Le dÃ©fi des entreprises europÃ©ennes face aux exigences rÃ©glementaires
Internet
PostÃ© par : JerryG
PubliÃ©e le : 24/1/2024 14:00:00

En 2023, la menace cyber a passÃ© un nouveau cap avec des attaques toujours plus sophistiquÃ©es, ciblant tous types dâ□□organisations, de tous horizons. La cybersÃ©curitÃ© est dÃ©jÃ , de fait, une prioritÃ© absolue en 2024, comme le souligne le rÃ©cent rapport du WEF sur le paysage mondial des risques.

Les organisations franÃ§aises sont particuliÃ¨rement mises Ã lâ□□Ã©preuve. A quelques mois des Jeux Olympiques, elles seront en ligne de mire des cybercriminels qui nâ□□hÃ©siteront pas Ã les cibler pour atteindre les citoyens franÃ§ais et touristes Ã©trangers.

Les plus vulnÃ©rables dâ□□entre elles (TPE, hÃ´pitaux ou collectivitÃ©s) sont dÃ©jÃ des cibles privilÃ©giÃ©es des groupes de cyberattaquants qui profitent de failles de sÃ©curitÃ© - principalement liÃ©es Ã lâ□□utilisation de solutions non europÃ©ennes et Ã un manque de prÃ©paration - pour compromettre non seulement ces entitÃ©s, mais aussi les organisations autour desquelles elles gravitent.

Cadre lÃ©gislatif en pleine Ã©volution

Lâ□□objectif est clair : renforcer la rÃ©silience des entreprises europÃ©ennes en matiÃ¨re de cybersÃ©curitÃ© et pour cela, lâ□□Union EuropÃ©enne nâ□□hÃ©site pas Ã multiplier les rÃ¨glementations (NIS, DORA, Cyber Solidarity Act, Cyber Resilience Actâ□¦). Pour TEHTRIS, leader dans la neutralisation automatique en temps rÃ©el et sans action humaine des cyberattaques, cet enjeu est dâ□□abord Ã©troitement liÃ© Ã la souverainetÃ© des donnÃ©es, le RGPD sâ□□inscrivant comme point de dÃ©part contre de possibles violations de donnÃ©es et cyberattaques, notamment pour se protÃ©ger des lois extraterritoriales.

Alain Ter-Markossian, Directeur de lâ□□IngÃ©nierie Â« les failles de sÃ©curitÃ© engendrÃ©es par les solutions de cybersÃ©curitÃ© non-europÃ©ennes sont une rÃ©alitÃ©, encore peu connue, pour de nombreuses entreprises. Face Ã cette menace, il est nÃ©cessaire de durcir le ton. Bien que lointaines, les aspirations de souverainetÃ© europÃ©enne auront un impact consÃ©quent sur les entreprises. Mitiger les risques liÃ©s aux solutions Ã©trangÃ¨res de cybersÃ©curitÃ© notamment lâ□□espionnage industriel, est un rÃ©el enjeu. Â»

Lâ□□entrÃ©e en vigueur de la directive NIS2, prÃ©vue pour octobre 2024, obligera ainsi les entreprises Ã passer un niveau supÃ©rieur en matiÃ¨re de cybersÃ©curitÃ©. Plus sÃ©vÃ¨re que sa prÃ©dÃ©cesseur, NIS1, elle sâ□□appliquera Ã un plus large Ã©ventail de secteurs et dâ□□entreprises et imposera des exigences de sÃ©curitÃ© plus Ã©levÃ©es. Un nouveau travail mÃ©ticuleux de mise en conformitÃ© auxquels elles devront se soumettre.

Le chemin vers la conformitÃ©

TEHTRIS rappelle Ã juste titre quâ□□il existe dÃ©jÃ des solutions pour ne pas se laisser dÃ©border par les normes europÃ©ennes. Si lâ□□arrivÃ©e de NIS2 imposera Ã©galement aux fournisseurs de repenser leurs offres pour sâ□□adresser autant aux grandes entreprises du CAC40 que les PME, la plupart des outils europÃ©ens conduisent dÃ©jÃ vers la conformitÃ© Ã ISO/IEC 27001 et au RGDP, voire Ã NIS2 pour les plus avancÃ©es.

Â« La transposition de NIS2 en France et lâ□□ensemble des mesures qui y sont adjointes feront grandement avancer la souverainetÃ© europÃ©enne. Les fournisseurs de solutions de cybersÃ©curitÃ© europÃ©ennes nâ□□auront de choix que de sâ□□adresser Ã lâ□□ensemble des entreprises concernÃ©es et tant que les donnÃ©es sont hÃ©bergÃ©es hors US, les entreprises seront mieux protÃ©gÃ©es. Â» prÃ©cise Alain Ter-Markossian.

Choisir des solutions de cybersÃ©curitÃ© soumises Ã des lÃ©gislations extÃ©rieures, revient de nos jours Ã faire courir un risque direct aux entreprises. La souverainetÃ© europÃ©enne, quâ□□elle soit en termes de cybersÃ©curitÃ© ou de donnÃ©es, prend donc toute son importance et protÃ¨ge leur avenir. Lâ□□accompagnement sera clÃ© pour atteindre la cyber-rÃ©silience Ã lâ□□instar de la charte cyber, rÃ©cemment publiÃ©e par cybermalveillance.gouv.fr. Elle a dÃ©jÃ Ã©tÃ© signÃ©e par plus de 80 entreprises et collectivitÃ©s et est en phase dâ□□adoption massive par les PME.Â