infoblox

ESTUDIO DE CASO

Askari Bank moderniza y mejora su postura de ciberseguridad con Threat Defense Advanced de Infoblox

RESUMEN

Askari Bank abrió sus puertas en abril de 1992 y ha crecido hasta convertirse en una de las instituciones financieras líderes de Pakistán.

Askari ofrece una gama completa de servicios bancarios personales y empresariales, cajeros automáticos y banca móvil, así como tarjetas de crédito y débito, y cuenta con 537 sucursales en todo Pakistán. Desde sus inicios, el banco se ha centrado en el crecimiento mediante la mejora de la calidad del servicio, la inversión en tecnología y en las personas, y el uso de su amplia red de sucursales, que incluye banca islámica y agrícola. La visión de Askari es apoyar con dedicación el éxito de sus clientes y deleitarlos con la calidad de su servicio. Un elemento clave de esta dedicación al servicio es mantener los más altos niveles de privacidad y seguridad para los clientes del banco.

EL DESAFÍO

Fortalecer la postura de seguridad para contrarrestar las amenazas emergentes

Al igual que todas las instituciones financieras a nivel mundial, el Askari Bank de Pakistán es objetivo habitual de ciberataques maliciosos. Mantener una postura de seguridad sólida es desde hace mucho tiempo una prioridad para el equipo de TI de Askari, por lo que el banco implementó múltiples soluciones de ciberseguridad a lo largo de los años, incluida una solución de orquestación, automatización y respuesta de seguridad (SOAR) y un producto de seguridad DNS de Cisco en el que confió durante años. Al colaborar con los consultores de Secure Networks, el equipo de Askari comprendió que las amenazas de la capa del DNS habían evolucionado con el tiempo y que explorar otras opciones en tecnología del DNS contribuiría a reforzar la seguridad general del banco.

> *«Durante la ejecución de la prueba de concepto en varios escenarios, no tuvo éxito ni un solo evento de infiltración o exfiltración de datos. Ver BloxOne Threat Defense en acción bloqueando la actividad maliciosa en nuestro propio entorno nos dio mucha confianza en la solución de Infoblox».*

Jawad Khalid Mirza
CISO en Askari Bank

askaribank LIMITED

«Como sabemos, el DNS no está diseñado desde una perspectiva de seguridad», explica Jawad Khalid Mirza, director de Seguridad de la Información de Askari Bank. «La arquitectura abierta del DNS lo ha convertido en objetivo prioritario para los adversarios. En el sector financiero, estas amenazas se manifiestan con mayor frecuencia en intentos de exfiltrar o infiltrar datos de la empresa».

«Las soluciones de seguridad heredadas están diseñadas para contrarrestar las amenazas bloqueando las consultas al DNS», explica Asad Effendi, director ejecutivo de Secure Networks, que colaboró en la prueba de concepto. «Pero con los escenarios de ataques de malware que vemos hoy en día, limitarse a bloquear el tráfico sospechoso no siempre es el mejor enfoque».

LA SOLUCIÓN

Seguridad del DNS avanzada con BloxOne Threat Defense™

Con una versión de prueba de BloxOne Threat Defense instalada en el centro de datos de Askari Bank, el equipo probó una serie de hipótesis de tráfico de red utilizando las técnicas más recientes de infiltración y exfiltración de datos características de DNSMessenger y los ataques de flujo rápido. «Durante la ejecución de la prueba de concepto en varios escenarios, no tuvo éxito ni un solo evento de infiltración o exfiltración de datos», afirma Khalid Mirza. «Ver BloxOne Threat Defense en acción bloqueando la actividad maliciosa en nuestro propio entorno nos dio mucha confianza en la solución de Infoblox».

BloxOne Threat Defense opera a nivel del DNS para ver y detectar amenazas que otras soluciones pasan por alto y detiene los ataques antes en el ciclo de vida de la amenaza. Gracias a la automatización generalizada y la integración del ecosistema, también impulsa la eficiencia de las operaciones de seguridad para mejorar la eficacia de la pila de seguridad existente. Estas capacidades constituyeron una sólida consideración secundaria para el equipo de Askari, que confía en su solución SOAR para gestionar sus operaciones de seguridad generales. Ahora que el equipo de Askari conoce todas las capacidades y ventajas de BloxOne Threat Defense, ha tomado la decisión de seguir adelante con la implementación completa en producción.

LOS RESULTADOS

Detección de amenazas más rápida, tiempos de respuesta a incidentes reducidos

«BloxOne Threat Defense hace que toda nuestra pila de seguridad sea más eficaz», explicó Umair Shakil, director de la Unidad del Centro de Operaciones de Seguridad del Askari Bank. «Con la solución de Infoblox integrada en nuestra plataforma SOAR existente, todas las herramientas de nuestra pila de seguridad tienen ahora acceso a información en tiempo real sobre la red y las amenazas. Ahora todo funciona al unísono para identificar y solucionar mejor las amenazas, gracias a una amplia automatización».

El exclusivo diseño de seguridad híbrido de BloxOne Threat Defense aprovecha el potencial de la nube para detectar una amplia gama de amenazas y se integra a la perfección con el ecosistema local. También proporciona un nivel de resiliencia y redundancia que no tienen las soluciones solo en la nube. A través de una consola común, el equipo de Askari ahora puede proteger de forma centralizada y automática el IoT y otros dispositivos, aplicaciones, máquinas virtuales y puertos de conmutación dondequiera que se encuentren. BloxOne Threat Defense ha permitido al equipo de Askari reducir la carga de los dispositivos de seguridad perimetral, como cortafuegos, IPS y proxis web, ya que convierte los potentes servidores del DNS ya disponibles en la primera línea de defensa. El equipo espera obtener más valor de su pila de seguridad mediante el intercambio de información sobre amenazas y atacantes, así como aumentar la productividad de sus analistas de amenazas y administradores de seguridad.

Cliente: ***Askari Bank***
Sector: ***servicios financieros***
Ubicación: ***Pakistán***

INICIATIVAS:

- Prevenga las técnicas de infiltración y exfiltración de datos mediante análisis y aprendizaje automático, incluyendo la exfiltración de datos basada en el DNS, DGA, DNSMessenger y ataques de flujo rápido
- Detecte y bloquee exploits, phishing, ransomware y otro software malicioso moderno
- Identifique la propagación y el movimiento lateral del software malicioso mediante la monitorización del tráfico este-oeste.
- Restrinja el acceso de usuarios a determinadas categorías de contenido web y supervise la actividad
- Proteja la marca con la monitorización de dominios similares para las propiedades de internet más valiosas
- Controle los riesgos del creciente uso de DoH: bloquee el acceso a dominios DoH (DNS sobre HTTPS) y revierta con elegancia las peticiones DoH a los DNS existentes y de confianza

«BloxOne Threat Defense permite a nuestros analistas del SOC tomar decisiones más rápidas basadas en información contextual de gran precisión, lo que optimiza el tiempo total de análisis», afirma Hasan Imam, ingeniero técnico jefe de Secure Networks. «Dado que el DNS se ha convertido en un vector de ataque cada vez más importante, las medidas proactivas y la profesionalidad de Askari Bank para proteger esta brecha son muy admirables y constituyen un sólido ejemplo en el sector sobre cómo abordar la seguridad».

«En mi opinión, ningún otro proveedor de soluciones ofrece el nivel de seguridad del DNS que proporciona Infoblox con BloxOne Threat Defense», concluye Khalid Mirza. «Al asociarnos con Infoblox, Askari Bank cuenta con la protección necesaria para la infraestructura del DNS, lo que nos permite cumplir nuestro objetivo de ofrecer servicios seguros a los clientes de nuestro banco en todo Pakistán».

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com