Presseinformation

SecuStack nutzt SCONE und die Intel® Software Guard Extensions für neuartige sichere Cloud-Anwendungen

[Essen, 17. September 2020] **SecuStack, das sicherheitsgehärtete Cloud-Betriebssystem made in Germany, unterstützt bald die Intel® Software Guard Extensions (SGX) Enklaven auf Basis der SCONE Plattform von Scontain. Dadurch lassen sich Cloud-Anwendungen in den Bereichen maschinelles Lernen (ML) und verteiltes Rechnen (Multi-Party Computing) zur sicheren Übertragung von Daten realisieren. So können etwa Krankenhäuser ML-Modelle zur Übertragung und Verarbeitung von Patientendaten nutzen, während die Daten selbst vor dem Zugriff des Cloud-Providers geschützt bleiben. Intel SGX ermöglicht den Datenaustausch auch bei fehlendem Vertrauen in den Cloud-Provider.**

Der Anbieter der SecuStack Plattform, die secustack GmbH, ist ein Joint Venture der secunet Security Networks AG und der Cloud&Heat Technologies GmbH. SecuStack richtet sich an Unternehmen und Behörden mit sicherheitskritischen Anwendungen.

SecuStack ist ein Cloud-Betriebssystem, das auf der Basis von “Infrastructure-as-a-Service” (IaaS) einfach und sicher Ressourcen für den Betrieb von Cloud-Anwendungen bereitstellt. Die Plattform ist als Erweiterung von OpenStack konzipiert und damit voll kompatibel. Auf transparente Weise integrierte kryptographische Mechanismen ermöglichen die sichere Übermittlung, Speicherung und Verarbeitung von Daten sowie die Vernetzung von Ressourcen in einer OpenStack Umgebung. Dank SecuStack können verschiedene Branchen erstmals Cloud Computing nutzen, die das aufgrund hoher Sicherheitsanforderungen oder aus mangelndem Vertrauen bisher nicht konnten oder wollten.

Ein Beispiel bildet das Gesundheitswesen. Im Rahmen der zunehmenden Digitalisierung bestand für Krankenhäuser durch Sicherheits- und Datenschutzbestimmungen häufig kein Zugang zu Patientendaten. Nun können die anonymisierten Rohdaten von berechtigten Institutionen verwendet, aggregiert und analysiert werden, um wichtige medizinische Erkenntnisse zu gewinnen.

Mit Intel SGX ausgestattete CPUs können kritische Infrastrukturdienste wie Identitätsmanagement, Schlüsselmanagement oder VPN-Dienste innerhalb von vertrauenswürdigen, hardwaregeschützten Enklaven ausführen. Intel SGX stellen dabei eine weitere Schutzebene für die Integrität und Vertraulichkeit von Programmcode und Daten außerhalb der CPU zur Verfügung und erhöhen damit die Hürde für Angreifer enorm. Dies sorgt für zusätzliche, zuvor nicht vorhandene Sicherheit in der Infrastrukturschicht. Mit der SCONE Plattform von Scontain können Dienste in Intel SGX-Enklaven einfach integriert, ausgeführt und damit Funktionen wie Laufzeitverschlüsselung, Secrets Management und Autorisierung besonders sicher in SecuStack integriert werden. Die Kombination von Intel SGX-Enklaven mit einer Open-Source-basierten, gehärteten und kryptographisch abgesicherten Infrastrukturschicht bietet den umfassendsten Schutz, der heute verfügbar ist. Sie bietet Sicherheit für Daten und Anwendungen, ohne die Hoheit darüber zu gefährden. Die Integrität der Infrastrukturschicht bleibt gewahrt.

Neben der Infrastruktur-Absicherung unterstützt SecuStack künftig auch Confidential Cloud Native Applications. Anwendungsdienste laufen damit beispielsweise innerhalb von Intel SGX-Enklaven eines Kubernetes-Clusters. Eines der Ziele dabei ist es, maschinelles Lernen mit vertraulichen Daten zu ermöglichen. So können Anwender etwa ihre TensorFlow und PyTorch Modelle in einem sicheren Kontext trainieren. Dabei bleiben selbst die Trainingsdaten, der Code und die Modelle geschützt, die Cloud-Provider haben keinen Zugriff. Auf diese Weise lassen sich neuartige Anwendungen umsetzen. Ein Beispiel: Krankenhäuser, die eine sichere Cloud-Infrastruktur mit SecuStack nutzen, können mit der SCONE Plattform lokales maschinelles Lernen

Presseinformation

mit vertraulichen Daten umsetzen. Die ML-Modelle bleiben lokal und können dennoch mit Modellen anderer Krankenhäuser kombiniert werden (Confidential Federated Machine Learning). So können ML-Modelle krankenhausübergreifend trainiert werden, ohne dass Patientendaten das Krankenhaus, zu dem sie gehören, verlassen müssen. Der Datenschutz bleibt jederzeit gewährleistet.

Mehr Informationen zu SecuStack erhalten Sie auf der folgenden Website: www.secustack.de.

Pressekontakt

Patrick Franitza
Pressesprecher

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen/Germany
Tel.: +49 201 5454-1234
Fax: +49 201 5454-1235
E-Mail: presse@secunet.com
http://www.secunet.com

Über secunet

secunet ist einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Mehr als 600 Experten konzentrieren sich auf Themen wie Kryptographie, E-Government, Business Security und Automotive Security und entwickeln dafür innovative Produkte sowie hochsichere und vertrauenswürdige Lösungen. Zu den mehr als 500 nationalen und internationalen Kunden gehören viele DAX-Unternehmen sowie zahlreiche Behörden und Organisationen. secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit. secunet wurde 1997 gegründet und erzielte 2019 einen Umsatz von 226,9 Millionen Euro. Die secunet Security Networks AG ist im Prime Standard der Deutschen Börse gelistet.

Weitere Informationen finden Sie unter www.secunet.com.