



# Protección **contra virus** y otros tipos de **software malicioso**

**Ricardo Cañizares Sales**

DIRECTOR REVISTA **a+**

**C**omo hoy en día la amenaza no son solamente los virus, hablamos de software malicioso, cuya acepción cubre todos las posibles variantes del mismo, como virus, gusanos, troyanos, spyware, y otros, tanto los actualmente existentes, como los que aparecerán en el futuro.

Aunque inicialmente se habló de virus, hoy en día debido a la proliferación de diferentes tipos de software indeseable, se habla de software malicioso, cuya acepción cubre todos las posibles variantes del mismo, como virus, gusanos, troyanos, spyware, y otros, tanto los actualmente existentes, como los que aparecerán en el futuro.

La amenaza es grave, pero no nueva, el software malicioso ha existido desde el comienzo de la aparición del primer sistema informático comercial y existirá

mientras existan los sistemas informáticos. Lo mismo que no podemos entender la vida del hombre sin la existencia de las enfermedades, no podemos contemplar la existencia de sistemas de información, sin la existencia del software malicioso. Podremos erradicar algún tipo de software mali-

«Tenemos que aprender a convivir con los virus y otros tipos de software malicioso»

cioso, lo mismo que se erradicó la viruela, pero aparecerán otros, lo mismo que aparecen enfermedades como la gripe aviar.



En diciembre de año 2003, después de un grave incidente por infección de virus, la certeza de que a corto plazo era imposible erradicar completamente el virus del sistema informático, y la consciencia de lo ardua y costosa que sería la tarea, me llevo a escribir en un informe la siguiente aseveración: «Tenemos que aprender a convivir con los virus y otros tipos de software malicioso».

Con la afirmación que efectué en aquel momento, estaba avisando de que nunca podremos erradicar el software malicioso, podremos mantenerlo bajo control, disminuir sus efectos, evitar su propagación, blindar nuestros sistemas, pero en ningún caso podremos hacer desaparecer el software malicioso de la faz de tierra, por lo tanto nuestros sistemas informáticos siempre estarán expuestos a la amenaza que supone el software malicioso.

Cuando digo que «Tenemos que aprender a convivir con los virus y otros tipos de software malicioso», me refiero a que

**U**na adecuada protección contra virus y otros tipos de software malicioso, debe incluir como mínimo:

- Política de concienciación
- Normas de uso de estaciones de trabajo, correo y uso de Internet
- Utilización de software anti-virus, con capacidades avanzadas
- Procedimientos de emergencia
- Personal debidamente cualificado e instruido



tenemos que actuar ante este tipo de amenaza de la misma manera que actuamos ante las enfermedades: tomando medidas de prevención y aplicando medidas terapéuticas cuando la persona esta enferma. En el caso de un sistema informático estableciendo medidas de protección, tanto organizativas como técnicas, y medidas correctivas cuando el sistema está comprometido.

La grave amenaza que suponen para nuestros sistemas informáticos, las diferentes variantes del software malicioso, son la causa de que las empresas inviertan ingentes recursos, en la protección antivirus, pero en muchos casos dicha protección se ha basado únicamente en la instalación de software especializado en estas tareas, pero como todos ustedes conocen, desde que aparece un nuevo software malicioso, hasta que los fabricantes de antivirus lo incluyen en su producto, existe un espacio de tiempo en el que nuestros sistemas se encuentran desprotegidos, los fabricantes

Para «Hablar de» «Virus y otros tipos de software malicioso», en este número hemos seleccionado:

**El problema del spyware en las empresas**

**100**

**El SPAM nos invade**

**104**

**Filtros web: el brazo tecnológico de los Recursos Humanos**

**108**

**La creación de malware, como nuevo modelo de negocio**

**110**

intentan minimizar este tiempo, sacando actualizaciones a los ficheros de firmas de sus productos lo más rápido posible, incluso varias veces al día.

Para intentar minimizar el riesgo de infección, durante el periodo que transcurre entre la aparición de la nueva variante de software malicioso y el momento en el que está disponible el patrón de detección del mismo, se están desarrollando nuevas tecnologías de detección de software malicioso desconocido.

Para intentar garantizar la seguridad de nuestros sistemas informáticos, contra la amenaza que supone el software malicioso, es necesario disponer de mecanismos que nos proporcionen una alerta temprana, que nos informen de la aparición de las nuevas amenazas y del incremento del nivel de riesgo que suponen.

Pero sin lugar a dudas una de las medidas de protección contra el software malicioso más eficaz, es la formación y mentalización de los usuarios. Un usuario con la formación adecuada será capaz de detectar los vectores que utilizan las nuevas variantes del software malicioso, será capaz de detectar los ataques que reciba utilizando la «ingeniería social», rechazará un correo con un origen desconocido y un asunto sospechoso, y otros muchos ataques realizados por medio de software malicioso.

Por último, no hay que olvidar la importancia que se le debe dar a la investigación de nuevas tecnologías de protección contra virus y otros tipos de software malicioso, la amenaza del software malicioso es cada vez mayor, y necesitamos mejores herramientas de prevención y protección, tenemos que anticiparnos a nuestro enemigo, el software malicioso. ♦



## EN PRÓXIMOS NÚMEROS «HABLAMOS DE...»



**Aplicación de Normas y Estándares en las TIC [nº4]**



**Dispositivos de Protección de Perímetro**



**La LOPD y su Reglamento**



**La seguridad en los sistemas de información sanitarios**



**La seguridad en las comunicaciones móviles**