Redaktion: Helmut Reimer

Report

EDÖB: 28. Tätigkeitsbericht 2020/21

Pandemiebekämpfung – Bewährungsprobe für Datenschutz und Öffentlichkeitsprinzip, Mitteilung vom 29. Juni 2021
Das Berichtsjahr war geprägt von der Covid-19-Pandemie. Als Aufsichtsbehörde für Datenschutz überwachte der EDÖB eine hohe Anzahl von digitalen Projekten zu deren Bekämpfung. Als Schlichtungsstelle für Zugangsgesuche nach dem Öffentlichkeitsgesetz hat er vermittelnd darauf hingewirkt, das Bedürfnis der Bevölkerung nach Nachvollziehbarkeit der staatlichen Seuchenbekämpfung mit der für die Bundesverwaltung prioritären Durchführung dieser Aufgabe in Einklang zu bringen.

Covid-Bekämpfung mit digitalen Anwendungen
Die Aufsichtstätigkeit im Bereich Datenschutz konzentrierte sich auf staatliche und private Applikationen zur Pandemiebekämpfung wie die «SwissCovid App», das «Covid-Zertifikat», «meineimpfungen.ch» oder «SocialPass». Wie aus unseren laufenden Mitteilungen zu diesen Projekten hervorgeht, erwies sich die Aufarbeitung und Behebung datenschutzrelevanter Mängel als herausfordernd. Dies vor allem dann, wenn wie im Fall der beiden letztgenannten Projekte gegen die privaten Betreiber der Applikationen formelle Aufsichtsverfahren eröffnet werden mussten, die mit Blick auf den zeitgerechten Schutz der Bevölkerung mit der erforderlichen Beschleunigung zu führen sind.

Bedürfnis nach Transparenz
Ein signifikanter Anteil an Zugangsgesuchen zu amtlichen Dokumenten wies einen Bezug zu Covid-19 auf und wurde im Tätigkeitsbericht deshalb separat ausgewiesen. Mit Rücksicht auf die spezielle Belastung gewisser Bundesstellen durch die Seuchenbekämpfung setzte sich der Beauftragte im Rahmen seiner Schlichtungstätigkeit gegenüber Medienschaffenden für die Erstreckung von Fristen ein. Auf Empfehlung des Beauftragten hat das Bundesamt für Gesundheit Zugangsgesuche zur Beschaffung von Covid-Impfstoffen zwecks Wahrung wirtschaftlicher Interessen der Schweiz aufgeschoben.

Neues Datenschutzgesetz auf der Zielgeraden – Herausforderungen steigen
Das totalrevidierte Bundesgesetzes über den Datenschutz vom 25. September 2020 wird voraussichtlich im zweiten Semester 2022 zusammen mit der Ausführungsverordnung in Kraft treten. Die erforderlichen Anpassungsarbeiten (Merkblätter, Meldeportale, Gebührenerhebung etc.) seitens des EDÖB sind im Gang. Angesichts der weiter voranschreitenden Dynamik der Digitalisierung wird der EDÖB seine Aufsichtstätigkeit auch nach Inkraftsetzung des neuen Gesetzes auf systemrelevante Datenschutzverletzungen schweizerischer Datenbearbeiter fokussieren müssen. Aller Voraussicht nach wird er schwerlich alle Erwartungen nach Behandlung individueller Datenschutzanliegen erfüllen können.

Die Erneuerung des Angemessenheitsentscheides der Europäischen Kommission ist weiterhin ausstehend.

Der 28. Tätigkeitsbericht 2020/2021 des EDÖB kann auf *www.edoeb.admin.ch* als e-Paper heruntergeladen werden.

TeleTrusT European Bridge CA: "PKI-Workshop" 2021

Der traditionelle „PKI-Workshop", den der Bundesverband IT-Sicherheit e.V. (TeleTrusT) im Rahmen der „European Bridge CA" (EBCA) in diesem Jahr am 30.09.2021 in Berlin ausrichtet, widmet sich Aspekten rund um das Thema PKI. Die Veranstaltung beleuchtet den Stand der Technik sowie neueste Entwicklungen und richtet sich über die EBCA-Beteiligten hinaus an alle interessierten Fachleute.

Geplante Themen:
- Markus Wichmann, Siemens, Sprecher der TeleTrusT European Bridge CA, Moderation
- Stephen Davidson, Chair of "S/MIME Certificate Working Group" in the "CA/Browser Forum", DigiCert: "Establishing Global Baseline Requirements for Publicly-trusted S/MIME Certificates -Overview of the CA/Browser Forum S/MIME Certificate Working Group"
- Enrico Entschew, D-Trust: „Trust Spaces – Ein Weg den Gordischen Knoten zwischen der EU und den Browsern zu lösen"
- Anna Katharina Pfeiffer, esatus: „Einsatz der SSI-Technologie im Rahmen des Innovationswettbewerbs ‚Schaufenster Sichere Digitale Identitäten'"
- Prof. Dr. Hermann Strack, Hochschule Harz; Marlies Gollnick, Hochschule Harz: „eIDAS-basierte Applikationen/Infrastrukturen für gesichertes ‚Campus'-Management für Hochschulwesen, Unternehmen und Verwaltungen"
- Heino Rätscher, Uniper: "Uniper Use Case: Microsoft Information Protection vs. S/MIME"

Darüber hinaus wird Gelegenheit für Gruppendiskussionen und fachlichen Gedankenaustausch gegeben. Für den Vorabend lädt TeleTrusT die Teilnehmer zu einer Networking-Veranstaltung ein.

Die TeleTrusT European Bridge CA (EBCA) ist ein Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKIen) zu einem PKI-Verbund. Sie ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen.

Vollständiges Programm und Anmeldung unter: *https://www.teletrust.de/veranstaltungen/tutorials-workshops/ebca-pki-2021/*

TeleTrusT-Innovationspreis 2021 für junge IT-Sicherheitsunternehmen: Bewerbungsverfahren

Seit 1999 verleiht der Bundesverband IT-Sicherheit e.V. (TeleTrusT) den „TeleTrusT-Innovationspreis". Der Preis ist für junge IT-Sicherheitsunternehmen bestimmt, die noch nicht länger als 3 Jahre am Markt sind und die innovative, vertrauenswürdige und praxistaugliche IT-Sicherheitslösungen für Wirtschaft und Ver-waltung entwickelt haben.

Eine Jury wählt den Preisträger anhand folgender Kriterien aus:

- Ist das IT-Sicherheitsniveau dem Schutzbedarf der Anwendung angemessen?
- Sind die Sicherheitsfunktionen integrierter Bestandteil des angebotenen oder genutzten Produktes?
- Sind die integrierten Sicherheitsfunktionen für den Anwender transparent und bedienerfreundlich?
- Ist die Anwendung interoperabel, idealerweise mit europäischer Reichweite?
- Trägt die Anwendung zur wirtschaftlichen Stabilität des Unternehmens bei?

Der Preis wird in größerem Rahmen vor einem Auditorium ausgewiesener IT-Sicherheitsexperten auf einer TeleTrusT-Veranstaltung im November in Berlin überreicht. Die ausgezeichnete Lösung und der Preisträger werden der breiteren Öffentlichkeit vorgestellt.

https://www.teletrust.de/teletrust-innovationspreis/2021/

Trend Micro warnt vor Ransomware, die auf industrielle Steuerungssysteme abzielt

Trend Micro, ein Anbieter von Cybersicherheitslösungen, veröffentlichte am 30. Juni 2021 einen neuen Bericht, der das steigende Risiko von Ausfallzeiten und Diebstahl sensibler Daten durch Ransomware-Angriffe auf Industrieanlagen hervorhebt.

„Industrielle Steuerungssysteme sind unglaublich schwer abzusichern. Dies führt zu zahlreichen Sicherheitslücken, die Cyberkriminelle immer gezielter ausnutzen", sagt Udo Schneider, IoT Security Evangelist Europe bei Trend Micro. „Angesichts der Tatsache, dass die US-Regierung Ransomware-Angriffe nun mit der gleichen Schwere wie Terrorismus behandelt, hoffen wir, dass unsere neuesten Studienergebnisse Betreiber von Industrieanlagen dabei unterstützen, ihre Sicherheitsanstrengungen zu priorisieren und neu auszurichten."

Als wesentlicher Bestandteil von Energieversorgungs- und Fertigungsanlagen sowie anderen industriellen Betrieben werden industrielle Steuerungssysteme (Industrial Control Systems, ICS) zur Überwachung und Steuerung industrieller Prozesse über IT-OT-Netzwerke hinweg eingesetzt.

Wenn Ransomware ihren Weg in diese Systeme findet, kann sie den Betrieb für Tage lahmlegen und das Risiko erhöhen, dass Entwürfe, Programme und andere sensible Dokumente ihren Weg ins Dark Web finden.

Der Bericht von Trend Micro zeigt, dass Varianten der Malware-Familien Ryuk (20 Prozent), Nefilim (14,6 Prozent), Sodinokibi (13,5 Prozent) und LockBit (10,4 Prozent) für mehr als die Hälfte der ICS-Ransomware-Infektionen im Jahr 2020 verantwortlich sind.

Im Vergleich zu Ländern wie Japan (4,7 Prozent) oder den USA (9,8 Prozent), die neben Deutschland zu den zehn Ländern mit der größten Anzahl an IT/OT-Netzwerken mit ICS-Endpunkten zählen, weist Deutschland mit 17,3 Prozent einen vergleichsweise hohen prozentualen Anteil an Grayware auf. Als Grayware werden potenziell unerwünschte Anwendungen, Adware (Programme, die unerwünschte Werbung anzeigen) oder Hacking-Tools bezeichnet. Darüber hinaus stellt die Studie des japanischen Sicherheitsanbieters fest, dass industrielle Steuerungssysteme in Deutschland weltweit mit der meisten Adware infiziert sind – meist aufgrund von Programmen, die mit Software-Tools gebündelt sind.

Die Studie beinhaltet darüber hinaus weitere Erkenntnisse:

- Bedrohungsakteure infizieren ICS-Endpunkte, um mit ungepatchten Betriebssystemen, die noch für EternalBlue anfällig sind, Kryptowährung zu schürfen.
- Varianten von Conficker verbreiten sich auf ICS-Endpunkten mit neueren Betriebssystemen durch Brute-Forcing von Admin-Freigaben.
- Legacy-Malware wie Autorun, Gamarue und Palevo sind in IT/OT-Netzwerken immer noch überall im Umlauf und verbreiten sich über Wechsellaufwerke.

Die Studie fordert IT-Sicherheits- und OT-Teams zu einer engeren Zusammenarbeit auf, um wichtige Systeme und Abhängigkeiten wie Betriebssystemkompatibilität und Laufzeitanforderungen zu identifizieren und so effektivere Sicherheitsstrategien zu entwickeln.

Trend Micro gibt darüber hinaus folgende Empfehlungen:

- Ein unmittelbares Patchen von Schwachstellen ist unerlässlich. Ist dies nicht möglich, sollten Unternehmen eine Netzwerksegmentierung oder virtuelles Patching in Betracht ziehen.
- Unternehmen können Ransomware nach dem Eindringen bekämpfen, indem sie die Ursachen der Infektion mithilfe von Software zur Anwendungskontrolle und Tools zur Threat Detection und Response eindämmen, um auf diese Weise Netzwerke nach IoCs (Indicator of Compromise) zu durchsuchen.
- Netzwerkfreigaben sollten eingeschränkt und starke Benutzername/Kennwort-Kombinationen erzwungen werden, um unbefugten Zugriff durch Brute-Forcing von Anmeldeinformationen zu verhindern.
- IDS (Intrusion-Detection-Systeme) oder IPS (Intrusion-Prevention-Systeme) können das normale Netzwerkverhalten erfassen und verdächtige Aktivitäten frühzeitig erkennen.
- Unternehmen sollten ICS-Endpunkte auch in vermeintlichen Air-Gap-Umgebungen regelmäßig mit Standalone-Tools scannen.
- Mit USB-Malware-Scanner können Wechsellaufwerke überprüft werden, die für den Datentransfer zwischen Air-Gapped-Endpunkten verwendet werden.
- Unternehmen sollten das Prinzip der geringsten Rechte auf OT-Netzwerkadministratoren und -betreiber anwenden.

Den vollständigen Bericht „2020 Report on Threats Affecting ICS Endpoints" können Sie in englischer Sprache einsehen: *https://www.trendmicro.com/vinfo/de/security/news/internet-of-things/2020-report-ics-endpoints-as-starting-points-for-threats*

Hochsichere digitale Signaturen für Mitarbeiter: Entrust stellt neuen Remote Signing Service vor

Entrust, ein Anbieter im Bereich vertrauenswürdige Identitäten, Zahlungen und Datenschutz, integriert mit seinem Remote Signing Service (RSS) hochsichere, verifizierbare Mitarbeiter-Signaturfunktionen in Dokumentanwendungen und Workflows. Zusammen mit dem kürzlich eingeführten Signing Automation Service bietet Entrust damit ein umfassendes Portfolio an Cloud-basierten Digital-Signing-as-a-Service-Lösungen.

Mit dem Wechsel in die Cloud und der zunehmenden räumlichen Verteilung von Belegschaften wird für Unternehmen die Unterstützung neuer Remote-Business-Szenarien essenziell. Der Entrust Remote Signing Service hilft öffentlichen und privaten Organisationen, diese neuen Herausforderungen zu meistern und sich von traditionellen handschriftlichen Signaturen und Papierdokumenten zu lösen – ohne Kompromisse in punkto Sicherheit und Vertrauen einzugehen.

Mit Entrust Remote Signing Service stehen workflow-unabhängige digitale Signierlösungen zur Verfügung, die sich in eine Vielzahl von Dokumentenmanagement-Software und Portalen integrieren lassen. Dies ermöglicht es mittleren und großen Unternehmen, Ineffizienzen und Verzögerungen durch herkömmliche papierbasierte Prozesse zu überwinden – stattdessen wird ein elektronischer Unterschriftenservice angeboten, der auf weltweit anerkannten Zertifikaten basiert. Darüber hinaus erleichtert Entrust RSS mit verifizierten Mitarbeiteridentitäten und starker Authentifizierung die Einhaltung von gesetzlichen und regulatorischen Anforderungen.

Mit dem zertifikatsbasierten Remote Signing Service übernimmt Entrust die Ausstellung, Speicherung und Wartung der Signaturinfrastruktur für seine Kunden, bei nahtloser Integration in deren jeweilige Dokumenten-Workflow-Umgebung. Basierend auf seiner jahrzehntelangen Expertise im Bereich Public Key Infrastruktur (PKI) und digitale Signaturen bietet Entrust damit eine einfache, hochperformante, sichere und skalierbare Lösung an. Unternehmen können damit vertrauensvoll digitale Workflows einführen und sind nicht länger auf papierbasierte Prozesse und persönliche Meetings angewiesen.

„Wir freuen uns, den Entrust Remote Signing Service in Adobe Sign verfügbar zu machen. Adobes Ansatz der offenen Standards für digitales Signieren bedeutet, dass wir mit den anerkanntesten Anbietern der Welt zusammenarbeiten, um unseren gemeinsamen Kunden sichere, hochmoderne Vertrauensdienste zur Verfügung zu stellen und eine Vielzahl von Anwendungsszenarien zu adressieren", so John Jolliffe, Strategic Development Team bei Adobe. „Der Entrust Remote Signing Service in Adobe Sign bietet Unternehmen eine skalierbare und Cloud-basierte Lösung – sie ermöglicht Mitarbeitern, mit vertrauenswürdigen digitalen Signaturen zu unterschreiben und unterstützt gleichzeitig bei der Erfüllung von rechtlichen und Compliance-Anforderungen."

„Digitale Signaturen werden zum neuen Standard für elektronische Transaktionen", kommentiert Frédéric Mauger, Mitgründer und Partner bei Sysmosoft. „Die Integration des Entrust Remote Signing Service in unser Produkt Let's Sign bringt unseren Kunden, die in stark regulierten Branchen wie Banken und Finanzinstituten tätig sind, große Vorteile. Sie können eine größere Mobilität mit vollständig digitalisierten Prozessen erreichen, ohne Kompromisse bei der Sicherheit und der Benutzererfahrung einzugehen."

Mehr zu Entrust Remote Signing Service erfahren Sie unter *https://www.entrust.com/digital-security/certificate-solutions/products/digital-signing/digital-signing-as-a-service/remote-signing-service*

Highspeed-VPN-Gateway unterstützt Georedundanz und digitale Souveränität von Rechenzentren

Mit genuscreen 40G VPN stellte der deutsche IT-Security-Spezialist genua am 08. Juli 2021 ein hochsicheres Highspeed-Gateway für Rechenzentren (RZ) und Unternehmen vor. Die FPGA-basierte VPN-Appliance wurde für den performanten, verschlüsselten Transfer großer Datenmengen ausgelegt. genuscreen 40G VPN eignet sich damit insbesondere für die sichere Koppelung von Rechenzentren. Mit der in Deutschland entwickelten Technologie für Virtual Private Networks (VPN) können RZ-Betreiber und Unternehmen die Forderung des Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Georedundanz erfüllen sowie gleichzeitig ihre digitale Souveränität schützen.

Rechenzentren sind sensible, teils kritische Kommunikationsinfrastrukturen für Wirtschaft, Staat und Gesellschaft. Um ihre Funktionsfähigkeit unter allen Umständen sicherzustellen, fordert das BSI für hoch- oder höchstverfügbare Rechenzentren deren Georedundanz mit einem Mindestabstand von 200 km. Damit soll sichergestellt werden, dass bei einem Großschadensereignis nicht beide Standorte gleichzeitig oder zeitnah getroffen werden. Mit genuscreen 40G VPN lassen sich solche Rechenzentren mit konstanten 40 Gbit/s bei gleichzeitiger IPsec-Verschlüsselung hochperformant koppeln.

Hochsichere Technologien schützen vor Datenmanipulation und Abhören

„Mit genuscreen 40G VPN bieten wir ein Highspeed-Gateway, das dank FPGA-Technologie eine äußerst schnelle Signalverarbeitung ermöglicht. Es unterstützt Rechenzentren dabei, ihre Systeme auch bei kritischen Vorfällen hochverfügbar zu halten," kommentiert Matthias Ochs, Geschäftsführer der genua GmbH. „Wir freuen uns, mit unserer Lösung ‚Made in Germany' einen Beitrag zur IT-Sicherheit und digitalen Souveränität kritischer Kommunikationsinfrastrukturen in Deutschland leisten zu können."

genuscreen 40G VPN basiert auf Lösungen, die im öffentlichen Sektor und von geheimschutzbetreuten Unternehmen eingesetzt werden. Die Appliance eignet sich damit für den zuverlässigen Schutz hochsensibler Kommunikationsverbindungen vor Manipulation und Abhören. Die Zulassung für VS-NfD (Verschlusssachen – nur für den Dienstgebrauch) wird angestrebt. Lösungen von genua verfügen darüber hinaus bereits über quantencomputerresistente Software-Signaturen. Sie sind damit schon heute wirksam vor zukünftigen IT-Sicherheitsrisiken geschützt.

Hoher Durchsatz bei minimaler Latenz dank FPGA

genuscreen 40G VPN nutzt Field Programmable Gate Arrays (FPGAs) für die außergewöhnlich schnelle Signalverarbeitung. Der Datendurchsatz beträgt konsistent 40 Gbit/s für bis zu 1024 verschlüsselte Verbindungen, bei einer Latenz von weniger als 20 µs. Diese Leistung wird selbst bei Verschlüsselung mit IPsec (Internet Protocol Security) und unabhängig vom Paketmix – groß, klein

oder IMIX – erzielt. Der Datenverkehr wird mit AES-256-GCM mit 16-Byte-Integritätsprüfung codiert. Der IPsec-Standard sorgt dabei für eine konforme Verschlüsselung auf Layer 3. Die verschlüsselten Frames bleiben aufgrund der Kapselung in IP- und IPsec-ESP-Header routingfähig. Layer 2 über Layer 3 ist ebenfalls möglich.

Auch anspruchsvolle Applikationen wie VoIP oder Videokonferenzen können dank der geringen Latenz abgesichert werden. Mit ihrer geringen Größe von nur zwei Höheneinheiten spart die Appliance wertvollen Raum im Rechenzentrum ein.
Weitere Informationen: *https://www.genua.de/vpn-sicherheitsloesungen/genuscreen*

Common Criteria: TÜViT evaluiert erstes IT-Produkt nach EAL7 im BSI Zertifizierungsschema

Die Arbit Data Diode 10GbE in Version 1.00 des dänischen Herstellers Arbit Cyber Defence Systems ApS (Arbit) zählt seit dem 22. Juni 2021 zu den einzigen beiden IT-Produkten, die offiziell nach dem höchsten Evaluation Assurance Level (EAL7+) der Common Criteria zertifiziert sind.

Nach erfolgreicher Evaluierung durch die TÜV Informationstechnik GmbH (TÜViT) und Anerkennung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) kann Arbit nun schwarz auf weiß nachweisen, dass ihre Datendiode mit der höchst möglichen Prüftiefe im Rahmen der Common Criteria (CC) untersucht wurde. Dies bestätigt das bislang erste im deutschen Zertifizierungsschema ausgestellte EAL7+-Zertifikat.

Die Datendiode – Schützt vor Datendiebstahl und -missbrauch

Bei der Arbit Data Diode handelt es sich um eine Datendiode, die Netzwerke durch ihre physikalischen Eigenschaften voneinander separiert. Sie gewährleistet, dass Daten von einem offenen Netzwerk über ein Common Criteria EAL7+ zertifiziertes Hardwaremodul (die Diode) in ein geschlossenes Netzwerk hinein-, aber nicht mehr hinausgelangen können. Auf diese Weise werden die im geschlossenen Netzwerk gespeicherten Daten nach außen hin abgeschirmt und damit gegenüber Datendiebstahl oder -missbrauch geschützt.

Erfolg des Projektes

Zu Projektbeginn musste zunächst die konkrete Prüfmethodologie für eine Evaluation gemäß EAL7+ erstellt werden. Dies betraf insbesondere die formale Spezifikation des Produkts, aber auch die funktionalen Tests, die sowohl vom Hersteller als auch dem Prüflabor durchzuführen waren. Daher wurden in enger Abstimmung mit dem BSI konkrete Prüfaufgaben für die zusätzlichen Anforderungen einer EAL7+-Evaluation definiert, die sich auf den speziellen Kontext der Arbit Datendiode bezogen.

Um das gesetzte Ziel zu erreichen, profitierte Arbit insbesondere von den Diensten der dänischen Firma Confiware und Arne Stig Peters, der das Unternehmen während des gesamten Zertifizierungsprozesses beratend unterstützte und maßgeblich an der Entwicklung, dem erforderlichen CC-Dokumentenpaket und den formalen Modellen der Arbit Data Diode beteiligt war.

„Entscheidend für den erfolgreichen Abschluss des Projekts war – neben einem fachlich versierten Team bei TÜViT – auch ein Hersteller, der sich den konkreten Anforderungen, die erst während des Verfahrens festgelegt wurden, mit Selbstvertrauen in das eigene Know-how offen gestellt hat. Ich möchte an dieser Stelle aber auch die zuständigen Zertifizierer beim BSI erwähnen, die uns jederzeit mit Kompetenz und Fokus zur Seite standen", fasst Dr.-Ing. Alexander Schasse, Projektleiter und IT-Sicherheitsexperte bei TÜViT, den Abschluss des Projektes zusammen.

„Arbit hat große Anstrengungen unternommen, um die Zertifizierung nach EAL7+ zu erreichen. An dieser Stelle möchte ich noch einmal meine persönliche Anerkennung für eine außergewöhnlich gute und professionelle Zusammenarbeit mit Dr. Ing. Alexander Schasse und Dr. Ing. Sebastian Becker zum Ausdruck bringen", so Rasmus Borch, Gründer von Arbit.

Erfolgreicher Nachweis über die Funktionsweise der Arbit Data Diode

Dass die Arbit Data Diode genauso funktioniert wie vom Hersteller versprochen, belegt die erfolgreiche Prüfung durch TÜViT, die nun vom BSI mit einem CC-Zertifikat gekrönt wurde.

TÜViT bietet neuen Evaluierungsservice für Mikrochips von eingebetteten Systemen

Der neue Evaluierungs- und Zertifizierungsansatz von TÜViT ermöglicht eine unabhängige Betrachtung des Mechanismus für Firmware-Updates und erlaubt die Zertifizierung seiner Sicherheit, ohne dabei andere Funktionalität zu berücksichtigen. Das am 29. Juni 2021 veröffentlichte Ergebnis ist ein Trusted Product-Zertifikat, mit dem Chiphersteller objektiv nachweisen können, dass ihr Firmware-Updater die höchsten Sicherheitsanforderungen erfüllt.

Die Firmware ist ein wichtiger Bestandteil der heutigen eingebetteten Elektronik. Ihre Authentizität und Integrität stellt einen Schlüsselfaktor dar, der die Betriebs- und Angriffssicherheit eingebetteter Systeme gewährleistet, z. B. bei intelligenten x-IoT-Produkten, die mit dem Internet verbunden werden. Obwohl Firmware-Updates die Funktionalität von Produkten auf einem Gebiet verbessern sollen, stellen sie auch den idealen Mechanismus für Angreifer dar, um ein Produkt zu hacken. Dies haben Sicherheitsforscher im Jahr 2015 demonstriert: Sie waren in der Lage, Lenkrad und Bremsen eines SUV fernzusteuern. Obwohl die originale Firmware des Fahrzeugs einen solchen Zugriff nicht erlaubt hatte, konnten die Angreifer problemlos ihre eigene, bösartige Firmware laden und erhielten so vollständigen Zugriff auf das Fahrzeug.

Aus diesem Grund hat TÜViT einen neuen Ansatz entwickelt, der es ermöglicht, den isolierten Firmware-Updater unabhängig von der eigentlichen lösungsspezifischen Firmware zu prüfen und zu zertifizieren. Das liegt daran, dass dieser Update-Mechanismus zur Hauptangriffsfläche für jedes eingebettete Produkt werden kann, wenn er nicht sorgfältig entworfen und implementiert wird.

Bestehende Zertifizierungsprogramme berücksichtigen stets die gesamte Sicherheit der produkt- oder branchenspezifischen Funktionalitäten der Komponente oder des Systems und fügen als Voraussetzung schließlich einen (sicheren) Firmware-Uploader als Teil der Zertifizierung hinzu. Dadurch wird es für Hersteller von Universalchips schwierig, ihr Produkt zertifizieren zu lassen: Während der Chipentwicklung und sogar während der Produktion ist der tatsächliche Anwendungsfall (und die entsprechende Firmware) oftmals noch nicht vollständig bekannt, doch die Chips werden

für den zukünftigen Verkauf auf Vorrat hergestellt. Um die Initialisierung solcher Chips zu einem späteren Zeitpunkt zu ermöglicht, muss jedoch zumindest ein grundlegender Firmware-Updater ab Werk enthalten sein. Dieser Firmware-Updater kann nun von TÜViT geprüft und zertifiziert werden.

Um die Aspekte im Hinblick auf Markteinführungszeit und Kosten zu erfüllen, setzt der neue Evaluierungsservice von TÜViT auf ein zeitgesteuertes Evaluierungskonzept. Drei verschiedene Sicherheitsstufen (niedrig, erheblich, hoch) spiegeln das unterschiedliche Angriffspotenzial durch verschiedene Zeitspannen wider. Zusätzlich zu einigen Pflichtanforderungen kann die Evaluierung durch die Auswahl optionaler Anforderungen, z. B. Verschlüsselung von Updates oder Verwendung von sicheren Post-Quantum-Algorithmen, erweitert werden. Einzigartig am Konzept von TÜViT ist das (optionale) Hinzufügen einer Fehlerbehandlungsroutine für fehlgeschlagene Updates: Während das Abschalten bei Standard-Sicherheitshardware (z. B. Kreditkartenchips) eine sinnvolle Option darstellt, müssen eingebettete Systeme, die sicherheitskritische Funktionen steuern, möglicherweise mit eingeschränkter Funktionalität weiterarbeiten. Beispielsweise sollte weder ein Automobilsteuergerät noch ein (intelligenter) Rauchmelder aufgrund eines fehlgeschlagenen Updates aufhören zu funktionieren. Stattdessen sollte das Gerät in einen Notfunktionsmodus wechseln oder auf die zuvor verwendete Firmware zurückgreifen.

TÜViT bietet ab sofort die Prüfung und Zertifizierung von Firmware-Update-Loadern nach diesem neuen Ansatz an.

Rhebo ist Träger des ECSO-Vertrauenssiegels »Cybersecurity Made In Europe«

Rhebo, ein Landis+Gyr-Unternehmen und ein in Europa führender Anbieter für industrielles Sicherheitsmonitoring, erhielt am 13. Juli 2021 offiziell das Vertrauenssiegel »Cybersecurity Made In Europe« der European Cyber Security Organisation (ECSO).

Das Anfang 2021 eingeführte Siegel steht für vertrauenswürdige Cybersecurity-Produkte und Leistungen. Rhebo schützt mit seinen Produkten und Dienstleistungen industrielle Netzwerke (Automatisierungstechnik, Operational Technology, OT) und Geräte in kritischen IoT-Netzen gegen Cyberangriffe und technische Fehlerzustände. Damit werden auch Kunden aus dem Bereich der Kritischen Infrastrukturen unterstützt, Sicherheitsvorgaben wie das aktualisierte IT-Sicherheitsgesetz sowie Standards wie ISO 27000 und IEC 62443 gezielt umsetzen. Das Kernprodukt Rhebo Industrial Protector überwacht mittels Anomalieerkennung die OT. Abweichungen der Kommunikation in den Netzwerken vom zu erwartenden Verhalten werden in Echtzeit erkannt und gemeldet. Die Sicherheitsverantwortlichen in Kritischen Infrastrukturen erhalten erstmalig Sichtbarkeit in ihre OT und können frühzeitig auf verdächtige Vorgänge wie Cyberattacken oder unberechtigte Eingriffe reagieren.

»Viele unserer Kunden sind im Bereich der Kritischen Infrastrukturen tätig«, betont Rhebo-Geschäftsführerin Kristin Preßler die Relevanz des Vertrauenssiegels. »Gerade dort darf das Vertrauen in die eingesetzte Technologie keine Zweifel offen lassen. Als deutsches Unternehmen haben wir deshalb von Anfang an kompromisslos auf die Sicherheit unserer Produkte geachtet. Die Auszeichnung mit dem ECSO-Vertrauenssiegel bestätigt uns darin«.

Als Träger des Siegels folgt Rhebo den strikten Anforderungen an Datenschutz entsprechend der Datenschutzgrundverordnung (DSGVO) und Datensicherheit gemäß der Richlinien der European Union Agency for Cybersecurity (ENISA). Die Erklärung umfasst u.a. auch eine Negativerklärung zur Spionage. Kunden von Rhebo können so sicher sein, dass die Produkte für industrielle Cybersicherheit und Stabilität u.a. keine Backdoors enthalten und von Grund auf sicher konzipiert sind. Die Anforderungen werden sowohl für das industrielle Netzwerkmonitoring mit Anomalierkennung (Rhebo Industrial Protector) als auch für das Sicherheitssystem für kritische IoT-Geräte (Rhebo IoT Device Protection) erfüllt.

Das Siegel »Cybersecurity Made In Europe« wird in Deutschland durch das europäische Kompetenzzentrum für Sicherheit in der Informationstechnologie eurobits e. V. verliehen *(https://www.eurobits.de/ecso-label-cybersecurity-made-in-europe/)*.

E-Mail- und Passwortdiebstahl: Deutschland auf Platz 4

Im Zuge der Covid-19-Pandemie hat die Nutzung von digitaler Kommunikation in staatlichen Behörden, Forschungseinrichtungen und Unternehmen erheblich zugenommen – und dadurch die potenzielle Angriffsfläche von Cyber-Attacken deutlich erhöht und neuen Spielraum für Spionage, Ausspähung und Sabotage durch Cyberangriffe eröffnet.

Der Bundesverband der Deutschen Industrie e. V. (BDI) stellte am 13. Juli 2021 fest, dass die deutsche Wirtschaft noch nie so stark angegriffen wurde wie heute. Die Anzahl der Angriffe ist in der Corona-Pandemie weiter gestiegen, weil Unternehmen im Homeoffice noch verwundbarer sind.

Der aktuelle CRIFBÜRGEL Cyber Report hat die Anfälligkeit von Einzelpersonen und Unternehmen für Cyberangriffe im Open und Dark Web untersucht und zeigt auf, welche Daten am meisten betroffen sind, welche Informationen im Web zu finden sind und wo sich der Datenverkehr konzentriert.

Deutschland auf Platz 4

Zu den Ländern, die aktuell am stärksten von E-Mail- und Passwortdiebstahl betroffen sind, gehören die USA, Russland, Frankreich und Deutschland, gefolgt von Großbritannien und Italien, das insgesamt auf Platz sechs liegt. Polen, die Tschechische Republik, Japan und Brasilien komplettieren die Top 10.

Des Weiteren wurde im Rahmen des Cyber Reports erhoben, welche Kontinente am stärksten von illegalem Kreditkartendatenaustausch betroffen sind. Dieses Ranking wird von Nordamerika angeführt, gefolgt von Europa und Asien, allerdings mit einem erheblichen Abstand zur Spitze. Am unteren Ende der Liste stehen Afrika und Ozeanien. Bei den einzelnen Ländern, die am stärksten betroffen sind, stehen die Vereinigten Staaten an der Spitze, gefolgt von Frankreich und Brasilien, die die Top drei vervollständigen.

Online-Streaming und Online-Spiele als Risiko

Konten, die mit Unterhaltungsseiten verknüpft sind, insbesondere Online-Spiele und Streaming, sind derzeit am stärksten dem Diebstahl persönlicher Daten ausgesetzt (51,5 Prozent aller Fälle). Ebenfalls stark betroffen sind soziale Netzwerke (31,8 Prozent), gefolgt von E-Commerce (10,7 Prozent) sowie Foren und Webseiten (5,9 Prozent).

Diese Daten kursieren im Dark Web

Im Dark Web zirkulieren überwiegend persönlichen Daten, welche daher am anfälligsten sind. Es handelt sich um Passwörter, persönliche oder Firmen-E-Mail-Adressen, Benutzernamen und Telefonnummern. Diese wertvollen Kontaktdaten könnten für Betrugsversuche genutzt werden, etwa durch Phishing oder Smishing. Es werden aber auch finanziell relevante Daten ausgetauscht, wie z. B. Kreditkartendetails und IBANs.

Noch interessanter ist es, die Hauptkombinationen der abgefangenen Daten im Web zu beobachten. E-Mail-Adressen sind fast immer mit einem Passwort verbunden (96,3 Prozent der Fälle). Bei den im Dark Web gefundenen Passwörtern handelt es sich zumeist um persönliche E-Mail-Konten. Bei den Kreditkarteninformationen sind neben der Kartennummer beinahe immer auch die Kartenprüfnummer und das Ablaufdatum vorhanden (98,6 Prozent der Fälle). Zudem sind bei rund einem Fünftel der Fälle auch der Vor- und Nachname des Karteninhabers zu finden.

Die häufigsten Passwörter

Laut einer Analyse von Passwörtern, die im Dark Web gefunden wurden, waren die Top 10 der meistgenutzten Passwörter „123456", gefolgt von „123456789" und „qwerty". Dies sind sehr einfache Kombinationen aus Zahlen und Buchstaben, die von Hackern leicht abgefangen werden können.

„Bei den Opfern handelt es sich typischerweise um Männer im Alter zwischen 41 und 60 Jahren. Es gibt zweifelsohne Verhaltensweisen, die die Risiken von Identitätsdiebstahl sinnvoll mindern können. Verbraucher sollten darauf achten, wie Passwörter, die mit verschiedenen Konten verbunden sind, festlegt und verwaltet werden. Zudem sollte die Sensibilität erhöht werden, mit der Verbraucher auf E-Mails, Nachrichten oder Anrufe reagieren", sagt CRIFBÜRGEL Geschäftsführer Dr. Frank Schlein.

Es ist auch wichtig, dass Benutzer, sofern möglich, die Zwei-Faktor-Authentifizierung aktivieren, um so zu verhindern, dass Hacker in Konten eindringen, selbst nachdem sie den Benutzernamen und das Passwort herausgefunden haben. Außerdem sollten Nutzer bei der Verwendung von öffentlichen WiFi-Netzwerken genau auf die Risiken achten, die mit der Speicherung von Anmeldedaten auf öffentlichen oder gemeinsam genutzten Computern verbunden sind.

Über die Studie

Für diese Studie hat CRIF im 2. Halbjahr 2020 Websites, Gruppen, Foren und spezialisierte Gemeinschaften des sogenannten „Dark Web" durchsucht und Milliarden von Datensätzen analysiert. Dabei sind technologische Methoden zum Einsatz gekommen, welche CRIF bereits für dessen Cyber Risk Lösungen im Einsatz hat.

Sie finden die Studie unter *https://bdi.eu/....*

BIMI-Standard: Entrust kündigt Verfügbarkeit von Verified Mark-Zertifikaten an

Entrust, Anbieter im Bereich vertrauenswürdige Identitäten, Zahlungen und Datenschutz, gab am 14. Juli 2021 die allgemeine Verfügbarkeit seiner Verified Mark Zertifikate (VMCs) zur Unterstützung des „Brand Indicators for Message Identification (BIMI)"-Standards für starke E-Mail-Authentifizierung bekannt. Dieser Schritt folgt auf die Ankündigung von Google, BIMI generell in Gmail zu unterstützen.

BIMI ist eine branchenübergreifende Initiative, die Übertragung und Verwendung von Markenlogos in E-Mails zu standardisieren. Da E-Mails für Unternehmen als Kommunikationskanal zu ihren Kunden mittlerweile eine zentrale Bedeutung einnehmen, könnte BIMI die breite Akzeptanz der E-Mail-Authentifizierung erhöhen, ohne Absender in ihren Branding-Möglichkeiten einzuschränken. E-Mail-Empfänger, die unterstützte E-Mail-Anbieter wie z.B. Gmail nutzen, bekommen in ihren E-Mails die verifizierten Markenlogos von BIMI-Anwendern angezeigt.

Neben erhöhter Sicherheit kann die Einführung von BIMI Kunden eines Unternehmens ein authentischeres und vertrauenswürdigeres Erlebnis in Gmail bieten. Die Förderung einer starken Absenderauthentifizierung mithilfe von DMARC und die erhöhte Akzeptanz für BIMI kommt dem gesamten E-Mail-Ökosystem zugute.

Mehrere große Marken haben bereits damit begonnen, BIMI-Standards und die Verwendung von VMCs zur Authentifizierung ihrer E-Mail-Kommunikation einzuführen. Ally Financial arbeitet seit einem Jahr mit Entrust zusammen, um die Verwendung von VMCs zu testen.

Die Verwendung von BIMI erfordert ein Verified-Mark-Zertifikat (VMC) von einer autorisierten Zertifizierungsstelle, das mit der Domain-based Message Authentication, Reporting and Conformance (DMARC) Protokollrichtlinie einer Organisation zusammenarbeitet. Entrust hat das ursprüngliche Konzept des VMC in Zusammenarbeit mit der AuthIndicators-Arbeitsgruppe entwickelt und das erste VMC im September 2019 ausgestellt.

„Wir sind stolz darauf, diesen neuen Standard für starke E-Mail-Authentifizierung einzuführen und zu sehen, wie er mit der Unterstützung von Gmail eine breite Akzeptanz findet – und wir rechnen damit, dass andere E-Mail-Anbieter sich anschließen werden", erklärt Chris Bailey, Vice President of Strategy and Business Development bei Entrust. „Wir arbeiten seit über vier Jahren mit der BIMI-Arbeitsgruppe zusammen und engagieren uns für die Bereitstellung von verifizierten Markenindikatoren in E-Mails als wichtigen Vorteil für Marken und ihre Kunden."

Weitere Informationen: Entrust Verified Mark-Zertifikate (VMCs): *https://www.entrust.com/vmc,* BIMI Radar – Registrierte VMCs: *https://www.bimiradar.com*

E-Rezept: BSI bestätigt Sicherheit

Mit der Bestätigung der Informationssicherheit der E-Rezept-App vom 01. Juli 2021 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Freigabe für das E-Rezept erteilt. Damit kann die zuständige gematik die E-Rezept-App in den App-Stores zur Verfügung stellen. Geplant ist zunächst eine regionale Testphase, bevor das E-Rezept im 4. Quartal 2021 bundesweit eingeführt werden soll. Das BSI ist mit der Bestätigung des externen Sicherheitsgutachtens für das Frontend des Versicherten E-Rezepts gemäß § 360 Abs. 10 SGB V seiner Kontroll- und Aufsichtsfunktion nachgekommen.

Dazu BSI-Präsident Arne Schönbohm:
„Das E-Rezept ist ein echter Meilenstein in der Digitalisierung des Gesundheitswesens. Es wird vielen Patientinnen und Patienten das Leben erleichtern und ihnen viele beschwerliche Wege ersparen. Informationssicherheit ist ein wesentlicher Vertrauensfaktor für die Bürgerinnen und Bürger, insbesondere, wenn sensible medizinische Daten verarbeitet werden. Das BSI hat die gematik von Anfang an bei der Gestaltung sicherer elektronischer Prozesse für

das E-Rezept unterstützt. So tragen wir zu einer sicheren Digitalisierung bei."

Die App ermöglicht den Versicherten eine medienbruchfreie Versorgung mit notwendigen Medikamenten. Das E-Rezept kann elektronisch zur Verfügung gestellt und eingelöst werden. Neben weiteren Funktionen ist auch die Verwaltung der Rezepte über die App und die Verschiebung der Rezepte in die elektronische Patientenakte möglich.

Voraussetzungen für den sicheren Einsatz des E-Rezepts sind eine NFC-fähige elektronische Gesundheitskarte, ein NFC-fähiges Smartphone (ab IOS 14, Android 6) und die Freischaltung der Krankenkasse für das Verfahren. Auch die verordnende Praxis muss entsprechende technische Voraussetzungen erfüllen.

Neben einer elektronischen Transaktion kann ein Rezept künftig auch mit einem durch die Ärztinnen und Ärzte ausgedruckten QR-Code in einer Apotheke eingelöst werden. Das derzeitige Rezeptformular wird künftig nur noch im Stör- oder Notfall gültig sein.

BSI: Erstes Zertifikat nach dem Schema „Beschleunigte Sicherheitszertifizierung"

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 21. Juni 2021 das erste Zertifikat nach dem neuen Schema der Beschleunigten Sicherheitszertifizierung (BSZ) der LANCOM Systems GmbH für ihren Businessrouter Lancom 1900EF erteilt.

Pandemiebedingt erfolgte die Zertifikatsübergabe trotz des Novums in der Zertifizierung des BSI online. Arne Schönbohm, Präsident des BSI, überreichte das Zertifikat an Ralf Koenzen, Mitbegründer und Geschäftsführer Lancom Systems GmbH.

Dazu Arne Schönbohm:

„Zertifizierung ist ein wichtiger Baustein der Informationssicherheit, um Verwaltung und Wirtschaft, aber auch Bürgerinnen und Bürgern, sichere Produkte und Dienstleistungen anzubieten. Zertifikate schaffen Transparenz und damit Vertrauen. Ich freue mich, dass Lancom Systems GmbH das erste Unternehmen ist, das mit uns die erste Beschleunigte Sicherheitszertifizierung (BSZ) durchlaufen hat.

Zertifizierungen sind der Goldstandard, aber sie erfordern für die Unternehmen auch Zeit und Zeit ist Geld. Mit der Beschleunigten Sicherheitszertifizierung wollen wir diesen Prozess für die Wirtschaft einfacher und schneller gestalten, dabei aber unseren hohen Standards treu bleiben. Insbesondere wird die Expertise von erfahrenen Prüfern und Prüferinnen genutzt, um gezielt nach Sicherheitsrisiken und Schwachstellen zu suchen. So wird ein hohes Niveau an Vertrauen in die Sicherheitsaussagen geschaffen."

Ein BSZ-Zertifikat bietet den Unternehmen eine eindeutige und verständliche Darstellung der Sicherheitseigenschaften sowie eine belastbare Aussage über die Widerstandsfähigkeit des zertifizierten Produkts. Zusätzlich wird gewährleistet, dass der Hersteller über einen definierten Zeitraum von in der Regel zwei Jahren das Produkt durch Sicherheitsupdates auf dem neuesten Stand hält.

Die BSZ ergänzt neben der Zertifizierung nach Common Criteria, der Zertifizierung nach Technischen Richtlinien und dem IT-Sicherheitskennzeichen das Portfolio des BSI und wird mithelfen, die IT-Sicherheit in Deutschland zu erhöhen. BSI-Zertifikate genießen weltweit einen sehr guten Ruf und werden, auch im Rahmen internationaler Anerkennungsvereinbarungen, anerkannt.

Das BSZ-Schema ist kompatibel zur französischen CSPN und eine gegenseitige Anerkennung ist in Vorbereitung. Die Kompatibilität zum Fixed-Time-Ansatz (FIT CEM/prEN 17640) bildet eine Basis für die Integration auf europäischer Ebene in zukünftige CSA-Schemata.

Ab Herbst 2021 steht die BSZ allen Interessierten zur Nutzung offen.

BSI erteilt SecurePIM Government SDS die Zulassung für die Geheimhaltungsstufe „NATO RESTRICTED"

Behörden und Organisationen können die mobile Kommunikationslösung SecurePIM Government SDS von Virtual Solution ab dem 14. Juli 2021 auch für die Geheimhaltungsstufe „NATO RESTRICTED" einsetzen. Das ermöglicht den Austausch sicherheitskritischer Verschlusssachen innerhalb der NATO, aber auch zwischen Behörden und Unternehmen.

Die Systemlösung SecurePIM Government SDS hat vom Bundesamt für Sicherheit in der Informationstechnik (BSI) die Zulassung für den Einsatz bei klassifizierten Verschlusssachen der Geheimhaltungsstufe NATO RESTRICTED für iOS-Geräte (ab iOS-Version 14) erhalten. Die Lösung kann jetzt innerhalb der NATO, zwischen NATO-Mitgliedstaaten sowie zwischen der NATO und Nicht-NATO-Organisationen eingesetzt werden. Gleichzeitig hat SecurePIM Government SDS auch hohe Relevanz für Firmen, die mit NATO-Behörden zusammenarbeiten, sowie für Dienstleister und Unternehmen der Sicherheits- und Verteidigungsindustrie. Die Einstufung „NATO RESTRICTED" entspricht der deutschen Geheimhaltungsstufe VS-NfD (VS-NUR FÜR DEN DIENSTGEBRAUCH).

Nachdem das BSI die Systemlösung für iOS bereits 2017 für die Geheimhaltungsstufe VS-NfD zugelassen hat, bedeutet das NATO-Siegel für Virtual Solution einen wichtigen Schritt im Rahmen des strategischen Ausbaus der internationalen Marktposition. SecurePIM Government SDS ist die einzige iOS-Lösung, die neben der VS-NfD Zulassung auch die Klassifizierung „NATO RESTRICTED" erhalten hat. Die Android-Version hat im März 2020 die Freigabeempfehlung für VS-NfD erhalten und befindet sich in der Endphase des Zulassungsprozesses.

Damit ist SecurePIM Government SDS prädestiniert für den Einsatz in der länderübergreifenden Kommunikation zwischen Behörden, in der sicherheitsbetreuten Industrie und auch im Umfeld kritischer Infrastrukturen (KRITIS). Durch die einfache Handhabung ist die Container-Lösung besonders anwenderfreundlich, kaum anfällig für Fehlbedienungen und erhöht damit gleichzeitig Akzeptanz und Sicherheit. Die gesamte Kommunikation und alle Datenzugriffe erfolgen über einen hochsicher verschlüsselten eigenen Bereich.

Über Virtual Solution

Virtual Solution ist ein auf sichere mobile Anwendungen spezialisiertes Softwareunternehmen mit Sitz in München und Entwicklungsstandort in Berlin. Das Unternehmen entwickelt und vertreibt die Applikationen SecurePIM, SecureCOM und die Sicherheitsarchitektur SERA für iOS und Android.

Weitere Informationen: *https://www.virtual-solution.com/mobile-kommunikation-fuer-behoerden/*

Veranstaltungskalender

9 | 2021

Veranstaltungen September		
Zeit und Ort	**Thema der Veranstaltung**	**Veranstalter**
01. – 03. September 2021 in Bochum	Cybersecurity-Awareness-Beauftragter (TÜV) -Informationssicherheit	isits AG International School of IT Security Huestr. 30, 44787 Bochum Tel,; 0234/927898-0: Fax: 0234/927898-20
01. – 03. September 2021 in Köln	Cyber-Security für Versicherer	VdS – Bildungszentrum, Pasteurstr. 17 a, 50735 Köln Tel.: 0221/7766-555; Fax: 0221/7766-499 E-Mail: lehrgang@vds.de
06. September 2021 Online	Ausbildung zum IT Risk Manager gemäß ISO 31000, ISO 27005 und BSI IT-Grundschutz (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
08. –10. September 2021 in Berlin	Sicherheit in IP-Netzen – Firewalls und Intrusion Detection, sichere Netzwerke	SMLan – Software & Management Training Kastanienallee 53, 10119 Berlin Tel.: 030/4492545; Fax: 030/443404358
13. – 15. September 2021 in Berlin	Wireshark Datenextrahierung	allskills Training Kastanienallee 53, 10119 Berlin Tel.: 030/4492545; Fax: 030/443404358
13. – 17. September 2021 Online-Seminar	ISMS Auditor/Lead Auditor nach ISO/IEC 27001 (IRCA) – Informationssicherheitsmanagementsystem	isits AG International School of IT Security Huestr. 30, 44787 Bochum Tel: 0234/927898-0: Fax: 0234/927898-20
13. – 14. September 2021 in Berlin	IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
14. – 15. September 2021 in Berlin	Check Point Certified Endpoint Specialist R80.X	allskills Training Kastanienallee 53, 10119 Berlin Tel.: 030/4492545; Fax: 030/443404358
20. – 24. September 2021 in Karlsruhe	T.I.S.P. – TeleTrusT Information Security Professional	Secorvo Security Consulting GmbH Ettlinger Straße 12-14, 76137 Karlsruhe Tel.: 0721/255171-0; Fax: 0721/255171-100
20. – 23. September 2021 Online	Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) gemäß ISO und BSI IT-Grundschutz (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
21. – 24. September 2021 in Ludwigsburg	Hacking Extrem	cirosec GmbH Ferdinand-Braun-Str.4, 74074 Heilbronn Tel.: 07131/594550; Fax: 07131/59455-99 E-Mail; info@cirosec.de
22. – 23. September 2021 in Köln	Crashkurs IT- und Informationssicherheit – Bedrohungen und Maßnahmen heute	cirosec GmbH Ferdinand-Braun-Str.4, 74074 Heilbronn Tel.: 07131/594550; Fax: 07131/59455-99 E-Mail; info@cirosec.de
23. September 2021 Web-Seminar	Netzwerksicherheit – Grundkenntniss	isits AG International School of IT Security Huestr. 30, 44787 Bochum Tel,; 0234/927898-0: Fax: 0234/927898-20
23. September 2021 in Berlin	Elektronische Signatur und Vertrauensdienste – TeleTrusT/ VOI-Informationstag	Bundesverband IT-Sicherheit e.V. (TeleTrusT) Chausseestraße 14, 10115 Berlin Tel.: 0241/8946822; Fax: 030/40054311
27. – 30. September 2021 Online	Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
28. – 30. September 2021 in Karlsruhe	IT Security Insights – T.I.S.P. Update -Aktuelles für IT-Sicherheitsverantwortliche	Secorvo Security Consulting GmbH Ettlinger Straße 12-14, 76137 Karlsruhe Tel.: 0721/255171-0; Fax: 0721/255171-100
28. September 2021 Online	FIT FOR IEC 62443	TÜV Informationstechnik GmbH Langemarckstr. 20, 45141 Essen Tel.: 0201/8999-404; Fax: 0201/8999-888 E-Mail: info@tuvit.de

DATENSCHUTZ UND DATENSICHERHEIT

DuD – Datenschutz und Datensicherheit
Recht und Sicherheit in Informationsverarbeitung und Kommunikation
Ausgabe 9/2021, 45. 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 2021 EUR 315,51
Jahresabonnement 2021 (Firmen, Institutionen und Bibliotheken) EUR 630,23
Jahresabonnement 2021 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 liegen Beilagen der Kunden Verlag Dr. Otto Schmidt KG aus Köln und Nomos Verlagsgesellschaft mbH & Co. KG aus Baden-Baden bei. Wir bitten unsere Leser und Leserinnen um Beachtung.