Redaktion: Helmut Reimer

Report

EDSA: Task Force zu Beschwerden gegen Nutzung von Google- und Facebook-Services

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber, einigte sich mit seinen Kolleginnen und Kollegen des Europäischen Datenschutzausschusses (EDSA) darauf, eine Task Force zu gründen. Sie soll die schnelle und europaweit einheitliche Bearbeitung der Beschwerden der Organisation „Non-of-your-business" (noyb) zur Nutzung von Google- und Facebook-Services durch europäische Anbieter gewährleisten.

Dazu sagte der BfDI am 03. September .2020: „Der EDSA sendet mit der Task Force ein starkes Signal. Die entscheidende Frage, ob diese Google- und Facebook-Services das europäische Datenschutzrecht einhalten, kann jetzt endlich europaweit einheitlich beantwortet werden."

Die Nicht-Regierungsorganisation noyb hatte nach Verkündung des Schrems II-Urteils 101 Beschwerden gegen die Nutzung von Google Analytics und Facebook Connect durch europäische Unternehmen eingereicht. Die Beschwerden sind an alle nationalen Aufsichtsbehörden, darunter auch fünf deutsche Landesdatenschutzaufsichtsbehörden, gerichtet. Inhaltlich betreffen die Beschwerden die Frage, ob Google und Facebook über die genannten Produkte weiter personenbezogene Daten in die USA übermitteln dürfen und damit die Nutzung zum Beispiel durch Websites europäischer Anbieter legal ist oder nicht.

Beide Konzerne stützen sich inzwischen auf die sogenannten Standardvertragsklauseln der Europäischen Union. Ob sie dafür die vom EuGH geforderten „zusätzlichen Maßnahmen" als Ergänzung der Standardvertragsklauseln ergriffen haben und ob diese Maßnahmen ausreichen, um das vom EuGH geforderte Schutzniveau in den USA zu gewährleisten, ist die inhaltliche Kernfrage der Beschwerdeverfahren. Als Konsequenz hat der EDSA auf gemeinsame Initiative von Deutschland und Frankreich eine zweite Task Force ins Leben gerufen. Diese soll insbesondere Kriterien für die Bewertung einer Datenübermittlung im Einzelfall, Kriterien für zusätzliche Maßnahmen und Verfahrensaspekte für
deren Umsetzung erarbeiten.

Außerdem verabschiedete der EDSA in seiner gestrigen Sitzung Leitlinien zu den in der Datenschutz-Grundverordnung zentralen Begriffen „Verantwortlicher" und „Auftragsverarbeiter" sowie Richtlinien bezüglich der Zielgruppenansprache von Social-Media-Nutzern. Der EDSA wird beide Dokumente auf seiner Internetseite *www.edpb.europa.eu* veröffentlichen.

SecuStack: Lösung für neuartige sichere Cloud-Anwendungen

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

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

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

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

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

Neben der Infrastruktur-Absicherung unterstützt SecuStack künftig auch Confidential Cloud Native Applications. Anwendungsdienste laufen damit beispielsweise innerhalb von Intel SGX-Enklaven eines Kubernetes-Clusters. Eines der Ziele dabei ist es, maschinelles Lernen mit vertraulichen Daten zu ermöglichen. So können Anwender etwa ihre TensorFlow und PyTorch Modelle in einem sicheren Kontext trainieren. Dabei bleiben selbst die Trainingsdaten, der Code und die Modelle geschützt, die Cloud-Provider haben kei-

nen Zugriff. Auf diese Weise lassen sich neuartige Anwendungen umsetzen. Ein Beispiel: Krankenhäuser, die eine sichere Cloud-Infrastruktur mit SecuStack nutzen, können mit der SCONE Plattform lokales maschinelles Lernen mit vertraulichen Daten umsetzen. Die ML-Modelle bleiben lokal und können dennoch mit Modellen anderer Krankenhäuser kombiniert werden (Confidential Federated Machine Learning). So können ML-Modelle krankenhausübergreifend trainiert werden, ohne dass Patientendaten das Krankenhaus, zu dem sie gehören, verlassen müssen. Der Datenschutz bleibt jederzeit gewährleistet.

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

Projekt DEMIS: Sichere Datenübertragung zwischen Laboren und Gesundheitsämtern

Die Corona-Pandemie hat verdeutlicht, wie wichtig ein schnelles, zuverlässiges Meldesystem für Infektionskrankheiten ist. D-TRUST, der qualifizierte Vertrauensdiensteanbieter der Bundesdruckerei, leistet einen Beitrag für die sichere Übertragung von Gesundheitsdaten: Im Projekt „Deutsches Elektronisches Melde- und Informationssystem für den Infektionsschutz" (DEMIS) stellt D-TRUST die digitalen Zertifikate bereit.

DEMIS ist das elektronische Melde- und Informationssystem für Infektionskrankheiten in Deutschland. Das Projekt ist im Sommer gestartet und wird im Auftrag des Bundesministeriums für Gesundheit (BMG) vom Robert Koch-Institut (RKI) gemäß dem Infektionsschutzgesetz (IfSG) umgesetzt. Ziel ist eine durchgängig elektronische Informationsverarbeitung: Labore übermitteln ihre Daten an die Gesundheitsämter und Landesbehörden. Neben diesen kann auch das RKI die Daten pseudonymisiert abrufen. Erste meldepflichtige Labore wurden bereits an das System DEMIS angebunden und melden nun sicher, digital und schnell an die Gesundheitsämter die positiven Testergebnisse. Dem RKI liegen damit die Zahlen positiv getesteter COVID-19-Fälle mehrere Tage früher als bislang vor. Anfangs dauerte die Übertragung bis zu zehn Tage, da die Datenweitergabe in der Regel per Fax erfolgte.

„DEMIS leistet einen wichtigen Beitrag, um das Meldeverfahren von Infektionskrankheiten wie COVID-19 zu vereinfachen und zu beschleunigen – wir sorgen dabei für die Sicherheit bei der Datenübertragung. Sämtliche Gesundheitsämter und Labore beziehen zukünftig über das RKI unsere Zertifikate", sagt Dr. Kim Nguyen, Geschäftsführer von D-TRUST GmbH.

Die Anbindung der Labore an DEMIS erfordert ein digitales Zertifikat, damit authentisiert sich beispielsweise das Labor gegenüber dem System, und die Daten werden verschlüsselt übertragen. Mit der Zertifikatsprüfung wird auch die Identität der übermittelnden Organisation sichergestellt. Das RKI verwaltet die Zertifikate für alle anzubindenden Stellen. Die Labore beantragen die benötigten Zertifikate direkt beim RKI.

Insgesamt werden schrittweise die rund 170 Labore, 400 Gesundheitsämter und das Robert Koch-Institut über das neue Meldesystem miteinander verbunden.

Mehr Informationen zu den Produkten von D-TRUST finden Sie hier: *https://www.bundesdruckerei.de/de/Loesungen/Vertrauensdienste*

Fälschung ausgeschlossen

FOM Hochschule für Ökonomie & Management und TrustCerts etablieren einen Blockchain basierten Vertrauensdienst zur Absicherung von Zeugnissen.

Seit dem 21. August 2020 kann jedes neu ausgestellte Hochschulzeugnis der FOM in digitaler Form auf seine Echtheit überprüft werden.

Die Fälschung von Hochschulzeugnissen ist im digitalen Zeitalter einfacher denn je. Experten gehen davon aus, dass heutzutage in Deutschland bereits jedes zehnte Hochschulzeugnis manipuliert oder sogar komplett gefälscht wurde. In anderen europäischen Ländern wird dieser Anteil sogar noch größer geschätzt. Dabei können die Folgen von gefälschten Zeugnissen gravierend sein. So werden bspw. Mitarbeiter anhand von gefälschten Unterlagen und Urkunden eingestellt, was in vielen Berufsfeldern und Berufszweigen zu schwerwiegenden Konsequenzen führen kann – nicht nur in der Medizin.

Gefälschte oder manipulierte Hochschulzeugnisse stellen allerdings auch für die jeweilige Hochschule einen Vertrauensverlust dar. Keine Hochschule möchte ihren Namen bei Personalabteilungen oder Führungskräften mit gefälschten Zeugnissen in Verbindung gebracht sehen.

Aus dieser Motivation heraus und um der fortschreitenden technischen Entwicklung gerecht zu werden, haben die FOM Hochschule, mit 55.000 Studierenden die größte private Hochschule in Deutschland, und das junge Cyber-Security Unternehmen TrustCerts aus Gelsenkirchen gemeinsam eine Lösung für den Schutz von Zeugnissen gegen ebendiese Fälschung erarbeitet. Mit ihrem innovativen Ansatz können Hochschulen ihre Zeugnisse unkompliziert und kostengünstig gegen Fälschungen absichern. Die entsprechenden Anspruchsgruppen, wie Personalabteilungen und Geschäftsleitung, können barrierefrei in wenigen Sekunden die Echtheit eines Zeugnisses überprüfen.

Möglich macht dies die Blockchain, die als manipulationssicherer Speicher agiert. In ihr werden die digitale Prüfsumme des Nachweises sowie die Signatur der FOM hinterlegt und auf mehreren Servern deutschlandweit gespeichert. Der Absolvent entscheidet über die Weitergabe seines Nachweises vollkommen souverän und somit darüber, wer Einsicht in seine Daten bekommt. Ein Empfänger des digitalen Zeugnisses kann den Nachweis dabei über ein Online-Portal per Drag-and-Drop prüfen lassen, wobei das Dokument auf dem Endgerät des Prüfers verbleibt und keine personenbezogenen Daten über das Internet versendet werden. Mit Hilfe dieses Verfahrens kann eindeutig und unveränderlich festgestellt werden, ob es sich bei dem Zeugnis um ein Original handelt, wer es ausgestellt hat, zu welchem Zeitpunkt es erstellt wurde und ob es weiterhin Gültigkeit besitzt. Selbst für den Anbieter der Technologie selber, die TrustCerts GmbH, ist es unmöglich Daten im Namen der FOM zu signieren, da alle Vorgänge über die Blockchain protokolliert werden. Dabei funktioniert der Manipulationsschutz unabhängig vom Dateiformat für alle digitalen Originale und kann somit auch zur Absicherung weiterer Dokumente im Hochschulkontext, wie z.B. Studien- und Semesterbescheinigungen, verwendet werden.

Von der Technologie zeigt sich Markus Felten, Vizekanzler der FOM Hochschule begeistert: „Wir setzen die neue Technologie bereits an allen unseren 32 Hochschulzentren der FOM in Deutschland ein. Bereits in kurzer Zeit konnten wir so über 10.000 Zeug-

nisse absichern und für Personalverantwortliche überprüfbar machen."

Für TrustCerts ist die Umsetzung der Technologie ein weiterer Schritt, die Blockchain-Technologie unabhängig von Bitcoin zu etablieren so Mirko Mollik, Gründer von TrustCerts: "Wir sind froh, dass wir beweisen konnten, dass die Blockchain-Technologie spannende Anwendungsfelder weit außerhalb des Bitcoin-Hypes besitzt. Wir sind stolz darauf, die FOM als Partner für das Projekt gewonnen zu haben. Mit der Technologie von TrustCerts kann nicht nur die Hochschullandschaft in Deutschland ein Stückweit sicherer gemacht werden, sie ist auch ein weiterer wesentlicher Schritt, den stattfindenden digitalen Wandel, aktiv und sicher zu gestalten."

Von den Funktionen der TrustCerts-Lösung und ihren Vorteilen konnte sich auch bereits der Minister für Wirtschaft, Innovation, Digitalisierung und Energie in NRW, Prof. Dr. Andreas Pinkwart überzeugen: „Mit der Idee eines digitalen Notars zeigt das Start-up beispielhaft, welches Potenzial in den jungen Gründerinnen und Gründern in Gelsenkirchen steckt. Auch wenn ihre Vorhaben noch in den Startlöchern stehen, wollen wir ihnen die nötige Unterstützung geben und sie ermutigen, dran zu bleiben."

Weitere Informationen zum Projekt und TrustCerts finden Sie unter: *https://www.fom.de und https://www.trustcerts.de*

F-Secure: Globale Angriffskampagne auf die Kryptowährungsbranche

Die Cybersecurity-Spezialisten von F-Secure haben am 25. August 2020 einen Report veröffentlicht, in dem sie Details eines gezielten Angriffs auf ein Unternehmen aus der Kryptowährungsbranche mit der Lazarus Group in Verbindung bringen. Die Hackergruppe, die mutmaßlich in enger Verbindung zur Demokratischen Volksrepublik Korea (DVRK) steht, ist bekannt für ihr hochprofessionelles Vorgehen, das rein finanzielle Interessen verfolgt. Im Bericht kommt F-Secure durch die Verknüpfung von aus dem Angriff gewonnenen Hinweisen und Mustern mit bereits vorhandenen Forschungsergebnissen zu dem Schluss, dass der überprüfte Vorfall Teil einer global angelegten Kampagne der Lazarus-Gruppe ist. Diese richtet sich gegen Unternehmen aus der Kryptowährungsbranche aus den Vereinigten Staaten, Großbritannien, den Niederlanden, Deutschland, Singapur, Japan und weiteren Ländern.

Der Bericht analysiert die Logs, Protokolle und weitere technische Artefakte, die von F-Secure während der forensischen Untersuchung eines Angriffes auf eine Krypto-Organisation sichergestellt werden konnten. F-Secures Sicherheitsexperten stellten dabei fest, dass die Angriffsmethoden nahezu identisch mit den Praktiken sind, die so zuvor auch von der Lazarus-Gruppe – auch als APT38 bekannt – eingesetzt wurden.

Darüber hinaus beinhaltet der Bericht Details zu Taktiken, Techniken und Verfahren (TTP), die während des Angriffs zum Einsatz kamen. So konnten von den Angreifern beispielsweise per „Spearphishing" vertrauenswürdige externe Dienste instrumentalisiert werden. In diesem konkreten Fall wurde ein gefälschtes und speziell auf das Profil des Empfängers zugeschnittenes Stellenangebot über die Plattform LinkedIn versendet.

Auf der Grundlage von Phishing-Artefakten, die nach dem Angriff der Lazarus Group sichergestellt wurden, konnten die Forscher von F-Secure den Vorfall mit einer umfangreichen, bereits seit Januar 2018 laufenden Kampagne in Verbindung bringen. Dem Bericht zufolge wurden ähnliche Artefakte bei Angriffen in mindestens 14 Ländern festgestellt: in den Vereinigten Staaten, China, Großbritannien, Kanada, Deutschland, Russland, Südkorea, Argentinien, Singapur, Hongkong, den Niederlanden, Estland, Japan und den Philippinen.

Um die Abwehr des betroffenen Unternehmens während des Angriffs zu umgehen, hat die Lazarus-Gruppe einen erheblichen Aufwand betrieben. So konnte sie beispielsweise Antiviren-Software auf den kompromittierten Hosts deaktivieren und hinterlassene Beweise für ihre Aktivitäten entfernen. Und obwohl der Bericht den Angriff als hochprofessionell charakterisiert, weist er doch darauf hin, dass die Bemühungen der Lazarus Group, ihre Spuren im Nachhinein zu verwischen, nicht ausreichend waren. Zahlreiche versteckte und nicht beseitigte Indizien ergaben für F-Secure schlussendlich eindeutige Beweise für die Aktivitäten der Angreifer.

„Die Untersuchung des Angriffs erfolgte durch erfahrene Spezialisten unserer Incident Response, Managed Detection & Response und Tactical Defense Teams. Dabei stellte sich heraus, dass dieser Angriff eine Reihe von Ähnlichkeiten mit bekannten Aktivitäten der Lazarus-Gruppe aufwies. Wir sind davon überzeugt, dass sie auch für diesen Angriff verantwortlich waren", so Matt Lawrence, Director of Detection and Response bei F-Secure. Unternehmen können sich den Bericht nun zur Hand nehmen, um sich mit der konkreten Cyberattacke, den TTPs und der Lazarus-Gruppe im Allgemeinen vertraut zu machen. Darüber hinaus werden direkte Sicherheitsempfehlungen gegeben, um sich vor Angriffen der Hackergruppe zu schützen.

Der vollständige Bericht ist bei F-Secure Labs verfügbar: *https://labs.f-secure.com/publications/ti-report-lazarus-group-cryptocurrency-vertical/*

Kontaktdaten-Erfassung: Risiken auch bei Apps und Webservern

Die Corona-Bekämpfungsverordnung Schleswig-Holstein verpflichtet u. a. Gastronomen und Veranstalter zur Erfassung von Kontaktdaten ihrer Gäste. Diese Daten dürfen aber nicht in falsche Hände gelangen. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat am 28. August 2020 erneut auf Probleme hingewiesen: Sammlungen per Liste, herumfliegende Zettel, in Einzelfällen sogar Missbrauch der Daten. Geht es mit technischen Lösungen besser?

Für Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, ist dies nicht selbstverständlich: „Bei den Kontaktformularen sehen die Gäste, wie damit umgegangen wird. Gastronomen und Veranstalter können aktiv dafür sorgen, dass die Papierdaten so gelagert werden, dass sie für Unbefugte nicht zugänglich sind. Beim täglichen Schreddern nach der Aufbewahrungsfrist von vier Wochen bleiben nur noch kleine Schnipsel über – die Daten sind dann weg. Bei technischen Angeboten muss man sich dagegen in der Regel auf Dienstleister verlassen. Leider sind schon mehrfach Datenlecks der Kontaktdaten-Server solcher Angebote vorgekommen. Das betrifft dann nicht nur ein einzelnes Restaurant, sondern oft sind in solchen Fällen sämtliche gespeicherte Daten abrufbar. Aus diesen Daten geht hervor, wer wann wo gegessen hat – und wer zur selben Zeit ebenfalls vor Ort war."

Nach Hansens Überzeugung sollten nicht nur Berufsgruppen wie Anwälte oder Journalisten darauf achten, dass ihre Gesprächspartnerinnen und -partner nicht in Corona-Kontaktdatenbanken landen, bei denen es zu unerwünschten Abrufen kommen kann. „Im Prinzip betrifft es uns alle: Es geht keinen etwas an, wo und wann wir essen gehen oder an Veranstaltungen teilnehmen. Deswegen ist die sichere Verwahrung der Daten so wichtig, die eben nur während der Pandemie und nur für den Zweck der Kontaktnachverfolgung im Infektionsfall erfasst werden dürfen. Für Datenschutz und Datensicherheit von IT-Angeboten muss der Betreiber ständig am Ball bleiben: Pfusch geht nicht, Sorgfalt und Qualität sind stets mit Kosten verbunden." Die Landesbeauftragte für Datenschutz hat zwar Verständnis dafür, wenn man zur Vereinfachung technische Angebote wählen möchte, doch sie gibt zu bedenken: „Nicht jede Person hat ein Smartphone und kann ihre Daten per App oder Webbrowser melden. Das bedeutet für die Gastronomen und Veranstalter, dass ohnehin auch noch eine Lösung ohne Informationstechnik bereitgehalten werden muss."

Offen ist Hansen für die Entwicklung datenschutzfreundlicher Technik, die deutlich datensparsamer Kontaktdaten erheben könnte – zum Beispiel mit pseudonymen digitalen Erreichbarkeitsadressen, die jeweils nur einmal verwendet werden und nicht den Namen und die Postadresse enthalten. „Das würde einige Datensicherheitsprobleme lösen. Doch es ist noch Zukunftsmusik und in dieser Form bisher nicht in den aktuellen Corona-Verordnungen zugelassen." Heutzutage benötigen die Gesundheitsämter für ihre Aufgabe der Kontaktnachverfolgung den Namen und die Adresse.

Das ULD gibt auf seiner Webseite Hinweise zur Kontaktdatenerfassung auf Papier und in elektronischer Form: *https://www.datenschutzzentrum.de/artikel/1336-.html*

Die Informationen der Landesbeauftragten für Datenschutz zu Themen der Corona-Pandemie werden unter dem folgenden Link bereitgestellt und regelmäßig aktualisiert: *https://www.datenschutzzentrum.de/corona/*

"SSI für Deutschland" Konsortium startet dezentrales Identitäts-Netzwerk

Das "SSI für Deutschland"-Konsortium hat am Freitag, 21. August 2020, den Betrieb eines dezentralen Netzwerks für digitale Identitäten begonnen. Das Netzwerk wird zunächst als Testnetzwerk von acht unterschiedlichen Knoten betrieben und schon innerhalb des nächsten Monats auf fünfzehn dezentrale Knoten ausgebaut. Zukünftig soll das dezentrale Identitäts-Netzwerk von einer Europäischen Genossenschaft unter dem Namen "IDunion" verwaltet werden, die Partnern in ganz Europa offen steht.

Das "SSI für Deutschland"-Konsortium ist ein Zusammenschluss öffentlicher und privater Institutionen, die sich zum Ziel gesetzt haben, ein offenes Ökosystem für die Identitätsverwaltung in Europa aufzubauen. Die Lösung des Konsortiums baut auf offenen Standards und Open-Source-Technologie für Self-Sovereign Identity (SSI) auf und zeichnet sich besonders durch Datensparsamkeit und -transparenz aus. Nutzer*innen erhalten mit der Lösung die Möglichkeit, ihre Identitätsinformationen selbst zu verwalten und zu entscheiden, wann und mit wem sie diese teilen möchten. Das Konsortium wird durch das Bundesministerium für Wirtschaft und Energie (BMWi) im Rahmen der Wettbewerbsphase des Projekts "Schaufenster Sichere digitale Identitäten" gefördert. Das Konsortium wird aktuell von der Main Incubator GmbH geleitet.

"Wir sind stolz darauf, bei diesem Vorzeigeprojekt mit so großartigen Partnern unsere technische Expertise und langjährige SSI-Erfahrung breitbandig einbringen zu können", so der CIO der esatus AG, Dr. André Kudra. „Das ganze Self-Sovereign Identity Team der esatus AG unterstützt ‚SSI für Deutschland' mit größtem Engagement. Mein besonderer Dank gilt unserem Blockchain Lead Developer, Christopher Hempel, der die Launch Ceremony professionell geleitet hat."

Kudra und die esatus AG wollen weiter durchstarten: „Wir freuen uns auf die gemeinsamen nächsten Schritte mit den Konsortialpartnern. Wir werden ihnen jetzt sehr schnell unsere Enterprise Identity & Access Management Lösung im Testnetzwerk bereitstellen."

Im Konsortium arbeiten Bundesdruckerei GmbH, esatus AG, Main Incubator GmbH (Konsortialführer), Robert Bosch GmbH und Technische Universität Berlin.

Als assoziierte Partner beteiligen sich Bank-Verlag GmbH, Commerzbank AG, Creditreform Boniversum GmbH, Deutsche Bahn AG, GS1 Germany GmbH, Festo SE & Co. KG, ING Deutschland (ING-DiBa AG), Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, regio iT GmbH, Siemens AG, Stadt Köln, Telekom Innovation Laboratories (Deutsche Telekom AG), Verband der Vereine Creditreform e.V.

SSL: Von der defensiven zur offensiven Waffe

Die massenhafte Einführung bestimmter Technologien wird immer von Bemühungen begleitet, ihre breite Anwendung durch eine Reihe von Sicherheitslücken auszunutzen. Die Verschlüsselungstechnologie SSL bildet keine Ausnahme von dieser Regel und hat eine große Anzahl publizierter Schwachstellen gezeigt, die die Benutzer zwingen, auf neue, sicherere Versionen und letztendlich auf ein Ersatzprotokoll wie Transport Layer Security (TLS) umzusteigen.

Die Ausnutzung neu identifizierter Schwachstellen ist jedoch nicht die einzige Art und Weise, in der SSL als Waffe in den Händen böswilliger Angreifer genutzt wird. Nach Erkenntnissen von Radware (mitgeteilt am 09. September 2020) wird SSL immer häufiger eingesetzt, um die Erkennung des Angriffsverkehrs sowohl bei Bedrohungen auf Netzwerk- als auch auf Anwendungsebene zu verschleiern und weiter zu erschweren.

Viele Formen von SSL-Angriffen

SSL-Angriffe sind bei Angreifern beliebt, da nur eine kleine Anzahl von Paketen erforderlich ist, um einen Denial-of-Service für einen ziemlich großen Dienst zu verursachen. Angreifer starten Angriffe, die SSL verwenden, weil jeder SSL-Sitzungs-Handshake 15 Mal mehr Ressourcen auf dem Server als auf dem Client verbraucht. Infolge dieses Verstärkungseffekts kann selbst ein kleiner Angriff zu lähmendem Schaden führen.

SSL-basierte Angriffe nehmen viele Formen an, unter anderem:

Verschlüsselte SYN Floods. Diese Angriffe ähneln in ihrer Art den normalen, nicht verschlüsselten SYN-Flood-Angriffen, indem sie die vorhandenen Ressourcen erschöpfen, um den SYN-ACK-Handshake zu vervollständigen. Der Unterschied besteht darin, dass diese Angriffe die Herausforderung noch komplizierter machen, in-

dem sie den Verkehr verschlüsseln und die Verwendung von SSL-Handshake-Ressourcen erzwingen.

SSL-Neuverhandlung. Solche Attacken initiieren einen regulären SSL-Handshake und verlangen sofort die Neuverhandlung des Schlüssels. Das Tool wiederholt diese Neuverhandlungsanforderung ständig, bis alle Server-Ressourcen erschöpft sind.

HTTPS Floods. Erzeugen Floods von verschlüsseltem HTTP-Verkehr, oft als Teil von Multi-Vektor-Angriffskampagnen. Zu den Auswirkungen „normaler" HTTP Floods kommen bei verschlüsselten HTTP-Angriffen noch einige andere Herausforderungen hinzu, wie z. B. die Belastung durch Ver- und Entschlüsselungsmechanismen.

Verschlüsselte Angriffe auf Webanwendungen. Kampagnen für Multi-Vektor-Angriffe nutzen zunehmend auch Angriffe auf Webanwendungslogiken, die nicht auf DoS basieren. Durch die Verschlüsselung des Datenverkehrs passieren diese Angriffe oft unbemerkt von Abwehrmaßnahmen gegen DDoS und Schutzmechanismen für Webanwendungen.

Erschwerte Erkennung und Eindämmung

Auf die gleiche Weise, wie SSL und Verschlüsselung die Integrität legitimer Kommunikation schützen, verschleiern sie auch viele Attribute des Datenverkehrs, mit denen festgestellt wird, ob es sich um böswilligen oder legitimen Datenverkehr handelt. „Das Identifizieren bösartigen Traffics innerhalb verschlüsselter Verkehrsströme gleicht dem Auffinden einer Nadel im Heuhaufen im Dunkeln", so Michael Tullius, Managing Director DACH von Radware. „Die meisten Sicherheitslösungen haben Mühe, potenziell böswilligen Verkehr aus verschlüsselten Verkehrsquellen zu identifizieren und für weitere Analysen und eine potenzielle Schadensbegrenzung zu isolieren."

Viele Lösungen, die ein gewisses Maß an Entschlüsselung leisten können, tendieren dazu, sich auf eine Begrenzung der Anforderungsrate zu verlassen, was dazu führt, dass der Angriff effektiv beendet wird. Allerdings wird dabei auch legitimer Datenverkehr blockiert. Schließlich erfordern viele Lösungen, dass der Kunde Serverzertifikate teilen muss, was die Implementierung und Zertifikatsverwaltung erschwert.

Schutz vor SSL-Angriffen

Die bedauerliche Realität ist, dass die Mehrheit der DDoS-Angriffsschutzlösungen nur Schutz für bestimmte Arten von Angriffen bietet und in vielen Fällen mit SSL-Angriffen zu kämpfen hat. Um einen wirksamen Schutz zu bieten, müssen die Lösungen unter dem Strich eine vollständige Abdeckung der Angriffsvektoren (einschließlich SSL) und eine hohe Skalierbarkeit bieten, um den wachsenden Anforderungen gerecht zu werden und wirksamen Schutz zu bieten. Insbesondere muss die Abwehr gegen SSL-Attacken alle gängigen Versionen von SSL und TLS unterstützen und einen asymmetrischen Einsatz ermöglichen, bei dem nur der eingehende verschlüsselte Datenverkehr die Mitigations-Engine durchläuft. Zudem sollte sie verdächtigen verschlüsselten Datenverkehr mithilfe einer Verhaltensanalyse isolieren, um die Auswirkungen auf legitime Benutzer zu begrenzen. Schließlich sollte eine solche Lösung erweiterte Challenge-/Response-Mechanismen zur Validierung von verschlüsseltem Datenverkehr bieten, der als verdächtig gekennzeichnet ist, sich aber nur auf die erste Benutzersitzung auswirkt.

Weitere Informationen finden Sie unter *www.radware.com*

Proofpoint: MFA – neue Sicherheitslücken

Proofpoint, Inc. (*https://www.proofpoint.com/de*), eines der führenden Next-Generation Cybersecurity- und Compliance-Unternehmen, hat am 15. September 2020 über mehrere kritische Sicherheitslücken bei der Implementierung von Multi-Faktor-Authentifizierung (MFA) informiert. Diese betreffen Cloud-Umgebungen, bei denen zur Authentifizierung das Protokoll WS-Trust verwendet wird. Mittels dieser Schwachstellen ist es Angreifern möglich, MFA zu umgehen und auf Cloud-Anwendungen zuzugreifen, die das betreffende Protokoll verwenden. Unter Umständen betrifft dies auch Microsoft 365. Im Falle eines erfolgreichen Angriffs könnte ein Hacker vollen Zugang zum Konto des Opfers erhalten (einschließlich E-Mails, Dateien, Kontakten, sensiblen Daten etc.). Darüber hinaus bieten auch andere von Microsoft bereitgestellte Cloud-Dienste, darunter Produktions- und Entwicklungsumgebungen wie Azure und Visual Studio, ein lukratives Einfallstor.

Die Multi-Faktor-Authentifizierung (MFA) – beispielsweise als SMS zur Bestätigung einer Anmeldung in einem Online-Dienst oder die TAN beim Online-Banking – hat sich seit einiger Zeit zu einem unverzichtbaren Sicherheitselement für Cloud-Anwendungen entwickelt. Und gerade im Zuge der aktuellen Pandemie stieg die Nachfrage nach Cloud-basierten Anwendungen wie Messaging- und Kollaborationsplattformen sprunghaft an, da unzählige Mitarbeiter nunmehr ihre Arbeit von zu Hause aus verrichten mussten. Mit dieser Entwicklung ging zudem einher, dass vermehrt von privaten und folglich nicht verwalteten Geräten auf Unternehmensanwendungen zugegriffen wurde. Obendrein kam es gerade in der Hochphase der Pandemie vermehrt zu Cyberattacken, die die Sorgen vieler Angestellter auszunutzen versuchten, um Zugangsdaten zu erbeuten. Dadurch stieg in der Folge auch das Risiko, dass sich unbefugte des Zugriffs auf Cloud-Anwendungen von Unternehmen bemächtigen könnten. Die Anwendung von MFA sollte daher dazu beitragen, die Angriffsfläche des Unternehmens zu reduzieren, indem eine zusätzliche Schutzebene die Sicherheit erhöht.

Wie Angreifer MFA umgehen

Doch auch MFA ist kein Allheilmittel. So sind bereits seit längerem verschiedene Methoden bekannt, die es Angreifern ermöglichen, Multi-Faktor-Authentifizierungsmethoden zu umgehen. Dazu zählen Echtzeit-Phishing, Channel Hijacking und die Verwendung von Legacy-Protokollen:

Phishing in Echtzeit

Im Gegensatz zum klassischen Phishing geht es beim Echtzeit-Phishing darum, die Daten beider Anmeldungen, also das Passwort wie auch den zweiten Faktor der MFA zu stehlen. Hierzu bedienen sich Cyberkriminelle zuweilen eines Proxys, der zwischen der eigentlichen Website der Cloud-Anwendung und dem Opfer geschalten wird. Die auf dem Proxy befindliche Website sieht dabei der ursprünglichen zum Verwechseln ähnlich. Mittels dieser betrügerischen Website manipuliert der Angreifer das Opfer so, dass es den Authentifizierungscode der MFA im Anschluss an seine Anmeldedaten aushändigt. Solche Angriffe können mit Werkzeugen wie Modlishka automatisiert werden. Allerdings müssen die Angreifer ihre Tools häufig aktualisieren, um nicht entlarvt zu werden und sie benötigen eine komplexe Infrastruktur.

Eine weitere Echtzeit-Phishing-Methode, die Angreifer verwenden, ist die „Challenge Reflection", bei der die Benutzer aufgefordert werden, MFA-Zugangsdaten auf einer Phishing-Site auszufüllen. Die Zugangsdaten werden dann unmittelbar danach mit den Hackern ge-

teilt. Die erfolgreiche Umsetzung dieser Methode erfordert jedoch eine manuelle Echtzeit-Aktion der Cyberkriminellen im Hintergrund.

Channel Hijacking

Beim Channel Hijacking wird das Telefon oder der Computer des Opfers in der Regel mit Malware angegriffen. Die entsprechende Malware kann sodann eine sogenannte Man-in-the-Browser-Technik oder Web-Injects nutzen, um die relevanten Daten zu erbeuten. Natürlich können Daten auch direkt vom Mobiltelefon gestohlen werden, beispielsweise über Textnachrichten oder durch hacken der Sprachbox der zugehörigen Telefonnummer.

Legacy-Protokolle

Eine einfachere und billigere Methode zur Umgehung von MFA stellt die Ausnutzung von Legacy Protokollen für Angriffe auf Cloud-Accounts dar. Viele Organisationen erlauben noch immer die Unterstützung dieser Protokolle für Legacy-Geräte oder -Anwendungen wie Kopierer oder gemeinsam genutzte Konten – z.B. für Konferenzräume.

Im Falle älterer E-Mail-Protokolle wie POP und IMAP wird MFA zum Teil nicht unterstützt. Das hat zur Folge, dass nicht zwingend ein zweiter Faktor zur Authentifizierung benötigt wird, um Zugriff auf einen Account zu erhalten. Diese Umgehungsmethode lässt sich leicht automatisieren und mittels Login-Daten nutzen, die aus früheren Angriffen stammen oder via Phishing erbeutet wurden.

Analysen von Proofpoint in Sachen Cloud-Bedrohungen haben gezeigt, dass in der ersten Jahreshälfte 2020 97 Prozent der untersuchten Organisationen von Brute-Force-Angriffen betroffen waren. 30 Prozent davon hatten zudem mindestens ein kompromittiertes Cloud-Konto zu beklagen. Bei der Untersuchung-E-Mail-basierter Cloud-Angriffe (Credential Phishing, Malware usw.) konnte das Unternehmen feststellen, dass 73 Prozent aller überwachten Systeme attackiert und 57 Prozent von ihnen kompromittiert wurden.

Wenn es um Cloud-Sicherheit geht ist MFA kein Garant für die Vermeidung erfolgreicher Cyberangriffe. Je mehr Organisationen die Technologie implementieren, desto mehr Anwender und Sicherheitslücken gibt es, die von Angreifern missbraucht werden können. MFA kann jedoch dazu beitragen, die generelle Situation in puncto IT-Sicherheit zu verbessern. Dies gilt besonders in Kombination mit auf den Menschen ausgerichteten Sicherheitstrainings und stetigen Zugangskontrollen.

Weitere Informationen zu den von Proofpoint entdeckten Sicherheitslücken sowie allgemeine Hintergrundinformationen zum Thema MFA, finden Sie im aktuellen Blog von Proofpoint.

G DATA Security Alert: Warnung vor aktiver Spam-Kampagne

Eine Mail, die angeblich vom Bundesgesundheitsministerium stammt, enthält einen Downloader für eine Schadsoftware. Der Dateianhang mit dem Namen „Bund-Arbeitsschutzregel-Corona-September.zip" enthält vorgeblich ein Dokument mit aktualisierten und ab sofort verbindlichen Regeln für den Infektionsschutz am Arbeitsplatz. Der Text der Mail lässt den Schluss zu, dass in erster Linie Unternehmen zur Zielgruppe gehören. Aus diesem Grund ist momentan für Unternehmen besondere Vorsicht geboten, wenn vermeintliche Mails von Behörden im Postfach landen. Uns sind Berichte über derzeit aktive Infektionen bekannt.

„Die Corona-Pandemie sorgt noch immer für viel Unsicherheit – und die Mischung aus viel Homeoffice und Hygieneregeln am Arbeitsplatz stellt Arbeitgeber tatsächlich vor große Herausforderungen", sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense. „Gerade deshalb sollten die Verantwortlichen aber sehr genau hinschauen und nur offiziellen Quellen vertrauen. Denn eine Infektion mit Schadsoftware können Unternehmen im Moment noch weniger gebrauchen, als ohnehin schon."

Der Text der Mail weist auf ein Treffen zwischen den Gesundheitsministern der EU hin, bei dem die aktualisierten Vorschriften überarbeitet worden seien. Dass es solch ein Treffen gegeben hat, mag vielleicht sogar stimmen – allerdings werden solche Informationen in der Regel nicht per Mail von den Ministerien versendet, sondern auf einem eigenen Portal veröffentlicht. Es findet kein proaktiver Versand per Mail statt.

Des Weiteren nimmt der Mailtext Bezug auf ein Treffen, welches „heute" stattgefunden habe. Es befinden sich auch einige Zeichenfehler in der Mail, vor allem den Buchstaben U, W, C und D sowie bei Umlauten. Die Mail enthält auch eine falsche Absendeadresse, die auf „bundesministerium-gesundheit.com" verweist – diese Domain gehört jedoch nicht zum Gesundheitsministerium. Die im Mailtext erwähnte Adresse „poststelle@bmg.bund.de" ist jedoch tatsächlich korrekt.

Um sich vor einer Schadsoftwareinfektion aus einer solchen Mail zu schützen, sollten Unternehmen und Privatpersonen alle Informationen rund um die COVID19-Pandemie und entsprechende Schutzmaßnahmen ausschließlich aus offiziellen Quellen beziehen. Alle aktuellen Informationen rund um Corona und COVID19 sind auf der Internetseite des Bundesministeriums für Gesundheit (BmG) gesammelt.

Weitere Details sowie Screenshots der Spam-Nachrichten finden Sie in einem aktuellen G DATA-Blog-Beitrag.

Website-Zertifikate: Browserhersteller schwächen Verbraucherschutz

Seit September 2020 gelten neue verkürzte Laufzeiten für TLS-Zertifikate, mit denen Webseiten abgesichert werden. Diese dürfen nun maximal 13 Monate (397 Tage) gültig sein. Die Browserhersteller versprechen sich davon mehr Sicherheit. Dr. Kim Nguyen, Geschäftsführer von D-TRUST, einem Unternehmen der Bundesdruckerei und Anbieter digitaler Zertifikate, ist jedoch skeptisch: „Kürzere Laufzeiten von Website-Zertifikaten können sogar zu mehr Unsicherheit im Netz führen: Eine reduzierte Gültigkeitsdauer für alle Zertifikatstypen verringert aufgrund des zusätzlichen Aufwands die Attraktivität von TLS-Zertifikaten mit Identitätsprüfung." Wie wichtig deren Beitrag für eine sichere Online-Kommunikation ist, zeigt der Betrug bei den Corona-Soforthilfe-Anträgen im Frühjahr dieses Jahres. Der Einsatz identitätsgeprüfter Zertifikate hätte mit hoher Wahrscheinlichkeit einen Missbrauch verhindert: Die Antragsteller hätten laut Nguyen über die Anzeige der Zertifikatsinformationen feststellen können, ob sie sich auf einer vertrauenswürdigen Behörden-Webseite befinden – oder einer Phishing-Seite von Betrügern. Zudem weist Nguyen auf die politische Dimension der Verkürzung hin: „Europa setzt bei der Internet-Sicherheit auf Zertifikate mit einer gründlichen Identitätsprüfung und hoher Rechtsverbindlichkeit – von der nun vorgegebenen Verkürzung profitieren jedoch vor allem Angebote mit niedrigem Sicherheitsniveau, für den Anwender sinkt der Verbraucherschutz."

Browserhersteller haben Verkürzung vorgegeben

Die Entscheidung für verkürzte Laufzeiten von TLS-Zertifikaten wurde vom CA/Browser-Forum im Juli 2020 getroffen. Das Forum ist eine Plattform für den Austausch zwischen Zertifikatsanwendern – also beispielsweise den großen Browserherstellern aus den USA – und den sogenannten Certificate Authorities (CA), die Zertifikate ausstellen. Anfangs von einem Browser-Hersteller forciert, ist das gesamte Forum auf starken Druck der anderen Browseranbieter auf diesen Kurs eingeschwenkt. „D-TRUST als europäischer CA ist von der Laufzeitverkürzung betroffen: Wir verstehen uns als Anbieter von Zertifikaten mit den höchsten Sicherheitsniveaus, also ausführlicher Identitätsprüfung – diese werden jetzt für Anwender unattraktiver", erläutert Nguyen.

D-TRUST konzentriert sich auf organisationsvalidierte und erweitert validierte Zertifikate mit Identitätsinformationen (OV-, EV- und QWAC-Zertifikate). Hierbei wird die Identität des Webseitenbetreibers gründlich geprüft. Das erfordert einen höheren Aufwand, der jetzt in immer kürzeren Abständen notwendig ist. Der Mehraufwand für Webseitenbetreiber bei Laufzeitverkürzungen lässt sich zwar durch automatisierte Prozesse vermeiden, doch kann dies in der Regel nur von Unternehmen mit spezialisierten IT-Abteilungen oder Dienstleistern umgesetzt werden. Es besteht daher die Gefahr, dass Anwender aufgrund des höheren Aufwands eher zu sogenannten domainvalidierten Zertifikaten (DV-Zertifikate) tendieren. Bei DV-Zertifikaten wird die Identität des Antragstellers im Antragsprozess nicht überprüft.

Studie widerspricht Argumentation der Browseranbieter

Bei der Internet-Sicherheit konzentrieren sich die Browserhersteller auf die technischen Aspekte. Im Mittelpunkt steht dabei der verschlüsselte Datentransfer zwischen Webseiten und dem Computer des Internet-Nutzers. Kürzere Laufzeiten verringerten laut Browserhersteller allgemein das Zeitfenster, in denen TLS-Zertifikate gefährdet sind oder missbraucht werden können. Langfristig erhoffen sich die Browser davon, dass sie gänzlich auf die Zertifikatvalidierung verzichten können, um die Geschwindigkeit der Browser zu beschleunigen. Dies erhöht jedoch nach Ansicht von Nguyen für Nutzer das Risiko, Opfer von Phishing-Attacken zu werden.

Unterstützt wird dieses Argument durch eine aktuelle Studie der RWTH Aachen University. Deren Ergebnisse verdeutlichen, dass für ein Optimum an Internet-Sicherheit nicht nur technische Maßnahmen notwendig sind, sondern auch ein Identitäts-Check bei Zertifikaten. Laut der Studie nutzten 49,4 Prozent der in 2018 entdeckten Phishing-Webseiten das HTTPS-Protokoll. HTTPS-Webseiten übertragen die Daten verschlüsselt und signalisieren dem User damit Sicherheit. Eine Verschlüsselung allein ist also kein Kennzeichen sicherer Webseiten. Dass kürzere Zertifikatslaufzeiten die Sicherheit verbessern, wird durch die Analyse ebenfalls nicht bestätigt. Im Gegenteil: Die Gültigkeitsdauer sicherer Webseiten ist mit durchschnittlich 412 Tagen länger als diejenige gefälschter Webseiten mit 252 Tagen. Auch bei der ausgewählten Methode der Identitätsprüfung gibt es ein eindeutiges Ergebnis: 84,6 Prozent der Phishing-Angriffe werden über Webseiten durchgeführt, die entweder ausschließlich DV-Zertifikate oder gar keine Zertifikate enthalten. Hingegen besaßen nur 0,4 Prozent der gefälschten Webseiten ein EV-Zertifikat mit umfangreicher Identitätsprüfung.

Mehr europäische Unabhängigkeit von den Browserherstellern

Die EU-Kommission hat deshalb bereits 2014 in der Verordnung über elektronische Identifizierung und Vertrauensdienste das qualifizierte Webseitenzertifikat (QWAC) definiert. Ziel ist es, in ganz Europa eine sichere und vertrauenswürdige elektronische Kommunikation zu etablieren.

Allerdings erkennen die Browserhersteller QWACs bislang nicht an: Diese besonders sicheren Website-Zertifikate werden weder verarbeitet, noch im Browser angezeigt. Jetzt kommen zusätzlich die kürzeren Laufzeiten hinzu, die den Trend hin zu Zertifikaten ohne Identitätsnachweis verstärken. „Das Vorgehen von Google und Co. beim Umgang mit Website-Zertifikaten zeigt, dass eine starke Abhängigkeit der digitalen Sicherheitsinfrastrukturen in Europa von den Browserherstellern besteht", so Nguyen.

Es gilt viel mehr, die digitale Souveränität Europas zu stärken. Browserhersteller müssen endlich die Verarbeitung und Anzeige der QWACs unterstützen. Wichtig wäre es zudem, den Sicherheitsstatus der QWACs verlässlich zu visualisieren, zum Beispiel durch das „EU Trust Mark Logo". Diese Lösungsvorschläge werden auch vom Digitalverband Bitkom geteilt, der jüngst ein umfangreiches Positionspapier[1] zum Thema veröffentlichte.

SINA Workflow vom BSI zur Nutzung für Verschlusssachen bis GEHEIM freigegeben

SINA Workflow, die Lösung von secunet für eine durchgehend digitale Bearbeitung von Verschlusssachen (VS), hat am 24. August 2020 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Freigabeempfehlung bis einschließlich GEHEIM erhalten (BSI-VSA-10158). Mit der Freigabeempfehlung ist SINA Workflow die aktuell einzige evaluierte und ganzheitliche Lösung für das digitale VS-Dokumentenmanagement inklusive VS-Registratur.

SINA Workflow ermöglicht Kunden, VS-Dokumente komplett digital zu erstellen, zu registrieren und zu verwalten sowie gemäß dem Prinzip „Kenntnis nur, wenn nötig" („need to know") in der eigenen Organisation sicher zu verteilen. Dabei stellt die Lösung sicher, dass für jede Verschlusssache im System belastbare Nachweise darüber enthalten sind, welche Verarbeitungs- und Verwaltungsschritte damit ausgeführt wurden. Die Nutzer werden vom Vorschriftenoverhead entlastet. Digitale Prozesse (Workflows) innerhalb der Lösung ermöglichen zudem die kollaborative Arbeit an Dokumenten sowie die zentrale Modellierung von wiederkehrenden Prozessen wie etwa Mitzeichnungen. Auch organisationsspezifische Abläufe lassen sich abbilden. Auf papiergebundene Schritte bei der VS-Bearbeitung können die Nutzer vollständig verzichten.

In der Verwaltung hat SINA Workflow das Potenzial, die gesamte digitale VS-Bearbeitung deutlich zu vereinfachen. Nationale und internationale Behörden können von der Lösung profitieren, da sie den Umgang mit eingestuften Informationen um ein Vielfaches beschleunigen kann.

Im Umfeld der Geheimhaltungsstufe GEHEIM setzt SINA Workflow auf die bewährte SINA Workstation H auf. Somit können Bestandskunden die Lösung mit den bereits vorhandenen SINA Krypto-Clients nutzen.

secunet strebt an, die allgemeine Zulassung für eine der nächsten Versionen kurzfristig zu erreichen. Durch die erteilte Freigabeempfehlung kann SINA Workflow jedoch bereits jetzt für Verschlusssachen bis GEHEIM eingesetzt werden.

Weitere Informationen finden Sie unter *www.secunet.com*

1 https://www.bitkom.org/European-Strategy-for-a-Sustainable-and-Smart-Mobility

Veranstaltungskalender

11 | 2020

Veranstaltungen November		
Zeit und Ort	**Thema der Veranstaltung**	**Veranstalter**
02.- 03. November 2020 in Nürnberg	IT-Sicherheit in der Entwicklung von Webapplikationen	OHM Professional School – Technische Hochschule Nürnberg Keßlerstraße 1, 90489 Nürnberg Tel.: 0911/5880-2808; Fax: 0911/5880_6800 E-Mail: ohm-professional-school@th-nuernberg.de
02. – 06. November 2020 in Berlin	CompTIA CySA+ Bundle: Kurs und Prüfungsvoucher	SMLan – Software & Management Training Kastanienallee 53, 10119 Berlin Tel.: 30/4492545; Fax: 030/44340435
02. – 04. November in Berlin	Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20 E-Mail: akademie@dgi-ag.de
05. – 06. November 2020 in Bochum	Cloud Security Sichere Cloud-Nutzung	isits International School of IT Security Huestr. 30, 44787 Bochum Tel.: 0234/927898-0; Fax: 0234/927898-20 E-Mail: info@is-its.org
05. – 07. November 2020 in Bochum	Cyber Awareness – Grundlagen	isits International School of IT Security Huestr. 30, 44787 Bochum Tel.: 0234/927898-0; Fax: 0234/927898-20 E-Mail: info@is-its.org
09. – 11. November 2020 in Berlin	Ausbildung zum Kryptographie Security Expert (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20 E-Mail: akademie@dgi-ag.de
09. – 12. November 2020 in Karlsruhe	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering	Secorvo Security Consulting GmbH Ettlinger Straße 12-14, 76137 Karlsruhe Tel.: 0721/255171-0; Fax: 0721/255171-100
09. – 12. November 2020 in Karlsruhe	PKI – Grundlagen, Vertiefung, Realisierung	Secorvo Security Consulting GmbH Ettlinger Straße 12-14, 76137 Karlsruhe Tel.: 0721/255171-0; Fax: 0721/255171-100
10. – 12. November 2020 in Hamburg	Hacking Extrem Web-Applikationen	cirosec GmbH Ferdinand-Braun-Str.4, 74074 Heilbronn Tel.: 07131/594550, Fax 07131/59455-99 E-Mail: info@cirosec.de
14. – 15. November 2020 in Berlin	Virtual Private Networks (VPN) Konzeption und Realisierung	SMLan – Software & Management Training Kastanienallee 53, 10119 Berlin Tel.: 30/4492545; Fax: 030/44340435
16. – 17. November 2020 in Nürnberg	Business Continuity & Security Implementierung eines Business Continuity Management Systems gem. DIN EN ISO 22301:2012	qSkills GmbH & Co. KG Süd-West-Park 65, 90449 Nürnberg Tel.: 0911/8010324; Fax: 091178010-339 E-Mail: info@qskills.de
19. – 20. November 2020 in Velden	IT-Grundschutz-Praktiker (Präsenz, Online, Selbst, Inhouse) (mit Personenzertifikat)	DresPleier GmbH Vils 8, 84149 Velden Tel.: 08742/5870894; Fax: 03222/4170655
23. – 27. November 2020 in Bochum	T.I.S.P.-Zertifikat – TeleTrusT Information Security Professional Expertenzertifikat	isits International School of IT Security Huestr. 30, 44787 Bochum Tel.: 0234/927898-0; Fax: 0234/927898-20 E-Mail: info@is-its.org
24. – 26. November 2020 in Ludwigsburg	Forensik Extrem – Incident Handling & IT-Forensik im Unternehmen	cirosec GmbH Ferdinand-Braun-Str.4, 74074 Heilbronn Tel.: 07131/59455-0, Fax: 07131/59455-99 E-Mail: info@cirosec.de
25. – 26. November 2020 in Regensburg	Lehrgang zum Informationssicherheitsbeauftragten (ISB)	Bayerisches IT-Sicherheitscluster e.V. Franz-Mayer-Str. 1 / 1. OG, 93053 Regensburg Tel.: 0941/604889-0; Fax +49-941-604889-35

DATENSCHUTZ UND DATENSICHERHEIT

DuD – Datenschutz und Datensicherheit
Recht und Sicherheit in Informationsverarbeitung und Kommunikation
Ausgabe 11/2020, 44. Jahrgang | www.dud.de

Verlag
Springer Gabler | Springer Fachmedien Wiesbaden GmbH | Abraham-Lincoln-Straße 46 | 65189 Wiesbaden
Amtsgericht Wiesbaden, HRB 9754 | USt-IdNr. DE811148419
www.springer-gabler.de

Bezugsmöglichkeiten
Jährlich erscheinen 12 Hefte.
Jahresabonnement 2020 EUR 318,78
Jahresabonnement 2020 (Firmen, Institutionen und Bibliotheken) EUR 484,-
Jahresabonnement 2020 (Studenten) EUR 98,- oder zum Vorzugspreis EUR 149,- gültig für persönliche Mitglieder der AwV (Arbeitsgemeinschaft für wirtschaftliche Verwaltung), des BvD (Berufsverband der Datenschutzbeauftragten Deutschlands e.V.), der DVD (Deutschen Vereinigung für Datenschutz e.V.), der DGRI (Deutsche Gesellschaft für Recht und Informatik), des FIfF (Forum Informatiker/Innen für Frieden und Gesellschaftliche Verantwortung e.V.), der GI (Gesellschaft für Informatik), für persönliche Mitglieder von TeleTrusT (Der IT-Sicherheitsverband Deutschlands). Der Vorzugspreis wird eingeräumt, wenn eine Bestätigung der Mitgliedschaft bzw. eine Studienbescheinigung vorgelegt wird.

Einzelheftpreis EUR 43,-

Alle Preise gelten zuzüglich Versandkosten. Alle Bezugspreise und Versandkosten unterliegen der Preisbindung.

Bezug durch den Buchhandel oder den Verlag. Abbestellungen müssen schriftlich spätestens 6 Wochen vor Ende des Bezugszeitraumes erfolgen. Im laufenden Jahrgang kann jeweils ein Sonderheft erscheinen, das nach Umfang berechnet und den Abonnenten im Erscheinungsjahr mit einem Nachlass von 25% des jeweiligen Ladenpreises geliefert wird. Bei Nichtgefallen kann das Sonderheft innerhalb einer Frist von 3 Wochen zurückgegeben werden.

Hinweise für Autoren
Bitte beachten Sie die ausführlichen Informationen unter www.dud.de. Manuskripte möglichst in maschinenlesbarer Form (Word-Datei) an den zuständigen Herausgeber (Report: Herr Reimer, Recht: Frau Mester oder Herr Buchner und Technik: Herr Fox) senden. Leserbriefe an die Herausgeber sind erwünscht, deren Publikation und eventuelle Kürzungen vorbehalten.

Geschäftsführer
Stefanie Burgmaier
Joachim Krieger
Juliane Ritt

Gesamtleitung Produktion
Ulrike Drechsler

Leiter Media Sales
Volker Hesedenz

Abonnentenverwaltung | Leserservice
Springer Customer Service Center GmbH
Haberstr. 7 | D-69126 Heidelberg
Telefon: (06221) 345-4303
Telefax: (06221) 345-4229
Montag bis Freitag, 8.00 Uhr bis 18.00 Uhr
E-Mail: springergabler-service@springer.com

Produktmanagement
Elke Janosch
Telefon: (030) 82 787-5367
Telefax: (030) 82 787-5365
E-Mail: elke.janosch@springer.com

Anzeigen
Anzeigenverkauf: Kerstin Feindler-Koch
Telefon: (0611) 7878-217
Telefax: (0611) 7878-78217
E-Mail: kerstin.feindler@springer.com

Anzeigendisposition: Petra Steffen-Munsberg
Telefon: (0611) 7878-164
Telefax: (0611) 7878-78164
E-Mail: petra.steffen-munsberg@springer.com

Es gilt die Anzeigenpreisliste vom 01.10.2018.

Produktion
Eva-Maria Krämer

Technische Redaktion
Oliver Reimer
Am Hohlstedter Weg 1a | 99441 Großschwabhausen
Telefon: (036454) 130040
Telefax: (036454) 130041
E-Mail: oliver.reimer@cmyk.one

Satz
Oliver Reimer | Großschwabhausen

Druck und Verarbeitung
Wilco | Amersfoort | Niederlande

Gedruckt auf säurefreiem und chlorarm gebleichtem Papier. | Printed in Germany

ISSN print 1614-0702

Dieser Ausgabe liegt eine Beilage vom Kunden Tüv Nord aus Hamburg und 2 Beilagen aus dem Verlag C.H. Beck aus München sowie 1 Beilage von WEKA Akademie aus Kissing, bei. Wir bitten unsere Leser und Leserinnen um Beachtung.