GOBIERNO DE LA
REPÚBLICA DOMINICANA

Gobierno gestiona efectivamente ataque cibernético

El incidente impactó a 14 sitios web del Estado dominicano y fue solucionado por la OGTIC y el CSIRT-RD, del Centro Nacional de Ciberseguridad.

Santo Domingo, 6 de febrero de 2022. La Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) y el Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT-RD), del Centro Nacional de Ciberseguridad (CNCS), informaron sobre un ataque cibernético realizado a varios portales gubernamentales, los cuales fueron afectados por un incidente conocido técnicamente como "Defacement", el cual fue auto adjudicado por el grupo de hackers denominado Hunter Bajwa Pakistan Zindabad. Dicho ataque ocurrió el domingo 6 de febrero de 2022, impactando en la portada principal de 14 portales institucionales informativos, de un total de 46 que comparten la misma infraestructura de alojamiento.

Este ataque de tipo "Defacement", o desconfiguración de la estructura web, es un ataque menor que consiste en el aprovechamiento de vulnerabilidades no identificadas en los manejadores de contenido para cambiar la apariencia de un portal web determinado con el propósito de llamar la atención por parte de quien lo realiza.

El incidente fue mitigado por el equipo del departamento de seguridad de la información de la Oficina Gubernamental de Tecnología de la Información y Comunicación (OGTIC), en coordinación con el Equipo Nacional de Respuesta a Incidente Cibernéticos (CSIRT-RD) del Centro Nacional de Ciberseguridad, quienes informaron que esta clase de ataques son superficiales, cuyo riesgo por lo general es bajo desde la perspectiva operacional ya que por diseño, los portales institucionales desarrollados y gestionados afectados únicamente ofrecen informaciones a la ciudadanía y la población en general y se encuentran aislados de los sistemas de información, plataformas y aplicaciones críticas para el funcionamiento de las instituciones públicas, conforme a lo estipulado en las normas y estándares técnicos impulsados por la OGTIC, conforme las buenas prácticas y metodologías para el diseño, desarrollo y administración de servicios y aplicaciones digitales, por lo que el mismo no generó daños ni pérdida de datos e información crítica para el correcto desempeño de la labor institucional.

Como plan de acción ante esta situación, los equipos técnicos de las instituciones involucradas activaron el plan y los protocolos de respuesta y recuperación de incidentes cibernéticos y de continuidad de las operaciones para restablecer el funcionamiento de los portales web en el menor tiempo posible, el cual fue logrado en tiempo record.

Así mismo, informaron que tras recuperar la disponibilidad de los servicios, ambos equipos de respuesta, establecieron nuevos controles para prevenir futuros incidentes de este tipo, salvaguardando la disponibilidad, confidencialidad e integridad de los datos e informaciones alojados en las instalaciones del Datacenter del Estado. Según informaciones ofrecidas, este ataque no afectó ningún servicio crítico, servicios transaccionales gubernamentales ni las operaciones de los servicios institucionales.