PrÃ©sidentielles 2022 : CESIN, 10 propositions pour la cybersÃ©curitÃ©
Internet
PostÃ© par : JulieM
PubliÃ©e le : 21/2/2022 15:00:00

Depuis les derniÃ¨res Ã©lections prÃ©sidentielles, la transformation numÃ©rique de la sociÃ©tÃ©, des entreprises et des administrations sâ□□est considÃ©rablement accÃ©lÃ©rÃ©e nous rendant, tant Ã titre professionnel que personnel, grands consommateurs mais aussi totalement dÃ©pendants du numÃ©rique.

La conquÃªte du monde par les gÃ©ants du numÃ©rique sâ□□est largement confirmÃ©e, ne laissant que trÃ¨s peu de place aux solutions souveraines. Notre pays sâ□□est ainsi retrouvÃ© en position de colonie numÃ©rique de grandes puissances Ã©trangÃ¨res.

Des dÃ©pendances prÃ©occupantes sur le plan sanitaire avaient Ã©tÃ© mises en exergue au dÃ©but de la crise COVID, et le sujet de la dÃ©pendance avait enfin Ã©mergÃ© sur la scÃ¨ne politique. Nos dÃ©pendances au numÃ©rique sont Ã©galement trÃ¨s fortes et trÃ¨s Ã©tendues dans nos sociÃ©tÃ©s. Lâ□□Ã©volution du numÃ©rique vers le cloud a encore accentuÃ© cette dÃ©pendance et confÃ¨re aux risques cyber une nature systÃ©mique.

La surface dâ□□attaque sâ□□Ã©tant considÃ©rablement Ã©largie, les cyberattaques se sont multipliÃ©es avec des impacts de plus en plus forts sur des entreprises de toutes tailles et de tous secteurs dâ□□activitÃ©, rendant notre environnement numÃ©rique fragile et incertain. La cybersÃ©curitÃ© sâ□□est invitÃ©e dans les ComitÃ©s exÃ©cutifs.

Les responsables cybersÃ©curitÃ© rÃ©unis au sein du CESIN ont travaillÃ© ces derniÃ¨res annÃ©es pour sÃ©curiser les systÃ¨mes dâ□□Information et le patrimoine informationnel de leur entreprise, ainsi que pour assurer la cyber rÃ©silience des activitÃ©s.

Dans le mÃªme temps, de nombreuses initiatives en matiÃ¨re de cybersÃ©curitÃ© ont vu le jour tant en France quâ□□au niveau europÃ©en, mais il reste encore beaucoup de chemin Ã parcourir pour que le numÃ©rique soit synonyme dâ□□indÃ©pendance et de sÃ©curitÃ© afin quâ□□il apporte toute sa valeur Ã notre sociÃ©tÃ©.

Câ□□est pourquoi le CESIN Ã©met 10 propositions en matiÃ¨re de cybersÃ©curitÃ© pour la future mandature. Lâ□□ordre de prÃ©sentation de ces propositions ne constitue pas Ã une priorisation. A noter que ces propositions ne traitent pas de ce qui relÃ¨ve des cyberattaques contre les Ã□tats.

Dans sa vocation Ã rÃ©unir les Responsables cybersÃ©curitÃ© de moyennes et grandes entreprises, le CESIN se concentre sur ce qui concerne les entreprises ainsi que sur lâ□□Ã©ducation des jeunes, pour prÃ©parer le futur de la cybersÃ©curitÃ©.

Proposition nÂ°1 â□□ CrÃ©er un MinistÃ¨re du NumÃ©rique : le numÃ©rique en France reprÃ©sente 6% du PIB, 150Md de dÃ©penses et environ 1 million dâ□□emplois salariÃ©s (1) Au-delÃ des chiffres, câ□□est une place tellement stratÃ©gique dans notre sociÃ©tÃ© quâ□□elle mÃ©rite absolument quâ□□un ministÃ¨re de plein droit soit crÃ©Ã©, qui sâ□□appuierait sur un secrÃ©tariat dâ□□Ã□tat dÃ©diÃ© Ã la cybersÃ©curitÃ©.

Proposition nÂ° 2 â□□ Promouvoir un vÃ©ritable numÃ©rique de confiance europÃ©en : il sâ□□agit dâ□□aider au dÃ©veloppement dâ□□offres europÃ©ennes, en favorisant des solutions et services de grande diffusion, accessibles au plus grand nombre, plutÃ´t que pour des usages

nâ□□impliquant que des donnÃ©es sensibles qui restent des sujets de niche.

Lâ□□indÃ©pendance ne se gagne que si le pÃ©rimÃ¨tre couvert est large et vise des usages quotidiens et massifs. Cela vaut tant pour les offres digitales au sens large que pour les solutions de cybersÃ©curitÃ©. Lâ□□objectif est double : nous rendre moins dÃ©pendants de solutions Ã©trangÃ¨res et assurer dâ□□une maniÃ¨re gÃ©nÃ©rale une protection de nos donnÃ©es vis-Ã -vis de lois extraterritoriales souvent Ã©quivalentes Ã des permis dâ□□espionner. Car les gÃ©ants du numÃ©riques sâ□□enrichissent avec des souscriptions et des licences, et captent intensivement nos donnÃ©es qui nourrissent leurs industries.

Proposition nÂ°3 â□□ Favoriser lâ□□innovation : de nombreuses initiatives sont prises pour financer lâ□□innovation. Le tissu de startups dans le monde numÃ©rique, et particuliÃ¨rement en cybersÃ©curitÃ©, est Ã©loquent. Cependant rien nâ□□est fait ou presque pour que ces solutions Ã©mergent vraiment et gagnent par rapport Ã la concurrence Ã©trangÃ¨re.

Dans le numÃ©rique tout le monde a sa chance de devenir le gÃ©ant de demain avec de lâ□□audace et du soutien. Il faut inventer les mÃ©canismes qui poussent des initiatives sur des terrains stratÃ©giques, et qui favorisent les solutions innovantes franÃ§aises et europÃ©ennes pour les donneurs dâ□□ordre. Il faut aussi penser lâ□□aprÃ¨s startup pour que les licornes franÃ§aises ne soient pas quasi automatiquement rachetÃ©es par des entreprises Ã©trangÃ¨res.

Proposition nÂ°4 â□□ En finir avec cet afflux de logiciels vulnÃ©rables : la gÃ©nÃ©ralisation du numÃ©rique a mÃ©caniquement augmentÃ© le nombre de logiciels que nous utilisons au quotidien.

Or nos entreprises font face Ã un nombre exponentiel de vulnÃ©rabilitÃ©s Ã traiter, soit parce que les Ã©diteurs ont produit vite et mal, des applications comportant des failles logicielles, et ces cas sont en nette augmentation ces derniÃ¨res annÃ©es, soit parce quâ□□un attaquant a rÃ©ussi Ã sâ□□introduire chez un Ã©diteur et Ã insÃ©rer un code malveillant au sein des logiciels produits.

Cette escalade nâ□□est plus supportable car câ□□est aux clients de ces Ã©diteurs de faire ensuite les efforts pour compenser ce niveau de sÃ©curitÃ© dÃ©plorable. Les clients doivent installer des correctifs pour supprimer ces failles de sÃ©curitÃ©, ce qui reprÃ©sente un coÃ»t Ã©levÃ© de maintien en condition de sÃ©curitÃ©. Ils doivent de surcroit compenser les dÃ©fauts de ces briques logicielles par des mesures additionnelles coÃ»teuses.

Et comme si cela ne suffisait pas, ils doivent aussi assumer les consÃ©quences, si ces vulnÃ©rabilitÃ©s sont exploitÃ©es par des acteurs malveillants pour mener des cyberattaques. Il faut obliger les Ã©diteurs Ã prendre des engagements formels sur la sÃ©curitÃ© intÃ©grÃ©e dans les logiciels quâ□□ils produisent.

Cela passe par des labels, des organismes de certification tiers adaptÃ©s aux nouvelles chaÃ®nes de dÃ©veloppement, et par des lois qui introduisent un niveau de responsabilitÃ© de lâ□□Ã©diteur, comme câ□□est le cas pour des produits matÃ©riels.

Proposition nÂ°5 - CrÃ©er un guichet unique en cybersÃ©curitÃ© pour simplifier les parcours : au fil des ans et des problÃ©matiques Ã traiter, diffÃ©rentes autoritÃ©s et points dâ□□entrÃ©e en matiÃ¨re de cybersÃ©curitÃ© se sont dÃ©veloppÃ©s. De nombreuses initiatives ont Ã©tÃ© menÃ©es Ã lâ□□Ã©chelle nationale ou rÃ©gionale pour aider les entreprises et les particuliers.

Toutes partent dâ□□une bonne intention, mais cette offre est devenue complexe Ã utiliser. Le dirigeant dâ□□entreprise ne sait pas Ã qui sâ□□adresser pour comprendre le sujet cyber, pour se former, pour vÃ©rifier un label ou une certification ou pour se faire aider et dÃ©poser une plainte lorsquâ□□il est confrontÃ© Ã une cyberattaque.

Et ce nâ□□est pas plus simple pour les particuliers. La crÃ©ation dâ□□un guichet unique national de la cybersÃ©curitÃ© devrait permettre dâ□□amÃ©liorer la lisibilitÃ© des dispositifs cyber et dâ□□y recourir facilement et avec une meilleure efficacitÃ©. Par exemple, il est tout Ã fait inappropriÃ©, voire incongru, dâ□□aller physiquement dans un commissariat de quartier pour dÃ©poser une plainte cyber alors que lâ□□entreprise est dans la tourmente dâ□□une cyberattaque.

Proposition nÂ°6 â□□ Des Responsables CybersÃ©curitÃ© obligatoires dans les entreprises et les administrations : la sÃ©curitÃ© est lâ□□affaire de tous dit lâ□□adage, mais lorsque le sujet est incarnÃ© par une personne chargÃ©e particuliÃ¨rement de ce dossier, le changement est radical.

Câ□□est pourquoi Ã lâ□□instar de ce qui sâ□□est fait avec le RGPD et la crÃ©ation de postes de DPO obligatoires dans les entreprises, il faut rendre le Responsable CybersÃ©curitÃ© obligatoire dans toutes les entreprises. La protection du numÃ©rique est devenue trop stratÃ©gique pour que sujet soit traitÃ© de faÃ§on optionnelle. Des postes de Responsables CybersÃ©curitÃ© Ã temps partagÃ© peuvent Ãªtre envisagÃ©s pour les petites et moyennes structures.

Proposition nÂ° 7 â□□ Une formation cyber obligatoire pour les dirigeants : Tous les dirigeants dâ□□entreprises devraient suivre une courte formation obligatoire annuelle nationale sur les risques cyber (enjeux, prioritÃ©s, principes de gouvernance, connaissance des actions essentielles et de la rÃ©glementation).

Ce dispositif commencerait dÃ¨s lâ□□enregistrement de lâ□□entreprise. Cette formation rÃ©currente pourrait conditionner toute forme de subvention aux entreprises dans le domaine des technologies de lâ□□information et des communications.

Proposition nÂ°8 â□□ Un diagnostic flash cybersÃ©curitÃ© obligatoire : Les entreprises devraient Ãªtre tenues de faire rÃ©aliser annuellement un diagnostic flash (par exemple dâ□□une durÃ©e dâ□□une journÃ©e) sur quelques points de contrÃ´le des mesures de sÃ©curitÃ© essentielles en analogie avec le contrÃ´le technique dâ□□un vÃ©hicule ou la vÃ©rification dâ□□une installation contre lâ□□incendie.

Personne ne doute quâ□□un ensemble de dispositifs de dÃ©tection contre lâ□□incendie soit nÃ©cessaire pour protÃ©ger les personnes et les biens matÃ©riels. Mais il nâ□□y a pas encore la mÃªme perception sur lâ□□immatÃ©riel. Une cyberattaque peut avoir de gros impacts opÃ©rationnels, financiers et/ou rÃ©putationnels, et aller jusquâ□□Ã paralyser une entreprise gravement et mÃªme dÃ©finitivement.

Combien dâ□□entreprises connaissent les mÃ©canismes coupe-feu, de dÃ©tection ou dâ□□extinction dans le domaine du numÃ©rique ? A lâ□□issue de ces diagnostics, les entreprises devraient avoir lâ□□obligation de traiter les points critiques identifiÃ©s sous un certain dÃ©lai, comme câ□□est le cas quand des dÃ©fauts importants sont trouvÃ©s sur des installations ou sur des vÃ©hicules, car ces dÃ©fauts peuvent mettre en danger la vie de lâ□□entreprise.

Proposition nÂ°9 â□□ Nos jeunes passent la moitiÃ© de leur temps dans le monde numÃ©rique et ne sont pas Ã©duquÃ©s au numÃ©rique et Ã la sÃ©curitÃ© : il faut absolument intÃ©grer une Ã©ducation complÃ¨te Ã la vie numÃ©rique dans les collÃ¨ges et les lycÃ©es, pour former les jeunes Ã une approche critique et responsable des outils numÃ©riques et dâ□□Internet.

Par ailleurs, la pÃ©nurie de ressources en matiÃ¨re de cybersÃ©curitÃ© nâ□□est plus Ã dÃ©montrer. Le flÃ©chage vers des formations supÃ©rieures de Â« cyber-spÃ©cialistes Â» est faible voire inexistant et la reprÃ©sentation actuelle des mÃ©tiers de la cybersÃ©curitÃ© comporte encore des clichÃ©s qui nâ□□incitent pas les lycÃ©ennes en particulier Ã rejoindre cette filiÃ¨re. Il faut continuer de dÃ©velopper lâ□□offre de formations supÃ©rieures, la faire connaÃ®tre et la promouvoir pour encourager les jeunes Ã sâ□□orienter vers cette filiÃ¨re.

Proposition nÂ°10 - Traiter le cas des rÃ©seaux sociaux : lâ□□extrÃªme pÃ©nÃ©tration des rÃ©seaux sociaux dans nos vies personnelles mais aussi professionnelles nâ□□est plus Ã dÃ©montrer.

Dâ□□un point de vue cybersÃ©curitÃ©, cela veut dire au quotidien des vols de donnÃ©es, des usurpations dâ□□identitÃ©, la propagation de fakes news sans compter dâ□□autres dÃ©rives qui peuvent, in fine, atteindre Ã la sÃ©curitÃ© des personnes, des entreprises et des Etats.

Ces rÃ©seaux sociaux vÃ©hiculent des incitations Ã la violence, des atteintes au bien-Ãªtre des personnes, des menaces, intimidations et autres agressions. Et nous savons que les intelligences artificielles que ces plateformes utilisent, sâ□□appuient sur des algorithmes qui amplifient ces phÃ©nomÃ¨nes.

On ne peut pas juste faire le constat dâ□□une zone de non droit, de lieux de lâ□□ultra violence et de lâ□□atteinte constante Ã la vÃ©ritÃ©. Dâ□□une part il faut pouvoir donner un statut Ã ces plateformes pour quâ□□elles portent une responsabilitÃ© sur les contenus postÃ©s. Et ce doit Ãªtre possible car des plateformes ont dÃ©jÃ bloquÃ© les comptes de personnalitÃ©s publiques.

Si elles lâ□□ont fait pour au moins une personne, câ□□est quâ□□elles sâ□□octroient la capacitÃ© de rÃ©guler les contenus, donc allons jusquâ□□au bout du raisonnement et assignons un devoir de rÃ©gulation. AprÃ¨s tout, dans le monde physique, si vous ouvrez largement votre appartement et que vos invitÃ©s font un tapage nocturne, vous Ãªtes responsableâ□¦

Et de mÃªme que lâ□□on notifie, sur des contenus audiovisuels, la prÃ©sence de contenus pouvant choquer et que lâ□□on affiche un Ã¢ge minimum recommandÃ© sur certains films, pourrait-on imposer Ã ces rÃ©seaux de tagger les contenus inappropriÃ©s et de ne pas avoir le droit de servir plus de N% de contenus entrant dans ces catÃ©gories. Cela freinerait les ardeurs des algorithmes amplificateurs.

Plus d'information.