PrÃ©sidentielles 2022 : la cybersÃ©curitÃ© au cÅ□ur de la campagne
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 15/12/2021 15:00:00

En mai 2022, les FranÃ§ais se rendront aux urnes pour Ã©lire leur PrÃ©sident. Un moment essentiel de la RÃ©publique franÃ§aise, mais aussi une pÃ©riode propice aux incidents de cybersÃ©curitÃ©.Â

Lors de la derniÃ¨re Ã©lection prÃ©sidentielle en 2017, la campagne avait Ã©tÃ© marquÃ©e par les Â« Macron Leaks Â» : deux jours avant le scrutin du second tour, 20 000 courriers Ã©lectroniques liÃ©s Ã la campagne dâ□□Emmanuel Macron, candidat de lâ□□Ã©poque et actuel prÃ©sident de la RÃ©publique, avaient Ã©tÃ© rÃ©vÃ©lÃ©s au grand public.Â

Une attaque qui nâ□□avait rien de surprenant mais qui ne doit pas se reproduire 5 ans aprÃ¨s. Pourtant, ces temps politiques forts sont propices aux cybermenaces susceptibles de vulnÃ©rabiliser une nation via des attaques gÃ©opolitiques, qui prennent aujourdâ□□hui la forme dâ□□incidents de cybersÃ©curitÃ© et peuvent donner lâ□□avantage Ã des candidats de lâ□□opposition ou des nations concurrentes, grÃ¢ce Ã la propagation de dÃ©sinformations et de fausses informations.

Pour JÃ©rÃ´me Colleu, IngÃ©nieur Avant-vente chez CyberArk, la cybersÃ©curitÃ© doit Ãªtre un axe majeur de la campagne pour que les campagnes des candidats ne soient pas victimes de cyberattaques, de vols de donnÃ©es ou mÃªme dâ□□ingÃ©rence Ã©trangÃ¨re. Pour ce faire, une stratÃ©gie globale et complÃ¨te de gestion des accÃ¨s Ã privilÃ¨ges et de protection des identitÃ©s est essentielle.

Â« Durant les Assises de la SÃ©curitÃ© en Octobre dernier, lâ□□Agence Nationale de SÃ©curitÃ© des SystÃ¨mes Informatiques (ANSSI), par la voix de son directeur Guillaume Poupard, a rappelÃ© lâ□□importance de la cybersÃ©curitÃ© dans le paysage politique actuel. Lâ□□appel Ã©tait dâ□□autant plus important que des faits similaires se sont dÃ©roulÃ©s lors des prÃ©cÃ©dentes Ã©chÃ©ances, en France, ou encore aux Etats-Unis, comme dans dâ□□autres pays du monde.Â

Comme en 2017, les attaques centrÃ©es sur l'identitÃ© seront trÃ¨s probablement utilisÃ©es contre les militants Ã©lectoraux, quel que soit leur statut et leur importance dans le parti quâ□□ils dÃ©fendent. Chaque membre du personnel, chaque bÃ©nÃ©vole et chaque sous-traitant connectÃ© Ã la campagne a en effet le potentiel de devenir un initiÃ© privilÃ©giÃ© en fonction des donnÃ©es ou des applications auxquelles il a accÃ¨s.

Les cybercriminels le savent et chercheront Ã exploiter ce statut - en ciblant ces individus avec des attaques d'ingÃ©nierie sociale, oÃ¹ le hacker se sert de connaissances personnelles sur les victimes afin de les duper, pour voler leur accÃ¨s Ã privilÃ¨ges. Selon le rapport Verizon Data Breach Investigations, ces campagnes malveillantes augmentent d'annÃ©e en annÃ©e, et plus de 80 % des violations de donnÃ©es liÃ©es au piratage impliquent le vol et l'utilisation d'identifiants dÃ©robÃ©s.Â

Avec un niveau Ã©levÃ© dâ□□informations rendues disponibles par lâ□□accÃ¨s exploitÃ©, les cybercriminels peuvent exfiltrer du matÃ©riel et des informations confidentielles, utiliser leur statut pour diffuser de la dÃ©sinformation sur les rÃ©seaux sociaux et par email, ou mÃªme verrouiller les opÃ©rations de campagne via des attaques ciblÃ©es de malware et de ransomware.

Alors que les pirates informatiques chercheront certainement Ã infiltrer les proches de chaque parti, la menace est bien plus vaste. Les gouvernements Ã©tatiques et locaux chargÃ©s dâ□□organiser et de protÃ©ger les Ã©lections seront Ã©galement des cibles attrayantes, de mÃªme que les organisations et les Ã©lecteurs. Une supply chain politique et sociÃ©tale est alors en place.Â

Il suffit en effet d'un seul compte compromis pour qu'un attaquant puisse potentiellement corrompre l'ensemble de l'infrastructure d'une organisation. Câ□□est pour cette raison que Meta, nouveau nom du groupe Facebook, a annoncÃ© sa volontÃ© dâ□□obliger lâ□□authentification Ã double facteur pour se connecter au compte dâ□□un candidat Ã une Ã©lection.

De plus, si lâ□□Ã©lection se dÃ©roule de faÃ§on traditionnelle, avec un bulletin et une urne, de plus en plus de personnes sont aujourdâ□□hui prÃªtes Ã une digitalisation plus poussÃ©e de lâ□□acte citoyen. Le gouvernement, par la voix du ministre de lâ□□IntÃ©rieur, GÃ©rald Darmanin, a dâ□□ailleurs dÃ©clarÃ© travailler vers le vote Ã distance. En outre, la part de personnes non-inscrits ou mal-inscrits sur les listes Ã©lectorales inquiÃ¨tent les hommes politiques.Â

Selon une Ã©tude de CÃ©line Braconnier, 17 % de la population franÃ§aise et 51 % des jeunes de 25 Ã 29 ans sont mal-inscrits. Certains parlementaires, mÃªme sâ□□ils annoncent que la mise en place du vote par correspondance serait compliquÃ©e, Å□uvrent pour une digitalisation plus grande de lâ□□inscription, afin dâ□□Ã©viter des pertes de citoyens dans le processus. Si cette hypothÃ¨se se confirme, cette part numÃ©rique du vote devra Ãªtre hautement surveillÃ©e pour ne pas intÃ©grer de fausses identitÃ©s ou faire parvenir des bulletins frauduleux.

Si les identitÃ©s des candidats ou des votants, dans le cadre dâ□□une potentielle Ã©lection Ã distance, ne sont pas protÃ©gÃ©es, les consÃ©quences politiques pourraient Ãªtre importante avec le rÃ©sultat dâ□□une Ã©lection qui ne reflÃ¨terait pas lâ□□opinion gÃ©nÃ©rale. En effet, cela pourrait Ãªtre trÃ¨s problÃ©matique si la vision des Ã©lecteurs Ã©tait altÃ©rÃ©e par la propagation de fausses informations Ã cause de failles de cybersÃ©curitÃ©.

La sÃ©curisation des Ã©lections prÃ©sidentielles de 2022 et les suivantes nÃ©cessite une approche globale qui prend en compte la sÃ©curitÃ© des identitÃ©s avec une base solide dans la gestion des accÃ¨s Ã privilÃ¨ges. Cette approche permettra de renforcer les dÃ©fenses contre un paysage des menaces en pleine expansion, de se protÃ©ger contre l'Ã©volution des vulnÃ©rabilitÃ©s et de minimiser la capacitÃ© des hackers Ã exploiter les personnes associÃ©es aux campagnes. Â»