TLS-Traffic analysieren

Frühjahr 2019

www.ix.de

iX KOMPAKT

Ein Sonderheft des Magazins für professionelle Informationstechnik

IT-SICHERHEIT

Praxiswissen

Zugang zum LAN kontrollieren

Security Operations Center – machen oder mieten?

Pentesting von A bis Z:
Wie Red Teams arbeiten

Regulierung

DSGVO: Risikofolgenabschätzung unerlässlich

Der „Stand der Technik“ in der IT-Sicherheit

Security-Trends

Selbstschutz zur Laufzeit

Malware-Erkennung mit KI

Werkzeuge

DSGVO-konforme Datenhaltung

Absicherung von Containern

Durchbruch bei Spectre & Co.:

CPU-Lücken vorhersagen

storage2day

17.–19. September 2019

Print Media Academy,
Heidelberg

Die Konferenz
zu Speichernetzen
und Datenmanagement

PROGRAMM ONLINE
Frühbucher bis 26.07.2019

AUSZUG AUS DEM PROGRAMM:

- **Software Defined Storage**
  - SDS-Grundlagen
  - Erasure Coding
  - Praxisbericht: SDS im Petabyte-Bereich
  - Einführung, Betrieb und Ausbau einer produktiven Ceph-Umgebung
- **Cloud-Storage**
  - Grundlagen des Cloud-Storage
  - Cloud-Sicherheit
  - Cloud-Storage und DSGVO
- **Archivierung und Backup**
  - Revisionssichere Speicherung sensibler Daten
  - Disaster Recovery
  - Die Zukunft von Tape Storage
- **Storage-Infrastruktur und Vernetzung**
  - NVMe-oF – Grundlagen und Möglichkeiten
  - Sichere Dateidienste
  - Speicherinfrastrukturen für Künstliche Intelligenz

www.storage2day.de

Platinsponsor

THOMAS KRENN®

Goldsponsoren

aikux.com · cisco · CLOUDIAN · DATACORE · FUJITSU · PURESTORAGE

Silbersponsoren

EUROstor · Lenovo · TOSHIBA

Veranstalter

iX · dpunkt.verlag

Gefühlte Sicherheit

Mit der IT-Sicherheit ist es ein wenig wie mit dem Radfahren: Viele Velobegeisterte setzen sich einen Helm auf, verzieren ihre Jacken mit grell fluoreszierenden Accessoires und denken „jetzt kann mir nichts mehr passieren“. Ähnlich tickt die IT-Welt: Systemverantwortliche sowie Manager sind häufig der Ansicht, der Kauf einer Firewall oder anderer Sicherheitssysteme genüge, um ein ausreichendes Maß an Schutz im Unternehmen zu gewährleisten. Sie fühlen sich sicher.

Nun wird, anders als oft beim Fahrradhelm, der Nutzen eines IT-Sicherheits-Devices nicht grundsätzlich bezweifelt. Gemeinsam ist aber – oder sollte zumindest sein – die Erkenntnis, dass für Sicherheit noch eine Menge mehr vonnöten ist als eine solche singuläre Maßnahme. Das zeigt sich, um noch einen Moment im Bild zu bleiben, an Ländern, in denen es weniger gravierend Verletzte oder gar Tote gibt als hierzulande, obgleich die Zahl der Helmtragenden niedriger ist. Grund dafür ist eine sichere Infrastruktur, eine rechtliche Regulierung, die auch durchgesetzt wird, sowie ein geschärftes Bewusstsein für Gefahren bei allen Beteiligten.

All diese Faktoren lassen sich problemlos auf die IT-Sicherheit übertragen und finden sich auch in diesem Sonderheft wieder. Neben Marktübersichten mit durchaus nützlichen Tools (ab Seite 103) zeigen praxisorientierte Artikel (ab Seite 27), wie man mit grundlegenden Sicherheitsmaßnahmen, etwa der Authentifizierung oder Verschlüsselung, zu einer sicheren Infrastruktur beitragen kann. Auch neuere Trends wie das Vorfiltern von Malware mittels KI oder das isolierte Ausführen von Anwendungen in Containern können ein Mehr an Sicherheit bewirken (ab Seite 7).

Orientierung durch Standards wie die ISO27000er Familie oder IT-Grundschutz sowie rechtliche Regulierungen gibt es schon lange. Aber erst durch das scharfe Schwert der DSGVO, die ja IT-Sicherheit nicht nur vorschreibt, sondern bei Sicherheitsvorfällen die Nachlässigkeit auch empfindlich bestraft, erlangen die regulatorischen Vorgaben eine neue Bedeutung. Das Sonderheft fasst die wichtigsten zusammen (ab Seite 137).

Ein besonderes Highlight der vorliegenden Ausgabe ist die Artikelserie rund um das Thema Red Teaming (ab Seite 61). Die Beiträge bieten eine vertiefende Einführung in nahezu alle Aspekte dieser Form von Sicherheitstests – von der vorbereitenden Informationsbeschaffung über das gezielte Manipulieren von Mitarbeitern und das Eindringen in die Firmen-IT bis hin zum Aufbau von Kontrollstrukturen durch den Angreifer. Unternehmen werden so sensibilisiert, lernen ihre Schwächen und Sicherheitslücken kennen und können zukünftige Angriffe besser erkennen und im Idealfall auch abwehren.

Das iX kompakt Security, das die wichtigsten, noch einmal aktualisierten Sicherheitsartikel der letzten Monate aus der iX versammelt, soll dazu beitragen, alle Sicherheitsaspekte ins Bewusstsein zu bringen. Damit aus der eingangs dargestellten „gefühlten Sicherheit“ ein wenig mehr reale Sicherheit wird.

UTE ROOS

Inhaltsverzeichnis

Security-Trends

Sicherheit in der Praxis

Red Teaming

Marktübersichten

Gesetze und Regulierungen

Sonstiges

Wir ändern die **Spielregeln.**

Kompromisslose IT-Sicherheit – dank künstlicher Intelligenz

Unsere brandneue **DeepRay®** -Technologie schützt mit künstlicher Intelligenz und Machine Learning vor den ausgefeilten Taktiken von Hackern. Cyberkriminelle tarnen ihre Schadsoftware mit verschiedenen Verschleierungstechniken.

Doch damit ist jetzt Schluss:
Dank **DeepRay®** erkennen unsere Sicherheitslösungen getarnte Malware sofort.

Informieren Sie sich jetzt

gdata.de/dr

G DATA
TRUST IN GERMAN SICHERHEIT

Es gibt 10 Arten von Menschen.

iX-Leser und die anderen.

Jetzt Mini-Abo testen:
3 Hefte + Leiterplatten-Untersetzer
nur 14,70 €

www.iX.de/test

www.iX.de/test 49 (0)541 800 09 120 leserservice@heise.de

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Security-Trends: Der Wunsch nach Kontrollierbarkeit

Beim Schlagwort KI (Künstliche Intelligenz) verdreht so mancher genervt die Augen, denn in der IT-Welt wird dieses Konzept derzeit überstrapaziert. Fakt ist aber, dass gerade dort, wo Massenangriffe automatisiert auf Systeme losgelassen werden, die effektivste Verteidigung auch im intelligenten Erkennen und Herausfiltern besteht. Doch nicht nur mit neuen Ansätzen versucht man, die IT-Risiken beherrschbar zu machen: Derzeit wird beispielsweise die gute alte Verschlüsselung aufgemöbelt, um sie für eine (nahe?) Zukunft mit Quantencomputern fitzumachen.

Neue Verfahren in der Schadcode-Erkennung

Schlau wie nie

Stefan Strobel

Sind KI, Machine Learning und Co. neue Wunderwaffen im Kampf gegen Hacker oder handelt es sich dabei nur um ein vollmundiges Marketingversprechen? *iX* hat genauer hingeschaut.

Zahlreiche Hersteller von Produkten der IT-Sicherheit werben derzeit mit Buzzwords wie künstliche Intelligenz, maschinelles Lernen, Big Data oder Data Science. Sowohl beim Erkennen von Schadcode als auch von Einbrüchen im internen Netzwerk sind die etablierten Verfahren in den letzten Jahren an ihre Grenzen gekommen. Fast jeder Hersteller bemüht sich, darauf hinzuweisen, dass seine Lösungen nicht nur auf Signaturen basieren, sondern auch auf dem Erkennen von bösartigem Verhalten und inzwischen noch auf Verfahren der künstlichen Intelligenz und des maschinellen Lernens.

In vielen Fällen ist jedoch Skepsis angebracht. Begriffe wie „KI“ und oder „Machine Learning“ haben von sich aus schon eine breite Bedeutung und erlauben stark unterschiedliche Interpretationen, die kaum etwas miteinander zu tun haben. Zudem neigen die Vertriebs- und Marketingstrategen der Hersteller von Sicherheitsprodukten immer wieder dazu, alle verfügbaren Hype-Begriffe auch auf das eigene Produkt anzuwenden. So findet man Produkte auf dem Markt, die tatsächlich neuronale Netzwerke oder Deep Learning zur Erkennung von Malware verwenden, aber auch solche, die das Feststellen einer Abweichung von einem „gelernten“ statistischen Durchschnittswert als Machine Learning verkaufen. Der Kunde muss daher selbst tiefer einsteigen und die vom Hersteller verwendeten Verfahren sowie deren Sinnhaftigkeit hinterfragen.

Der IT-Sicherheitsmarkt bietet mehrere prominente Beispiele. Viel Aufsehen erregen Hersteller, die ihre Produkte als Antivirus (AV) der nächsten Generation gegen die etablierten Virenschutzlösungen positionieren. Sie versprechen meist bessere Erkennungsraten von Malware, insbesondere von Ransomware. Zahlreiche Anwender und Unternehmen sind trotz vorhandenem klassischem Virenschutz in den letzten Monaten Opfer solcher Angriffe geworden. Dabei wurden wichtige Daten verschlüsselt und ein Lösegeld für die Entschlüsselung gefordert.

Erkennen anhand eines mathematischen Modells

Das Produkt von Cylance beispielsweise klinkt sich genauso wie klassische AV-Produkte in die Windows-Schnittstelle für Virenschutz ein, erkennt Malware jedoch nicht an Signaturen, sondern mit einem mathematischen Modell beziehungsweise einem neuronalen Netzwerk, das im Labor des Herstellers mit Millionen von Malware-Objekten und ebenso vielen gutartigen Dateien trainiert wurde. Das Lernen findet damit nur beim Hersteller statt. Ein offensichtlicher Vorteil dieser Technik ist, dass neuer Schadcode in den meisten Fällen sofort erkannt wird und man nicht erst ein Signatur-Update des Herstellers benötigt. Der Kunde bekommt nur im Abstand von mehreren Monaten ein Update des mathematischen Modells.

Einige Hersteller klassischer Virenschutzprodukte setzen ebenfalls auf KI-Methoden, allerdings meist nicht innerhalb des Agenten, der auf dem PC des Kunden läuft, sondern in ihren Laboren zum schnelleren Erzeugen von Signaturen. Die Anwendung der künstlichen In-

telligenz ist damit ein komplett anderes Szenario und der Endanwender ist nach wie vor auf laufend aktualisierte Signaturdateien angewiesen. Für die klassischen AV-Hersteller sind die KI-Methoden ein Versuch, die riesige Datenmenge zu bewältigen, denn auch die Heerscharen an Malware-Analysten bei solchen Firmen reichen schon heute nicht mehr aus, alle eingehenden Objekte manuell zu untersuchen und daraus Signaturen zu erstellen.

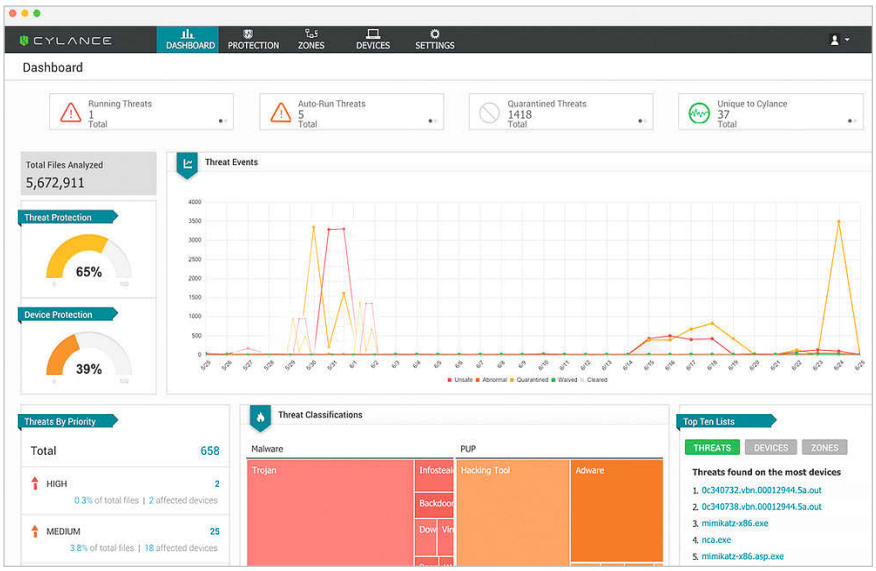
Es wäre jedoch falsch zu behaupten, dass die etablierten AV-Hersteller nach wie vor nur auf Signaturen setzen. Viele integrieren zusätzliche Erkennungs- und Schutzmechanismen, die beispielsweise auf Verhaltenserkennung, Host-Intrusion-Prevention-Methoden oder Exploit-Mitigation-Techniken basieren. Oft sind diese Zusatzfeatures jedoch in der Praxis deaktiviert oder müssen sogar mit einer Zusatzlizenz erworben werden.

Verschiedene Einsatzszenarien von KI

KI und maschinelles Lernen sind nicht auf Malware-Schutz begrenzt. Gerade das Erkennen von Einbrüchen wird derzeit viel mit solchen Schlagworten beworben. Die Technik, die dabei zum Einsatz kommt, ist jedoch wieder eine andere. Auf der Suche nach Malware teilt man Dateien in zwei Klassen auf: harmlose und (potenziell) schädliche. Beim Aufspüren von Sicherheitsvorfällen oder Einbrüchen soll das Verhalten eines Anwenders oder die Aktivität eines Endgeräts im Netzwerk als auffällig erkannt werden. Hier gibt es kein einfaches „Gut“ und „Böse“, denn ein bestimmtes Verhalten kann für einen Administrator üblich, für einen normalen Anwender aber verdächtig sein. Hier kommt deshalb maschinelles Lernen nicht im Labor von Produktherstellern zum Einsatz, sondern im Netzwerk des Kunden. Damit soll „normales“ Verhalten gelernt werden, sodass später signifikante Abweichungen davon als sicherheitsrelevante Anomalien erkannt werden können.

Bekannte Anbieter von Produkten für sogenannte User Behavior Analytics sind beispielsweise die Hersteller Exabeam oder Securonix. Beide analysieren vor allem Log-Daten, die das Verhalten der Anwender dokumentieren.

Dieser Ansatz birgt neben den offensichtlichen juristischen Problemen in einem deutschen Unternehmen auch zahlreiche technische Herausforderungen. Die Aufgaben und das normale Verhalten von Anwendern im Unternehmen unterschei-



Hinter den Malware-Funden steckt keine klassische Signaturerkennung, sondern ein mathematisches Modell.

den sich von Gruppe zu Gruppe. Die Gruppenzugehörigkeiten selbst sollte das Produkt ebenfalls lernen können und auch diese ändern sich mit der Zeit oder sind von vornherein saisonabhängig. Zudem muss verhindert werden, dass bösartiges Verhalten als gutartiges Verhalten gelernt wird. Für maschinelles Lernen ist es wichtig, sowohl Ausgangsdaten für normales Verhalten zu besitzen als auch solche für Angriffe. Die verfügbaren Daten sind jedoch asymmetrisch, denn es fehlt die gewünschte Menge an aktuellen Angriffsdaten.

Unterstützung in speziellen Anwendungsfällen

Trotz aller Hürden sind solche Produkte eine spürbare Arbeitserleichterung und Qualitätsverbesserung für Firmen, die entsprechende Log-Daten schon in einem SIEM-System (Security Information and Event Management) sammeln und auswerten. Der Anwendungsrahmen ist auch in der Praxis relativ klar umrissen. Es geht um typische Betrugsfälle, Extraktion von Daten, Missbrauch von Zugangsrechten und Ähnliches. Für diese bekannten Anwendungsfälle ist der Lernbedarf im Netzwerk des Kunden eher gering und die gesuchten Verhaltensmuster sind zu einem nicht unerheblichen Teil bereits bekannt und in den Produkten implementiert.

Andere Anbieter konzentrieren sich auf die Analyse der Kommunikation im internen Netzwerk. Als Beispiel sei hier der Hersteller LightCyber genannt, der von Palo Alto Networks übernommen wurde. Auch hier lernt das System das „normale“ Kommunikationsverhalten je Endgerät beziehungsweise Anwender, allerdings alarmiert das Produkt bei einer Anomalie nicht sofort, sondern automatisiert zunächst die Verifikation auf dem Endgerät. Dazu kann es sich mit Domänen-Credentials auf dem auffälligen Endgerät einloggen und dort die laufenden Prozesse, geöffnete Dateien et cetera in die Bewertung einbeziehen.

Ein generelles Problem haben alle Erkennungstechniken gemeinsam: In der IT-Sicherheit hat man es mit Gegnern zu tun, die nicht erkannt werden wollen. Bei der Erkennung von Sprache oder Schrift, bei der Diagnose von Krankheiten, bei der Entdeckung von Produktionsfehlern oder anderen industriellen Anwendungen kann man mit modernen Techniken beeindruckende Ergebnisse erzielen, aber die zu findenden Objekte wehren sich in den meisten Fällen nicht gegen die Erkennung.

Sicherheit duldet keine Fehlertoleranz

Die Paradedisziplin moderner Lernverfahren mit riesigen Datenmengen ist vermutlich die gezielte Werbung. Empfehlungen für Produkte, die den Kunden auch interessieren könnten, treffen zwar oft zu, aber für IT-Sicherheitsanwendungen ist „oft“ nicht oft genug. Fehlalarme beziehungsweise False Positives sind ebenso unerwünscht und mit hohen Betriebskosten verbunden wie False Negatives, also fehlende Alarme beziehungsweise übersehene Angriffe. Der Qualitätsanspruch ist deutlich höher als bei Werbung, die auch einmal unpassende Produkte anzeigen darf. Aber selbst bei der Werbung ist die vermeintliche Intelligenz der Technik bei Weitem nicht immun gegen gezielte Manipulationen.

Schon kurz nach der kommerziellen Verfügbarkeit der ersten IDS-Produkte gab es Vorträge auf Hacker-Konferenzen, in denen gezeigt wurde, wie man ein IDS überlisten kann und nicht entdeckt wird. Das Gleiche ist mit Sandbox-Analyse-Produkten passiert. Auch hier findet ein professioneller Angreifer Wege, seine Malware so zu schreiben, dass einschlägige Produkte sie nicht als bösartig erkennen. Angreifer, die über genügend Budget verfügen, können sich die Sicherheitsprodukte selbst kaufen und testen, ob und unter welchen Umständen ihre Malware gefunden wird und wie sie dies verhindern können. Auch künstliche Intelligenz ändert daran nichts. Das bedeutet jedoch nicht, dass KI und maschinelles Lernen keinen Fortschritt für die IT-Sicherheit bringen würden. Gegenüber den klassischen Erkennungsverfahren sind die modernen Techniken überlegen. Die Erkennungsraten sind oft besser und der Betriebsaufwand sinkt. Für Firmen, die IT-Sicherheit ernst nehmen, ist der Einsatz moderner Techniken mit Methoden der künstlichen Intelligenz daher eine Qualitätsverbesserung und eine Reduktion der Betriebskosten gegenüber klassischem Virenschutz und klassischer Angriffserkennung.

Perfekte Sicherheit wird es zwar auch hier nicht geben und gezielte professionelle Angriffe wird man so auch nicht erkennen können. Diese Lücke lässt sich aber nicht mit menschlicher Intelligenz und dem Outsourcing der Suche an ein externes SOC (Security Operation Center) schließen. Auch hier müssen massiv automatisierte Erkennungsmethoden zum Einsatz kommen, damit man die Services überhaupt betriebswirtschaftlich sinnvoll anbieten kann. Es gibt überdies nicht genügend IT-Security-Experten am Arbeitsmarkt, um sie in einem SOC rund um die Uhr Events analysieren zu lassen. Techniken aus dem Bereich der künstlichen Intelligenz sind deshalb auch hier nötig, um Auffälligkeiten erkennen und sinnvoll darstellen zu können. Selbst wenn die Methoden aus dem Bereich der Big-Data-basierten Werbung nicht perfekt auf IT-Security übertragbar sind, einen spürbaren Fortschritt bringen sie dennoch. (ur)

Stefan Strobel
ist Buchautor sowie Gründer und Geschäftsführer des IT-Sicherheitshauses cirosec in Heilbronn.

Mit einer Lösung dreimal compliant

Unternehmen sind umzingelt von Gesetzen, Vorgaben und Standards, die unter anderem den Umgang mit sensiblen Daten regulieren. Häufig müssen drei oder mehr Regelungen umgesetzt werden: Zur DSGVO, die für alle Unternehmen in der EU verpflichtend ist, kommen das Geschäftsgeheimnisschutzgesetz (GeschGehG) für Firmeninformationen mit wirtschaftlicher Bedeutung. Im Kontakt mit Partnern ab einer gewissen Größe und in bestimmten Branchen sowie im internationalen Kontext ist eine Zertifizierung nach ISO 27001 erforderlich.

Laut DSGVO muss die Vertraulichkeit personenbezogener Daten, beispielsweise die der eigenen Mitarbeiter, bei der Verarbeitung durch „geeignete technische und organisatorische Maßnahmen“ gewährleistet werden. Das GeschGehG stellt Bedingungen, damit Firmen den Diebstahl und die Verwendung von geschäftskritischen Informationen untersagen und verfolgen können: So müssen Geschäftsgeheimnisse „durch technische und organisatorische Maßnahmen geschützt werden, die geeignet sind, interne und externe Verletzungen der Geheimhaltung zu verhindern“. In ISO 27001 sind in den sogenannten „Controls“ im Anhang A der Norm Sicherheitsanforderungen und Ziele zum Schutz von sensiblen Daten vorgegeben. Sie stehen beispielsweise im Zusammenhang mit der Verwaltung der Werte (A.8), der Informationsübertragung (A.13.2) sowie der Compliance mit gesetzlichen, vertraglichen oder selbstauferlegten Anforderungen (A.18).

Keine Angaben zu „geeigneten technischen Maßnahmen“

Konkretisiert werden die technischen Maßnahmen, mit denen die Anforderungen umzusetzen wären, in keiner der drei Regelungen; allenfalls verweisen Kommentare zu den ISO 27001-Controls auf den Einsatz einer DLP-Lösung. In jedem Fall müssen passende Lösungen den Schutz der Vertraulichkeit für unterschiedliche Arten von sensiblen Daten gewährleisten und sich möglichst ressourcenschonend für die Herstellung von Compliance mit unterschiedlichen Regelungen eignen.

DLP-Lösungen bieten ein geeignetes Funktionsspektrum

Dies ermöglichen Lösungen für Data Loss Prevention wie Endpoint Protector an entscheidenden Punkten. Zunächst einmal stellen sie sicher, dass Transfers unterbunden werden, die die Vertraulichkeit von Daten potenziell gefährden können und dass Firmenrichtlinien technisch überwacht werden. Die zentralen Funktionsbereiche von DLP-Lösungen sind:

- Device Control-Funktionalität verhindert, dass Mitarbeiter USB-Sticks, Notebooks und andere mobile Geräte am Arbeitsplatzrechner anschießen und Daten darauf speichern.
- Sind Daten als sensibel in die Inhaltskontrolle definiert, können sie nicht per E-Mail versandt, in Cloud-Speicher oder Filesharing-Tools geladen oder mit Social-Media-Anwendungen verwendet werden. Auch das Ausdrucken der Daten und Screenshots der Bildschirmansicht werden blockiert.
- eDiscovery-Funktionen finden Daten, die auf Arbeitsplatzrechnern gespeichert sind und deren Inhalte als sensibel eingestuft wurden.

Die besondere Bedeutung von Logs und Reports

Gute DLP-Lösungen erfassen alle Ereignisse und erstellen Aufzeichnungen. Dazu gehören die revisionssichere Protokollierung aller Übertragungen sowie Übertragungsversuche von Dateien auf Wechseldatenträger und mobile Devices, in und über Online-Anwendungen und Cloud-Dienste sowie Mitschnitte sämtlicher übertragenen Dateien. Auswertungen der Logfiles machen Verstöße gegen Richtlinien und entsprechende Versuche sowie Datenlecks oder potentielle Datenlecks sichtbar, die beispielsweise durch verändertes Mitarbeiterverhalten oder die Verwendung neuer Tools und Anwendungen entstehen können. Zudem ermöglichen sie kontinuierliche Anpassungen und Verbesserungen von Richtlinien und Schutzmaßnahmen, mit denen sich die Eintrittswahrscheinlichkeit oder die Auswirkungen von Vorfällen verringern lassen.

Nachweispflichten werden erfüllt

Weiterhin sind die Reports Grundlage für die Erfüllung von Nachweispflichten: bei Audits, gegenüber der Datenschutzbehörde und für gerichtliches Vorgehen. Mit ihnen lassen sich für ISO 27001 Teilbereiche des für ein ISMS enorm wichtigen Ziels der Protokollierung und Erbringung von Nachweisen (A.12.4) abdecken. Im Rahmen der DSGVO sind die Firmen durch die Aufzeichnungen hinsichtlich der Umsetzung von Schutzmaßnahmen gegenüber den Datenschutzbehörden nachweisfähig. Im Fall eines Datenverlustes können sie mit Hilfe der Logs Verursacher und Umfang des Schadens sowie Austrittspunkte ermitteln und sind in der Lage, eine forensische Untersuchung zu betreiben. Beim Abfluss von Geschäftsgeheimnissen können sie Maßnahmen zum Schutz der Informationen sowie Verletzungen gerichtsfest nachweisen und Ansprüche gegen Verursacher von Verletzungen durchsetzen.

Fazit

DLP-Lösungen wie Endpoint Protector sind ausgereifte Systeme mit umfassender Funktionalität zum Schutz vor nicht erwünschtem Datenabfluss. Unternehmen können mit dem Einsatz einer einzigen Lösung personenbezogene Daten und digitale immaterielle Werte gleichermaßen schützen und im Rahmen von DSGVO, GeschGehG, ISO 27001 und weiteren internationalen Standards ihren Nachweispflichten nachkommen. So entsteht mehrfacher Nutzen bei gleichen Kosten.

ENDPOINT PROTECTOR

Endpoint Protector GmbH
Gebhardstrasse 7 · 88046 Friedrichshafen
Deutschland
Tel.: +49 7541 978267 30 · Fax: +49 7541 9782627 9
E-Mail: info@endpointprotector.de
Internet: www.endpointprotector.de

IT-Grundschutz in LXC-Container verpackt

Streng separiert

Inés Atug, Daniel Jedecke

LXC, Kubernetes und Docker sind beliebte Container-Formate. Im produktiven Einsatz vernachlässigen jedoch viele das Thema Compliance, das einen später oft wieder einholt. Der Artikel zeigt anhand des IT-Grundschutz-Kompendiums, wie sich die Compliance in einer LXC-Umgebung technisch umsetzen lässt.

Der BSI IT-Grundschutz bietet eine Methodik, mit der sich Informationen einer Institution oder eines Unternehmens angemessen schützen lassen (er ist über ix.de/ix1914012 zu finden). Er besteht aus den BSI-Standards 200-1 bis 200-3 sowie dem IT-Grundschutz-Kompendium (siehe Seite 146). Die Vorgehensweise, die in den BSI-Standards festgelegt ist, dient zur Definition eines Informationssicherheitsmanagementsystems (ISMS) und ist kompatibel zum ISO-27001-Standard.

Die BSI-Standards fungieren als Leitfaden zur Umsetzung des ISMS und sollen sowohl für IT-Verantwortliche als auch für Administratoren Informationen und Hilfestellungen liefern. Das IT-Grundschutz-Kompendium ist thematisch in Bausteine unterteilt, in denen Anforderungen zu unterschiedlichen Themen definiert sind. Speziell für Container steht der Baustein „SYS.1.6 Container“ zur Verfügung, derzeit noch als Community Draft (siehe Tabelle: Maßnahmen des Bausteins „Container“). Da bei diesem Baustein noch die Veröffentlichung aussteht, ist nach Methodik des IT-Grundschutzes darauf zu achten, dass noch eine Risikoanalyse durchgeführt wird.

Für einen umfassenden Schutz ist es wichtig, die Systematik der Bausteine des IT-Grundschutz-Kompendiums zu verstehen. Hierzu muss zunächst die Virtualisierungsumgebung als Ganzes modelliert werden (Modellierung nach IT-Grundschutz). Daraus ergeben sich weitere anwendbare Bausteine. Ein typisches Beispiel ist der Baustein „SYS.1.1 Allgemeiner Server“. Er ist immer anzuwenden, wenn ein IT-System als Server betrieben wird. Er enthält generische Bedrohungen und Maßnahmen zum Thema Server, während der Baustein „Container“ die Anforderungen zur Absicherung von Containern enthält.

Der Baustein enthält 27 Anforderungen. Dabei sind vorrangig die Basis-Anforderungen umzusetzen (siehe Tabelle „Priorisierung der Maßnahmen“). Die Standard-Anforderungen sollten grundsätzlich realisiert werden, da sie gemeinsam mit den Basis-Anforderungen den Grundschutz darstellen. Die Anforderungen bei erhöhtem Schutzbedarf sind dann umzusetzen, wenn sie nach einer Risikoanalyse als Maßnahmen definiert wurden.

IT-Verbund „LXC“

Dieser Artikel beschreibt, wie man die technischen Anforderungen des IT-Grundschutzes in einer LXC-Umgebung umsetzen kann. Berücksichtigt werden hier nur

iX-TRACT

- Will man als Institution oder Unternehmen seine vertraulichen Informationen schützen, ist das Separieren von Daten und Anwendungen in abgeschotteten sogenannten Containern eine gute Wahl.
- Wie man solche Container in virtuellen Infrastrukturen sicher betreibt, beschreiben verschiedene Bausteine des BSI IT-Grundschutzes und die dazugehörigen Maßnahmen der praktischen Umsetzung.
- Statt des verbreiteten Docker oder kommerzieller Virtualisierungsumgebungen können erfahrene Linux-Administratoren LXC (Linux Containers) einsetzen, das gegenüber den genannten Verfahren einige Vorteile mit sich bringt.

die Vorgehensweisen „Basis-Absicherung“ und „Standard-Absicherung“. Eine Erweiterung von LXC ist LXD, das ein Management der Container über eine REST-API ermöglicht und vereinfacht. Für das Grundlagenwissen zu LXC (Linux Containers) und LXD sei auf mehrere zu diesem Thema erschienene Artikel verwiesen. In diesem Artikel liegt der Fokus darauf, die Container konform zum IT-Grundschutz zu betreiben.

Am Anfang jeder IT-Grundschutz-Umsetzung steht die Modellierung eines IT-Verbundes. Im vorliegenden Beispiel ist die Modellierung vereinfacht und eine kleine Umgebung definiert. Die Vorgehensweise lässt sich aber ohne Weiteres auf viele Hundert Anwendungen skalieren und abbilden. Die Umgebung besteht der Einfachheit halber daher nur aus dem LXC-Server und zwei Containern.

Bei den Containern handelt es sich um einen Webserver sowie einen Test-Webserver. Als Betriebssystem wird Ubuntu 18.04 eingesetzt und Apache als Webserver (siehe Abbildung). Nach der IT-Grundschutz-Modellierung sind die folgenden Bausteine auf den vereinfachten IT-Verbund „LXC“ anzuwenden: Allgemeiner Server (SYS.1.1), Server mit Unix (SYS.1.3), Container (SYS 1.6), Anwendung Webserver (APP 3.2) und Webanwendungen (APP 3.1).

Die Aufzählung ist nicht komplett, da für eine vollständige Umsetzung des BSI IT-Grundschutzes weitere Bausteine erforderlich sind. So fehlen zum Beispiel in dieser Modellierung die Bausteine zu Räumen, Netzen und Personal. Stattdessen stellt der Artikel die technischen Anforderungen aus dem Baustein „Container“ detaillierter dar.

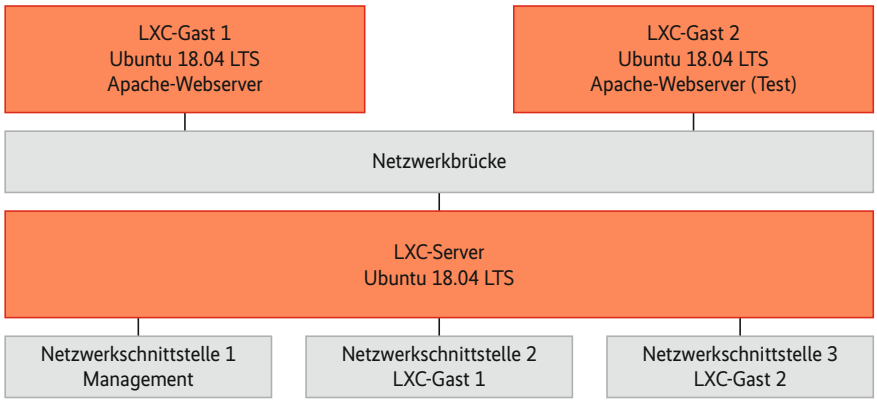
Gut geeignet für den konformen Einsatz im Rahmen des IT-Grundschutzes ist Ubuntu 18.04. Es bietet langen Support in der gleichnamigen Variante (LTS, Long Term Support) und der Hersteller Canonical unterstützt LXC, sodass für Ubuntu stets aktuelle Versionen bereitstehen. LXC und LXD sind in der Servervariante von Ubuntu 18.04 bereits vorinstalliert.

Die Sicherheit beginnt mit der Konzeptionierungsphase und so sollte vor dem Einsatz von Containern alles geplant und dokumentiert werden (SYS.1.6.A1). Ein besonderes Augenmerk sollte man dabei auf die Separierung der in den Containern betriebenen Anwendungen legen (SYS.1.6.A2). Auch die Anforderungen an das Deployment, die Protokollierung und das Schwachstellenmanagement sind bei der Planung zu beachten. Zudem sollte sowohl die Verwaltungssoftware als auch deren Identitäts- und Berechtigungsmanagement festgelegt werden (SYS.1.6.A19).

Quelle: BSI

Priorisierung der Maßnahmen

Kennzeichnung	Bedeutung
Basis-Absicherung	Bei der Basis-Absicherung handelt es sich um eine grundlegende Absicherung der Geschäftsprozesse und Ressourcen einer Institution. Sie ermöglicht einen ersten Einstieg in den Sicherheitsprozess, um schnellstmöglich die größten Risiken zu senken. Im nächsten Schritt können die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Diese Vorgehensweise ist daher besonders für kleinere Institutionen geeignet, die noch am Anfang ihres Sicherheitsprozesses stehen.
Standard-Absicherung	Diese entspricht in den Grundzügen der bekannten und bewährten IT-Grundschutz-Vorgehensweise.
Kern-Absicherung	Die Kern-Absicherung dient als weitere Einstiegsvorgehensweise zum Schutz der essenziellen Geschäftsprozesse und Ressourcen einer Institution. Sie unterscheidet sich vom klassischen IT-Grundschutz durch die Fokussierung auf einen kleinen, aber sehr wichtigen Teil eines Informationsverbunds, die sogenannten „Kronjuwelen“. Die Kern-Absicherung ist vor allem für Institutionen geeignet, die einige wenige Geschäftsprozesse identifiziert haben, die wesentlich für den Fortbestand der Institution sind und vorrangig abgesichert werden müssen.



So könnte ein LXC-Verbund aussehen, mit dem sich Daten in einer virtualisierten Umgebung grundschutzkonform schützen lassen.

Verteiltes Administrieren von Servern

Die erste technische Maßnahme des Bausteins „Container“ besteht darin, das Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur (SYS.1.6.A15) anzusprechen. Für das Rechtemanagement kann man das von Linux angebotene Konzept einsetzen. Benutzer lassen sich entweder lokal oder per Anbindung an einen Verzeichnisdienst wie Active Directory oder LDAP verwalten. Ebenso wichtig bei der Planung ist eine Definition der späteren Systembenutzer. Da LXC-Container nicht als privilegierte Benutzer ausgeführt werden sollten, sind entsprechende nicht privilegierte Benutzer anzulegen. Im Baustein finden sich diese Anforderungen unter der Maßnahme SYS.1.6.A15 „Identitätsmanagement der Administratoren“ sowie SYS.1.6.A16 „Accounts der Anwendungsdienste“.

Durch den Zugriff auf den LXC-Server können sich weitere Angriffsszenarien ergeben. Daher sollte auch zwischen Administratoren der eigenen Institution und Dritten unterschieden werden. Lässt man Dritte auf einen Container zugreifen, sollte man ihnen keinesfalls Zugriff auf den LXC-Server gewähren.

Administratoren der Container sollten auf dem LXC-Server maximal mit den Rechten eines normalen Benutzers arbeiten dürfen. LXC erlaubt beispielsweise das Ausführen eines Containers als normaler Systembenutzer. In sehr kleinen Institutionen entfällt diese Trennung vermutlich, da hier meist nur ein bis zwei Administratoren das System betreiben und warten.

„Container-Ausführung ohne privilegierten Account“ heißt die nächste für den Baustein relevante Maßnahme (SYS.1.6.A17). LXC nutzt die Namespaces und Cgroups des aktuellen Linux-Kernels, um die verschiedenen Container untereinander und vom LXC-Server zu trennen. In älteren Versionen werden die Container im Normalfall in Linux unter der UID 0 und GID 0 ausgeführt, also di-

rekt als Benutzer *root*. Diese Container nennt man auch privilegierte Container. Der Schutz zwischen dem Gast und dem LXC-Server basiert auf Funktionen wie AppArmor, SELinux, seccomp-Filter, Cgroups und Namespaces (siehe ix.de/ix1914012).

Ein Fehler in einer dieser Funktionen kann das Ausbrechen aus dem Gastkontext begünstigen. Daher sollte man beim Einsatz von LXC mit unprivilegierten Containern arbeiten und für jedes Gastsystem einen eigenen Benutzer (lxcuser1 und so weiter) anlegen. So lässt sich die vom IT-Grundschutz geforderte Isolierung und Kapselung virtueller IT-Systeme gut umsetzen.

Unprivilegierte Container laufen unter einer anderen UID und GID, was bei einem Ausbruch aus dem Gastkontext nur begrenzt kritische Risiken mit sich bringt. Sofern noch nicht geschehen, muss für den LXC-Benutzer eine SubUID und SubGID definiert werden:

```
usermod --add-subuids 100000-165536 $lxcuser1
usermod --add-subgids 100000-165536 lxcuser1
```

Anschließend ist die LXC-Konfiguration so anzupassen, dass sie eine Ausführung unter den neuen UIDs und GIDs erlaubt. Dazu muss die Datei *~/.config/lxc/default.conf* die folgenden Zeilen enthalten:

```
lxc.network.type = veth
lxc.network.link = lxcbr0
lxc.network.flags = up
lxc.network.hwaddr = 00:16:6e:2a:ff:e1
lxc.id_map = u 0 100000 65536
lxc.id_map = g 0 100000 65536
```

Normalerweise legt Linux beim Einsatz von LXC eine gemeinsame Netzwerk-Bridge an, was allerdings zu weiteren Problemen führen kann. Daher sollte der Systemverantwortliche für die Gruppe von Gastsystemen eine eigene Netzwerk-Bridge anlegen. Wichtig ist dabei, in der Datei */etc/lxc/lxc-usernet* die Benutzer auf diese Netzwerk-Bridge zu limitieren:

```
lxcuser1 veth lxcbr0 10
```

In modernen Versionen von LXC (in Kombination mit LXD) werden die Container automatisch als unprivilegiert angelegt. Hier entfällt die manuelle Konfiguration.

Das im Grundschutz geforderte Monitoring der Umgebung lässt sich durch den Einsatz eines normalen Ubuntu-Servers mit den üblichen Monitoring-Systemen bewerkstelligen. Hier kann man etwa Nagios und NSCA (Nagios Service Check Acceptor) nutzen. Bei der Protokollierung ist darauf zu achten, dass diese außerhalb der Container (und möglichst auch des LXC-Servers) gespeichert werden (SYS.1.6.A5).

Schwieriger wird das Verwalten von Geräten und Ressourcen. Je nachdem, welche Ressourcen erforderlich sind, konfiguriert man diese zentral oder in den jeweiligen Benutzerverzeichnissen. Unter Ubuntu 18.04 lässt sich der Speicher beispielsweise einfach durch den Befehl *lxc config set lxc-gast1 limits.memory 64MB* anpassen.

Sichere Konfiguration ist unerlässlich

Leider lassen sich auf diese Art nicht alle Ressourcen verwalten. So kann es nötig sein, zusätzlich die Berechtigungen für Ressourcen unter dem Verzeichnis */dev* anzupassen. Beides kann nur der Administrator des LXC-Servers durchführen. Wie man ein Netz für virtuelle Infrastrukturen sicher konfiguriert, beschreibt die gleichnamige technische Anforderung im Baustein Container SYS.1.6.A9 „Separierung der Netze“. Da LXC auf einem gängigen Linux-System betrieben wird, kann man die üblichen Werkzeuge zur Administration nutzen. Diese bestehen im Enterprise-Umfeld oft aus Anwendungen zum zentralisierten Verwalten wie Puppet oder Ansible (siehe ix.de/ix1914012). Mithilfe dieser Tools wurde auf dem Testsystem auch die Härtung des Host-Systems sowie der Container durchgeführt (SYS.1.6.A3 „Härtung des Host-Systems“ und SYS.1.6.A4 „Härtung der Software im Container“).

Daher lässt sich auch ohne Weiteres die Fernadministration des LXC-Servers vom Administrieren der Container trennen. Das könnte man einerseits durch eine eigene Netzwerkkarte erreichen, die nur den Containern oder dem LXC-Server zur Verfügung steht, oder andererseits über eine Access Control List auf den SSH-Zugang zum LXC-Server. Die Administration von LXC erfolgt per Konsole auf dem LXC-Server. Somit greifen die üblichen Schutzmaßnahmen für den Zugriff auf den Server, zum Beispiel die Absicherung des SSH-Zugangs.

Hierdurch können die Anforderungen der Maßnahme SYS.1.6.A11 „Administrativer Fernzugriff auf Container“ sowie SYS.1.6.A14 „Verschlüsselung der Netzkommunikation“ erfüllt werden. Auch lassen sich weitere Überwachungsaufgaben wie auf normal betriebenen Linux-Servern umsetzen. So kann der Administrator

Maßnahmen des Bausteins „Container“

Quelle: BSI

Nummer	Name
Basis-Absicherung	
SYS.1.6.A1	Planung des Container-Einsatzes
SYS.1.6.A2	Planung der Separierung
SYS.1.6.A3	Härtung des Host-Systems
SYS.1.6.A4	Härtung der Software im Container
SYS.1.6.A5	Persistenz von Protokollierungsdaten
SYS.1.6.A6	Persistenz von Nutzdaten
SYS.1.6.A7	Verwendung sicherer Images
SYS.1.6.A8	Speicherung von Zugangsdaten
SYS.1.6.A9	Separierung der Netze
SYS.1.6.A10	Einbinden von Volumes
SYS.1.6.A11	Administrativer Fernzugriff auf Container
Standard-Absicherung	
SYS.1.6.A12	Freigabe von Images
SYS.1.6.A13	Updates von Containern
SYS.1.6.A14	Verschlüsselung der Netzkommunikation
SYS.1.6.A15	Identitätsmanagement der Administratoren
SYS.1.6.A16	Accounts der Anwendungsdienste
SYS.1.6.A17	Container-Ausführung ohne privilegierten Account
SYS.1.6.A18	Nur ein Dienst pro Container
SYS.1.6.A19	Planung der Verwaltung und Orchestrierung
Kern-Absicherung	
SYS.1.6.A20	Limitierung der Ressourcen pro Container (A)
SYS.1.6.A21	Automatisierte Auditierung (CIA)
SYS.1.6.A22	Eigene Trusted Registry (CIA)
SYS.1.6.A23	Reduzierte Rechte (CIA)
SYS.1.6.A24	Erstellung erweiterter Richtlinien für Container (CIA)
SYS.1.6.A25	Host Based Intrusion Detection (CIA)
SYS.1.6.A26	Hochverfügbarkeit (A)
SYS.1.6.A27	Verschlüsselte Datenhaltung (C)

C = Confidentiality/Vertraulichkeit; I = Integrity/Integrität; A = Avalability/Verfügbarkeit

etwa das System mit Nagios überwachen und Änderungen per Puppet oder Ansible dokumentieren und umsetzen. Bei den Anforderungen an die Verschlüsselung der Netzkommunikation ist darauf zu achten, das diese Anforderung sowohl den Container selbst betrifft als auch dort betriebene Services. Daher ist das frühzeitige Einbeziehen der Anwendungsentwickler wichtig. Innerhalb der LXC-Struktur dienen Netzwerk-Bridges dem Verteilen des Verkehrs. Sie lassen sich mit *iptables* absichern. Außerdem kann man damit das Routing anpassen beziehungsweise unsichere Protokolle sperren.

Im Beispiel-IT-Verbund „LXC“ gewährleisten drei Netzwerkkarten eine physische Trennung der Verbindung. Das lässt sich natürlich auch durch virtuelle Netzwerk-Bridges realisieren. Man muss dabei allerdings genau prüfen, dass keine ungewollten Bridges ermöglicht werden.

Falls die Container nicht lokal gespeichert werden sollen, ist darauf zu achten, dass der Zugriff auf beispielsweise das NAS nur vom LXC-Server aus möglich ist. Nach dem Einrichten der virtuellen Systeme gilt es, diese im Blick zu behalten und auf Unregelmäßigkeiten zu kontrollieren. Weiterhin müssen nach SYS.1.6.A6 „Persistenz von Nutzdaten“ die Daten der Anwendungen außerhalb der Container gespeichert werden. Hierzu kann mithilfe des Befehls *lxc config device add <Container> <Bezeichner> disk path=<Ziel> source=<Quelle>* ein externer Speicher zum Container hinzugefügt werden. Über das Unix-Rechtemanagement können hierbei auch die Anforderungen der Maßnahme SYS.1.6.A10 „Einbinden von Volumes“ erfüllt und nicht benötigte Rechte eingeschränkt werden.

Da die Konfiguration von LXC vollständig in Dateien abgebildet ist, lassen sich diese mithilfe von Checksummen oder entsprechenden Werkzeugen auf Veränderungen hin überprüfen. Dazu kann man etwa das Host-basierte Open-Source-Intrusion-Detection-System OSSEC nutzen. Es überwacht die Verzeichnisse */etc/lxc/* sowie */.config/lxc/* in den Benutzerverzeichnissen oder die LXD-Konfigurationsdatenbank. So hat man alle dateibasierten Konfigurationsänderungen im Blick. Modifikationen im Netzwerk dagegen sind schwieriger zu überwachen, da die laufende Konfiguration geändert werden kann. Als pragmatischer Ansatz hat sich etabliert, die *iptables*-Regeln einmal zu definieren und durch einen Cronjob regelmäßig prüfen zu lassen.

Sehr wichtig ist eine gute Dokumentation der Dateien */etc/lxc/lxc-usernet* (LXC) sowie der *iptables*-Regeln. Sie beeinflussen alle Netzzuordnungen, was maßgeblich zur Sicherheit der virtuellen Umgebung beiträgt.

Um die Anforderungen der Bausteine SYS.1.6.A7 „Verwendung sicherer Images“, SYS.1.6.A12 „Freigabe von Images“ sowie SYS.1.6.A13 „Updates von Containern“ zu erfüllen, sollte die Containerregistrierung verwendet werden. Hierdurch können sichere Basis-Container zur Verfügung gestellt werden sowie die genannten Management-Tools Puppet und Ansible, um die Einstellungen regelmäßig zu prüfen.

Fazit

LXC und LXD können ohne großen Aufwand IT-Grundschutz-konform betrieben werden. Ein großer Vorteil liegt in der Integration in alle modernen Kernel. Somit ist man nicht von einem Hersteller abhängig, sondern kann seine eingesetzte Linux-Distribution weiterverwenden. Der Einsatz von Ubuntu bringt den zusätzlichen Vorteil, dass dessen Entwickler an LXC und LXD aktiv weiterarbeiten und es überdies offizielle Pakete für alle aktuellen Long-Term-Support-Varianten von Ubuntu gibt. Dadurch ist der Support für mehrere Jahre sichergestellt und man hat Planungssicherheit.

Durch die einfache Einbindung in ein Linux-System lassen sich ohne Weiteres etablierte Überwachungs- und Administrationstools nutzen. Einziges Manko für den produktiven Einsatz ist aktuell noch die im Vergleich zu anderer Software spärliche Dokumentation. Als Basis für weitere Lösungen wie Docker und OpenStack lässt dich LXC und LXD jedoch sehr gut nutzen. (ur@ix.de)

Quellen

[1] Informationen und Hintergründe zu den im Text genannten Tools und Bausteinen sind unter ix.de/ix1914012 zu finden.

Daniel Jedecke und Inés Atug
sind Managing Consultants der HiSolutions AG mit Schwerpunkt Cloud-Sicherheit.

Selbstverteidigung zur Laufzeit

Gut abgewehrt

Maik Schäfer

Anwendungen können sich nun selbstständig vor Angriffen schützen – das zumindest versprechen Hersteller, die auf die „Runtime Application Self-Protection“ setzen.

Ein neuer Ansatz, die „Runtime Application Self-Protection“ (RASP), soll Anwendungen mit der Fähigkeit ausstatten, Angriffe auf Schwachstellen zur Laufzeit zu erkennen und zu verhindern, dass sie erfolgreich sind. Selbst Angriffe auf bisher unbekannte Schwachstellen (Zero-Day-Exploits) sollen entdeckt und abgewehrt werden.

Das klingt nun so, als könnte RASP wie von Zauberhand sämtliche Anwendungen von heute auf morgen unangreifbar machen und alle Sicherheitsprobleme aus der Welt schaffen. Aber geht das wirklich? Und wie soll das funktionieren? Bevor sich der Artikel diesen Fragen widmet, einige Worte zum Begriff an sich.

Analysten von Gartner definieren RASP als Sicherheitsmechanismus, der sich in eine Anwendung beziehungsweise deren Ausführungsumgebung einklinkt und dadurch die Anwendung von innen heraus vor Angriffen schützt (dieser und alle weiteren Links des Artikels sind unter ix.de/ix1914016 zu finden). Diese Definition klingt ziemlich abstrakt und weit gefasst, da sie viele technische Fragen aufwirft, etwa zu den unterstützten Verfahren oder den verwendeten Implementierungen. Andererseits bringt die Definition ziemlich gut auf den Punkt, was RASP von bisherigen Verfahren unterscheidet: die Integration der Schutzmechanismen in die zu schützende Anwendung und das Operieren der Mechanismen aus dem Inneren heraus.

Auf diese Art können viele Informationen aus dem Anwendungskontext dazu verwendet werden, Angriffe zu identifizieren. Außerdem lassen sich diese dann aus dem Inneren heraus zur Laufzeit blockieren. Zu den kontextuellen Informationen, die ausschließlich den RASP-basierten Schutzsystemen vorbehalten sind, zählen sowohl die intern verarbeiteten Daten und die verwendeten Codepfade der Anwendung als auch ihre Dateioperationen und Zugriffe auf externe Bibliotheken oder das Betriebssystem.

Unternehmen, die Sicherheitsprodukte unter dem Schlagwort RASP vermarkten, konzentrieren sich hauptsächlich auf in Java geschriebene Webanwendungen, die insbesondere im Unternehmensumfeld verbreitet sind. Daher beschränkt sich dieser Artikel ebenfalls auf Java-Anwendungen, um die verschiedenen RASP-Ansätze technisch vergleichen zu können. Dennoch gibt es einige Hersteller, die RASP bereits für andere Plattformen anbieten, etwa für PHP, Node.js, .NET oder Python. Nachfolgend werden drei verschiedene Ansätze für Java-Anwendungen vorgestellt (siehe Abbildungen). Beim ersten werden die RASP-Mechanismen direkt in den Quellcode der zu schützenden Anwendung einprogrammiert (Abbildung 1). Ein Hersteller aus dieser Sparte (Prevoty) stellt dafür ein Software Development Kit (SDK) zur Verfügung. Das SDK dient dazu, an kritischen Stellen im Programmcode, für die Überprüfungen gewünscht sind, Prevotys Funktionen zu integrieren. Das geschieht, indem man einen API-Aufruf für die Analysekomponente einfügt.

In den Code geschrieben

Erreicht die Programmausführung diese Stelle im Code, werden alle verfügbaren kontextuellen Anwendungsdaten gesammelt und an Prevotys Security Engine übertragen. Die Security Engine ist ein Webdienst, der auf drei Arten benutzbar ist: als vom Hersteller bereitgestellter Dienst, als Amazon-Cloud-Instanz oder als selbst betriebener Dienst im eigenen Netzwerk. Die Security Engine bildet das eigentliche Auswertungssystem, das anhand der Anwendungsdaten entscheidet, ob ein Angriff stattfindet oder nicht. Die Grundlage für die Entscheidung bilden zuvor vorgenommene Konfigurationen (im Prevoty-Manager) sowie einige proprietäre Mechanismen.

Der Schutz vor SQL-Injection-Angriffen sieht beispielsweise folgendermaßen aus: Nachdem die Anwendung über die API-Aufrufe die auszuführende SQL-Query an die Security Engine übertragen hat, parst diese sie und erzeugt daraus einen abstrakten Syntaxbaum, der die Struktur der Query repräsentiert. Die Security Engine überprüft nun, ob diese Struktur derjenigen entspricht, die zuvor