SEGURIDAD DE LA INFRAESTRUCTURA CIBERNÉTICA: CAMPAÑAS POLÍTICAS

Los incidentes cibernéticos que afectan a las campañas políticas son cada vez más complejos y pueden tener serias consecuencias. Utilice las estrategias recomendadas a continuación para ayudar a proteger su campaña contra actividades maliciosas.

IMPLEMENTACIÓN DE LA AUTENTICACIÓN MULTIFACTOR (MFA)

MFA (por sus siglas en inglés) es un enfoque en varios pasos para la seguridad de cuentas, aplicaciones y datos en línea. Requiere que un usuario presente una combinación de dos o más credenciales para verificar su identidad al iniciar una sesión. Asegúrese de que la MFA esté activada para el correo electrónico de la campaña, las redes sociales, las cuentas electrónicas, las aplicaciones o cualquier otro servicio electrónico relacionado con la campaña.

- Para obtener más información sobre MFA, consulte el sitio web Más que una contraseña (*More than a Password*) de CISA en https://www.cisa.gov/MFA.

USE CONTRASEÑAS SEGURAS

El uso de contraseñas simples o de información de identificación común, como fechas de cumpleaños, no son seguras para proteger las cuentas importantes. Vaya más allá de las contraseñas fáciles de adivinar y reduzca el riesgo de piratería de contraseñas:

- Use administradores de contraseñas para generar y proteger contraseñas que protejan su entorno de usuarios no verificados. Requiera el uso de contraseñas largas, aleatorias y únicas para cada cuenta para contrarrestar los ataques de software automatizados.
- Para obtener más información sobre la creación de contraseñas seguras, consulte el sitio web de CISA Use Contraseñas Seguras (*Use Safe Passwords*) en https://www.cisa.gov/secure-our-world/use-strong-passwords.

ACTUALICE EL SOFTWARE RÁPIDAMENTE

Las actualizaciones de software se publican para corregir los riesgos de seguridad. Mantener el software actualizado es una manera fácil de mantenerse más seguro.

- Siempre que sea posible, esté atento a las notificaciones, instale las actualizaciones lo antes posible y active las actualizaciones automáticas. Para obtener más información sobre la actualización del software, consulte la página web de actualización de software de CISA en https://www.cisa.gov/secure-our-world/update-software.

CIFRE LOS SERVICIOS DE MENSAJERÍA Y OTROS SISTEMAS

En el caso de comunicaciones confidenciales, utilice servicios de mensajería cifrada para proporcionar un nivel adicional de protección. El uso del cifrado de extremo a extremo ayuda a proteger la privacidad de su comunicación.

ASEGURE LOS DISPOSITIVOS DE CAMPAÑAS Y PERSONALES

Los miembros de la familia del candidato suelen ser objetivo de los piratas informáticos que buscan un punto de entrada para acceder a información y datos confidenciales de la campaña, ya que sus dispositivos pueden ser menos seguros que los propios dispositivos del candidato.

- Asegúrese de que los dispositivos personales y de campaña para el personal y los miembros de la familia se contabilicen y se mantengan seguros. Como mínimo, todos los dispositivos y cuentas personales deben estar actualizados y utilizar contraseñas seguras y MFA.

RECONOZCA Y DENUNCIE LA CIBERESTAFA (*PHISHING*)

La Ciberestafa (*phishing*) es una táctica común en la que se "engaña" a los usuarios para que abran enlaces, correos electrónicos o archivos adjuntos dañinos que solicitan información confidencial o descargan software malicioso. Los mensajes a menudo están diseñados para aparentar que provienen de una fuente confiable.

- Eduque al personal de campaña acerca del funcionamiento de estas tácticas y realice pruebas de ciberestafa para que el personal practique su identificación y denuncia. La ciberestafa debe ser reportada a https://www.cisa.gov/report o a report@cisa.gov.

CREAR UN PLAN DE RESPUESTA A INCIDENTES CIBERNÉTICOS

Aun con la implementación de todas las prácticas recomendadas, es posible que se produzcan incidentes. Crear y practicar un plan de respuesta a incidentes organizacionales ayudará a todos los miembros del equipo a comprender, prepararse y mitigar los riesgos de posibles incidentes cibernéticos. Para obtener más información sobre cómo crear un plan de respuesta a incidentes, consulte la Guía de planificación de respuesta a incidentes de CISA en https://www.cisa.gov/resources-tools/resources/cyber-incident-guide.

- Cree un plan de respuesta a incidentes cibernéticos que los miembros del equipo conozcan y les permita estar capacitados sobre los procedimientos de respuesta.
- Denuncie los incidentes cibernéticos a CISA en https://www.cisa.gov/report enviando un correo electrónico a **report@cisa.gov** o al (888) 282-0870.