Ein IT-Sicherheitskonzept für das vernetzte Entwicklungs- und Prüflabor

Projekt NetLab

NetLab ist ein Projekt zur Erforschung eines verteilten Entwicklungs-, Mess- und Prüflabors, in dem wesentliche Ressourcen sicher und effizient zwischen ansonsten gegebenenfalls in Konkurrenz stehenden Entitäten geteilt werden können. Besonders hohe Sicherheitsanforderungen ergeben sich dabei nicht nur bei Übertragung, Speicherung und Zugriff durch die verschiedenen Parteien, sondern auch bei der physischen Sicherheit. Die prototypische Implementierung des NetLab soll als Plattform für weitere Forschungsarbeiten nutzbar sein, damit auch neue Technologien, die gegenwärtig noch nicht sinnvoll verwendet werden können, wie 5G und volle homomorphe Verschlüsselung, auf ihre Einsatztauglichkeit im Kontext der verteilten Entwicklungs- und Prüflabore untersuchbar werden.

Gerade kleine und mittelständische Unternehmen (KMU) besitzen oft eine hohe Expertise in einem Nischenbereich, die sie zu Marktführer macht. Allerdings besitzen sie dabei nicht unbedingt die Ressourcen, ein Gesamtsystem bereitzustellen, für das sie eigentlich nur Teilkomponenten herstellen. Somit werden diese dann zwar umfangreich isoliert getestet, Integrationstests und globale Optimierungen allerdings von anderen Unternehmen durchgeführt.

Dafür müssen nicht nur die Daten der Komponententests, sofern sie für weiterführende Tests notwendig sind, an die entsprechenden Unternehmen weitergeleitet werden, sondern auch die Bauteile selbst. Das bedeutet einen logistischen und finanziellen Mehraufwand. Vollständige Testdatensätze befinden sich gegebenenfalls schnell im Terabyte-Bereich und werden daher bisweilen auf Festplatten kopiert, die dann per Boten übertragen werden. Bauteile können dagegen schon auf Grund der Größe und des Gewichts sehr teuer und umständlich für den Transport werden, wie zum Beispiel Autos.

Simulationen sind besonders hilfreich, um das Fehlen von Komponenten auszugleichen oder potenzielle Gefahrenquellen zu untersuchen, benötigen aber für realitätsnahe Ergebnisse und eine hohe Aussagekraft auch genaue Modelle. Einerseits können die Hersteller der jeweiligen Komponenten diese Modelle präziser erzeugen als andere und darüber hinaus auch kontinuierlich weiterentwickeln. Auf der anderen Seite will aber auch nicht jeder seine Modelle zum Testen weitergeben, da sie per Definition präzise mathematische Beschreibungen der selbst entwickelten Komponenten und damit Geschäftsgeheimnisse enthalten, die aus den Modellen zurückgewonnen werden könnten.

An dieser Stelle setzt das Projekt NetLab an, das eine Infrastruktur konzipiert und prototypisch implementiert, mit der unterschiedliche und potenziell in Teilbereichen konkurrierende Unternehmen Entwicklungs- und Testdaten austauschen können, ohne dabei zu viele Unternehmenswerte preisgeben und die jeweiligen Komponenten oder Datenträger transportieren zu müssen.

So kann beispielsweise ein Hersteller eines Antriebsstrangs für ein Elektrofahrzeug eine Simulation durchführen, in der die Wechselwirkungen einer in der Entwicklung befindlichen Komponente mit einem bestimmten

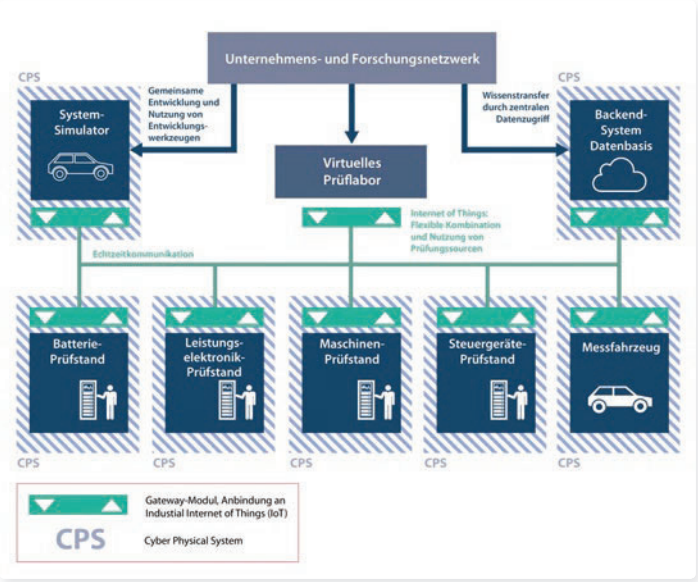

Bild 1: Struktur des verteilten Prüflabors NetLab im RuhrValley

Batteriesystem untersucht werden, ohne dass das genaue Modell des Batterieherstellers vollständig übertragen oder auf der eigenen Infrastruktur betrieben werden muss.

Mit diesem Digitalisierungsschritt wird der Ressourcenaufwand des Datenaustausches deutlich reduziert, der Prozess flexibler gemacht und eine bessere Skalierbarkeit geschaffen. Allerdings eröffnet die Digitalisierung auch neue Risiken in Bezug auf die Daten- und Systemsicherheit. Daher benötigt das NetLab neben einem System für den schnellen Datentransfer auch ein modernes und robustes Sicherheitskonzept.

Abgrenzung zu VPN-Lösungen

Der sichere Zugang zu geschützten Netzwerken, und damit auf geschützte Daten, kann über verschiedenste IT-Sicherheitstechniken und -Systeme erreicht werden. Das häufig genutzte Virtual Private Network (VPN) wird beispielsweise von Mitarbeitern im Home-Office oder Außendienst verwendet, um über ein ungesichertes Netz wie das Internet auf unternehmensinterne Daten zugreifen zu können.[1] Diese Zugänge sind natürlich individuell konfigurierbar, sodass nicht jeder Mitarbeiter auf alle Daten zugreifen kann. Genauso kann auch externen Personen ein Zugriff auf die Daten bereitgestellt werden. Allerdings ist die Konfiguration eines solchen Zugriffs je nach Security-Policy des Unternehmens zeitaufwendig und gerade bei dringenden Änderungen fehleranfällig. Zudem potenziert sich diese Anfälligkeit bei der Teilnahme von mehreren Unternehmen, die untereinander Daten austauschen wollen. Hier müsste in der Regel jedes Unternehmen eine eigene VPN-Lösung anbieten und verwalten, sodass sich eine enorme Menge an Zertifikaten oder im schlimmeren Fall sogar Passwörtern ansammeln würde.

Das NetLab-System zentralisiert dagegen sowohl das Identitäts-Management (IdM) als auch die Datenpersistenz, sodass die aufwendige Konfiguration und Wartung einer VPN-Lösung entfällt und weniger Daten lokal vorgehalten werden müssen. Damit wird die Infrastruktur der teilnehmenden Organisationen deutlich entlastet und die Komponenten des NetLab einfacher zu testen und zu warten.

Durch die Zentralisierung des IdM und den Einsatz von etablierten Standards sowie offenen Protokollen wird zudem die Flexibilität in Bezug auf den Austausch einzelner Komponenten gesteigert. Somit können Implementierungen gewählt werden, die eine hohe Skalierbarkeit und Auditierbarkeit garantieren, was der Effizienz und Sicherheit zugutekommt.

Transportsicherheit

Da das verteilte Laborsystem über inhärent unsichere Netze wie das Internet kommuniziert, müssen alle Transportdaten zu jedem Zeitpunkt geschützt werden. Die Basis für diesen Schutz liefern getestete und standardisierte Protokolle und Verfahren der

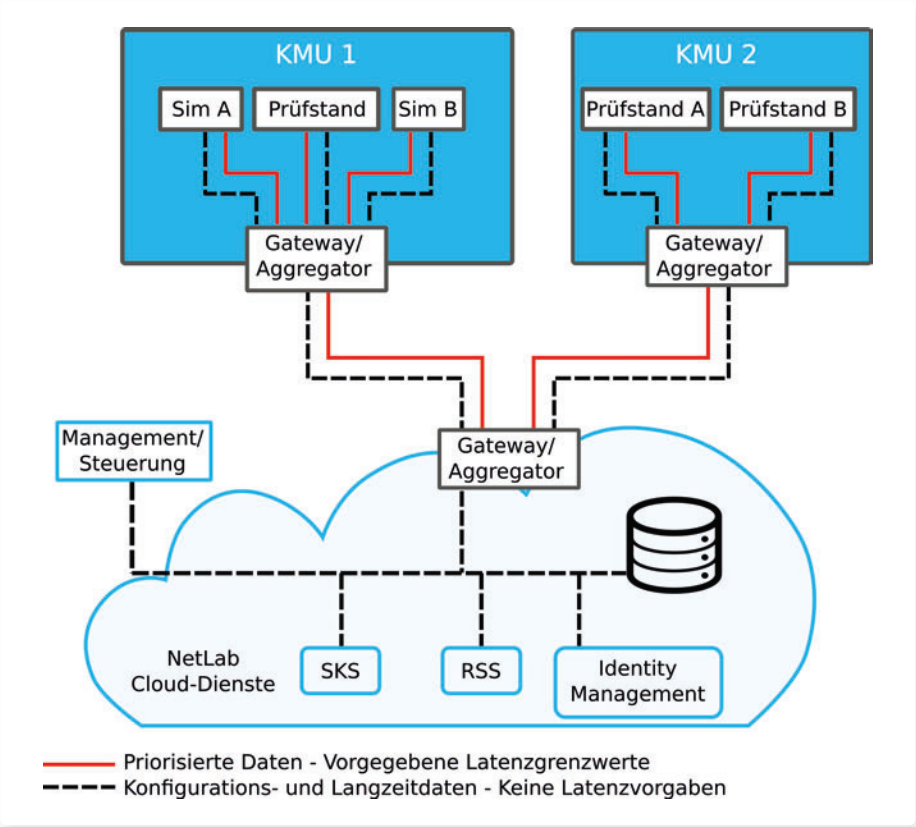

Bild 2: Da das verteilte Laborsystem über inhärent unsichere Netze wie das Internet kommuniziert, müssen alle Transportdaten zu jedem Zeitpunkt geschützt werden.

Transport Layer Security (TLS), die auch in Internet-Browsern für HTTPS-Verbindungen verwendet werden.[1] Damit werden alle Daten innerhalb des verteilten Netzwerkes nur über gesicherte Verbindungen ausgetauscht. Darüber hinaus werden auch die Nutzdaten selbst ausschließlich verschlüsselt versendet. Auch hierbei wird auf anerkannte IT-Sicherheitsstandards gesetzt. Darüber hinaus finden auch aktuelle Empfehlungen der einschlägigen Sicherheitsbehörden Beachtung.

Diese zusätzliche Verschlüsselung erfordert einen gewissen Mehraufwand, der die Sendeverzögerung von Datenpaketen in das Netzwerk erhöht. Der Mehraufwand hängt maßgeblich vom verwendeten Verfahren, der Schlüssellänge und der zur Verfügung stehenden Hardware-Unterstützung ab. Bei einer regulären Übertragung über handelsübliche Internetleitungen ohne Spezialhardware waren die durchschnittlichen Latenzen bei experimentellen Voruntersuchungen jedoch im zweistelligen Millisekundenbereich und damit um mehrere Größenordnungen höher als die Verschlüsselungsdauer. Folgeuntersuchungen in diesem Bereich werden vor allem dann interessant, wenn Teile der Kommunikationsnetze auf 5G-Technologie umgestellt werden, bei der streckenweise Latenzen im einstelligen Millisekundenbereich zu erwarten sind.

Identitätsmanagement

Im NetLab werden Identitäten zentral verwaltet. Hierbei wird auf etablierte Standard-Systeme gesetzt, denen durch den täglichen weltweiten Einsatz ein hoher Reifegrad unterstellt werden kann. Dieser zentrale Ansatz erlaubt eine einfache und einheitliche Verwaltung von Benutzern, Gruppen und deren Berechtigungen. So kann es beispielsweise nicht dazu kommen, dass eine Entität, deren Zugriffsberechtigung widerrufen wurde, auf Grund der noch nicht aktualisierten Datenlage eines Teilsystems unberechtigten Zugriff erhält.

Zur Authentifikation kommen sowohl wegen des hohen Verwaltungsaufwands als auch auf Grund von offensichtlichen Nachteilen in Bezug auf das Sicherheitsniveau für die im NetLab teilnehmenden Endgeräte keine Passwörter in Frage. Stattdessen wird eine Public-Key-Infrastruktur mit X.509-Zertifikaten eingesetzt, die vom IdM ausgestellt und verwaltet werden. Durch die Verwendung des Online Certificate Status Protocol (OCSP) kann jede Entität jederzeit prüfen, ob ein Zertifikat noch gültig ist oder widerrufen wurde.

Auch die Benutzerrollen werden über das IdM verwaltet. Wesentliche Basis-Rollen im NetLab sind Standortadministratoren, Geräteadministratoren, Test-Manager und Test-Techniker. Standortadministratoren übernehmen die Verwaltung für einen gesamten teilnehmenden Standort, beispielsweise eine Hochschule oder ein Unternehmen. Diesen unterstellt sind ein oder mehrere Geräteadministratoren, die für das Eintragen, Löschen und Umkonfigurieren von Geräten des NetLab-Systems zuständig sind. Sie legen auch mit Hilfe eines Konfigurationsprogramms fest, welcher Klasse ein Gerät entspricht.

Diese Informationen benötigt ein Test-Manager, wenn ein Vorgang im Management-Service vorbereitet wird und Ressourcen reserviert werden müssen. Schließlich werden Test-Techniker nach einem erfolgreich geplanten Ablauf benötigt, um die entsprechenden physischen Vorbereitungen an einem Standort durchzuführen – beispielsweise einen Prüfling in einen Messstand einzulegen – und zu quittieren.

Schlüsselverwaltung

Wenn alle Vorbereitungen getroffen wurden und ein Mess- oder Prüfvorgang gestartet werden kann, generieren alle Daten erzeugenden Geräte starke symmetrische Sitzungsschlüssel. Diese werden anschließend mit dem öffentlichen Schlüssel im Zertifikat des jeweiligen Empfängers verschlüsselt und an den Session Key Service (SKS) gesendet, der diese verschlüsselt persistiert. Somit kann jede Entität das notwendige Schlüsselmaterial von einer zentralen Stelle abfragen, die selbst niemals Kenntnis über die tatsächlichen Schlüssel erhält.

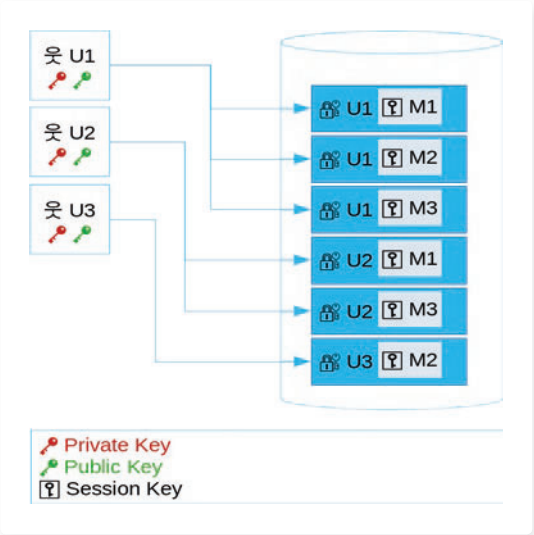

Bild 3: Wenn alle Vorbereitungen getroffen wurden und ein Mess- oder Prüfvorgang gestartet werden kann, generieren alle Daten erzeugenden Geräte starke symmetrische Sitzungsschlüssel. Diese werden anschließend mit dem öffentlichen Schlüssel im Zertifikat des jeweiligen Empfängers verschlüsselt und an den Session Key Service (SKS) gesendet, der diese verschlüsselt persistiert.

Als besonders kritisches Material sind die Schlüssel somit auch über mehrere Ebenen gesichert. Zum einen kann der SKS niemals auf die eigentlichen Schlüssel schließen, da diese immer mit dem öffentlichen Schlüssel aus dem Zertifikat des jeweiligen Empfängers verschlüsselt sind. Somit kann auch niemand einen Session Key lesen, der an eine andere Entität – Gerät oder Person – gerichtet ist. So kann beispielsweise eine Entität, der aus dem Prozess entfernt werden soll, bei der Key-Rotation einfach ausgelassen werden. Sie hat fortan keinen Zugriff mehr auf neue verschlüsselte Daten. Zum anderen wird der Zugriff auf die entsprechenden Daten im SKS durch das IdM unterbunden, sodass ein weiterer IT-Sicherheitsmechanismus auf der Ebene des Datenbank-Management-Systems (DBMS) greift.

Auch NetLab-interne Systeme benötigen zeitweise Schlüsselmaterial, das für die Ausführung ihrer Arbeiten über einen längeren Zeitraum sicher abgelegt werden muss. Somit stellt der SKS einen essentiellen Basis-Sicherheitsdienst für das NetLab dar.

LastPass by LogMeIn

Sichere Passwörter jetzt!

81 % aller Datenlecks haben unsichere Passwörter als Ursache – steuern Sie jetzt mit LastPass dagegen!

Enterprise Passwort Management

Gemäß BSI C5

Zero Knowledge Sicherheitsmodell

Vereintes Identitätsmanagement

Bewährt bei 47.000 Kunden

CHIP Testsieger
Vergleichstest: Passwort-Manager
CHIP 03/2019
LastPass Premium
Unabhängige Tests seit 1978
CC151708

Stiftung Warentest test
Test-Fazit: empfehlenswert
LastPass Premium
Ausgabe 10/2017
www.test.de

Jetzt hier informieren: www.lastpass.com

Datensicherheit at Rest

Viele Daten müssen irgendwann persistiert werden. Vor allem Informationen über die jeweiligen Unternehmen, die am verteilten System teilnehmen, müssen ebenso wie Testergebnisse über einen längeren Zeitraum gespeichert werden. Da diese potenziell riesigen Datensätze enorme Unternehmenswerte darstellen, müssen sie auf vielfältige Weise geschützt werden. Das NetLab sieht dabei für Langzeitdatenspeicherung einen zentralen Datenbank-Service vor, der auf verschiedene Knoten repliziert werden kann. So können klassische DBMS-Sicherheitsmechanismen im Sinne der Benutzer- und Rollen-Modelle eingesetzt werden.

Konnte ein Angreifer trotzdem Zugriff auf die Datenbank erlangen, beispielsweise durch eine bisher unbekannte Schwachstelle, sind die Daten immer noch durch die Verschlüsselung abgesichert. So können gestohlene Datensätze, außer zu statistischen Zwecken, trotz allem nicht weiter verwertet werden. Des Weiteren kann mit Hilfe von verschlüsselten Metadaten sichergestellt werden, dass keine neuen Daten eingebracht oder bestehende Daten verändert wurden, ohne dass dieser Umstand erkannt wird. Schließlich werden regelmäßige Backups durchgeführt und Daten begrenzt lokal vorgehalten. Im Notfall können damit Daten wiederhergestellt werden, wenn sie von einem Angreifer aus der Datenbank gelöscht oder durch einen Hardware-Ausfall zerstört wurden.

Die Sicherheit der Unternehmenswerte im Langzeitdatenspeicher wird damit auf mehreren Ebenen durchgesetzt. Allerdings sollten, wie auch bei Passwörtern, die verwendeten Schlüssel regelmäßig gewechselt werden, um Angriffe auf die Verschlüsselung zu erschweren.

Im Zuge der Forschungsarbeit wurden deshalb unterschiedliche Verfahren untersucht, um effizient und sicher mit dem Schlüsseltausch umzugehen. Das Kernziel war die Wahrung der Ende-zu-Ende-Verschlüsselung, ohne dabei zu hohen Overhead zu erzeugen.

Erste Überlegungen enthielten naive Verfahren wie die n-fache verschachtelte Verschlüsselung oder Ver- und Entschlüsselung auf Datenbankseite. Diese Verfahren erfüllen aber für sich nicht alle der genannten Ziele – entweder durch wachsende Kosten pro Umschlüsselung oder durch das Brechen der Anforderung von durchgehender Ende-zu-Ende-Verschlüsselung. Die schließlich gewählte Lösung vereint jedoch die Vorteile aus beiden Ansätzen.

Das Ergebnis ist das „Re-Sealing System" (RSS). Diese Komponente erzeugt bei der Speicherung eine weitere Verschlüsselungsschicht über den Daten und benutzt die bestehende Infrastruktur des SKS, um Schlüssel für berechtigte Empfänger zu erzeugen.

Müssen Schlüssel getauscht werden, kann das RSS einfach seine Verschlüsselungsschicht aufheben und eine neue Ebene erzeugen. Im selben Schritt können bereits gegebene Zugriffsberechtigungen widerrufen oder neue erteilt werden, indem nur der neuen Menge an Berechtigten die Schlüssel für die äußere Schicht mitgeteilt werden. Anwendungsbeispiele dafür sind etwa ausscheidende oder neu angestellte Mitarbeiter.

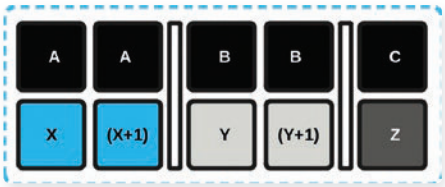

Bild 4: RSS erzeugt zusätzlich Schlüssel A, B und C für drei unterschiedliche Datensätze.

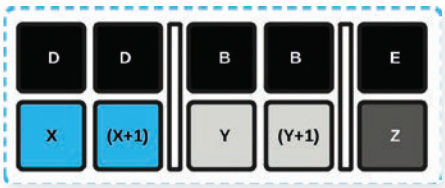

Bild 5: RSS erneuert die zusätzliche Sicherungsschicht mit den neuen Schlüsseln D sowie E.

Dieser Vorgang soll mit den Bildern 4 und 5 beispielhaft veranschaulicht werden. Die Datenpakete X und (X+1) wurden mit dem gleichen Sitzungsschlüssel verschlüsselt, ein weiterer Schlüssel wurde für Y und (Y+1) verwendet und ein dritter Schlüssel wurde bei Datensatz Z benutzt. Für jeden dieser Datensätze erzeugt das RSS einen zusätzlichen Schlüssel A, B sowie C (Bild 4).

Verlässt nun ein Mitarbeiter mit Zugriff auf die Datenpakete X und (X+1) das entsprechende Unternehmen, entschlüsselt das RSS die Sicherungsschicht A, generiert einen neuen Schlüssel D und verschlüsselt die (verschlüsselten) Daten mit dem neuen Schlüssel, der anschließend in den SKS gegeben wird. Je nach Policy der Daten generierenden Entität kann dieser Prozess auch durch andere Ereignisse ausgelöst werden. Beispielsweise könnte der Datensatz Z bereits so lange im Langzeitdatenspeicher liegen, dass dieser als IT-Sicherheitsmaßnahme mit einem neuen Schlüssel E gesichert wird (Bild 5). Bei diesem Verfahren ist sowohl der Aufwand beim Zugriff auf die Daten seitens eines Clients als auch für das Re-Sealing für den Server pro Vorgang konstant. Zudem besteht zu keinem Zeitpunkt die Chance, dass unverschlüsselte Daten auch nur im Arbeitsspeicher eines Servers liegen.

Physische Systemsicherheit

Während das NetLab-Sicherheitskonzept hauptsächlich auf die digitalen Werte abzielt, müssen für einen sinnvollen und realistischen Betrieb eines verteilten Labors auch strikte Regeln im Bereich der physischen Systemsicherheit umgesetzt und kontrolliert werden. So können zwar die übertragenen Daten durch Verschlüsselung und Signaturen vor (unbemerkten) Manipulationsversuchen geschützt werden, die Daten erzeugenden Anlagen selbst können aber gegebenenfalls viel einfacher angegriffen werden. Daher sollten nach Möglichkeit vergleichbare Maßnahmen ergriffen werden, wie sie in gängigen Datenzentren vorzufinden sind.

Schließanlagen und Wachpersonal erschweren dabei den physischen Zugriff, Überwachungsanlagen helfen bei der Alarmierung vor und der Aufklärung von Zwischenfällen und Anlagen-spezifische Sicherungsmaßnahmen verhindern eine versehentliche oder mutwillige Fehlbedienung von Betriebsmitteln.

Da aber viele Mess- und Prüfstände hochspezialisierte Geräte sind, die einfach dahingehend manipuliert werden können, dass sie fehlerhafte Daten generieren oder gar Schaden nehmen, kann auch eine Betriebsverordnung in Betracht gezogen werden, die ein Mehr-Augen-Prinzip einfordert. Im Bereich der Datensicherheit von Langzeitdatenspeicher, IdM und Test-Management-System ist dagegen der physische Zugriff als vergleichsweise geringes und kalkulierbares Risiko zu betrachten, da alle Nutzdaten verschlüsselt vorliegen, die Festplatten der benutzten Server voll-verschlüsselt sind und alle Dienste redundant ausgelegt sind.

Wer es bei den Netlab-Clouddiensten also schafft, einzelne Komponenten wie Festplatten zu stehlen, verursacht so zwar einen nicht unerheblichen finanziellen Schaden, bringt damit aber nicht zwangsläufig das Gesamtsystem zum Stillstand.

Grenzen der Sicherheit

Viele typische Angriffe können durch das IT-Sicherheitskonzept im NetLab systematisch ausgeschlossen oder ihnen kann entschärfend begegnet werden, andere dagegen lassen unter Umständen keine sinnvolle Mitigation zu.

Gerade die Daten erzeugenden Systeme und Standorte, also unter anderem KMU (kleine und mittlere Unternehmen), sind auf Grund der eigenen Infrastruktur weniger gegen Angriffe gewappnet. Während verteilte Datenzentren durch Umleitungen und redundant ausgelegte Hardware bis zu einem gewissen Grad gegen Distributed-Denial-of-Service-Angriffe (DDoS) verteidigt werden können, sind Kommunikationsendpunkte mit schwacher Infrastruktur in diesem Punkt im Nachteil. Unterbrechungen der Internetverbindung können in einigen Fällen durch die Zwischenspeicherung der Daten in der lokalen Gateway-Komponente ausgeglichen werden.

Dauern die Unterbrechungen aber länger an, kann ein Vorgang mit engeren zeitlichen Vorgaben davon beeinträchtigt werden. Somit kann sich die Sicherheit einer verteilten Messung/Prüfung auf die Verfügbarkeit der einzelnen partizipierenden Standorte reduzieren, was bei der Planung entsprechend mitbedacht werden sollte.

Wird beispielsweise eine Komponente vorgesehen, die zur Zeit der Vorgangsplanung nicht redundant verfügbar ist, muss darauf geachtet werden, dass sie über entsprechende Ausfallsicherheitsmaßnahmen verfügt. So sollte beispielsweise nach Möglichkeit eine zweite Internetleitung angebunden sein und eine Notfallstromversorgung existieren.

Ausblick

Die prototypische Implementierung des NetLab soll als Plattform für weitere Forschungsarbeiten nutzbar sein, damit auch neue Technologien, die gegenwärtig noch nicht sinnvoll verwendet werden können, auf ihre Einsatztauglichkeit im Kontext der verteilten Entwicklungs- und Prüflabore untersuchbar werden. Darunter fallen zukünftige Untersuchungen der tatsächlich auftretenden durchschnittlichen Latenzen beim realistischen Einsatz von 5G-Technologien, auch in Bezug auf die Auswirkungen des Standorts und der Entfernung zwischen den Daten erzeugenden Parteien. Für aussagekräftige Daten werden groß angelegte Studien mit entsprechendem Datenaufkommen über eine längere Laufzeit sinnvoll.

Des Weiteren zeigt sich eine interessante Entwicklung in einem relativ neuen Feld der Kryptografie, die sich in Zukunft im NetLab einsetzen lassen könnte: vollständige Homomorphe Verschlüsselung („Full Homo-

morphic Encryption", FHE). Bei der Entwicklung des NetLab werden die Systeme nach Möglichkeit auf den Einsatz von solchen modernen kryptografischen Verfahren vorbereitet, da diese eine direkte Verarbeitung von verschlüsselten Daten in der Cloud ohne deren Entschlüsselung ermöglichen würden. Das wiederum würde die Angriffsfläche in Bezug auf potenziell unerlaubte Zugriffe auf kritische Testdaten gegebenenfalls stark reduzieren. Allerdings eignen sich die FHE-Verfahren wegen fehlender Standardisierungen durch etablierte Normierungsorganisationen wie ISO, ANSI, NIST und BSI aktuell noch nicht für einen produktiven Einsatz.

Zusammenfassung

Moderne Authentifikationsverfahren mit starken Verschlüsselungstechnologien und einem flexiblen Identitäts- und Schlüsselmanagement legen den Grundstein für die experimentelle Bestimmung von Parametern für und Grenzen von diversen Anwendungsmöglichkeiten und potenziellen Geschäftsfeldern in den Bereichen Internet of Things (IoT) und Infrastructure as a Service (IaaS). Damit schafft das NetLab eine moderne Versuchsplattform für eine sichere verteilte Laborumgebung, die eine weitere Erforschung eines alltagstauglichen Betriebs komplexer moderner Infrastrukturen in potenziell konkurrierenden Netzwerkzusammenschlüssen erlaubt.

Das zentrale Identitätsmanagement erlaubt eine flexible Handhabung der beteiligten Benutzer, Rollen und ihrer Berechtigungen und kann durch Replikation beliebig ausfallsicher gestaltet werden. Die Möglichkeit, Erweiterungen für das IdM zu entwickeln, erlaubt eine Einbindung verschiedener Protokolle und Identitätsprovider, sodass neben Zertifikaten beispielsweise auch Hardware-Security-Module oder Hardware-Token verwendet werden können.

Starke Sitzungsschlüssel sorgen in Verbindung mit der eigenen Public-Key-Infrastruktur für eine sichere Verschlüsselung, sodass nicht nur die Transportebene verschlüsselt wird, sondern auch die sich im Transit befindenden sowie persistierte Nutzdaten. Dabei erhalten nur die entsprechend berechtigten Nutzer Zugriff auf die Schlüsseldatenbank und die für sie bestimmte aktuelle Version des Schlüsselmaterials.

Alle Daten im Langzeitdatenspeicher werden mindestens mit einem starken Sitzungsschlüssel verschlüsselt und können selbst vom DBMS nicht entschlüsselt werden. Schlüsselrotationen und Aktualisierungen von Zugriffsberechtigungen werden durch das Zusammenspiel von IdM, SKS und RSS umgesetzt und erlauben die Aufrechterhaltung des Sicherheitsniveaus auch über längere Zeiträume und bei Sicherheitsvorfällen. ■

Quellen

[1] *N. Pohlmann: Lehrbuch „Cyber-Sicherheit", Springer Vieweg Verlag, Wiesbaden 2019, ISBN 978-3-658-25397-4*

DOMINIK GRAFE,
Mitarbeiter im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Er beschäftigt sich mit der Erforschung eines sicheren, vertraulichen und verteilten Entwicklungs-, Mess- und Prüflabors.

MARCEL ROTHE,
Mitarbeiter im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Er beschäftigt sich mit der Erforschung eines sicheren, vertraulichen und verteilten Entwicklungs-, Mess- und Prüflabors.

ILLYA SIROMASCHENKO,
Mitarbeiter im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Er beschäftigt sich mit der Erforschung eines sicheren, vertraulichen und verteilten Entwicklungs-, Mess- und Prüflabors.

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.