La santÃ© face aux cybercriminels : le profit financier ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 22/2/2021 13:00:00

Une semaine aprÃ¨s l'hÃ´pital de Dax-CÃ´te d'Argent, l'hÃ´pital de Villefranche-sur-SaÃ´ne, dans le RhÃ´ne, est Ã son tour victime d'une attaque informatique Â« Ã grande Ã©chelle Â». Le ransomware identifiÃ©, RYUK, Â« impacte fortement Â» les sites de Villefranche-sur-SaÃ´ne, Tarare et TrÃ©voux de l'HÃ´pital du Nord-Ouest.

Les rÃ©seaux tÃ©lÃ©phoniques et Internet ont Ã©tÃ© coupÃ©s, mais l'Ã©tablissement a signalÃ© qu'aucun transfert de patients n'est prÃ©vu pour le moment.

Pierre-Louis Lussan, Country Manager France et South-West Director chez Netwrix, explique pourquoi le secteur de la santÃ© est plus que jamais au cÂ□ur des cyberattaques et comment il peut se protÃ©ger :

Â« Les organisations du secteur de la santÃ© collectent et stockent de grandes quantitÃ©s d'informations personnelles et de santÃ© qui ont une valeur marchande Ã©levÃ©e sur le Darknet. Les hÃ´pitaux, les centres mÃ©dicaux et les autres Ã©tablissements de soins sont alors une cible attrayante pour les cybercriminels.

Il est difficile de garantir une protection complÃ¨te contre les ransomware, mais les organisations peuvent encore faire beaucoup pour minimiser les dÃ©gÃ¢ts. Il est faux de penser aujourdâ□□hui que les ranÃ§ons ne visent que les grandes entreprises bien connues.

La mise en place de contrÃ´les de cybersÃ©curitÃ© fondamentaux, tels que des alertes sur la copie de fichiers en masse et sur l'Ã©lÃ©vation des privilÃ¨ges, la segmentation du rÃ©seau ou encore l'authentification Ã deux facteurs, est primordial si ce nâ□□est pas dÃ©jÃ fait.Â

Cela permet en effet de mieux voir ce qui se passe avec les donnÃ©es sensibles, et de dÃ©clencher rapidement des alertes en cas d'accÃ¨s illÃ©gitime aux donnÃ©es, plutÃ´t que de permettre aux criminels de se cacher dans les rÃ©seaux pendant des semaines voire plus.

Le fait qu'il s'agisse d'une nouvelle attaque ciblÃ©e sur un Ã©tablissement de santÃ© est le signe que le ransomware est non seulement un moyen de rÃ©cupÃ©rer de lâ□□argent mais aussi d'influencer les dÃ©cisions prises par les institutions et le gouvernement au niveau national. Ã□ l'avenir, la prochaine gÃ©nÃ©ration de ransomware sera conÃ§ue pour causer des dommages plus difficiles Ã rÃ©parer afin de forcer les organisations Ã agir.

Nous devons anticiper l'expansion des attaques portÃ©es par les cybercriminels vers de nouvelles cibles, telles que les technologies opÃ©rationnelles et les dispositifs IoT, qui sont susceptibles dâ□□avoir un impact beaucoup plus visible sur le monde physique.

Les organisations du secteur de la santÃ© sont de plus en plus souvent la cible de cyberattaques pour des raisons qui ne se limitent pas au profit financier.Â

Â Elles doivent constamment Ã©valuer les risques et se mettre Ã l'abri des pirates informatiques, en se demandant quels sont les dispositifs de valeur qu'elles possÃ¨dent, si leur infrastructure peut Ãªtre exploitÃ©e pour atteindre une cible plus prÃ©cieuse et ce qu'elles peuvent faire pour

minimiser l'impact d'une brÃ¨che, par exemple.

Telles sont les questions que tout Ã©tablissement doit se poser pour protÃ©ger ses donnÃ©es et celles de ses patients ainsi que son activitÃ© de toute tentative de compromission ; d'autant plus dans la santÃ©, au regard de la situation actuelle de pandÃ©mie qui met le secteur sous pression, avec des enjeux majeurs relatifs Ã la vie et aux soins des patients. Â»

Pierre-Louis Lussan, Country Manager France et South-West Director chez Netwrix