Protocolo de transferencia de hipertexto seguro (HTTPS)

¿Qué es?: *El protocolo de transferencia de hipertexto seguro (HTTPS, por sus siglas en inglés) es un protocolo de comunicación de internet que se utiliza para cifrar y transmitir información de manera segura entre el navegador web de un usuario y el sitio web al que está conectado.*
Está diseñado para proteger mejor la integridad y confidencialidad de la información de los usuarios cuando visitan sitios web.
El HTTPS logra esto mediante el uso de un certificado de capa de sockets seguros (SSL, por sus siglas en inglés), que establece una conexión cifrada. El certificado también ayuda a autenticar que el sitio web y el usuario son quienes dicen ser cuando se comunican. Estas características hacen que sea más difícil para los actores maliciosos manipular la comunicación. El HTTPS se basa en el protocolo de transferencia de hipertexto (HTTP), el protocolo de comunicación utilizado para transmitir datos entre un sitio web y un usuario, pero HTTP transmite contenido sin cifrarlo. El HTTPS se está convirtiendo en la norma en Internet. Por ejemplo, a partir del 31 de diciembre de 2016, se requiere HTTPS en todos los sitios web del gobierno federal.

¿Por qué es importante?: Cuando la comunicación se transmite sin cifrar, se envía a través de texto sin formato entre el usuario y el sitio web conectado. Esto puede exponer la comunicación a actores maliciosos que rastrean el tráfico en una red o intentan manipular sus contenidos. El cifrado es especialmente importante en las páginas web que recopilan información a través de formularios o requieren que el usuario inicie sesión, como el registro de votantes en línea.
Además, a partir de julio de 2018, el navegador Google Chrome comenzará a marcar los sitios web que no usan HTTPS como "No seguros". Google Chrome tiene más del 50 % de participación en el mercado y se clasifica como el navegador más utilizado a partir de 2018. Los usuarios seguirán teniendo acceso a los sitios web de las oficinas electorales que continúen usando HTTP después de la fecha límite de julio, pero verán la etiqueta "No seguro" en su barra de direcciones, como se muestra a continuación. Esta etiqueta puede afectar negativamente la confianza del público en los sitios web electorales que no utilizan HTTPS.

¿Qué puede hacer?: Si el sitio web de su oficina electoral actualmente no usa HTTPS, considere implementarlo antes de julio de 2018. Esto incluye verificar que su organización tenga un certificado SSL válido de una autoridad de certificación de confianza. Recursos como el sitio web HTTPS, la guía de Google para habilitar HTTPS en sus servidores de Qualys Labs documentación sobre certificados SSL, proporcione información adicional para ayudar en la implementación.

Para una actualización sobre el cifrado en general, revise el EI-ISAC del 30 de marzo de 2018 Cybersecurity Spotlight.

Operaciones de Seguridad 24×7 Centro
de Análisis e Intercambio de Información de Infraestructura Electoral (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

Aprenda, obtenga asistencia y colabore

- Para obtener información sobre los programas cibernéticos del DHS, visite https://www.dhs.gov/cyber
- Para acceder a la gama completa de recursos cibernéticos del DHS, envíe un correo electrónico a SLTTCyber@hq.dhs.gov
- Para obtener más información sobre asesores regionales de seguridad y asesores de ciberseguridad, visite https://www.dhs.gov/protective-security-advisors
- Para convertirse en miembro de EI-ISAC, visite https://learn.cisecurity.org/ei-isac-registration
- Para obtener más información sobre el Portal HSIN, comuníquese con HSIN.Outreach@hq.dhs.gov
- Para obtener información sobre el entorno de capacitación virtual federal, visite https://fedvte.usalearning.gov

Homeland Security