

Baja la ciberdelincuencia pero empeora la seguridad de impresoras y PLC

Empresa | 23/06/2023



GironaNotícies.com[®]

En el periodo enero-marzo, el número de casos disminuyó un 30% con respecto al trimestre anterior. Sin embargo, aumentó el riesgo de las impresoras conectadas a la red y los controladores lógicos programables (PLC). El robo de datos sigue siendo el principal daño causado por los piratas informáticos

2023 se estrena con un descenso general de las ciberamenazas respecto a periodos anteriores, pero aumenta el riesgo de los dispositivos como impresoras y controladores lógicos programables (PLC) expuestos en la red y mal protegidos.

Así se desprende del nuevo 'Threat Intelligence Report' elaborado por el Observatorio de Ciberseguridad de Exprivia, que tiene en cuenta 35 fuentes abiertas entre las que se incluyen sitios de empresas afectadas, sitios públicos de interés nacional, agencias de noticias online, blogs y redes sociales.

Según el informe elaborado por el grupo ICT de Apulia, los fenómenos de ciberdelincuencia cayeron un 30% entre enero y marzo en España, con 105 casos frente a los 150 del último trimestre del año pasado, y con el mes de enero, por sí solo, registrando el mayor número de casos (39).

En comparación con el mismo periodo de 2022, los incidentes de seguridad se han reducido incluso más de la mitad (-64%), sin embargo, los ataques han aumentado un 155% y las violaciones de la privacidad se han incrementado en torno al 5%. En concreto, en los tres primeros meses del año se produjeron 51 ataques, 14 incidentes de seguridad -es decir, ataques exitosos- y 40 violaciones de la privacidad.

“Es cierto que el número de incidentes detectados, en comparación con el pasado, es mucho menor, hasta el punto de que no registramos un número tan bajo de incidentes desde septiembre de 2021”, comenta Domenico Raguseo, Director de Ciberseguridad de Exprivia. “Sin embargo, no debemos acostumbrarnos a la ciberdelincuencia, especialmente a medida que aumenta el número de dispositivos conectados a la red. Al mismo tiempo, aumenta el riesgo de incurrir en amenazas que interrumpan servicios críticos, como los relacionados con el mundo sanitario”.

El informe muestra cómo ha aumentado hasta un 9% el número de dispositivos IoT conectados en red en España (más de cinco millones) que son más susceptibles de ser atacados por hackers.

Además, ha empeorado la seguridad de impresoras y controladores lógicos programables (PLC), es decir, ordenadores especializados en la gestión de procesos industriales, según el índice de evaluación elaborado por el Observatorio Exprivia.

El nivel de seguridad de los servicios en red, cada vez más vulnerables debido al aumento de las actividades digitales y los pagos en línea, también empeora: los atacantes comprometen su disponibilidad, provocando la ineficacia de los sistemas.

Según los expertos del Observatorio de Ciberseguridad de Exprivia, que apuesta por fomentar la cultura de la ciberseguridad también a través de cursos de formación, el sector más atacado por los agresores en el primer trimestre del año fue el de Software/Hardware (empresas TIC, servicios digitales, plataformas de comercio electrónico, dispositivos y sistemas operativos) con 31 casos. En segundo lugar se situaron Otros (por ejemplo, individuos), con 23 casos, y en tercer lugar, con 12 fenómenos, el sector Múltiple. Le siguen Finanzas y Administración Pública, con 9 y 6 fenómenos respectivamente.

También en el primer trimestre del año, el robo de datos encabezó la lista de los principales tipos de daños causados por los piratas informáticos, representando el 46% del número total de casos (48 de un total de 105 sucesos); una cifra, sin embargo, un 59% inferior a la de la encuesta anterior (117). El robo de datos consiste en el almacenamiento o transferencia ilegal de información personal, financiera o de propiedad, como contraseñas, códigos de software, algoritmos y procesos, causando graves consecuencias para las personas u organizaciones afectadas. Ex aequo, en segundo lugar, se sitúa el daño a la privacidad (divulgación de datos por terceros sin el consentimiento del interesado), con un 37% de los casos, y la exigencia de dinero, con cerca de un 10%; seguidos de la interrupción del servicio (3%), es decir, la detención del funcionamiento normal de la red, de una aplicación o de un servicio informático.

Entre los tipos de ataques, sobresalen las vulnerabilidades conocidas, con el 38% del total de casos (40 fenómenos frente a los 10 del trimestre anterior); también caen los ataques de malware, en segundo lugar, con 35 casos frente a los 65 registrados entre octubre y diciembre de 2022. Según el informe, la ciberdelincuencia sigue siendo la principal amenaza para la seguridad de la red en España, con un 61% de los casos (64) del total. Le siguen las violaciones de datos (brechas de seguridad que implican la destrucción, pérdida, modificación, acceso o divulgación no autorizada de datos personales) con un 38% de los sucesos detectados.

Exprivia

Exprivia es un grupo internacional especializado en Tecnología de la Información y Comunicación capaz de abordar los motores del cambio empresarial de sus clientes a través de las tecnologías digitales.

Con un know-how consolidado y una dilatada experiencia dada por una presencia constante en el mercado, el grupo cuenta con un equipo de expertos especializados en diferentes ámbitos y dominios tecnológicos, desde Capital Market, Credit & Risk Management a IT Governance, de BPO a Cybersecurity, de Big Data a Cloud, de IoT a Mobile, de networking a colaboración empresarial al mundo SAP. El grupo da soporte a sus clientes en los sectores de Banking&Finance, Telco&Media, Energy&Utilities, Aerospace&Defence, Manufacturing&Distribution, Healthcare y Public Sector. La oferta incluye soluciones compuestas por productos propios y de terceros, servicios de ingeniería y consultoría.

En la actualidad, el grupo cuenta con unos 2.400 profesionales distribuidos en 7 países de todo el mundo. Exprivia S.p.A. cotiza en la Bolsa italiana, en el mercado Euronext Milán (XPR).

La empresa está sujeta a la dirección y coordinación de Abaco Innovazione S.p.A.

Autor: Redacción