



Un banco evalúa los riesgos relacionados con la identidad con Proofpoint para completar una F&A con total seguridad

El desafío

- Evaluar el nivel de seguridad de otro banco que está en proceso de adquirir.
- Identificar las vulnerabilidades relacionadas con la identidad (en un momento en que no disponía de una solución para este fin).
- Respetar los plazos ajustados para cerrar la adquisición.

La solución

- Proofpoint Identity Threat Defense
- Proofpoint Spotlight

Los resultados

- Evaluación completa de los riesgos asociados a la identidad del banco adquirida en menos de 30 días.
- Descubrimiento de miles de riesgos críticos insospechados relacionados con la identidad.
- Obtención de datos cuantitativos concretos que convencieron al equipo directivo de posponer la plena integración de TI hasta que se hubieran resuelto los problemas.

La empresa

La empresa es un holding bancario regional estadounidense con unos activos de unos 200 000 millones de dólares. Fundado hace más de 150 años, el banco y sus filiales ofrecen a particulares, pymes, grandes empresas, municipios y otras organizaciones una gama completa de servicios bancarios y otros servicios financieros. La empresa emplea a unas 25 000 personas y gestiona más de 1000 sucursales.

El desafío

La empresa opera en un sector en el que la consolidación es la norma. En los últimos 20 años, el número de bancos comerciales asegurados por la Corporación Federal de Seguro de Depósitos (FDIC) se ha reducido casi a la mitad, debido principalmente a las adquisiciones. Por término medio, este banco realiza una adquisición cada tres años. Cada vez que ha llevado a cabo una fusión o adquisición (F&A), su departamento de TI ha tenido que consolidar diferentes sistemas, programas de software, datos, procesos y organizaciones.

Si un banco adquiere una empresa con un nivel de seguridad de TI inferior (o incluso mínimamente clara), puede poner en peligro a toda la empresa. La evaluación de la seguridad es esencial y a menudo debe realizarse con gran rapidez.

Como explica el jefe de ingeniería de ciberseguridad del banco: "Tuvimos un máximo de cuatro meses, entre el anuncio de la transacción y su conclusión, para evaluar el nivel de seguridad de TI del otro banco. Necesitábamos saber si podíamos confiar en él".

"Estoy encantado de que hayamos utilizado Proofpoint Identity Threat Defense. Todo el mundo comprende su utilidad. Utilizaremos el mismo enfoque para nuestra próxima fusión y adquisición".

Director de Ingeniería de ciberseguridad

La solución

Como toda la seguridad del banco adquirido se basa en la seguridad de la identidad, era esencial comprender sus posibles vulnerabilidades relacionadas con la identidad. Como cliente de Proofpoint, el banco adquirente estaba muy familiarizado con la solución y valoraba su información exclusiva. "Hemos utilizado Proofpoint para que analizara continuamente nuestras estaciones de trabajo durante al menos seis meses. Así sabíamos qué tipo de información podía proporcionarnos".

Los resultados

La evaluación del banco adquirido dio lugar a un cuadro de mando de riesgos en el que se comparaban las dos organizaciones de TI, y resultó que los riesgos eran suficientes para convencer a la dirección de la necesidad de mantener separados los entornos informáticos, al menos inicialmente.

Aunque existen varios ámbitos de riesgo para la identidad, uno ha destacado rápidamente. "Lo que más nos llamó la atención fue el número de administradores de dominio en sus estaciones de trabajo. Había 3000. Era indicativo de sus deficientes prácticas de seguridad. Si alguien hubiera comprometido una de estas estaciones de trabajo, habría tenido el control de todo el entorno. Ellos tampoco lo sabían y se pusieron manos a la obra".

Los resultados globales de la comparación fueron convincentes. "El debate habría sido mucho más difícil sin el análisis del riesgo de identidad realizado antes de la integración. Nos ayudó a justificar la mayor protección que necesitábamos en esta fase inicial".

Además de las fusiones y adquisiciones, el banco utiliza Proofpoint Identity Threat Defense para analizar continuamente su propio entorno para identificar vulnerabilidades relacionadas con la identidad. Esta plataforma forma parte de una solución completa que incluye Qualys, Kenna, ServiceNow y otras soluciones de gestión de amenazas y vulnerabilidades.

Preguntado por el futuro, el director afirma: "Estoy encantado de que hayamos utilizado Proofpoint Identity Threat Defense. Todo el mundo comprende su utilidad. Utilizaremos el mismo enfoque para nuestra próxima fusión y adquisición".

MÁS INFORMACIÓN

Para obtener más información, visite [proofpoint.com/es](https://www.proofpoint.com/es).

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 85 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.