Homeland Security

# Proteger los datos del registro de votantes

según la Dirección de Programas y Protección Nacional del Departamento de Seguridad Nacional

*26 de junio de 2018*

## Descripción general

Las bases de datos del registro de votantes (VRDB, por sus siglas en inglés) son objetivos importantes y pueden ser objetivos atractivos para las intrusiones informáticas. Este problema no es exclusivo de los estados individuales: Se comparte en todo el país. Las claves de una buena ciberseguridad son la concientización y la vigilancia constante.

## ¿Cuáles son las amenazas que pueden poner en riesgo los datos de los votantes?

Los actores maliciosos pueden usar una variedad de métodos para interferir con los sitios web y las bases de datos del registro de votantes. Algunos métodos de ataque se enumeran a continuación y brindan orientación aplicable a las VRDB y a muchas otras redes informáticas.

- Los intentos de *phishing* son correos electrónicos, textos y otros mensajes falsificados que se utilizan para manipular a los usuarios con el fin de que accedan enlaces maliciosos o descarguen archivos adjuntos maliciosos. Los ataques de *phishing* pueden conducir al robo de credenciales (por ejemplo, contraseñas) o pueden actuar como un punto de entrada para que los actores de amenazas propaguen *malware* en una organización, roben información de los votantes o interrumpan las operaciones de votación. Para obtener información sobre cómo defenderse contra el *phishing*, consulte el Consejo del Equipo de preparación para emergencias informáticas de los Estados Unidos (US-CERT, por sus siglas en inglés) sobre cómo Evitar ataques de ingeniería social y phishing.
- Los defectos de inyección son una técnica amplia de ataque que intenta enviar comandos a un navegador, base de datos u otro sistema, lo cual permite que un usuario regular pueda controlar el comportamiento. El ejemplo más común es la inyección de lenguaje de consulta estructurada (SQL, por sus siglas en inglés), que subvierte la relación entre una página web y su base de datos de apoyo, generalmente para obtener información contenida dentro de la base de datos del registro de votantes. Otra forma es la inyección de comandos, en la que un usuario que no es de confianza puede enviar comandos a un sistema operativo compatible con una aplicación web o una base de datos. Consulte la publicación de US-CERT acerca de Inyección SQL para más información.
- Las vulnerabilidades de secuencias de comandos entre sitios (XSS) permiten a los actores maliciosos insertar y ejecutar código no autorizado en aplicaciones web. Los ataques XSS exitosos en los sitios web del registro de votantes pueden proporcionar al atacante acceso no autorizado a la información de los votantes. Para conocer estrategias de prevención y mitigación contra XSS, consulte el enlace Alerta sobre servidores web y shells web comprometidos de US-CERT.
- Los ataques de negación del servicio (DoS, por sus siglas en inglés) impiden que los usuarios legítimos accedan a información o servicios. Un ataque DoS puede hacer que un sitio web del registro de votantes no esté disponible o niegue el acceso a los datos del registro de votantes. Póngase en contacto con su proveedor de servicios de Internet (ISP) para analizar las formas en que ellos pueden ayudar a bloquear los ataques DoS dirigidos a su organización. Para obtener más información sobre DoS, consulte la lista de consejos del US-CERT para Comprender los ataques de negación del servicio.
- Las vulnerabilidades de un servidor pueden explotarse para permitir el acceso no autorizado a información confidencial. Un ataque contra un servidor mal configurado que ejecuta un sitio web del registro de votantes puede permitir un acceso negativo a información crítica y a la base de datos del registro de votantes. Consulte las sugerencias de US-CERT acerca de Seguridad del sitio web para obtener información adicional.
- El *ransomware* es un tipo de software malicioso que infecta un sistema informático y restringe el acceso de los usuarios a los recursos o datos del sistema hasta que se pague un rescate para desbloquearlo. No es aconsejable que las organizaciones afectadas paguen dicho rescate, ya que esto no garantiza que el acceso a una VRDB comprometida sea restaurado. Para obtener más información sobre el *ransomware*, consulte la publicación de US-CERT sobre el Secuestro de datos.

## ¿Qué medidas de prevención debo emplear para protegerme contra estas amenazas?

El DHS anima a los funcionarios electorales y administradores de redes a implementar las siguientes recomendaciones, que pueden prevenir hasta un 85 % de los ataques cibernéticos dirigidos.
Estas estrategias son parte del sentido común para muchos, pero el DHS sigue observando intrusiones causadas por el hecho de que las organizaciones no utilizan estas medidas básicas:

- Aplicación de parches y sistemas operativos: Las aplicaciones y los sistemas operativos vulnerables son el objetivo de la mayoría de los ataques. Asegurarse de que tengan parches con las últimas actualizaciones reduce en gran medida la cantidad de puntos de entrada explotables disponibles para un atacante.
- Lista blanca de aplicaciones: La lista blanca es una de las mejores estrategias de seguridad, ya que permite que solo se ejecuten programas específicos mientras todos los demás son bloqueados, incluido el software malicioso.
- Restricción de privilegios administrativos: Esto evita que se ejecute software malicioso o limita su capacidad de propagación en la red.
- Validación de entrada: La validación de entrada es un método para limpiar la entrada de datos por parte de un usuario no confiable proporcionada en una aplicación web y puede prevenir muchos tipos de fallas de seguridad dicha aplicación web, como SQLi, XSS y *Command Injection*.
- Conocimiento de los *firewalls*: Cuando cualquiera puede acceder a su red en cualquier momento, su red es más susceptible de ser atacada. Los *firewalls* se pueden configurar para bloquear datos de ciertas ubicaciones (lista blanca de IP) o aplicaciones mientras permiten el paso de datos relevantes y necesarios.

Un compromiso dirigido hacia el uso de buena seguridad cibernética y de mejores prácticas es fundamental para proteger los datos del registro de votantes. Aquí hay algunas preguntas que puede hacerle a su organización para ayudar a prevenir ataques contra sitios web y bases de datos del registro de votantes:

- Copias de seguridad: ¿Hacemos copias de seguridad de toda la información crítica? ¿Las copias de seguridad se almacenan fuera de línea? ¿Hemos probado nuestra capacidad para utilizar las copias de seguridad en caso de un incidente?
- Análisis de riesgos: ¿Hemos realizado un análisis de riesgos de ciberseguridad en la organización?
- Capacitación del personal: ¿Hemos capacitado al personal en la implementación de mejores prácticas de ciberseguridad?
- Escaneo y parches de vulnerabilidades: ¿Hemos implementado escaneos regulares de nuestra red y sistemas, e incorporado parches apropiados para vulnerabilidades identificadas en el sistema?
- Lista blanca de aplicaciones: ¿Permitimos que solo los programas aprobados se ejecuten en nuestras redes?
- Respuesta a incidentes: ¿Tenemos un plan de respuesta a incidentes y lo hemos puesto en práctica?
- Continuidad operacional: ¿Somos capaces de mantener las operaciones sin acceso a ciertos sistemas? ¿Por cuánto tiempo? ¿Hemos comprobado esto?
- Pruebas de penetración: ¿Hemos intentado piratear nuestros propios sistemas para probar la seguridad de nuestros sistemas y nuestra capacidad de defensa ante dichos ataques?

## ¿Cómo respondo al acceso no autorizado a los datos del registro de votantes?

Implemente su respuesta a incidentes de seguridad y su plan para la continuidad de operaciones. Puede tomar tiempo para que los profesionales de IT (por sus siglas en inglés) de su organización aíslen y eliminen las amenazas a sus sistemas y restablezcan la normalidad en sus operaciones. Mientras tanto, debe tomar medidas para mantener las funciones esenciales de su organización de acuerdo con su plan de continuidad de operaciones. Las organizaciones deben mantener y poner a prueba periódicamente los planes para copias de seguridad, los planes para recuperación ante desastres y los procedimientos de continuidad de operaciones.

Comuníquese con el DHS o con la policía de inmediato. Lo animamos a que se comunique con el Centro Nacional de Integración de Comunicaciones y Ciberseguridad (NCCIC) de DHS (NCCICcustomerservice@hq.dhs.gov o 888-282-0870), o con el FBI a través de una oficina local o la División Cibernética del FBI (CyWatch@ic.fbi.gov o 855-292-3937) para informar acerca de una intrusión y solicitar recursos de respuesta a incidentes o cualquier tipo de asistencia técnica.