Les données de votre entreprise sont exposées sur le Dark Web ! Que faire ?

Nous entendons parler depuis des annÃ©es du Dark Web. Ce Web cachÃ© gÃ©nÃ¨re en effet beaucoup de fantasmes, dâ€™interrogations voire de craintes. Le Dark Web est un ensemble de sites web anonymes dont les adresses IP sont cachÃ©es afin de rendre impossible l'identification de l'hÃ´te par les utilisateurs. Il est donc totalement accessible au public mÃªme sâ€™il nâ€™est pas indexÃ© par les moteurs de recherche traditionnels ; il requiert simplement lâ€™utilisation dâ€™un navigateur particulier - TOR Ã©tant certainement le plus connu - pour y accÃ©der.

Se rendre sur le Dark Web nâ€™a donc rien dâ€™illÃ©gal, ce qui nâ€™est pas le cas en revanche de ce dont on y fait commerce. Et dÃ©sormais, Ã cÃ´tÃ© de produits illÃ©gaux en tout genre, le Dark Web est devenu un haut lieu de commerce illicite dâ€™informations sensibles, rendues disponibles Ã la suite de fuites de donnÃ©es. Explications :

Selon le rapport 2019 sur l'Ã©tat mondial de la cybersÃ©curitÃ© dans les petites et moyennes entreprises publiÃ© par lâ€™Institut Ponemon(1), 63 % des PME ont signalÃ© un incident impliquant la perte d'informations sensibles concernant leurs clients et leurs employÃ©s au cours de lâ€™annÃ©e 2019.

Ces donnÃ©es sensibles se retrouvent ensuite trÃ¨s rapidement en vente sur le Dark Web, Ã des prix allant de quelques euros Ã plusieurs centaines dâ€™euros.

Câ€™est aujourdâ€™hui un commerce des plus rentables car les acheteurs sont nombreux. Ce commerce reprÃ©sente en fait trÃ¨s simplement la premiÃ¨re Ã©tape de la cybercriminalitÃ© dâ€™aujourdâ€™hui. Avec ces donnÃ©es sensibles (gÃ©nÃ©ralement dans le cas des entreprises, il sâ€™agit de donnÃ©es dâ€™identification - A titre dâ€™exemple, dâ€™aprÃ¨s une Ã©tude rÃ©cente dâ€™Accenture(2), des accÃ¨s prÃ©Ã©tablis Ã des rÃ©seaux dâ€™entreprises se monnayent entre 300 et 10 000 dollars sur le Dark Web), des groupes cybercriminels vont pouvoir mener des actions malveillantes plus poussÃ©es, en pÃ©nÃ©trant les rÃ©seaux dâ€™entreprise pour diffuser des attaques sophistiquÃ©es en vue de dÃ©truire des systÃ¨mes, de voler de lâ€™argent (directement ou en menant des attaques par ransomware) ou mÃªme de lâ€™information ; on parle alors de vol de propriÃ©tÃ© intellectuelle.

Alors que faire lorsquâ€™on se rend compte que les donnÃ©es d'identification de son entreprise ont Ã©tÃ© exposÃ©es sur le Dark Web ?

Tout dâ€™abord, si lâ€™on sait que le domaine de son entreprise a Ã©tÃ© compromis lors d'une fuite de donnÃ©es publique, un rapport sur le Dark Web peut aider Ã dÃ©terminer si des informations sensibles telles que des comptes de messagerie et des mots de passe sont dÃ©sormais vulnÃ©rables et potentiellement en vente sur cette partie du Web. Et si tel est bien le cas, il faut absolument mettre en place plusieurs mesures de sÃ©curitÃ© incontournables telles que :

Â· RÃ©initialiser les mots de passe dans toute l'entreprise aprÃ¨s avoir alertÃ© le service informatique

Â· ProcÃ©der Ã un audit de sÃ©curitÃ© pour identifier dâ€™Ã©ventuelles vulnÃ©rabilitÃ©s supplÃ©mentaires qui pourraient avoir Ã©tÃ© causÃ©es par la fuite de donnÃ©es

Â· Activer lâ€™authentification multifacteur (MFA) : si lâ€™authentification multifacteur nâ€™a pas encore Ã©tÃ© mise en Å“uvre, c'est le moment. On ne sait jamais quand les employÃ©s seront victimes dâ€™une nouvelle faille. Le MFA constitue selon les professionnels une vÃ©ritable solution capable dâ€™empÃªcher que des comptes utilisateurs ne soient compromis, par exemple sur des applications mÃ©tiers hÃ©bergÃ©es dans le Cloud, mais Ã©galement capable de sÃ©curiser les accÃ¨s au VPN qui a par ailleurs Ã©tÃ© fortement sollicitÃ© cette annÃ©e.

Â· Promouvoir la sensibilisation interne : si on a la preuve que les donnÃ©es d'identification dâ€™employÃ©s ont Ã©tÃ© exposÃ©es sur le Web, il est important de mener des actions de sensibilisation afin de rappeler auxdits employÃ©s lâ€™ensemble des pratiques de sÃ©curitÃ© Ã adopter pour accÃ©der aux plateformes et aux informations de l'entreprise. Plus important encore, il est nÃ©cessaire de rappeler Ã chacun de garder ses mots de passe professionnels et personnels distincts.

Â· Ne pas se contenter de faire une seule recherche sur le Dark Web : les fuites de donnÃ©es se produisent tout le temps. Il est recommandÃ© d'effectuer des recherches frÃ©quentes et cohÃ©rentes sur le Dark Web afin de pouvoir agir rapidement si le domaine de lâ€™entreprise vient Ã Ãªtre exposÃ©.

La relation entre cybersÃ©curitÃ© et PME a mis du temps Ã Ãªtre Ã©tablie mais les PME semblent dÃ©sormais mieux informÃ©es et mieux prÃ©parÃ©es Ã faire face Ã la cybercriminalitÃ©. Il faut toutefois reconnaÃ®tre que le thÃ¨me de la cybersÃ©curitÃ© est complexe : chronophage, il reprÃ©sente aussi un coÃ»t, et doit engager toute lâ€™entreprise, des dirigeants aux employÃ©s.

Malheureusement se sÃ©curiser est devenu un impÃ©ratif incontournable car les attaques se multiplient (malwares, ransomwares, fraude bancaire, vol, modification ou destruction dâ€™informations etc.) et elles touchent tout le monde. Mais cela peut aussi devenir un atout. Lâ€™image dâ€™une entreprise repose en effet dÃ©sormais en grande partie sur sa sÃ©curitÃ© et sa capacitÃ© Ã dÃ©montrer quâ€™elle veille Ã la sÃ©curitÃ© des donnÃ©es de ses clients, de ses partenaires et de ses employÃ©s. Dâ€™oÃ¹ lâ€™importance de maÃ®triser ces donnÃ©es et dâ€™Ã©viter Ã tout prix quâ€™elles ne se retrouventâ€¦ sur le Dark Web.

(1) https://www.keeper.io/hubfs/PDF/2019%20Keeper%20Report%20V7.pdf

(2)
https://www.accenture.com/us-en/blogs/cyber-defense/destructive-relationship-between-network-access-sellers-and-ransomware-groups