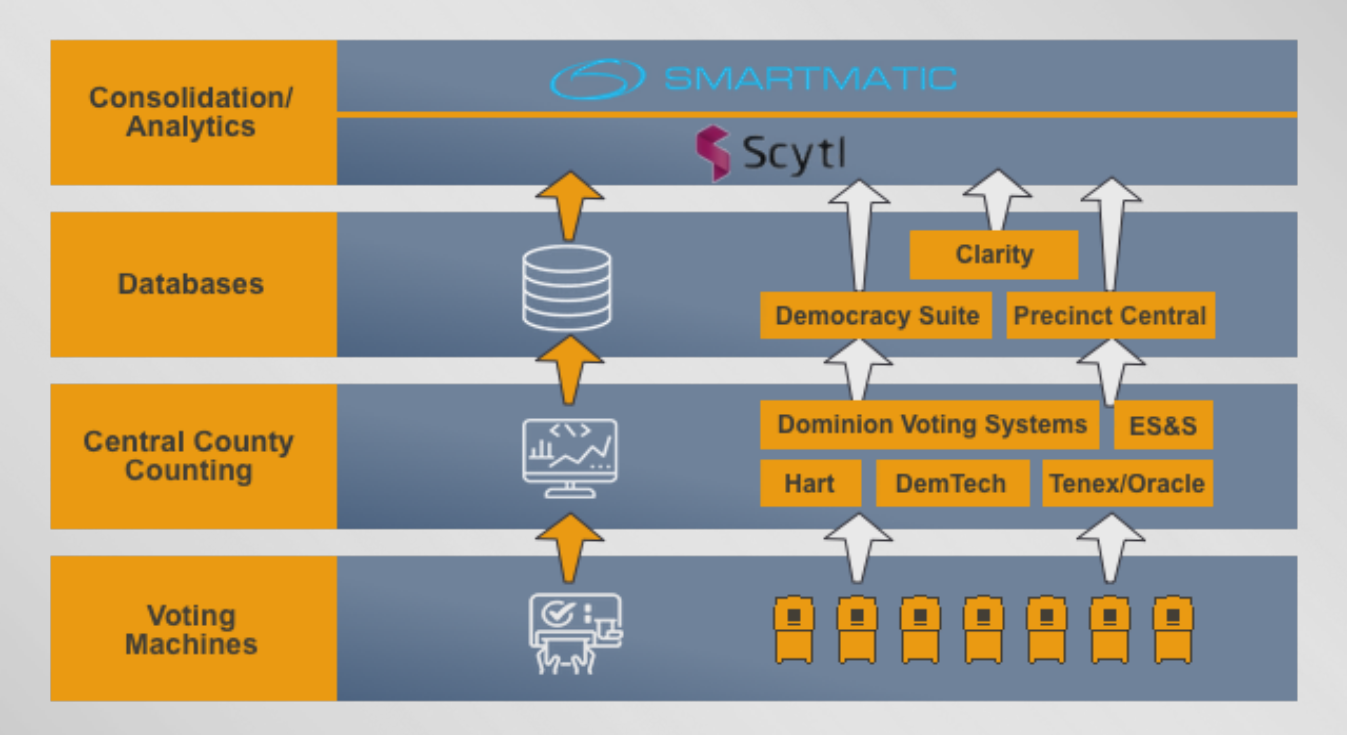
Un Servidor Español

Acerca de Scytl y una computadora electoral en Frankfurt

#Scytl #SmartMatic #Elections #Fraud

Todos están familiarizados con los acontecimientos de Torrero en España, en los que un hombre normalmente valiente entra en una arena para enfrentarse directamente a un toro. Solo equipado con un pañuelo rojo, el Torrero logra en su mayoría dejar al toro completamente exhausto, lo que le permite colocar armas letales en el cuello del toro después de muchas horas. Uno casi recuerda ese espectáculo cuando un congresista de los EE.UU. insinuó a mediados de noviembre de 2020 que alguien en Alemania había difundido el mensaje de que el ejército de los EE.UU. había confiscado un servidor informático en la capital bancaria alemana, Frankfurt, el 9 de noviembre de 2020, o había al menos obtenido digitalmente todos sus contenidos. El servidor originalmente pertenecía a una empresa llamada Scytl, con sede en Barcelona, España. Ahora en manos de un banco, el servidor de Frankfurt supuestamente estaba conectado a varias bases de datos de resultados electorales de EE. UU. 2020, administradas y operadas por Scytl, que presentó bancarrota en el verano de 2020 y estaba a punto de ingresar al proceso de liquidación final.

La mayoría de los condados estatales de EE. UU. utilizan máquinas de votación para contar los millones de boletas y utilizan algunos sistemas de software importantes para recopilar los resultados electrónicos enviados por estas máquinas. El software más utilizado por la gran mayoría de los condados de EE. UU. Son Dominion Voting Systems, Tenex, ES&S, Hart o DemTech. Una vez que se han recibido las boletas del condado, los diversos sistemas de software envían los recuentos de votos y la información a un puñado de bases de datos, se ejecutan en la infraestructura de TI en la nube de Amazon AWS y se denominan Clarity, Democracy Suite, Precinct Central. Si bien la base de datos de Clarity es propiedad exclusiva de Scytl, las otras son operadas o al menos accesibles por la compañía española.



La empresa, ubicada en el centro de la capital catalana, Barcelona, tiene una interesante historia que vale la pena contar. Fue fundada en 2001 por los investigadores de sistemas de votación electrónica Andreu Riera y Carles Rovira de la Universidad de Barcelona justo después de que estallara la burbuja de las puntocom. Los dos eligieron cuidadosamente el nombre de la empresa como cifrado del primer método de cifrado conocido llamado Skytale, que se utilizó con fines militares en la antigua Grecia hace unos 2500 años. Pere Valles se incorporó a la empresa desde el principio, al igual que un grupo financiero local. En 2006, el fundador Riera murió en un accidente automovilístico. Unos años más tarde, Nauta Capital se convirtió en accionista y en 2010 Scytl pagó 10 millones de dólares por la empresa estadounidense SOE Software, un importante proveedor de soluciones de gestión eléctrica. Las ventas alcanzaron los 25 millones de dólares, la empresa tenía oficinas en Washington, DC, Toronto, Nueva Delhi, Atenas, Kiev y Singapur y una plantilla de más de 400 personas. En 2013, el cofundador de Microsoft Paul Allen invirtió 40 millones de USD a través de su famoso Fondo de Capital Vulcan.

Sin embargo, curiosamente, a pesar de los planes para incorporar a la empresa en NASDAQ, la fama de Scytl se erosionó en los próximos años. Las razones son al menos dudosas: los proyectos fracasaron y los extraños esfuerzos de reorganización estaban saboteando el éxito proyectado de Scytl. En diciembre de 2019, la empresa entró en un proceso preconcursal, un tribunal español declaró el fin formal y legal de la empresa de Barcelona el 2 de junio de 2020. Anteriormente, los accionistas de Scytl, JB Capital, Vulcan Capital, Nauta Capital y Spinnaker pudieron convencer al fondo estadounidense Sandton Capital para hacerse cargo de los procedimientos de quiebra y, aparentemente, Sandton Capital no dudó mucho en volver a conectar uno de los servidores de Scytl en Frankfurt a Internet. ¿O vino el pedido del nuevo propietario de Scytl, Paragon Group, que compró los restos comerciales de Scytl en un acuerdo el 20 de octubre de 2020, coincidentemente exactamente 14 días antes de las elecciones presidenciales de Estados Unidos ?

Otra empresa que se está dedicando al conteo de votos a nivel mundial es SGO Smartmatic , que en 2014 se re-formó como una empresa del Reino Unido bajo el presidente Mark Malloch-Brown. Conectado con George Soros por haber sido el vicepresidente del Fondo Cuántico del multimillonario, ahora llamado Open Society Global, Sir Malloch-Brown está profundamente vinculado a la ONU, los Clinton y otras organizaciones Soros. Smartmatic fue objeto de escrutinio en 2005 cuando compró una empresa estadounidense llamada Sequoia Voting Systems. Los congresistas estadounidenses solicitaron al Comité de Inversión Extranjera en los Estados Unidos (CFIUS) que examinara más de cerca el acuerdo en ese entonces, ya que se alegaba que Sequoia tenía vínculos con el gobierno venezolano. Los funcionarios estadounidenses declararon en 2006que "parece haber habido un esfuerzo obvio para ocultar la propiedad de la empresa", refiriéndose a la red oculta de fideicomisos y fondos de Smartmatic que participan en la empresa del Reino Unido.

En 2017, las elecciones generales venezolanas fueron amañadas por alrededor de 1 millón de votos, gestionados por el software Smartmatic, que estuvo en contacto con el gobierno venezolano desde 2004. Un total de 8 millones de personas votaron en esa elección, a la que se refirió el director general de Smartmatic, Antonio Mugica.frente a un cuerpo de prensa burlado en Londres, afirmando que “sabemos, sin ninguna duda, que la participación de la reciente elección para una Asamblea Nacional Constituyente [de Venezuela] fue manipulada”. Un denunciante declaró en 2020 que Smartmatic usa el mismo software que Dominion Voting Systems, este último se usa en casi 30 estados de EE. UU., Y que el software fue fundamental en el pasado para mantener a Hugo Chávez en el poder en Venezuela:

En 2019, un grupo internacional de investigadores de fraude electoral en Suiza descubrió que el software de Scytl podía manipularse fácilmente. Los auditores de software encontraron que una falla de puerta trasera en el sistema permitió que las boletas legítimas fueran reemplazadas por completo por otras fraudulentas:

> La vulnerabilidad es asombrosa. En elecciones normales, no hay una sola persona que pueda defraudar indetectablemente a toda la elección. Pero en este sistema que construyeron, hay un partido que podría hacer eso.
>
> Matthew Green, profesor de criptografía en la Universidad Johns Hopkins

Scytl se apresuró a minimizar la vulnerabilidad de seguridad, afirmando que los piratas informáticos necesitaban acceso a la infraestructura de TI del Swiss Post, que compró los derechos del código fuente del software de Scytl en abril de 2019. Se afirmó que "la ayuda de varios expertos con conocimientos Swiss Post o los cantones" era necesario, mientras que al mismo tiempo se ignoraba el hecho de que el grupo de expertos en seguridad no tenía ese acceso al detectar el problema de software con bastante rapidez.

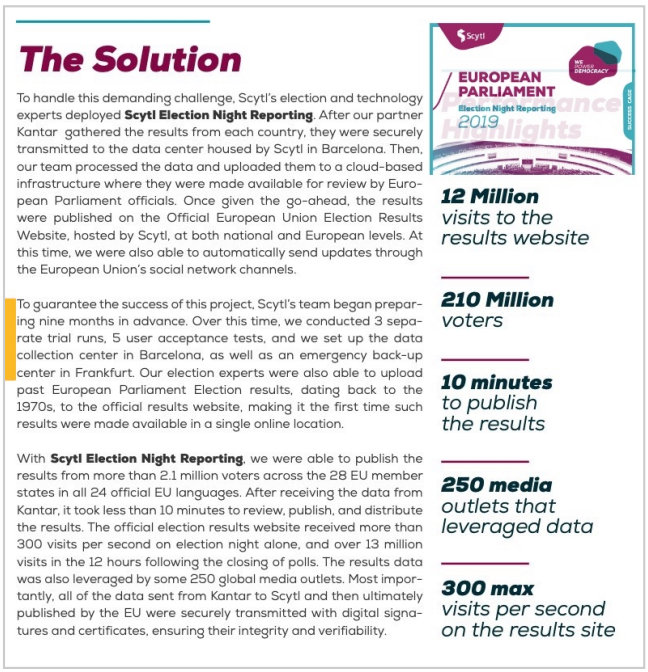
Un incidente similar ocurrió después del evento electoral de Torrero en EE. UU. 2020, cuando Scytl se

apresuró a desacreditar cualquier acusación sobre fraude masivo, también en su servidor de Frankfurt. Un informe confidencial sobre irregularidades electorales, realizada en los meses previos a las elecciones presidenciales de EE. UU. 2020, sin embargo, establece que los datos electorales se enviaron a múltiples servidores fuera de EE. UU., explícitamente también a un servidor propiedad de la empresa de Barcelona:

> Los registros de votación para las elecciones generales de 2018 se enviaron automáticamente desde el sitio web clarityelections.com a múltiples direcciones DNS nacionales y extranjeras, incluidas ES&S, Scytl en Barcelona, Smartmatic en Londres y un servidor ruso en la Universidad Estatal de South Ural en Chalyabinsk, un conocido GRU instalación.
>
> Informe resumido sobre irregularidades en las elecciones de agosto de 2020

La propia Scytl insinuó en 2019 que está ligada a la ciudad alemana de Frankfurt a pesar de su afirmación de 2020 "no tenemos servidores ni oficinas en Frankfurt". La empresa también fue seleccionada para proporcionar la infraestructura de TI para las elecciones de la UE de 2019. En un estudio de caso de Scytl de 2019, la compañía declaró lo siguiente:

> Para garantizar el éxito de este proyecto [Elecciones UE 2019], el equipo de Scytl comenzó a prepararse con nueve meses de anticipación. Durante este tiempo, realizamos 3 pruebas independientes, 5 pruebas de aceptación de usuarios y establecimos el centro de recopilación de datos en Barcelona, así como un centro de respaldo de emergencia en Frankfurt.
>
> Estudio de caso de éxito de Scytl para las elecciones de la UE de 2019, página 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.

No muy diferente de los eventos de torrero españoles, donde generalmente, al final, el toro era arrastrado por las calles para exhibición pública y, por lo tanto, todos lo veían.

https://www.sun24.news/es/un-servidor-espanol-acerca-de-scytl-y-una-computadora-electoral-en-frankfurt.html