USE CASE

Sandbox Security Instanz

Mails ohne Malware sind eine sichere Bank.

Projektumfeld

„Ihre persönlichen Daten auf dem Rechner sind verschlüsselt! Zahlen Sie innerhalb von fünf Tagen die geforderte Summe per Bitcoin. Ansonsten geht nichts mehr!“ Dieser Modus Operandi von kriminellen Hackern zählt nicht erst seit der großen Wannacry- und Petya-Attacke zum globalen Horrorszenario – und das für professionelle IT-Admins genauso wie für ganz normale Endanwender. Das Prozedere: Ein so genannter Cryptolocker hat als Attachment per E-Mail den Computer und oft auch ein ganzes Netzwerk mit Erpressersoftware infiziert. Dort startet er mit der Verschlüsselung von Dateien. Darunter vor allem Office-Dokumenten (xls, doc, ppt, etc.) oder sogar ganzen Datenbanken. Und dabei geht es den Erpressern in erster Linie um eins: Geld! Kein Wunder, dass entsprechende Angriffe dann besonders gern dort versucht werden, wo viel zu holen ist. In diesem Fall bei einer der traditionsreichsten deutschen Privatbanken, die zum Glück aber als langjähriger Kunde auch auf die Security-Expertise von Axians zählen kann.

Projektanforderungen & Projektziele

Daten werden erst in Form von Dokumenten zu lohnenden Informationen. Und genau auf diese haben es Angreifer abgesehen! Denn auch die Business Prozesse einer Bank basieren in weiten Teilen darauf, dass Anwender Office Dokumente per E-Mail erhalten bzw. versenden können. Und als derart attraktives Ziel wurde der Kunde bereits 2015 von der ersten größeren „Welle“ von Cryptolocker-Attacken erfasst. Die IT-Leitung der Bank beschloss daraufhin als erste Gegenmaßnahme, alle Mails mit Microsoft Dokumenten im Anhang zur genaueren Überprüfung in eine digitale Quarantäne zu stellen. Bei rund 1.000 involvierten Anwendern und entsprechend hohem E-Mail Aufkommen tagtäglich allerdings eine echte Mammutaufgabe – und auf die Dauer schließlich weder praktikabel noch akzeptabel. Wurden doch damit sehr viele essentielle Geschäftsvorgänge in der Bank und für deren Kunden drastisch verlangsamt. Gefragt war also eine effiziente und effektive Lösung, um alle E-Mails mit aktiven Inhalten schnell und sicher auf Malware, Trojaner oder sonstige bösen Überraschungen zu checken. Das Ganze umgesetzt vom Trusted Advisor der Bank, wenn es um wind- und wetterfeste Lösungen für betriebssichernde Anwendungskonzepte geht: Dem Axians Team für IT Security.

NUTZEN

- Keine aufwendige manuelle Prüfung tausender E-Mails mit Attachments
- Automatisierter Check auf potentielle Gefahren per Sandboxing
- Maximale Zuverlässigkeit beim Erkennen von Ransomware, Trojanern, etc.
- Schnelle Prozesse bei gesenkten Kosten

USE CASE

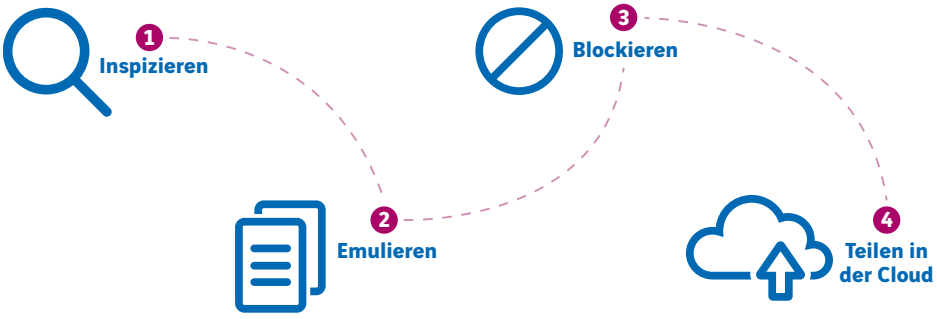
Sandbox Security Instanz

Umsetzung

Das Lösungsdesign von Axians bestand hier aus einer Verbindung der schon vorhandenen Check Point-Firewall mit einer neuen Sandbox Lösung. Sandboxing ist ein extrem effektives Konzept beim Überprüfen auf Malware. Denn ein eminentes Problem etwa bei Ransomware ist, dass dort so gut wie keine Signatur zweimal auftaucht – und daher alle klassischen signaturbasierten Virenscanner diese gar nicht erst erkennen können. Mit der Sandbox werden sowohl E-Mails wie auch Webtraffic vollautomatisch überprüft. In die Sandbox werden dazu neben ausführbaren Dateien (.exe und .scr), Java (.jar) und Flash (.swf) auch Dokumente mit eventuell aktiven Inhalten von MS Office und Adobe PDF geschickt sowie die gängigen Archiv-Formate (.zip, .tar, .tgz, usw.) verarbeitet. Per „Threat Extraction" werden dann alle potentiell gefährlichen Komponenten aus den Dateien entfernt und die Mails daraufhin mit minimaler Zeitverzögerung an den Empfänger geschickt. Für die schnelle Umsetzung bei der Bank war hier aber auch ein Kunstgriff von Axians gefordert. Denn eigentlich sollte der Kunde aus Revisionsgründen keine Cloud-Services nutzen. Allerdings war der Handlungsbedarf derart groß, dass Axians mit der vorhandenen Check Point-Firewall "kurzerhand" die cloudbasierte Anwendung für eingehende E-Mails aktivieren konnte. Damit wurden zunächst alle Mails mit Office Dokumenten von einer Sandbox in der Cloud gescannt. Nach wenigen Tagen erfolgte dann die Lieferung der on-site Lösung fürs Sandboxing an den Kunden – inklusive sofortiger Umstellung mit identischen Funktionalitäten beim Mail-Check.

Projektergebnis

Im Sinne einer gesicherten Geschäftstätigkeit der Bank war hier hohe Flexibilität bei der Umsetzung das erste Gebot. Insofern bildete bereits das „Up and Runnig" der Lösung nach wenigen Stunden den ersten Erfolgsfaktor. Denn dank Check Point-Firewall konnte Axians quasi unmittelbar nach der Anfrage das effektive Sandboxing in der Cloud starten. Und auch die darauf folgende on-site Konfiguration lief anschließend unter allen geforderten Aspekten perfekt. Das Arbeiten mit geschäftskritischen Office Dokumenten klappt ab sofort auf sicherer Grundlage, die manuelle Prüfung von E-Mails mit Attachments wurde automatisiert und damit sowohl zentrale Prozesse beschleunigt wie auch Kosten gespart. Aber das Wichtigste: Seit der Etablierung des Sandboxing verzeichnet der Kunde bei seiner IT keinen einzigen Befall durch Trojaner oder anderweitige Malware, der auf eingehende E-Mails zurückzuführen wäre!



ÜBER AXIANS

Axians in Deutschland ist ein agiles Unternehmensnetzwerk aus spezialisierten ICT-Dienstleistern und Softwareherstellern unter der globalen ICT-Marke Axians der VINCI Energies. Durch eine flächendeckende Präsenz in 24 Städten existiert eine unmittelbare Nähe zum Kunden. Das Netzwerk begleitet seine Kunden – privatwirtschaftliche Unternehmen, kommunale Verwaltungen, öffentliche Einrichtungen, Netzbetreiber und Service Provider – während der gesamten ICT-Prozesskette. Die Kernkompetenzen aus IT-Lösungen, IT-Sicherheit, Netzwerkinfrastruktur und Netztechnik werden durch eigene Branchensoftware ergänzt und unterstützen den Kunden bei allen Anforderungen der Core-ICT und der digitalen Transformation. Durch die Kombination aus Beratung, Implementierung, Service und Betrieb können Kunden Technologien und Applikationen genau nach Bedarf nutzen, Prozesse optimieren und ihre digitalen Geschäftsstrategien zukunftssicher umsetzen. Mit 1.700 Spezialisten stellt Axians in Deutschland für jede Herausforderung eine individuelle Lösung mit dem besten Team aus dem Netzwerk bereit.

ANSPRECHPARTNER

Dirk Demuth (Vertrieb, Axians IT Security) · E-Mail: info-itsecurity@axians.de · Tel.: +49 40 271661-0

axians.de

Stand 07/17

VINCI ENERGIES