TIEMPO DE INACTIVIDAD EN LAS ELECCIONES: GUÍA PARA LA DENEGACIÓN DE SERVICIO

PERSPECTIVA GENERAL

Esta guía ofrece pasos proactivos para que los funcionarios electorales y los proveedores de tecnología electoral reduzcan la probabilidad y el impacto de los incidentes de denegación de servicio (DoS, por sus siglas en inglés), incluyendo los ataques distribuidos de denegación de servicio (DDoS) y las interrupciones no maliciosas del servicio.

Los funcionarios electorales y sus socios en el sector privado dependen cada vez más de sitios web, aplicaciones web y otros sistemas conectados a la red para informar y proporcionar servicios a los votantes. Los sitios web y las aplicaciones web de las oficinas electorales a menudo están sujetos a grandes volúmenes de tráfico de Internet y pueden seguir siendo objetivos llamativos para los actores de amenazas cibernéticas que buscan interrumpir o socavar la confianza en las elecciones estadounidenses. Varias oficinas electorales estatales y locales experimentaron interrupciones temporales en sus sitios web como resultado de ataques DDoS e interrupciones no maliciosas del servicio durante el ciclo electoral de mitad de período de 2022.

En las elecciones, los incidentes de DoS podrían hacer que los sitios web de las oficinas electorales, las aplicaciones web u otros sistemas dependientes de Internet no tengan acceso temporalmente, lo que podría afectar la capacidad de los votantes para recibir información electoral oficial o aprovechar los servicios electorales en línea (por ejemplo, verificar el estado del registro de votantes y la información del sitio de votación, ver una boleta de muestra, solicitar una boleta por correo / para voto en ausencia, registrarse para votar, etc.). Esto podría incluir interrupciones en la disponibilidad de sistemas importantes en momentos clave del ciclo electoral, como un portal de registro de votantes en línea alrededor de la fecha límite de registro de votantes o una herramienta de búsqueda de lugares de votación el día de las elecciones. Tales interrupciones, ya sean resultado de un ataque DDoS o de interrupciones del servicio no maliciosas, también pueden brindar oportunidades para que los actores extranjeros de amenazas difundan desinformación y busquen socavar la confianza pública en las elecciones estadounidenses, por ejemplo, haciendo o amplificando afirmaciones falsas o exageradas sobre la interrupción de un sitio web electoral.

DoS y DDoS

Un incidente de **denegación de servicio (DoS, por sus siglas en inglés)** ocurre cuando los usuarios legítimos no pueden acceder a los sistemas de información, dispositivos u otros recursos en la red. Los servicios afectados pueden incluir correo electrónico, sitios web, cuentas en línea (por ejemplo, banca) u otros servicios que dependen del computadora o red afectados. Una condición DoS se logra inundando el host o la red de destino con tráfico hasta que el objetivo no pueda responder o simplemente se bloquee, lo que impide el acceso de los usuarios legítimos. Los incidentes de DoS pueden ocurrir por razones no maliciosas (por ejemplo, altos volúmenes de tráfico legítimo de Internet que causan una interrupción del sitio web) o debido a las acciones de un actor de amenazas cibernéticas.

Un incidente DoS se clasifica como un ataque de **denegación de servicio distribuido (DDoS)** cuando el tráfico de sobrecarga se origina en más de una máquina atacante que operando en conjunto. Los atacantes DDoS a menudo aprovechan un **botnet,** un grupo de dispositivos conectados a Internet secuestrados, para llevar a cabo ataques a gran escala que, desde la perspectiva de la entidad objetivo, parecen provenir de muchos atacantes diferentes.

Sistemas que pueden experimentar incidentes DoS

Servicios disponibles al público

- Sitios web de información electoral o para votantes
- Sitios web de información en la noche de las elecciones
- Servicios en línea (por ejemplo, búsqueda de información de votantes, búsqueda de sitios de votación, registro de votantes, solicitud de boleta por correo o para voto en ausencia, presentación de candidatos, etc.)

Sistemas de oficina dependientes del Internet

- Libros electorales electrónicos
- Sistemas de procesos de negocio (RRHH, contabilidad, líneas telefónicas)
- Aplicaciones de correo electrónico
- Sistemas telefónicos de voz sobre protocolo de Internet (VOIP)

INTERRUPCIONES DEL SERVICIO NO MALICIOSAS

En cada ciclo electoral, las jurisdicciones de todo el país experimentan servicio no malicioso. Estos incidentes pueden incluir ancho de banda de Internet limitado, configuraciones incorrectas u otras razones relacionadas con planificación o ejecución insuficientes. A menudo, el alto tráfico en línea puede simplemente agobiar un sistema y deshabilitarlo temporalmente. También debe tenerse en cuenta que otros incidentes no maliciosos, como un evento meteorológico o un accidente de construcción que corta una línea telefónica, cable o fibra, pueden provocar interrupciones en el sitio web o en el sistema que pueden parecer, pero no ser realmente, ataques DDoS.

Cuando IT es importante

Las fechas y eventos importantes en el calendario electoral generan un mayor tráfico en los sitios web electorales y los servicios en línea. El aumento del tráfico puede causar interrupciones del servicio si las jurisdicciones no están correctamente preparadas. Las fechas y eventos importantes a tener en cuenta incluyen:

- Día Nacional de Registro de Votantes
- Campañas de registro de votantes, campañas y plazos
- Plazos de solicitud de boletas por correo/para voto en ausencia
- Fechas de votación anticipadas en persona
- Día de las elecciones durante las horas de votación
- Informes de resultados

PREPÁRESE PARA INCIDENTES DE DOS

Los funcionarios electorales y los proveedores de tecnología electoral pueden tomar medidas proactivas para reducir la probabilidad y el impacto de los incidentes de DoS.

Coordinar con los proveedores de servicios

Un primer paso clave para mitigar el riesgo asociado con posibles incidentes de DoS es que los funcionarios electorales revisen los contratos existentes y coordinen tanto con los proveedores de servicios de sitios web como con los proveedores de servicios de Internet antes de que ocurra un incidente. Esto garantiza que los funcionarios electorales sepan a quién contactar en caso de un incidente y comprendan las protecciones que sus proveedores de servicios pueden ya tener implementadas.

A continuación, los funcionarios electorales deben identificar qué medidas adicionales de mitigación y redundancia de DoS están disponibles. La mayoría de los principales proveedores de servicios tienen protecciones disponibles, que pueden ofrecerse sin costo para servicios básicos o a un costo adicional para servicios avanzados. El Kit de herramientas de ciberseguridad y recursos para proteger las elecciones de CISA incluye una lista de herramientas, servicios y recursos sin costo proporcionados por CISA, miembros de la Colaboración Conjunta de Defensa Cibernética (JCDC) de CISA y otros en toda la comunidad de ciberseguridad que los funcionarios electorales pueden usar para protegerse contra incidentes DoS.

Por último, los funcionarios electorales también deben coordinar de antemano con todos los proveedores de servicios (proveedores de servicios de sitios web, proveedores de servicios de Internet y proveedores de servicios de protección DoS) para compartir información sobre fechas y lugares importantes de las elecciones, solicitando que haya una amplia solución de problemas disponible durante los períodos clave y asegurando el conocimiento mutuo de cualquier mantenimiento planificado que pueda afectar las operaciones electorales.

Monitorear sitios y actividad

El mejor mecanismo para detectar e identificar un incidente DoS es monitorear y analizar el tráfico en la red. El tráfico en la red se puede monitorear a través de un firewall o un sistema de detección de intrusos. Un administrador puede incluso configurar reglas que creen una alerta al detectar una carga de tráfico anómala e identificar la fuente del tráfico o los paquetes de red descartados que cumplan ciertos criterios.

Los funcionarios electorales deben comprometerse con sus proveedores de servicios para comprender mejor qué actividades ya monitorean y cómo se ve el tráfico "normal" en sus sitios web. Además de coordinar con los proveedores de servicios, hay ciertos indicadores que los funcionarios electorales pueden buscar directamente en sus propios sistemas, lo que puede indicar un posible incidente de DoS. Como se mencionó anteriormente, la capacidad de identificar con éxito la actividad inusual, inesperada o anormal depende de la comprensión de cómo se ve la línea de base "normal" para cada sistema o servicio.

Estos indicadores pueden incluir:

- Rendimiento de red inusualmente lento (lento al abrir archivos o acceder a sitios web)
- Indisponibilidad de un sitio web en particular
- Imposibilidad de acceder a cualquier sitio web
- Rendimiento lento de las aplicaciones
- Utilización inesperadamente alta del procesador y la memoria
- Tráfico de red inusualmente alto

PREPÁRESE PARA RESPONDER A UN INCIDENTE DE DOS

Los procesos resilientes son críticos para el éxito de las operaciones electorales, para incluir las operaciones cibernéticas. Esto significa tener recursos y protocolos de respuesta a incidentes cibernéticos organizacionales y planes de comunicaciones que incluyan respuesta y mitigación del impacto de los incidentes de DoS.

Identificar del problema

Si los funcionarios electorales estiman que un posible incidente de DoS está ocurriendo, deben **comunicarse con su administrador de red** para confirmar si la interrupción se debe al mantenimiento o a un problema interno de la red. Los administradores de red también pueden supervisar el tráfico de red para confirmar un incidente, identificar el origen y mitigar la situación mediante la aplicación de reglas de firewall y, posiblemente, el redireccionamiento del tráfico a través de un servicio de protección DoS.

Después de comunicarse con el administrador de la red, es posible que los funcionarios electorales deban **comunicarse con el proveedor de servicios** de su sitio web para preguntar si hay una interrupción en su extremo o incluso si su red es el objetivo del ataque y el sitio web es una víctima indirecta. En este caso, los proveedores de servicios del sitio web pueden asesorar acerca del curso de acción apropiado. Si la interrupción del servicio sucede dentro de un período electoral crítico o puede tomar algún tiempo para remediarla, los funcionarios electorales deben **estar preparados para promulgar planes de continuidad** para implementar alternativas u opciones de respaldo hasta que los servicios regulares puedan ser restaurados a un nivel aceptable.

En el caso de un ataque, los funcionarios electorales no deben perder de vista a otros hosts, activos o servicios que residen en la red. Los atacantes pueden realizar ataques DDoS para desviar la atención de su objetivo primordial y aprovechar la oportunidad para realizar ataques secundarios en otros servicios dentro de la red.

CISA recomienda que los funcionarios electorales y los proveedores de tecnología electoral informen de inmediato los presuntos ataques cibernéticos a:

- CISA, al report@cisa.gov o al (888) 282-0870
- El FBI, a través de la oficina local del FBI
- El EI-ISAC, en SOC@cisecurity.org o 866-787-4722
- Otras autoridades estatales o locales, según corresponda a la jurisdicción

Tener métodos alternativos listos para usar para compartir información

Las operaciones electorales exitosas tienen que ver con la resiliencia. Esto significa tener recursos y planes de contingencia practicados que aborden la mitigación de incidentes DoS.

Las oficinas electorales que experimentan un incidente de DoS pueden verse impedidas para comunicar información al público, con otras oficinas electorales e incluso con otras oficinas en el mismo edificio. Mucho antes de cada elección, los funcionarios electorales deben preparar métodos alternativos para difundir información electoral, incluidos los resultados electorales no oficiales, en caso de que un incidente de DoS haga que los sitios web u otras aplicaciones no estén disponibles. Esto se puede lograr de múltiples maneras. Las jurisdicciones estatales o locales pueden alojar un sitio web de respaldo en una infraestructura completamente separada del sitio web principal, lo que también puede beneficiar a las oficinas durante los períodos de mantenimiento o actualización. Las oficinas electorales con sitios web

de informes de la noche de las elecciones también pueden considerar cargar un PDF de los resultados en su sitio web principal y otros sitios web en su red estatal o local. Finalmente, se recomienda a las oficinas electorales establezcan relaciones con los medios de comunicación que pudiesen ayudar a transmitir información, como información correcta sobre el lugar de votación o resultados electorales no oficiales, en caso de un incidente.

Desarrollar un plan interno de comunicaciones para incidentes DoS

Paralelamente a la planificación de la respuesta a incidentes, los funcionarios electorales deben incorporar tanto los ataques DDoS como las interrupciones no maliciosas del servicio en su plan de comunicaciones. Los planes de comunicación deben identificar un equipo de comunicaciones de crisis (incluidos los miembros de los equipos de TI y comunicaciones), definir roles y responsabilidades y establecer procedimientos para mantener los canales de comunicación durante un incidente. El equipo de comunicaciones de crisis debe estar preparado para mantener las comunicaciones sin acceso a la red de la oficina principal o teléfonos móviles. Los funcionarios electorales también pueden considerar desarrollar una lista de términos y definiciones clave relacionados con incidentes de DoS para uso de todo el personal.

Los funcionarios electorales también deben considerar preparar declaraciones de retención que puedan adaptarse y usarse según sea necesario durante un incidente de DoS. Las declaraciones de retención no solo deben proporcionarse al personal superior y a los funcionarios de comunicaciones, sino también al personal de primera línea que responde a las llamadas y recibe preguntas del público y los medios de comunicación.

PLANIFIQUE Y CAPACITE PARA INCIDENTES DE DOS

Como se destacó anteriormente, los funcionarios electorales deben incluir escenarios de incidentes DoS en sus planes de respuesta y recuperación de incidentes. Los planes deben guiar a la organización en la identificación, mitigación y recuperación rápida de tales incidentes, así como en el mantenimiento de comunicaciones efectivas durante la respuesta y recuperación de incidentes. La Guía de Planificación de Notificaciones y Detección de Incidentes Cibernéticos de CISA para Seguridad Electoral puede ser útil para desarrollar el plan de respuesta a incidentes en la organización.

Los planes de respuesta a los incidentes de DoS, al igual que con otros incidentes cibernéticos, deben designar roles y responsabilidades para todas las partes interesadas, incluidos los líderes organizacionales y los proveedores de servicios. Como mínimo, el plan debe describir los procedimientos para confirmar el incidente, comprender la naturaleza del incidente, implementar mitigaciones, monitorear efectividad y recuperación.

La planificación de incidentes de DoS también debe considerar la continuidad de procesos y los procedimientos de recuperación ante desastres, especialmente si los canales de comunicación interna se ven afectados por dicha interrupción (por ejemplo, un sistema telefónico de voz sobre protocolo de Internet inaccesible). El liderazgo organizacional debe estar familiarizado con los canales de comunicación alternativos o de respaldo para comunicarse con el personal, los proveedores de servicios o los votantes de manera rápida y efectiva, como árboles telefónicos, correos electrónicos alternativos o sistemas de notificación de emergencia.

Después de un incidente, una vez que se han restablecido los servicios, los funcionarios electorales deben realizar un informe del incidente para discutir las lecciones aprendidas de la implementación del plan de respuesta a incidentes y el plan de comunicaciones, y actualizar los procedimientos a partir de ello.

Finalmente, todo el personal debe estar capacitado y practicar regularmente la respuesta a incidentes. Los funcionarios electorales pueden considerar incluir incidentes de DoS en ejercicios de mesa u otros entrenamientos basados en escenarios. La práctica rutinaria es fundamental para garantizar que todas las personas comprendan sus roles y responsabilidades durante un incidente, ayuden a identificar brechas en el plan de respuesta, permitan a las partes interesadas practicar la urgencia y la cadencia de un evento real y generen confianza tanto en el plan como en las medidas de mitigación implementadas. El recurso Elections Cyber Tabletop in a Box de CISA incluye un ataque DDoS como parte del escenario del ejercicio. Los asesores regionales de ciberseguridad (CSA) de CISA también están disponibles para proporcionar evaluaciones y recursos de protección, incluida la orientación de gestión de riesgos sobre incidentes DoS.

RECURSOS ADICIONALES

La información proporcionada en esta guía no exhaustiva se complementa con recursos adicionales vinculados a lo largo del documento y a continuación. Se alienta a los funcionarios electorales y a los proveedores de tecnología electoral a revisar estos recursos para prepararse aún más y mitigar los riesgos asociados con posibles incidentes de DoS.

- CISA FBI MS-ISAC Understanding and Responding to Distributed Denial-of-Service Attacks
- CISA Understanding Denial-of-Service Attacks
- CISA Cybersecurity Toolkit and Resources to Protect Elections
- CISA Distributed Denial-of-Service (DDoS) Quick Guide
- CISA Cyber Incident Detection and Notification Planning Guide for Election Security
- CISA Elections Cyber Tabletop in a Box
- Election Infrastructure Joint GCC-SCC Managing Mis/Disinformation Working Group Mis-, Dis-, and Malinformation (MDM) Planning and Incident Response Guide
- CISA Capacity Enhancement Guide: Volumetric DDoS Against Web Services Technical Guidance