Les cybercriminels se faisant passer pour des utilisateurs légitimes représentent le risque de sécurité le plus élevé | Le Net Expert Informatique

	Les cybercriminels se faisant passer pour des utilisateurs légitimes représentent le risque de sécurité le plus élevé

Les cyber-attaques consistant à pirater les comptes à privilèges et administratifs, c'est-à-dire les identifiants utilisés pour contrôler et utiliser l'infrastructure IT d'une organisation, constituent la principale menace de sécurité dans les entreprises, selon une récente étude conduite par CyberArk.

61% des personnes interrogées ont retenu l'usurpation de comptes à privilèges comme étant le type de cyber-attaque le plus difficile à contrer, contre 44% du même avis l'année dernière. En outre, 48% pensent que les violations de données résultent des mauvaises habitudes des employés en matière de sécurité, tandis que 29% attribuent ceci à la sophistication des attaques. Ces conclusions proviennent de la 9e enquête annuelle réalisée par CyberArk sur le panorama mondial des cyber-menaces avancées Threat Landscape Survey, pour lequel l'entreprise a interrogé 673 cadres dirigeants et responsables de la sécurité IT.

CyberArk a analysé les divergences potentielles entre les cyber-menaces préjudiciables et la confiance qu'une organisation accorde à son système de sécurité. Bien que le lien entre la prise de contrôle de comptes à privilèges comme étant le premier vecteur d'attaque et les récentes, et très médiatisées, violations de données soit mieux établit, les entreprises persistent à se concentrer sur une défense « périmétrique ». Plus de la moitié des interrogés étant convaincus qu'ils pourraient détecter une attaque en quelques jours, CyberArk a indiqué que de nombreux responsables IT et chefs d'entreprises ne disposent pas de la visibilité suffisante sur leurs programmes de sécurité IT. Les défenses périmétriques et les attaques d'hameçonnage (phishing) ne sont que la partie visible de l'iceberg, et les organisations doivent aujourd'hui veiller à se protéger face à des attaques beaucoup plus dévastatrices qui, comme le « Golden Ticket » Kerberos et les attaques « Pass-the-Hash », s'opèrent au cœur-même du réseau.

Les principales conclusions du sondage 2015 incluent : Au-delà de la simple violation – Les pirates cherchent à prendre le contrôle total du réseau

Comme nous avons pu le constater lors des attaques qui ont visé Sony Pictures, le Bureau américain de gestion du personnel et bien d'autres encore, les pirates ayant pris possession des comptes à privilèges peuvent ensuite s'en servir pour prendre de force le contrôle d'une infrastructure réseau ou voler d'importants volumes de données confidentielles. Ces comptes à privilèges permettent en effet aux cybercriminels d'avoir le même niveau de contrôle que les administrateurs IT de haut rang, et ce sur n'importe quel réseau. Grâce à leur capacité de se faire passer pour des utilisateurs légitimes, ces pirates peuvent alors continuer à acquérir des privilèges et à parcourir l'ensemble du réseau afin d'y exfiltrer des données précieuses.

A quelle phase une attaque est-elle la plus difficile à contrer selon les interrogés :

- 61% ont cité la violation des comptes à privilèges, contre 44% en 2014
- 21% mentionnent l'installation du logiciel malveillant
- 12% évoquent la phase de reconnaissance menée par le cybercriminel

Les vecteurs d'attaque représentant les risques de sécurité les plus élevés selon les interrogés sont :

- 38% indiquent la violation de comptes à privilèges ou administratifs
- 27% mentionnent les attaques d'hameçonnage
- 23% citent les logiciels malveillants sur le réseau

Trop de confiance accordée aux stratégies de sécurité dans les entreprises

Le sondage de CyberArk illustre que les interrogés ont entière confiance dans les stratégies de sécurité de leur PDG et de leurs directeurs, mais que les tactiques employées par les organisations sont en contradiction avec les meilleures pratiques en matière de sécurité. Même si les études spécialisées révèlent qu'il faut habituellement une moyenne de 200 jours pour qu'une organisation puisse déceler un pirate sur leurs réseaux, la plupart des interrogés pensent qu'ils sont capables de détecter un pirate endéans quelques jours ou quelques heures. Les interrogés persistent également à croire qu'ils sont parfaitement à même d'empêcher les cybercriminels de pénétrer dans le réseau, malgré de nombreuses preuves indiquant le contraire.

- 55% pensent qu'ils seront capables de détecter une violation en l'espace de quelques jours ; 25% estiment pouvoir détecter une infraction en quelques heures
- 44% continuent de croire qu'ils peuvent parfaitement empêcher les cybercriminels de pénétrer dans un réseau spécifique
- 48% pensent que ce sont les mauvaises habitudes des employés qui sont à la base des violations de données, tandis que 29% mentionnent tout simplement la sophistication des attaques
- 57% des personnes interrogées ont confiance dans les stratégies établies par leur PDG ou leur Conseil d'administration

Les organisations ne semblent toujours pas reconnaître les dangers liés aux attaques de l'intérieur

Les cybercriminels ne cessent de développer de nouvelles tactiques afin de cibler, dérober et exploiter des comptes à privilèges qui leur permettront d'obtenir l'accès aux données les plus sensibles et les plus précieuses d'une organisation. Alors que bon nombre d'entre elles se concentrent sur la défense périmétrique afin de lutter contre des attaques telles que le phishing ou l'usurpation d'identité, ce sont les attaques lancées depuis l'intérieur des organisations qui sont les plus potentiellement dévastatrices. Il a été demandé aux interrogés d'établir un classement des types d'attaques qu'ils redoutent le plus :

- Piratage de mots de passe (72%)
- Attaques d'hameçonnage (70%)
- Piratage de clés SSH (41%)
- Attaques Pass-the-Hash (36%)
- Attaques de Golden Ticket (23%)
- Attaques Overpass-the-Hash (18%)
- Attaques de Silver Ticket (12%)

Les attaques Overpass-the-Hash, Golden Ticket et Silver Ticket sont toutes des attaques Kerberos, permettant d'obtenir un contrôle total d'un réseau spécifique par le piratage du contrôleur de domaine. L'une des attaques les plus dangereuses est celle du Golden Ticket, car elle peut paralyser une organisation entièrement et briser ainsi la confiance accordée à l'infrastructure IT.

« Il est inacceptable qu'une organisation continue de penser que ses programmes de sécurité sont en mesure d'empêcher les cybercriminels de pénétrer dans leur réseau. En outre, le fait de se retrancher derrière la sophistication des attaques et les mauvaises habitudes des utilisateurs ne fait qu'aggraver le problème, déclare John Worrall, Directeur du marketing chez CyberArk. Les attaques les plus dévastatrices sont celles où les pirates volent des identifiants à privilèges et administratifs afin d'obtenir les mêmes droits d'accès que les administrateurs systèmes en interne. Une organisation se retrouve ainsi à la merci du cybercriminel, que ses motivations soient financières, liées à des activités d'espionnage ou visent à causer la fermeture de l'entreprise. Alors que le sondage souligne que les organisations sont de plus en plus conscientes des effets dévastateurs des violations de comptes à privilèges, celles-ci consacrent encore trop d'efforts à vouloir stopper les attaques périmétriques telles que le hameçonnage. »

Source : http://www.globalsecuritymag.fr/Etude-les-cybercriminels-se,20150930,56282.html