InnoTec colabora con el CCN-CERT en la protección de las AAPP y empresas estratégicas españolas

Tags: Seguridad Ciberseguridad

También te puede interesar:

- ENISE abordará la colaboración pública-privada en ciberseguridad
- Comienza el Mes Europeo de la Ciberseguridad (ECSM)

En los nueve primeros meses del año, InnoTec ha trabajado sobre más de 10.000 incidentes de los cuales cerca de 1.200 fueron catalogados como una criticidad de entre muy alto y crítico.

CSO España

InnoTec System, división de ciberseguridad del Grupo Entelgy, acaba de anunciar que colabora, de manera activa, con el CCN-CERT, del Centro Criptológico Nacional en la detección proactiva, protección y contención de las ciberamenazas sufridas por las **Administraciones Públicas y empresas de interés estratégico para España.**

Es más, y tal y como destaca en un comunicado, en los nueve primeros meses del año, se ha trabajado sobre más de 10.000 incidentes (frente a los 6.000 detectados en el mismo periodo del año anterior), de los cuales cerca de 1.200 fueron catalogados con una criticidad de entre muy alto y crítico.

"El Ciberespionaje y el robo de propiedad intelectual constituyen sin duda una de las principales amenazas detectadas, que buscan particularmente información relevante y sensible, con alto valor estratégico, económico o político con fines de lucro o mejora competitiva para el atacante. De hecho,

dirigidos contra objetivos cada vez más sofisticadamente seleccionados", destaca InnoTec Systems en un comunicado.

La colaboración de **InnoTec con el CERT Gubernamental Nacional** se centra principalmente en el Servicio de Alerta Temprana (SAT) de internet, destinado a la detección rápida de incidentes y anomalías con el fin de realizar acciones preventivas, correctivas y de contención. Su principal función, por tanto, es actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Adicionalmente, la firma está desarrollando para el CCN-CERT una herramienta ad-hoc denominada MARTA (Motor de Análisis Remoto de Troyanos Avanzados) cuya función principal es el análisis automático de malware con el que hacer frente a las nuevas variantes de ataques, así como a las novedosas formas de infección que sufren las organizaciones.