Instituto Dominicano de las Telecomunicaciones

INF-I-000002-21

Informe sobre la necesidad de adquisición de Firewall de Nueva Generación
Solución de Seguridad Perimetral UTM (Unified threat management)

Santo Domingo, R.D.
15 e febrero 2021

El día 11 de enero de 2021, el **INDOTEL** fue objeto de un bloqueo de acceso a su servidor de dominio activo, el cual afectó la operatividad de la institución. Ante el evento suscitado, el **INDOTEL** solicitó al **Departamento Nacional de Investigaciones (DNI)** una investigación y auditoría forense informática a los fines de determinar las causas de lo ocurrido y obtener las recomendaciones técnicas de un organismo autorizado a dicho fines. Posteriormente, el día 26 de enero de 2021, el **DNI** notificó al **INDOTEL** un Informe contentivo de la *investigación y recomendaciones, por bloqueo de acceso al servidor de dominio activo (active directory)*, concluyendo de la manera siguiente:

> "[...] b.- Le recomendamos de manera **URGENTE!!!**,, el cambio de los equipos perimetrales de seguridad informática, que cumplan con los estándares y regulaciones internacionales, debido a que dentro del análisis preliminar, se han detectado ataques persistentes a la infraestructura de la institución."

Posteriormente, el Consejo Directivo del **INDOTEL**, basándose en lo crítico del caso y en el informe pericial elaborado por el **DNI**, el 4 de febrero de 2021 aprobó la Resolución núm. 007-2021 declaró de urgencia la adquisición de una "Solución de Seguridad Perimetral UTM" para el reforzamiento de la seguridad informática del **INDOTEL**.

Es importante resaltar que el referido informe de acuerdo a su contenido y a la naturaleza del **DNI**, el cual es un organismo de seguridad nacional del Estado, está clasificado confidencial. Todo esto, en virtud de lo dispuesto en la Ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones en su artículo 2, Párrafo IV, establece lo siguiente:

Párrafo IV.- Toda la información relacionada con el objeto de la presente ley será de libre acceso al público de conformidad con lo establecido en la Ley General de Libre Acceso a la Información Pública de la República. **Con excepción de las que se refieran a los asuntos de seguridad nacional.** (El resaltado es nuestro)

En tal virtud, el presente informe técnico elaborado por la Dirección de Tecnología de la Información y Comunicación (TIC) contiene información complementaria al proceso de urgencia, la cual puede ser conocida y publicada, en aras de no afectar los Principios de Transparencia y publicidad.

Instituto Dominicano de las Telecomunicaciones

INF-I-000002-21

Debido a los últimos acontecimientos que se han experimentado en el **INDOTEL** y demás instituciones del Estado, además de las condiciones actuales de la infraestructura tecnológica de nuestra institución, estamos recomendando al igual que el DNI que se adquieran de forma urgente los equipos necesarios para fortalecer la seguridad de las redes del INDOTEL. La seguridad de la red es un problema cada vez más prioritario, la mejora en las redes es necesaria y un Firewall de Nueva Generación es una pieza clave. Los firewalls tradicionales se limitan a la inspección de paquetes por estado y a reglas de control de acceso, pero a medida que los ataques se hacen más sofisticados, las amenazas son más avanzadas y este sistema ha dejado de ser eficaz.

Con el fin de proteger al Estado de amenazas en constante evolución, el Firewall de Nueva Generación **(Unified threat management (UTM))** es capaz de ofrecer un nivel más profundo de seguridad de red. Para ello, la clave es garantizar la inspección de todos los bytes de cada paquete, pero esto ha de conseguirse manteniendo el rendimiento elevado y la baja latencia para que la redes con mucho tráfico sigan funcionando de forma óptima. Además de combatir amenazas de forma eficaz y abordar problemas de productividad cada vez más acuciantes, el Estado requiere un nivel más profundo de seguridad y control. Para ello necesitamos firewalls de nueva generación que contengan al menos:

- Control de aplicaciones basado en contexto: La popularidad de las aplicaciones basadas en acceso de red se ha disparado en los diez últimos años, lo que ha complicado a los administradores la tarea de supervisar la actividad de los usuarios y el uso del tráfico por parte de las aplicaciones.
- Mantenerse informado de todas esas amenazas gracias al uso de bases de datos en la nube que se actualicen constantemente es fundamental para bloquear las nuevas amenazas en cuanto aparecen.
- Control y mantener el uso apropiado de internet en toda la institución.
- Prevenir cualquier actividad sospechosa de los equipos conectado a la red.

Finalmente, el propósito de la declaratoria de urgencia es adquirir una solución de seguridad que permita brindar protección y visibilidad en todos los segmentos de red, tanto en redes físicas como virtuales del INDOTEL, evitando acciones deliberadas contra las mismas.

Preparado por:

Juan P. Noboa
Director
Dirección de Tecnología de Información