Schutz von kritischer nationaler Luftfahrtinfrastruktur

2021

kaspersky BRING ON THE FUTURE

Der Flughafen München ist Internetkriminellen immer einen Schritt voraus - mit den aktuellsten und zuverlässigsten Daten und Analysen zur Cybersicherheit von Kaspersky Threat Intelligence Services.

Der Flughafen München hat ein jährliches Passagieraufkommen von beinahe 50 Mio. Fluggästen und ist der erste Flughafen, der vom Skytrax Institute, dem renommierten Londoner Luftfahrtforschungsinstitut, mit dem prestigeträchtigen Qualitätssiegel „5-Star-Airport“ ausgezeichnet worden ist.

Luftfahrt

- Land: München, Deutschland
- Einsatz von Kaspersky Threat Intelligence Services

Bevor COVID-19 den Luftverkehr erheblich beeinträchtigte, bedienten jedes Jahr mehr als 100 Fluggesellschaften Flüge von München zu 250 Zielorten in 75 Ländern und die Passagierzahlen waren in weniger als 30 Jahren um mehr als 300 % gestiegen.

Der nur 30 Minuten Fahrzeit von der bayerischen Hauptstadt entfernte Großflughafen beschäftigt mehr als 38.000 Personen in über 500 verschiedenen Firmen. Die Bayern lieben ihr Bier und es ist kaum überraschend, dass München der einzige Flughafen der Welt mit eigener Brauerei auf dem Flughafengelände ist!

Herausforderung

Die Größe, Komplexität und kritische Infrastrukturrolle eines Großflughafens wie München erfordern höchste Priorität für ein hochentwickeltes und umfassendes IT-Sicherheitsprofil.

„Kasperskys Threat Intelligence Services unterstützen uns dabei, ein deutlich vollständigeres Bild der weltweiten Bedrohungslandschaft und der potenziellen Gefahren für den Flughafen München zu gewinnen.“

Marc Lindike, Leiter Flughafen und IT-Sicherheit, Flughafen München

Kunden, Fluggesellschaften, Einzelhändler, Rettungsdienste, die Flughafenverwaltung und zahlreiche andere Unterstützungsorganisationen verlassen sich auf Live-Daten und voll funktionsfähige IT-Systeme, um den reibungslosen und sicheren Ablauf des Flughafenbetriebs und der Flüge zu ihren Zielorten sicherzustellen.

Der hohe Bekanntheitsgrad und die große wirtschaftliche Bedeutung von Flughäfen lässt sie zu offensichtlichen Zielen für Internetkriminelle werden, die es darauf abgesehen haben, den Luftverkehr zu stören, Daten zu stehlen oder Erpressungsgelder zu fordern, indem sie IT-Systeme oder einzelne Mitarbeiter anvisieren. Das Gelände des Flughafens München hat mit 15 Quadratkilometern praktisch die Größe einer Kleinstadt.

Daher suchen Marc Lindike, Leiter Flughafen und IT-Sicherheit der Flughafen München, und sein Team fortlaufend nach Möglichkeiten, die Sicherheitsfähigkeiten und das Sicherheitsprofil des Flughafens zu stärken.

„Es ist besonders wichtig für uns, möglichst frühzeitig Warnungen in Bezug auf die globale Bedrohungslandschaft zu erhalten, damit wir sachkundige proaktive Maßnahmen zum Schutz der Tausenden von Menschen hier am Flughafen, die sich auf ihre IT-Systeme verlassen, einleiten können. Zu diesem Zweck benötigen wir Zugang zu den aktuellsten und besten Informationen und Analysen aus den vertrauenswürdigsten und zuverlässigsten Quellen.“

Die Kaspersky-Lösung

2018 begann der Austausch zwischen Marc Lindike und dem deutschen Kaspersky-Team zur Identifizierung von Cybersicherheitsdiensten, welche die Verteidigungsfähigkeiten des Flughafens stärken könnten.

Daraufhin wurde ein Testprogramm für wichtige Komponenten des Kaspersky Threat Intelligence-Portfolios gestartet, das Marc Lindike und seinem Team eine ausführliche Bewertung der Leistungsfähigkeit, Eignung und Kostenwirksamkeit der angebotenen Dienste gestattete.

50
Mio. Passagiere
pro Jahr

300 %
Wachstum in weniger
als 30 Jahren

Intelligence Reporting zu Advanced Persistent Threats (APT, fortgeschrittene andauernde Bedrohung) bietet exklusiven proaktiven Zugang zu Kasperskys aktuellen Untersuchungen und Erkenntnissen zur Offenlegung der von Cyberkriminellen angewandten Methoden, Taktiken und Werkzeugen.

Da APTs zu den gefährlichsten und komplexesten Kategorien von Cyberangriffen gehören, führen die Berichte von Kaspersky im Detail auf, wie jeder Angriff funktioniert, wo sein Ursprungsort liegt und welche Art von Infrastruktur wahrscheinlich anvisiert wird.

Indicators of Compromise (Gefährdungsindikatoren), d. h. von den Fachleuten bei Kaspersky gefundene forensische Daten, liefern Organisationen wie dem Flughafen München Erkenntnisse, aus denen sie direkt die nächsten Schritte ableiten können, um ihre Firewalls und andere Systeme, die einen Kompromittierungsversuch feststellen können, zu stärken.

Marc Lindike und sein Team testeten und kauften außerdem Kaspersky Threat Lookup, einen Service, der Echtzeitsuchen in enormen Mengen von Bedrohungsdaten ermöglicht, die von Kaspersky im Lauf seiner Unternehmensgeschichte gesammelt, kategorisiert und analysiert wurden, und eine globale Sicht auf Bedrohungen und deren Zusammenhänge bietet. Hier kann der Anwender verdächtige Dateien oder Objekte zur Analyse hochladen und anschließend alle relevanten Informationen zu den Punkten bzw. Themen der Bedrohung erhalten, die von Kaspersky über Jahrzehnte erfasst wurden.

Abschließend abonnierte der Flughafen München eine Reihe von Kaspersky Threat Data Feeds, die rund um die Uhr alle 10 Minuten Live-Updates zu den aktuellsten auftretenden Malware-Bedrohungen und anderen verdächtigen Aktivitäten liefern.

Ein vollständigeres Bild weltweiter Bedrohungen

Diese Dienstleistungen werden vom Global Research and Analysis Team (GReAT) von Kaspersky erstellt, das weltweite Anerkennung für seine fundierten und tiefgreifenden Erkenntnisse über einige der berüchtigsten Bedrohungskampagnen der Welt genießt.

GReAT liefert kontinuierlich Berichte über die von Cyberkriminellen bei weithin bekannten Cyberspionagekampagnen verwendeten Taktiken und Werkzeuge. Hierbei werden Kriminelle branchen- bzw. sektorübergreifend anvisiert, damit Gegenmaßnahmen zur Bekämpfung der komplexesten Angriffe getroffen werden können.

Sicher
Gewährleistet die volle Funktionsfähigkeit von kritischer internationaler Infrastruktur

Kontrolle
Einfacher Zugang zu Daten und Analysen über ein maßgeschneidertes Portal

Leistung
Kasperskys GReAT ist als eines der besten Forschungs- und Analyse-Teams der Welt anerkannt

Die Experten bei Kaspersky zählen zu den fähigsten, erfahrensten und erfolgreichsten APT-Jägern der Branche und liefern sofortige Alarme über von ihnen festgestellte Veränderungen bei den von cyberkriminellen Vereinigungen angewendeten Taktiken.

Flughafen München war von den Ergebnissen der Tests so beeindruckt, dass sie einen langfristigen Vertrag mit Kaspersky zur Lieferung von Threat Intelligence Services abschlossen. Diese Dienstleistungen schützen die gesamte IT-Infrastruktur der Flughafenbehörden, Fluggesellschaften, Einzelhändler und anderer Organisationen auf dem Flughafengelände.

Marc Lindike sagt: „Kasperskys Threat Intelligence Services spielen eine bedeutende Rolle bei unseren Anstrengungen, alle Personen, die hier am Flughafen München arbeiten, gegen Cyberangriffe zu schützen. Sie unterstützen uns dabei, ein deutlich vollständigeres Bild der weltweiten Bedrohungslandschaft und der potenziellen Gefahren für den Flughafen München zu gewinnen. Das Threat Intelligence Portal gewährt uns einen einfachen und bequemen Zugang zu Threat Data Feeds, APT-Berichten und dem Threat Lookup Service. Außerdem bietet es uns ein nützliches API (Application Program Interface) und Werkzeuge zur Implementierung von automatisierter Datenverarbeitung für unsere bestehenden Sicherheitslösungen."

Cyber Threats News: www.securelist.com
IT Security News: kaspersky.de/blog/category/business/
IT Security for SMB: kaspersky.de/business
IT Security for Enterprise: kaspersky.de/enterprise

www.kaspersky.de

kaspersky **BRING ON THE FUTURE**