USE CASE

Sicher vor Ransomware

Die Mail-Check-Offenbarung: Aktueller als der Angreifer!

Projektumfeld

Arbeiten am PC. Oder mobil. In einer Firma mit vielen Kollegen und Partnern in aller Welt. Da ist die Mailbox zigmal am Tag der zentrale Anlaufpunkt. Dann ein falscher Klick... schon ist Feierabend! Denn Ransomware im Anhang nimmt den eigenen Rechner als Geisel – und wenn möglich auch gleich das ganze Unternehmensnetzwerk dazu. Und ob WannaCry, Petya oder die neueste kriminelle Kreation, ob reine Geldgier oder generelle Sabotage als Motiv: der Schaden durch gesperrte und verlorene Dateien ist in jedem Fall enorm. Genau mit dieser Art von Bedrohung sah sich der Auftraggeber des hier vorgestellten Projekts konfrontiert. Bei dem langjährigen Axians Kunden handelt es sich um einen international tätigen deutschen Hersteller von Maschinen und Anlagen für die Genussmittelindustrie. Darüber hinaus ist das betroffene Unternehmen – und damit eben auch sein IT-Netzwerk – Teil eines weltweit engagierten Technologiekonzerns mit über 10.000 Mitarbeitern an rund 100 Standorten rund um den Globus.

Projektanforderungen & Projektziele

Mehrere E-Mail-Eingänge mit zerstörerischen Trojanern, sogenannter Ransomware, im Anhang hatten 2016 das angesprochene Maschinenbau-Unternehmen alarmiert – und nach einem Hilferuf der IT-Abteilung schließlich die Spezialisten von Axians auf den Plan gerufen. Denn hier ging es um nichts weniger, als für alle Angestellten in der Firma die tägliche Arbeit mit modernen Kommunikationsmedien wieder auf eine sichere Grundlage zu stellen. Selbstverständlich verfügte der Kunde bereits über Antiviren-Programme, Anti-Spyware-Tools oder Browser-Plugins, die seine IT vor Attacken schützen sollten. Eine fatale Folge davon ist freilich auch ein trügerisches Sicherheitsgefühl bei den Nutzern! Denn im Wettlauf zwischen Cyberkriminellen und Sicherheitstechnik entwickeln Angreifer heute fast täglich auch immer trickreichere Waffen und Methoden. Konkret galt es daher für Axians, eine maximal effektive Lösung für den sicheren Mailverkehr von rund 7.000 Mitarbeitern zu etablieren. Mit einem Konzept, das auch auf aktuellste Bedrohungen zuverlässig reagiert und dabei den Empfang von E-Mails möglichst ohne Verzögerungen gewährleistet.

NUTZEN

- Schutz vor E-Mails mit Ransomware-Attachments
- Erkennung von Malware bereits in der Exploit-Phase
- Kombi von Erkennung auf CPU-Ebene mit Sandboxing auf Ebene des Betriebssystems.
- On-Premise Lösung für Mails von rund 7.000 Mitarbeitern
- Auch Schutz vor Zero Day Exploit Attacken

USE CASE

Sicher vor Ransomware

Umsetzung

Nach eingehender Analyse des Bedrohungspotentials einerseits und der Infrastruktur beim Kunden andererseits, empfahl das Axians Team eine Sicherheits-Lösung aus zwei Security-Appliances in der E-Mail Kette des Unternehmensnetzwerks. Das Prinzip: Effiziente Gefahrenabwehr mit umgehungssicherem Sandboxing inklusive Threat Extraction. Und weil es sich dabei um hochinnovative „Emerging Technologies" handelt, war hier auch die spezielle Expertise des Axians Teams gefordert. Die entscheidendste Innovation bei diesem Konzept stellt ganz sicher die antizipierende Gefahrenerkennung auf CPU-Ebene dar. Der Kunstgriff dabei ist es, Bedrohungen schon vor dem Zeitpunkt der Infizierung zu erkennen – also geplante Angriffe zu stoppen, bevor die Malware überhaupt eine Chance hat, auf dem PC oder im Netzwerk aktiv zu werden. Genau das bedeutet einen fundamentalen Vorteil gegenüber den konventionellen Sandbox-Konzepten, die zum einen mehr Zeit für die Identifikation erfordern und zum anderen mit ihren Erkennungsstrategien vor neuartigen Umgehungsversuchen des Öfteren schlicht kapitulieren müssen. Dagegen steht jetzt das neue kombinierte Sicherheitskonzept für den Kunden: Threat Emulation plus Threat Extraction als Kombination aus innovativer Identifizierung auf CPU-Ebene mit neu ausgewertetem Sandboxing als weitere Instanz auf der Ebene des Betriebssystems. Sprichwörtlich nach der Devise: Vorsicht ist besser als Nachsicht!

Projektergebnis

Seit August 2016 ist das neue Sicherheitskonzept beim Kunden aktiv. Und Mails aller Art sind somit dort keine Gefahrenquelle für die IT-Infrastruktur mehr. Die Lösung sorgt für eine umgehende Lieferung sicherer Dateiversionen wie unter anderem MS Office, PDF oder Flash. Selbst ein Zero Day Exploit Attack (ZETA), also ein Angriff am selben Tag, an dem eine Schwachstelle in einer Software entdeckt bzw. ausgenutzt wird, ist dank der Erkennung von Malware in der Exploit-Phase ausgeschlossen. Statt dessen erfolgt jetzt für alle Anwender die sofortige Bereitstellung von sicheren Inhalten – oder eben von zuverlässig „entschärften" Versionen potenziell gefährlicher Dateien. Und das Ganze, ohne den Geschäftsbetrieb in irgendeiner Weise zu unterbrechen.

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

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

axians.de

Stand 07/17

VINCI ENERGIES