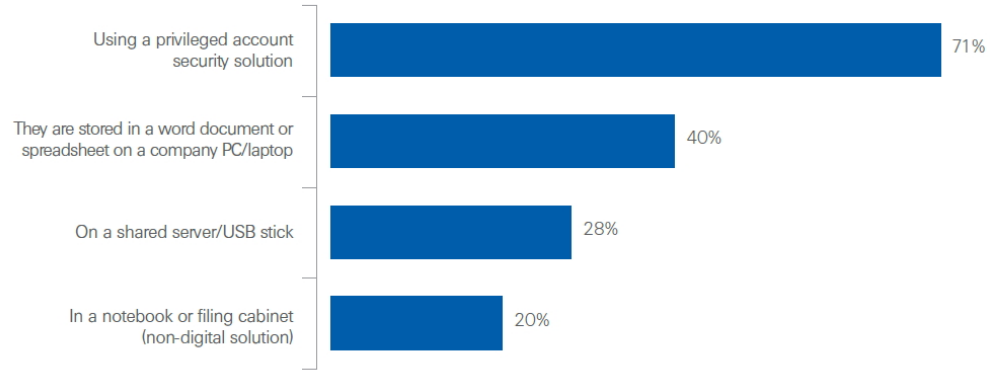
Les sysadmins continuent à stocker les identifiants sur Word ou Excel

L'idée selon laquelle la plus grosse faille de sécurité se trouve entre la chaise et l'ordinateur se vérifie une nouvelle fois. Quatre responsables en sécurité sur dix avouent stocker les identifiants de connexion dans un fichier Word ou Excel enregistré dans le PC de bureau ou, pire, un ordinateur portable. Et si 28% utilisent un serveur de partage ou une clé USB, 20% privilégient encore le carnet de notes. *« Il est clair que l'adoption des meilleures pratiques est encore loin »*, commente CyberArk qui, dans le cadre de son étude *Global Advanced Threat Landscape Survey 2016*, a interrogé 750 administrateurs systèmes. Même si 71 % des sondés déclarent utiliser une solution privilégiée pour sécuriser leurs comptes administrateurs.

Un tiers des entreprises en cours d'attaque

Stocker des login/mot de passe dans un document texte n'est pas dangereux en soi. C'est la façon dont on peut accéder au contenu de ce fichier qui l'est. Autrement dit, si le fichier (ou l'ensemble du disque dur) n'est pas protégé par du chiffrement, il constitue une manne pour les malwares de type RAT (remote administration tool) qui, une fois installés sur la machine victime, s'empressent de parcourir le disque dur à la recherche de documents susceptibles de contenir des identifiants de connexion.

Fig. 5: **How does your organization store and manage its privileged and/or administrative passwords?**



Ce qui est d'autant plus inquiétant que 36% des interrogés pensent que le réseau de leur entreprise est actuellement attaqué ou l'a été au cours des 12 dernier mois (8 % ne le savent pas). Et 46 % déclarent avoir été victime d'un ransomware ces deux dernières années. Néanmoins, les organisations gagneraient en confiance. Leurs responsables sécurité sont 75 % à penser être en mesure de contrer les tentatives d'intrusions dans le réseau. Une belle progression en regard des 44 % relevés en 2015.

Attaques DDoS en tête

Leur attention va d'ailleurs se tourner vers les risques d'attaques DDoS (pour 19□% des répondants), le phishing (14□%), les ransomwares (13□%). Les attaques par exploitation de comptes à privilège n'arrivant qu'en quatrième position avec 12□% des réponses. Et la perte des données clients arrive en tête des principales préoccupations en cas d'attaque réussie (pour 68□% des sondés), loin devant le vol d'informations financières (52□%), la perte de confiance des consommateurs (35□%) ou la réputation de la société (33□%). Les pertes d'argent n'arrivent qu'en huitième position des préoccupations (à 20□%) derrière l'incapacité à fonctionner (32□%), la récupération d'e-mails internes (24□%) et d'adresses IP corporate (24□% aussi).

A noter que 35□% des entreprises prévoient de mettre en place de nouvelles mesures de gestions des comptes administrateurs. Ce qui reste peu en regard des 79□% qui déclarent avoir pris conscience des dangers à l'occasion d'attaques largement médiatisées et pris des mesures en conséquence. 17□% avouent en revanche ne pas y être sensibilisé.

Lire également
iOS 10 : les sauvegardes sont à la portée des hackers
Un nouveau malware téléchargé toutes les 4 secondes
Cyberattaques : des entreprises trop confiantes face au risque