***CyberArk : DonnÃ©es personnelles de 20 millions de CorÃ©ens vendues.***
**Internet**
PostÃ© par : JulieM
PubliÃ©e le : 22/1/2014 11:00:00

Les donnÃ©es personnelles de 20 millions de CorÃ©ens du Sud vendues par un employÃ© malveillant â dixit CyberArk.

Le service de surveillance financier CorÃ©en (Korean Financial Supervisory Service - FSS), a annoncÃ© lâaccusation dâun consultant intÃ©rimaire du bureau Sud-CorÃ©en dâanalyse des crÃ©dits Korea Credit Bureau (KCB), pour la vente supposÃ©e dâinformations personnelles de prÃ¨s de 20 millions de clients Sud-CorÃ©ens Ã  des agences marketing.

Lâindividu aurait extrait les donnÃ©es sensibles de ces clients incluant noms, numÃ©ros de sÃ©curitÃ© sociale et informations bancaires des serveurs du bureau.

**Olivier MÃ©lis**, Country Manager France chez CyberArk, a fait les commentaires suivants :

Â« *Une violation de donnÃ©es de telle ampleur, sur prÃ¨s de 20 millions de personnes, est vraiment alarmante. Les consÃ©quences rÃ©sultant dâabus dâutilisateurs Ã  privilÃ¨ges internes ont Ã©tÃ© dÃ©montrÃ©es maintes fois et plus rÃ©cemment avec la cÃ©lÃ¨bre fuite au sein de la NSA par lâex-employÃ© de la CIA, Edward Snowden.*

*Les entreprises accordent des comptes Ã  privilÃ¨ges et codes dâaccÃ¨s puissants Ã  leurs employÃ©s et consultants externes, mais sans la mise en place dâun systÃ¨me pour contrÃ´ler et surveiller efficacement ces comptes, elles restent vulnÃ©rables aux consÃ©quences potentiellement catastrophiques dâabus ou de mauvaises utilisations de ces privilÃ¨ges internes.*

*Dans le cas de la CorÃ©e du Sud, le fait quâun salariÃ© ait eu la possibilitÃ© dâaccÃ©der et de vendre une importante quantitÃ© de donnÃ©es clients est trÃ¨s inquiÃ©tant. Un employÃ© â et dans ce cas, un consultant intÃ©rimaire â nâaurait jamais dÃ» avoir accÃ¨s, ni pouvoir tÃ©lÃ©charger des donnÃ©es sensibles sans attirer lâattention sur cette activitÃ© suspecte.*

*Il est essentiel que des entreprises mettent en place un systÃ¨me capable de gÃ©rer, surveiller et contrÃ´ler tous les accÃ¨s Ã  privilÃ¨ges et les activitÃ©s qui y sont associÃ©es, avec la possibilitÃ© dâ□□interrompre une session malveillante si nÃ©cessaire.*

*Alors que ce cas semble Ãªtre lâ□□exemple classique dâ□□une Â« attaque interne Â» - ce qui correspond Ã  lâ□□utilisation abusive dâ□□un accÃ¨s privilÃ©giÃ© â□□ la menace venant de lâ□□intÃ©rieur peut Ã©galement impliquer une mauvaise utilisation accidentelle de comptes Ã privilÃ¨ges ou le dÃ©tournement de ces comptes par des hackers.*

*Ceux-ci cherchent lâ□□accÃ¨s Ã  ces identifiants dÃ¨s quâ□□ils ont intÃ©grÃ© une entreprise afin de voler les informations et propager des malwares dans les systÃ¨mes.*

*Le dÃ©tournement de donnÃ©es clients peut entraÃ®ner des consÃ©quences dÃ©sastreuses pour une entreprise : perte de confiance des clients, pertes financiÃ¨res mais Ã©galement sanctions financiÃ¨res sÃ©vÃ¨res si la preuve dâ□□une nÃ©gligence dans la protection de ces informations est apportÃ©e. De tels incidents devraient servir de rappel continu aux entreprises sur le danger de la suffisance en ce qui concerne la prÃ©sence permanente de menaces internes.* Â»

Â