WHITE PAPER

Amenazas Informáticas:

Protege tu empresa en la nube

prodware

LA NUBE

La transformación digital implica un cambio de hábitos en la forma de trabajar, de gestionar documentos, comunicarse e interactuar.

La digitalización significa el uso de nuevas tecnologías y herramientas a la vez que la implementación de nuevos procesos y nuevas formas de trabajo. Hablar de digitalización es también hablar de la nube, la posibilidad de gestionar el almacenamiento en remoto ha sido clave en el desarrollo de muchas empresas y nacimiento de otras.

La gestión del almacenamiento de forma masiva a través de datacenters ha permitido escalar precios y acercar a las empresas con menos recursos soluciones complejas a costes asequibles.

Además, la nube ofrece movilidad y accesibilidad, elementos fundamentales para los actuales modelos de empresa, más dinámicos y descentralizados. La nueva era de la tecnología ya está aquí y debemos saber adaptarnos y aprovechar sus ventajas.

"La era digital en la que estamos inmersos exige agilidad para competir y diferenciarse y las empresas que apuesten por el cloud ganan en eficiencia para aprovechar oportunidades"
Vicepresidente Microstrategy

WHITE PAPER

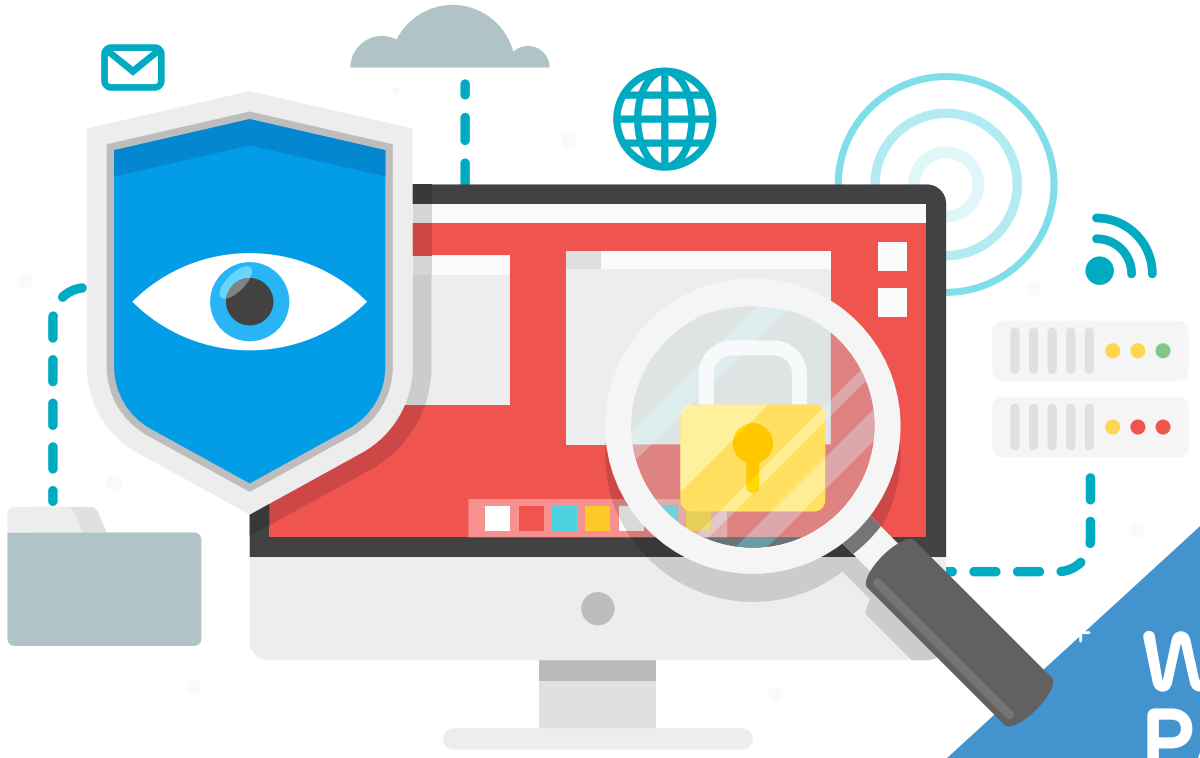
Nuevas tecnologías traen consigo nuevas amenazas y nuevos retos. A medida que los sistemas conectados e internet crecen también las amenazas que buscan acceder a ellos y demostrar sus capacidades.

La digitalización, el trabajo a distancia, el uso de redes diferentes, abren puertas muy jugosas a los hackers. Convivimos con el riesgo, pero no debemos temer a la tecnología por ello.

Los hackers buscan accesos que puedan comprometer a las empresas a través de sus servidores o correos electrónicos encriptando o raptando sus datos. Y sus víctimas pueden ser tanto pequeñas como grandes empresas, aunque cada vez más y por ser menos estrictas en su seguridad las pymes son las víctimas más habituales.

"Según los datos del Instituto Nacional de Seguridad *(Incibe)*, en 2016 se detectaron más de 115.000 ciberincidentes, de los cuales el 70% fueron dirigidos contra medianas y pequeñas empresas."

A priori no existen servidores más o menos seguros, la configuración y los protocolos de seguridad establecidos son los que garantizan su protección. En este ámbito, la nube ofrece un entorno más favorable para establecer garantías de seguridad superiores a gran escala.



WHITE PAPER

Los datacenters que conforman la nube, almacenan volúmenes inmensos de información de numerosas empresas e individuales, y son gestionados por equipos dedicados exclusivamente a garantizar su estabilidad y seguridad. Los servidores locales, sin embargo, requieren de un equipo especializado que los gestione y actualice periódicamente para garantizar su protección. El mayor problema al que se enfrentan las empresas que cuentan con servidores locales, es la falta de recursos dedicados a la gestión de su seguridad, por lo que, en muchos casos, tras una configuración inicial no existen actualizaciones periódicas, lo que incrementa en gran medida su vulnerabilidad ante amenazas.

El auge de las soluciones cloud computing, ha situado a las empresas IT en una posición cada vez más importante en la estrategia de los negocios de las empresas. Mientras la reducción de costes sigue siendo una prioridad clave para la mayoría de las compañías, escalabilidad y agilidad toman cada vez más relevancia. Como resultado, el gasto en soluciones cloud se espera que crezca un 30% entre 2013 y 2018, comparado al 5% del crecimiento de las empresas IT.

"En 2020 la nube dejará de ser pública o privada. Será simplemente la única forma de hacer negocios y desarrollar tecnología." – *IDC*

Todavía muchos CIOs dudan de adoptar una estrategia completamente cloud. Esta duda viene en parte por las inseguridades derivadas del desconocimiento sobre la privacidad y la seguridad.
IT y responsables de negocios necesitan confiar en sus proveedores para cubrir el agujero entre innovación y seguridad. Con las tecnologías adecuadas y procesos, hasta la más compleja empresa puede moverse a la nube con confianza y garantías.

Fuentes:
http://www.revistabyte.es/cloud-computing/toda-la-empresa-la-nube-especial-cloud-computing/
https://www.incibe.es/
https://www.bt.es/img/gestor/informe_idc_beneficios-adopcion-estrategia-cloud-empresa.pdf
http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/digital-enterprise-narrative-final-january-2016.pdf

PRINCIPALES AMENAZAS INFORMÁTICAS

Para entender las garantías que ofrece la nube es importante conocer el entorno que nos rodea, las amenazas a las que nos enfrentamos y como pueden evitarse.

Tendemos a pensar que las amenazas provienen de agentes externos que actúan buscando vulnerabilidades en nuestros sistemas. Sin embargo, la mayor parte de los ciberataques según INCIBE provienen de agentes internos, es decir, empleados de la empresa que abren la puerta a las amenazas a través de emails, descarga de archivos o uso de hardware infectados.

Ambos canales de entrada deben ser tratados con la misma seriedad, prevenir, educar y proteger deben ir de la mano en lo que a ciberseguridad se refiere. Existen multitud de variantes dentro de las amenazas informáticas, sin embargo, podemos **categorizarlas en 5 grupos** en base a origen, impacto y forma de prevenirlas.

01. Descuidos o desconocimiento

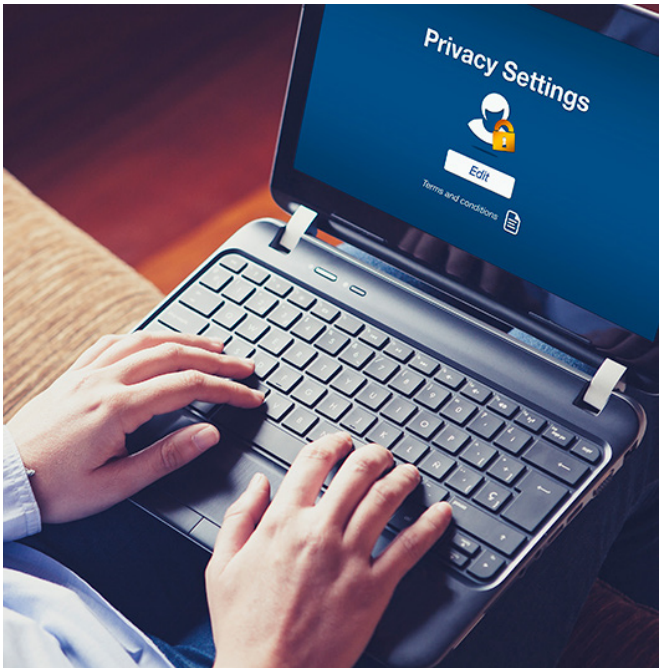
A pesar de no ser de forma intencionada es una de las amenazas más frecuentes en las empresas.

Las amenazas internas son las más habituales, pero también son las más sencillas de prevenir, por tener su raíz dentro de la empresa. Con el avance de las tecnologías y habitualmente aconsejadas por consultores, las grandes empresas han desarrollado fuertes protocolos para impedir errores internos que puedan exponerlas a amenazas.

Sin embargo, las pequeñas y medianas empresas, han tenido que ir aprendiendo sobre la marcha, con pocos o ningún recurso personal en el campo y con escasos recursos económicos para dedicar a la prevención.

La gestión de accesos y permisos es un buen comienzo para prevenir este tipo de ataques, la mayoría de los software y soluciones en la nube ofrecen servicios complementarios para impedir que cualquier empleado se descargue programas o acceda desde redes peligrosas a los sistemas corporativos.

Además, existen servicios adicionales de seguridad, de detección de virus en la descarga de documentos o de análisis del riesgo de los sistemas que garantizan una seguridad extra.



Más información

02. Correo electrónico malicioso

El correo electrónico es el canal de entrada de la gran mayoría de las amenazas.

A través del email los hackers entregan links o documentos infectados con troyanos, virus, spyware y ataques enfocados a obtener información personal.

En este caso es importante contar con un correo electrónico que permita identificar posibles amenazas y alertarnos antes de abrirlos y sea demasiado tarde. Es el caso de Exchange el servicio Advanced Threat Protection detecta las amenazas e informa antes de entregarlo en la bandeja de entrada.

Es también fundamental educar a los empleados para que estén siempre alerta ante emails sospechosos, por ejemplo: Mensajes que no incluyen dirección de e-mail en los campos Para: o CC:, emails con adjuntos, o facturas inesperadas son algunos de los casos más comunes.

Más información

03. Malwares

Programas o códigos informáticos maliciosos cuya función es dañar un sistema o causar un mal funcionamiento del mismo.

Malware es la abreviatura de "Malicious software" y engloba la mayoría de las amenazas externas a las que están expuestos nuestros sistemas: Virus, Troyanos, Gusanos, Spyware, Adware, Hijackers, Keyloggers, Rogues, Ransomwares etc....

El malware destructivo usará herramientas de comunicación populares para extenderse, incluyendo gusanos enviados a través de e-mails y mensajes instantáneos, troyanos que entran a través de páginas Web y archivos infectados por virus descargados en conexiones directas entre usuarios. El malware buscará la manera de explotar las vulnerabilidades del sistema entrando de un modo silencioso y sencillo.

Por supuesto es fundamental la prevención en este caso también, sin embargo, contar con servicios de seguridad que protejan la entrada ahorrará muchos riesgos. El poder de estas amenazas es que se mantienen en constante evolución en busca de no ser detectadas por los antivirus y firewalls. En este ámbito las soluciones en la nube tienen mucho que aportar, gracias a estar conectadas a la red, cuentan siempre con las últimas actualizaciones de seguridad frente amenazas.

04. Phishing

El phishing es básicamente un fraude online, y los phishers no son más que estafadores tecnológicos.

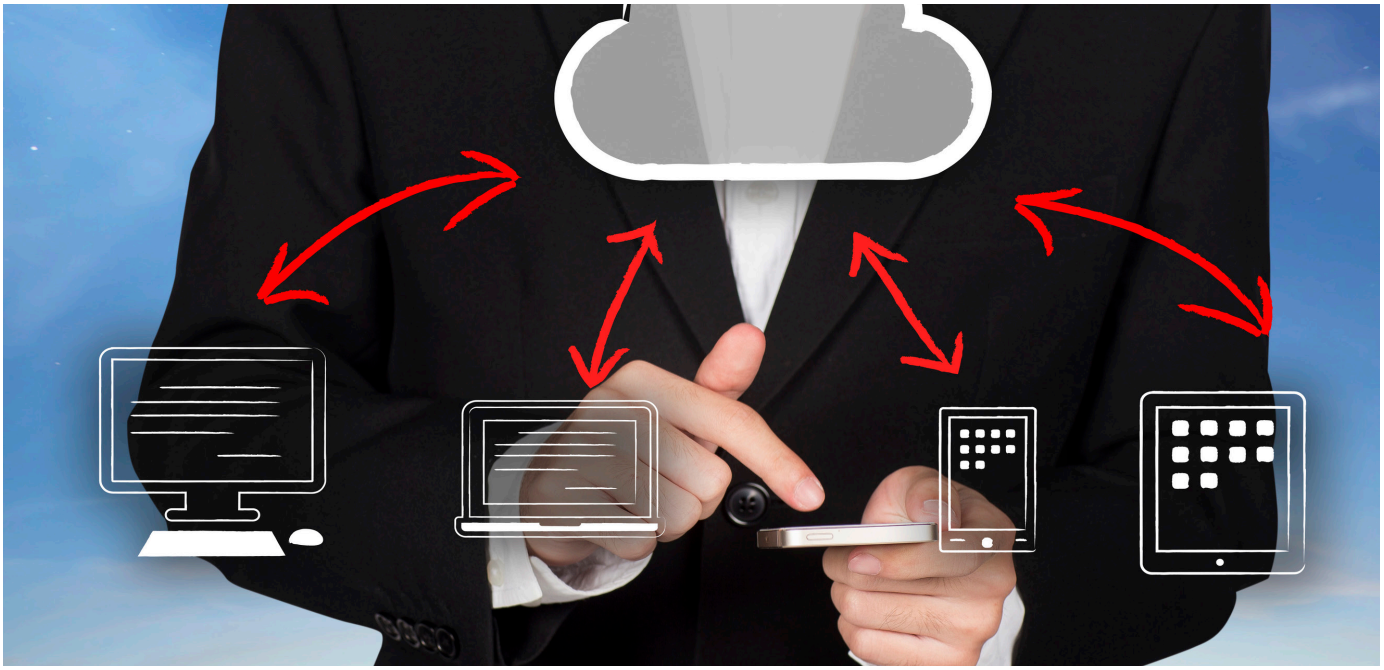
Estos utilizan spam, páginas Web fraudulentas, e-mails y mensajes instantáneos para hacer que las personas divulguen información delicada, como información bancaria y de tarjetas de crédito, o acceso a cuentas personales.

El canal de entrada de los phishers suele ser el buscador, por ello es importante asegurarse de tener activadas las opciones de seguridad en los buscadores.

Una vez entrada la amenaza contar con los protocolos de seguridad en el total del sistema evitará que éste se expanda y corrompa toda la información.

05. Sucesos físicos

Son aquellas amenazas originadas por fallos en el entorno o en el funcionamiento de los hardware.



Se enfrentan a esta amenaza principalmente, los servidores locales, los ordenadores de empresa y los dispositivos de almacenamiento portátil como USB o discos duros.

En general los fallos del sistema permiten recuperar la información almacenada en los discos duros, sin embargo, la exposición de los hardware a sucesos físicos los hace muy vulnerables ante las amenazas de su entorno. Robos, catástrofes, averías en el entorno, como inundaciones o incendios, pueden acabar con toda la información de la empresa de forma rápida y sin retorno.

Aunque la pérdida de los hardware en estos casos es casi inevitable, asegurar la información de los mismos en la nube, es fundamental para no poner en riesgo el futuro de la empresa. Aunque no cuentes con un servidor en la nube, asegúrate de contar con un backup remoto como garantía para la empresa.

Más información

La nube como motor de crecimiento para las empresas

Aunque el nacimiento de las soluciones en la nube se remonta a finales de los años noventa, es ahora cuando la nube se ha convertido en una solución a gran escala, al que todas las empresas e individuos pueden acceder.

Todavía en una fase incipiente de desarrollo, los proveedores de soluciones en la nube deben demostrar y convencer a los clientes de sus posibilidades y ventajas. En muchos casos la nube todavía es un mundo desconocido que genera inseguridades que deben ser suplidas por expertos.

Además de apoyar en el proceso de decisión, las empresas proveedoras de soluciones en la nube, deben ofrecer garantías, datos y protocolos que aseguren su eficiencia y generen confianza.

La nube ofrece a las empresas un entorno flexible, ágil y escalable para almacenar su información. Un espacio gestionado, que garantiza estándares de seguridad mucho mayores a las que ofrece cualquier servidor auto gestionado.

La seguridad informática debe ser una prioridad para las empresas hoy en día. El riesgo que supone un ataque puede en muchos casos comprometer el futuro de las empresas, sobre todo aquellas con menores capacidades y menor poder de reacción.

Además de seguridad, la nube ofrece un espacio óptimo en cuanto a aprovechamiento de recursos y en cuanto a gestión de información, lo que impacta directamente en la mejora de la productividad y la eficiencia de los equipos.

Más información aquí

SOBRE PRODWARE:

Prodware España, perteneciente al grupo francés Prodware, está especializada en el diseño, puesta en marcha y mantenimiento de soluciones de tecnología aplicadas a la mejora de procesos de negocio.
La compañía es el primer Partner de Microsoft Dynamics en España y Europa y uno de los tres primeros Partners en el mundo.

WHITE PAPER