Advanced Threat Protection: Technologiekonzern erweitert Partnerschaft mit Retarus

Der marktführende Technologiekonzern mit Hauptsitz in Deutschland entwickelt, produziert und vertreibt eine breite Palette modernster Kommunikations-, Informations- und Sicherheitstechnik für die Wirtschaft und den öffentlichen Sektor. Das Unternehmen erzielt mit rund 11.000 Mitarbeitern in über 70 Ländern einen Umsatz von zwei Milliarden Euro.

AUSGANGSSITUATION Langjähriges Vertrauen

Der Technologiekonzern zählt zu den weltweit führenden Anbietern von Messtechnik, Fernseh- und Hörfunktechnik, Funktechnik und Cybersicherheit und beliefert neben Kunden in der privaten Wirtschaft, etwa in der Automobilindustrie, auch Betreiber kritischer Infrastrukturen, Forschung und Lehre sowie Behörden und Streitkräfte. Das Unternehmen schützt seine E-Mail-Infrastruktur bereits seit über zehn Jahren effektiv mit der bewährten Essential Protection mit vier unterschiedlichen, parallel eingesetzten Virenscannern der Retarus Email Security vor Viren, Spam und weiterer Malware. Mit der zunehmenden Verbreitung von Advanced Threats sah die IT-Abteilung des Konzerns die Notwendigkeit, die insgesamt rund 16.000 Mailboxen der Mitarbeiter sowie Funktionspostfächer noch umfassender abzusichern und die Essential Protection durch die Advanced Threat Protection (ATP) und durch die patentierte Patient Zero Detection® (PZD) von Retarus zu ergänzen.

ZIELSETZUNG Schutz vor Advanced Threats

Neben der Flut aus gewöhnlichen Spam- und Viren-Mails, welche die Retarus Essential Protection bereits seit Jahren zuverlässig von den Mailboxen des Konzerns fernhält, registrierte die IT-Abteilung zunehmend komplexere Bedrohungen wie Phishing- und Social-Engineering-Angriffe. Ziel war es, durch eine Verbesserung des Schutzniveaus solchen Advanced Threats effektiv vorzubeugen. Dabei sollte die IT-Abteilung des Unternehmens möglichst nicht mit zusätzlichen Aufgaben belastet werden, da diese parallel eine Migration von Lotus Notes/Domino zu Microsoft Exchange realisieren musste. Dementsprechend bestand die Voraussetzung, dass die eingesetzte Email-Security-Lösung samt Advanced Threat Protection zuverlässig mit beiden E-Mail-Systemen funktioniert. Außerdem sollte

die Security-Lösung flexibel skalierbar sein, um Tochterunternehmen und Firmenzukäufe weltweit anbinden zu können. Nicht zuletzt spielen für den Konzern, der Kunden in sicherheitsrelevanten Sektoren hat, Ausfallsicherheit und Datenschutz eine essenzielle Rolle.

HERAUSFORDERUNG Permanente Feinjustierung der Systeme

Die Advanced Threat Protection (ATP) von Retarus, die neben einer zuverlässigen CxO-Fraud-Detection das Sandboxing-System des Partners Palo Alto beinhaltet, wurde zunächst in einem vierwöchigen Proof of Concept (PoC) getestet. Zusätzlich wollte sich der Technologiekonzern mit der patentierten Retarus Patient Zero Detection® absichern. Diese identifiziert besonders perfide Malware (Patient Zeros), falls diese trotz ausgeklügelter ATP-Mechanismen in das Unternehmensnetz gelangt ist, sehr schnell und alarmiert Administratoren und Anwender unverzüglich. Den PoC haben die Security-Experten von Retarus mit permanenten Abstimmungen und Feinjustierungen der Systeme begleitet, die Zwischenergebnisse wurden wöchentlich mit den Ansprechpartnern des Technologiekonzerns besprochen und weiter optimiert. Nach der positiven Abschlussbesprechung hat der Konzern die Retarus Services mit den im PoC erarbeiteten Optimierungen übernommen.

> *Mit Retarus hat der Technologiekonzern einen langjährigen, verlässlichen Partner im Bereich E-Mail-Sicherheit. Dank unserer zuverlässigen und innovativen Services ist das Unternehmen auch vor Advanced Threats und Social-Engineering-Angriffen auf seine Mitarbeiter optimal geschützt. Im Proof of Concept haben wir die Services gemeinsam mit dem Kunden an seinen Bedarf angepasst und setzen im Rahmen des Retarus Service Managements kontinuierlich weitere Optimierungen um.*
>
> Miriam-Carena Schmitt, Vice President Expert Sales D-A-CH, retarus GmbH

NUTZEN UND VORTEILE Zusätzliche Optimierungen durch Retarus Service Management

Mit den Bausteinen Essential Protection, Advanced Threat Protection und Patient Zero Detection® der Retarus Email Security hat sich der Technologiekonzern für eine Security-Lösung entschieden, welche die E-Mail-Infrastruktur des Unternehmens weltweit umfassend schützt und die eigene IT-Abteilung entlastet. Die redundante Anbindung im Retarus-eigenen Hauptrechenzentrum in München und in einem weiteren von Retarus in Frankfurt/Main betriebenen Rechenzentrum sorgt für die per SLA vereinbarte Ausfallsicherheit und die Einhaltung sämtlicher Datenschutzanforderungen des Technologiekonzerns. Im PoC wurden die Services von Retarus genau auf den Bedarf des Konzerns abgestimmt. Durch das hinzugebuchte Retarus Service Management erhält die Unternehmens-IT zusätzliche Serviceopti-

mierungen. Ein persönlicher Retarus-Ansprechpartner koordiniert Service- und Support-Anfragen und übernimmt gegebenenfalls das Eskalationsmanagement. In monatlichen Service-Calls und Service-Reports werden weitere Maßnahmen und Optimierungsempfehlungen abgestimmt sowie eventuell angefallene Tickets erläutert und protokolliert.

FAZIT UND AUSBLICK

Business Continuity weltweit

Mit Retarus Email Security verfügt der Technologiekonzern über einen Cloud Service, der sich nahtlos in die sich wandelnde Kommunikations-Infrastruktur einfügt und nach den strengen europäischen Datenschutzrichtlinien betrieben wird. Der Dienst, der nun um die Komponenten Advanced Threat Protection mit Sandboxing und CxO Fraud Detection sowie die patentierte Patient Zero Detection® von Retarus erweitert wurde, erfüllt die zentralen Anforderungen an Compliance sowie Business Continuity und bietet eine transparente Kostenstruktur. Zusätzliche Mailboxen von Tochterunternehmen und Firmenzukäufen weltweit lassen sich problemlos vollumfänglich mit absichern. Durch den vorangegangenen Proof of Concept sowie das hinzugebuchte Service Management sind die Retarus Services stets genau auf den Bedarf des Unternehmens abgestimmt.

KEY FACTS

- **Zuverlässige Erkennung neuer Viren- und Malware-Varianten**
- **Erweiterter Schutz vor Social Engineering**
- **Zuverlässige Erkennung der Empfänger von Patient Zeros**
- **Sofortige Alarmierung**
- **Detaillierte Reports und Analysen**
- **Entlastung der konzerneigenen IT**