ACCIONES DE CONFIANZA

El negocio de la banca hecho posible gracias a la flexibilidad y la capacidad de respuesta seguras

"La principal preocupación de nuestros clientes es saber si es seguro hacer negocios con nosotros. Si no podemos demostrar que somos lo suficientemente inteligentes como para confiar en nosotros, los habremos perdido y no podremos recuperarlos."

Director Ejecutivo, Organización Bancaria Internacional, febrero de 2018

Protección y seguridad: ese es el tema número 1 cuando se habla acerca del mercado digital con las organizaciones. Dentro de esa esfera, no existe un ámbito más sensible que el de los grupos financieros comerciales que hacen negocios a través de Internet. Cuando los clientes están indefensos ante las vulnerabilidades de los datos, las organizaciones de servicios y productos financieros se arriesgan a la exposición completa de la base monetaria que hace que dichas empresas sean viables.

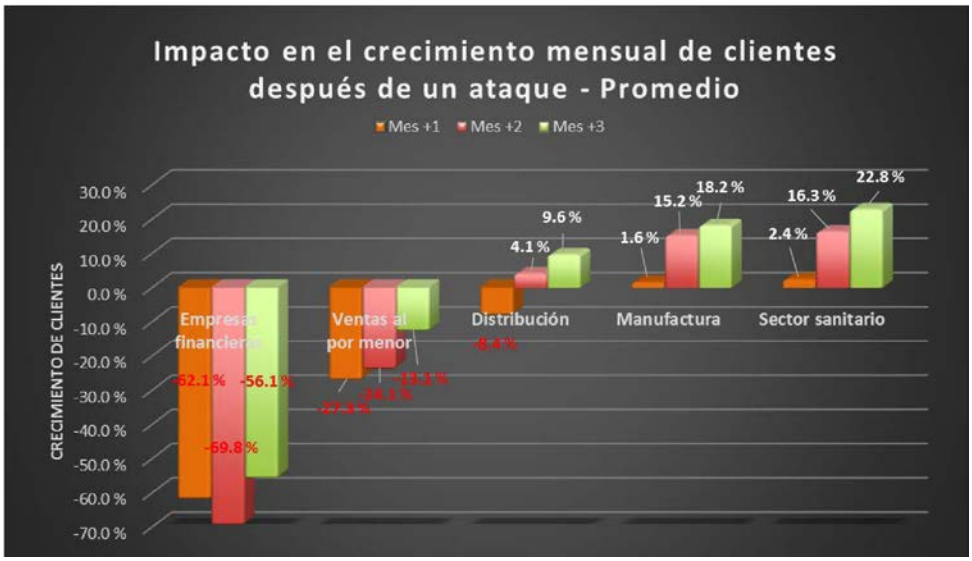
CIMIENTO DEL MERCADO DIGITAL

Si una organización de servicios financieros comerciales desea tener éxito como una empresa próspera y saludable, es esencial que pueda demostrar su capacidad para proteger la información de los clientes.

La agilidad y la flexibilidad son importantes para competir en el mercado digital, pero es vital que todas las transacciones realizadas por una organización sean seguras, especialmente en el área de servicios financieros. La erosión de la confianza después de una vulneración importante es una estocada en el corazón de una organización.

En un estudio reciente de Solitaire Interglobal Ltd. (SIL), se tomaron varios tipos de industrias para analizar el efecto en la base de clientes de una organización. La rapidez y la intensidad de la respuesta adversa de los clientes a las vulnerabilidades de los proveedores de servicios financieros son mucho más grandes y más frágiles que en cualquier otra área.

Los clientes tienen que ser capaces de confiar en que la organización puede proteger la información que recopila de ellos y que utiliza para desempeñar sus actividades. Los errores en esta área erosionan la reputación de una organización más rápido que cualquier otro factor. Se perciben como una traición en un contrato tácito entre el comprador y el vendedor.



180 South Western Avenue, #275
Carpentersville, IL 60110
Teléfono: (847) 931-9100 Sitio web: www.sil-usa.com

La recuperación de los clientes financieros al nivel previo a la vulnerabilidad puede demorar hasta 19,5 meses. Incluso el tiempo promedio informado de 7,5 meses es extremadamente costoso para una organización financiera comercial.

Si una organización depende de clientes nuevos, el costo de obtener un cliente nuevo aumenta en un factor promedio de 1,32 en comparación con el gasto antes del ataque. Cualquier expansión del mercado tendrá que lidiar con el problema de restablecer la reputación para que los clientes nuevos se sientan lo suficientemente seguros como para comprometerse con la empresa. Para hacerlo, el historial de vulnerabilidades y errores de seguridad demostrados debe ser superado de forma activa.

Si una organización intenta atraer de nuevo a sus clientes perdidos, los costos informados por organizaciones financieras maduras son de hasta 18,6 veces el costo inicial de hacer negocios con ellos. Si la organización financiera no es madura (una que ha estado activa durante más de 5 años y con una retención de clientes anual normal superior al 80 %), la probabilidad de que perdure como una entidad viable e independiente en un año es solo del 34,2 %.

En otras palabras, ser víctima de un ataque informático exitoso es extremadamente malo para las empresas. En especial para las organizaciones financieras.

La viabilidad de la organización financiera también es extremadamente sensible al número de vulneraciones y a cómo se manejan tales sucesos. En algunos casos, las organizaciones han tratado de ocultar el hecho de que hubo un ataque significativo. Las reacciones emocionales de los clientes afectados se pueden atribuir directamente a la rapidez y la franqueza con que la empresa reacciona ante la vulneración.

> *"La confianza cibernética es crucial para las finanzas. La coherencia entre la seguridad y la amenaza es un factor clave para la reputación y la confianza de los clientes."*
>
> Stéphane Nappo, Director Global de Seguridad de la Información y Asesor de la Junta Directiva de IBFS, París, Francia

La pérdida de la integridad de los datos y de la protección de la información de los clientes puede ocurrir sin importar cuán estricta sea la protección establecida por una organización. La mayoría de los clientes lo entienden, por lo que un ataque de seguridad no es necesariamente el enorme problema que podría ser. Sin embargo, la sensación de traición y erosión de la confianza se magnifica cuando una organización no tiene una reacción y una postura categóricas ante la vulneración. Responsabilizarse de los problemas es una manera de humanizar una organización, pero esa solución no es apta para todas las empresas. Decidir la postura de la organización con respecto a la seguridad y los ataques es, por lo tanto, un componente vital de las políticas y procedimientos de una empresa.

Sin una postura lista, no hay manera de suavizar la reacción de los clientes cuando ocurre un ataque. Los clientes que se sienten traicionados por una empresa tienen muchas menos probabilidades de volver a dicha organización. En un estudio de más de 175.000 organizaciones, más del 78 % de los clientes se negaron a regresar después de una vulneración si la organización no se responsabilizó del suceso inmediatamente. Más del 79 % esperaba que la organización vulnerada explicara con precisión lo que estaba haciendo para remediar la vulneración y reparar cualquier daño que se hubiera hecho.

Tratar de encubrir el incidente fue visto por más del 95 % de los clientes que respondieron a las preguntas como una falta de respeto para ellos como individuos. O como un encuestado escribió en sus notas: "¿Por qué querría hacer negocios con el comerciante que ha demostrado que no me ve como persona? ¿Por qué querría relacionarme con alguien que no me valora?".

¿Cuánto vale la viabilidad de una organización? ¿Qué efecto tendría la pérdida de una parte importante de los clientes actuales en el balance final? Esta es la compensación realista a las dificultades y los gastos de la ciberseguridad. Si los clientes no confían en una organización, no harán negocios con ella.

Esto se traduce en una caída inmediata y prolongada de los ingresos. También exacerba aún más la reputación ya dañada de la empresa. Dependiendo de los factores correctivos, es posible que estos clientes nunca regresen. Si lo hacen, será solo después de un desembolso importante en gastos de servicios, equipos y personal para restablecer una posición de confianza y volver a atraer a los clientes.

SOLUCIONES LINUXONE PARA LA BANCA

Una forma de abordar este riesgo es construir sobre un cimiento que tenga una mayor seguridad de nivel de base demostrable. Eso hace que la elección de la plataforma sea algo más que un costo inmediato, ya que exige que las empresas examinen en su totalidad el riesgo y la exposición que conllevan los *cibernegocios* con sus muy lucrativas promesas.

IBM LinuxONE es un componente importante en la construcción de un cimiento para la transformación. Aborda las áreas clave del éxito en el creciente mercado de la seguridad, la resiliencia y el rendimiento que permite a las organizaciones responder con agilidad a los desafíos que se evidencian cada día en el ciberespacio.

Los costos específicos se ven afectados positivamente por la solución LinuxONE. Minimizar los gastos con menos personal requerido y un costo de propiedad significativamente menor es extremadamente beneficioso. Las diferencias en esta área son significativas con *ahorros de hasta el 80 %* en el costo total de propiedad y *niveles de personal más bajos en hasta un 60 %* o más.

La seguridad es donde la solución LinuxONE hace la mayor diferencia. Cuando la ciberseguridad fundamental tiene un punto de partida más estricto, los hackers tienen muchas menos probabilidades de vulnerar las protecciones que son necesarias para los inventarios digitales. De hecho, las implementaciones de LinuxONE reportan *menos de 0,01 %* de ataques de seguridad exitosos por cada 1000 aplicaciones implementadas que otras arquitecturas.

El menor costo de protección de la reputación de la organización y el impacto en los ingresos son tan significativos que pueden hacer la diferencia entre una organización viable o una que no lo es. La protección contra ataques se traduce fácilmente en una mayor confianza de los clientes, lo que a su vez genera mayores ingresos y una mayor lealtad de los clientes.

En el volátil mundo de los cibernegocios, la confianza en las organizaciones que tienen el control primordial de las finanzas es la más frágil y sensible. Proteger dicha confianza supera otras preocupaciones como la velocidad y la flexibilidad, ya que la velocidad para una empresa que no puede proteger y conservar a sus clientes es irrelevante.

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) ha recopilado datos sobre la evolución del mercado y el comportamiento de la producción durante más de 40 años. Con el respaldo que brinda a más de 6000 clientes y la realización de más de 100 millones de modelos predictivos cada año, SIL también ha dirigido el Global Security Watch durante los últimos 22 años. Este servicio para miembros le ha permitido a SIL construir un repositorio que supera los 550 PB de datos a un nivel muy granular. Cada hora se le hace minería a estos datos para detectar tendencias, hacer comparaciones y buscar un umbral que ayude a las organizaciones a tener éxito.

ATRIBUCIONES Y EXENCIONES DE RESPONSABILIDAD

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.

42018942COES