CybersÃ©curitÃ© : les six tendances majeures en 2022
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 5/1/2022 13:00:00

Cette nouvelle annÃ©e devrait voir un renforcement des lÃ©gislations et des normes de sÃ©curitÃ©, mais aussi une inquiÃ©tante montÃ©e en puissance des ransomwares et des risques technologiques.

Netwrix, fournisseur de cybersÃ©curitÃ© qui simplifie la sÃ©curitÃ© des donnÃ©es, dÃ©voile les tendances clÃ©s en matiÃ¨re de cybersÃ©curitÃ© qui devraient concerner directement les entreprises en 2022.

Avec lâ augmentation rÃ©guliÃ¨re des cyberattaques, et notamment la pratique dÃ©sormais trÃ¨s rÃ©pandue du ransomware, les Ã©quipes IT et les professionnels de la sÃ©curitÃ© informatique doivent plus que jamais rester sur leur garde. Pierre-Louis Lussan, Directeur South-West Europe et Country Manager France de Netwrix, fournit ici six pistes de rÃ©flexion pour aider les entreprises dans leur gestion des donnÃ©es, face aux nouvelles menaces pour la sÃ©curitÃ© des donnÃ©es :

1. La lÃ©gislation devrait se renforcer compte tenu des incidents de sÃ©curitÃ© qui affectent les entreprises privÃ©es et impactent Ã©galement la sÃ©curitÃ© au niveau national.

Lâimpact des ransomwares et autres types de cyberattaques ne concerne plus uniquement lâentreprise qui en est la premiÃ¨re victime : les attaques touchent dÃ©sormais des rÃ©gions entiÃ¨res.

A titre dâexemple, les attaques rÃ©cemment menÃ©es dans certaines rÃ©gions contre des entreprises de distribution alimentaire ou de carburant ont eu pour consÃ©quence des manques dâapprovisionnement dans les rayons des supermarchÃ©s et des files dâattente grandissantes dans les stations service. Il faut donc sâattendre Ã ce que les exigences de sÃ©curitÃ© des entreprises privÃ©es, dans les secteurs les plus sensibles, deviennent plus sÃ©vÃ¨res.

En particulier, les rÃ¨gles de notification seront concernÃ©es, dans la mesure oÃ¹ les services gouvernementaux requiÃ¨rent une plus grande visibilitÃ© sur le caractÃ¨re spÃ©cifique des cyberattaques, afin dâamÃ©liorer et de renforcer les lÃ©gislations en vigueur. Dans certains cas, les gouvernements pourraient opter pour la stratÃ©gie de la carotte et du bÃ¢ton, avec par exemple des exonÃ©rations fiscales attribuÃ©es aux entreprises ayant investi dans des systÃ¨mes de cyberdÃ©fense plus sophistiquÃ©s.

2. Le coÃ»t des assurances couvrant les incidents de cybersÃ©curitÃ© devrait augmenter et les nouvelles polices imposeront des normes de sÃ©curitÃ© plus drastiques.

Les indemnisations devenant Ã la fois plus frÃ©quentes et plus coÃ»teuses, le montant des primes dâassurance liÃ©es Ã la cybersÃ©curitÃ© a dÃ©jÃ connu une envolÃ©e notable. Selon une Ã©tude, l'index des prix des contrats d'assurance cyber-risque a augmentÃ© de 32% au niveau global entre juin 2020 et juin 2021.

Il faut donc sâattendre Ã des hausses continues en 2022. Les polices dâassurance devraient

Ã©galement exiger la mise en Å□uvre de contrÃ´les critiques permettant de rÃ©duire les risques dâ□□incidents liÃ©s Ã la cybercriminalitÃ©. Les attaques devenant plus frÃ©quentes, les compagnies dâ□□assurance nâ□□en viendront Ã verser des indemnisations que dans des cas exceptionnels.

3. Les attaques cibleront de plus en plus les fournisseurs de services dâ□□infogÃ©rance afin dâ□□infiltrer les grandes entreprises ou les services gouvernementaux.

Les attaquants ont mis en Å□uvre une stratÃ©gie trÃ¨s efficace pour accÃ©der aux grandes entreprises â□□ via les infrastructures IT plus vulnÃ©rables des PME qui offrent leurs services. En consÃ©quence, les fournisseurs de services dâ□□infogÃ©rance devront Ã©largir et renforcer leurs mesures de sÃ©curitÃ©, dâ□□autant que de nombreuses PME comptent sur eux pour assurer leur sÃ©curitÃ©.

4. Lâ□□informatique quantique devrait commencer Ã perturber les capacitÃ©s de chiffrement.

La plupart des concepteurs dâ□□algorithmes sâ□□appuient aujourdâ□□hui sur lâ□□idÃ©e selon laquelle il nâ□□existe aucun processeur suffisamment puissant pour les Â« craquer Â» dans un temps raisonnable. Mais lâ□□informatique quantique va inaugurer une Ã¨re nouvelle, avec lâ□□arrivÃ©e de processeurs capables de ce type de performance.

Bien que cette technologie soit encore Ã©loignÃ©e de telles applications pratiques, lâ□□inquiÃ©tude commence toutefois Ã poindre. Les Etats-Unis, par exemple, ont annoncÃ© des contrÃ´les Ã lâ□□export sur huit sociÃ©tÃ©s chinoises dâ□□informatique quantique, sur la base de fortes suspicions quant Ã la capacitÃ© de la Chine Ã forcer le chiffrement. Avec la venue Ã maturitÃ© de cette technologie, il faut sâ□□attendre Ã lâ□□adoption massive de standards de chiffrement post-quantiques.

5. Les entreprises devront relever les dÃ©fis du machine learning.

Plus de la moitiÃ© (59 %) des grandes entreprises utilisent dÃ©jÃ la data science et le machine learning. Offrant de nombreux avantages, ces technologies sont Ã©galement porteuses de risques.

Les algorithmes de machine learning sont particuliÃ¨rement vulnÃ©rables pendant la phase dâ□□apprentissage, dans la mesure oÃ¹ des cybercriminels peuvent manipuler les donnÃ©es en entrÃ©e afin de modifier les rÃ©sultats.

Cela peut alors provoquer la rupture de processus critiques, voire mettre des vies en danger lorsque ces malversations touchent le secteur de la santÃ©, ou quand elles perturbent volontairement le fonctionnement des feux de signalisation des villes intelligentes, par exemple. Les entreprises qui utilisent le machine learning doivent comprendre et Ã©valuer ces menaces Ã leur juste mesure, et redoubler dâ□□efforts pour sâ□□en prÃ©munir.

6. Les attaquants utiliseront les rÃ©seaux domestiques comme infrastructures.

Il est beaucoup plus simple dâ□□infecter un rÃ©seau domestique avec un logiciel malveillant que de sâ□□introduire dans un environnement IT professionnel sÃ©curisÃ©. Avec lâ□□augmentation de la puissance de traitement et de la largeur de bande dÃ©diÃ©e Ã la connectivitÃ© dans les rÃ©sidences privÃ©es, les rÃ©seaux domestiques vont devenir beaucoup plus attractifs pour les personnes mal intentionnÃ©es.

Par exemple, en infectant de nombreux dispositifs, elles seront en mesure de modifier les adresses IP, voire les noms de domaines de maniÃ¨re dynamique pendant des campagnes dâ□□attaques par

logiciels malveillants, en contournant les dÃ©fenses communes comme le blocage sÃ©lectif des adresses IP et le filtrage DNS.

Les Ã©quipes informatiques doivent garder Ã lâ□□esprit ce nouveau vecteur de menace lorsquâ□□elles revisiteront leurs stratÃ©gies de sÃ©curitÃ© et leurs plans de rÃ©ponse aux incidents. Qui plus est, lâ□□industrie informatique doit chercher Ã mieux sensibiliser les utilisateurs et favoriser les bonnes pratiques pour rÃ©duire le nombre de victimes â□□ souvent des proies faciles pour des personnes aux intentions malveillantes.

Â« La priorisation est la seule faÃ§on pour les entreprises de gÃ©rer les risques de cyberattaques dans cette nouvelle Ã¨re de technologies avancÃ©es, explique Pierre-Louis Lussan, Directeur South-West Europe et Country Manager France de Netwrix.

Autrement dit, les entreprises doivent veiller Ã protÃ©ger leurs actifs les plus importants et les plus prÃ©cieux des incidents les plus probables en actualisant rÃ©guliÃ¨rement leurs rÃ¨gles de sÃ©curitÃ©. Il est de plus en plus Ã©vident que les polices dâ□□assurance contre les cyberattaques ne seront plus une bouÃ©e de sauvetage dans un avenir proche. Lâ□□Ã©valuation des risques est de notre propre responsabilitÃ©. Â»