La Gaceta de Salamanca
Salamanca
04/10/18
Prensa: Diaria
Tirada: 11.943 Ejemplares
Difusión: 9.734 Ejemplares
Cód: 120917005
Página: 12
Sección: LOCAL Valor: 3.053,00 € Área (cm2): 642,1 Ocupación: 70,02 % Documento: 1/1 Autor: C.A.S. | SALAMANCA Núm. Lectores: 101000

"Los cibercriminales chequean 24 horas las puertas virtuales que dejamos abiertas"

Recreaciones para chantajear y acceder a información, y modificaciones de proyectos de arquitectura e innovación, dos de los delitos que preocupan al Centro de Ciberseguridad

C.A.S. | SALAMANCA

"Si vas por la calle y alguien te pide la tarjeta de crédito, no se la das. ¿Por qué entonces por qué se da tan a ligera cuando una página de internet o un email pide tu número de tarjeta de crédito?". El general Arturo Espejo, jefe de los Servicios Técnicos de la Guardia Civil que ayer inauguró la Jornada de Ciberseguridad en el Paraninfo de la Universidad de Salamanca, advierte: "No estamos concienciados". La sociedad está totalmente expuesta a sufrir un ataque de ciberdelincuentes. "Si dejas la puerta de tu casa abierta, igual nadie se da cuenta, pero si dejas abiertas las puertas y ventanas virtuales de tu ordenador, teléfono o negocio, fuera los malos están permanentemente chequeando. Todas las vulnerabilidades se publican en un portal de internet así como la forma de atacar", señala y por eso recomienda a las pymes, autónomos y particulares "hacer al menos dos copias de seguridad en dos discos duros externos grandes, y ubicarlos en un lugar seguro".

Enrique Ávila, director del Centro Nacional de Excelencia en Ciberseguridad (CNEC), reconoce que en España "nunca vamos a tener los recursos suficientes para combatir el cibercirmen, pero luchamos por ello". "Intentamos no quedarnos atrás. La Guardia Civil está muy por delante en cuanto a recursos humanos pero nunca serán suficientes porque los escenarios y vectores de ataque son infinitos y el perímetro de defensa, limitado. Cada vez llegamos a más y somos mejores, pero necesitamos recursos y talento", subraya Ávila a este periódico.

La Europol ha alertado del aumento y creación de nuevas técnicas de cibercrimen. ¿Cómo se combaten? "No vale de nada escribir en leyes si no tienes recursos y talento. Son dos acciones decisivas que deben de tomar en cuenta los gobiernos y estados", agrega el director del Centro de Ciberseguridad que avanza los nuevos ataques que les preocupan.

Arturo Espejo y Enrique Ávila, ponentes en la Jornada de Ciberseguridad.

Clausura con el general Ceña y Encarnación Pérez. | ALMEIDA

> "No es que te roben el proyecto de un puente, sino que te lo cambian para que la obra se desplome y se hunda la empresa"

> "Para luchar contra el cibercrimen necesitamos muchos recursos y talento. Lo debe tener en cuenta el Estado"

Uno de ellos tiene que ver con la recreación de caras y voces con técnicas avanzadas. Suplantan a una persona de forma virtual y la introducen en un escenario conflictivo o delictivo recreado de forma digital. Por ejemplo, recrean la imagen de un importante directivo o empresario en una escena de pedofilia para chantajearle. Pero no piden un rescate, sino que reclaman acceder a una información. "Aunque sea mentira, es difícilmente demostrable que es mentira. Eso es muy preocupante", avisa Enrique Ávila.

La inteligencia competitiva y económica es otro de los ámbitos donde apuntan los cibercriminales. "Cuánta gente se queda fuera del mercado sin saber por qué. No porque les hayan robado sino porque conocen su estrategia comercial o les hacen un ataque reputacional. La gente tiene que aprender porque si no sabes de ciberespacio lo tienes muy mal", asegura el director del Centro de Ciberseguridad.

El general Arturo Espejo también habla de los peligros que sufren los proyectos de I+D+i y aquellos proyectos de arquitectura o grandes obras, algo en lo que España es un referente. "No es que te roben el proyecto de un puente, sino que te lo cambian. Ahí está el problema más grave. Que accedan al proyecto y cambien el punto de amarre. A lo mejor pasan días, meses o años y ya no puedes tirar de la copia de seguridad porque el ciclo ya ha pasado y no lo tienes", explica el jefe de los Servicios Técnicos de la Guardia Civil.

Para prevenir los ciberdelitos, la Guardia Civil cuenta con un personal muy técnico y formado. Ante los alumnos de Derecho presentes en el Seminario en el Paraninfo, los expertos en Cibercriminalidad de la Policía Judicial de la Guardia Civil hablaron de las nuevas medidas de investigación. El agente infiltrado es algo que ya está funcionando, por ejemplo, en grupos de pedofilia de forma tanto virtual como real, previa autorización judicial, según confirma el general Espejo.

Fundamental también es la cadena de custodia "transparente" a la hora de incautar un teléfono móvil u ordenador. "Hacemos un clonado y la parte original se queda a disposición judicial. Con autorización judicial sólo se captura información específica y evidencias relacionadas con el delito", detalla Espejo.