Kai Martius

SINA: IT-Sicherheit als Infrastruktur betrachtet

Cyberangriffe nehmen stetig zu, werden immer vielfältiger und professioneller. Im Umfeld von kritischen Infrastrukturen wie etwa Energie- und Wasserversorgern oder im Verkehr können sich potenzielle Cyberrisiken deshalb fatal auswirken. Gleiches gilt im Rahmen der landes- oder bundesbehördlichen Ver- und Bearbeitung von sensiblen Verschlusssachen (VS), bei deren Handhabung die gesetzlichen Vorschriften des nationalen Geheimschutzes, der Verschlusssachenanweisung sowie in Teilen auch Regelungen der EU und NATO berücksichtigt werden müssen. Der folgende Beitrag zeigt, wie die Sichere Inter-Netzwerk Architektur (SINA) hierbei einen Beitrag zur Kommunikationssicherheit liefern kann.

1 Einführung

Gezielte Angriffe auf diese Infrastrukturen bedrohen nicht nur die Geheimhaltung, sondern können in der Folge auch messbare, physische Schäden anrichten oder sogar das Wohl der Bevölkerung gefährden.

Im Zuge der Corona-Pandemie erfahren Unternehmen und Behörden einmal mehr, wie wichtig es ist, proaktiv beim Thema IT-Sicherheit zu agieren. Denn Kriminelle aus dem In- und Ausland haben ihre Angriffsstrategien schnell und flexibel an die neuen Gegebenheiten – die Arbeit im oftmals weniger gesicherten Homeoffice und die vermehrte Digitalisierung analoger Prozesse – angepasst. Laut dem aktuellen Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Zahl neuartiger Schadprogramme zwischen dem 1. Juni 2019 und dem 31. Mai 2020 um insgesamt 117,4 Millionen angewachsen[1].

2 Ganzheitliche Sicherheitsarchitektur statt Einzellösungen

Um die IT-Sicherheit bei sensiblen Daten und Informationen zu gewährleisten, wird zum Teil immer noch auf technische Einzellösungen (womöglich von unterschiedlichen Anbietern) gesetzt. Dies mag oft dem klassischen Vorgehen von IT-Abteilungen entsprechen, kundenspezifische Gesamtlösungen selbst zusammenzubauen und zu betreiben, birgt aber Nachteile in der Administration und letztlich sogar große IT-Sicherheitsrisiken. Im Zeitalter der Spezialisierung sollten IT-Sicherheitslösungen ganzheitlich zusammenspielen – und dort, wo es bereits abgestimmte Lösungen gibt, diese präferiert eingesetzt werden.

Dagegen wird bei Einzellösungen bereits die Gefahrenanalyse als solche entweder erschwert oder für bestimmte Bereiche gar nicht durchführbar, da Informationen zwischen Endpunkten, Netzwerken und Schnittstellen möglicherweise nicht geteilt werden. Im Ernstfall kann es zu Zeitverzögerungen kommen, wenn verschiedene IT-Sicherheitslösungen nebeneinander existieren. Ein effektives und frühzeitiges Eingreifen wird damit gehemmt. Hinzu kommt, dass ein maschineller Lerneffekt der jeweiligen Technologien hinsichtlich neuer potenzieller Sicherheitsbedrohungen ausbleibt, weil sie dafür nicht eng genug zusammenarbeiten. Abgesehen von diesen unerwünschten Folgen ist es durch die ständig wachsende Bedrohungsvielfalt kaum mehr möglich, Schwachstellen oder gar Angriffe manuell zu bewältigen. Das gilt vor allem angesichts riesiger Datenmengen im Umfeld von Rechenzentren beziehungsweise der Cloud: Sogar ein geschultes Team mit deutlich aufgestocktem Fachpersonal würde hier nicht ausreichen, um potenziellen Bedrohungen oder bereits bestehenden Anomalien händisch Herr zu werden; die Anzahl der beteiligten IT-Systeme bzw. die sich daraus ergebend zu analysierende Datenmenge ist dafür schlichtweg zu groß.

Gefahrenanalysen und das damit eng verknüpfte Patchmanagement können automatisiert werden. Aber auch hier greift eine taktische Grundhaltung, die für jedes Problem eine spezifische technische Lösung sucht, langfristig zu kurz. Umfassender, effizienter, aber vor allem sicherer ist es hingegen, auf eine strategische IT-Sicherheitslösung zu setzen und beispielsweise Automatisierungsprozesse innerhalb einer standardisierten sowie ganzheitlichen digitalen Infrastruktur zu verankern. Anders formuliert: Anstatt mit unterschiedlichen Einzellösungen lediglich zu reagieren, sollte mithilfe einer dynamischen Sicherheitsarchitek-

1 Dazu bspw. der Bericht des Bundesamts für Sicherheit in der Informationstechnik 09/2020: Die Lage der IT-Sicherheit in Deutschland 2020. S. 9.

Dr. Kai Martius

ist seit 2007 im Geschäftsbereich Hochsicherheit der secunet und seit 2019 im secunet Vorstand. Er zählt maßgeblich mit zu den Architekten von SINA.

E-Mail: kai.martius@secunet.com

tur, die als Gesamtlösung von Client bis zum Netzwerk fungiert, vorausschauend agiert werden.

3 SINA – eine Erfolgsgeschichte

Eine solche Gesamtlösung ist SINA, die Sichere Inter-Netzwerk Architektur. In Deutschland wird sie vorrangig bei Bundes- und Landesbehörden eingesetzt, ebenso in den Bundesministerien, aber auch bei Kritischen Infrastrukturen sowie der Bundeswehr kommt SINA zum Einsatz. Ausgangspunkt für die Entwicklung war die Verlegung des Parlaments- und Regierungssitzes von Bonn nach Berlin im Jahr 1999. Das BSI hatte sich im Zuge dessen zum Ziel gesetzt, umständliche analoge Sicherheitslösungen für Verschlusssachen durch digitale Technologien zu ersetzen. Deshalb initiierte das BSI ein Projekt zur Absicherung von IP-basierten Netzen unter Verwendung kryptographischer Sicherungsmechanismen. Nach ersten erfolgversprechenden Prototypen beauftragte das BSI dann die (Weiter-)Entwicklung und Produktion. Seitdem wurde das SINA-Portfolio vielfach erweitert und immer wieder neuen Anforderungen angepasst.

4 Sichere digitale Infrastruktur für Bundes- und Landesbehörden

Die Vorgaben des BSI, um mit Verschlusssachen arbeiten zu dürfen, erfordern ein umfassendes Sicherheitskonzept, welches unter anderem einen unumgehbaren VPN-Client (Virtual Private Network), eine Festplattenverschlüsselung sowie eine Schnittstellenkontrolle vorsieht. In SINA sind alle Anforderungen mit einer Gesamtlösung abgedeckt. Das hat nicht nur sicherheitstechnische Vorteile gegenüber Einzellösungen, sondern auch wirtschaftliche und bürokratische. Eine stimmige Gesamtarchitektur spart langfristig Geld und Ressourcen, da nicht regelmäßig an verschiedenen Stellen nachgebessert werden muss. Zudem müssen sich die nutzenden Institutionen mit SINA nicht eigenhändig einzelne Komponenten für sichere Arbeitsplätze zusammenstellen und anschließend für diese spezielle Konfiguration Freigabeprozesse durchlaufen, denn SINA umfasst bereits alle für den VS-konformen Betrieb notwendigen und aufeinander abgestimmte Bestandteile und gewährt dabei höchste Sicherheit für Daten – wenn erforderlich sogar bis zur Einstufung GEHEIM[2]. Zahlreiche Landes- und Bundesbehörden arbeiten aus diesen Gründen schon seit vielen Jahren mit dieser Gesamtlösung. Einige Bundesministerien haben ihre Arbeitsplätze vollständig mit der SINA-Technologie mit Zulassung für das Sicherheitsniveau VS-NfD (NUR FÜR DEN DIENSTGEBRAUCH) ausgestattet.

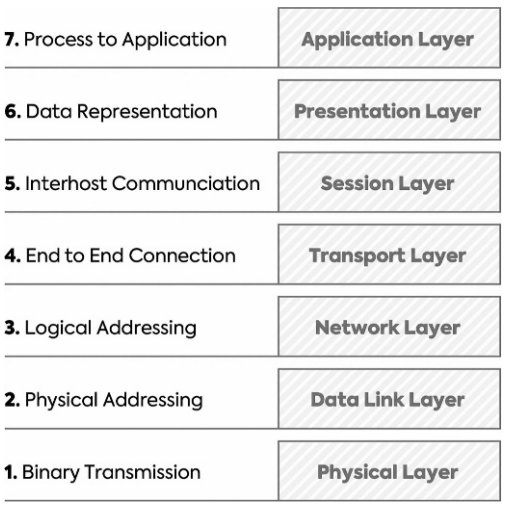
Dabei wird auch die Nutzerfreundlichkeit geschätzt. Anwender können mit SINA-Sicherheitsfunktionen in ihren gewohnten Umgebungen, also mit den bekannten Betriebssystemen und Softwareprodukten, arbeiten. Die SINA-Komponenten eignen sich für verschiedenste Anwendungsszenarien, wie zum Beispiel der sicheren Anbindung von Standorten, der Nutzung mobiler Arbeitsplätze oder dem Betrieb von unterschiedlich schutzbedürftigen Arbeitsplatzsitzungen auf nur einem Rechner. Die Hard- und Software-Architektur ist auch für internationale Geheimhaltungsstufen (NATO RESTRICTED und RESTREINT UE) zugelassen und findet mittlerweile in über 25 Ländern Anwendung. Insgesamt gibt es derzeit rund 180.000 Installationen des Systems.

4.1 Ganzheitlicher Ansatz: vom Client bis zur Infrastruktur

SINA besteht aus vier aufeinander abgestimmten und modularen Primärkomponenten: SINA Client, SINA Box, SINA Management und SINA Workflow. SINA Clients sind in verschiedenen Formfaktoren wie Laptop und Desktop verfügbar und durch mehrere ineinandergreifende Schutzmaßnahmen abgesichert. Durch eine hochinnovative Client-Virtualisierung besteht beispielsweise Schutz gegenüber Windows Malware, da ein direkter Zugriff des virtualisierten Windows-Betriebssystems auf die physische Hardware nicht möglich ist. Die Virtualisierung stellt zwar grundsätzlich höhere Anforderungen an die Hardware (CPU, RAM), aber das Plus an Sicherheit steht klar im Vordergrund.

SINA Boxen sind Krypto-Gateways und ermöglichen die sichere Übertragung von Daten. Sie setzen auf Layer 2 oder 3 des Open Systems Interconnection(OSI)-Schichtenmodells an. Je nach Variante und Krypto-Algorithmus sind die Gateways für unterschiedliche Geheimhaltungsgrade von VS-NUR FÜR DEN DIENSTGEBRAUCH über VS-VERTRAULICH bis zu GEHEIM zugelassen. Zum Teil sind die Produkte neben den bereits beschriebenen digitalen Sicherheitstechnologien zusätzlich gegen physische Manipulationen geschützt. Ein elementarer Vorteil – insbesondere gegenüber Einzellösungen – ist das SINA Management, mit dem alle Komponenten und Benutzer des Systems zentral sowie aufgrund von Remote Access bei Bedarf auch standortunabhängig verwaltet werden können. Mithilfe der grafischen Benutzeroberfläche ermöglicht SINA Management eine einfache Steuerung von Sicherheitsbeziehungen und Zugangsberechtigungen. Übergreifend nutzt das Produkt SINA Workflow die sicheren Infrastrukturkomponenten, um eine VSA-konforme, nachweissichere Digitalisierung des Workflows von VS-Dokumenten zu ermöglichen.

Abbildung 1 | OSI-Schichtenmodell



2 Siehe dazu auch die „Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA)"

4.2 Die richtige Lösung für jede Anwendung

Der primäre Zweck der SINA Boxen ist es, eine sichere Verbindung über ein unsicheres Transportnetz, beispielsweise das Internet, bereitzustellen. Diese wird entweder via L2 (Layer 2: Ethernet-basiert) oder L3 (Layer 3: IP-basiert) hergestellt. Je nach Bedarf der Applikationsumgebungen eignen sich L2- oder L3-Lösungen für verschiedene Einsatzbereiche: Layer-2-Verschlüsselungen bieten sich aufgrund des hohen Datendurchsatzes vor allem für die sichere Kopplung von Rechenzentren, zum Beispiel eines Hauptstandorts mit mehreren Nebenstandorten oder zweier Systeme bei Cloud-Anwendungen (client- und serverseitig) an. L3-basierte Lösungen hingegen haben unter anderem bei einer hohen Anzahl von Endpunkten mit kleinem Bandbreitenbedarf Skalierungsvorteile, wenn beispielsweise im Access-Bereich eine Vielzahl von Clientgeräten wie die SINA Workstation aus dem Homeoffice heraus mit einem Netzwerk verbunden werden.

4.3 Geschütztes, digitales Arbeiten und standortunabhängiges VS-Management

Eine SINA Workstation, egal ob als Desktop-PC, Laptop oder Tablet, kann als Client wiederum eine kryptographisch geschützte Verbindung über einen VPN-Tunnel mit einer SINA Box herstellen. Auf diese Weise ist zum Beispiel der gesicherte und standortunabhängige Zugriff auf vertrauliche Dokumente oder aber das gesamte Behördennetzwerk möglich. Die Nutzer arbeiten in ihrer gewohnten Umgebung, welche virtualisiert in das SINA-Sicherheitsbetriebssystem eingebettet ist. Zusätzlich verschlüsselt die SINA Workstation alle lokal gespeicherten Daten und schützt sie mit einer starken Zwei-Faktor-Authentisierung. Gelangt der Client doch einmal in die falschen Hände, sind die Daten ohne die Chipkarte mit passender PIN sicher vor unberechtigten Zugriffen.

Mit SINA Workflow hat die Ver- und Bearbeitung von VS zudem ein neues Level erreicht. Das digitale Verschlusssachenmanagementsystem befähigt Nutzer, eingestufte Dokumente direkt vom üblichen Arbeitsplatz aus komplett digital zu erstellen, zu registrieren, zu verwalten und sicher zu verteilen; papiergebundene Schritte fallen gänzlich weg. SINA Workflow ist bislang die einzige ganzheitliche und vom BSI bis einschließlich zur Einstufung GEHEIM freigegebene Lösung für das digitale VS-Dokumentenmanagement.

5 Neue Anforderungen, neue Lösungen

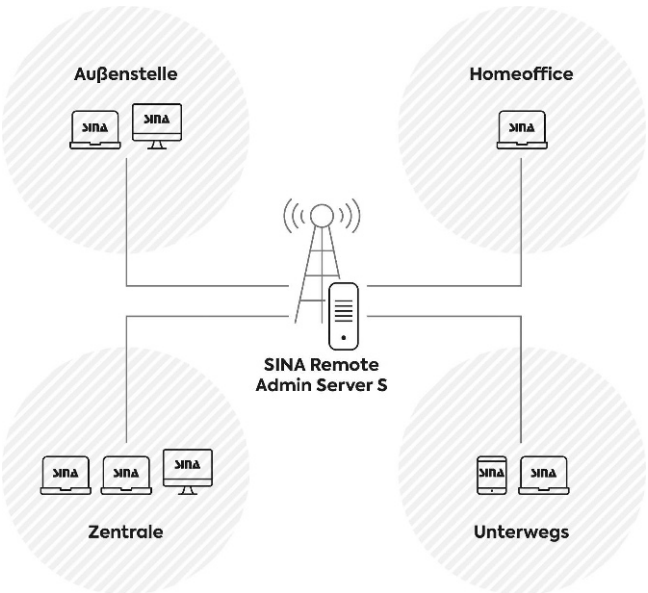
Im Zuge neuer Gegebenheiten sowie veränderter Arbeitsweisen und Ansprüche an das Equipment wurde in Zusammenarbeit mit dem BSI das SINA-Lösungsportfolio stets breiter. Während zunächst die sichere Verbindung von Standorten und die vertrauenswürdige Datenübermittlung im Vordergrund stand, waren später vor allem Office-Anwendungen und ein sicherer Arbeitsplatz gefragt. Heute haben Kollaborationsdienste wie Telefon-, Video- und Webkonferenzen, aber auch grafikaufwendige Anwendungen einen nicht zu vernachlässigenden Stellenwert. Eine Arbeitswelt ohne ortsübergreifende Kommunikation und standortunabhängiges kreatives Zusammenwirken ist heute kaum mehr denkbar.

Hinzu kommt, dass der klassische Büroarbeitsplatz – auch in Folge der COVID-19-Pandemie –ernstzunehmende Konkurrenz durch das Homeoffice bekommen hat. Auch bei Behörden spielen die Themen Mobilität und Flexibilität am Arbeitsplatz eine immer größere Rolle. Um die neuen Formen des Zusammenarbeitens VS-konform zu realisieren, statten Behörden ihre Mitarbeiter deshalb zunehmend mit der SINA Workstation S (zugelassen für VS-NfD) aus. Als komfortable Kollaborationsarbeitsplätze ermöglichen die Clients eine effektive und sichere Zusammenarbeit zwischen Mitarbeitern, mit denen diese beispielsweise auch auf Dienstreisen und aus dem Homeoffice heraus auf interne Daten zugreifen oder digitale Kommunikationsanwendungen nutzen können.

5.1 SINA RAS: Wartung und Problembehebung auch im Homeoffice

Über die sichere technische Lösung hinaus bringt die Umstellung für IT-Administrationen neue Herausforderungen mit sich, da ein großer Teil der Belegschaft nur noch über das Internet mit dem Behördennetz verbunden ist. Besonders mühsam wird es, wenn die IT-Verantwortlichen keinen physischen Zugriff mehr auf die Infrastrukturkomponenten haben. Mit der SINA-Lösung Remote Admin Server (SINA RAS) steht eine komfortable Fernwartungs-Software zur Verfügung. Mit dieser kann sich der IT-Support einen Überblick über alle im Netzwerk angebundenen SINA Clients verschaffen, einschließlich einer ganzen Reihe von entscheidenden Parametern, und so beispielsweise Softwareaktualisierungen für die Clients bereitstellen.

Abbildung 2 | SINA RAS



Zukünftig wird zudem ein neuer RAS Wartungsmodus implementiert, der die Administration laufender virtualisierter Arbeitsplätze vereinfacht. Geplant ist darüber hinaus eine Optimierung der internen Schnittstellen zur SINA Workstation S, um die Bedienung noch aufgabenorientierter zu gestalten. Weiter sollen der SINA RAS mit dem SINA Management und anderen

Administrationswerkzeugen in einem SINA Management Center gebündelt werden.

5.2 Vom Videostream zur Web-Konferenz: Grafikleistung ist gefragt

Wenn eine Belegschaft ihre SINA Workstations S regelmäßig als flexible Kollaborationsarbeitsplätze nutzt, verändern sich unweigerlich auch die Anforderungen an die Grafikleistung, die beispielsweise für digitale Videokonferenzen benötigt wird. Die Corona-Pandemie hat diesen Trend weiter befeuert. In enger Zusammenarbeit mit der Cyberus Technology GmbH wurde die SINA Workstation S weiterentwickelt und unter anderem dafür gesorgt, dass die physische Grafikkarte der Clients nutzbar gemacht werden kann, die zuvor aus Sicherheitsgründen für die Gastsysteme virtualisiert wurde. Mittlerweile ist die Grafikbeschleunigung für alle unterstützten Hardware-Modelle verfügbar, ohne dass dabei die Sicherheitsanforderungen reduziert werden müssen. Die Beschleunigung wirkt sich nicht nur positiv auf die Qualität der Bewegtbild-Anwendungen aus, sondern auch auf das Gesamtsystem, weil dadurch die CPU entlastet wird.

Neben der optimierten Grafikleistung profitieren Nutzer der SINA Workstation S künftig ebenso von secunet Desktop, der einen offenen Arbeitsplatz virtualisiert. Mit ihm können auch kommerzielle Anwendungen wie Teams, Skype oder Zoom genutzt werden, ohne die VS-Daten zu gefährden. Denn durch die Virtualisierungstechnologie – mit vergleichsweise kleiner Trusted Code Base des Hypervisors – wird sichergestellt, dass die offene Echtzeitkommunikation getrennt von dem VS-Netz stattfindet. Zahlreiche Anwendungen und Browser-Anbindungen werden von secunet Desktop unterstützt – eine wichtige Voraussetzung für die anwenderfreundliche SINA Workstation S.

Als umfassender Kollaborationsarbeitsplatz verfügt die SINA Workstation S mit dem SINA Voice-over-IP-Client zudem über ein integriertes Softphone, welches mit einer entsprechenden Infrastruktur sichere Telefongespräche ermöglicht. Der Einsatz von Privatgeräten zum Beispiel im Home-Office wird dadurch vermieden. Damit geht die SINA Workstation mit ihrer zukunftsweisenden Client-Virtualisierung auf Basis modernster, Open Source-basierter Hypervisor-Technologie weit über eine in Windows integrierte Software-VPN-Lösung hinaus. Nur diese Architektur bietet neben dem Schutz der Daten auf dem Transportweg umfassende Möglichkeiten der Strukturierung von Sicherheitszonen und deren Separation. Mikrosegmentierung ist im Sinne einer resilienten Infrastruktur ein „must have“, welche die SINA Technologie mit einer durchgehenden Virtualisierung leicht umsetzen lässt. Bleiben Anwender bei ihrem Anruf innerhalb ihres VS-Netzes, sind sogar VS-NfD-konforme Anrufe möglich. Der Aufbau einer umfassenden IP-basierten Kommunikationsinfrastruktur ist für alle Organisationen unumgänglich, haben doch

die deutschen Netzbetreiber mittlerweile fast alle ISDN-Anschlüsse abgeschaltet und durch IP-Telefonie ersetzt.

5.3 Das Ende für ISDN, ein Anfang für SINA Communicator H

Die ISDN-Abschaltung ist für Behörden, die auf geheime Sprachkommunikation angewiesen sind, ein akutes Problem. Denn für diesen Zweck der geheimen Sprachkommunikation gab es bis vor kurzem nur ISDN-basierte Verschlüsselungssysteme. Um deren Lebensdauer zu verlängern, setzen manche Behörden auf ISDN-IP-Gateways. Da die beiden zugrundeliegenden Technologien ISDN und IP aber sehr unterschiedlich sind, kommt es immer wieder zu Kompatibilitätsproblemen, die sich nie ganz ausgleichen lassen.

Eine modernere und hochsichere Lösung steht aber bereits in den Startlöchern: Der SINA Communicator H, ein Endgerät für die Sprach- und Datenkommunikation mit 10 Zoll großem Touch-Display, ist für den Schreibtischeinsatz konzipiert. Zulassungsfähig bis zum Einstufungsgrad GEHEIM sowie vergleichbare internationale Level und kann sowohl innerhalb von Behördennetzen als auch direkt mit Internetzugang betrieben werden. Er nutzt bewährte Internetstandards für Voice-over-IP (VoIP) und unterstützt damit vorhandene Session Initiation Protocol (SIP)-fähige Vermittlungsinfrastrukturen. Auch Protokolle der NATO, wie etwa das Secure Communication Interoperability Protocol (SCIP)[3], werden umgesetzt und so eine abgesicherte Kommunikation mit internationalen Bündnispartnern ermöglicht. Weitere Entwicklungen wie zum Beispiel Textkommunikation, Videotelefonie und eine Thin-Client-Funktionalität sind vorgesehen. Der SINA Communicator H ist insofern ein SINA Client neuer Generation, der sich nahtlos in die Architektur und „Multi-Level" Nutzungsszenarien von SINA integriert. Er bringt zudem eine völlig neue Softwarearchitektur mit, die auf einem in der Programmiersprache SPARK geschriebenen Separation Kernel und einer „Komponentenbasierten Architektur" beruht. Diese Architektur wird in den nächsten Jahren auch Einzug in die SINA Workstation H finden. Sie wird durch neue Formen der Nachweise die Zulassungszeiten neuer Versionen deutlich verringern und zudem neue Nutzungsszenarien ermöglichen.

5.4 SecuStack – SINA goes Cloud

Mit dem Produkt SecuStack wurde in enger Kooperation mit dem Partner Cloud&Heat zudem eine Lösung entwickelt, die sich als mandantenfähiges Rechenzentrum perfekt in die SINA Lösungsarchitektur einbettet. SecuStack ist eine betriebsfertige OpenStack Installation, die mit Sicherheitsfunktionen aus dem secunet- / SINA-Portfolio erweitert wurde, um durchgängige Datenverschlüsselung zu gewährleisten. Sie besteht aus schlüsselfertiger Hardware, geprüfter Software und einem sicheren Cloud-Betriebssystem. Die Lösung ist unabhängig von Software-Unternehmen und beinhaltet die lückenlose Überprüfbarkeit der Cloud und die Kontrolle aller zum Einsatz kommenden Komponenten. Dabei bietet die hochsichere Cloud-Infrastruktur den Schutz von geschäftskritischen Anwendungen, sensiblen Daten und vertraulichen Informationen. Zudem gewährleistet SecuStack die Sicherstellung und den Betrieb von unterschiedlichen Cloud-Modellen die Private-, Public-, und Multi-Cloud Szenarien. Die Transparenz, Datenhoheit und Unabhängigkeit führen schließlich zur vollständigen digitalen Souveränität in der Cloud.

6 Ein Blick in die Zukunft

Über die Jahre hinweg hat sich SINA unter anderem in zahlreichen Bundes- und Landesbehörden bewährt und ist zur führenden IT-Sicherheitsarchitektur der Bundesrepublik Deutschland geworden. Damit das weiterhin so bleibt, sind zahlreiche Neuerungen und Weiterentwicklungen des SINA-Produktportfolios geplant. Neben einer generellen Performance-Steigerung der SINA Workstation S mithilfe einer optimierten Systemarchitektur wird zum Beispiel in naher Zukunft die Benutzeroberfläche der Clients noch anwenderfreundlicher gestaltet. Im Zuge dessen wird auch eine Zertifizierung der Barrierefreiheit nach der Barrierefreien-Informationstechnik-Verordnung (BITV)[4] angestrebt, deren Voraussetzung eine vollständige Tastatursteuerbarkeit ist.

Um die digitale und VS-konforme Zusammenarbeit von unterschiedlichen Organisationen zu vereinfachen, die dafür bislang noch auf ein großes zusammenhängendes Intranet angewiesen sind, sollen die SINA Clients außerdem um den integrierten Dienst SINA Collaboration erweitert werden. Mit dieser Neuerung wären Behörden und Unternehmen in der Lage, ohne zusätzliche Infrastruktur, nur über je einen SINA Client VS-konform miteinander zu kommunizieren. Als gänzlich neuer Baustein des SINA Management Centers ist das SINA Monitoring vorgesehen. Das bietet insbesondere bei komplexen Systemen mit vielen Teilnehmern einen großen Mehrwert, da aktuelle Zustandsinformationen automatisch überwacht und Fehler schneller aufgespürt und behoben werden können.

7 SINA: Eine Gesamtlösung für höchste Sicherheitsanforderungen

IT-Systeme werden immer größer und komplexer. Gleiches gilt für die Bedrohungslage. Die Antwort darauf können Einzellösungen nicht liefern, denn diese sind entweder gar nicht oder nur schlecht skalierbar, haben sicherheitstechnische Nachteile und verkomplizieren die meist ohnehin schon sehr komplexen IT-Infrastrukturen noch weiter.

Der simplere, strategische und vor allem sichere Weg ist ein anderer: Die gesetzlich vorgeschriebene Absicherung eingestufter Informationen lässt sich am besten in Form einer Gesamtlösung – einer ganzheitlich sicheren Infrastruktur – umsetzen. SINA hat sich seit vielen Jahren in Deutschland und zunehmend auch international bewährt. Dabei wird die Sicherheitsarchitektur ständig weiterentwickelt, auch um den alten Widerspruch zwischen Sicherheit und Benutzerfreundlichkeit immer weiter aufzulösen.

3 Für die Details siehe bspw. https://en.wikipedia.org/wiki/Secure_Communications_Interoperability_Protocol

4 Siehe dazu auch https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html