Garantía de cumplimiento de los sistemas de información con la normativa actual

Implantación de software para conseguir la máxima seguridad de TI y cumplir con la regulación vigente

_betasystems

Libro blanco

Introducción

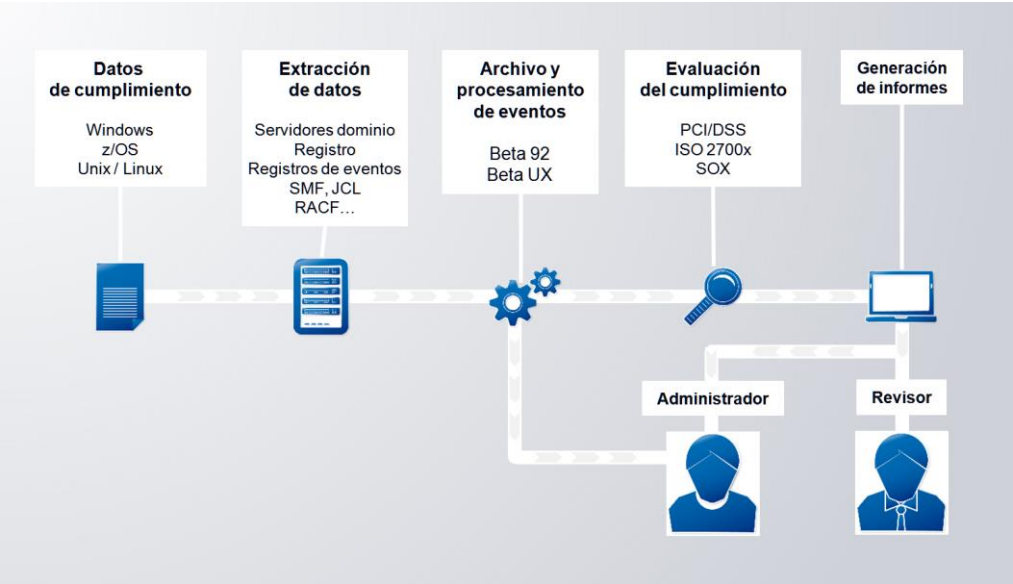
En Europa, el 39 % de los profesionales que toman decisiones en materia de TI creen que hay usuarios no autorizados que acceden a sus servicios de información (*Data Security Confidence Index,* 2014). Es obvio que las nuevas tecnologías están cambiando radicalmente la visión convencional de los sistemas de información empresariales. Nunca había habido tantas amenazas contra la seguridad de los sistemas de TI de las empresas, y las personas encargadas de su protección pocas veces se han sentido tan mal equipados para llevar a cabo su trabajo.

Al mismo tiempo, el creciente número de regulaciones y obligaciones legales (Basilea III, ley Sarbanes-Oxley, etc.) obligan a las empresas a implantar un exhaustivo sistema de administración de la seguridad de TI, y a comprobar perpetuamente que sus sistemas cumplan con estas obligaciones regulatorias. Las empresas también tienen que informar de estas comprobaciones mediante auditorías de TI.

Estas regulaciones toman diferentes formas, bien sea a través de normas ISO internacionales (27001) o bien a través de normativas y directivas industriales que cubren necesidades de seguridad específicas. Este es el caso de la norma PCI-DSS para la industria de las tarjetas de pago, y que tiene como objetivo mantener la confidencialidad y seguridad de las operaciones bancarias. La Oficina federal alemana para la seguridad de la información (BSI), así como la Agencia Nacional de Protección de Datos española ANPD también emiten directivas y procedimientos regulatorios muy estrictos destinados a garantizar la seguridad de los sistemas de información.

Por último, las empresas pueden hacer uso de manuales para la aplicación de los métodos más recomendables, como el ITIL 2011 y el Cobit 5. Dentro de estos marcos de trabajo, las empresas pueden llevar a cabo su administración de TI, destinada a adecuar sus mecanismos organizativos a sus sistemas de TI con el fin de proveer servicios TI eficientes y seguros, que cumplan con regulaciones vigentes.

Reorganización del entorno de TI



Análisis de datos multiplataforma para el cumplimiento de objetivos de auditoría

Estos cambios deben permitir la supervisión dinámica en tiempo real de los sistemas empresariales, y garantizar, al mismo tiempo, que puedan comprobarse y auditarse periódicamente. Tales funciones de supervisión —que pueden requerir el procesamiento en tiempo real o el registro histórico continuo de

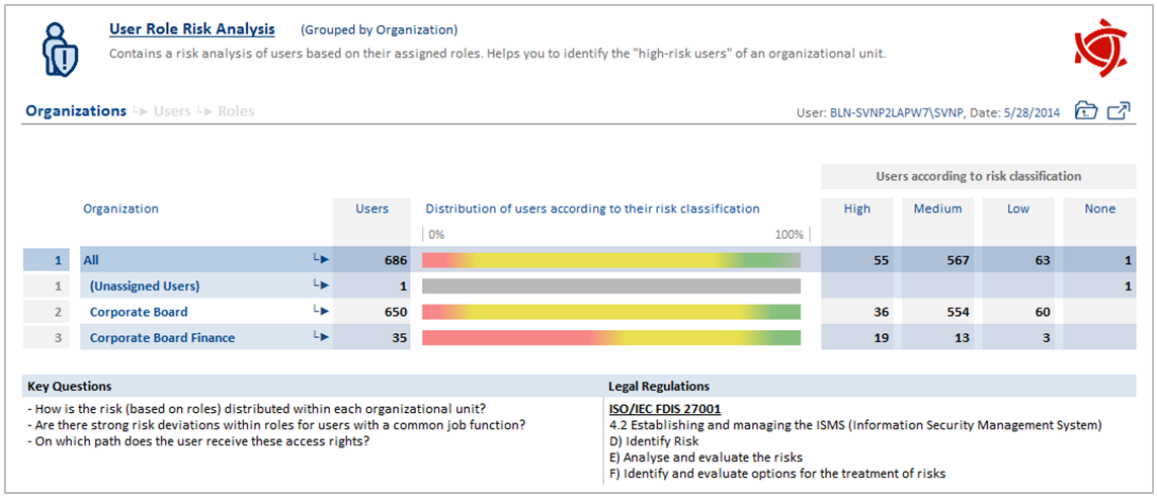
datos en los casos más extremos— deberán suplementar las comprobaciones necesarias del acceso a los recursos de TI e identidades de usuario.

Para disponer de una cobertura completa, resulta fundamental que los datos de todos los sistemas y aplicaciones —ya sean mainframe o distribuidos— se recopilen constantemente y se archiven en un único lugar para luego analizarlos y compilarlos en informes que se enviarán automáticamente a los gerentes.

Para cumplir de manera más sencilla con la norma ISO 2700X, las empresas harán uso de una solución que dispone de pruebas de seguridad y procedimientos dinámicos de auditoría ajustados a los requisitos de la norma. También pueden definirse los procedimientos de comprobación y auditoría personalizados con el fin de aplicar las políticas y procedimientos internos de una compañía.

Detección de los riesgos de accesos

Las empresas procurarán garantizar la mejor protección de sus datos y recursos de TI contra intrusiones no autorizadas y potencialmente peligrosas. Con las soluciones de análisis de accesos pueden asegurarse de que todos los datos relacionados con el acceso (usuarios, roles, permisos del sistema, etc.) queden registrados y documentados. Haciendo uso de informes dinámicos y una interfaz gráfica mejorada para permitir la manipulación de datos, el análisis inteligente de los accesos de los usuarios posibilita la identificación de posibles puntos débiles y del nivel de riesgo asociado. Debe incluirse un gran número de informes típicos. Estos paneles también pueden personalizarse para obtener el nivel de detalle que se necesite, basándose en el uso que hagan de ellos los auditores internos, los responsables de seguridad de TI o los altos directivos. Por último, es importante que la solución disponga de funciones de registro dinámico del historial de datos, de manera que cualquier cambio realizado en el pasado o en tiempo real, se pueda identificar, rastrear y consultar con mucha facilidad.



Representación de los potenciales niveles de riesgo relacionados con usuarios.

La supervisión dinámica

Los procedimientos de control integrados dentro del sistema de administración de accesos simplificarán la generación de informes de auditoría. También en este caso, a las empresas les resultará más sencillo garantizar el cumplimiento normativo de los sistemas de acceso si la solución permite la realización de auditorías descentralizadas por parte de auditores no especializados en TI. Estos instrumentos de apoyo a la auditoría son especialmente prácticos para aquellas empresas que necesiten hacer informes periódicos de los controles y las auditorías realizadas.

Sin embargo, según la normativa vigente (concretamente, la ISO 2700x), las empresas también están obligadas a aplicar sistemas de supervisión dinámica de la seguridad de TI. Por tanto, los departamentos de TI deben supervisar la configuración y los eventos de seguridad en tiempo real, registrando y analizando los datos de SMF. De este modo, pueden enviarse automáticamente advertencias de seguridad a los destinatarios predeterminados en caso de que se produzca cualquier infracción.

Una administración de la seguridad simplificada

Para que la supervisión del acceso sea eficiente, los departamentos de TI de las empresas deben poder administrar las identidades y derechos de acceso usando una única interfaz que les permita tener una visión global. Para reforzar la seguridad, las identidades y los permisos de acceso al sistema serán cruzados automáticamente. Cuando hay un gran número de usuarios, la administración centralizada de los accesos resulta más complicada para los administradores de TI. En estos casos, las empresas pueden delegar ciertas tareas de administración en los responsables de equipos; por ejemplo, la aprobación de solicitudes de acceso y la recertificación de derechos de acceso ya existentes, con el consiguiente ahorro de tiempo y la mejora de la eficiencia. En tales circunstancias, es fundamental que la solución cuente con una interfaz para web o Windows que facilite el manejo y el tiempo de aprendizaje.

Conclusión

Garantizar que los sistemas de información cumplan las normativas vigentes es un proceso complejo pero necesario. Para llevar a cabo este proceso, las empresas deben dar prioridad a los sistemas de administración de accesos diseñados para adecuarse exactamente a las normas y marcos correspondientes, y que, además, faciliten las auditorías y ofrezcan el máximo nivel de seguridad.

Beta Systems brinda asistencia y orientación a más de 1300 clientes en todo el mundo en materia de seguridad para sus procedimientos de TI, de modo que puedan cumplir los requisitos de administración, gestión de riesgos y cumplimiento normativo (GRC). Beta Systems cuenta con 20 años de experiencia en el ámbito IAM (Identity Access Management), lo que le permite ofrecer una amplia gama de software para la administración de accesos a recursos de TI basados en identidades y roles de usuarios.

Garancy Access Intelligence Manager es un sistema de inteligencia empresarial que ofrece análisis de auditoría y asistencia que puede emplearse para comprobar el cumplimiento de los derechos de acceso otorgados a los usuarios, así como para evaluar los riesgos de acceso al sistema mediante informes estándar y personalizados.

SAM Business Process Workflow facilita la gestión de los flujos de peticiones y autorizaciones automatizando la certificación y recertificación de los usuarios y de sus derechos de acceso. Esta solución hace posible, por tanto, la aplicación de reglas de administración de TI.

SAM Enterprise Identity Manager es un sistema de aprovisionamiento de gran alcance con conectores para más de 50 sistemas de destino que pueden emplearse para gestionar identidades y accesos a recursos en todas las plataformas y aplicaciones.

Beta 96 Compliance Auditor ofrece una auditoría dinámica y multiplataforma de sistemas de información con el fin de detectar y analizar los eventos críticos y comprobar la seguridad de los sistemas de TI. La solución dispone de comprobaciones de seguridad y de procedimientos de auditoría que cumplen con la norma ISO 2700x.

Información sobre Beta Systems

Beta Systems es una empresa de desarrollo de software líder en la Gestión de los Centros de Proceso de Datos y de la Seguridad Informática de las empresas. Desde hace más de 30 años, nuestros productos demuestran diariamente su gran calidad en el tratamiento eficaz, seguro y fiable de grandes cantidades de datos.

Beta Systems permite a sus clientes automatizar y asegurar sus procedimientos de tratamiento de datos y su gobernanza empresarial basada en la identidad y los accesos de los usuarios. Más de 1300 clientes de todo el mundo se apoyan en nuestras soluciones para garantizar la seguridad de sus procesos IT y responder a las exigencias en el campo de gobernanza, gestión de riesgos y cumplimiento de normativas (GRC). Nuestros clientes son grandes empresas líderes en sectores como Banca y Seguros, Finanzas, Industria, Transporte, Seguridad.

La compañía tiene su sede en Berlín y comercializa sus productos internacionalmente a través de sus 14 filiales y de su red de socios distribuidores. Beta Systems está presente en España con su propia filial local desde 1998.

Vea más información en www.betasystems.es.

Contacto

marketing-f@betasystems.com

+34 9 13 07 76 75

Libro blanco – Marso de 2015
Beta Systems Software España, S.L.