REUNA
Ciencia y Educación en Red

UC DESARROLLA SOLUCIÓN CON EDUSCAN PARA MEJORAR LA SEGURIDAD DE SU RED INTERNA

Desafío

Los encargados técnicos de cada facultad necesitan conocer en detalle las vulnerabilidades de sus sistemas y redes, para corregirlas.

Solución

La UC desarrolló un sistema para extraer la información de los reportes de eduSCAN y visualizar los resultados en Kibana.

Beneficio

eduSCAN junto con esta herramienta son muy eficaces para hacer una gestión detallada y así evitar que se produzcan incidentes de seguridad.

eduSCAN es el servicio de escaneo de vulnerabilidades de REUNA, que tiene como objetivo ayudar a las áreas de TI a robustecer sus sistemas de seguridad informática. Para ello, proporciona diversos análisis, que permiten identificar potenciales amenazas, tanto dentro como fuera de la infraestructura de la institución, entregando una visión del nivel de vulnerabilidad en múltiples escenarios. Adicionalmente, suministra pautas para el tratamiento y la corrección de las vulnerabilidades detectadas.

Con este servicio a su disposición, en la Dirección de Informática de la Pontificia Universidad Católica de Chile (UC) se propusieron implementar un sistema que les permitiera realizar análisis a la infraestructura de cada facultad de manera centralizada, para luego extraer la información y visualizar los resultados en Kibana. “Nos dimos cuenta de que la instalación local de Nessus usa una API, que podemos usar Python y, en nuestro caso, ya contábamos con Elasticsearch/ Logstash/Kibana, entonces el flujo de ir a meter los datos ahí fue relativamente sencillo. Lo que sí requiere tiempo es conocer la estructura de datos, de la información que Nessus entrega a través de la API y ver cómo organizar esos resultados a la medida, de acuerdo a lo que nosotros necesitamos. Además, teníamos que implementar control de acceso por grupos o facultades”, explicó Andrés Altamirano, jefe del Área de Seguridad UC.

El resultado es un dashboard al que el responsable de cada facultad puede ingresar con su propia cuenta, donde es posible visualizar las vulnerabilidades detectadas (con los detalles de la detección y posible solución entregada por Nessus en el reporte), los dispositivos afectados, el tipo de detección y el registro de los análisis ejecutados a la fecha, entre otros.

A nivel técnico, la arquitectura del desarrollo es la siguiente: “El servidor Nessus dispone de una API y construimos un extractor en Python, que usa esta API Key y hace un pull de la información, recorriendo los escaneos que se han hecho en las últimas 48 horas. Todos los registros se envían a Syslog. Tenemos un servicio central que corre en un clúster, donde recibimos los logs de los equipos de comunicaciones, servidores, aplicaciones, etc. como un gran storage, donde se guarda todo eso. Y esos registros los leemos con Logstash, que es parte Elasticsearch, y que nos sirve para normalizar la data y eventualmente enriquecerla, si es necesario, con otro flujo de datos. Posteriormente, se indexa en el clúster de datos de Elasticsearch propiamente tal, lo cual deja los datos disponibles, para que luego en Kibana los podamos ver en un dashboard, más fácil de leer”, detalló el profesional.

Finalmente, Altamirano aseguró que eduSCAN, junto esta herramienta, les ha sido muy útil para hacer una gestión más detallada y realizar un seguimiento en las facultades, con el objetivo de evitar que se produzcan problemas de seguridad que afecten la red local y, eventualmente, se extiendan a la red de toda la universidad.

Para más información, ingresa a **https://noc.reuna.cl/eduscan/**

ANDRÉS ALTAMIRANO
Jefe del Área de Seguridad UC