INFORME DE ACTIVIDADES, CIBERAMENAZAS Y TENDENCIAS

Semestre I
2020

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
UNIÓN EUROPEA

ÍNDICE

1. SOBRE EL PRESENTE INFORME 3

2. CSIRT- CV 3

3. PANDEMIA POR COVID19 5
- 3.1. Gestión de crisis. pandemia y teletrabajo 6
- 3.2. Servicios ofrecidos 8

4. GESTIÓN DE INCIDENTES DE SEGURIDAD 9

5. TENDENCIAS EN CIBERATAQUES 9

6. PLAN VALENCIANO DE CAPACITACIÓN 10
- 6.1. Publicación de informes 11
- 6.2. Campañas de concienciación 12
- 6.3. Cursos de formación en SAPS 12
- 6.4. Plan de capacitación en ciberseguridad para empresas 13
- 6.5. Jornadas de ciberseguridad en centros de secundaria 14
- 6.6. Material gráfico 14

7. OBSERVATORIO DE SEGURIDAD 16

8. CULTURA DE CIBERSEGURIDAD 17

1. SOBRE EL PRESENTE INFORME

Buena parte de la información aquí recogida es el resultado de la experiencia del CSIRT-CV durante el primer semestre de 2020, en el desarrollo de sus competencias. Asimismo, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, públicas y privadas.

2. CSIRT- CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana.

Nace en junio del año 2007, como una apuesta de la Generalitat Valenciana por la seguridad en la red. En 2020 cumple 13 años de andadura, en los que se ha consolidado como un CSIRT de referencia a nivel nacional y con presencia internacional en foros como CSIRT.es, Trusted Introducer y FIRST.

Se trata de una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico. Actualmente **CSIRT-CV** está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Consellería de Hacienda y Modelo Económico.

CSIRT-CV ofrece servicios dentro de la Comunitat Valenciana (Alicante, Castellón y Valencia), con vocación de servicio público y sin ánimo de lucro, por lo que sus servicios se ofrecen gratuitamente.

Los colectivos destinatarios de estos servicios son:

- Los ciudadanos de la Comunidad Valenciana.
- Los profesionales y empresas privadas, especialmente las de menor tamaño.
- La Administración Pública, tanto local como autonómica. Principalmente esta última por la ubicación del centro.

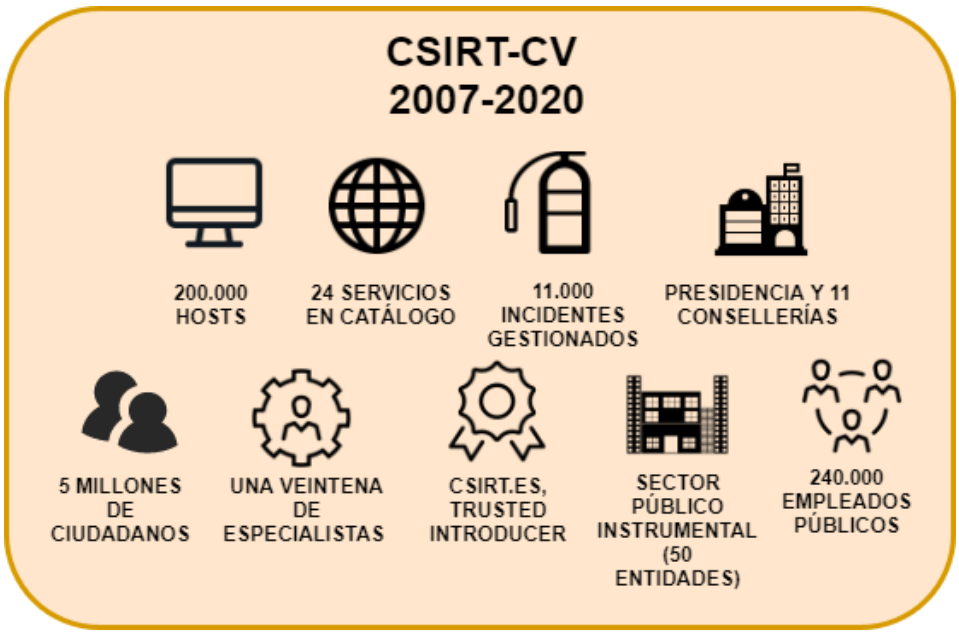
El ámbito de actuación del **CSIRT-CV,** como se observa, es muy amplio puesto que incluye a la Generalitat Valenciana, formada por Presidencia y 11 Consellerías, entre las que se incluyen 2 Vicepresidencias. También se incluye el sector público instrumental[1] y medio cent enar de entidades, con un número de empleados públicos que supera los 240.000[2] . Por último, cabe mencionar que la Comunitat Valenciana representa cerca de un 11% de la población nacional con unos 5 millones de habitantes (2019), siendo la 4ª Comunidad Autónoma de España en lo que a población se refiere.

Respecto a la infraestructura TI de Generalitat, es altamente heterogénea y compleja, dando servicio a cerca de 200.000 dispositivos, entre los que se incluyen tanto equipamiento IT como OT.

El principal objetivo del **CSIRT-CV** es contribuir a la mejora de la seguridad de los sistemas de información dentro de su ámbito, así como promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías de forma que se minimicen los incidentes de seguridad y permita afrontar de forma activa las nuevas amenazas que pudieran surgir.

1 http://www.gvaoberta.gva.es/es/sector-publico-instrumental

2 Según datos publicados en el Boletín Estadístico del Personal al Servicio de las Administraciones Públicas, a fecha julio 2019.



3. PANDEMIA POR COVID19

La pandemia por coronavirus (SARS-CoV-2) de 2019-2020 fue reconocida como global el 11 de marzo de 2020 por la Organización Mundial de la Salud (OMS). En respuesta al número creciente de casos de COVID-19, el Gobierno de España declaró el 14 de marzo de 2020 el estado de alarma, lo que conllevó la imposición de una cuarentena nacional como medida de emergencia para reducir el contagio. Esta cuarentena obligó a todos los ciudadanos residentes en España a quedarse en sus residencias habituales, exceptuando diversas situaciones como la adquisición de alimentos o medicinas, acudir al puesto de trabajo en determinados sectores esenciales o atender emergencias.

Esta situación supuso que se implantara el teletrabajo en todos los ámbitos en los que fuese posible, incluida la Administración Pública; un alto porcentaje de empleados pasó a la modalidad de teletrabajo a partir del día 16 de marzo, a la vez que se habilitó la tramitación telemática de determinados servicios ante el cierre presencial de oficinas. Este hecho provocó un impacto en los servicios tanto de CSIRT-CV como de toda Generalitat que tuvieron que ser adecuados a este nuevo escenario tal y como se explicará en epígrafes posteriores.

3.1. Gestión de crisis. Pandemia y teletrabajo

Tal y como se ha mencionado, la pandemia por coronavirus supuso la implantación del teletrabajo de forma inmediata en un alto porcentaje de empleados públicos, que pasó a esta modalidad de trabajo.

Para minimizar el impacto en la prestación de servicios en esta excepcional situación, el 12 de marzo la Generalitat puso en marcha el "Comité Ejecutivo COVID-19" con representantes de las diferentes áreas de la DGTIC. El principal objetivo de este comité fue definir los escenarios para posibilitar el teletrabajo a la mayor parte del personal de la Administración Pública. Este comité decidió crear a su vez otro subcomité -integrado por miembros del área de Comunicaciones, SAUPT y CSIRT-CV- para la búsqueda de soluciones técnicas para la definición de los escenarios del teletrabajo planteados.

Desde el mismo día 13 de marzo se suceden varias definiciones técnicas de posibles escenarios de teletrabajo para los que CSIRT-CV presentó recomendaciones de seguridad. Además, CSIRT-CV elaboró dos guías detalladas: una enfocada a los técnicos que tienen que implantar las medidas que se acuerden, y otra para los usuarios que van a teletrabajar, que se entrega a ambos comités.

Finalmente se consensúan dos escenarios para llevar a cabo el teletrabajo[3]:

- Teletrabajo con PTN (Puesto de Trabajo Normalizado)
- Teletrabajo con equipo informático doméstico

El teletrabajo conlleva riesgos de ciberseguridad en muchos contextos, sobre todo en los casos en los que el teletrabajador hace uso de sus equipos personales y/o se conectan a redes WiFi domésticas. La seguridad del hogar del teletrabajador también influye en la seguridad de la propia red corporativa, tal y como se describe en la Guía de Seguridad en el Teletrabajo[4] que publicó CSIRT-CV en 2018, y que fue tomada como referencia por diferentes instituciones como la Consellería de Innovación, Universidades, Ciencia y Sociedad Digital, para divulgar una serie de recomendaciones prácticas dirigidas a empresas[5], para organizar el teletrabajo.

---

3 Teletrabajo GVA http://www.dgtic.gva.es/es/teletreball
4 Guía de Seguridad en el Teletrabajo
https://concienciat.gva.es/wp-content/uploads/2018/03/infor_guia_de_seguridad_en_el_teletrabajo.pdf
5 Guía práctica para organizar el teletrabajo
http://innova.gva.es/documents/169273725/169715173/Gu%C3%ADa+pr%C3%A1ctica+para+organizar+el+teletrabajo/5588747e-f7f7-4567-ac62-62f862445e9a

CSIRT-CV además, puso en marcha una serie de iniciativas internas para incrementar las medidas de seguridad ante el potencial aumento del riesgo derivado del teletrabajo y para fortalecer la vigilancia ante uno de los colectivos más críticos durante la pandemia: el sector salud. A continuación un resumen de algunas de ellas:

- Se reforzó la vigilancia en dicho sector aumentando la sensibilidad en las sondas de detección de intrusos
- Se analizaron los logs de la VPN para reforzar la vigilancia en sus conexiones.
- Se atendieron consultas específicas con las conexiones remotas desde diferentes organismos.
- Se realizaron acciones informativas y de concienciación en el teletrabajo.[6]
- Se realizaron auditorías a varias iniciativas desarrolladas para ofrecer información actualizada sobre la COVID-19: portales Web, aplicaciones como App GVA Coronavirus o App GVA Responde, entre otros.

Para hacer frente a la pandemia, se pusieron en marcha diferentes Hospitales de Campaña, Hoteles Medicalizados o Pabellones. CSIRT-CV, tras evaluar desde el punto de vista de la ciberseguridad el despliegue técnico de estas infraestructuras TI, aportó una serie de recomendaciones para minimizar el riesgo de las mismas aumentando su securización.

Cabe destacar que el teletrabajo ha provocado cambios en la infraestructura tecnológica de Generalitat y en la forma en la que ésta presta sus servicios, por lo que, desde el punto de vista de la seguridad, se ha adaptado la ciberdefensa y vigilancia al nuevo modelo.

6 Quédate en casa pero ciberseguro
https://concienciat.gva.es/infografias/quedate-en-casa-pero-ciberseguro/

3.2. Servicios ofrecidos

CSIRT-CV dispone de un amplio abanico de servicios ofrecidos a su ámbito:

Prevención	Detección	Respuesta
Auditorías de seguridad	Sistemas de decepción	Gestión de incidentes de seguridad
Test de intrusión	Securización de entornos	Grupo de intervención rápida
Informes y alertas. Observatorio de seguridad	Auditoría de seguridad semántica	Gabinete de crisis
Consultoría técnica y legal	Informe forense pericial	
Plan Valenciano de Capacitación	Detección de intrusos	
Intercambio de información	Detección de APT	
Cuadro de mando de seguridad	Test de intrusión	
I+D+i		
Laboratorio de malware		
Monitorización de servicios Web		
Normalización		
Auditoría ENS		
Validación de código		
Consultoría sobre las ISO 27001:2013		
Análisis de riesgos		
Auditoría LOPD		
Ciberseguridad industrial		
Planes de mejora de la seguridad		

Los servicios ofertados por CSIRT-CV pueden ser realizados de manera proactiva o bajo petición. La siguiente tabla muestra algunos datos de los más relevantes:

Servicio ofrecido	Total semestre 1 de 2020
Test de intrusión	18
Auditorías de seguridad	45
Consultoría técnica, organizativa y legal	130
Emisión de alertas tempranas	27

Entre las consultas atendidas predominan las relacionadas con la seguridad en navegadores Web, formación para ciudadanos, aplicaciones de mensajería, certificados digitales y correos phishing.

4. GESTIÓN DE INCIDENTES DE SEGURIDAD

La actividad principal de CSIRT-CV se centra, como todo CSIRT, en la gestión de incidentes de seguridad. Para ello se dispone de una solución integral capaz de dar respuesta a cualquier compromiso relacionado con seguridad de la información, incluyendo entre otros el fraude electrónico, phishing, compromiso por malware, detección de comportamiento sospechoso en el equipo y en las cuentas digitales, suplantación de identidad, robo de contraseñas o secuestro de información.

El primer semestre de 2020 deja 3295 incidentes gestionados, cifra que duplica los datos registrados en todo 2019. Se observa un aumento significativo de incidentes provocados por código dañino, intentos de obtención de información a través de phishing y por intrusiones.

En la siguiente figura se muestra una evolución temporal de los incidentes gestionados por tipología en los últimos doce meses (de junio de 2019 a junio de 2020) donde se observa un aumento de actividad de marzo a mayo:

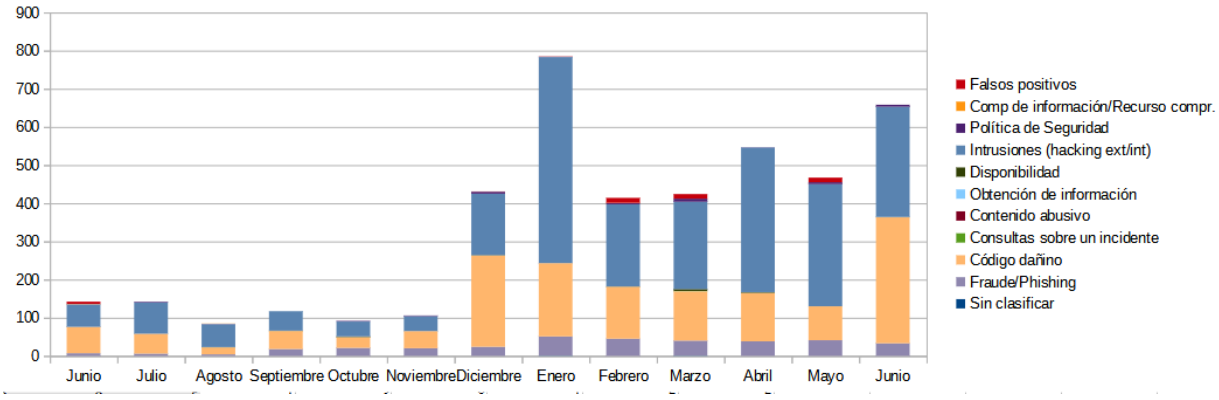


Figura 1: Desglose de incidentes gestionados en los últimos 12 meses por CSIRT-CV

5. TENDENCIAS EN CIBERATAQUES

Con la llegada del confinamiento y del teletrabajo en muchos ámbitos, incluido el de la Generalitat, las ciberamenazas han cambiado evolucionando a la explotación de nuevos puntos de entrada en las comunicaciones (concentradores VPN, servicios en la nube, etc.) y en el aprovechamiento de los fallos de seguridad de los equipos y/o redes domésticas usados para el teletrabajo.

Los gestores de contenido (CMS) como Liferay, Wordpress o Moodle, también han sido un objetivo elegido por los atacantes en numerosas ocasiones.

Entre las vulnerabilidades Web que más se han intentado explotar, predominan las relacionadas con ThinkPHP, una tecnología ampliamente extendida. Es destacable también el continuado intento de explotación de vulnerabilidades, antiguas o recientes, relacionadas con bases de datos Oracle o MySQL.

Cabe también destacar el incremento y diversidad de ataques de ingeniería social detectados. Se han recibido intentos de phishing suplantando instituciones estatales como la DGT o la Agencia Tributaria, o incluso la propia Generalitat, haciendo uso de sus imágenes corporativas.

En cuanto a la procedencia de los ciberataques por países, encabezan el ranking Países Bajos, España, Estados Unidos, Rusia y China, seguidos por Alemania y Gran Bretaña. Es importante recordar que la geolocalización desde la que se recibe el ataque no necesariamente corresponde con el origen del atacante, y que en la atribución a esos países influye también el hecho de que en los mismos se concentre un mayor volumen de equipos y de servicios, por lo que existe también una mayor probabilidad de recibir ataques desde allí.

En relación a los destinos de los intentos de intrusión a través de ataques Web, hay que señalar que los organismos más afectados por este tipo de ataques han sido la Consellería de Educación, la Consellería de Sanidad y la Diputación de Valencia, principalmente porque los sitios Web de los centros educativos, así como los de los Ayuntamientos son un objetivo clave para los hacktivistas. Es relevante también el aumento de los incidentes en el Sector Sanitario. Esto refleja la tendencia observada a nivel mundial[7] de atacar a los activos sanitarios, ya que actualmente son uno de los objetivos más valiosos.

7 https://securityboulevard.com/2020/05/healthcare-cyberattacks-increasing-during-covid-19/

6. PLAN VALENCIANO DE CAPACITACIÓN

Conseguir una gestión eficaz de la ciberseguridad no depende sólo de la implantación de medidas técnicas o de la definición de procedimientos: es fundamental la implicación de las personas. Esta circunstancia queda claramente reflejada en la Agenda Digital de la Comunidad Valenciana, estableciendo líneas de trabajo destinadas a mejorar la cultura en ciberseguridad de ciudadanos y empresas. De la misma forma se incluyen en la estrategia nacional y europea de ciberseguridad. La divulgación y concienciación es algo consustancial a la manera de entender la ciberseguridad en CSIRT-CV, por lo que el centro puso en marcha el Plan Valenciano de Capacitación que sitúa a las personas en uno de sus principales ejes de actuación. Para abordar este plan de la mejor forma posible, se definió un calendario donde se contemplan acciones concretas dirigidas a los colectivos identificados: ciudadanos, Generalitat, PYMES y otras administraciones públicas. Entre estas acciones podemos destacar jornadas familiares de seguridad, conferencias, guías y estudios.

Campaña de concienciación “Ciber-vuelta al cole” en nuestra web concienciaT y RRSS

Las principales acciones del Plan Valenciano de Capacitación en el primer semestre de 2020 se resumen a continuación.

6.1. Publicación de informes

Durante este semestre CSIRT-CV ha publicado su informe de actividad correspondiente al año 2019 en el portal principal y también se han actualizado las guías de “Uso seguro de Android” y “Uso seguro de iOS” en el portal de concienciaT para su descarga.

Este semestre, el material publicado por CSIRT-CV en sus principales portales ha sumado más de 26.000 descargas.

6.2. Campañas de concienciación

En los seis primeros meses del año, CSIRT-CV ha lanzado tres campañas de concienciación en las redes sociales en las que está presente, Facebook y Twitter así como en el portal concienciaT:

- Campaña “Siete errores de ciberseguridad que no deberías cometer”. El objetivo de la campaña es, que a través de 7 errores que habitualmente se cometen al navegar por Internet, los usuarios entiendan los riesgos a que se someten y mejoren sus hábitos digitales.

- Campaña “Stop Fake News”. Relanzando de nuevo esta campaña se pretendió ayudar a los ciudadanos a identificar noticias falsas con unos sencillos consejos.

- Campaña “Ciber-vuelta al cole: no te la dejes para septiembre”. Durante la pandemia por COVID-19 los niños han intensificado su contacto con la tecnología y dispositivos de casa. Muchos de ellos han adoptado nuevas costumbres que a veces no son todo lo ciberseguras que deberían ser. Por este motivo y con el objetivo de que los menores se muevan por la Red con todas las garantías de seguridad, CSIRT-CV a través de esta campaña emite algunas recomendaciones tanto para ellos como para sus familias.

6.3. Cursos de formación en SAPS

Durante la primera edición del año de los cursos de CSIRT-CV en la plataforma SAPS

(de enero a junio) se han formado 2376 alumnos. Este semestre se ha incorporado un nuevo curso “Instalación y guía de uso de Wireshark”, pasando a ser 18 los cursos que CSIRT-CV ofrece en su catálogo.

Los cursos que más alumnos han tenido este semestre han sido el de “Navegación Segura” con 199 alumnos, “Introducción a la seguridad informática” con 188 alumnos y el de “Instalación y guía de uso de Wireshark” con 171 matriculados.

6.4. Plan de capacitación en ciberseguridad para empresas

El pasado mes de febrero, la Dirección de CSIRT-CV presentó el “Plan de capacitación en ciberseguridad para empresas” en una jornada sobre Prevención del Delito en el

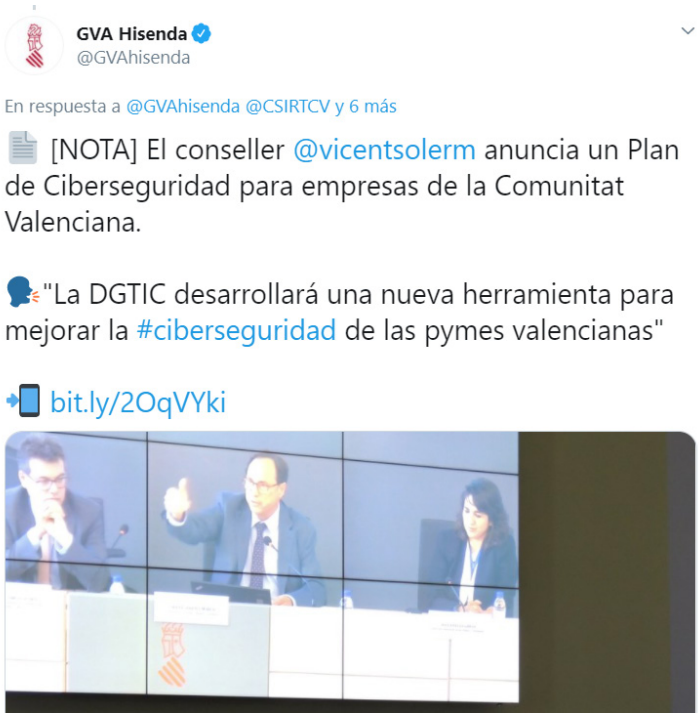


Figura 3: Detalle promoción Plan de Ciberseguridad para empresas en la Comunitat Valenciana

Sector Público Instrumental ante un total de 175 asistentes. Ese mismo día se publicaba en concienciaT un nuevo espacio denominado “Empresas” que permite el acceso a los contenidos del plan de capacitación.

La finalidad es ayudar a las empresas a mejorar su nivel de madurez en ciberseguridad y su confianza en el uso de la tecnología. Para conseguirlo, se ofrece formación y capacitación tanto a directivos como al resto de empleados, puesto que es necesario implicar a las personas para que el factor humano se convierta en uno de los pilares de la ciberseguridad de la organización.

Forma parte de este Plan de Ciberseguridad para Empresas, la herramienta Avalua'T que pretende ayudar a las empresas a autoevaluar el nivel de seguridad de sus sistemas y obtener una primera aproximación sobre los niveles de riesgo a los que se enfrenta su organización, atendiendo a su tecnología, sus procesos y sus empleados. Además, esta herramienta ofrece una relación de aquellos aspectos a mejorar, por lo que servirá tanto para la evolución como para la mejora continua en ciberseguridad.

También forman parte de este Plan de Ciberseguridad para Empresas, diferentes cursos online y videos interactivos.

6.5. Jornadas de ciberseguridad en centros de secundaria

Antes de que se declarara el estado de alarma a mediados de marzo, CSIRT-CV pudo visitar 28 centros de secundaria de la Comunidad Valenciana para realizar las Jornadas de Concienciación en Ciberseguridad con los alumnos de 2º y 1º de ESO, padres, madres y docentes.

Este semestre se han formado 3.061 personas (2.283 alumnos, 357 padres y 421 docentes), que desafortunadamente tuvieron que ser canceladas por la declaración del estado de alarma.

6.6. Material gráfico

Se han publicado dos nuevas infografías en el portal de concienciaT: por un lado una correspondiente al "Día de Internet Segura" en formato interactivo para acceder a todos los contenidos de concienciaT y otra relacionada con la repentina situación de teletrabajo global a causa de la COVID-19, "Quedate en casa, pero ciberseguro"

Figura 4: Detalle infografía publicada en el primer semestre de 2020

7. OBSERVATORIO DE SEGURIDAD

Tal y como se ha mencionado, el primer semestre de 2020 ha venido marcado por la pandemia global por coronavirus.

Esta situación supuso que se implantara el teletrabajo en un alto porcentaje de empleados públicos. Desde el punto de vista de ciberseguridad, el teletrabajo conlleva nuevos riesgos asociados principalmente a la exposición de nuevos servicios a Internet y uso de dispositivos personales (BYOD) y redes WiFi domésticas, por lo que es preciso adaptar las estrategias de ciberdefensa de las organizaciones a este nuevo escenario.

Muchas compañías y organizaciones han puesto en marcha diferentes soluciones para hacer posible el teletrabajo y nuevos proyectos tecnológicos relacionados con mejorar el rendimiento de los recursos virtuales.

Añadir que, la adquisición apresurada de nuevas soluciones tecnológicas que ayuden al desarrollo del teletrabajo, o la adopción de nuevos protocolos de actuación insuficientemente probados debido a la urgencia de la situación, conlleva que no se hayan contemplado todos los riesgos a los que hacer frente y puede facilitar que los atacantes encuentren debilidades para llevar a cabo sus intrusiones.

En definitiva, la pandemia ha ocasionado que el teletrabajo se imponga en todos los ámbitos en los que sea posible y que a lo largo de 2020 y años sucesivos, se prevean numerosos cambios en la infraestructura tecnológica de todas las empresas y organizaciones a nivel mundial y en la forma en la que éstas prestan sus servicios. Es por ello que desde el punto de vista de ciberseguridad, se ha de adaptar la ciberdefensa y vigilancia a este nuevo modelo que conlleva un tipo de riesgo y amenazas diferentes.

En cuanto a las principales amenazas identificadas en este primer semestre de 2020 mencionar que los ataques por ransomware evolucionan y se sofistican haciéndose más dirigidos y con la finalidad de obtener el mayor impacto posible. Los atacantes eligen cuál es el mejor momento para lanzar cada una de las fases del ataque, especialmente en la distribución del ransomware (*Human-operated ransomware*).

La situación geopolítica de los últimos años marca la tendencia creciente al ciberespionaje, una amenaza que confirma el interés de los atacantes por obtener información sensible de sus víctimas. Estos agentes están creando nuevas Tácticas, Técnicas y Procedimientos para intentar robar la propiedad intelectual de sus objetivos. El incremento de estas nuevas técnicas como *Living off the Land o fileless malware* dificultan la detección de las amenazas. Es fundamental, por tanto, ampliar

la monitorización a los clientes finales y ser capaces de modelar su comportamiento para detectar posibles anomalías. Herramientas como CLAUDIA (agente endpoint de CARMEN) permiten detectar este tipo de situaciones.

Mencionar por último que desde el mes de marzo se encuentran en curso multitud de campañas de desinformación en todo el mundo acerca de la COVID-19 y la pandemia global centradas en la publicación de contenido falso o distorsionado sobre diferentes narrativas: COVID-19 como arma biológica, xenofobia, control social, desconfianza en las instituciones, nuevo orden mundial, impacto económico, estadísticas falsas o engañosas, orígenes y propagación del coronavirus, politización, etc. Es preciso establecer un aumento de la vigilancia digital sobre esta nueva temática para detectar cualquier tipo de amenaza al respecto sobre nuestro ámbito.

8. CULTURA DE CIBERSEGURIDAD

CSIRT-CV está presente en las redes sociales Facebook y Twitter, canales de comunicación que utiliza - junto a otros – para crear una cultura de ciberseguridad entre sus seguidores a través de la emisión de noticias, recomendaciones, alertas y consejos sobre ciberseguridad. En la misma línea, el servicio de comunicación persigue convertir al centro en el referente de la Comunidad Valenciana en materia de ciberseguridad y fomentar una sociedad segura e informada.

De forma similar, CSIRT-CV ha participado como ponente en 2020 en los siguientes eventos:

- Se presenta el plan de empresas de CSIRT-CV ante el sector público instrumental (Febrero, 2020)
- Entrevista en el programa La Ventana CV, de Radio Valencia SER a Lourdes Herrero, Directora del CSIRT-CV (Marzo, 2020)
- Participación de Lourdes Herrero en la mesa redonda de FestinFor de la UPV “Seguridad de los datos a partir de la COVID19” (Mayo, 2020).
- Participación en un programa de La SER por parte de Lourdes Herrero para hablar sobre ciberataques durante la pandemia (Mayo, 2020)
- Participación en el programa de radio “Al ras” de Á punt para hablar sobre la campaña de concienciación “Cibervuelta al cole: no te la dejes para septiembre”.

CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana