Transparenz für die Netzwerksicherheit

Verkehrsbetriebe Zürichsee und Oberland AG nutzen Penetrationstest

Referenzprojekt

© Verkehrsbetriebe Zürichsee und Oberland AG

„Mit dem Penetrationstest von T-Systems/Deutsche Telekom Security haben wir Transparenz über unser Netzwerk erhalten und können das Sicherheitsniveau zielorientiert erhöhen."

Dominik Trachsel, Leiter ICT, Verkehrsbetriebe Zürichsee und Oberland AG

Über 60.000 Fahrgäste täglich vertrauen auf das Transportangebot der Verkehrsbetriebe Zürichsee und Oberland AG (VZO). Mit über 300 Mitarbeitenden stellt das Unternehmen sicher, dass Pendler, Schüler und Gelegenheitsfahrer innerhalb von 250 km^2 im Züricher Oberland und am rechten Zürichseeufer rechtzeitig und zuverlässig ihre Fahrziele erreichen. Die VZO stellt der Bevölkerung ein optimales Verkehrsangebot für den Wirtschaftsraum Zürich bereit – und leistet ihren Beitrag zum Umweltschutz. Die Qualität der Leistungen belegen auch Messungen des Zürcher Verkehrsverbunds, welcher als Auftraggeber der VZO fungiert.

Das Verkehrsunternehmen unterhält eine topmoderne Flotte mit über 100 Bussen. Aber es investiert auch stark in seine Mitarbeitenden. So wurde es 2021 mit dem Swiss Arbeitgeber Award ausgezeichnet, der bedeutendsten Auszeichnung für Arbeitgeberattraktivität in der Schweiz. Regelmässige Weiterbildungen des Personals sowie betriebliche Gesundheitsförderung gehören zu den Leistungen, welche die VZO ihren Mitarbeitenden anbietet.

Mit der Corona-Pandemie verschoben sich auch die Arbeitsumfelder innerhalb der VZO – wesentlich weniger Menschen nutzten das Verkehrsangebot, Mitarbeitende mit Büroarbeitsplätzen arbeiteten vermehrt aus dem Home Office.

Die Verantwortlichen waren sich bewusst, dass die neue Arbeitssituation auch im Hinblick auf die Cybersicherheit relevant ist. Ein erfolgreicher Cyberangriff könnte den kompletten Betrieb massiv behindern. Sie entschlossen sich, ihre IT-Security-Kapazitäten auf den Prüfstand zu stellen und schalteten dazu die Sicherheitsexperten von T-Systems/Deutsche Telekom Security ein.

Auf einen Blick

- Wunsch nach Erhöhung des Sicherheitsniveaus
- Bestandsaufnahme über Lage der IT-Sicherheit
- Beauftragung Deutsche Telekom Security
- Penetrationstest: Externer Blick offenbart Stärken und Schwächen
- Konsequente Analyse der Schwachstellen
- Risikobewertung
- Priorisierte Handlungsempfehlungen
- Volle Transparenz über Schwächen
- Sicherstellung des Geschäftsbetriebs auch bei kontinuierlich steigender Bedrohungslage

T Systems

Let's power higher performance

Referenz im Detail

Herausforderung

Die VZO nahm die veränderte Situation zum Anlass, ihre Cybersecurity kritisch zu überprüfen. Dazu setzte sie zum einen auf eine Sensibilisierung der Mitarbeitenden, zum anderen wollte sie aber auch Technologien, Prozesse und Methoden innerhalb der IT selbst überprüfen. Mögliche Schwachstellen sollten erkannt, evaluiert und behoben werden, so dass das Unternehmen auch in Zukunft seinen Geschäftsbetrieb – bei einer zunehmend verschärften Risikolage – zuverlässig aufrechterhalten kann. Sie beauftragte Experten von T-Systems/Deutsche Telekom Security mit einem Sicherheitscheck und einem Risk Assessment.

Lösung

Externe Penetrationstests sind eine bewährte und effiziente Methode, den aktuellen Sicherheitszustand von (Informations-) Systemen technisch und objektiv zu überprüfen. Mittels Penetrationstests werden Netzwerke, Systeme und/oder Applikationen überprüft. Vor der Überprüfung legten die VZO-Verantwortlichen und Deutsche Telekom Security den Umfang, die Ziele und die Vorgehensweise in einer so genannten „Permission to Attack“ fest.

Innerhalb von zwei Monaten untersuchten die Sicherheitsexperten das Netzwerk der VZO intensiv. Über öffentliche Quellen werden zunächst Informationen gesammelt, die potenzielle Eingangstore für einen Angriff identifizieren. Automatisierte Port Scans steuern Informationen über die Services und Betriebssysteme bei.

Auf Basis der gewonnen Informationen bewerteten die Security-Experten das Risiko der gefundenen Schwachstellen. Um das Risiko des Unternehmens zu minimieren und die identifizierten Lücken zu schliessen, unterbreiteten die Experten eine priorisierte Liste von Lösungsvorschlägen. Die Ergebnisse der Überprüfung wurden in einem Bericht dokumentiert, der eine Zusammenfassung der Ergebnisse und eine Beschreibung des verwendeten Ansatzes sowie eine Analyse jeder Schwachstelle enthält. Er enthält auch die Risikoeinschätzung, eine Auflistung der betroffenen Systeme, eine Beschreibung inklusive der Auswirkung der Schwachstelle, eine Massnahmenempfehlung sowie Nachweise der Schwachstellen.

Kundennutzen

Mit der Analyse durch externe Experten gewinnen die Verantwortlichen der VZO Transparenz über die Stärken und Schwächen des Netzwerks. Die Priorisierung und Risikobewertung erlaubt ihnen, zielorientiert und effizient eventuelle Schwachstellen zu schließen und so das Sicherheitsniveau des Unternehmens dauerhaft zu erhöhen. Die VZO stellen so den Geschäftsbetrieb auch vor dem Hintergrund einer zunehmend verschärften Bedrohungslage sicher.

Kontakt
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
E-Mail: referenzen@t-systems.com
Internet: www.t-systems.com

Herausgeber
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland

Letzte Änderung : 11/2022 | Konzipiert durch: Creative Factory, TSIN