# CIFRADO INTEGRAL EN RESUMEN

*Un nuevo paradigma de protección*

*"He sido hacker profesional durante más de 15 años. Encuentro problemas de ciberseguridad en la tecnología para hacer que esa tecnología sea más segura. Pero después de dedicarme a esto durante tantos años, me siento frustrado. Veo los mismos problemas una y otra vez. No estamos mejorando. Y aunque dependemos cada vez más de la tecnología, la tecnología se vuelve cada vez más insegura".*

Cesar Cerrudo, hacker profesional y director de tecnología (CTO) de IOActive Labs

Todo el ciberespacio y su infraestructura subyacente son vulnerables a una amplia gama de riesgos procedentes de amenazas y peligros tanto físicos como cibernéticos. Sofisticados grupos e individuos cibernéticos explotan las vulnerabilidades independientes y congregadas para robar dinero e información, o interrumpir, poner en peligro y dañar las operaciones. La combinación de una amplia oportunidad para el crimen en el ciberespacio con la capacidad de ejecución desde ubicaciones geográficamente dispersas ha causado la transformación de las actividades delictivas tradicionales.

El ciberespacio es extremadamente difícil de proteger. La creciente integración entre el ciberespacio y el mundo físico ha ampliado de manera exponencial las oportunidades de robo, daño y corrupción. Reducir las vulnerabilidades y minimizar las consecuencias en redes cibernéticas complejas son los objetivos, pero estos son cada vez más difíciles de lograr. El tratamiento básico de la seguridad está demostrando ser inadecuado ante las exigencias de la naturaleza agresiva del ambiente. Es necesario un cambio de paradigma, y pronto.

Los datos de la investigación fueron compilados por Solitaire Interglobal, Ltd. (SIL). Los datos del estudio base están conformados por la información de organizaciones interesadas en la efectividad de la seguridad, complementada con la información de amenazas y seguridad del Global Security Watch (GSW), cuyo enfoque principal es el impacto en las operaciones comerciales, los activos de las organizaciones y los costos de prevención y corrección. Este análisis examinó el impacto en el mundo real de la seguridad empresarial basada en la arquitectura de plataforma. Para tal fin, se compararon las métricas de arquitecturas importantes como las plataformas z Systems de IBM, UNIX y productos x86. Algunos de los hallazgos destacados se pueden ver en el resumen a continuación.

La versión actual de la plataforma IBM Z tiene una ventaja sustancial en términos de costo total de propiedad, rendimiento y riesgo en comparación con las otras opciones de plataformas en el mercado actual. El nivel actual de cifrado selectivo disponible y la resistencia de la plataforma nativa a los vectores de amenazas comunes brindan a las organizaciones una importante protección fundamental.

La llegada del cifrado integral cambia radicalmente no solo la protección que está disponible en las ofertas de Z, sino también la industria en general. Este cambio de paradigma es un desafío para cualquier otra oferta que intente cubrir los negocios de hoy.

## RESUMEN DE LOS HALLAZGOS

***Resumen rápido***

| Categoría | Comentario | Conclusión rápida |
|---|---|---|
| Velocidad de respuesta | Las mismas actividades comunes en Z consumen hasta un *85.80%* menos de tiempo que aquellas ejecutadas en otras plataformas. | Z proporciona una respuesta de seguridad más rápida. |
| Riesgo | Los perfiles de riesgo de SIL establecen la clasificación de riesgo de la plataforma Z en menos de *1/20* de cualquiera de las soluciones alternativas. | El riesgo de seguridad es significativamente menor cuando se hacen implementaciones en las plataformas Z. |
| Efectividad de seguridad | Tomando como base las instalaciones iniciales, la solución fundamental de seguridad de Z proporciona hasta *8,5 veces* el nivel de interceptación de las soluciones de plataformas alternativas con un 93% menos de costo en el gasto general y un 81% menos de esfuerzo. | Las plataformas IBM Z proporcionan los entornos de aplicaciones más seguros. |
| Efectividad de seguridad | Las plataformas Z ofrecen una intercepción de incursión base que es hasta un *20,74%* mejor que las soluciones de plataformas alternativas con seguridad completamente aumentada. | La seguridad base entregada por las plataformas Z es más efectiva que las soluciones aumentadas en plataformas alternativas. |

| Categoría | Comentario | Conclusión rápida |
|---|---|---|
| Esfuerzo del personal | Los estudios de tiempo y movimiento muestran que las soluciones de seguridad de Z requieren un *81%* menos tareas para implementar niveles de protección estándar. | IBM Z requiere menos esfuerzo del personal para la protección. |
| Corrección | Los costos de corrección en las implementaciones de seguridad de Z promedian un *98,82%* menos que las plataformas alternativas. | Reparar daños de seguridad es menos costoso en Z. |
| Costo total de propiedad para la seguridad | El costo total de propiedad para las implementaciones de seguridad de Z es hasta un 83,72% más baja que para otras plataformas. | El dinero que gasta en seguridad le trae más en Z. |
| Costo total de la información | Las implementaciones de IBM Z muestran un costo total de la información hasta un 84,83% más bajo en organizaciones de una amplia gama de tamaños. | Trabajar con su información en Z es menos costoso. |
| Cifrado integral | La arquitectura de mainframe de IBM es capaz de cifrar hasta 18.4 veces más rápido, por solo el 5% del costo de otras soluciones de plataforma. | El cifrado integral marca la diferencia. |
| Financiamiento de la mitigación del riesgo | Una organización con un presupuesto de TI de $12 millones vería una diferencia en las reservas requeridas de $764,400 para x86 frente a $160,524 para IBM Z. | El menor riesgo en Z se traduce en menos reserva financiera para la póliza de seguros cibernética. |
| Unicidad | En este momento, IBM Z es la única arquitectura que puede soportar el modelo de cifrado integral. | Proteja sus activos de TI ahora. |

Los periodos prolongados de presencia de incursiones activas pueden tener un efecto negativo importante en la viabilidad de una organización. Las empresas pueden sufrir entre el 16,2% y el 63,7% de reducción promedio en los ingresos brutos y la valoración si una incursión dura más de tres meses.

Cuando la capacidad de respuesta táctica incluye la adición de capas de seguridad y protección, la arquitectura resultante comienza a parecerse a una cebolla, con capas que brindan seguridad adicional. Sin embargo, las capas mismas pueden crear puntos adicionales de topología vulnerable.


Cada lugar en el que se "adiciona" una solución parcial se convierte en un nuevo objetivo para un hacker experto. Mientras más complejas sean las capas, más alta puede ser la topología vulnerable. Esta vulnerabilidad es parte de un perfil de riesgo de seguridad que las compañías de seguros utilizan cada vez más para determinar la exposición de una organización a daños cibernéticos significativos.

El aumento en el uso de software de virtualización crea una presión adicional en la seguridad. Cada una de las máquinas virtuales crea nuevos puntos de vulnerabilidad y aumenta la complejidad del desafío de la seguridad. Esta diferencia significativa surge de la estructura base y la estrategia desarrollada detrás de la arquitectura de plataforma, el diseño de chips, el sistema operativo y el método de integración de pila.

No es solo el número de ataques lo que ha cambiado. La cara de las incursiones mismas ha cambiado significativamente.

Uno de los vectores de amenazas de más rápido crecimiento es el ataque de ransomware. En este tipo de ataque, la incursión bloquea los archivos, directorios y otros componentes del sistema. Se le pide al propietario que pague por un código de desbloqueo que puede o no funcionar.

La medida de seguridad es reflexiva, ya que se evalúa por la ausencia de molestias y problemas. Los fallos de seguridad son altamente visibles, mientras que el éxito es invisible. El estudio se ha dirigido principalmente al valor de la seguridad desde una perspectiva empresarial, de modo que aquellos cuyo rol consista en liderar los negocios puedan entender el beneficio de las ofertas de seguridad de IBM Z con cifrado integral al evaluar las soluciones de seguridad.

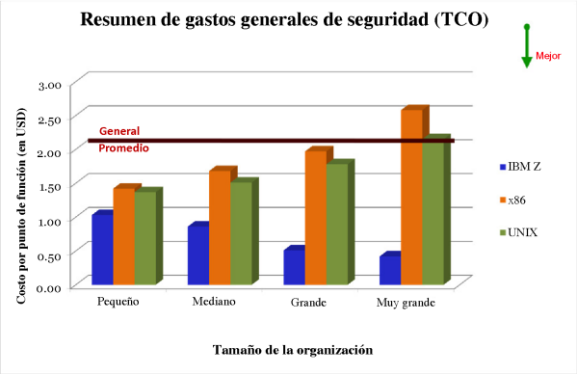
En la recopilación y el análisis de los datos del estudio se obtuvieron varias características. Estas características afectan la capacidad, eficiencia y confiabilidad manifiestas del entorno protegido. También se examinó la sinergia de la seguridad y las operaciones comerciales. La perspectiva empresarial abarca una gran cantidad de factores, entre los que se incluyen la confiabilidad, los grados de seguridad, los niveles de personal, el costo total de la seguridad (incluida la recuperación) y otros efectos. Estos se relacionan directamente con las decisiones que los gerentes de TI, los CTO y los líderes empresariales deben tomar diariamente.

## COSTO TOTAL DE PROPIEDAD

El costo total de propiedad (TCO, por sus siglas en inglés) proporciona una de las principales métricas de eficiencia operativa para las empresas. Una vez más, los proyectos y sus gastos se normalizaron de acuerdo con la base estándar, lo que permite que los gastos de organizaciones grandes y pequeñas se comparen con mayor precisión.

Los patrones de gastos muestran tendencias crecientes para algunos de los tipos de plataformas a medida que crece la complejidad de la implementación. La tendencia es contradictoria en el caso de IBM Z. Un patrón decreciente del gasto unitario se traduce en eficiencia de escala, donde el aprovechamiento del marco de trabajo y las bases permiten un patrón

rentable de inversión financiera. Como se ve en el siguiente cuadro, los gastos para las implementaciones de seguridad de Z son hasta un 83,72% más bajos que para las de otras plataformas. Esto se debe en parte a la combinación de la base de seguridad de la arquitectura y la plataforma altamente escalable.




*"Nuestro mainframe de IBM tiene un costo mucho más bajo que cualquiera de las otras cosas que hacemos como empresa. En realidad, los costos se han reducido en los últimos tres años, aunque nuestro personal financiero nos sigue diciendo que los costos son demasiado altos. Les insisto en que el costo general es más bajo, ya que tenemos menos problemas, menos personal y menos posibilidades de problemas".*

Director financiero (CFO) - Un distribuidor muy grande

En situaciones donde la seguridad se maneja con una serie de componentes de protección adicionados o donde el control principal de la seguridad reside únicamente en la aplicación implementada, la comparación global de gastos da un salto significativo cuando se agregan nuevos servicios. La siguiente tabla muestra ese tipo de efecto. Los proyectos incluidos en esta parte del análisis muestran el impacto a corto plazo de la adquisición de seguridad. En todos los casos, estas 16,027 organizaciones agregaron una sola aplicación de nube a las implementaciones de nube existentes. Las implementaciones se enfocaron en nubes privadas, públicas e híbridas y fueron diseñadas para más de 1000 usuarios.

Comunicar el costo real y el impacto de la seguridad es otro desafío. La articulación de un caso comercial de ampliación y mejoras de seguridad es un tema de discusión frecuente y un objeto de queja por parte de los profesionales de seguridad en todo el mundo. La mayoría de los ejecutivos empresariales no comprende claramente el impacto en los costos de la seguridad como un aspecto de la eficiencia operativa. En un conjunto de datos recopilados en 2015-2016 que incluía a más de 9,5 millones de ejecutivos de organizaciones, menos del 11% había visto un caso comercial para gastos de seguridad. Menos del 0,9% de estas personas afirmaron comprender cómo se derivaban los costos de seguridad, las economías de escala y los gastos proyectados. Lamentablemente, menos del 35% de las personas responsables de tomar decisiones estratégicas en las organizaciones creían que su personal de seguridad entendía cómo proyectar o calcular los costos. Todo esto contribuye a una situación en la que la reducción, o el aumento, de las asignaciones de costos para las cargas de trabajo de seguridad en general, sean imprevistos y menospreciados. Con ese punto débil en particular, la administración ejecutiva es incapaz de comprender la eficiencia considerable de las implementaciones de seguridad de IBM Z.

## EFECTIVIDAD DE SEGURIDAD

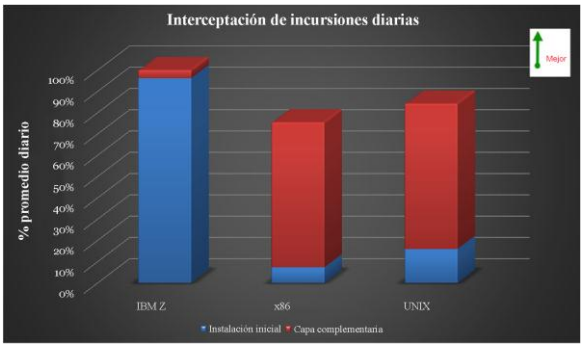
Con el fin de examinar el área de la efectividad de la seguridad, SIL encontró comparaciones medibles en una combinación de métricas objetivas y subjetivas. Las métricas objetivas incluían la capacidad de las medidas de seguridad para capturar y prevenir las incursiones exitosas, tanto en las incursiones reportadas como en aquellas descubiertas por auditorías detalladas. La información contenida en esta medición tiene aplicabilidad tanto en el aspecto técnico como en el aspecto comercial de una organización, ya que la cantidad de incursiones puede traducirse en gran medida en el efecto sobre el balance final de la organización.

Cada una de estas áreas proporciona una diferenciación clave para la solución de seguridad cibernética de IBM Z.

## RESISTENCIA A LAS INCURSIONES

La métrica principal del éxito de la seguridad es el número de incursiones que se atrapan, neutralizan o evitan para que no causen ningún tipo de daño. Las incursiones agregadas en esta métrica no incluyen aquellas incursiones que han sido bloqueadas por firewalls y dispositivos de seguridad adicionales. En su lugar, solo se contabilizaron aquellas bloqueadas por la solución de seguridad presente en la plataforma.

El nivel de bloqueo de incursiones proporcionado por la instalación inicial para cada una de las plataformas constituye la base para cualquier seguridad adicional requerida o instalada. Este gráfico muestra la seguridad proporcionada por la instalación inicial y la capa complementaria, expresada como un porcentaje de las incursiones que se han bloqueado. Sobre la base de las instalaciones iniciales, las soluciones de seguridad de base de IBM Z proporcionan hasta *13.21 veces* el nivel de interceptación de las soluciones de las plataformas alternativas. Además, la solución de Z proporciona una protección de base que supera el 92,1%, incluso sin los complementos añadidos que requieren las arquitecturas alternativas.



Las capas de seguridad suplementarias son aplicaciones adicionales, tácticas y técnicas, etc. Estas difieren de una organización a otra, pero varían en función de la supervisión, la postura y el control individuales de la seguridad. Unos niveles más altos de requisitos de seguridad complementaria indican mayores niveles de esfuerzo por parte del personal y el software de seguridad.

La combinación de capital intelectual y servicios automatizados, junto con el diseño de arquitectura de las soluciones de seguridad cibernética de IBM Z, resulta en la interceptación de un porcentaje significativamente mayor de incursiones. La plataforma Z ofrece una intercepción de incursiones de base que es hasta un *20.74%* mejor que la seguridad básica aumentada con los esfuerzos extensos, competentes y rigurosos de las tácticas, técnicas y procedimientos de seguridad complementaria proporcionados por otras soluciones de plataformas alternativas.

> *"No tengo idea exactamente de por qué hay menos problemas de seguridad con la plataforma z (sic); simplemente sé que no tenemos ninguno. La gente de seguridad me dice constantemente cosas sobre esto y aquello, lo que realmente se reduce a que simplemente funciona. La última vez que tuvimos un problema con la seguridad en esa plataforma, resultó ser que alguien se robó la contraseña de otra persona. La última vez que tuve un problema en una plataforma diferente fue hace aproximadamente una hora. ¡Pregúntenme cuál preferiría!".*

Director de información (CIO) - Un gran distribuidor

La naturaleza de la seguridad integrada de Z es significativamente diferente a la que se produce con las soluciones de protección adicionada. Con un grupo más amplio de interfaces a proteger, la protección de los datos y los procesos de la organización es más vulnerable cuando se define a nivel de dispositivo. Una estrategia más efectiva lleva el control y la definición de políticas a un punto más centralizado. La pila de seguridad altamente integrada de Z proporciona una ventaja significativa en esta área.

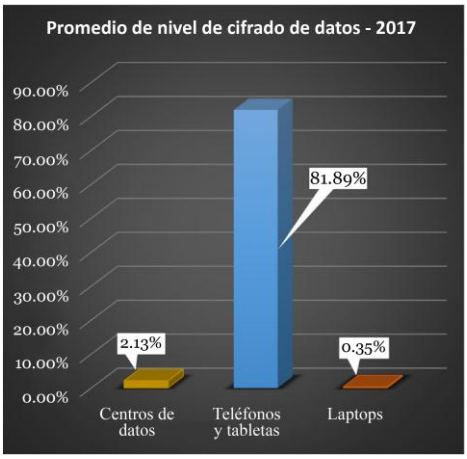
## FACTORES DE RIESGO DE SEGURIDAD

El riesgo de seguridad se puede definir como la posibilidad de que una amenaza determinada aproveche con éxito las vulnerabilidades de un proceso o un activo o grupo de activos, causando daños a la organización o a los clientes a los que sirve. Se mide en términos de una combinación de la probabilidad de ocurrencia de tal suceso y sus consecuencias asociadas. SIL crea perfiles de riesgo que son construcciones actuariales que se utilizan para proporcionar una visión consolidada del riesgo general de una organización. Esto incorpora la contribución de riesgo individual de las aplicaciones, interfaces, estructuras de gestión, aspectos de ingeniería social, etc.

> *"Una variedad de ataques nos ha dejado aturdidos por la desaparición de clientes, los costos de corrección y otras influencias horrorosas. Toda la experiencia resultó en una enorme pérdida de la confianza de los clientes. Nos estamos moviendo rápidamente a un MSP que ejecuta parte de la carga de trabajo en un gran mainframe, ya que parece ser el único lugar seguro para trabajar en estos días".*

Director - Una empresa de distribución mediana

## CIFRADO INTEGRAL




Los datos corporativos y de clientes de una organización son un recurso clave. Literalmente no tienen precio, ya que constituyen la principal ventaja en el mercado y el capital intelectual de cualquier empresa. El cifrado ha sido una manera de proteger estos activos ya que, una vez cifrados, se elimina su disponibilidad y vulnerabilidad para los hackers. Muchos de esos activos se encuentran desprotegidos en la actualidad.

La perspectiva es diferente en otras áreas de las comunicaciones de datos. El uso de dispositivos móviles se ha desarrollado sobre una perspectiva de la privacidad que incluía el cifrado desde el diseño inicial. Comparar los diferentes niveles de cifrado es esclarecedor.

Este resumen destaca la diferencia básica en el enfoque de comunicaciones móviles y de TI principales. Dado que la industria de la comunicación se dio cuenta pronto de la importancia del cifrado cuando se trataba de dispositivos móviles, aproximadamente el 82% de los datos en esas plataformas están cifrados. La discordancia de la falta de cifrado en los valiosísimos recursos organizacionales ubicados en centros de datos y en laptops es grave.

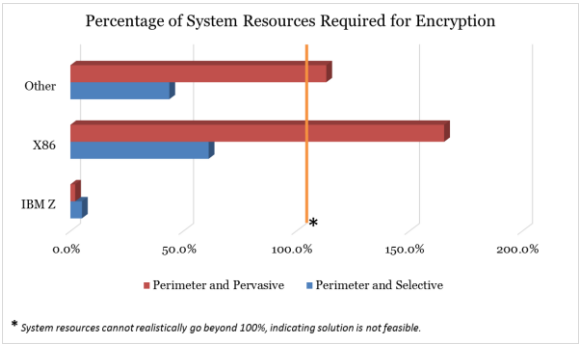
Hay varias razones principales para los bajos niveles de cifrado. El costo en términos de tiempo y capacidad de los sistemas ha alentado a las organizaciones a concentrarse en técnicas de defensa perimetral y cifrado selectivo. Dado que

la creciente demanda de defensa de seguridad perimetral consume hasta el 61,2% de la capacidad de la plataforma alternativa, se necesita un cambio de paradigma.

Un avance reciente en uno de los aspectos fundamentales de nuestro entorno informático actual está a punto de marcar la diferencia en el mercado. El cambio es la ampliación del cifrado actual de IBM Z de un modelo selectivo a uno integral. Una modificación tan significativa en la estructura básica de la computación y su efecto en la seguridad causará un efecto disruptor importante.

El concepto general es no introducir una capa de decisión que diga qué se cifrará o y qué no. En su lugar, será posible que el cifrado forme parte de los procesos normales. La eliminación de la decisión de cifrado selectivo es un ahorro adicional en el costo general y una reducción en la dificultad de usar el cifrado en el mercado actual.

La barrera más grande para hacer el cifrado a gran escala ha sido el costo del cifrado y la carga de rendimiento que dicha actividad pone en la plataforma informática. Sin embargo, en el caso de las organizaciones que participan en este estudio, las soluciones añadidas que se están implementando han causado que la capacidad de los sistemas crezca, de tal manera que haya cargas de procesos de seguridad que consumen hasta el 61% de la carga del sistema. Eso se traduce en una cantidad significativa de costos de infraestructura, reducciones de rendimiento, etc.




Los requisitos de recursos de cifrado actuales se pueden ver claramente en la tabla anterior. Incluso sin los avances más recientes, la arquitectura de Z ofrece un cifrado con un gasto de recursos más efectivo y menos costoso. Ofrece más de ***8,5 veces*** la protección de seguridad con un ***93% menos de costo*** en el gasto general y con un ***81% menos de esfuerzo***. Esto se refiere, no obstante, al cifrado selectivo que disminuye algo de la protección que se necesita desesperadamente.

El impacto total del motor de cifrado más rápido y la capacidad de cifrar información de forma masiva crea una solución totalmente integral que se ejecuta más de ***18,4 veces más rápido*** y con solo un ***5% del costo*** de otras soluciones.

Si bien el cifrado integral es factible en el mainframe Z, actualmente no es posible implementarlo en otras arquitecturas. La arquitectura más restrictiva, vinculada a las soluciones x86, requeriría *7,32 veces* la capacidad actual para ejecutar la carga de trabajo necesaria para el cifrado integral en un solo servidor. Usando el promedio por arquitectura dentro del grupo de estudio, eso se traduce en *12,2 veces* el número de plataformas actualmente instaladas en esos sitios. De lo contrario, los requisitos para este tipo de solución requerirán avances significativos en el diseño de chips para esas plataformas alternativas, en la base del sistema operativo y en otras restricciones internas de capacidad de las plataformas. Dichos avances son cambios a largo plazo en el diseño y la fabricación de chips, con tiempos de espera típicos de 2 a 3 años, suponiendo que se pueda crear la tecnología base.

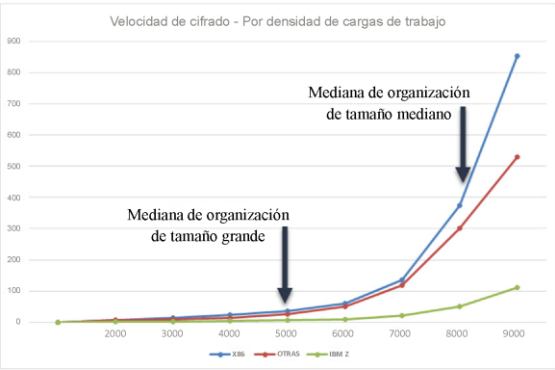
Si eso no se hace, entonces las demandas de cifrado integral no se podrán satisfacer en esas plataformas. Los sistemas que residen en tales plataformas continuarán funcionando con perfiles de riesgo y exposición más altos, requerirán una cantidad excesiva de tiempo y gasto de personal, y consumirán cantidades desproporcionadas de recursos organizacionales.

La aplicación del cifrado en una capa integral reduciría significativamente el porcentaje de la plataforma que debe dedicarse a los procesos de seguridad en sí mismos. Para las organizaciones analizadas en un estudio reciente de SIL, la reducción sería de hasta un 91,7%.

La carga de trabajo y la velocidad de respuesta son muy importantes cuando se trata de seguridad. En la comparación de cifrado selectivo frente al integral en ese mismo estudio, el modelo integral manejó un 87,2% más de incursiones de forma automática.

Para aquellas que requerían una respuesta, la velocidad de la respuesta fue mucho más rápida en el lado integral. En las pruebas, la velocidad de respuesta requirió solo el 14,2 % del tiempo requerido para la respuesta del cifrado selectivo.

La topología vulnerable también se reduce. Con menos puntos vulnerables en las capas, las amenazas se pueden abordar de una manera más completa y menos compleja. Esta menor complejidad también podría reducir significativamente el riesgo de futuras intrusiones. La topología vulnerable pasó de un promedio de 2423 puntos vulnerables a 196, lo que es reducción general ***de casi el 92%.***




Con un modelo integral, SIL exploró el riesgo de exposición e incursiones utilizando un mecanismo combinado de emulación y medición para probar la nueva tecnología. El uso del cifrado selectivo frente al integral mostró que la combinación de menos tareas manuales y el aumento de la velocidad producían ahorros hasta un 81,63% más que en x86.

Donde hoy la carga de personal de seguridad para IBM Z requiere aproximadamente un 80% menos de personal, el uso de la seguridad integral permitirá que el nivel de personal permanezca estático, mientras

que las plataformas alternativas continuarán creciendo sustancialmente cada año.

Los ahorros en costos generales también fueron significativamente diferentes. El TCO para la misma unidad operativa con cifrado integral frente al selectivo fue solo el 36,7% del presupuesto total de TI. El impacto en la organización en su conjunto es sustancial, y afecta un gran número de áreas, desde la línea de negocios hasta el desarrollo de aplicaciones.

Si bien la arquitectura de mainframe de IBM puede entregar transacciones individuales 2,87 a 3,24 veces más rápido, la inclusión de la topología y el enfoque integrales aumenta ese multiplicador significativamente. El flujo de actividades subyacente permite que el modelo integral se ocupe de lotes de transacciones como una unidad en lugar de como cifrados individuales, lo que da como resultado un cifrado que es 18,4 *veces* más rápido que las plataformas alternativas. El costo operativo resultante para el cifrado integral es del 5,1-8,0% del costo de otras opciones.

Un área de interés era el subconjunto de incursiones que se basaban en el robo de claves de cifrado. La información robada era parte del emparejamiento público y privado utilizado en la industria para proteger las actividades dentro de la plataforma. Esta exposición fue eliminada completamente por el modelo de cifrado de hardware que está presente en la solución de Z. Sin la necesidad de la autenticación por emparejamiento, no se informaron incursiones exitosas en la ventana de 14 meses del estudio.

Dado que el impacto de los robos de otras claves de cifrado ascendió a más de $6,587,500 en el plazo del estudio, esa protección es otra ventaja sustancial para la solución de seguridad integral.

## SUCESOS RECIENTES

Durante el estudio de SIL, se presentaron varios sucesos importantes en el mundo de la seguridad que están relacionados con los desafíos que aborda el cifrado. Se liberó un virus adaptado como arma que imitaba un ataque de ransomware. En realidad estaba hecho para destruir. El daño de este ataque deliberado fue amplio y considerable.

Gobiernos, hospitales, aeropuertos y empresas fueron atacados y dañados. Los costos causados aún están siendo tabulados y probablemente seguirá así por muchos años. El impacto neto, sin embargo, fue que este tipo de ataque puede y volverá a ocurrir. El tipo de cifrado que representa este nuevo avance lo habría detenido, ya que la capacidad de subvertir el control de archivos es un aspecto protegido de la capa de cifrado y, por lo tanto, no sería vulnerable a ataques de hackers.

Los billones de dólares en efectos se habrían ahorrado, y las personas que fueron lastimadas físicamente y las empresas que se vieron afectadas negativamente habrían estado a salvo. Este cambio fundamental en el paradigma de seguridad para la industria es profundo.

En este momento, ninguna otra arquitectura de chips puede soportar el modelo de cifrado integral. Esto se debe a las limitaciones técnicas de ancho de banda y gastos. Será un desafío para esas arquitecturas construir y desarrollar esta capacidad, pero es una que la industria necesita con urgencia.

## EFECTOS NETOS

El TCO del cifrado requerirá que las empresas revisen sus presupuestos de TI. Dado que gran parte del presupuesto de TI está orientado hacia el desarrollo de aplicaciones, con un promedio de 41,5-68,2% en las organizaciones del estudio, cualquier cambio que permita reducir esto tiene un efecto inmediato en el balance final de una organización.

Al trasladar el cifrado como un aspecto de seguridad fundamental al centro de un entorno informático, el efecto neto en el presupuesto de TI sería una reducción de aproximadamente el 22,1%.

> *"Las implicaciones de esto significan que el ataque cibernético podría interpretarse como un acto de guerra, según la organización. El miércoles, el secretario general de la OTAN, Jens Stoltenberg, dijo que un ataque cibernético podría accionar el Artículo 5, el principal para la defensa colectiva".*
>
> Luke Graham |@LukeWGraham, viernes, 30 de junio de 2017 | 9:50 a. m. ET, Tech Transformers, un informe especial de CNBC

Este documento se desarrolló con fondos de IBM. Aunque el documento puede utilizar material disponible públicamente de varios proveedores, incluido IBM, no refleja necesariamente las posiciones de dichos proveedores sobre los problemas tratados en este documento.

ZSL03467-COES-00