DOMPDF_ENABLE_REMOTE is set to FALSE
file_get_contents(/var/www/html/mincom/sites/all/themes/mincom/logo.png): failed to open stream: No such file or directory

DOMPDF_ENABLE_REMOTE is set to FALSE
file_get_contents(/var/www/html/mincom/sites/default/files/styles/large/public/ciberseguridad_2_hi.jpg): failed to open stream: No such file or directory

Proteger las aplicaciones críticas, una cuestión de negocio

Source:
computerworld

El 58% de las organizaciones ya ha sufrido durante los dos últimos años pérdidas de información, problemas de integridad o interrupciones del servicio que afectan a sus aplicaciones.

La ciberseguridad muta a velocidades de vértigo. Y, en consecuencia, las estrategias de las empresas deben estar en continuo reciclaje y prestar siempre atención a las nuevas tendencias, procesos y tecnologías para contar con una protección efectiva de sus negocios. En definitiva, la ciberseguridad se ha convertido en un elemento transversal, quizá el más importante, de toda compañía que se haga llamar digital. Para disfrutar de la explotación de los datos o de las bondades del comercio online, por ejemplo, es necesario tener buenos sistemas de detección, prevención y respuesta ante amenazas, asegurar la disponibilidad y contar con el talento técnico imprescindible.

Pero, decíamos, el primer imperativo es saber en qué paradigma estamos, conocer qué es lo que hay que defender y cómo. Ya no nos movemos en un entorno en el que la mayoría de los datos de las empresas se encuentran físicamente en las instalaciones y solo tenían que hacer hincapié en la seguridad de la red y los dispositivos, basándose en un perímetro sólido. Pero el perímetro se ha difuminado y los atacantes pueden entrar a las compañías mediante cualquier vector. Una de esas puertas de entrada la conforman las aplicaciones críticas, muchas de ellas ya en la nube. Más si tenemos en cuenta que en España no se está dando la prioridad necesaria a su seguridad. Según un estudio de Cyberark, el 73% de las empresas locales no le da la importancia suficiente a este aspecto. Una estadística que choca con los casos reales de uso porque más de la mitad de los encuestados reconoce que incluso el menor tiempo de inactividad que afecte a estas herramientas puede suponer graves impactos en el negocio. Además, el 58% de las organizaciones ya ha sufrido durante los dos últimos años pérdidas de información, problemas de integridad o interrupciones del servicio que afectan a sus aplicaciones. A pesar de ello, un 75% de los encuestados piensa que puede detener de manera eficaz los ataques a la seguridad de los datos o infracciones en el perímetro. Los números son peligrosos si tenemos en cuenta que desde los sistemas bancarios, el I+D, hasta el servicio al usuario y la cadena de suministro se ejecutan con aplicaciones críticas.

Obviamente, lo que se considera crítico puede variar en función del sector industrial y de cada empresa: desde Office 365 hasta los sistemas de planificación de recursos empresariales (los llamados ERP). En cualquier caso, explican desde Cyberark, su alteración influye inmediatamente en los resultados económicos y la pérdida de datos comprometidos comporta riesgos comerciales y fiscales permanentes. Por ejemplo, el coste medio de un ataque a un sistema ERP oscila en torno a los 5,5 millones de dólares. O, una alteración en un software de gestión con el cliente (CRM, de sus siglas inglesas) puede afectar a la continuidad de los procesos de ventas y fidelización de clientes.

Cómo proteger las aplicaciones críticas

Para poder cimentar una estrategia de defensa efectiva, lo primero que hay que tener en cuenta es de dónde vienen los ataques. El 80% de las filtraciones de datos guarda relación con credenciales privilegiadas comprometidas, como contraseñas, tokens, claves y certificados, según la consultora Forrester. Por ello, proteger las aplicaciones comerciales críticas significa que el acceso debe estar reservado a personas o máquinas con las credenciales y permisos adecuados. Este tipo de herramientas ahora operan en entornos locales, en la nube y a través de aplicaciones SaaS y, en muchas ocasiones, mediante una combinación de las tres. En este contexto, hay una gran variedad de usuarios privilegiados que requieren acceso: empleados que trabajan tanto en instalaciones como en puntos finales remotos, socios externos o proveedores y desarrolladores que introducen cambios en dichas aplicaciones. Por otra parte, las credenciales privilegiadas

también están integradas en las interacciones máquina a máquina. De este modo, hay que administrar y rastrear de manera efectiva los accesos sin desequilibrar los presupuestos. Pero, ¿cómo operar eficientemente en este paradigma tan complejo? Desde Cyberark han desgranado cinco claves.

La primera es identificar qué aplicaciones son verdaderamente críticas para la empresa. El responsable de ciberseguridad debe saber las funciones clave de finanzas, marketing y recursos humanos. Así, estará mejor posicionado para identificar las aplicaciones comerciales más relevantes para su negocio. En segundo lugar, y en un mundo en el que el término cloud es más que una tendencia, familiarizarse con la nube y protegerla es un imperativo. El Ciso debe entender cuál es su estrategia en este ámbito, su plan de migración y lo que se está desplazando hacia la nube. Asociarse con los interlocutores multifuncionales para garantizar que la seguridad de acceso privilegiado es una consideración prioritaria a la hora de migrar aplicaciones a la nube o de adoptar nuevas.

Asimismo, hay que proteger el acceso de los administradores que gestionan las aplicaciones comerciales críticas. Es necesario almacenar y rotar todas las contraseñas relacionadas con estas aplicaciones, incluida la infraestructura subyacente. También es necesario realizar un seguimiento de auditoría completo de todas las actividades privilegiadas que involucren a estas herramientas. Por supuesto, no hay que olvidarse de las máquinas. El uso de credenciales de codificación fija comporta un riesgo de seguridad importante y debería erradicarse.

Por último, se vuelve imprescindible limitar el riesgo derivado de las estaciones de trabajo de usuarios finales no administradas. Para ello, hay que eliminar los derechos de administrador local para evitar la descarga de virus. Hay que invertir también en protección contra el phishing y en formación y concienciación para que los usuarios sean capaces de reconocer este tipo de amenazas.

Disponible en:

https://cso.computerworld.es/tendencias/proteger-las-aplicaciones-critic... [1]

Links
[1] https://cso.computerworld.es/tendencias/proteger-las-aplicaciones-criticas-una-cuestion-de-negocio