

El 90,3% de las pequeñas empresas españolas afirma que les da confianza realizar operaciones bancarias a través de Internet.

- La utilización de herramientas y buenas prácticas de seguridad está ampliamente extendida entre las pequeñas y microempresas españolas. La inmensa mayoría de ellas declara contar con una solución antivirus en sus ordenadores (97,8%) y realizar copias de seguridad (94,2%).
- Otras medidas instaladas en los equipos de la empresa como los cortafuegos (72,4%) o los medios de control de acceso, como contraseñas (66,8%), tienen una presencia generalizada en estas organizaciones.
- La creciente importancia de la seguridad de la información para los responsables de estas empresas también tiene su reflejo en la implantación de medidas de seguridad a nivel corporativo. Este es el caso de los sistemas de copias de seguridad (82,4%) o los sistemas de prevención de intrusos (51,7%).
- La pequeña y microempresa española es consciente de estar sujeta a la normativa sobre protección de datos y cumple de forma mayoritaria la obligación de inscripción de ficheros ante el registro de la AEPD (así lo hace el 52,6%), la obligación de solicitud de consentimiento (62,3%) y la obligación de información a los titulares de los derechos (67,1%). Además, en todos los casos, la evolución experimentada desde 2008 es muy positiva, confirmando la efectividad de las actividades de concienciación y formación puestas en marcha hasta la fecha.
- El 48,4% de los ordenadores de las empresas analizados con iScan, la herramienta desarrollada por INTECO, tiene algún código malicioso o malware en junio de 2009.
- Aún así se confirma la confusión y el desconocimiento real de las empresas sobre lo que sucede en sus equipos. Un 42,9% de las entidades afirma haber sufrido ataques de virus cuando la auditoría de seguridad no ha identificado ni una sola variante.

De los resultados del “*Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas*” elaborado por el Observatorio de la Seguridad de la Información de INTECO se desprende un crecimiento en la realización de transacciones bancarias y económicas a través de Internet por parte de empresas de nuestro país. Así, el 84,2% de las entidades realiza operaciones bancarias a través de Internet, ofreciéndoles a un 90,3% mucha o bastante confianza el efectuar actividades de banca online.

Otras actividades relacionadas con el comercio electrónico, como pueden ser los servicios de compra y venta a través de Internet son también empleados de forma considerable por las pequeñas y microempresas (un 41% y un 40,6% respectivamente), al igual que de los servicios de pago por Internet, utilizados por un 41,5%. El grado de confianza para cada una de estas

acciones es de 82,7% para las compras a proveedores por Internet, 85% para la venta online y 75,1% para los pagos online.

Destaca así mismo el grado de confianza que les genera a las pequeñas y microempresas españolas la realización de otras gestiones como son los trámites con la Administración Pública (57,2%) y el uso de firma electrónica (50,2%). Mientras que en el caso de los trámites, el 90,1% de las entidades les genera mucha o bastante confianza y, en el caso de la firma, es el 90,8% de las empresas.

De esta manera y considerando el nivel de uso como el indicador más limpio respecto al nivel de e-confianza en la Sociedad de la Información se encuentra en niveles más que razonables, y son pocos los casos en los que las empresas no usan estos servicios porque saben cómo hacerlo o les falta confianza.

Acuerdo metodológico para el diagnóstico y la métrica de la seguridad de la información en el ámbito de la PYME

La experiencia de INTECO en la realización de estudios basados en el contraste entre la percepción sobre la situación de seguridad de la información de los usuarios y el nivel de seguridad real de los equipos ha resultado clave para conocer el estado real de seguridad de las pequeñas y microempresas españolas. Se está por tanto, ante un estudio que se puede convertir en referente nacional al identificar la problemática que tiene este tipo de empresas que representan a 9 de cada 10 entidades españolas.

Para el presente estudio se han realizado 2.206 entrevistas a empresarios obteniéndose su percepción sobre la situación de seguridad de la información de su empresa y su e-confianza, y se han realizado 622 auditorías de seguridad remotas en los equipos informáticos de las empresas para conocer el nivel de seguridad real tanto del sistema de sus ordenadores.

Situación de seguridad de la pequeña y microempresa española

Las empresas, conscientes de la importancia de sus datos y de la información que albergan sus equipos, no sólo disponen de herramientas de seguridad sino que también llevan a cabo buenas prácticas, planes y políticas que garanticen la autenticidad, confidencialidad, integridad y disponibilidad de la información que necesitan para poder desarrollar su actividad cotidiana.

De las primeras, las herramientas, cuentan en el mercado con multitud de soluciones de las que se aprovechan para conseguir este objetivo. Así disponen de herramientas destinadas para los propios equipos y otras generales para aplicar a la empresa, consiguiendo de esta forma que su nivel de seguridad mejore.

Entre las herramientas residentes en los ordenadores, las más ampliamente utilizadas son aquellas asociadas a la protección de la navegación en Internet, como es el caso de los antivirus (utilizadas por el 97,8% de las organizaciones), los cortafuegos personales (por el

72,4%), las que impiden el correo basura (61%) o las de bloqueo de ventanas emergentes (54,4%).

El grado de implantación de algunas de estas soluciones en España es tal que si se compara con la situación internacional, el nivel de utilización es superior como sucede en el caso del uso de los antivirus (donde la diferencia es de 17,8 puntos porcentuales), de los cortafuegos (8,3 puntos) y 22,9 puntos en el caso del control de acceso al equipo.

Por otro lado, entre las soluciones generales de aplicación en el ámbito de las empresas son de implantación entre las entidades que cuentan con una mayor estructura organizacional como es el caso de las que cuentan con más de 10 trabajadores. Se trata entre otras de herramientas como los sistemas de copias de seguridad de los datos, los cortafuegos en red o los sistemas de prevención o detección de intrusos que son usados según declaración de los empresarios por el 82,4%, el 72,9% el 51,7% y el 32,5% respectivamente.

Comparativamente aún son pocas las pequeñas empresas que cuentan con un responsable de seguridad

Dos elementos que condicionan la implementación de las diversas soluciones son por un lado, la presencia de un responsable de seguridad informática en el seno de las empresas y, por otro, la cuantía y valoración de la inversión realizada en productos de seguridad.

En relación con la existencia del personal de informática y por ende de un director de seguridad, el 17,8% de las empresas participantes afirma disponer de personal de informática y de ellos el 28,1% de las entidades cuenta entre su plantilla, además, con una persona encargada en exclusiva de dirigir la seguridad informática y un 52% adicional lo hace compaginándolo con otras funciones. Así, la presencia de un director hace que por ejemplo en el uso de las herramientas que permiten el acceso a la red desde fuera de la oficina la diferencia sea de 28 puntos porcentuales. Es decir, mientras que un 44,2% de las organizaciones con director utilizan este tipo de solución, aquellas que no disponen de este perfil son el 16,2%.

El 79,9% de las entidades considera adecuada la inversión en seguridad realizada por su empresa en relación con el gasto total en informática. Además parece existir, en general, una buena consideración de las empresas a la hora de valorar un producto de seguridad primando el 66,6% de las pequeñas y microempresas españolas participantes en el estudio la calidad / efectividad.

Entre las buenas prácticas que realizan las empresas destacan la realización de copias de seguridad (por el 94,2% de las organizaciones) y la actualización de los programas y sistemas operativos (realizada por el 88,9% de las entidades). La importancia de la actualización radica en que el no contar con ella puede suponer que se produzcan desde fallos hasta un mal funcionamiento del hardware añadido.

Finalmente la disposición de planes y políticas de seguridad por parte de las pequeñas y microempresas españolas es otra de las prácticas que permiten a las entidades disponer de una estrategia para el aumento progresivo del nivel de seguridad. Entre las empresas participantes se materializa disponiendo o teniendo previsto disponer de un plan de seguridad (en esta situación se encuentra el 34,3% de las organizaciones), en la tenencia de un plan de concienciación (17,6%) o de uno de continuidad de negocio (11,9%).

El malware se diversifica

Un 48,4% de los equipos analizados con iScan, la herramienta desarrollada por INTECO, tiene algún código malicioso o malware en junio de 2009. Lo cual supone un incremento del nivel de infección de 8,4 puntos porcentuales desde el 2008.

Además se confirma la confusión y el desconocimiento real de lo que sucede en sus equipos. Esto tiene su reflejo en tres conceptos como son los virus, los troyanos y el software espía. Respecto de los primeros siguen siendo los grandes desconocidos de los usuarios ya que un 42,9% afirma haberlos sufrido cuando la auditoria de seguridad no ha identificado ni una sola variante.

En el caso de los troyanos, la presencia real de este código malicioso en los equipos (27,8%) supera el nivel percibido por los empresarios (21,7%). Por último, el software espía se encuentra presente en los equipos en menor medida (1,4%) de lo que opinan las pequeñas y microempresas españolas participantes (15,1%).

Estos datos reflejan la tendencia al abandono del desarrollo de los virus a favor de troyanos motivada porque estos últimos suelen suministrar a sus creadores algún tipo de beneficio económico. Ésta evolución también se refleja en el porcentaje de variantes únicas detectadas donde la mayor parte corresponde a troyanos (35,1%).

En este sentido, y desde el punto de vista cualitativo, las familias de malware con mayor presencia a parte de los troyanos son las herramientas (32,6%), y el software publicitario no deseado (26,9%).

Se puede concluir que el código malicioso presenta un alto nivel de diversificación y heterogeneidad: así, en los 1.381 archivos infectados reconocidos entre febrero y junio de 2009 se han identificado 963 variantes únicas de malware. De ellas, 678 sólo han sido detectadas en un único equipo (detecciones únicas de variantes únicas).

Este dato constata la velocidad con que aparecen nuevas manifestaciones: con el fin de dificultar su detección, los creadores de malware modifican sus códigos constantemente, creando miles de ejemplares nuevos cada día. El alto nivel de diversificación y heterogeneidad se convierte en el principal obstáculo para la efectividad de los programas antimalware basados en el reconocimiento de especímenes.

Desconocimiento del nivel real de implantación de las herramientas y el estado de seguridad de los equipos

El análisis cruzado de la percepción de seguridad de los empresarios con la situación real de los equipos pone al descubierto las empresas que se encuentran o pudieran encontrarse ante un riesgo potencial cuyo origen está en la creencia incorrecta respecto a la disponibilidad o no de los programas antivirus en sus equipos, la actualización del sistema operativo y/o los programas y el estado de infección de los equipos.

Respecto a los antivirus el análisis permite identificar y distinguir entre las empresas que afirman disponer de ellos (el 97,8%) y los que realmente los tienen en sus equipos (el 93,1%). En el caso de la actualización, mientras que el 88,9% de las empresas afirma haberlo realizado, el análisis de iScan señala que el 58,5% efectivamente lo ha hecho. Por último, el 66,4% cree que su equipo tiene malware mientras que el análisis de la auditoría refleja que el 48,4% de las empresas tienen sus equipos infectados.

Consecuencias, reacciones y respuesta de las empresas ante las incidencias de seguridad

El 77,4% de las pequeñas y microempresas españolas participantes en el estudio afirman haber sufrido algún incidente de seguridad, lo cual ha supuesto para el 54,9% la pérdida de tiempo de trabajo.

Sin embargo, y a pesar de ese tiempo el análisis de la encuesta permite comprobar como la empresa no está asociando las incidencias sufridas con las posibles pérdidas económicas o a efectos negativos sobre la imagen empresarial. De hecho un 69% de las empresas españolas afirma que no existe ningún tipo de impacto monetario sobre el negocio.

Respecto a las reacciones que las organizaciones tienen frente a las incidencias el 42,9% responde instalando o actualizando una herramienta de seguridad, realizando copias de seguridad de los archivos (24,6%) o cambiando de contraseñas (20,7%).

Evolución positiva respecto al conocimiento y la adecuación a la normativa sobre protección de datos

En este último año ha habido una evolución positiva del porcentaje de empresas que reconocen estar afectadas por la normativa de protección de datos. El incremento ha sido de 26,2 puntos porcentuales, situándose en 2009 en un 60,2% de empresas las que reconocen estar afectadas, llegando incluso a un 80% de entidades las que se saben afectadas por el hecho de disponer de ficheros con datos personales.

Otros aspectos en los que se distingue la evolución son la notificación de ficheros ante el Registro General de la Agencia Española de Protección de Datos, el deber de solicitar el consentimiento del afectado para proceder al tratamiento de los datos y el deber de informarles en la recogida de los datos personales.

En el caso del registro, el 52,6% de las empresas lo ha realizado en 2009 frente al 37% en 2008. Mientras que respecto al consentimiento el incremento ha sido de 33,3 puntos porcentuales, llegando en 2009 al 62,3% de las empresas participantes en el estudio que reconocen solicitarlo. Por último, el 67,1% de las pequeñas y microempresas españolas participantes en el estudio afirman cumplir el deber de información, lo que supone un aumento de 38,1 puntos con respecto a la lectura del año anterior.

A expensas de conocer en futuros estudios si las empresas revisan el cumplimiento de la Ley Orgánica de Protección de Datos en las auditorías de seguridad, dado el carácter bienal de esta obligación implantada a través del Reglamento de Desarrollo de la Ley de Protección de Datos (RDLOPD) en 2008. Actualmente el 15,8% de las empresas con más de 10 empleados llevo a cabo esta revisión. Este dato está en línea con el cumplimiento a nivel internacional, donde un 13,5% lleva a cabo esta práctica.

Sobre el Instituto Nacional de Tecnologías de la Comunicación (INTECO)

El Instituto Nacional de Tecnologías de la Comunicación, promovido por Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

Tiene un doble objetivo: contribuir a la convergencia de España con Europa en la Sociedad de la Información y promover el desarrollo regional, enraizando en León un proyecto con vocación global.

El Instituto alberga la Oficina de Seguridad de Internauta, el Centro de Respuesta a Incidentes de Seguridad, el Observatorio de la Seguridad de la Información, el Centro Demostrador de Seguridad para la PYME, el Centro de Referencia en Accesibilidad y Estándares Web y el Laboratorio Nacional para la Calidad del Software, entre otros.

Más información: <http://www.inteco.es>

Sobre el Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de seguridad y e-confianza.

En cumplimiento de uno de los objetivos encomendados a INTECO en el marco del Plan Avanza, su misión es describir de manera detallada y sistemática el nivel de seguridad y confianza en la Sociedad de la Información en los hogares, empresas y Administración, así como generar conocimiento divulgativo y especializado en la materia, así como la elaboración de recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones de futuro por parte de la industria y los poderes públicos.

Más información: <http://observatorio.inteco.es>

Sobre la Metodología del estudio

En la definición de la metodología del estudio, se ha considerado una fórmula que permita obtener información relativa al nivel de seguridad y e-confianza de las pequeñas y microempresas españolas. La necesidad de unos datos robustos que permitan contrastar lo percibido con la situación real en los equipos.

- Percepción sobre la situación de la seguridad de la información y nivel de e-confianza de los empresarios. Los datos se extraen de encuestas personales a un total de 2.206 pequeñas y microempresas, de acuerdo con los criterios del muestreo aleatorio simple en las que $p=q=0,5$ y para un nivel de confianza del 95,5%, el error muestral para $n=2.206$ es de $\pm 2,1\%$.
- Nivel de seguridad real de los equipos informáticos existentes en las empresas. Para ello, se utiliza el software iScan, desarrollado por INTECO, que analiza los sistemas y las incidencias de seguridad en los equipos gracias a la utilización conjunta de 46 motores antivirus. Este software se instala en los equipos y los analiza, detectando todo el malware residente en los mismos y recogiendo además datos del sistema operativo, del estado de su actualización y de las herramientas de seguridad instaladas. El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada. El número total de análisis remotos de seguridad ha sido 622.