A comienzos de esta semana, ServiceNow hizo público en su sitio de soporte que configuraciones incorrectas en su plataforma podrían derivar en *«acceso no intencionado»* a información sensible. Para las organizaciones que emplean ServiceNow, esta vulnerabilidad de seguridad se convierte en una preocupación de máxima relevancia, ya que podría haber desencadenado una fuga significativa de datos corporativos delicados. ServiceNow ha tomado acciones para solventar este problema.

Este artículo efectúa un análisis exhaustivo del inconveniente, explicando por qué esta configuración crítica en la aplicación podría haber tenido graves repercusiones para las empresas y sugiere pasos de corrección que las compañías podrían haber adoptado de no haber sido por la solución implementada por ServiceNow. (Aunque se recomienda verificar que la corrección haya efectivamente eliminado la exposición de la organización).

¿Qué es ServiceNow?

ServiceNow es una plataforma basada en la nube utilizada para automatizar la gestión de servicios de TI, la administración de operaciones de TI y la gestión de operaciones de negocios de TI, que incluyen el servicio al cliente, recursos humanos, operaciones de seguridad y una amplia gama de otros dominios. Esta aplicación como servicio (SaaS) se considera una de las aplicaciones críticas para las empresas debido a su naturaleza infraestructural, su capacidad de expansión como plataforma de desarrollo y su acceso a datos confidenciales y propietarios en toda la organización.

Simple List es un elemento de interfaz que extrae datos almacenados en tablas y los emplea en cuadros de mando. La configuración predeterminada de Simple List permite que los datos en las tablas sean accesibles de forma remota por usuarios no autenticados. Estas tablas incluyen datos sensibles, como el contenido de los tickets de TI, bases de conocimientos clasificadas internas, información de empleados y mucho más.

Estas configuraciones incorrectas han estado presentes desde la implementación de las Listas de Control de Acceso en 2015. Hasta la fecha, no se han reportado incidentes relacionados. Sin embargo, dada la reciente publicación de la investigación sobre la filtración

de datos, no resolver este problema habría podido exponer a las empresas más que nunca.

Esta exposición fue el resultado de una única configuración predeterminada, y existen cientos de configuraciones que abarcan el control de acceso, la prevención de fugas de datos, la protección contra malware y otros aspectos que deben ser protegidos y mantenidos. Las organizaciones que emplean una solución de Gestión de la Postura de Seguridad de SaaS (SSPM), como Adaptive Shield, pueden identificar de manera más sencilla configuraciones incorrectas de alto riesgo y verificar si cumplen o no con los estándares (consulte la imagen 1 a continuación).

Configuraciones Incorrectas de ServiceNow

Es importante recalcar que este problema no se originó en una vulnerabilidad del código de ServiceNow, sino en una configuración existente en la plataforma.

Este inconveniente tiene su origen en los controles de seguridad de un elemento de Lista de Control de Acceso de ServiceNow (ACL) llamado Simple List, que organiza registros en tablas de fácil lectura. Estas tablas organizan información procedente de diversas fuentes y cuentan con configuraciones que permiten el acceso público de manera predeterminada.

Debido a que estas tablas son la columna vertebral de ServiceNow, el problema no se limitaba a una sola configuración que pudiera corregirse de forma aislada. Era necesario aplicar correcciones en múltiples ubicaciones dentro de la aplicación, en combinación con el uso del elemento de interfaz de usuario, y en todos los inquilinos. Añadiendo mayor complejidad al asunto, modificar una sola configuración podía afectar negativamente a flujos de trabajo existentes relacionados con las tablas de Simple List, lo que desencadenaría una interrupción significativa en los procesos en curso.

Pasos para la Solución

Tal como lo detalla ServiceNow en su artículo de conocimiento en su base de datos titulado «*Información General | Posible Configuración Errónea del Widget Público*«, la evaluación de la

exposición y las acciones correctivas recomendadas son las siguientes:

1. Examinar las Listas de Control de Acceso (ACL) que estén en blanco por completo o que, en su lugar, incluyan la función «Público».
2. Evaluar los widgets públicos y desactivar la opción «Público» cuando no sea coherente con los casos de uso.
3. Contemplar la implementación de medidas de control de acceso más rigurosas mediante los controles incorporados que ServiceNow ofrece, como el Control de Acceso por Dirección IP o la Autenticación Adaptativa.
4. Valorar la instalación del Complemento de Roles Explícitos de ServiceNow. Según ServiceNow, este complemento previene que usuarios externos accedan a datos internos, y las instancias que utilizan este complemento no se ven afectadas por este problema (el complemento garantiza que cada ACL establezca al menos un requisito de rol).

Estos pasos recomendados para la corrección aún pueden ser útiles para organizaciones que sigan expuestas (incluso después de la solución), ya que es importante realizar una revisión adicional para asegurar la máxima seguridad en toda la organización.

Automatizar la Prevención de Fugas de Datos en ServiceNow

Las organizaciones que emplean una solución de Gestión de la Postura de Seguridad de Aplicaciones SaaS (SSPM), como Adaptive Shield, tienen la capacidad de obtener visibilidad en las configuraciones de ServiceNow y cualquier otra aplicación SaaS, así como de aplicar medidas correctivas a problemas de configuración.

Los SSPM alertan a los equipos de seguridad cuando existen configuraciones de alto riesgo, permitiéndoles ajustar dichas configuraciones y prevenir cualquier tipo de fuga de datos. De esta forma, las empresas obtienen una comprensión más precisa de la superficie de ataque de su organización, el nivel de riesgo y su postura en materia de seguridad al utilizar un

SSPM.