infoblox

FALLSTUDIE

Askari Bank modernisiert und verbessert Cybersicherheitslage mit Infoblox Threat Defense Advanced

ÜBERSICHT

Die Askari Bank wurde im April 1992 eröffnet und hat sich seitdem zu einem der führenden Finanzinstitute Pakistans entwickelt.

Askari bietet eine umfassende Palette an Bankdienstleistungen für Privat- und Geschäftskunden, Geldautomaten, Mobile-Banking sowie Kredit- und Debitkarten und unterhält 537 Filialen in ganz Pakistan. Seit ihrer Gründung hat sich die Bank auf Wachstum durch die Verbesserung der Servicequalität, Investitionen in Technologie und Personal sowie die Nutzung ihres ausgedehnten Filialnetzes konzentriert, das auch islamisches Bankwesen und Agrar-Banking umfasst. Die Vision von Askari ist es, den Erfolg seiner Kunden mit Leidenschaft zu unterstützen und sie mit der Qualität seiner Dienstleistungen zu begeistern. Ein Schlüsselelement dieses Engagements ist die Wahrung des absolut höchsten Niveaus an Datenschutz und Sicherheit für die Kunden der Bank.

DIE HERAUSFORDERUNG

Stärkung der Sicherheitslage, um neuen Bedrohungen entgegenzuwirken

Wie alle Finanzinstitute weltweit ist auch die pakistanische Askari Bank ein beliebtes Ziel bösartiger Cyberangriffe. Die Aufrechterhaltung einer guten Sicherheitslage hat für das IT-Team von Askari seit langem oberste Priorität, und die Bank hat im Laufe der Jahre mehrere Cybersicherheitslösungen eingeführt, darunter eine SOAR-Lösung (Security Orchestration, Automation and Response) und ein Cisco DNS-Sicherheitsprodukt, auf das sie jahrelang gesetzt hat. Durch die Zusammenarbeit mit den Beratern von Secure Networks erkannte das Askari-Team, dass sich die Bedrohungen auf DNS-Ebene im Laufe der Zeit weiterentwickelt hatten und dass das Ausloten anderer DNS-Technologie-Optionen helfen könnte, die allgemeine Sicherheit der Bank zu verbessern.

> *„Als wir den PoC durch verschiedene Szenarien laufen ließen, gab es keinen einzigen Fall einer erfolgreichen Dateninfiltration oder eines Exfiltrationsvorgangs. Zu sehen, wie BloxOne Threat Defense bösartige Aktivitäten in unserer eigenen Umgebung blockiert, hat uns viel Vertrauen in die Infoblox-Lösung gegeben.“*
>
> **Jawad Khalid Mirza**
> **CISO bei Askari Bank**

askaribank LIMITED

„Wie wir wissen, wurde DNS nicht im Hinblick auf Sicherheitsaspekte entwickelt“, erklärt Jawad Khalid Mirza, der Chief Information Security Officer der Askari Bank. „Die offene Architektur des DNS hat dazu geführt, dass es zu einem Hauptziel für Angreifer geworden ist. Im Finanzsektor manifestieren sich diese Bedrohungen am häufigsten in Versuchen, Daten aus dem Unternehmen zu exfiltrieren oder dort einzuschleusen.“

„Legacy-Sicherheitslösungen sind so konzipiert, dass sie Bedrohungen durch das Blockieren von DNS-Abfragen entgegenwirken“, erklärt Asad Effendi, CEO von Secure Networks, der bei der Durchführung des PoC mitgewirkt hat. „Aber bei den Malware-Angriffsszenarien, die wir heutzutage erleben, ist es nicht immer die beste Lösung, verdächtigen Datenverkehr einfach zu blockieren.“

DIE LÖSUNG

Erweiterte DNS-Sicherheit mit BloxOne Threat Defense™

Mit einer Testversion von BloxOne Threat Defense, die im Rechenzentrum der Askari Bank installiert wurde, führte das Team eine Reihe von Netzwerkverkehrsszenarien durch, wobei die neuesten Techniken zur Dateninfiltration und -exfiltration verwendet wurden, die für DNSMessenger- und Fast-Flux-Angriffe charakteristisch sind. „Als wir den PoC durch verschiedene Szenarien laufen ließen, gab es keinen einzigen Fall einer erfolgreichen Dateninfiltration oder eines Exfiltrationsvorgangs“, so Khalid Mirza. „Zu sehen, wie BloxOne Threat Defense bösartige Aktivitäten in unserer eigenen Umgebung blockiert, hat uns viel Vertrauen in die Infoblox-Lösung gegeben.“

BloxOne Threat Defense arbeitet auf DNS-Ebene, um Bedrohungen zu erkennen und aufzudecken, an denen andere Lösungen scheitern. Zudem stoppt es Angriffe früher im Bedrohungszyklus. Durch umfassende Automatisierung und Ökosystem-Integration wird auch die SecOps-Effizienz gesteigert, um die Wirksamkeit des bestehenden Sicherheitsstacks zu verbessern. Diese Fähigkeiten stellten für das Askari-Team, das für die Verwaltung seiner gesamten Sicherheitsabläufe auf seine SOAR-Lösung setzt, einen wichtigen zusätzlichen Faktor dar. Da dem Askari-Team ab diesem Punkt der volle Umfang der Fähigkeiten und Vorteile von BloxOne Threat Defense klar war, wurde die Entscheidung getroffen, mit einer vollständigen Produktionsbereitstellung fortzufahren.

DIE ERGEBNISSE

Schnellere Bedrohungserkennung, verkürzte Reaktionszeiten auf Vorfälle

„BloxOne Threat Defense macht unseren gesamten Sicherheitsstack effektiver“, so Umair Shakil, der Leiter der Security Operations Center Unit der Askari Bank. „Da die Infoblox-Lösung in unsere bestehende SOAR-Plattform integriert ist, haben alle Tools in unserem Sicherheitsstack jetzt Echtzeit-Zugriff auf Netzwerk- und Bedrohungsinformationen. Jetzt greift alles ineinander, damit Bedrohungen durch umfassende Automatisierung besser erkannt und behoben werden können.“

Das einzigartige hybride Sicherheitsdesign von BloxOne Threat Defense nutzt die Leistungsfähigkeit der Cloud, um ein breites Spektrum an Bedrohungen zu erkennen, während es nahtlos in das lokale Ökosystem integriert wird. Außerdem bietet es eine Ausfallsicherheit und Redundanz, die bei reinen Cloud-Lösungen nicht gegeben ist. Über eine gemeinsame Konsole kann das Askari-Team nun IoT- und andere Geräte, Anwendungen, virtuelle Maschinen und Switch-Ports zentral und automatisch sichern, wo auch immer sie sich befinden. BloxOne Threat Defense hat es dem Askari-Team ermöglicht, die Belastung überbeanspruchter Perimeter-Sicherheitsgeräte wie Firewalls, IPS und Web-Proxys zu verringern, da es leistungsstarke und bereits verfügbare DNS-Server zur ersten Verteidigungslinie macht. Das Team erwartet, dass es durch den Austausch von Informationen über Bedrohungen und Angreifer einen größeren Nutzen aus seinem Sicherheitsstack ziehen und auch die Produktivität seiner Bedrohungsanalysten und Sicherheitsadministratoren steigern kann.

Kunde: ***Askari Bank***
Branche: ***Finanzdienstleistungen***
Ort: ***Pakistan***

INITIATIVEN:

- Verhindern von Dateninfiltrations- und -exfiltrationstechniken mit Analysen und maschinellem Lernen, einschließlich DNS-basierter Datenexfiltration, DGA, DNSMessenger und Fast-Flux-Angriffen
- Erkennen und blockieren von Exploits, Phishing, Ransomware und anderer moderner Malware
- Identifizieren der Verbreitung und lateralen Bewegung von Malware durch die Überwachung des Ost-West-Traffics
- Beschränken Sie den Benutzerzugriff auf bestimmte Kategorien von Webinhalten und verfolgen Sie Aktivitäten
- Schutz der Marke mit Lookalike Domain Monitoring für die wertvollsten Internetobjekte
- Beherrschen Sie die Risiken der zunehmenden DoH-Nutzung: Blockieren Sie den Zugriff auf DoH-Domänen (DNS über HTTPS) und leiten Sie DoH-Anfragen zuverlässig auf bestehende, vertrauenswürdige DNS um.

„BloxOne Threat Defense ermöglicht es unseren SOC-Analysten, schnellere Entscheidungen auf der Grundlage hochpräziser Kontextinformationen zu treffen, was die Gesamtanalysezeit verbessert“, sagt Hasan Imam, leitender technischer Ingenieur bei Secure Networks. „Da DNS mittlerweile zu einem immer wichtigeren Angriffsvektor geworden ist, sind die proaktiven Maßnahmen und die Professionalität der Askari Bank beim Schließen dieser Lücke äußerst bewundernswert. Sie bietet ein extrem gutes Beispiel innerhalb der Branche, wie man in Sachen Sicherheit führend ist.“

„Für mich bietet kein anderer Lösungsanbieter dasselbe Niveau an DNS-Sicherheit wie Infoblox mit BloxOne Threat Defense“, schließt Khalid Mirza. „Durch die Partnerschaft mit Infoblox verfügt die Askari Bank über den notwendigen Schutz für ihre DNS-Infrastruktur. Das wird es uns ermöglichen, unsere Ziele bei der Bereitstellung sicherer Dienstleistungen für unsere Bankkunden in ganz Pakistan zu erreichen.“

infoblox.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com