HTTPS en todas partes: tendencias de la industria y la necesidad del encriptado

Michael Rodriguez

Serials review, ISSN 1879-095X, Vol. 44, n. 2, 2018, p. 131-137

La privacidad y confidencialidad del usuario es un valor fundamental a cargo del bibliotecario. La capacidad de las personas para buscar información sin miedo a la interferencia o vigilancia de terceros es vital para la libertad intelectual y la democracia. Las bibliotecas deberían implementar Protocolos de Transferencia de Hipertexto Seguros (HTTPS) en todas las web gestionadas o utilizadas por ellas. HTTPS encripta los datos durante su transmisión a través de Internet. Esto significa que la actividad en línea es privada entre los navegadores y los servidores que lo solicitan y también valida la integridad de los datos, lo que significa que los delincuentes no pueden acceder a conexiones no encriptadas para buscar contraseñas, manipular los datos en tránsito, introducir códigos maliciosos o redireccionar el tráfico a sitios web falsos que se hacen pasar por legítimos. Es solo el primer paso para garantizar la privacidad y seguridad. Los delincuentes todavía pueden conocer qué sitios web visitan los usuarios, pero si esos sitios web están utilizando HTTPS, las terceras partes no pueden ver qué páginas web específicas ven los usuarios o que enlaces pinchan. No impide que los sitios web capturen datos sobre los visitantes, ni tampoco evitan a los proveedores de servicios de monitoreo de tráfico web. El encriptado HTTPS se ha mantenido en gran medida fuera del radar de los bibliotecarios que gestionan recursos electrónicos, publicaciones seriadas, metadatos, y colecciones en general. En este estudio podremos comprobar los beneficios de utilizar esta aplicación, así como sus tendencias industriales, bibliotecarias y de los proveedores, además del riesgo de violación de datos y la propia implementación del servicio. Los lectores de esta revista probablemente trabajen en aspectos técnicos, no en tecnología de la información *per se*. Manejan recursos electrónicos y publicaciones seriadas, recursos de catálogo, bases de conocimiento, servicios de descubrimiento y negocian contratos con proveedores. Por lo tanto, están bien situados para abogar por la encriptación y garantizar la privacidad del usuario, además de la seguridad de datos y redes. Junto a los servicios técnicos bibliotecarios, pueden auditar a los proveedores para la implementación de HTTPS y mejores prácticas, responsabilizar a los proveedores de las vulnerabilidades de los datos y los incumplimientos y plasmar estas exigencias en los contratos. Tener esta protección en todas partes es una necesidad para proteger la privacidad del usuario y crear espacios seguros en línea, reflejando los valores fundamentales de la labor bibliotecaria.

Resumen realizado por José María Amate Sánchez

Amate Sánchez