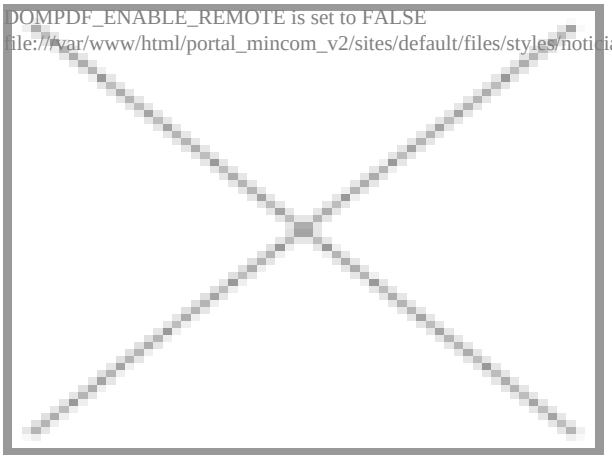

Source:
ComputerWorld

El Laboratorio Europeo de Física de Partículas Elementales constituye una de las principales instituciones científicas a nivel global. Asegurarla frente a los riesgos en TI es un desafío en constante evolución. "La ciberseguridad es inconveniente. Afrontémoslo", reconoce a COMPUTERWORLD Stefan Lüders, CISO del CERN.

Pocas instituciones de investigación hay en el mundo con las dimensiones y el calado de la Organización Europea p?ara la Investigación Nuclear, el CERN. Fundado en 1954 por doce países europeos, el Laboratorio Europeo de Física de Partículas Elementales se localiza en el municipio suizo de Meyrin, en el cantón de Ginebra, aunque sus instalaciones se extienden a lo largo de la frontera franco-suiza. Entre ellas está el Gran Colisionador de Hadrones (LHC), el acelerador de partículas más grande del mundo. La colaboración internacional está en la base de su origen: más de 3.500 personas componen su plantilla fija. Una pequeña villa que se expande a 17.000 habitantes cuando se suma el personal científico de alrededor de 950 instituciones de más de 80 países distintos que colabora en proyectos del centro —o que lo hizo en 2024—. En este ecosistema propio, la gestión del riesgo de TI supone un reto a la altura de la institución.

"El principal problema es que estamos gestionando una organización enorme", explica Stefan Lüders, CISO del CERN. "Somos uno de los institutos de investigación de física de partículas más importantes del planeta. Hacemos cosas sofisticadas e interesantes, lo que nos convierte en blanco de ataques de diferentes comunidades", resume. Enumera varias de estas potenciales amenazas: script kiddies o hackers con un conocimiento básico, que suponen así y todo un riesgo potencial de seguridad; ransomware o exfiltración de datos; sabotajes al trabajo del CERN; acciones de espionaje y de grupos criminales que intentan infiltrarse a través de ordenadores o dispositivos.

“Aquí es donde entra la gente. Porque tenemos una comunidad de investigadores muy amplia, heterogénea y muy fluctuante. Hay muchos físicos que se unen a la organización cada año. Entran y salen para hacer su doctorado, investigan en el CERN y luego se van”, describe, apuntando al desafío de “cuidar a esta comunidad de usuarios. El otro desafío es el mundo flexible y de rápido desarrollo de las TI”. Añade también la programación —la importación de bibliotecas de código abierto, su seguridad, etc.— y la IA. “Cuanto más sofisticada se vuelve la IA, mayor es la probabilidad de que esas herramientas de seguridad o ataque impulsadas por la IA intenten infiltrarse en la organización”.

Asegurando el CERN

Con esta situación de partida, ¿cómo se asegura una implementación efectiva de las iniciativas en ciberseguridad, que no interrumpan el trabajo científico? “No puedes”, afirma Lüders. “La ciberseguridad es inconveniente. Afrontémoslo”. Lüders lo equipara a cerrar con llave la puerta de casa o utilizar el PIN para sacar dinero del cajero; pueden ser molesto, pero necesario. “Intentamos explicar a nuestra comunidad por qué se necesitan medidas de seguridad”, señala. “Y si adaptamos nuestras medidas de seguridad a nuestro entorno, la gente las adopta. Sí, hace la investigación algo más complicada, pero solo un poco”.

Lüders insiste en el factor del trabajo en investigación. “No somos un banco. No tenemos billones de dólares. No somos una base militar, lo que significa que no debemos proteger a un país. Investigamos, lo que implica adaptar el nivel de seguridad y el de libertad académica para que ambos vayan de la mano. Y esa es una conversación constante con nuestra comunidad de usuarios”. Esta engloba desde el personal científico al de gestión de sistemas de control industrial, el departamento de TI o recursos humanos. “Para afrontar ese reto, es fundamental hablar con la gente. Por eso, insisto, la ciberseguridad es un tema muy sociológico: hablar con la gente, explicarles por qué hacemos esto”. Por ejemplo, no todo el mundo usa de buen grado los sistemas multifactor porque “admitámoslo, son un fastidio. Es mucho más fácil escribir una contraseña e, incluso, ¿quién quiere escribir una contraseña? Solo quieres entrar. Pero para las necesidades de protección, hoy en día tenemos contraseñas y autenticación multifactor. Así que le explicas a la gente qué estás protegiendo. Les decimos por qué es importante proteger su trabajo, al igual que los resultados de la investigación. Y la gran mayoría entiende que se necesita un cierto nivel de seguridad”, asegura. “Pero es un desafío porque aquí conviven muchas culturas diferentes, nacionalidades diferentes, opiniones y pensamientos diferentes, y orígenes diversos. Esto es lo que intentamos adaptar permanentemente”.

Se suma a la conversación Tim Bell, líder de la sección de gobernanza, riesgo y cumplimiento de TI del CERN, quien se encarga de la continuidad del negocio y la recuperación ante desastres. Bell introduce el problema del empleo de tecnología propia. “Si eres visitante de una universidad, querrás traer tu portátil y usarlo en el CERN. No podemos permitirnos retirar estos dispositivos electrónicos al llegar a las instalaciones. Sería incompatible con la naturaleza de la organización. Esto implica que debemos ser capaces de implementar medidas de seguridad del tipo BYOD”.

Porque en el núcleo de todo se mantiene siempre el carácter colaborativo del CERN. “Los trabajos académicos, la ciencia abierta, la libertad de investigación, son parte de nuestro centro. La ciberseguridad necesita adaptarse a esto”, constata Lüders. “Tenemos 200.000 dispositivos en nuestra red que son BYOD”. ¿Cómo se aplica entonces la adaptación de la ciberprotección? “Se llama defensa en profundidad”, explica el CISO. “No podemos instalar nada en estos dispositivos finales porque no nos pertenecen, (…) pero tenemos

monitorización de red". De este modo, y aunque no se tenga acceso directo a cada aparato, se advierte cuándo se está realizando algo en contra de las políticas del centro, tanto a nivel de ciberseguridad como de usos no apropiados, como por ejemplo emplear la tecnología que proveen para intereses particulares.

Estas medidas se extienden, además, a sistemas obsoletos, que la organización es capaz de asimilar porque cuentan con una red lo suficientemente resistente como para que, aunque un equipo se vea comprometido, no dañe ningún otro sistema del CERN. El problema de la tecnología heredada se extiende al equipo necesario para los experimentos de física que se realizan en el centro. "Estos están protegidos por redes dedicadas, lo que permite que la protección de la red se active y los proteja contra cualquier tipo de abuso", explica Lüders. Sobre los dispositivos conectados IoT no diseñados con la ciberseguridad en mente, "un problema para todas las industrias", Lüders es tajante: "Nunca se conseguirá seguridad en los dispositivos IoT". Su solución pasa por conectarlos a segmentos de red restringidos donde no se les permite comunicarse con nada más, y luego definir destinos a los que sí comunicarse.

Marco general

Esto es parte de un reto mayor: alinear la parte de TI y la de OT, de tal forma que se establezca una continuidad en la seguridad en toda la organización. Un reto que pasa por la centralización. "Hoy en día la parte de OT, los sistemas de controles del CERN, están empleando virtualización de TI", explica Lüders. "La estrategia es reunir a la gente de TI y la de control, de tal modo que la gente de control pueda usar los servicios TI en su beneficio". Desde el departamento tecnológico se provee con un sistema central con distintas funcionalidades para operaciones, así como por otras áreas de la organización, accesible a través de un único punto de entrada. "Ese es el poder de la centralización". En este sistema entran, además, nuevas herramientas como las de IA en LLM, en el que tienen en funcionamiento un grupo de trabajo para buscar la mejor manera de emplearlas. "Nos enfrentamos a un gran descubrimiento y, más adelante, lo centralizaremos mediante un servicio central de TI. Y así es como lo hacemos con todas las tecnologías".

Igual que las materias que investigan en el CERN van evolucionando, así lo hace su marco de gobernanza de TI. Este ha ido siguiendo las novedades del sector, explica Bell, de la mano de auditorías que permiten funcionar según las mejores prácticas. "La parte de la gobernanza está volviéndose más formal. En general, todo estaba bien organizado; solo se trataba de estandarizarlo y desarrollar marcos de políticas a su alrededor". Pese al establecimiento de estos estándares, el resultado es lo contrario de rígido, explica Bell, quien lo ejemplifica con el caso de una auditoría reciente de ciberseguridad en la que el CERN fue evaluado según uno de los estándares internacionales, lo que sirvió para mejorar el nivel de madurez. "Estamos adoptando una política de gobernanza de TI bastante flexible, aprendiendo de la experiencia de otros en la adopción de estándares del sector", concluye.

Disponible en:

https://www.computerworld.es/article/4081251/cern-como-gestiona-el-riesg... [1]

Links
[1] https://www.computerworld.es/article/4081251/cern-como-gestiona-el-riesgo-una-institucion-de-

investigacion-internacional.html