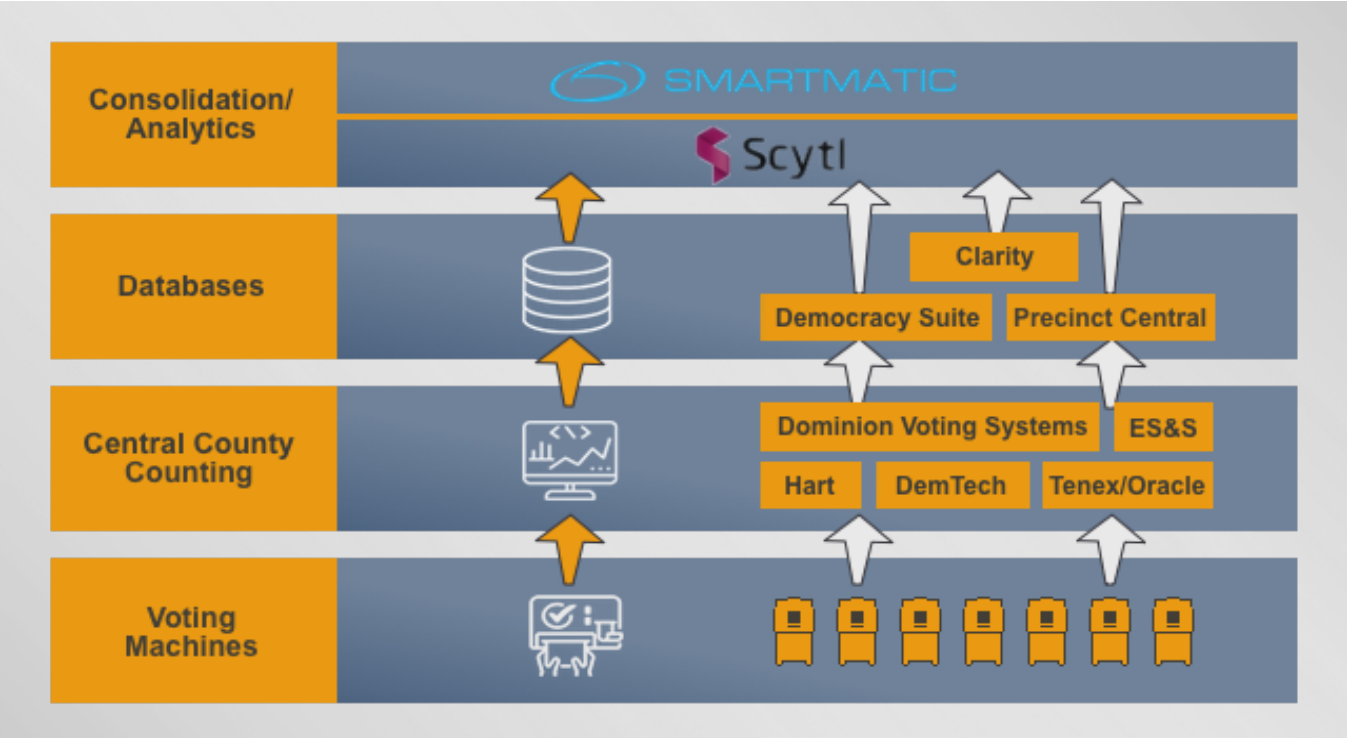
Un Serveur Espagnol

À propos de Scytl et d'un ordinateur électoral à Francfort

#Scytl #SmartMatic #Elections #Fraud

Mtous sont familiers avec les événements de Torrero en Espagne, dans lesquels un homme généralement courageux entre dans une arène pour s'engager directement avec un taureau. Seulement équipé d'un tissu rouge, le Torrero parvient la plupart du temps à laisser le taureau complètement épuisé, lui permettant de placer des armes mortelles dans le cou du taureau après de nombreuses heures. On se souvient presque d'un tel spectacle lorsqu'un membre du Congrès américain a laissé entendre à la mi-novembre 2020 que quelqu'un en Allemagne avait propagé le message que l'armée américaine aurait confisqué un serveur informatique dans la capitale bancaire allemande Francfort le 9 novembre 2020, ou avait au moins obtenu numériquement tout son contenu. Le serveur appartenait à l'origine à une société nommée Scytl, basée à Barcelone, en Espagne. Désormais entre les mains d'une banque, le serveur de Francfort aurait été connecté à diverses bases de données de résultats des élections américaines de 2020, gérées et exploitées par Scytl, qui a déclaré faillite à l'été 2020 et était sur le point d'entrer dans le processus de liquidation final.

La plupart des comtés des États américains utilisent des machines à voter pour compter les millions de bulletins de vote et utilisent quelques systèmes logiciels importants pour recueillir les résultats électroniques soumis par ces machines. Les logiciels les plus largement utilisés par la grande majorité des comtés américains sont soit Dominion Voting Systems, Tenex, ES&S, Hart ou DemTech. Une fois les bulletins de vote des comtés reçus, les différents systèmes logiciels transmettent les décomptes et les informations à une poignée de bases de données, exécutés sur l'infrastructure informatique cloud d'Amazon AWS et nommés Clarity, Democracy Suite, Precinct Central. Alors que la base de données Clarity appartient entièrement à Scytl, les autres sont soit exploitées, soit au moins accessibles par la société espagnole.



L'entreprise, située dans le centre-ville de la capitale catalane, Barcelone, a une histoire intéressante à raconter. Il a été fondé en 2001 par les chercheurs en systèmes de vote électronique Andreu Riera et Carles Rovira de l'Université de Barcelone juste après l'éclatement de la bulle Internet. Les deux ont soigneusement choisi le nom de l'entreprise comme cryptage de la première méthode de cryptage connue appelée Skytale, utilisée à des fins militaires dans la Grèce antique il y a environ 2500 ans. Pere Valles a rejoint l'entreprise très tôt, tout comme un groupe financier local. En 2006, le fondateur Riera est décédé dans un accident de voiture. Quelques années plus tard, Nauta Capital est devenu actionnaire et, en 2010, Scytl a payé 10 millions USD pour la société américaine SOE Software, un fournisseur majeur de solutions de gestion électrique. Les ventes ont atteint 25 millions USD, la société avait des bureaux à Washington, DC, Toronto, New Delhi, Athènes, Kiev et Singapour et un effectif de plus de 400 personnes. En 2013, le co-fondateur de Microsoft Paul Allen a investi 40 millions USD via son célèbre Vulcan Capital Fund.

Curieusement, malgré les plans pour enrôler la société au NASDAQ, la renommée de Scytl s'est érodée dans les années à venir. Les raisons sont au moins douteuses: les projets ont échoué et d'étranges efforts de réorganisation sabotaient le succès projeté de Scytl. En décembre 2019, la société a engagé une procédure de pré-faillite, un tribunal espagnol a déclaré la fin formelle et légale de la société de Barcelone le 2 juin 2020. Auparavant, les actionnaires de Scytl, JB Capital, Vulcan Capital, Nauta Capital et Spinnaker, pouvaient convaincre le fonds américain Sandton Capital pour reprendre la procédure de faillite et apparemment, Sandton Capital n'a pas beaucoup hésité à reconnecter l'un des serveurs de Scytl à Francfort à Internet. Ou est-ce que la commande du nouveau propriétaire de Scytl, Paragon Group, qui a racheté l'entreprise de Scytl reste dans un accord le 20 octobre 2020, par coïncidence exactement 14 jours avant l'élection présidentielle américaine ?

Une autre société qui se consacre au décompte des voix dans le monde est SGO Smartmatic , re-créée en 2014 en tant que société britannique sous le président Mark Malloch-Brown. Connecté à George Soros en ayant été le vice-président du fonds quantique du milliardaire - maintenant appelé Open Society Global - Sir Malloch-Brown est profondément lié à l'ONU, aux Clinton et à d'autres organisations Soros. Smartmatic a fait l'objet d'un examen minutieux en 2005 lorsqu'elle a acheté une société américaine nommée Sequoia Voting Systems. Les membres du Congrès américain ont demandé au Comité sur l'investissement étranger aux États-Unis (CFIUS) d'examiner de plus près l'accord déjà à l'époque, car Sequoia aurait eu des liens avec le gouvernement vénézuélien. Des responsables américains ont déclaré en 2006qu "il semble y avoir eu un effort évident pour masquer la propriété de l'entreprise", faisant référence au réseau caché de fiducies et de fonds de Smartmatic qui s'engagent dans la société britannique.

En 2017, les élections générales vénézuéliennes ont été truquées par environ 1 million de voix, gérées par le logiciel Smartmatic, qui était en contact avec le gouvernement vénézuélien depuis 2004. Un total de 8 millions de personnes ont voté lors de cette élection, ce à quoi le PDG de Smartmatic, Antonio Mugica, a fait référence.devant un groupe de presse bouleversé à Londres, déclarant que «nous savons, sans aucun doute, que le taux de participation aux récentes élections pour une Assemblée nationale constituante [du Venezuela] a été manipulé». Un dénonciateur a déclaré en 2020 que Smartmatic utilise le même logiciel que Dominion Voting Systems, ce dernier étant utilisé dans près de 30 États américains, et que le logiciel a joué un rôle dans le passé pour maintenir Hugo Chavez au pouvoir au Venezuela:

En 2019, un groupe international de chercheurs en fraude électorale en Suisse a découvert que le logiciel de Scytl pouvait facilement être manipulé. Les auditeurs du logiciel ont constaté qu'un problème de porte dérobée dans le système permettait de remplacer entièrement les bulletins légitimes par des bulletins frauduleux:

> La vulnérabilité est étonnante. Lors d'élections normales, il n'y a pas une seule personne qui pourrait frauder de manière indétectable toute l'élection. Mais dans ce système qu'ils ont construit, il y a un parti qui pourrait le faire. (Matthew Green, professeur de cryptographie à l'Université Johns Hopkins)

Scytl n'a pas tardé à minimiser la vulnérabilité de sécurité, déclarant que les pirates informatiques avaient besoin d'accéder à l'infrastructure informatique de la Poste Suisse, qui a acheté les droits du code source du logiciel de Scytl en avril 2019. Il a été affirmé que "l'aide de plusieurs initiés ayant des connaissances spécialisées sur La Poste Suisse ou les cantons" étaient nécessaires, tout en ignorant le fait que le groupe d'experts en sécurité n'avait pas un tel accès pour détecter assez rapidement le problème logiciel.

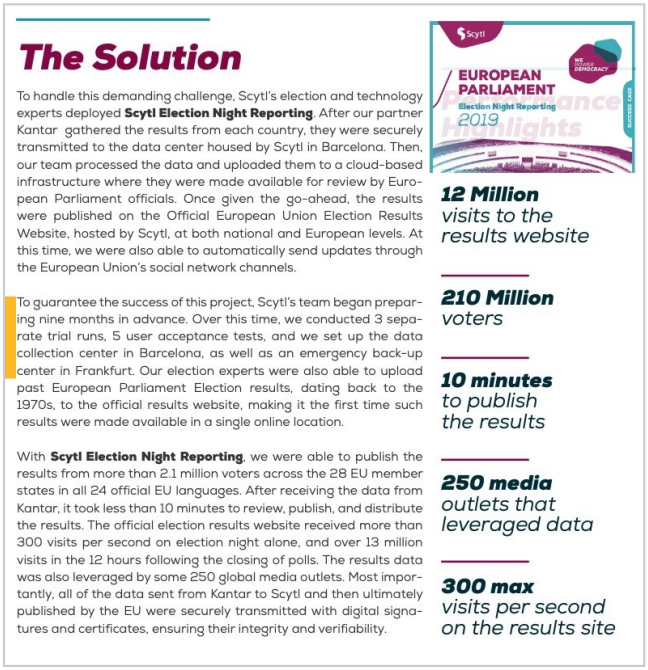
Un incident similaire s'est produit à la suite de l'élection de Torrero US 2020, lorsque Scytl n'a pas tardé

à démystifier toute allégation de fraude massive, également sur son serveur de Francfort. Un rapport confidentiel sur les irrégularités électorales, menée dans les mois précédant les élections présidentielles américaines de 2020, indique cependant que les données électorales ont été transmises à plusieurs serveurs en dehors des États-Unis, explicitement également à un serveur appartenant à la société de Barcelone:

> Les registres de vote pour l'élection générale de 2018 ont été automatiquement transmis du site Web clarityelections.com à plusieurs adresses DNS nationales et étrangères, y compris ES&S, Scytl à Barcelone, Smartmatic à Londres et un serveur russe à l'Université d'État du Sud de l'Oural à Chalyabinsk, un GRU connu installation.
>
> (Rapport de synthèse sur les irrégularités électorales d'août 2020)

Scytl lui-même a laissé entendre en 2019 qu'elle était liée à la ville allemande de Francfort malgré son affirmation de 2020 "nous n'avons ni serveurs ni bureaux à Francfort". L'entreprise a également été sélectionnée pour fournir l'infrastructure informatique pour les élections européennes de 2019. Dans une étude de cas Scytl 2019, la société a déclaré ce qui suit:

> Pour garantir le succès de ce projet [Élections UE 2019], l'équipe de Scytl a commencé à se préparer neuf mois à l'avance. Au cours de cette période, nous avons effectué 3 essais distincts, 5 tests d'acceptation par les utilisateurs et nous avons mis en place le centre de collecte de données à Barcelone, ainsi qu'un centre de secours d'urgence à Francfort.
>
> (Étude de cas de réussite Scytl pour les élections européennes de 2019, page 3)



The Solution

To handle this demanding challenge, Scytl's election and technology experts deployed **Scytl Election Night Reporting**. After our partner Kantar gathered the results from each country, they were securely transmitted to the data center housed by Scytl in Barcelona. Then, our team processed the data and uploaded them to a cloud-based infrastructure where they were made available for review by European Parliament officials. Once given the go-ahead, the results were published on the Official European Union Election Results Website, hosted by Scytl, at both national and European levels. At this time, we were also able to automatically send updates through the European Union's social network channels.

To guarantee the success of this project, Scytl's team began preparing nine months in advance. Over this time, we conducted 3 separate trial runs, 5 user acceptance tests, and we set up the data collection center in Barcelona, as well as an emergency back-up center in Frankfurt. Our election experts were also able to upload past European Parliament Election results, dating back to the 1970s, to the official results website, making it the first time such results were made available in a single online location.

With **Scytl Election Night Reporting**, we were able to publish the results from more than 2.1 million voters across the 28 EU member states in all 24 official EU languages. After receiving the data from Kantar, it took less than 10 minutes to review, publish, and distribute the results. The official election results website received more than 300 visits per second on election night alone, and over 13 million visits in the 12 hours following the closing of polls. The results data was also leveraged by some 250 global media outlets. Most importantly, all of the data sent from Kantar to Scytl and then ultimately published by the EU were securely transmitted with digital signatures and certificates, ensuring their integrity and verifiability.

12 Million *visits to the results website*

210 Million *voters*

10 minutes *to publish the results*

250 media *outlets that leveraged data*

300 max *visits per second on the results site*

Ce n'est pas différent des événements de torrero espagnols, où généralement, à la toute fin, le taureau était traîné dans les rues pour être exposé au public et donc tout le monde à voir.

https://www.sun24.news/fr/un-serveur-espagnol-a-propos-de-scytl-et-dun-ordinateur-electoral-a-francfort.html