McAfee OpenDXL im Praxistest

solutionIT

Partnerprofil:
solutionIT ist ein ITSicherheits-dienstleister und Systemhaus mit mehr als 15 Jahren Erfahrung im Bereich Security.

IT-Umgebung:
Das Unternehmen verfügt über langjährige Expertise z.B. für Netzwerk- und Gateway-Sicherheitsprodukte. Die Berater und Techniker von solutionIT betreuen Kunden aus verschiedensten Branchen und von unterschiedlicher Unternehmens-größe. Das Team bietet sowohl Analysen und Konzepte als auch Implementierungen von IT-Infrastrukturen und Netzwerken.

IT-Sicherheit ist ein Teamsport: Erst der Austausch von Bedrohungsinformationen ermöglicht den ganzheitlichen Schutz eines Unternehmens. Die IT-Sicherheitsexperten der solutionIT setzen daher auf den McAfee Data Exchange Layer (DXL), um Lösungen verschiedener Hersteller zu integrieren.

Die solutionIT GmbH mit Sitz im norddeutschen Bad Oldesloe ist ein Systemhaus und Beratungsunternehmen mit Fokus auf IT-Sicherheit. Die Mitarbeiter kümmern sich deutschlandweit um Unternehmen aller Branchen und Größen – und bieten umfassenden IT-Service von der Analyse über Konzepte bis zur Implementierung und Betreuung von IT-Infrastrukturen und Unternehmensnetzen. Eine der Kernaufgaben der solutionIT ist es, die IT-Sicherheit ihrer Kunden zu gewährleisten. Dabei stießen die Berater immer wieder auf die Herausforderung, verschiedene Sicherheitssysteme in einem Unternehmensnetz miteinander abzustimmen.

„Unternehmen können sich die beste Firewall und das teuerste Web Gateway anschaffen, doch erst die Vernetzung beider Systeme bringt die PS auf die Straße", kommentiert Olaf Otahal, Geschäftsführer der solutionIT. „Wenn die Firewall einen Angriff registriert, muss sie die Bedrohungsinformationen weitergeben. Sonst bleiben die anderen Systeme blind und der Angreifer im Vorteil."

Austausch der Bedrohungsinformationen

Die solutionIT pflegt seit 15 Jahren eine enge Partnerschaft mit McAfee. Als diese 2016 mit dem McAfee Data Exchange Layer (DXL) eine neue Open-Source-Strategie einschlugen, war für die solutionIT die Gelegenheit gekommen, die Integration der Sicherheitssysteme konkret umzusetzen. Der McAfee Data Exchange Layer ermöglicht den herstellerübergreifenden Austausch zwischen verschiedenen Sicherheitssystemen im Unternehmen. Dabei werden die Informationen nicht nur über die DXL-Schnittstelle weitergereicht, sondern auch angereichert und zur Weiterverarbeitung vorbereitet.

„Der Data Exchange Layer ist für uns die Antwort auf unsere Frage nach einer besseren Vernetzung verschiedener Sicherheitssysteme", erklärt Otahal. „Durch die Öffnung der Schnittstelle mit OpenDXL war für uns der Zeitpunkt gekommen, das System in der Praxis zu testen. Und ich kann sagen: wir sind begeistert. Die Flexibilität und strukturierte Einfachheit bei der Arbeit mit OpenDXL ist beeindruckend. Für uns stellen derartige Integrationen einen deutlichen Mehrwert bei der Betreuung und Bindung unserer Kunden dar."

OpenDXL im Praxistest

Ende 2016 begann die solutionIT mit der Umsetzung, zunächst als Demonstration einer Standardumgebung für Kunden. Der Data Exchange Layer war schnell aufgesetzt und zeigte eine Store&Forward- sowie eine Push-Integration aus McAfee-Produkten und einer Forcepoint-Firewall, bei der automatisch erzeugte Sicherheitsbedrohungen und deren Abwehr live verfolgt werden können.

Bei der Store&Forward-Integration werden Meldungen über bösartige IP-Adressen, URLs und Hashwerte sowie situationsabhängige Meldungen (etwa zu DDoS-Attacken) zentral in einer Threat Intelligence Platform zusammengetragen. So können die einzelnen Informationen anderen Sicherheitsvektoren zugeteilt werden. Es bilden sich Bedrohungsdatenbanken, die Unternehmen innerhalb oder außerhalb mit anderen Unternehmen austauschen können.

Beim Ansatz der direkten OpenDXL-Integration erfolgt keine Zwischenspeicherung. Stattdessen werden alle erreichbaren Netzwerkkomponenten innerhalb kürzester

So funktioniert OpenDXL

Ein Unternehmen sichert in diesem Beispiel seine Infrastruktur mit einer Firewall. Diese nimmt jeglichen Zugriff von innen wie außen wahr und blockt externe Angriffsversuche – vom Port Scan über Exploits bis zur DoS-Attacke. Damit endet traditionell die Aufgabe der Firewall, obwohl sie bei ihrer Arbeit wertvolle Informationen registriert wie die Art des Angriffs und die IP des Angreifers. Doch diese Informationen werden bisher nicht weiter genutzt.

Mit dem Data Exchange Layer können Informationen an nachgelagerte Systeme übertragen und ausgewertet werden. Die Erkenntnisse lassen sich anreichern und wieder zurückspielen, etwa um die Firewall eine automatische Block-Liste mit IPs aus dem Quellbereich des Angreifers füllen zu lassen. So werden zukünftige Angriffsversuche schneller unterbunden. Auf der anderen Seite können die Erkenntnisse auch an andere Systeme weitergereicht werden, die über eine DXL-Schnittstelle verfügen – etwa ein Web Gateway, das einem Client Zugriffe auf die ermittelten IP-Adressen verbietet. So können über Herstellergrenzen hinweg Bedrohungsinformationen ausgetauscht und angereichert werden, um einen ganzheitlichen Schutz der Infrastruktur zu erreichen. Die einzige Voraussetzung: Die einzelnen Systeme benötigen eine DXL-Schnittstelle.

Zeit geschützt. Zu diesem Zweck ist beispielsweise die zentrale Forcepoint-Verwaltungskonsole SMC in der Lage, IP-Adressen direkt an das McAfee Web Gateway und den McAfee TIE-Server weiterzuleiten. Über die Information an den TIE-Server werden alle vorhandenen McAfee-Sicherheitslösungen ebenfalls automatisch informiert.

„DXL erhöht unsere Sicherheit und die angereicherten Bedrohungsinformationen sind für uns ein weiteres Schutzkriterium. Es wäre fahrlässig, wenn wir die Vorteile nicht auch selbst nutzen würden – die Feldtauglichkeit des OpenDXL-Standards war für uns schnell bewiesen. So haben wir aus einer Demo-Umgebung schnell eine Produktionsumgebung für uns selbst gemacht", erklärt Otahal.

Auch die Kunden der solutionIT wissen den Mehrwert zu schätzen. Die Vernetzung ihrer bestehenden Security-Systeme sorgt für ein höheres Schutzniveau sowie einen sehr hohen Automatisierungsgrad ihrer IT Security. Dabei fallen weder große Investitionen an noch entsteht ein besonderer Aufwand.

Der Vorteil der Offenheit: OpenDXL vermehrt gefragt

„In den letzten Monaten sehen wir bei unseren Kunden ein enormes Interesse heranwachsen. Die Anbindung von Lösungen mittels DXL-Schnittstelle ist dank OpenDXL einfach universell geworden – das führt dazu, dass wiederum die Effektivität des ganzen Systems steigt. Denn ganzheitliche Sicherheit bedeutet im besten Falle, dass das ganze System angeschlossen ist", ergänzt Otahal.

In Zukunft sieht die solutionIT ein starkes Wachstum für OpenDXL voraus. Der Plan sieht daher neben der Portierung der DXL-Systeme für Kunden auch eine Weiterentwicklung der Standardumgebung – mit zusätzlichen Angriffsszenarien, neuen Interaktionen und proaktiven Maßnahmen bei bestimmten Ereignissen vor. Außerdem ist die Integration von McAfee Advanced Web Defense im Gespräch. So wird der ganzeinheitliche Schutz für Unternehmen mit McAfee und der solutionIT stetig weiterentwickelt und immer wieder den neusten Bedrohungen angepasst.

Die Zukunft wird spannend

Stephan Lehniger, Channel Technical Manager, blickt nach vorne: „Wir haben mit der solutionIT, einem langjährigen, aktiven und treuen Partner, die Grundlage für eine neue Dimension der Zusammenarbeit geschaffen: Die Potenziale aus Multi- und Single-Vendor-Integrationen können den heutigen Standard unserer Sicherheitsumgebungen und deren Sicherheitsniveau um ein Vielfaches steigern. Wir arbeiten fokussiert mit Partnern daran, Kunden diese Mehrwerte in den verschiedensten Lösungskombinationen zugänglich zu machen und ich bin gespannt, was wir bereits in wenigen Monaten alles an lauffähigen Umgebungen im Feld sehen werden."

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de