Las nuevas funcionalidades hacen que la MFA y el cifrado sean accesibles para las pymes mientras la nueva directiva de protección de datos supone un reto para las empresas europeas

Un white paper de IDC
patrocinado por ESET
febrero 2017

autor: Alexei Proskura
Mark Child

IDC
Analyze the Future

La opinión de IDC

Existen limitaciones obvias para los recursos que las pequeñas y medianas empresas (pymes) pueden asignar a la seguridad, siendo ya bastante duro para ellas gestionar la informática en general. Al mismo tiempo, el mercado está experimentando un cambio en el centro de atención desde la infraestructura en sí a la seguridad de la información, puesto que el perímetro desaparece y la información se hace omnipresente. Los dispositivos móviles/múltiples se añaden a la complejidad de la informática y la seguridad. Estos desarrollos están provocando la necesidad de las pymes de reevaluar y actualizar sus estrategias en el campo de la informática y la seguridad.

Para hacer frente a los retos que plantea la seguridad de la información, hay que tener en cuenta dos elementos clave: 1) la gestión del acceso de los usuarios, que se basa en una autenticación fiable de los usuarios; y 2) la protección de la información, tanto para la información en reposo como en tránsito, incluyendo el caso de haber sido puesta en peligro.

1. De las violaciones de datos confirmadas, el 63% se atribuye a contraseñas robadas u obtenidas sin autorización (DBIR, 2016), lo cual indica la necesidad imperiosa de un factor de autenticación adicional o alternativo. Sin embargo, la plantilla típicamente reducida del departamento de sistemas de las pymes convierte la carga adicional de la gestión de la autenticación en una barrera a la hora de implementarla en muchas de esas empresas. Cualquier propuesta de solución debe contener la promesa de ser fácil de usar y consumir el mínimo de recursos del departamento.
2. Una opción es la anonimización de la información y otra el cifrado: ambas tienen sus pros y contras. La anonimización es un buen enfoque pero puede ser derrotada mediante la correlación de información de múltiples fuentes. El cifrado resuelve este inconveniente, pero al menos hasta hace poco, se consideraba algo demasiado complejo y caro para la mayoría de Pymes. Con la implantación de la nube, este ya no es el caso.

La amplia oferta de servicios en la nube a precios asequibles, el menor coste de los *smartphones* y *tablets*, y los avances en tecnologías de seguridad están cambiando el escenario de operaciones de las pymes. Es el momento de acceder de nuevo a tecnologías de seguridad que en otro tiempo eran inalcanzables debido a los costes de adquisición y/o mantenimiento y a los requisitos para proporcionar soporte.

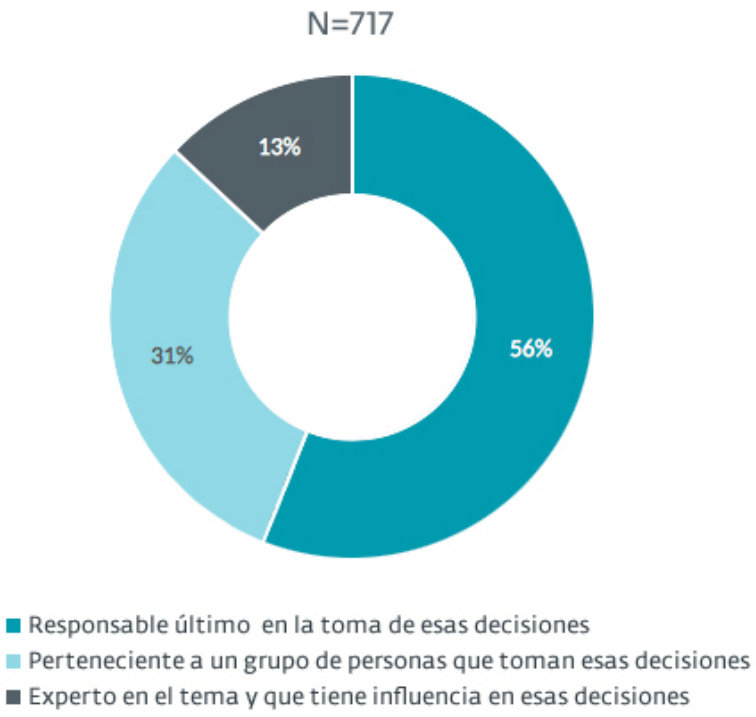
Metodología

El informe de IDC se basa en los resultados de un extenso trabajo de campo y la realización de encuestas a más de 700 empresas en siete países europeos: República Checa, Alemania, Italia, Holanda, Eslovaquia, España y el Reino Unido. La encuesta se centró en pymes con un rango de 50-499 equipos a proteger en distintos sectores. Los encuestados de nivel C, seguridad, administradores de sistemas o puestos de dirección respondieron sobre un amplio rango de temas relacionados con la seguridad incluyendo las soluciones de protección de equipos implementadas o deseadas en su empresa, las regulaciones que les afectan, las medidas tomadas para mejorar la seguridad de la información, las barreras para mejorar sus medidas de seguridad, la actitud frente al uso de la nube para la seguridad, y el impacto de cualquier violación de seguridad sufrida.

GRÁFICO 1

Participación del encuestado en las decisiones de seguridad informática

P. ¿Cómo describirías mejor tu grado de participación en las decisiones de seguridad informática que afectan a tu empresa?



Fuente: IDC, 2017

En este *white paper*

El entorno actual de la seguridad de la información cada vez supone un reto mayor para las empresas, que deben adaptarse a una legislación cambiante al tiempo que protegen unos activos de información cada vez mayores y más dispersos frente una diversidad creciente de amenazas. Las empresas se enfrentan a decisiones difíciles sobre cómo priorizar sus inversiones en seguridad, cómo cumplir las directivas de la mejor forma posible y cómo reaccionar cuando ocurren incidencias de seguridad.

Este *white paper* se centra en las soluciones de seguridad de la información que las empresas europeas están implementando y los criterios que utilizan para seleccionarlas, los retos a los que se enfrentan al seleccionarlos para mejorar su nivel de seguridad, y su nivel de conocimiento y concienciación de los riesgos y amenazas. El estudio está basado en un amplio trabajo de campo en Europa, así como en la información e investigación existente de la consultora IDC en los campos de seguridad de la información, procesos y tecnologías de seguridad, el panorama de las amenazas y los marcos regulatorios.

Resumen de la situación

Cambios en la metodología de trabajo

Según un informe de *The European Business Review*, están ocurriendo cambios demográficos en el lugar de trabajo que cada vez afectarán a más empresas. Las empresas deberían prepararse para la generación que valora "las multitareas, el papel de la tecnología y de estar conectado, la conciliación laboral y la conciencia social." [1] Esto significa que para atraer a futuros talentos, las empresas deben ser capaces de satisfacer los nuevos requisitos de los empleados que, a su vez, implican más movilidad, múltiples dispositivos y la eliminación del perímetro en la empresa.

Desaparición del perímetro

Según el informe sobre Investigaciones en brechas de seguridad 2016 realizado por Verizon (DBIR, 2016), el 63% de todas las brechas de seguridad confirmadas en 2015 tenían como elemento común contraseñas predeterminadas, débiles o robadas[2]. En términos más simples, esto significa que se han eludido los perímetros de defensa. Este grupo de controles de seguridad valiosos no debería descartarse, pero ya no es suficiente con proteger la empresa. La gestión de la identidad y el acceso - que cubre áreas como la autenticación avanzada, la gestión de usuarios, el control de acceso, la gestión de perfiles y permisos de administración - está sobrepasando a las defensas perimetrales en importancia.

La seguridad de la información es el centro de atención

La infraestructura ya no es el objetivo principal de los cibercriminales. Aunque usarán con total seguridad cualquier dispositivo al que tengan acceso, ahora buscan básicamente información, que es más fácil de monetizar. Varios factores están haciendo la seguridad de la información algo mucho más desafiante en el entorno actual:

- Los vectores de amenazas pagados por los estados han entrado en escena con grandes recursos. La organización, destreza técnica y enfoque estratégico de estos grupos pagados por el Estado hace que sea excesivamente difícil para la mayoría de empresas defenderse de sus ataques sofisticados.
- Según el informe DBIR, el volumen de malware desconocido sigue siendo alto, al tiempo que siguen descubriéndose nuevas vulnerabilidades. Hasta que se creen e implementen firmas y parches para estos, las empresas continuarán luchando para proteger sus equipos e información contra esos exploits. Mientras tanto, las vulnerabilidades conocidas siguen siendo aprovechadas y son la causa de una gran proporción de violaciones de datos.
- La disponibilidad de marcos de exploits automatizados continúa creciendo, permitiendo que incluso atacantes con experiencia limitada lleven a cabo ataques cada vez con más frecuencia, extensión o intensidad. Cada vez más empresas se convierten en objetivo, una empresa ya no puede considerarse segura debido a su tamaño o tipo de sector al que pertenece.

Como consecuencia, si la información es sensible, el enfoque pragmático es asumir que los sistemas de la empresa podrían haberse puesto ya en riesgo o podría suceder en cualquier momento. Aquí es donde entra el cifrado al rescate. Implementar una solución de cifrado apropiada beneficiará a cualquier empresa, pero el cifrado es complicado de gestionar, especialmente para pymes, y la experiencia es cara. El cifrado también es

1 http://www.europeanbusinessreview.com/demographic-workplace/

2 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

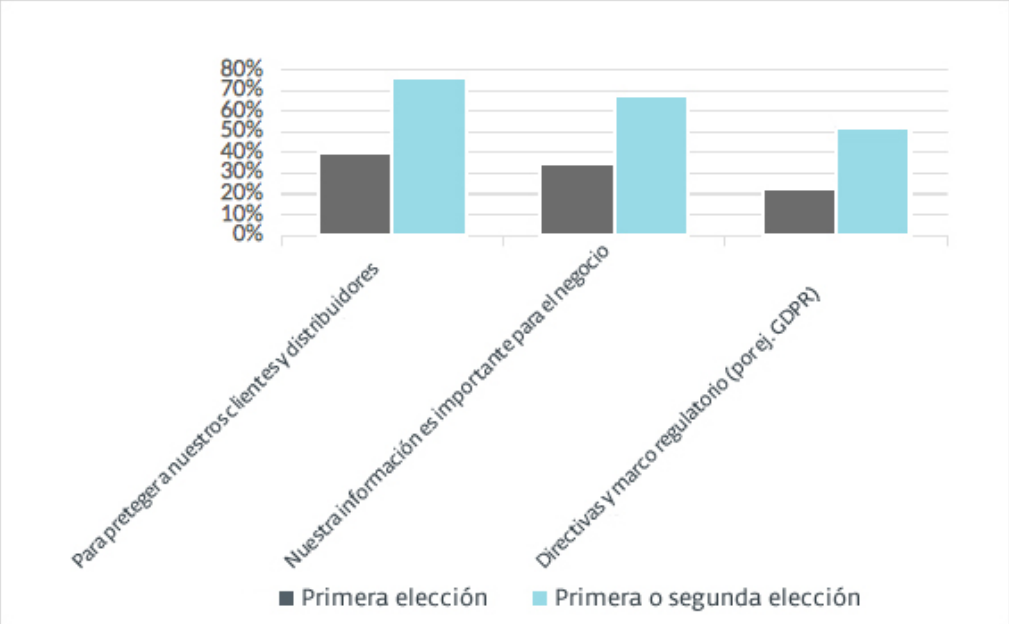
complejo desde el punto de vista del usuario, puesto que a menudo requiere un conocimiento básico de la tecnología. Las aplicaciones de código abierto tienden a ser más seguras pero no suelen ser muy amigables para el usuario, puesto que se asume que serán adoptadas por usuarios con un amplio conocimiento y capacidades técnicas.

Los datos de la encuesta de IDC demuestran que las pymes europeas están tomando las medidas adecuadas para proteger su información y las razones que las llevan a ello (ver Gráfico 2 a continuación). Proteger a los clientes y distribuidores es por supuesto primordial para continuar el éxito y la supervivencia de cualquier entidad, pero las empresas también reconocen cada vez más el valor empresarial de su información y son conscientes de los marcos legislativos cada vez más amplios a los que deben adecuarse y las multas derivadas de no hacerlo.

GRÁFICO 2

Motivos para proteger la información

P. ¿Qué hace que tu empresa evite el acceso no autorizado a la información?



Fuente: IDC, 2017

El panorama regulatorio

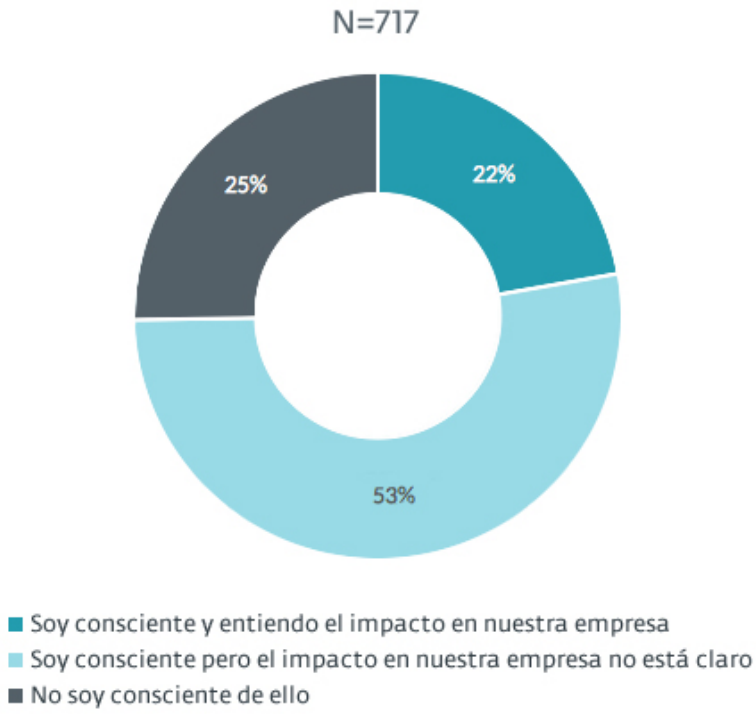
Mientras se establecen regulaciones para imponer más control sobre cómo se maneja la información, la mayoría tienen que ver sobre la información privada. La amplia disponibilidad y la creciente facilidad de acceso a la tecnología de *big data*, especialmente su aplicación en la nube, ha permitido que las pymes proporcionen servicios analíticos a clientes más grandes. Estas empresas deberían prestar más atención a la protección de datos, al estar también sujetas a los marcos regulatorios de protección de la privacidad de la información y al

tratar con grandes volúmenes de información privada. Sin embargo, a estas empresas a menudo les falta la experiencia apropiada para proteger su información.

En términos regulatorios, la mayor parte de los encuestados mencionó el estándar de seguridad de la información de la Industria de pagos por tarjeta (PCI, en inglés) como algo que afectaba a su empresa (46%). El Reglamento general de protección de datos de la UE (GDPR) y la Directiva de seguridad de las redes y sistemas de información (Directiva NIS) les seguían con el 37% y el 36%, respectivamente. La GDPR ha tenido una fuerte cobertura en los medios y en conferencias y seminarios en el pasado año, y a pesar de ello un 53% de los encuestados aún afirman que el impacto en su empresa no está claro, mientras que un cuarto de ellos no era en absoluto consciente de ella (ver Gráfico 3). De los que afirman ser conscientes de la GDPR, el 20% aseguran que ya están preparados, el 59% que están trabajando en ello, y el 21% reconoce que no está en absoluto preparado para ello (ver Gráfico 4).

GRÁFICO 3

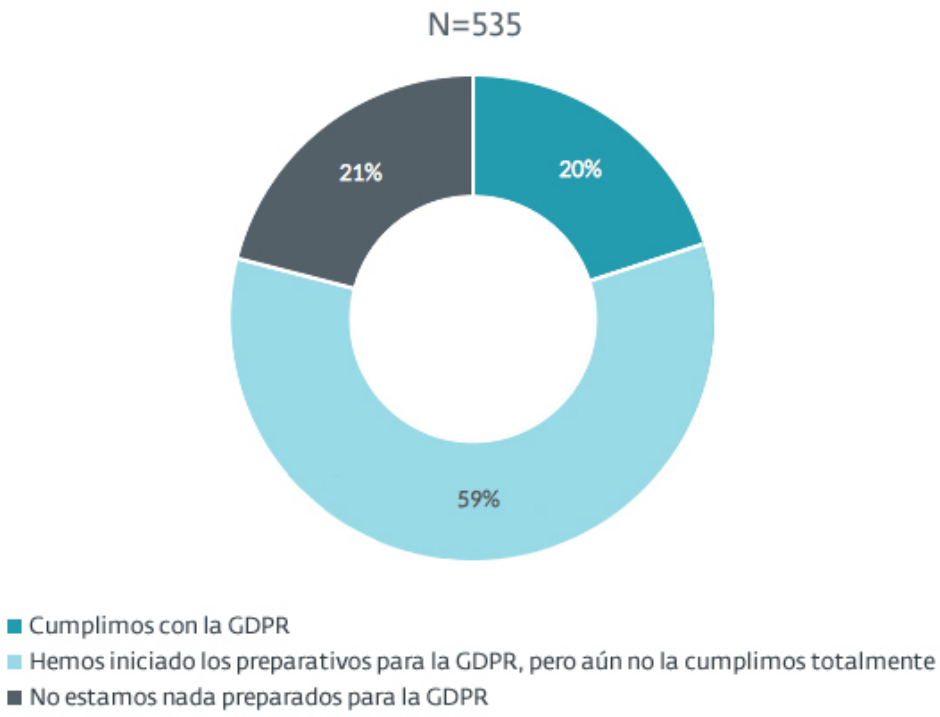
¿Cuál es tu conocimiento de la GDPR?



Fuente: IDC, 2017

GRÁFICO 4

Estado de los preparativos para la GDPR dentro de las empresas



Nota: solo encuestados que confirmaban conocer la GDPR en la pregunta anterior

Fuente: IDC, 2017

Las tecnologías de prevención de fugas de información (DLP) a menudo se perciben como una solución infalible para la protección de datos por las empresas que buscan adaptarse al nuevo marco regulatorio. Sin embargo, esta percepción puede ser engañosa, porque el DLP requiere tecnologías adicionales como la autenticación y la clasificación de información para ser totalmente eficaz. Puede parecer contradictorio pero, dependiendo de la idiosincrasia de cada empresa, una autenticación más fuerte (por ej., múltiples factores de autenticación) o el cifrado pueden ser controles de seguridad más rentables y también proporcionar ventajas de productividad adicionales (por ej., permitir la movilidad de los empleados).

La seguridad clásica para equipos no es suficiente para la protección de datos

Como era de esperar, las soluciones antivirus y antimalware obtuvieron la mayor tasa de penetración (84%) en todos los países encuestados (ver Gráfico 5 a continuación), seguidos del cortafuegos en el host (68%). Sin embargo, muchas empresas reconocen que su producto antimalware existente no es suficiente en el entorno actual de amenazas, y la mitad de los encuestados citaba esto como su área más importante a añadir o mejorar. Dentro del campo de las soluciones antimalware, muchos fabricantes están llevando a cabo mejoras cualitativas en sus tecnologías, al tiempo que están entrando en el mercado nuevos fabricantes desafiando a los ya establecidos. Las tendencias recientes en malware (como el aumento de los ataques de ransomware) están forzando a las empresas a reconsiderar sus defensas antimalware, y muchos están considerando actualizar o

complementar sus soluciones existentes. La mayor preocupación respecto a los cortafuegos es que los atacantes y exploits utilizan los puertos que están abiertos debido a requisitos operativos, como los que se utilizan para permitir el tráfico web. Esto provoca la necesidad de mover las defensas más profundamente hacia la infraestructura y más cerca de los datos en sí.

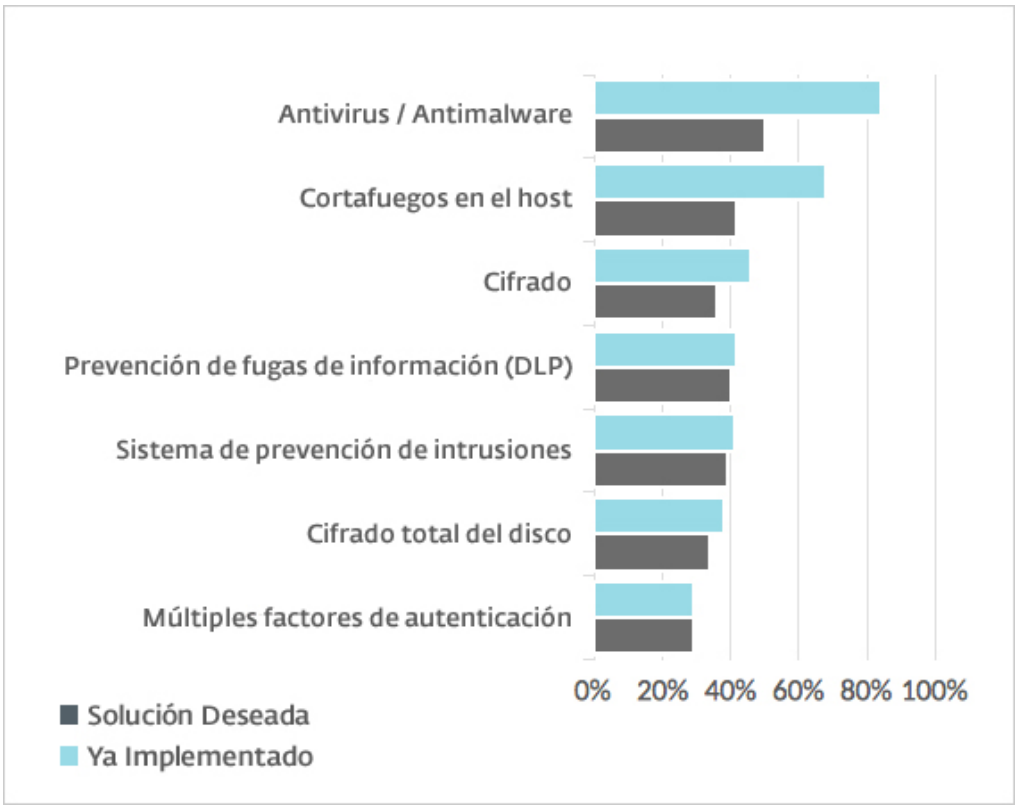
El cifrado y el control de acceso proporcionan los medios mediante los cuales pueden solucionarse estos retos, aunque la mentalidad clásica descrita anteriormente continúa dominando la planificación de la seguridad.

GRÁFICO 5

Soluciones de seguridad implementadas o deseadas por las empresas

P6. ¿Qué soluciones de seguridad para equipos se utilizan en tu empresa?

P7. Garantizando la aprobación presupuestaria, ¿qué tres soluciones de seguridad implementarías o mejorarías?



Fuente: IDC, 2017

Esta “creencia clásica” evita que las empresas tomen los pasos necesarios para mejorar el nivel de seguridad de su información, y también requiere una cuota de los recursos financieros para que estos pasos puedan tomarse.

Uno de los primeros pasos debería ser la implementación del Múltiple factor de autenticación (MFA), que funciona como medio para compensar las debilidades de la protección basada en contraseñas (como el requisito

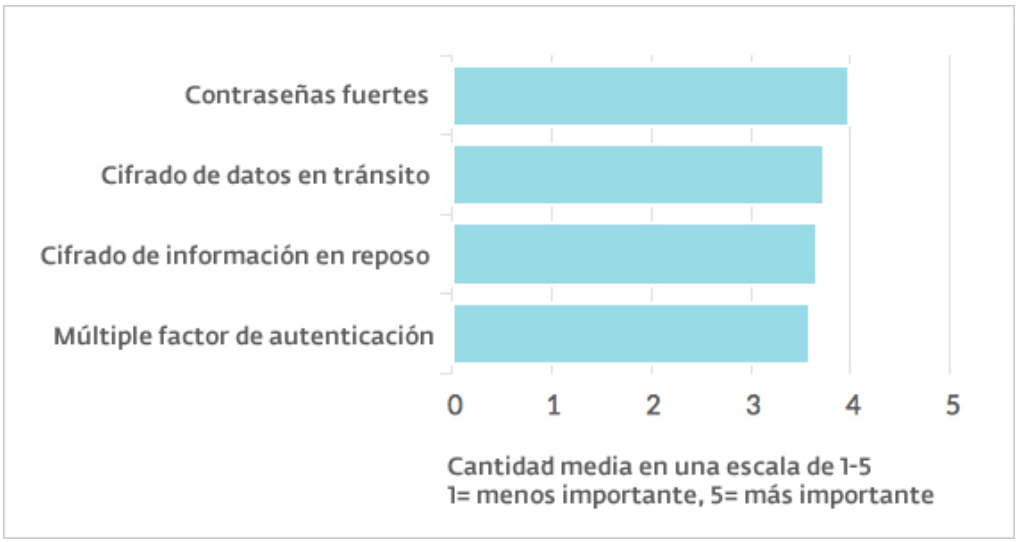
de los usuarios de memorizar cierta cantidad de contraseñas fuertes/complejas). La MFA hace que sea más difícil para los atacantes poner en peligro la identidad del usuario (por ejemplo, cuando se emplea un segundo dispositivo como uno de los factores). Esto sirve como función dual, ya que la MFA protege a nivel de inicio de sesión y a nivel de la aplicación, protegiendo así la información allí contenida. Como se ha señalado anteriormente en este *white paper*, las contraseñas en peligro son la causa de un 63% de las violaciones de datos, y por ello la MFA tiene un potencial significativo para reducir este tipo de incidencias.

Otro medio adicional de proteger la información es cifrarla, dejándola ilegible para cualquiera que la haya robado y que no tenga el medio de descifrarla. Las claves de cifrado se almacenan a menudo como parte del registro de identidad del usuario, que está disponible solo después de que el usuario se haya autenticado con éxito. Esto refuerza más el caso de MFA, puesto que combinar estas tecnologías mejora el nivel general de protección de la información, añadiendo capas de defensa que se solapan y refuerzan la eficacia de los controles de seguridad aislados.

Por tanto, existe claramente demanda del mercado de soluciones que amplíen las ventajas del cifrado y el múltiple factor de autenticación a las pymes que no cuentan con los mismos recursos que sus homólogas grandes. Sin embargo, existen más trabas a superar, la primera de las cuales aparece destacada en el Gráfico 6 a continuación:

GRÁFICO 6

Importancia de controles específicos para la protección de datos



Fuente: IDC, 2017

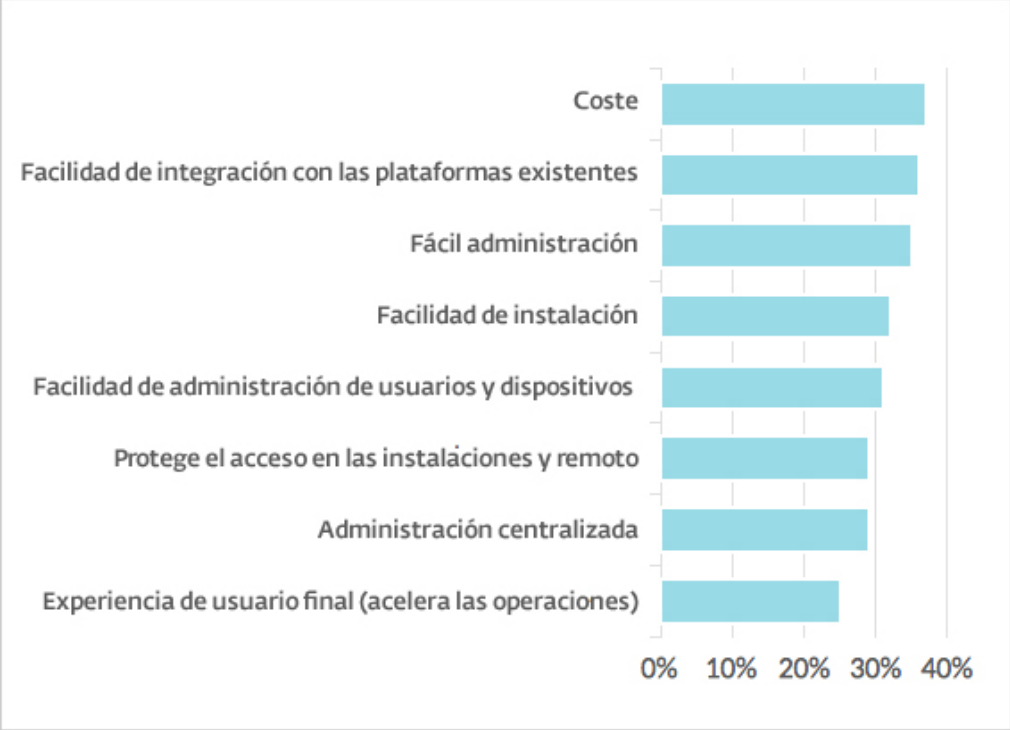
La protección de datos es un área compleja y el enfoque que cada empresa toma para solucionarlo depende de consideraciones empresariales que dependen de cada organización. Sin embargo, tal y como indica el Gráfico 6, las empresas aún depositan una gran confianza en el sistema de contraseñas que, a pesar de los mejores

esfuerzos y buenas prácticas, no proporciona el mismo nivel de protección que el que pueden proporcionar la combinación de MFA y el cifrado. Como consecuencia, no existe sentido de urgencia o necesidad de invertir en estas soluciones, y se requiere un esfuerzo en formación de parte de los fabricantes y expertos en seguridad para subrayar a los usuarios finales cómo pueden marcar estas tecnologías una diferencia significativa a su nivel de seguridad. IDC cree que debería prestarse mucha más atención a la MFA como un elemento fundamental para mejorar tanto la seguridad de la información como la de los equipos.

Según los datos de la encuesta, un criterio de selección importante es el coste. Como puede observarse en los Gráficos 7 y 8 siguientes, esta es una consideración crítica tanto para la MFA y el cifrado. Como se observa anteriormente, las empresas continúan dedicando una cuota significativa de su presupuesto de seguridad a tecnologías que: 1) ya han implementado, y 2) son familiares tanto en términos de uso de la tecnología y los beneficios que proporciona. Hasta la fecha, ha habido una disponibilidad de mercado limitada tanto de las soluciones MFA o de las de cifrado que son asequibles desde el punto de vista de un presupuesto de seguridad de una pyme estándar, puesto que la mayoría de las soluciones están pensadas para grandes empresas. Además, hay costes adicionales asociados con el mantenimiento de estas soluciones.

GRÁFICO 7

Criterios de selección para el Múltiple Factor de Autenticación (MFA)



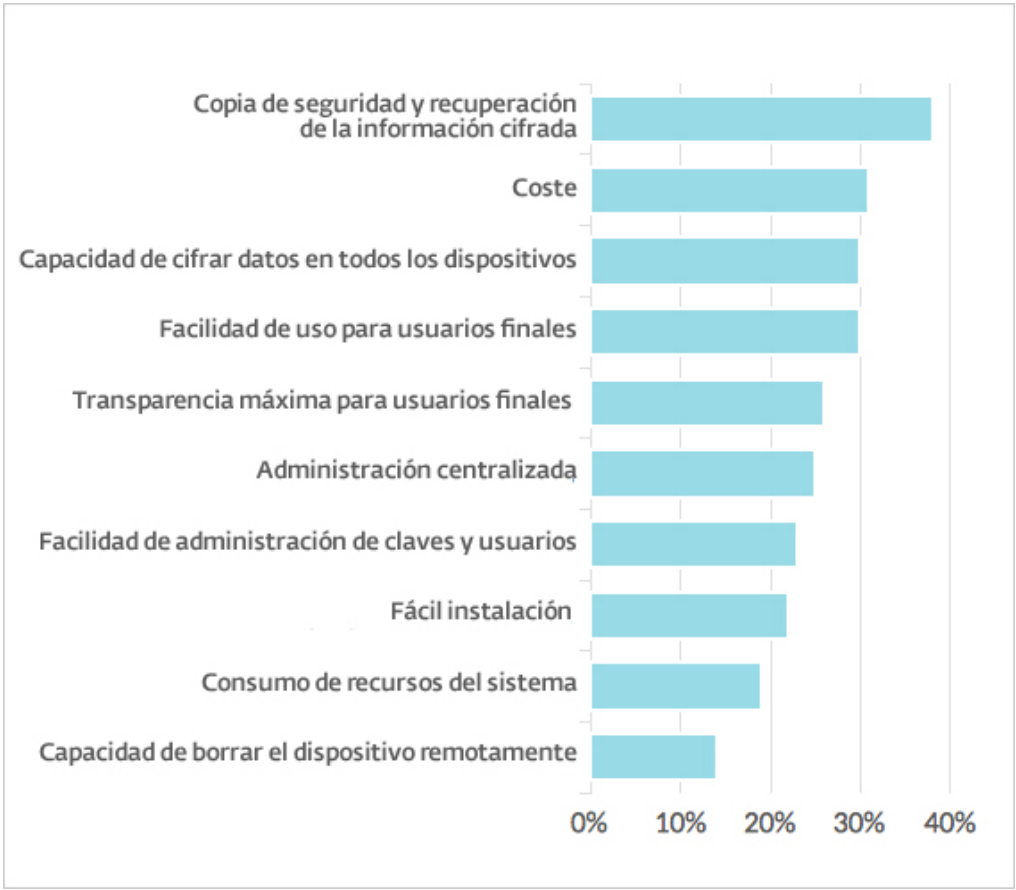
Fuente: IDC, 2017

El tercer criterio asociado con el múltiple factor de autenticación es la facilidad de uso. Al igual que con el cifrado, este es un reto con muchos aspectos que incluye la facilidad de uso desde la perspectiva tanto de los

usuarios finales como de los administradores del producto. Los criterios de selección para MFA y el cifrado son ligeramente diferentes, como puede comprobarse en los gráficos 7 y 8. Según la encuesta, las prioridades de MFA se centran más alrededor de la administración de la solución y la integración de la solución con plataformas que ya están en uso. Esto se puede explicar fácilmente, puesto que todos los beneficios de la MFA son más perceptibles cuando la tecnología se utiliza en todo el lote de aplicaciones (esto es, en las capas del sistema y aplicaciones).

GRÁFICO 8

Criterios de selección para el cifrado



Fuente: IDC, 2017

Al fijarse en los criterios de selección para el cifrado aparece una imagen ligeramente diferente. Aunque el coste sigue siendo uno de los factores más importantes, el coste se queda en segundo lugar en comparación con la copia de seguridad y recuperación. Ciertamente, la copia de seguridad de la información cifrada y su posterior recuperación contienen diversos retos, siendo el más importante la administración de claves. Una práctica común es asignar una fecha de expiración de claves y, como consecuencia, es importante o bien mantener la clave si ha sido usada para realizar la copia de seguridad de la información, o cifrar de nuevo la copia de

seguridad con una nueva clave, lo cual no siempre es factible y ciertamente no muy práctico. La situación es más complicada por la revocación de claves por cualquier motivo, incluyendo la pérdida del dispositivo o del medio que contiene la clave.

El reto de la facilidad de uso ha sido relacionado firmemente con la criptografía durante muchos años. Existe una percepción general del usuario que la criptografía es una de las tecnologías más difíciles de implementar y mantener. Trabajar con información cifrada supone que el remitente puede cifrar la información y que el destinatario puede descifrarla sea cual sea el dispositivo con el que están trabajando y de la forma más sencilla posible, de forma ideal sin ninguna interacción adicional del usuario que la solicitud de cifrar la información. Esta percepción la corroboran las respuestas de la encuesta acerca de los criterios de selección. Es de gran importancia entender que la complejidad de la administración para cualquier solución de cifrado consiste en diversas partes, y todas ellas deberían ser atendidas por los fabricantes para hacer que sus soluciones sean atractivas.

Si el punto de vista de la facilidad de uso para la MFA está en la parte de la administración de la solución, para el cifrado este punto de vista se centra en el usuario. La transparencia y la capacidad de cifrar la información en todos los dispositivos son más importantes para la adopción del producto, aunque esto no signifique que la facilidad de la instalación, implementación y la administración de usuarios y claves no sean importantes.

El orden de criterios de selección simplemente refleja el hecho de que los usuarios no usarán el cifrado si no están seguros de si el destinatario puede descifrar la información o si existen otras posibilidades para la información indescifrable. Las empresas también destacaron la importancia de la capacidad de cifrar información en todos los dispositivos, lo cual se está convirtiendo en algo vital en el mundo empresarial actual donde la mayoría de usuarios utilizan al menos dos dispositivos activamente (PC y *smartphone*).

La oferta de ESET

ESET es un fabricante de seguridad informática de Eslovaquia que se ha convertido en una fuerza en el mercado mundial con su suite de protección para equipos. El fabricante afirma que su objetivo es garantizar que todo el mundo, desde consumidores particulares a grandes empresas, puedan beneficiarse de las oportunidades y protección que la tecnología ofrece. Como muchos otros fabricantes antimalware, ESET ha reconocido que existe una oportunidad significativa de proporcionar una protección más robusta y exhaustiva a sus clientes, y ha ampliado su oferta. El fabricante ha adquirido recientemente dos empresas (FireID para autenticación y DESlock para el cifrado), y ha trabajado intensamente para integrarlas en su cartera de productos. En particular, estas adquisiciones permiten a ESET proporcionar múltiple factor de autenticación y cifrado a precios atractivos para las pymes –un segmento que no ha sido tenido en cuenta hasta ahora-. Sin embargo, estas soluciones también son suficientemente escalables para satisfacer las necesidades de grandes empresas.

Como puede observarse, ESET es un fabricante antimalware establecido con soluciones que protegen equipos y servidores. Como complemento se encuentran ahora la oferta de MFA y el cifrado, que mejoran significativamente la defensa añadiendo otras dimensiones, como se detalla a continuación.

Múltiple factor de Autenticación

ESET Secure Authentication

La solución de autenticación de ESET incorpora diversos principios importantes que solucionan de forma apropiada las preocupaciones del mercado señaladas en la sección anterior. Diseñado para una fácil instalación

(tan solo unos minutos), este producto reduce el número de incidencias potenciales de instalación, no solo comprobando la preparación del sistema, sino también proporcionando soporte a los usuarios si necesitan instalarse nuevos componentes. Además, el proceso de instalación detecta automáticamente las aplicaciones instaladas que pueden beneficiarse de ESET Secure Authentication. Esto incluye la ventaja de estar basada en la web, el acceso remoto y las aplicaciones de servicios en la nube, así como inicios de sesión lógicos.

ESET Secure Authentication se implementa en las instalaciones y puede integrarse directamente con plataformas existentes a través de la API o mediante un módulo de autenticación personalizado desarrollado con módulos de soporte del SDK disponible desarrollado en Java, PHP, y .NET. Las posibilidades de integración se amplían más con la compatibilidad con los Servicios de la Federación de Directorio Activo (ADFS, en inglés), implicando servicios como Office 365, aplicaciones de Google o cualquier otro servicio compatible con la integración de ADFS que pueda beneficiarse de ESET Secure Authentication.

ESET Secure Authentication favorece las plataformas móviles, en las que el software requerido puede instalarse fácilmente, y con la capacidad de proporcionar contraseñas de un solo uso (OTPs) mediante los servicios de datos y SMS. Aunque la adopción de la solución MFA de ESET no requiere ningún hardware adicional, proporciona flexibilidad operacional adicional al ser compatible con los módulos hardware de OTPs.

Otra característica que merece mención especial es la autenticación por pulsación. Este tipo de autenticación mejora la usabilidad de MFA evitando que los usuarios vuelvan a teclear las OTPs (enviadas por SMS o generadas por una aplicación móvil desde su dispositivo móvil) ante una petición de inicio de sesión. También soluciona los problemas de seguridad de la autenticación fuera-de-banda que aparecen en relación con los servicios sin cables (OTA) basados en SMS. La autenticación impulsada está disponible como parte de la oferta móvil del producto y es compatible con dispositivos Android e iOS, y también ponibles.

Los retos de la MFA

La integración con Active Directory es un requisito para la implementación de ESET Secure Authentication con Linux, Mac y Windows. En el momento de escribir este informe, el producto no incluye oferta en la nube: la autenticación en la nube la proporciona Active Directory y ESET MFA a través de ADFS, aunque la MFA aún no la proporciona en forma SaaS.

Cifrado

Solución de cifrado DESlock de ESET

La solución de cifrado DESlock de ESET está específicamente diseñada con los clientes pymes en mente, aunque esta solución puede ser fácilmente escalada para adaptarse a entornos empresariales internacionales. DESlock proporciona capacidades completas de copia de seguridad y recuperación como parte de la administración remota completa, que también permite a los administradores eliminar el acceso remotamente a todo el sistema o a cierta información específica. Además, el producto puede decidir si la información debería ser accesible a los administradores o no legible para nadie si el sistema está, por ejemplo, perdido para siempre. La oferta de DESlock se divide en tres ediciones que aumentan gradualmente la capacidad de aplicar el cifrado, desde objetos comunes de la empresa como archivos, carpetas, ficheros y correo electrónico, hasta dispositivos extraíbles y discos completos. Esta división gradual en tres ediciones permite que las pymes elijan la versión que más se adapta a sus necesidades y no paguen de más por las características que no utilizan.

También existe una oferta para móviles y puede utilizarse o bien en modo sin administrar (cuando el dispositivo no está administrado por la política de DESlock Enterprise Server de ESET) para lo cual solo está disponible en cifrado basado en contraseñas (y no en claves), o el modo administrado, donde la administración de claves y la aplicación de políticas la realiza Enterprise Server. Los dos modos de cifrado móvil de DESlock permiten a las empresas aumentar sus prácticas de seguridad manteniendo el programa en el dispositivo en sí, simplificando así su implementación. Lo que hace la oferta de ESET particularmente atractiva es el hecho de que Enterprise Server es gratuito para cualquier empresa con cinco o más licencias de Endpoint.

El cifrado de DESlock también ha ido evolucionando para solucionar las preocupaciones de facilidad de uso de los usuarios. Este programa está diseñado para que requiera la mínima interacción posible durante el uso de claves. Las claves se combinan en grupos y se asocian con grupos de usuarios haciendo que la administración de claves sea transparente para el usuario, mientras que la clave de recuperación que se genera simultáneamente con la clave de usuario y la copia de la clave del usuario del lado del servidor, garantizan la capacidad de copia de seguridad y recuperación de la misma.

Esta redundancia hace que el descifrado de información sea posible incluso en casos donde los usuarios han perdido sus claves junto a sus dispositivos. La capacidad del usuario de interactuar con la clave es limitada, reduciendo así la posibilidad de un error humano (por ej., cuando un usuario cambia accidentalmente la clave). Otro esfuerzo para mejorar la usabilidad se centra en la integración del cifrado de DESlock con otras aplicaciones de empresa. La integración con Microsoft Outlook, por ejemplo, se ejecuta en forma de barra de herramientas, lo cual contribuye además a la facilidad de uso para el usuario.

Los requisitos de Enterprise Server en cuanto a su administración son estándar, necesitando la plataforma Microsoft Windows que ya utiliza la mayoría de la audiencia potencial de ESET. La consola web de administración garantiza una curva de aprendizaje reducida en términos de administración de políticas y claves. Además, se puede acceder remotamente a la consola en casos donde el administrador de seguridad no está disponible a tiempo completo en las instalaciones. Este producto ha sido validado con FIPS 140-2 y es capaz de usar varios algoritmos de cifrado, incluyendo AES con longitud de claves para 128 y 256 bits.

Retos del cifrado

En general, la solución de cifrado DESlock de ESET es un paso más para hacer que la seguridad - antes solo accesible para grandes empresas- sea accesible para las pymes. Existen, sin embargo, diversos factores que deberían considerarse al evaluar el producto. Aunque DESlock combina de forma inteligente la criptografía de claves públicas y simétricas para eliminar la complejidad de la experiencia de usuario, aún existen retos tradicionales asociados con el uso de criptografía que necesitan recordarse. Algunos ejemplos serían garantizar que la clave esté disponible para descifrar información de una copia de seguridad realizada hace mucho tiempo, o minimizar las copias de información sensible y aplicar el cifrado a todas las demás copias. Aunque estos y otros principios de buenas prácticas no son exclusivos del producto ESET y son igualmente aplicables a cualquier solución de cifrado, los usuarios no deberían perder de vista el hecho de que las prácticas y procesos alrededor del cifrado son tan importantes como la seguridad de los canales de intercambio de claves y el almacenamiento de éstas.

En el momento de escribir este artículo, el cifrado móvil de DESlock solo está disponible para iOS, con una versión para Android en desarrollo.

Conclusión

El nivel de penetración en el mercado del múltiple factor de autenticación y el cifrado de información permanece bajo entre las pymes europeas. Parecen haber unas pocas razones para esto, con el alto coste en la parte alta de la lista, mientras que también existen preocupaciones sobre la facilidad de uso, facilidad de administración y de integración con las plataformas existentes. En el caso de las plataformas de cifrado, las empresas también destacaron la importancia de la capacidad de cifrar datos en todos los dispositivos.

- Las empresas afirman que están preocupadas por la protección de datos, aunque citan las contraseñas fuertes como el control más importante por delante del múltiple factor de autenticación y el cifrado de datos en reposo o en tránsito.
- El coste aparece destacado como criterio clave al elegir una solución para MFA o cifrado. Por una parte, esto supone un reto, puesto que las empresas aún se están centrando en el balance y no en lo que es mejor para su empresa. Por otra parte, presenta una oportunidad para cualquier fabricante con una oferta asequible para una cuota de mercado sin explorar hasta la fecha.

La oferta de ESET, en concreto la combinación de tres tecnologías de seguridad compatibles por un fabricante de seguridad con una larga trayectoria, abre la posibilidad de que las Pymes mejoren de forma significativa su nivel de seguridad, no solo en términos de protección de la información, sino también a nivel más amplio de la infraestructura del sistema. El paso siguiente es que el fabricante comunique este desarrollo al mercado y ayude a las empresas a darse cuenta de los pasos necesarios para integrar estas tecnologías - que ESET ha hecho más accesibles- en su infraestructura y procesos de la empresa.

Sobre IDC

International Data Corporation (IDC) es el mejor proveedor global de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnologías de la información, telecomunicaciones y consumidores. IDC ayuda a los profesionales de las tecnologías de la información, ejecutivos de empresa y la comunidad de inversores a tomar decisiones basadas en hechos sobre compras en tecnología y estrategias de negocio. Más de 1.100 analistas en IDC proporcionan experiencia global, regional y local sobre tecnología, oportunidades de la industria y tendencias en más de 110 países en todo el mundo. Durante 50 años, IDC ha proporcionado conocimiento estratégico para ayudar a nuestros clientes a lograr sus objetivos clave de negocio. IDC es una empresa subsidiaria de IDG, la empresa líder mundial de medios, investigación y eventos de tecnología.

IDC CEMA

Male namesti 13
110 00 Praha 1, Czech Republic
+420 2 2142 3140
Twitter: @IDC
idc-community.com
www.idc.com