LA SEGURIDAD INFORMÁTICA, A DEBATE

Los riesgos de la era digital

JOSÉ CARMONA
PRESIDENTE DE TIMUR

En el contexto social actual, la forma en que las personas, las empresas, las organizaciones e instituciones actúan, interactuaran y operan está marcada por el uso y utilización masiva de las tecnologías de la información y las telecomunicaciones.

Las actividades sociales, la creación de riqueza, la producción, la distribución, el comercio y el consumo de bienes y servicios, se han transformado, nos encontramos en la era digital.

La nueva cultura de la sociedad digitalizada dicta las normas prácticas, éticas y políticas con las que han de desenvolverse los seres humanos, las organizaciones e instituciones.

En esta era digital donde el ser humano, las organizaciones e instituciones se desenvuelven e interactúan en un contexto virtual, donde no se pueden establecer fronteras físicas, donde se han de asumir conceptos culturales como el trabajo y el aprendizaje colaborativo y en comunicación, la libertad de expresión y de difusión, la generación de sociedades alternativas según intereses y gustos personales o profesionales fuera del contexto social y geográfico, la desaparición de los límites entre actividades, profesiones, áreas del conocimiento, instituciones y nacionalidades, y el nacimiento de la ciudadanía digital global, han llevado a las empresas que se dedican a desarrollar productos y prestar servicios de tecnologías de la información y telecomunicaciones a tener en cuenta en sus diseños, desarrollos e implantaciones las necesidades de seguridad que se plantean en este mundo intercomunicado y globalizado.

Las necesidades de seguridad que se plantean en los sistemas de información y comunicaciones son los mismos que se plantean en el mundo real: la seguridad de las infraestructuras básicas que dan soporte al procesamiento y almacenamiento de la información (edificio), la seguridad de los sistemas de procesamiento y almacenamiento de la información (contenido o información), y la seguridad de los sistemas y redes de interconexión y comunicación entre sistemas y dispositivos (puertas entrada/salida).

La información es uno de los principales activos de las organizaciones. La protección de este activo es una tarea esencial para asegurar la continuidad del negocio, es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información), y además traslada confianza a los clientes y/o usuarios.

Los sistemas de gestión de seguridad de la información (SGSI) que se implementan por las empresas que se dedican a desarrollar productos y prestar servicios de tecnologías de la información y telecomunicaciones normalmente siguen la norma ISO 27001, norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa y es el medio más eficaz de minimizar los riesgos. Una gestión eficaz de la seguridad de la información permite garantizar su confidencialidad, asegurando que solo quienes estén autorizados puedan acceder a la información, su integridad, asegurando que la información y sus métodos de proceso son exactos y completos, y su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran. La ISO 27001 puede ser implementada en cualquier tipo de organización y está redactada por los mejores especialistas del mundo en el tema, proporcionando una metodología para implementar la gestión de la seguridad de la información.

Estos sistemas están diseñados para detectar y controlar cualquier fallo de seguridad que se produzca a cualquier nivel y provenga de cualquier sitio, de un fallo interno del sistema de almacenamiento o procesamiento o de un ciberataque externo que aprovecha alguna debilidad o falla en el software, en el hardware, e incluso en las personas que forman parte de un ambiente informático, con el fin de obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema.

> «En la era digital la seguridad es fundamental, ya que sin ella no habría confianza en los sistemas ni progreso en su desarrollo»

El ciberataque informático que se produjo el último sábado 13 de mayo se dirigió contra la red corporativa de Telefónica, que fue corrompida momentáneamente afectando a una parte puntual de sus trabajadores, pero no a toda la compañía, y en breve plazo la vulnerabilidad fue controlada. No se sabe si afectó a información valiosa o sensible de la empresa y si se pagó rescate por ella, cuando un equipo fue atacado, los ciberatacantes se hicieron con todos sus datos y bloquearon cualquier acceso a esa información. A partir de ese momento, los piratas extorsionaron y amenazaron a los usuarios de los equipos de la empresa a cambio de recuperar su información.

Desde Timur no se ha detectado ninguna empresa que haya sido afectada por el ciberataque y nuestros asociados nos han comunicado que los sistemas de seguridad de la información que tienen instalados sus clientes han funcionado correctamente.

En cualquier era se ha considerado básica la necesidad de seguridad, y en la era digital la seguridad informática, además de básica, es fundamental, ya que sin ella no habría confianza en los sistemas ni progreso en su desarrollo.

Manos arriba, esto es un atraco

TOMÁS JIMÉNEZ
DIRECTOR DEL ÁREA TECNOLÓGICA DE LA UMU

Desde el pasado 12 de mayo ya son objeto de conversación cotidiana los ciberataques, el malware y las criptomonedas. Términos hasta ahora restringidos a los técnicos de seguridad informática, 'gracias' al ataque WannaCrypt se han incorporado a nuestras tertulias y aparecen en todos los medios de comunicación y redes sociales.

La mala noticia es que estos ciberataques han llegado para quedarse. Aunque lo positivo puede ser que afrontar esta 'ciberguerra' nos hará más responsables, más fuertes, y lo superaremos...pero, desde luego, como toda guerra, no será sin víctimas, ni costes ni importantes inversiones.

En todas estas conversaciones que ahora florecen planea siempre la pregunta: ¿estamos realmente preparados para defendernos de estos ataques? Una primera observación es constatar los numerosos países donde el ataque ha surtido efecto, las grandes compañías que han sido atacadas y 'heridas' y cómo de sencillo, hasta cierto punto, ha sido penetrar en innumerables ordenadores personales y empresariales.

Siendo honestos, y sin alarmismo, lo cierto es que, en general, no podemos (NI DEBEMOS) afirmar categóricamente que nadie está fuera de peligro. En mayor o menor medida todos podemos estar expuestos a un ataque de este tipo, o de otros más sofisticados y 'menos estruendosos' que el actual.

Aunque pueda parecer descorazonadora esta primera afirmación, si reflexionamos bien, en el fondo sucede lo mismo, con muy similares conclusiones, con la seguridad de nuestras casas o de nuestra propia seguridad personal o familiar. Piense en la analogía entre ciberseguridad y seguridad ciudadana: ¿Podemos afirmar que estamos absolutamente seguros de que nuestras casas o nuestras vidas no corren ningún peligro y que no podríamos ser atacados mañana? ¿Afirmaría usted estar seguro de que ayer nadie entró en su casa y salió sin dejar rastro? Medite sobre ello.

> «Siendo honestos, y sin alarmismos, lo cierto es que, en general, no podemos afirmar categóricamente que nadie está fuera de peligro»

No pretendo fastidiarle el merecido fin de semana, pero seguro que me responderían que eso depende de las medidas de seguridad de su casa, de lo 'ostentoso' de su comportamiento, del número de visitantes con llave, o de las 'zonas que frecuenta'.

Pues en cierta manera podemos realizar un razonamiento similar respecto a la seguridad informática: Simplemente proteja sus activos, personales o empresariales, y siempre en función del valor de los mismos, porque igual que nadie tiene en su casa la caja fuerte de Fort Knox para guardar la paga semanal de sus hijos, no será tampoco necesario contratar a un experto en seguridad que duerma en la habitación de invitados para proteger su PC personal. En resumen: que las medidas de seguridad sean acordes al valor a proteger.

Pero si no tiene antivirus, su clave wifi es 1111, y la del administrador es 'admin', pues mal vamos. Pero mejoramos rápido con simples medidas de sentido común como actualizar antivirus y poner claves 'sensatas' que no sean adivinables por su hijo de 6 años. O si tiene Linux en casa ya habremos avanzado muchísimo más (aunque reconozco que esta es una 'cuña publicitaria' interesada).

Y sigo dando moral... volvamos nuevamente a las analogías y recordemos que hace bien poco tuvimos un virus más letal que el Ransomware: el sida, y aunque algunos 'fundamentalistas' proponían como solución la drástica medida de olvidarnos del sexo por completo (que indudablemente era efectiva, pero cuando menos aburrida), simplemente con concienciación, información y profilaxis, el sida no ha desaparecido pero sí ha sido minimizado, sin que por ello hayamos dejado de seguir 'haciendo amigos' cuando corresponde.

Pues aquí igual: No abandone internet, ni prescinda del smartphone ni rebusque en el sótano su vieja olivetti. Simplemente 'cuide sus amistades'. Conozca muy bien con quién se relaciona, no abra 'emails' desconocidos (otra mala noticia: no suele tocar la lotería tan frecuentemente, ni esa guapa rubia eslava está realmente buscando a su alma gemela en Murcia). No sea 'internet-promiscuo'. Visite solo páginas seguras y confiables. Revise el estado de sus preservativos antivirus que también 'caducan'... tampoco será necesario alarmarse innecesariamente. Precaución toda. Pánico ninguno.

Nota: Hablamos de sistemas personales. Todo se torna mucho más complejo en un entorno empresarial o de administración pública. Ahí, la codicia agudiza el ingenio, y a fe que los hay muy ingeniosos para vulnerar hasta sistemas de importantes compañías o entrar en la CIA a robar unos pocos 'emails' de una tal Hilary. Aquí ya hablamos de 'palabras mayores'.

¿Entonces qué? ¿Adiós a la administración electrónica? Para nada. Comience por seguir las fantásticas recomendaciones del CCN (www.ccn.cni.es) o del Incibe (www.incibe.es) para mejorar y proteger sus activos TI (Sí, créanlo: servicios de nuestra administración pública realmente útiles para administraciones y entidades. Enhorabuena)

Así pues, aunque la batalla promete ser larga y compleja, y muchos seremos 'daños colaterales' y campos de experimentación en busca de información más sensible, tenemos 'armas defensivas' a nuestro alcance. Simplemente dediquen menos tiempo al pánico y más a la seguridad. Y que ello no le impida disfrutar de las ventajas de internet.