enfin protection proactive contre les cybermenaces et le piratage.

Veiller Ã la performance du rÃ©seau de lâ□□entreprise

Analyser et administrer les usages Internet afin d'amÃ©liorer l'efficacitÃ© du rÃ©seau et faciliter la prise de conscience des collaborateurs est fondamental. Pour cela, il faut notamment maÃ®triser les usages dâ□□Internet et de la bande passante, rÃ©guler la navigation en gÃ©rant les accÃ¨s aux sites web, visualiser et optimiser l'utilisation des applications, des sites web en temps rÃ©el et associer les collaborateurs Ã une utilisation responsable dâ□□Internet.

Ne pas nÃ©gliger les aspects lÃ©galitÃ©

Sur ce point, il faut garantir le respect des droits et des devoirs des chefs dâ□□entreprise et des collaborateurs. Cela passe par la mise en place dâ□□une charte informatique personnalisÃ©e et automatisÃ©e, informant et responsabilisant les collaborateurs sur les usages et risques informatiques dans lâ□□entreprise.

Il faut aussi sâ□□assurer de la protection de la responsabilitÃ© pÃ©nale et civile du dirigeant, en dÃ©finissant les conditions dâ□□accÃ¨s et de restriction aux sites web (illicites, dangereux, etc.). Il est Ã©galement indispensable dâ□□Ãªtre garant d'un usage vertueux du systÃ¨me informatique en conservant les logs de connexion des acteurs internes de lâ□□entreprise et de prÃ©server lâ□□Ã©quilibre vie pro/perso des collaborateurs en respectant le temps de navigation privÃ©e.

Enfin, il nâ□□y a rien de mieux que de mettre Ã disposition des collaborateurs une charte personnalisÃ©e de protection des donnÃ©es personnelles, les informant des moyens mis en Å□uvre par lâ□□entreprise pour collecter et protÃ©ger leurs donnÃ©es et garantir ainsi un climat de confiance.

Emmanuel DELOGET, Expert en cybersÃ©curitÃ© chez Ã□ho.Link