La sécurité et la gestion des données n'est plus une option mais une nécessité

Dans une Ã©conomie numÃ©rique basÃ©e sur la demande et lâ€™instantanÃ©itÃ©, la donnÃ©e est le nouveau point de convergence de la valeur des entreprises. Plus que jamais au cÅ“ur du business - tous secteurs confondus, son potentiel est incommensurable. Elle est une vraie mine dâ€™or pour les entreprises qui souhaitent suivre le rythme des marchÃ©s en mutation constante. Mais, au travers de cyberattaques de plus en plus ciblÃ©es utilisant notamment des ransomwares, les hackers veulent leur part du gÃ¢teau.

Le ransomware, logiciel d'extorsion, sâ€™est particuliÃ¨rement dÃ©veloppÃ© au cours des derniÃ¨res annÃ©es car il reprÃ©sente une activitÃ© extrÃªmement lucrative pour les cybercriminels. GrÃ¢ce Ã ce type dâ€™attaque, les hackers restreignent lâ€™accÃ¨s au systÃ¨me dâ€™informations dâ€™une entreprise en cryptant ses donnÃ©es. Un ordinateur infectÃ©, via un ver informatique inclus dans un fichier tÃ©lÃ©chargÃ© ou reÃ§u par email, permet de corrompre tous les fichiers auquel il est reliÃ©. Lâ€™entreprise ne peut donc plus y accÃ©der sauf si elle dÃ©cide de sâ€™acquitter dâ€™une ranÃ§on. Mais le coÃ»t moyen global gÃ©nÃ©rÃ© pour lâ€™entreprise par ce type dâ€™attaque est beaucoup plus important quâ€™on pourrait le penser.

Si la simple ranÃ§on peut parfois atteindre plusieurs millions dâ€™euros, les coÃ»ts dÃ©coulant dâ€™une cessation dâ€™activitÃ© (moyenne de 16 jours avant de retrouver son rÃ©seau), de la dÃ©sinfection et du remplacement de certains Ã©quipements voire, sur le long terme du manque Ã gagner suite Ã lâ€™effet mÃªme de lâ€™attaque sur lâ€™image de lâ€™entreprise, sont aussi Ã prendre en compte. Dâ€™aprÃ¨s le FBI, les coÃ»ts totaux liÃ©s aux attaques par ransomwares devraient atteindre les 6 milliards de dollars dâ€™ici 2021 soit lâ€™Ã©quivalent du PIB de la troisiÃ¨me puissance mondiale.

Ces derniers mois, une longue liste dâ€™organisations franÃ§aises a Ã©tÃ© infectÃ©e par des ransomwares. AprÃ¨s la rÃ©gion du Grand Est, Bouygues Construction, le CHU de Rouen et le CNED, lâ€™AFPA est la derniÃ¨re victime en date. La rÃ©ussite de ces attaques sâ€™explique notamment par lâ€™amÃ©lioration et lâ€™optimisation des mÃ©thodes employÃ©es par les hackers. Ils sont ainsi plus sÃ©lectifs, dÃ©laissant les attaques de masse pour se focaliser sur des cibles quâ€™ils considÃ¨rent comme plus Â« juteuses Â» pouvant dÃ©couler Ã un meilleur rendement. Dâ€™ailleurs, en France, les attaques dâ€™envergure sont majoritairement orientÃ©es vers les institutions de santÃ©, les grands groupes, et les collectivitÃ©s territoriales car ils sont perÃ§us comme plus vulnÃ©rables ou encore davantage enclins Ã payer la ranÃ§on au vu de lâ€™importance des donnÃ©es pour leur activitÃ©s respectives.

Comment protÃ©ger les donnÃ©es dans un monde numÃ©rique qui dÃ©pend plus que jamais de leur disponibilitÃ© ?

MÃªme si les ransomwares sont de plus en plus connus des entreprises, celles-ci ne savent pas toujours comment sâ€™en prÃ©munir. Pour leur permettre de Â« cocher la case Â» sÃ©curitÃ© et de se rassurer, celles-ci ont tendance Ã mettre en place une solution informatique dÃ©diÃ©e, gÃ©nÃ©ralement proposÃ©e par des fournisseurs spÃ©cialisÃ©s, pensant Ã tort que cela sera suffisant. Effectivement, mÃªme si cela constitue une premiÃ¨re barriÃ¨re contre les ransomwares, des failles de sÃ©curitÃ© subsisteront, notamment liÃ©es Ã lâ€™action humaine.

Il est donc indispensable dâ€™aller plus loin. Le National Institute of Standards and Technology, rÃ©fÃ©rence en la matiÃ¨re, a Ã©tabli 5 points de mÃ©thodologie afin dâ€™aider les entreprises Ã Ã©tablir une sÃ©curitÃ© optimale et Ã faire face aux attaques par ransomware :

Identifier les donnÃ©es et avoir une rÃ©elle visibilitÃ© : il est nÃ©cessaire pour les entreprises de comprendre les services mÃ©tier critiques, leur architecture (sur site, cloud, ou encore multi cloud) et leurs relations. De plus, gagner en visibilitÃ© sur les lieux de stockage des donnÃ©es, leur type, leur accÃ¨s et leur durÃ©e de stockage est indispensable pour dÃ©tecter celles qui sont les plus susceptibles de faire lâ€™objet dâ€™une future attaque.

Se protÃ©ger des risques liÃ©s aux attaques par ransomware : les entreprises nâ€™ayant pas de stratÃ©gie de sauvegarde solide nâ€™ont dâ€™autre choix que de payer les ranÃ§ons pour rÃ©cupÃ©rer leurs donnÃ©es. La sÃ©curisation et la mise Ã disposition rapide des donnÃ©es critiques basÃ©es sur une plateforme adaptÃ©e et hautement Ã©volutive de sauvegarde sont des Ã©tapes indispensables pour assurer la rÃ©cupÃ©ration rapide des donnÃ©es.
De plus, un systÃ¨me visant Ã assurer la continuitÃ© des opÃ©rations critiques grÃ¢ce Ã des processus automatisÃ©s de recovery ou de basculement permettront aux entreprises de limiter, voire dâ€™Ã©viter, la cessation complÃ¨te dâ€™activitÃ© dans le cadre dâ€™une attaque. Cela permettra Ã©galement aux entreprises dâ€™effectuer des tests de ces mÃªmes dispositifs pour mettre Ã lâ€™Ã©preuve leur Ã rÃ©agir en cas dâ€™attaque.

Savoir dÃ©tecter les attaques et rÃ©agir : les solutions de sÃ©curitÃ© mises en place au sein des entreprises sont gÃ©nÃ©ralement en charge de la dÃ©tection des attaques. ComplÃ©ter ces solutions par une Ã©troite surveillance des signaux faibles (volumÃ©trie, extension, etc.) aidera lâ€™entreprise Ã rÃ©agir rapidement si besoin. On remarque en effet que lorsquâ€™un ransomware vient dâ€™intÃ©grer le rÃ©seau de lâ€™entreprise, la quantitÃ© de donnÃ©es augmente lÃ©gÃ¨rement - cela est dÃ» Ã la place prise par le chiffrage. En identifiant les signaux faibles rapidement, lâ€™entreprise peut prendre des contre-mesures, qui peuvent notamment prendre la forme dâ€™un verrouillage des accÃ¨s, dâ€™un basculement automatique des services critiques et dâ€™une stratÃ©gie rodÃ©e de reprise aprÃ¨s sinistre.

RÃ©cupÃ©rer les donnÃ©es qui auraient pu Ãªtre compromises : la rÃ©plication des sauvegardes de donnÃ©es et leur conservation dans un environnement hors ligne effectuÃ©es en amont permettent de garantir une restauration de donnÃ©es saines au sein du systÃ¨me dÃ¨s lors que les donnÃ©es altÃ©rÃ©es ont Ã©tÃ© identifiÃ©es et qualifiÃ©es. Pouvoir identifier les donnÃ©es touchÃ©es est dâ€™une importance capitale, aussi bien pour le recouvrement que pour de possibles futures audits.

Lâ€™ensemble de ces processus techniques permettent de minimiser les risques dâ€™attaques et de rÃ©cupÃ©rer les donnÃ©es de lâ€™entreprise en cas de dÃ©faillance. Mais le facteur humain reste en effet trÃ¨s important et lâ€™erreur dâ€™une seule personne peut malheureusement suffire Ã compromettre tout un systÃ¨me. Câ€™est pour cette raison quâ€™il reste essentiel pour toute entitÃ© dâ€™assurer la formation des employÃ©s concernant les menaces et de les familiariser avec les bonnes pratiques.

Centralisation et gestion de la donnÃ©e, essentiels Ã la pÃ©rennitÃ© du systÃ¨me

La gestion de la donnÃ©e est dÃ©sormais plus complexe et demande une plus grande flexibilitÃ© : de par des architectures rÃ©seaux hybrides ou multi-cloud complexes, la prÃ©sence de sources de donnÃ©es croissantes et lâ€™utilisation dâ€™un nombre important dâ€™applications, les entreprises doivent sâ€™assurer de pouvoir gÃ©rer un environnement hÃ©tÃ©rogÃ¨ne de plus en plus dense.

De plus, le passage obligÃ© au tÃ©lÃ©travail ces derniÃ¨res semaines - allant de pair avec un partage des donnÃ©es exacerbÃ© et lâ€™utilisation accrue des services cloud, bouleverse les entreprises et modifie leur faÃ§on de fonctionner notamment vis-Ã -vis des donnÃ©es. La mise Ã disposition, dans lâ€™urgence, de solutions ou dâ€™outils ponctuels pour rÃ©pondre aux besoins de tÃ©lÃ©travailler ne permet malheureusement pas aux entreprises dâ€™avoir une vue globale et transversale sur les diffÃ©rents silos existants. Ce manque de visibilitÃ© crÃ©e des Â« angles morts Â» et câ€™est prÃ©cisÃ©ment ce type de faille quâ€™utilisent les hackers.

Une visibilitÃ© amoindrie induit Ã©galement un temps de rÃ©action gÃ©nÃ©ralement plus long face aux attaques, puisque le temps de dÃ©tection et dâ€™identification de la menace est souvent proportionnel aux nombres de silos de donnÃ©es que lâ€™entreprise peut avoir. Pour y remÃ©dier, une plateforme visant Ã centraliser la gestion de donnÃ©es est idÃ©ale pour amÃ©liorer la visibilitÃ© sur ces derniÃ¨res et sur leur lieu de stockage. IndÃ©pendante du matÃ©riel et conÃ§ue pour fonctionner dans des contextes hybrides dÃ©sormais communs, celle-ci doit prendre en charge de nombreuses technologies visant Ã protÃ©ger les infrastructures, dÃ©tecter les attaques ou encore Ã mettre en place des procÃ©dures de recovery. En favorisant la gestion et surtout la classification, ces plateformes apportent une meilleure vue dâ€™ensemble sur les donnÃ©es et leur valeur, aidant ainsi Ã Ã©valuer les risques.

GrÃ¢ce Ã la prÃ©vention des risques et Ã une politique de gestion de donnÃ©es efficace, les entreprises seront Ã mÃªme de limiter les consÃ©quences directes et indirectes des attaques par ransomware, que ce soit en matiÃ¨re de coÃ»ts ou encore de rÃ©putation.