NOTA DE PRENSA
13 / 08 / 2020

Los secretos industriales en el punto de mira de los ciberataques

> El principal actor detrás de una fuga de información es, en un 93% de los casos, un atacante que viene del exterior con la intención de sustraer datos, o bien un proveedor, un partner o un tercero que mantiene relaciones comerciales con la empresa atacada

El sector industrial, que cuenta en Europa con más de 2.000 compañías especializadas en fabricación y da trabajo a más de 30 millones de persona de forma directa, es especialmente prolífico en cuanto a generación de patentes e I+D, y esto hace que exista un gran volumen de secretos industriales susceptibles de ser robados.

Para poder reducir e, incluso, atajar este problema, lo primero que debemos saber es cómo se produce la fuga de información crítica en las organizaciones. Según Forrester en su Global Business Technographics Security Survey, que analiza las formas más habituales de fuga de información de los últimos 12 meses, el 28% de dichas fugas ocurre mediante ataques externos dirigidos a las corporaciones, y el 19% surge por incidentes internos en un partner o proveedor externo que trabaja con la compañía. Por tanto, si nos fijamos en cómo se dan las fugas de datos en las empresas, vemos que una buena parte viene originada a través de terceros provocando que nuestra información pueda quedar desprotegida, a pesar de que dentro de nuestra organización hayamos puesto medidas para securizar nuestro entorno de trabajo.

Según el “Data Breach Investigations Report” publicado por Verizon, en el sector de fabricación/industria el principal actor detrás de una fuga de información es, en un 93% de los casos, un atacante que viene del exterior con la intención de sustraer datos, o bien un proveedor, un partner o un tercero (que mantiene relaciones comerciales con la empresa atacada) motivado por razones de espionaje en un 94% de los casos. De hecho, el tipo de datos más comúnmente robado en este sector –llegando a suponer el 91% de los datos sustraídos– son los asociados a la Propiedad Intelectual y

los secretos industriales.

Pensemos que se trata de un sector complejo donde las empresas colaboran con una amplia variedad de proveedores y clientes, y la propiedad intelectual tiene que viajar fuera de la empresa. Podemos tener visibilidad sobre lo que sucede con los datos dentro de la organización, pero esto es mucho más complicado cuando se necesita trazar los accesos a nuestra información o protegerla a lo largo de toda la cadena de suministro.

Las fugas en el ámbito del propiedad intelectual están más de actualidad que nunca con acusaciones entre diferentes países de robos de propiedad intelectual. Según se indica en este artículo de Forbes, para el gobierno de los Estados Unidos, el robo de propiedad intelectual estadounidense cuesta entre 225 y 600 millones de dólares anuales, y parte de esto se deriva de ciberataques. Hemos visto también como en las últimas semanas se ha generado una enorme polémica a nivel global por el posible intento de robo de propiedad intelectual derivada de las investigaciones de las vacunas para el Covid-19, donde directamente USA, UK y Canadá apuntan a hackers rusos.

Proteger la propiedad intelectual contenida en formato digital, incluyendo ficheros CAD

Los avances en los procesos de fabricación y redes industriales están suponiendo una gran transformación del sector industrial, hasta el punto de que ha surgido el concepto de Industria 4.0. La base de la nueva Industria Inteligente implica una profunda automatización de las fábricas, digitalización de los procesos de producción y nuevos canales de comunicación. Esto incrementa la posibilidad de ataques dirigidos a la información crítica de las empresas, dado que antes los datos circulaban sólo dentro del “perímetro” de seguridad de la red, y ahora tienen que ser compartidos con diferentes sistemas y actores externos.

En este contexto, resulta crítico poder proteger la propiedad intelectual contenida en formato digital tanto dentro como fuera de la organización. La información sensible se encuentra en diferentes formatos, desde documentación en formato Word, Excel o PDF, imágenes y por supuesto, diseños de CAD. Una buena parte de la propiedad intelectual se encuentra en diseños de CAD 2D y 3D que es necesario compartir tanto internamente como con colaboradores externos. Es crítico mantener esta información protegida para evitar riesgos de fuga por amenazas internas o externas.

¿Qué tipo de información del ámbito industrial está en riesgo?

En empresas de fabricación, energía, automoción o ingeniería, por ejemplo, los datos gestionados que deben ser protegidos son de muchas clases: desde documentación de soporte con detalles de piezas, componentes que deben ser intercambiados con clientes, proveedores o partners de fabricación;

pasando por resultados de investigaciones susceptibles de ser patentadas, que almacenamos en todo tipo de formatos digitales (o diseños de CAD; hasta datos de precios que tienen que intercambiarse con distribuidores en diferentes mercados, propuestas que se hacen a clientes donde se compite con otras empresas y que contienen información sensible; guías de calidad internas relacionadas con procesos de producción de la compañía y donde se recoge el know-how a nivel de procesos; o cumplimiento de auditorías y políticas de protección de sus clientes.

¿Qué podemos hacer para proteger nuestros diseños CAD y datos más sensibles?

SealPath, empresa especializada en la protección y control de información sensible, va más allá de la protección de información en formatos ofimáticos y acaba de lanzar una serie de actualizaciones en sus soluciones de protección de diseños de CAD, permitiendo a sus clientes securizar:

- Diseños CAD en formato .DWG, .DWF, DWS, .DWF, o .DWT, gestionados en **AutoDesk AutoCAD** (Electrical Mechanical, Civil, LT, etc.) o en aplicaciones como TrueView.
- Diseños 3D de **AutoDesk Inventor** en formato .IPT, .IAM, .IDW, .DWG o .IPN de forma que puedas limitar los permisos sobre el contenido (Ej. ver y modificar pero no extraer datos).
- Propiedad Intelectual contenida en **Siemens Solid Edge** en formatos .ASM, .DFT, .PAR, .PSM o .PWD controlando si alguien puede imprimirla, exportarla modificarla auditando todos los accesos.

Además, SealPath recomienda actuar realizando seis pasos para proteger la propiedad intelectual y ficheros CAD de una organización a través de toda la cadena de suministro:

- **Proteger la información con propiedad intelectual que se envía por email a los colaboradores:** Una de las principales formas de compartir datos sigue siendo el email. Enviamos continuamente adjuntos con información sensible a subcontratas, partners y terceros; debemos aplicar reglas en los emails y adjuntos que nos permiten controlar quién accede, cuándo, con qué permisos (ejemplo, dejar sólo ver, editar, pero no copiar y pegar o imprimir, etc.) nos ayudará a tener controlados nuestros datos, aunque estén en manos del destinatario.
- **Proteger diseños de CAD y documentación en repositorios de información:** En toda empresa se guarda documentación sensible en repositorios como Servidores de Ficheros, SharePoint, OneDrive, Box, Office 365, etc.; aunque se apliquen controles de acceso a la carpeta, sabemos que una vez descargados hemos perdido el control sobre ellos. Es necesario disponer de una protección que viaje con los datos de forma que, aunque se hayan descargado, pueda seguir teniendo el control sobre ellos de la misma forma que lo tengo cuando están en el repositorio.
- **Proteger los datos corporativos sensibles que comparto vía aplicaciones de trabajo colaborativo como Slack o Microsoft Team:** Es una vía de comunicación alternativa al email y

cada vez más extendida para una comunicación intra-empresarial. Muchos ficheros sensibles salen de nuestros repositorios a nuestras plataformas, por lo que no debemos olvidarnos de aplicarles protección también cuando viajan por estos medios.

- **Protección de ficheros descargados desde aplicaciones corporativas:** Existen multitud de aplicaciones desarrolladas internamente en las corporaciones que permiten exportar o descargar datos en formato fichero. Aplicar protección justo en el momento que se descarga el fichero ayudará a que podamos tener control sobre el mismo allí donde viaje.
- **Auditar accesos sobre la información:** Cuando se trata de nuestros ficheros en formato CAD o documentos muy sensibles es importante ver quién está accediendo, con qué permisos, en qué momento o si alguien intenta acceder sin tener permisos. Esta información bien gestionada puede avisarnos de posibles fugas de información.
- **Bloquear/Revocar el acceso a la información en caso de que alguien no deba seguir teniendo acceso:** Si he dejado de colaborar con una subcontrata, un partner, ¿Por qué debe poder seguir accediendo a mi información? Se deben utilizar mecanismos que permitan “destruir” o eliminar los documentos que estos exsocios tienen en su poder.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net