CIBERSEGURIDAD DE LA INFRAESTRUCTURA ELECTORAL LISTA DE VERIFICACIÓN DE PREPARACIÓN Y RESILIENCIA

INTRODUCCIÓN

La infraestructura de red y las aplicaciones conectadas a Internet sustentan y posibilitan una variedad de funciones en la realización de elecciones. Estas pueden incluir redes de infraestructura electoral que almacenan, alojan o procesan información de registro de votantes, sitios web electorales públicos que admiten funciones, como informes de la noche de las elecciones y búsqueda de lugares de votación, así como correos electrónicos y otras operaciones comerciales críticas. La infraestructura electoral y gubernamental siguen siendo objetivos atractivos para una variedad de agentes maliciosos, desde ciberdelincuentes hasta agentes de estados nacionales. Los defensores de la red tienen el poder de prevenir la mayoría de los incidentes de seguridad utilizando medidas de seguridad básicas. Tome medidas ahora para que, incluso si ocurre un incidente, las operaciones electorales esenciales puedan continuar. La siguiente lista de verificación fue diseñada para ayudar a los funcionarios de seguridad electoral y sus equipos de IT a revisar rápidamente las prácticas de ciberseguridad existentes para protegerse contra algunas de las amenazas más comunes, como ransomware o ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés), y tomar medidas para mejorar la preparación y resiliencia de la ciberseguridad de su organización durante este ciclo electoral.

CÓMO UTILIZAR ESTE RECURSO

Esta lista de verificación proporciona una serie de preguntas para orientar la toma de decisiones necesaria para prepararse ante posibles incidentes de ciberseguridad. Si responden a estas preguntas, el personal electoral y sus equipos de tecnología de la información (IT, por sus siglas en inglés) estarán mejor posicionados para evaluar su postura actual en materia de ciberseguridad frente a amenazas comunes e identificar acciones adicionales que se pueden tomar.

LISTA DE VERIFICACIÓN DE SEGURIDAD

Protéjase y responda: intentos de phishing dirigidos a su correo electrónico

SÍ/NO **¿Ha habilitado la autenticación multifactor (MFA, por sus siglas en inglés) en todas las cuentas?**

- Active la MFA para **todas las cuentas**.
- Asegúrese de que cada cuenta tenga sus propias credenciales únicas y no permita que se compartan.
- Aplique el principio del mínimo privilegio separando las cuentas de administrador y las cuentas de usuario.
- Asegúrese de que todos cambien sus contraseñas predeterminadas y se requieran contraseñas seguras para **todas las cuentas**.

SÍ/NO **¿Ha habilitado la autenticación basada en dominios para mensajes, informes y conformidad (DMARC, por sus siglas en inglés) para todas las cuentas de correo electrónico?**

- Habilite la DMARC en todas las cuentas de correo electrónico para facilitar que los remitentes y receptores de correo electrónico determinen si un correo electrónico se originó legítimamente del remitente identificado y proporcione al usuario instrucciones para manejar el correo electrónico si es fraudulento.

SÍ/NO **¿Se filtra el correo electrónico para proteger contra contenido malicioso?**

- Implemente el marcado de correos electrónicos externos para alertar a los usuarios para que tengan el debido cuidado al abrirlos.

SÍ/NO **¿Su personal electoral solo utiliza cuentas de correo electrónico oficiales para asuntos oficiales?**

- Capacite al personal para que sepa que solo debe utilizar sus cuentas de correo electrónico oficiales, que a menudo incluyen funciones de seguridad mejoradas, para asuntos oficiales.
- Implemente filtros en la puerta de enlace de correo electrónico para filtrar correos electrónicos con indicadores maliciosos conocidos.

SÍ/NO **¿Ha capacitado a su personal para detectar y denunciar correos electrónicos de phishing u otros correos electrónicos sospechosos?**

- Los agentes maliciosos están mejorando sus técnicas todo el tiempo, por lo que se debe brindar capacitación a intervalos regulares para educar al personal sobre las últimas tácticas y cómo responder a las comunicaciones sospechosas. Revise periódicamente los signos comunes de phishing para que el personal esté familiarizado con qué buscar y cómo denunciar.

Protéjase y responda: ataques de denegación de servicio distribuido (DDoS) dirigidos contra sus sitios web

SÍ/NO **¿Ha hablado con los proveedores de servicios del sitio web y de Internet sobre la preparación y respuesta ante un incidente DDoS?**

- Revise los contratos existentes y coordine con los proveedores de servicios del sitio web y de Internet antes de que ocurra un incidente. Comprenda las protecciones que los proveedores de servicios pueden tener ya implementadas.
- Identifique qué medidas adicionales de mitigación y redundancia de DDoS están disponibles. La mayoría de los principales proveedores de servicios tienen protecciones disponibles, que pueden ofrecerse sin costo para servicios básicos o con un costo adicional para servicios avanzados. Hay una serie de servicios de prevención de DDoS gratuitos disponibles para los funcionarios electorales que se pueden encontrar en: https://www.cisa.gov/topics/election-security/ protect-your-website.
- Asegúrese de saber a quién contactar en caso de incidente.
- Comparta información sobre fechas y lugares de elecciones importantes, solicite que se disponga de un amplio servicio de resolución de problemas durante períodos clave y garantice el conocimiento mutuo de cualquier mantenimiento planificado que pudiera afectar las operaciones electorales.
- Asegúrese de que la supervisión y el análisis del tráfico de la red estén habilitados a través de un firewall o un sistema de detección de intrusiones y que se estén revisando los registros.
- Tenga un plan alternativo para la difusión de información en caso de que su sitio web deje de funcionar. Asegúrese de probar ese plan.

Protéjase y responda: el ransomware ataca su red

SÍ/NO **¿La red electoral está segmentada de otras unidades de negocio mediante el uso de un firewall configurado para permitir únicamente comunicaciones conocidas?**

- Implemente y aplique la segmentación de red. La segmentación adecuada de la red es un mecanismo de seguridad eficaz para evitar que un intruso propague exploits o se mueva lateralmente dentro de una red interna. Esto incluye no transferir los resultados electorales a la red empresarial.

SÍ/NO **¿Se monitorea el tráfico de la red interna para detectar tráfico malicioso, mediante un software de detección y respuesta de puntos finales (EDR, por sus siglas en inglés) o un servicio similar?**

- Implemente software de EDR en dispositivos de punto final. Si es miembro del Centro de Análisis e Información de Infraestructura Electoral (EI-ISAC, por sus siglas en inglés), es elegible para obtener soluciones de EDR comerciales sin costo financiadas por la CISA.
- Verifique que se creen alertas y se siga el proceso de respuesta.

SÍ/NO **¿Su tráfico de red está protegido contra el enrutamiento a sitios maliciosos conocidos?**

- Implemente el bloqueo y la notificación de dominios maliciosos (MDBR, por sus siglas en inglés) en todos sus dispositivos de red para evitar que los sistemas de IT se conecten a dominios web dañinos. El MDBR puede bloquear la gran mayoría de las infecciones de ransomware simplemente evitando el alcance inicial a un dominio de distribución de ransomware. Los miembros del EI-ISAC son elegibles para recibir servicios comerciales de MDBR sin costo financiados por la CISA.

SÍ/NO **¿Tiene un plan de respuesta a incidentes de ciberseguridad y ha practicado su uso?**

- Desarrolle y mantenga planes de respuesta a incidentes que detallen específicamente cómo operar procesos de misión crítica en caso de un incidente de ciberseguridad.
- Pruebe sus planes de respuesta a incidentes con todos los agentes clave que estarían involucrados en la implementación de la respuesta. Puede aprovechar los recursos de la CISA, como ejercicios prácticos presenciales o virtuales, para ayudar a facilitar el evento de capacitación (https://www.cisa.gov/topics/election-security/election-security-training).

SÍ/NO **¿Mantiene copias de seguridad cifradas sin conexión de sus sistemas y datos críticos durante un mínimo de 30 días?**

- Mantenga copias de seguridad que permitan recuperar datos con un mínimo de hasta 30 días de anticipación.
- Cifre los archivos de respaldo y asegúrese de que las credenciales para acceder a las copias de seguridad no estén almacenadas en el entorno de destino. Con frecuencia, los agentes de ransomware buscan y recopilan credenciales almacenadas en el entorno atacado, y utilizan esas credenciales para intentar acceder a las soluciones de respaldo. También utilizan las vulnerabilidades públicamente disponibles para atacar las soluciones de respaldo sin correcciones.
- Asegúrese de que las copias de seguridad sean sin conexión, ya que la mayoría de los agentes de ransomware intentan encontrar y, posteriormente, eliminar o cifrar las copias de seguridad accesibles para hacer que la restauración sea imposible, a menos que se pague el rescate.

SÍ/NO **¿Ha practicado recientemente la restauración de sus copias de seguridad de datos?**

- Pruebe la disponibilidad e integridad de las copias de seguridad en un escenario de recuperación ante desastres.

Protéjase y responda: vulnerabilidades explotadas conocidas y sus sistemas conectados a Internet

SÍ/NO **¿Tiene un análisis de vulnerabilidades de higiene cibernética que identifica vulnerabilidades expuestas a Internet?**

- Regístrese para el escaneo de vulnerabilidades de higiene cibernética de la CISA o de un servicio equivalente que monitoree y analice continuamente los activos de red accesibles a Internet (direcciones IPv4 públicas y estáticas) para evaluar su estado de host y vulnerabilidad. El servicio de escaneo de vulnerabilidades de higiene cibernética de la CISA proporciona informes semanales de todos los hallazgos y alertas ad hoc sobre hallazgos urgentes, como servicios potencialmente riesgosos y vulnerabilidades explotadas conocidas.

SÍ/NO **¿Tiene un programa de gestión de parches que le permita cerrar vulnerabilidades conocidas o identificadas y errores de configuración rápidamente (15 días o menos)?**

- Desarrolle un plan de gestión de parches que (1) haga que la reducción del riesgo significativo de vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés) sea una prioridad máxima para la remediación; y (2) requiera que las vulnerabilidades críticas se remedien dentro de los 15 días calendario posteriores a la detección inicial.

RECURSOS

#Proteger2024 | CISA
cisa.gov/topics/election-security/protect2024

Recursos esenciales para funcionarios electorales estatales y locales, incluidos servicios de ciberseguridad, servicios de seguridad física y guías de mejores prácticas de seguridad.

Guía de #Detenerransomware | CISA
cisa.gov/resources-tools/resources/stopransomware-guide

Un recurso integral para ayudar a las organizaciones a reducir el riesgo de incidentes de ransomware a través de las prácticas recomendadas para detectar, prevenir, responder y recuperarse.

Sin interrupciones en las elecciones: una guía para mitigar los riesgos de denegación de servicio | CISA
cisa.gov/resources-tools/resources/no-downtime-elections-guide-mitigating-risks-denial-service

Orientación sobre cómo planificar, responder y recuperarse de ataques DDoS.

Servicios de higiene cibernética | CISA
cisa.gov/cyber-hygiene-services

Servicios gratuitos de ciberseguridad para ayudar a las organizaciones a reducir su exposición a amenazas mediante la adopción de un enfoque proactivo para monitorear y mitigar los vectores de ataque.

Bloqueo y denuncia de dominios maliciosos (MDBR) | MS-ISAC/EI-ISAC
cisecurity.org/ms-isac/services/mdbr

Una solución de seguridad web gratuita para entidades gubernamentales SLTT y que proporciona una capa adicional de protección cibernética que está probada, es efectiva y fácil de implementar.

Paquetes de ejercicios prácticos de seguridad electoral (CTEP, por sus siglas en inglés) de la CISA | CISA
cisa.gov/resources-tools/resources/election-security-cisa-tabletop-exercise-packages-cteps

Paquetes de capacitación personalizables con escenarios, preguntas para debate, referencias y recursos.

CONSEJOS RÁPIDOS SOBRE CIBERSEGURIDAD

Los funcionarios electorales y los profesionales de IT desempeñan un papel fundamental a la hora de garantizar la ciberseguridad de los sistemas críticos de los que dependen los funcionarios electorales. Estos consejos pueden mejorar la conciencia sobre la seguridad y contribuir a mejorar la higiene de la ciberseguridad.

Manténgase alerta:

- ☐ Si no espera un correo electrónico y le parece inusual, llame al remitente para asegurarse de que tenía la intención de enviarlo.
- ☐ Notifique cualquier comportamiento o actividad sospechosa a la CISA, el EI-ISAC o a la oficina local de la FBI.

Comprenda los planes de contingencia:

- ☐ Revise y actualice los planes de contingencia para ejecutar procesos electorales esenciales en caso de una interrupción en los sistemas de IT.
- ☐ Practique planes de contingencia para garantizar su eficacia.

Maneje los incidentes de seguridad de forma adecuada:

- ☐ Comuníquese con sus profesionales de IT y siga su plan de respuesta a incidentes.
- ☐ Notifique el incidente de ciberseguridad a la CISA, el EI-ISAC o a la oficina local de la FBI.

Manténgase informado:

- ☐ Manténgase actualizado sobre las alertas de seguridad, los anuncios y los cambios de procedimiento que faciliten la administración o los funcionarios electorales.
- ☐ Si es necesario, solicite aclaraciones sobre las medidas o los protocolos de seguridad.