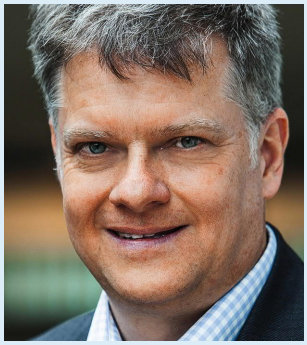
secorvo
security consulting

Secorvo Security News

Januar 2021



Gretchenfrage

Die nicht unerwartete Außerkraftsetzung des Privacy Shields durch den EuGH hat eine Welle von Vertragsneugestaltungen und viel Unsicherheit ausgelöst. Darf man personenbezogene Daten noch von US-Unternehmen verarbeiten lassen? Und wenn ja: wie?

Dabei gerät zunehmend die entscheidende Frage aus dem Blick. Denn worum geht es im Kern? Wir möchten einem fremden Dritten Daten anvertrauen, für die wir verantwortlich sind – und es, Vertrag hin oder her, auch bleiben. Die von der DSGVO geforderten vertraglichen Vereinbarungen und technisch-organisatorischen Zusicherungen, die wir mit dem Verarbeiter abschließen, sind dabei nur ein Instrument, um die Vertrauenswürdigkeit des Dritten zu untermauern. Sie sollten selbstverständlich sein.

Denn jedes Vertrauen braucht Fundierung: langjährige Zusammenarbeit, eigene Inspektion (Audits), Prüfung durch anerkannte Institutionen (Zertifikate), klare Vereinbarungen und rechtliche Absicherungen. Und selbst dann ist ein wenig verbleibende Skepsis kein Fehler.

Doch vertrauensbildende Maßnahmen erfordern die tiefere Beschäftigung mit Dienst und Dienstleister – keine gute Überlebensbedingung in einer schnelllebigen Zeit. Daher mutiert unser immer blinderes Vertrauen in die IT (in Programme, in Dienste und in Dienstleister) zu Vertrauensseligkeit. Ein perfekter „Nährboden“ für Täuschung und Betrug, siehe Enron, FlowTex oder Wirecard.

Während nicht nur unsere Abhängigkeit von der IT sondern auch die von kaum noch austauschbaren Diensten wächst, schrumpft zugleich das Fundament, auf dem Zusammenarbeit immer gründen sollte: solides Vertrauen. Wer seine Risiken beherrschen will, sollte sich daher häufiger die Frage stellen: Vertraue ich diesem Dienst, dieser Software wirklich? Und wenn die Antwort kein klares „Ja“ ist, sollte man sich besser damit beschäftigen. Oder zumindest nicht verwundert die Augen aufreißen, wenn der Blindflug schief geht.

Inhalt

secorvo
security consulting

Security News

Datenschutz im Homeoffice

Am 27.01.2021 trat die SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) des Bundesministeriums für Arbeit und Soziales in Kraft, befristet bis zum 15.03.2021. Nach § 2 Abs. 4 „hat der Arbeitgeber den Beschäftigten im Fall der Büroarbeit oder vergleichbaren Tätigkeiten anzubieten, diese Tätigkeiten in deren Wohnung auszuführen, wenn keine zwingenden betriebsbedingten Gründe entgegenstehen“. Homeoffice kann Telearbeit oder mobiles Arbeiten sein – in jedem Fall trägt der Arbeitgeber die datenschutzrechtliche Verantwortung. Dabei sind besondere Schutzmaßnahmen angezeigt. Die Checkliste des Bayerischen Landesamts für Datenschutzaufsicht kann dabei eine Hilfestellung sein.

Aus rechtlicher Perspektive ist die Norm problematisch, weil die Begrifflichkeiten des § 2 Abs. 4 teilweise unbestimmt sind. Was ist unter „zwingenden betriebsbedingten Gründen“ zu verstehen? Genügt es bereits, wenn im Homeoffice dem Datenschutz nicht hinreichend Rechnung getragen werden kann? Dann könnten sich fast alle Arbeitgeber auf den Ausnahmetatbestand berufen, denn eine gleichwertig sichere Infrastruktur ist zuhause selten gegeben.

DNSpooq

Ende Januar 2021 veröffentlichten Sicherheitsforscher von JSOF unter dem Namen DNSpooq sieben Schwachstellen für den DNS-Server dnsmasq, der in eingebetteten Systemen wie Routern und IoT-Geräten weit verbreitet ist. Meist übernimmt er darin die Rolle des DNS-Forwarders und leitet Namensanfragen zur Auflösung an DNS-Server weiter; die Antworten hält er in einem Cache vor. in einem Whitepaper erläutern die Forscher, wie die gefundenen Schwachstellen kombiniert werden können, um gefälschte Einträge in diesen Cache einzuschleusen. Damit tritt dieser Cache-Poisoning-Angriff in die Fußstapfen des 2008 von Dan Kaminski gezeigten Angriffs auf DNS. Die Angriffe können über das Internet, aus dem lokalen Netz oder sogar vom Browser des Opfers aus erfolgen.

Dagegen schützen würde der flächendeckende Einsatz von HSTS oder DNSSEC, die jedoch noch viel zu selten eingesetzt werden. Doch auch in der DNSSEC-Implementierung von dnsmasq entdeckten die Forscher Buffer Overflows, die es einem Angreifer ermöglichen könnten, Server aus der Ferne zu übernehmen. Von den Schwachstellen sind mehr als 40 Hersteller betroffen, von denen einige bereits aktualisierte Software zur Verfügung stellen. Doch ist zu vermuten, dass viele eingebettete Geräte verwundbar bleiben, da sie keine Updates erhalten. Schlimmstenfalls muss man die Geräte ersetzen. Wer Sicherheits-Schrott kauft, kauft oft zweimal.

Post-Brexit-Datenschutz

Am 01.01.2021 begann die Übergangsfrist von vier Monaten, innerhalb derer die Übermittlung von personenbezogenen Daten in das Vereinigte Königreich Großbritannien und Nordirland noch als Übermittlung innerhalb der EU behandelt werden darf (siehe Art. FINPROV.10A Abs. 4 b) des Handels- und Kooperationsabkommens vom 30.12.2020). Sofern weder die EU noch Großbritannien widersprechen, kann die Übergangsfrist um weitere zwei Monate verlängert werden.

Anschließend wird das Vereinigte Königreich in Bezug auf die Übermittlung von personenbezogenen Daten ein Drittland sein. Dann wird es zusätzlicher Garantien (Art. 44 ff DSGVO) für die Datenübermittlung bedürfen. Diese könnten in einem das Vereinigte Königreich betreffenden Angemessenheitsbeschluss (Art. 45 DSGVO) bestehen. Auch ohne Angemessenheitsbeschluss kann die Datenübermittlung zulässig sein, wenn ein Vertrag nach den Standardvertragsklauseln geschlossen wird. Dabei kann es allerdings erforderlich sein, dass deren effektive Einhaltung durch weitere Maßnahmen sichergestellt wird.

Unerwünschte Anrufe

Am 04.01.2021 teilte die Bundesnetzagentur mit, dass sie gegen den Betreiber eines Call-Centers ein Bußgeld in Höhe von 145.000 Euro verhängt hat. Dessen Anrufe dienten u. a. der Neukundenakquise für einen Pay-TV Anbieter. Weder Call-Center noch Auftraggeber hatten vor dem Kauf der Adressdaten geprüft, ob die angeblich erteilten Werbeeinwilligungen auch tatsächlich vorlagen. Dies ist aber im B2C-Bereich unerlässliche Voraussetzung für datenschutz- und wettbewerbsrechtlich zulässige Werbeanrufe. Auch im B2B-Bereich werden die Grenzen der mutmaßlichen Einwilligung von den Gerichten sehr eng gesteckt. Adresskauf und Auftrag entbinden den Werbetreibenden nicht von der Pflicht, die Einwilligungen nachzuweisen.

Vor einer anderen Art unerwünschter Anrufe, auch als Vishing (Voice Phishing) bezeichnet, warnte das FBI am 14.01.2021 in einer PIN (Private Industry Notification)-Warnung: Durch Anrufe über VoIP-Systeme wird versucht, ähnlich wie mit Links in Phishing-Mails, Angestellte dazu zu verleiten, Webseiten zu besuchen, auf denen Zugangsdaten abgefischt werden. Ähnliche Angriffe gibt es seit Jahren im privaten Bereich (z. B. von angeblichen Mitarbei-

tern des Microsoft-Support) – eine offenbar nach wie vor erfolgreiche Masche.

BSI-Standard zu BCM 2.0

13 Jahre nach der Veröffentlichung des IT-Grundschutz-Standards 100-4: Notfallmanagement hat das BSI am 19.01.2021 dessen grundlegende Überarbeitung als Community Draft BSI 200-4 Business Continuity Management (BCM) publiziert. Der Standard gibt auf 298 Seiten neben einer theoretischen Einordnung der verschiedenen BCM-Aspekte praktische Hilfestellung für den schrittweisen Aufbau eines BCM. Beispielsweise ist eine Abgrenzung zwischen BCM und IT-Service-Continuity-Management (ITSCM) hilfreich, um falsche Erwartungen zu vermeiden.

Ähnlich wie beim modernisierten IT-Grundschutz im Standard 200-2 werden verschiedene Ausbaustufen eines BCM vorgestellt und deren Vorteile und Grenzen beschrieben. Diese Ausbaustufen erlauben einen Einstieg mit überschaubaren Aufwänden. Vor dem Hintergrund verschärfter Anforderungen an die Notfallvorsorge ist diese aktualisierte Handreichung sehr zu begrüßen. Fazit: Lesenswert.

BND im Visier

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat am 11.01.2021 eine Beschwerde der Organisation „Reporter ohne Grenzen“ und des Rechtsprofessors Niko Härting aus dem Jahr 2017 gegen die Überwachungspraktiken des Bundesnachrichtendienstes (BND) angenommen. Die Beschwerde betrifft die Befugnisse nach dem G10-Gesetz und die Frage, ob gegen die Überwachung von E-Mail, Post und Telekommunikation effektive Rechtsmittel zur Verfügung stehen.

Nun muss die Bundesregierung Stellung nehmen, inwieweit tatsächlich Nachrichten der Beschwerdeführer abgefangen wurden und ob ihnen ein effektives Rechtsmittel zur Verfügung gestanden hat, denn die vorbefassten Gerichte hatten einen direkten Nachweis der Beobachtung von den Beschwerdeführern verlangt.

Das anstehende Verfahren entbehrt nicht einer gewissen Ironie, da der EuGH in seinem Schrems-II Urteil wegen genau solcher Einblicksbefugnisse ohne adäquaten Rechtsschutz ein angemessenes Datenschutzniveau in den USA verneint und mit den geäußerten Zweifeln an dessen Herstellbarkeit mittels Standardvertragsklauseln große Rechtsunsicherheit geschaffen hat.

CrypTool in Java

Das erfolgreiche CrypTool-Projekt, das Professor Esslinger aus Siegen seit mehr als 20 Jahren mit einem Team ehrenamtlicher Mitwirkender vorantreibt, hat Ende November 2020 die Java-Version des Kryptologie-Lernprogramms publiziert. Sie ergänzt das Windows-CrypTool 2 um eine vom Betriebssystem unabhängige Version. Mit Release 2020.1 war es im März 2020 um zahlreiche Funktionen (wie zum Beispiel einem visualisierten Tutorial zur Differentiellen Kryptoanalyse) erweitert worden.

Secorvo News

Secorvo-Seminare

Trotz der erfreulicherweise sinkenden Infektionszahlen ist derzeit schwer vorhersehbar, wann wir unsere Präsenz-Seminare wieder durchführen können – noch sind Hotels und Gastronomie geschlossen. Dennoch planen wir.

Sofern auch Sie planen möchten, können Sie Ihre Seminarteilnahme gerne buchen – selbstverständlich stornieren wir Ihre Buchung kostenfrei, wenn Ihnen die Teilnahme oder uns die Durchführung des Seminars aufgrund der Pandemie-Maßnahmen nicht möglich sein sollte.

Im September 2020 konnten wir unsere Infektionsschutzmaßnahmen noch auf mehreren Seminaren erfolgreich umsetzen: Durch eine Begrenzung der maximalen Teilnehmerzahl, interne „Wegführungen“, Lüftungspausen und Desinfektionsmaßnahmen sorgen wir während der Seminare für einen wirksamen Infektionsschutz.

Krypto-at-Home

Über 4.700 Schülerinnen und Schüler sowie ältere Kryptografie-Fans tauchten im Advent 2020 in die Welt der Verschlüsselung ein: Ein erneuter Teilnahmerekord bei unserem Online-Adventskalender "Krypto im Advent".

Als Beitrag der KA-IT-Si zum Home-Schooling haben wir nun die 36 Rätsel (und Lösungen) zusammengefasst und zum Download und Nachrätseln unter www.krypto-im-advent.de bereitgestellt. Perfektes Lernmaterial – nicht nur für den Informatik-Unterricht in den siebten Klassen. Verraten Sie es gerne weiter!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-26.02.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, virtuell)
März 2021	
15.-18.03.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
23.-25.03.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-21.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
27.-30.04.	BvD Verbandstag 2021 (BvD, Berlin)

Impressum

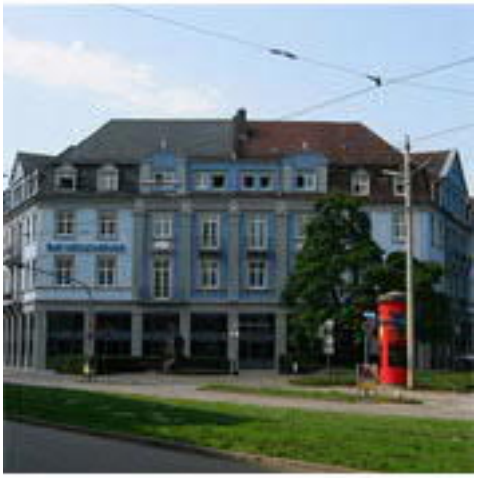
Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

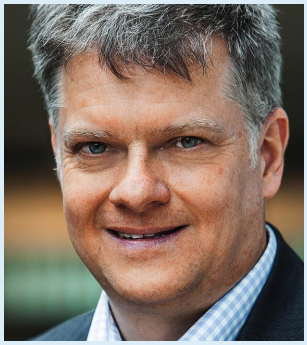
Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Februar 2021



Die schlechte gute Nachricht

Der 13.05.2019 dürfte in die Annalen des Heise-Verlags eingegangen sein. An diesem Montag schlug „Emotet“ im Verlagsnetz ein und bewies, dass auch ein technisch kompetentes und sicherheitsbewusstes Unternehmen zum Opfer werden kann. Anders als die meisten Emotet-Geschädigten ging der Verlag an die Öffentlichkeit und berichtete in schonungsloser Offenheit über den Vorfall, die eigenen Fehler und seine „Lessons learned“. Was dabei deutlich wurde: Die Hacker nutzten jeden Fehler und jede noch so kleine Nachlässigkeit, um sich nach ihrem Eindringen im Netz festzusetzen.

2014 hatte „Emotet“ begonnen, seine Trojaner-Infrastruktur zu einer Art „Cloud-Service für Angreifer“ auszubauen. Mit gut gemachten Spear-Phishing-Angriffen, die aus den E-Mails anderer Opfer konstruiert wurden, und bösartigen Makros in angehängten Office-Dateien hatte sich die Gruppe Zugang zu zigtausend IT-Systemen von Privatpersonen, Unternehmen und Behörden verschafft und „vermietete“ die Zugänge an Kriminelle zur Einschleusung von Online-Banking-Malware oder Verschlüsselungstrojanern.

Am 27.01.2021 meldete das Bundeskriminalamt, das seit 2018 gegen Emotet ermittelt hatte, dass es zusammen mit Europol deren Infrastruktur „ausgehoben“ habe. Die Zerschlagung stelle „eine wesentliche Verbesserung der Cybersicherheit in Deutschland dar“. Also „Ende gut, alles gut“? Ist das wirklich so? Seit Anfang Februar wertet das BSI die auf den Emotet-Servern entdeckten Credentials aus, die die Trojaner bei ihren Opfern „eingesammelt“ hatten, und informiert die betroffenen Unternehmen. Dabei zeigt sich, dass das erfolgreiche „Einnisten“ von Emotet in tausenden Unternehmen offenbar nicht einmal bemerkt worden war – zigtausend „Schläfer“-Rechner warteten noch immer auf ihren Einsatz.

Das ist keine gute Nachricht. Denn durch das Ausschalten eines einzelnen Angreifers verbessert sich die Cybersicherheit natürlich nicht. Sondern nur durch einen wirksameren Schutz der IT-Systeme.

Inhalt

secorvo
security consulting

Security News

„Human Supply Chain" Attack

Am 05.02.2021 versuchten Angreifer, in einer Wasseraufbereitungsanlage in Oldsmar (Florida) die chemische Zusammensetzung des Wassers zu verändern. Der Angriff wurde von einem Mitarbeiter erkannt, der die Mauszeigerbewegungen und eine Misstrauen erweckende Veränderung des Natriumhydroxid-Anteils bemerkte. Daraufhin setzte er diesen zurück und meldete den Vorfall. Einem Advisory des Massachusetts Department of Environmental Protection zufolge erfolgte der Angriff über einen TeamViewer-Zugang; drei Tage zuvor hatte es Datenleaks gegeben, die auch Credentials für die Wasseraufbereitungsanlage in Oldsmar enthielten.

Der Vorfall macht deutlich, wie wichtig es ist, dass kritische Industrial Control Systems nicht nur erfahrenes Personal und bspw. Intrusion-Detection-Systeme oder SIEM einsetzen, sondern auf diversitären Architekturen basieren. Eine Infrastruktur, die an verschiedenen Stellen getrennte Systeme verwendet, erlaubt es, gefälschte Werte, die (ähnlich wie bei Stuxnet) über ein kompromittiertes System eingespielt werden, auf Plausibilität zu prüfen und Abweichungen zu erkennen.

Zusätzlich empfehlen wir allen Betreibern kritischer Systeme die Beachtung gängiger Best Practices: So sollten Management-Schnittstellen nicht nach außen exponiert und Remote-Zugänge – falls überhaupt erforderlich – bestmöglich abgesichert werden. Hierzu gehört das Erzwingen starker Authentifizierungsmechanismen bspw. über eine Multi-Faktor-Authentifizierung und die strenge Kontrolle des Ursprungs der Authentifizierungs-Anfrage (Einschränkung auf IP-Bereiche und Geräte). Auch eine bedarfsabhängige Aktivierung des Remote-Zugangs verringert die Angriffsfläche. Passwörter sollten zudem nicht nur stark sein, sondern dürfen auch nicht geteilt werden, da sonst eine Zuordnung zu Benutzern und ein differenziertes Berechtigungsmanagement unmöglich sind.

Troja-X

Das 2019 gestartete europäische Projekt Gaia-X soll eine europäische Dateninfrastruktur der Zukunft entwickeln, die eine europaweite „digitale Souveränität" von Unternehmen und Geschäftsmodellen ermöglicht. Es soll sich an sieben Leitprinzipien ausrichten, zu denen insbesondere der „europäische Datenschutz" und „Offenheit und Transparenz" zählen. Bislang haben sich dem Projekt über 300 Organisationen aus ganz Europa angeschlossen.

Ob das Projekt mehr ist als politisches Marketing muss sich jedoch noch erweisen. So löste am 18.11.2020 eine Mitteilung der Nachrichtenagentur Dow Jones News über die Beteiligung des amerikanischen Big-Data-Unternehmens Palantir, der Cloud-Anbieter Microsoft, Amazon und Google sowie des chinesischen Unternehmens Huawei Diskussionen aus – sollte Gaia-X europäische Unternehmen und Behörden doch gerade von Anbietern unabhängig machen, deren Sicherheits- und Datenschutzniveau aufgrund staatlicher Eingriffsbefugnisse wie dem US-CLOUD Act in Zweifel stehen. Mit zu viel Offenheit wird aus Gaia-X jedenfalls bald ein Troja-X.

Rechtmäßigkeit der Verarbeitung

In einem am 11.01.2021 veröffentlichten Beschluss stellt das Verwaltungsgericht (VG) Wiesbaden fest, dass bei der Bearbeitung eines Löschbegehrens immer „erneut" die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DSGVO zu prüfen sei. Die ist sowohl vor Beginn einer Datenverarbeitung als auch anschließend regelmäßig zu prüfen; dasselbe gilt für die Angemessenheit der festgelegten Löschfrist.

Erreicht eine verantwortliche Stelle ein Löschbegehren, hat sie nach Auffassung des VG zunächst zu prüfen, ob die Voraussetzungen für eine rechtmäßige Datenverarbeitung noch vorliegen – und erst dann, ob diese dem Löschersuchen entgegenstehen. Anderenfalls ist die Verarbeitung ohnehin zu beenden und sind die Daten zu löschen.

Grundschutz-Kompendium 2021

Am 01.02.2021 veröffentlichte das BSI die jährliche Überarbeitung und Erweiterung des IT-Grundschutz-Kompendiums. Auf den ersten Blick überrascht der neue Baustein „INF.11 Allgemeines Fahrzeug". Da moderne Fahrzeuge eher einem Rechenzentrum mit vier Rädern ähneln, ist es jedoch sinnvoll, daran IT-Sicherheitsanforderungen zu stellen.

Nicht in diese Edition geschafft hat es der Baustein „SYS.1.2.3: Windows Server 2019", der bereits als Community Draft vorliegt. Die Verschiebung des Bausteins „APP.6 Allgemeine Software", der bisher auf anderer Ebene (CON.4) angesiedelt war, ist zu begrüßen; daraus ergeben sich Vorteile bei der Modellierung und den Soll-Ist-Vergleichen. Und der ehemalige Katalogbaustein „B 5.25 Allgemeine Anwendungen" hat nun einen Nachfolger; das hilft bei Migrationen.

Wie gewohnt sind alle im Kompendium vorgenommenen Verbesserungen systematisch in einem Änderungsdokument zusammengefasst. Das vereinfacht die Fortschreibung von IT-Sicherheitskonzepten. Fazit: Klasse.

Verzagte Neuregelung

Das Bundeskabinett beschloss am 10.02.2021 nach Eingang von 31 Stellungnahmen einen Entwurf für ein „Gesetz zur Regelung des Datenschutzes [...] in der Telekommunikation und bei Telemedien“ (TTDSG). Das Gesetz soll die bislang im Telekommunikationsgesetz (TKG) geregelten Datenschutzbestimmungen in einem Gesetz mit dem teilweise neu zu regelnden Datenschutz des Telemediengesetzes (TMG) zusammenführen. Die Anpassung des TKG setzt (verspätet) die europäische Richtlinie 2018/1972 über einen Kodex für elektronische Kommunikation vom 11.12.2018 um.

Der Entwurf enthält in § 24 eine neue Einwilligungsregelung zur Verwendung von Cookies und bereits im Endgerät gespeicherten Informationen. Die bisherigen Regelungen zum technischen und organisatorischen Datenschutz aus § 13 TMG werden teilweise gekürzt, dafür wird ein Auskunftsverfahren für Bestands- und Nutzungsdaten von Telemediendiensten umfangreich neu geregelt.

Was der Entwurf versäumt ist die Abgrenzung und Neuaufteilung der Pflichten zwischen Telekommunikations- und Telemediendiensten, für die die neuen Begriffsbestimmungen des Kodex für elektronische Kommunikation einen Ansatzpunkt bieten. So ist es beispielsweise an der Zeit, E-Mail-, Messenger- und Videokonferenzdienste als interpersonelle Kommunikationsdienste neu einzuordnen. Stattdessen kreist der Entwurf um neue Eingriffsbefugnisse und Datenschutzeinschränkungen.

Selbstverständliche Best Practices

Über Sinn und Unsinn von (immer wieder neuen) IT-Sicherheits-Checklisten kann man trefflich streiten. Das trifft auch auf die vom Bayrischen Landesdatenschutzbeauftragten bereits am 27.05.2020 veröffentlichte fünfseitige Checkliste zur „Cybersicherheit für medizinische Einrichtungen“ zu.

Sie ist eine übersichtliche Zusammenstellung geeigneter Schutzmaßnahmen. Allerdings sollte nicht der Eindruck entstehen, dass die Liste alle, nicht einmal alle wesentlichen Anforderungen abdeckt. Wie in der Einleitung angemerkt liegt der Fokus auf der Verfügbarkeit der verarbeiteten (personenbezogenen) Daten und weniger auf den in diesem Kontext mindestens ebenso wichtigen Zielen Integrität und Vertraulichkeit.

Die zahlreichen Verweise auf das IT-Grundschutz-Kompendium sind zweifellos sinnvoll, werfen aber die Frage auf, ob die Checkliste eher als „Lesehilfe“ für medizinische Einrichtungen gedacht ist, die sich die Mühe einer gründlichen Auseinandersetzung mit dem IT-Grundschutz ersparen möchten. Viele der in der Checkliste aufgeführten Punkte sind zudem simple Selbstverständlichkeiten („Empfehlung zur Vermeidung leicht zu erratender Passwörter oder Passwortbestandteile“), andere muten etwas merkwürdig an („Kenntnis der zuständigen Datenschutzaufsichtsbehörde“ – die sollte spätestens beim Lesen der Checkliste bekannt sein).

Hilfreicher erscheint die vom TeleTrusT Bundesverband IT-Sicherheit e. V. am 04.02.2021 in erweiterter Fassung (v1.8) veröffentlichte Handreichung zum „Stand der Technik in der IT-Sicherheit“ – mit 98 Seiten deutlich umfangreicher als die bayerische Checkliste, aber dafür eine umfassendere Zusammenstellung geeigneter technisch-organisatorischer Maßnahmen (TOMs).

Secorvo News

PKI, T.P.S.S.E. und T.I.S.P.

Unsere beiden Zertifizierungsseminare zum „TeleTrusT Information Security Professional“ (**03.–07.05.2021**) und zum „TeleTrusT Professional for Secure Software Engineering“ (**26.–29.04.2021**) sowie das Vertiefungsseminar zu Public-Key Infrastrukturen (**19.–22.04.2021**) hoffen wir wieder in bewährter Form und unter Einhaltung der Abstandsregelung als Präsenzveranstaltung durchführen zu können. Das Programm und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite. Teilnehmer des T.I.S.P.-Seminars erhalten nach Anmeldung zur Vorbereitung das T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“ zugesandt.

Lesen bildet

Der Ausfall zahlreicher Abendveranstaltungen hat die Bücherkäufe ansteigen lassen. Da wollen wir Sie nicht alleine lassen und laden Sie herzlich ein zum „1. Literarischen Kabinett“ der Karlsruher IT-Sicherheitsinitiative am 25.03.2021 um 18 Uhr (Teams). Sie werden zahlreiche Werke der Weltliteratur kennenlernen, die Sicherheits- und Datenschutzexperten gelesen haben müssen. Fünf Bücher werden wir etwas ausführlicher vorstellen – und freuen uns nicht nur auf Ihre Anmeldung, sondern auch über eine persönliche Rückmeldung: Welche Bücher gehören unbedingt auf diese Liste? Und: Haben Sie Lust, Ihr eigenes Lieblingsbuch, das Sie im Hinblick auf IT-Sicherheit oder Datenschutz nachdenklich oder betroffen gemacht hat, kurz in 10 Minuten vorzustellen? Dann schreiben Sie uns.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2021	
15.-18.03.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz/virtuell)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2021	
03.-07.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
12.05.	SecurityCruise (Connecting Media, Karlsruhe)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)

Fundsache

Datenschutz-Unterstützung für Vereine: Mit DS-GVO.clever bietet der LfDI Baden-Württemberg seit kurzem eine effiziente und effektive Hilfestellung für Vereine bei der Erstellung ihrer Datenschutzhinweise.

Impressum

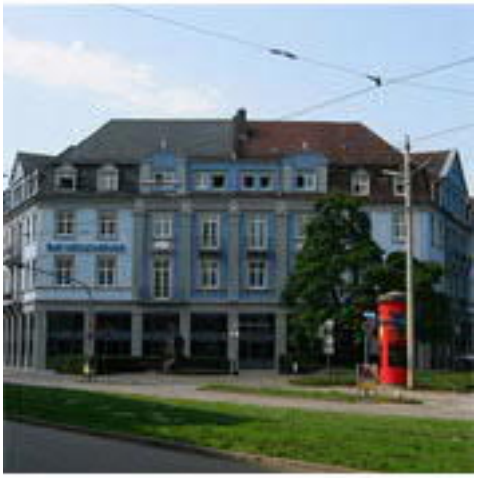
Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

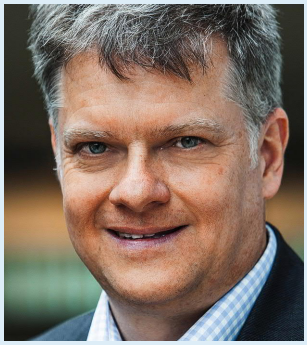
Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

März 2021



Hoheitsverhältnisse

Allen früheren Unkenrufen zum Trotz geht Deutschland „in die Cloud“: Spätestens seit Beginn der Pandemie schmelzen die ursprünglichen Bedenken deutscher Unternehmen wie Eis in der Sonne. Zugleich werden immer mehr Dienste (nur noch) Cloud-basiert angeboten.

Womöglich liegt das Cloud-Problem auch an ganz anderer Stelle als bisher diskutiert. Sicher, man muss dem externen Hoster seiner Daten vertrauen. Aber das galt schon, als Cloud-Dienste noch „Outsourcing“ hießen. Geändert hat sich aber, dass auch die Software „gemietet“ und vom Anbieter bereitgestellt wird. Und mit dem Versprechen, immer die aktuelle Version zur Verfügung gestellt zu bekommen, verschiebt sich die Hoheit über den Einsatz neuer Funktionen vom Nutzer zum Anbieter.

Wer in den vergangenen zwölf Monaten Microsoft Teams genutzt hat, konnte die kontinuierliche Weiterentwicklung der Videokonferenz-Software live miterleben: Fast täglich ändern sich Qualität und Details, oft zum Besseren – aber Einfluss hat der Kunde („Mieter“) darauf nicht. So bietet Teams seit Kurzem eine Transkriptions-Option: Auf Mausklick wird das gesprochene Wort in Text umgesetzt und als Untertitel angezeigt. Bisher funktioniert das nur bei amerikanischem Englisch halbwegs überzeugend. Aber das sind zweifellos Kinderkrankheiten, so wie die Tatsache, dass man zwar in den Einstellungen „Mich automatisch in Besprechungsuntertiteln und Transkriptionen identifizieren“ deaktivieren kann – Teams diese Einstellung aber im Hintergrund automatisch wieder aktiviert.

Ohne Zustimmung (und sogar gegen den Willen) des „Mieters“ überträgt Microsoft also die dem Fernmeldegeheimnis unterliegenden Inhalte der Telekommunikation an eine KI in der Cloud. Das fühlt sich ein wenig so an, als ließe ein Vermieter mal eben die Schlafzimmerwand durch eine transparente Glasscheibe ersetzen. Willkommen in der schönen neuen Welt.

Inhalt

secorvo
security consulting

Security News

Meldepflicht bei Schwachstellen

Am 05.03.2021 wies das BSI auf eine schwerwiegende Sicherheitslücke bei Microsoft Exchange hin. Anschließend äußerten sich verschiedene Datenschutzaufsichtsbehörden zu der Frage, ob die Anfälligkeit für eine solche Schwachstelle meldepflichtig ist. Zunächst ist vom Unternehmen eine Bewertung des Risikos für die (möglicherweise) Betroffenen vorzunehmen. Wird bei einer technischen Überprüfung der Systeme festgestellt, dass die Schwachstelle ausgenutzt wurde, muss – da sind sich die Aufsichtsbehörden einig – eine Meldung erfolgen. Ist keine Kompromittierung feststellbar und gibt es keine Hinweise darauf, dass ein Abfluss von personenbezogenen Daten stattgefunden hat, dann ist eine Meldung nach Art. 4 Nr. 12 DSGVO jedoch nicht zwingend.

Datenschutzkonformes Faxen?

Immer wieder wird diskutiert, ob der Versand personenbezogener Daten via Telefax datenschutzkonform ist. Am 01.03.2021 hat sich die Landesbeauftragte für Datenschutz und Informationsfreiheit von Bremen in einer Stellungnahme nun eindeutig positioniert und den Versand von Faxen als grundsätzlich datenschutzrechtlich unzulässig bewertet: Insbesondere wegen der zunehmenden Verwendung von Internet-Technologien und Computerfaxen sei der Versand nicht sicherer als eine Postkarte oder eine unverschlüsselte E-Mail.

In technischer Hinsicht „hinkt" der Vergleich jedoch erheblich. So ist heute für E-Mails – Edward Snowden sei Dank – eine Punkt-zu-Punkt-Verschlüsselung zwischen E-Mail-Servern Standard. Außerdem besteht bei Computerfaxen nicht mehr die Gefahr, dass ein Fax in allgemein zugänglichen Räumen eingeht und so von Unbefugten gelesen werden kann. Und schließlich nutzt die Faxübermittlung dieselbe Technologie wie ein Telefonat – die nach wie vor dem Telekommunikationsgeheimnis unterliegt. Insofern ist den Landesaufsichtsbehörden zuzustimmen, die hier etwas mehr Augenmaß anlegen: Es kommt darauf an, geeignete Sicherheitsmaßnahmen zu ergreifen. Dazu kann auch gehören, zu prüfen, ob es sicherere Möglichkeiten für den Versand eines Schriftstücks gibt.

Vom Pinguin zum Kaiserpinguin

Am 12.03.2021 veröffentlichten Sicherheitsforscher von GRIMM drei Schwachstellen im Linux Kernel, die kombiniert zu einer lokalen Erweiterung der Benutzerrechte (*Local Privilege Escalation*, LPE) führen können. Das Besondere an den Schwachstellen ist, dass sie seit 15 Jahren im für iSCSI und RDMA genutzen „ib_iser"-Kernelmodul stecken, das auf nicht speziell gehärteten Systemen auch von niedrig privilegierten Benutzern zur Laufzeit nachgeladen werden kann. Ein Proof of Concept Exploit ist bereits verfügbar und kann genutzt werden, um auf bestimmten Red Hat-, CentOS- und Fedora-Systemen Root-Rechte zu erlangen. Auch auf Debian- und Ubuntu-Systemen kann der Exploit funktionieren, erfordert allerdings einige Vorbedingungen wie z. B. am System angeschlossene RDMA-Hardware.

Die Schwachstelle hebelt auf vielen Linux-Systemen das Berechtigungskonzept komplett aus. Die entsprechenden Sicherheitsaktualisierungen sollten daher schnellstmöglich installiert werden. Zudem sollten weitere restriktive Maßnahmen getroffen werden, die auch ohne entsprechende Patches vor einer Ausnutzung geschützt hätten: Auch Linux-Systeme sollten so gehärtet sein, dass von einem (einfachen) Benutzer nur explizit erlaubter Code ausgeführt werden darf, beispielsweise mithilfe von grsecurity. Im konkreten Fall hätte das ein Nachladen des obskuren Kernelmoduls verhindert. Eine umfassende Überprüfung vorhandener Härtungsmaßnahmen ist z. B. mit dem freien Tool Lynis möglich.

Wieder Videokonferenzen

Die Berliner Landesdatenschutzbeauftragte hat nach den Erstauflagen von März und Juli 2020 ihre Bewertungsübersicht zu Videokonferenzangeboten im Ampelsystem am 18.02.2021 erneuert. Weiterhin stehen die Zeichen für alle größeren Anbieter auf rot. Unverändert wird die rechtliche Bewertung weitgehend auf die Vertragslage, vor allem das Vorliegen eines ausreichenden Auftragsverarbeitungsvertrages gestützt.

Damit setzt die Aufsichtsbehörde die Einstufung als Auftragsverarbeitung weiter unbegründet voraus; nur knapp wird auf künftige Änderungen durch die TKG-Novelle zur Umsetzung des Europäischen Telekommunikationskodex (siehe SSN 2/2021) eingegangen, auf das geplante TTDSG gar nicht.

Nach geltendem Recht sind Videokonferenzangebote Telemediendienste, je nach Konstellation auch schlicht Dienstleistungen. Zu begründen ist mindestens für Arbeitgeber die Übermittlung von Anmeldedaten an die Dienste. Doch Auftragsverarbeitung setzt eine weisungsgebundene Verarbeitung im Interesse und für Zwecke des Auftraggebers voraus. Da dies in vielen Fällen kaum konstruierbar ist, kann ein beanstandungsfreier AV-Vertrag kaum zustande kommen.

Unabhängig davon sind allerdings die regelmäßigen Transparenzprobleme bezüglich der Verarbeitung eine offene Flanke. Dieses Problem wird erst lösbar, wenn die Anbieter eine eigene, regulierte Stellung erhalten, die zu einer legitimen Übermittlung der Nutzungsdaten führt. Mit Geltung des aktuellen TKG-Entwurfs würden Videokonferenzdienste als „interpersonelle Kommunikationsdienste" unter das TKG und damit auch unter das neue Telekommunikationsdatenschutzrecht fallen. Dank gesetzlicher Rechtsgrundlage würde damit u. a. für Verkehrsdaten die Auftragsverarbeitung ohnehin entfallen.

Anspruch auf Negativauskunft

Am 03.02.2021 hat das AG Lehrte (Niedersachsen) entschieden, dass Betroffene nach Art. 15 Abs. 1.1. und 2. HS DSGVO das Recht haben, vom Verantwortlichen zu verlangen, dass dieser ihnen bestätigt, keine personenbezogenen Daten der Betroffenen zu verarbeiten. Kommt der Verantwortliche dem nicht nach, so hat er, wenn der Betroffene den Gerichtsweg einschlägt, die Kosten des Verfahrens zu tragen, deren Höhe sich nach dem vom Gericht festgelegten Streitwert bemisst.

Streitige Bußgelder

Nachdem bereits im November letzten Jahres mit dem Bußgeld gegen 1&1 ein hohes Bußgeld drastisch reduziert wurde, hat das LG Berlin nun mit Beschluss vom 18.02.2021 auch das Rekordbußgeld gegen die „Deutsche Wohnen SE" (15 Mio. €) aufgehoben. Noch ist das Verfahren offen, da die Staatsanwaltschaft Berlin Beschwerde eingelegt hat.

Anders als im 1&1-Fall (Verhältnismäßigkeit der Bußgeldhöhe) ist die Ursache diesmal ein rechtlich umstrittener Verfahrensfehler: Im Konflikt stehen hier Art. 83 DSGVO, der Bußgelder gegenüber den Verantwortlichen (juristischen Personen) vorsieht, und § 30 OWiG, der dafür ein Organverschulden voraussetzt. Da die Berliner Aufsichtsbehörde den Fall jedoch bereits vor Inkrafttreten der DSGVO angestoßen hatte, ist verwunderlich, dass sie diesbezüglich keine Ausführungen vorgelegt und offenbar nicht ermittelt hat. Für das Landgericht hätte sich allerdings die Frage einer Vorlage an den EuGH stellen müssen.

Zwar kann der Fall nicht als Argument für gute Erfolgschancen von Rechtsmitteln gegen hohe Datenschutz-Bußgelder herangezogen werden. Absehbar ist jedoch, auch wenn die endgültige Entscheidung noch auf sich warten lassen wird, dass die Aufsichtsbehörden künftig stärker das persönliche Verschulden von Geschäftsführungen und anderer Gesellschaftsorgane im Blick haben werden.

Secorvo News

PKI-Seminar online

Angesichts der großen Teilnahmezahlen bei unseren jüngsten Online-Events werden wir im April erstmals auch eines unserer Seminare online durchführen: Noch gibt es freie Plätze für das Seminar „Public Key Infrastrukturen – Grundlagen, Vertiefung, Realisierung„ vom **19. bis 22.04.2021** - Theorie und vertiefte Praxis mit unseren PKI-Experten. Das Seminar ist als Weiterbildung zur T.I.S.P.-Rezertifizierung anerkannt.

Das vollständige Programm und die Anmeldung finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme!

Heute schon gehackt?

Sie wollten schon immer einmal wissen, wie „Hacking" eigentlich funktioniert? Dann tauchen Sie gemeinsam mit uns in die Welt des Server-Hackings ab! Lernen Sie auf dem nächsten **KA-IT-Si-Event** am **29.04.2021** ab 18 Uhr, wie Hacker, Sicherheitsforscher und Penetrationstester Schwachstellen finden und ausnutzen.

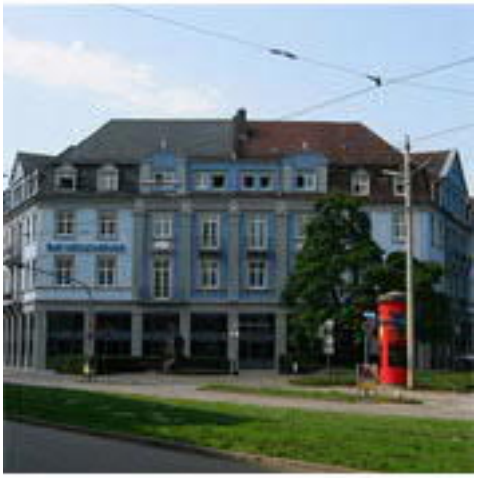
Fast jedes Unternehmen besitzt heutzutage eine IT-Infrastruktur, die in irgendeiner Weise mit dem Internet verbunden ist. Jede solche Anbindung kann ein Einfallstor für Angreifer darstellen. Anhand einer Live-Demonstration zeigen wir Ihnen, wie über das Internet erreichbare Systeme geprüft werden können und in welche Richtungen sich ein Penetrationstest in nachgelagerten Schritten weiter entwickeln kann. Zusätzlich werden Grenzen und Beschränkungen von Penetrationstests aufgezeigt, die dabei helfen können, das Mittel „Penetrationstest" als Sicherheitsmaßnahme besser zu verstehen und zu bewerten.

Bitte melden Sie sich **bis Freitag, 23.04.2021** für diese Veranstaltung an. Alle Teilnehmer erhalten auch diesmal wieder vorher eine kleine Überraschung per Post von uns.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, virtuell)
20.-22.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz/virtuell)
Mai 2021	
03.-07.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
12.05.	SecurityCruise (Connecting Media, Karlsruhe)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

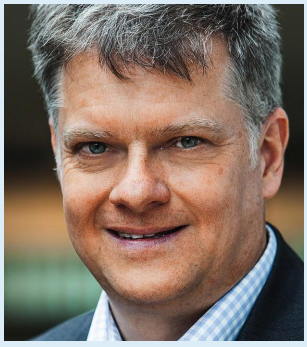
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

April 2021



Lesen bildet.

Häufig sind es Schriftsteller, die technische und gesellschaftliche Entwicklungen lange zuvor erahnen und beschreiben; manchmal prägen sie damit den gesellschaftlichen Diskurs der Technikfolgen. Kein Wunder, werden doch die theoretischen Möglichkeiten oft erst durch eine realistische Erzählung konkret vorstellbar. Gelingt es einem Autor dabei, in seiner Geschichte – meist einer Dystopie – die zentralen Fragen aufzuwerfen, kann eine solche Erzählung mehr Grundverständnis vermitteln als hundert Vorträge.

Das gilt vielleicht ganz besonders für den Datenschutz und die Informationssicherheit, leiden beide doch unter demselben Dilemma: Je erfolgreicher der Schutz, desto abstrakter und unkonkreter die Gefahr. Aus einer Diskussion mit Datenschutz- und Datensicherheitsexperten in Süddeutschland entstand daher kürzlich die folgende, zweifellos nicht vollständige Liste von zehn belletristischen Werken, die die Bedeutung von Datenschutz und Datensicherheit in besonders beeindruckender Weise konkret werden lassen:

1. George Orwell: 1984 (1948)
2. Clifford Stoll: Das Kuckucksei / Cuckoo's Egg (1989)
3. Robert Harris: Enigma (1995)
4. John Katzenbach: Der Patient (2006)
5. Jeffery Deaver: Der Täuscher (2009)
6. Marc Elsberg: Blackout (2012)
7. Dave Eggers: Der Circle (2013)
8. Marc Elsberg: ZERO (2014)
9. Marc-Uwe Kling: Quality Land (2017)
10. Andreas Eschbach: NSA (2018)

Einige werden Ihnen zweifellos bekannt sein. Die Lektüre der anderen legen wir Ihnen wärmstens ans Herz. Und wenn Sie das nächste Mal gefragt werden, warum Datenschutz oder Datensicherheit bloß so wichtig genommen werden: Empfehlen Sie einfach – ein Buch.

Inhalt

secorvo
security consulting

Security News

Urheberzensur

Am 11.03.2021 hat die „Clearingstelle Urheberrecht im Internet“ (CUII) ihre Arbeit aufgenommen. Ihr gehören Urheberrechtsvertreter (wie der Börsenverein des deutschen Buchhandels oder der Verband der Filmverleiher) sowie die größten deutschen Internet-Zugangsprovider an. Ihr Ziel: Die Ahndung von Urheberrechtsverletzungen im Internet in Gestalt von DNS-Sperren durch die Provider.

Voraussetzung für die Beantragung der Sperrung einer „strukturell urheberrechtsverletzenden Webseite“ (SUW) ist, dass die Inanspruchnahme des Webseitenbetreibers durch den Rechteinhaber keine Erfolgsaussichten hat, dieser aber „zumutbare Maßnahmen“ zur Aufdeckung der Identität des Webseitenbetreibers unternommen hat.

Die Entscheidung über eine Sperrung trifft ein Prüfausschuss einstimmig, den ein „unbefangener Vorsitzender“ mit Befähigung zum Richteramt leitet. Vor der Sperrung durch die Provider wird die Einhaltung der Netzneutralitätsvorgaben (EU 2015/2120) durch die Bundesnetzagentur geprüft. Ein sechsköpfiger Steuerkreis überwacht die Arbeit der CUII und beschließt über den Verhaltenskodex, in dem Antrags- und Sperrverfahren beschrieben sind.

Diese „Notwehrmaßnahme“ der Urheberrechtsinhaber hinterlässt trotz der Selbstbeschränkung auf jährlich maximal 200 Anträge einen schalen Beigeschmack, entscheidet doch ein privates Gremium statt unabhängiger Gerichte über die Zugänglichkeit von Webseiten – und damit über die Grundrechte Dritter, wie der Verfassungsblog am 24.03.2021 kritisierte.

Auch die Rolle der Bundesnetzagentur bleibt nebulös, denn sie ist „durch Briefwechsel“ nichtöffentlich vereinbart und schließt offenbar eine inhaltliche Prüfung der Sperrempfehlung nicht ein. Ein Verfahren also, bei dem sich erst erweisen muss, ob die Trennlinie zu „sonstigen unerwünschten Webseiten“ (SUW) klar gezogen bleibt.

Warnung vor IT-Produkten

Dürfen (Datenschutz-) Aufsichtsbehörden vor dem Einsatz bestimmter IT-Produkte warnen, wenn hierzu datenschutzrechtliche Bedenken bestehen? Die Zwischenergebnisse zu dieser Frage hat der Arbeitskreis (AK) “Grundsatz der DSK zu den Rahmenbedingungen für aufsichtsbehördliche Produktwarnungen der Datenschutzkonferenz” (DSK) bereits am 09.11.2020 in einem noch abzuschließenden Gutachten vorgestellt. Dabei wird auch die Frage beleuchtet, ob sich die aufsichtsrechtliche Legitimation aus Art. 57 Abs. 1 lit. b i.V.m. Art. 58 Abs. 3 lit. b DSGVO ergibt. Das Gutachten kommt zu dem Zwischenergebnis, dass eine Warnung unter drei Voraussetzungen rechtens sei:

- Richtigkeit der Information,
- Sachlichkeit der Information und
- Berücksichtigung des Verhältnismäßigkeitsgrundsatzes (Erforderlichkeit und Angemessenheit).

Überdies bestehe die Notwendigkeit der Überprüfung einer zeitlichen Befristung der Produktwarnung, die sich insbesondere aus § 40 Lebensmittel- und Futtermittelgesetzbuch (LFGB) ergebe. Noch nicht abschließend bewertet ist die Frage, ob den betroffenen Herstellern vor Publikation die Möglichkeit einer Stellungnahme gewährt werden sollte.

Noch gibt es zahlreiche offene Fragen. So werden nicht alle Aufsichtsbehörden dieselbe Einschätzung vertreten. Und welche Bewertungsmaßstäbe und -kriterien werden zu Grunde gelegt, um Einheitlichkeit und Vergleichbarkeit zu schaffen? Diese Fragen sollen auf der nächsten Datenschutzkonferenz am 28./29.04.2021 geklärt werden.

Trotz des offensichtlichen Nutzens einer im Idealfall einheitlichen Bewertung der Aufsichtsbehörden sind grundsätzliche Bedenken angebracht. Denn an Lebensmittelwarnungen werden sehr hohe Anforderungen gestellt, die weit über die des DSK hinausgehen: So müssen „hinreichende Anhaltspunkte dafür vorliegen, dass von einem Erzeugnis eine Gefährdung für die Sicherheit und Gesundheit ausgeht oder ausgegangen ist“. Ob Anhaltspunkte für eine Gefährdung beispielsweise bei den von der Berliner LDSI inkriminierten Videokonferenz-Lösungen (SSN 3/2021) vorliegen, muss ernsthaft bezweifelt werden.

Kryptotrojaner ohne Lösegeld

Danny Palmer beschrieb am 25.03.2021 auf ZDnet, wie die Firma Spectra Logic einen Kryptotrojaner loswurde – ohne Lösegeld zu bezahlen. Zwei Dinge waren dafür erforderlich: Die Entscheidung der Geschäftsführung gegen eine Lösegeldzahlung und eine IT-Abteilung, die bis zum Umfallen Überstunden machte, um die Firma wieder „ans Laufen“ zu bringen. Nach acht Tagen waren zumindest die wichtigsten Systeme wieder betriebsbereit. Das mutet an wie ein Königsweg – doch vor dem erleichterten Aufatmen sollte man zunächst drei Fragen beantworten:

- Wie würde Ihre Geschäftsführung entscheiden – für oder gegen eine Lösegeldzahlung?

- Gibt es in Ihrer IT-Abteilung Bereitschaftsregelungen für Notfälle? Können externe Dienstleister eingebunden werden – und wenn ja: welche und wie?
- Kennen Sie Ihre kritischen Prozesse und Systeme? Wie viele Tage würden Sie voraussichtlich benötigen, um die IT für die wesentlichen Geschäftsprozesse wiederherzustellen? Ab welcher Dauer ist ein IT-Ausfall existenzbedrohend?

Wer sich auf eine Selbstmedikation im Falle eines erfolgreichen Kryptotrojaner-Angriffs vorbereiten will, sollte sich dabei an Standards wie dem BSI-Standard 200-4 orientieren – und seine Backup- und Notfall-Pläne auch üben. So realistisch wie möglich. Und sie vor allem ausdrucken, damit der Kryptotrojaner sie nicht mitverschlüsselt.

TKG novelliert

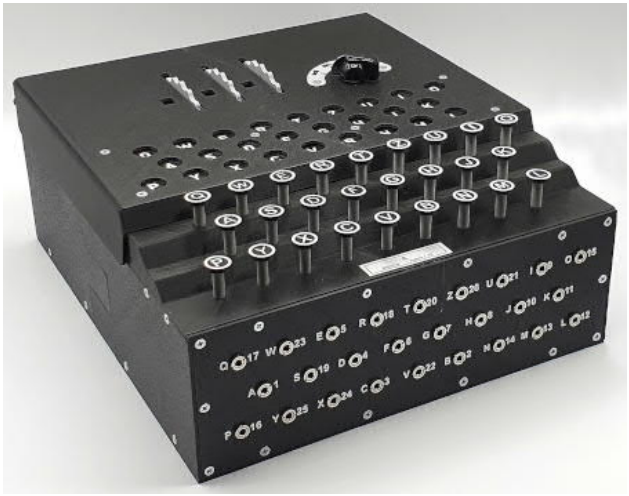
Am 22.04.2021 wurde die Novelle des Telekommunikationsgesetzes (TKG) verabschiedet. Wer gehofft hatte, dass damit Klarheit hinsichtlich der rechtlichen Behandlung von Videokonferenzen geschaffen würde, wurde enttäuscht. Aber es ist ein Trend erkennbar, der zumindest für das in Abstimmung befindliche Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) hoffen lässt. Mit den Regelungen über die sog. Universaldienste (§§ 78 ff. TKG) wird klar, dass die Ausweitung des Fernmeldegeheimnisses (§ 88 TKG) auf Anbieter von sog. Over-the-top-Diensten näher rückt.

Damit wäre die Forderung der Aufsichtsbehörden nach Auftragsverarbeitungsverträgen hinfällig: Die Verantwortlichkeit für die Sicherheit der Dienste läge bei den Dienstanbietern und nicht bei den Nutzern; zuständige Kontrollinstanz wäre die Bundesnetzagentur. Diese Entwicklung ist aus unserer Sicht dringend geboten und wird bereits seit langem gefordert (siehe z. B. das ZEW-Gutachten von Prof. Thomas Fetzer, Universität Mannheim, aus dem Jahr 2016).

Secorvo News

Enigma zum Selberdrucken

Die ENIGMA zählt zweifellos zu den faszinierendsten Verschlüsselungsverfahren in der Geschichte der Kryptografie. Berühmt wurde sie nicht nur durch ihre bedeutende Rolle im Zweiten Weltkrieg, sondern vor allem auch durch ihre geniale Entschlüsselung unter Mitwirkung des Informatik-Pioniers Alan Turing.



Enigma I aus dem 3D-Drucker (Foto: Prof. Wiest)

Seit 2017 rekonstruieren Studierende der Hochschule der Medien in Stuttgart im Projekt „ENIGMA R.D.E." diese berühmteste Chiffriermaschine der Welt, von der nur wenige Originalgeräte erhalten sind, im 3D-Druckverfahren. Ziel ist eine Konstruktionsanleitung, mit der Laien für unter 300 € Materialkosten ein funktionierendes Gerät in Originalmaßen anfertigen können. Das Projekt wurde 2019 mit dem Landeslehrpreis des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg ausgezeichnet.

Die Veröffentlichung der Anleitung ist für den Spätsommer 2021 geplant. Bei unserem kommenden KA-IT-Si-Event am **20.05.2021** dürfen Sie bereits einen Blick auf ein funktionierendes Modell werfen: Prof. Wiest wird von der bewegten Geschichte des Projekts berichten, gibt Einblicke in die Besonderheiten des Nachbaus und entschlüsselt selbstverständlich auch live Geheimbotschaften mit seiner ENIGMA.

Diesmal erhalten Sie kurz vor dem Event nicht nur eine kleine Stärkung per Post von uns, sondern auch Ihre ganz persönliche Enigma, damit Sie die Nachricht des Referenten entschlüsseln können. Lassen Sie sich überraschen! Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen – nach den überwältigenden Teilnehmerzahlen der letzten Events auch diesmal online – und kostenlos (zur Anmeldung).

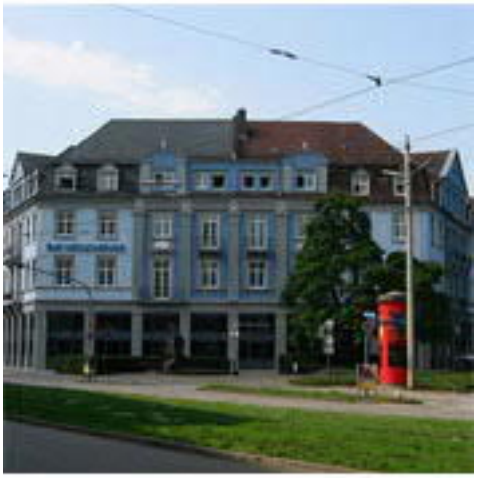
Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2021	
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
17.-20.05.	Security Cruise (Connecting Media, virtuell)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)
20.05.	Enigma zum Selberdrucken (KA-IT-Si, virtuell)
Juni 2021	
08.06.	Datenschutztag 2021 (COMPUTAS, Berlin)>
09.-11.06.	Entwicklertag 2021 (VKSI, GI, ObjektForum , virtuell)
14.-15.06.	DuD 2021 (COMPUTAS, Berlin)
17.-18.06.	Annual Privacy Forum 2021 (ENISA, DG Connect, Católica University of Portugal, virtuell)

Fundsache

Neben Kali Linux gibt es weitere Linux-Distributionen, die einen umfassenden Werkzeugkasten für Penetrationstester bieten, wie beispielsweise BlackArch und Parrot OS. Von letzterer erschien am 28.03.2021 Version 4.11. Zu den Änderungen zählen sowohl eine Vielzahl aktualisierter und besser kurierter Hacking-Werkzeuge als auch der Umstieg auf eine LTS-Version. Auch ARM-Architekturen werden wieder unterstützt. Wer in der Vergangenheit Schwierigkeiten mit Kali hatte, dem sei Parrot OS ans Herz gelegt – unseren Erfahrungen nach ist Parrot OS an einigen Stellen gepflegter, zuverlässiger und stabiler.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

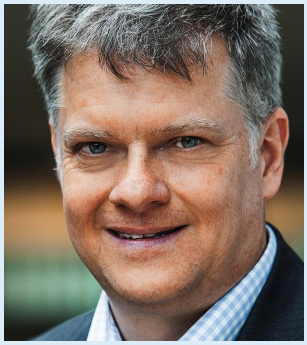
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Mai 2021



Zweck verfehlt

Am vergangenen Samstag erhielt ich im Zusammenhang mit einer Erbschaftsangelegenheit ein Schreiben von einem Finanzinstitut, bei dem ich bisher kein Kunde war. Betreff: „Datenschutzhinweise“. Sie ahnen, was beilag: Fünf eng bedruckte Seiten „zur Kenntnisnahme und für Ihre Unterlagen“. Immerhin nur fünf, dachte ich fast erleichtert.

Ähnliche Schreiben wurden seit Inkrafttreten der DSGVO millionenfach versandt. Sie dienen der Erfüllung der Informationspflicht aus Art. 13 DSGVO: Danach müssen Betroffene zu Beginn einer Verarbeitung erfahren, welche personenbezogenen Daten zu welchen Zwecken verarbeitet werden.

Ein wichtiges Prinzip des Datenschutzes: Transparenz. Nur: In dieser Umsetzung degeneriert es zur Farce, zu einer gigantischen Vergeudung von Ressourcen – denn gelesen werden solche Seiten wohl von den wenigsten Empfängern. Das sehen offenbar auch die Absender so: Das Schreiben beginnt mit den Worten „... aufgrund rechtlicher Bestimmungen der Datenschutz-Grundverordnung erhalten Sie ...“. Nicht etwa: „... mit diesem Schreiben möchten wir Sie über die Verarbeitung Ihrer folgenden personenbezogenen Daten informieren.“ Oder gar: „... für die Abwicklung unseres Vertrags müssen wir personenbezogene Daten von Ihnen verarbeiten. Der folgenden tabellarischen Übersicht können Sie entnehmen, zu welchen Zwecken wir welche Angaben erheben – und wann wir sie löschen.“

Darüber hätte ich mich tatsächlich gefreut: Eine übersichtliche Darstellung auf einer Seite, der ich auf einen Blick entnehmen kann, welche Daten konkret erfasst werden – und wann sie wieder aus den Systemen verschwinden. Stattdessen: Reichlich allgemeine Formulierungen über mögliche Verarbeitungen, die dem Art. 13 formal genügen mögen – mich aber weitgehend im Unklaren darüber lassen, welche Daten denn nun konkret von mir verarbeitet werden.

Aber vielleicht weiß das ja auch dort niemand so ganz genau.

Inhalt

secorvo
security consulting

Security News

Fragmentation meets Exploitation

Am 11.05.2021 veröffentlichte das Team um den Sicherheitsforscher Mathy Vanhoef (bekannt von den KRACK- oder Dragonblood-Angriffen) mit FragAttacks eine neue Gruppe von Schwachstellen in Wi-Fi-Netzen. Bei den neuen Schwachstellen handelt es sich um drei Design- sowie diverse Implementierungsfehler. Betroffen sind allen relevanten Wi-Fi-Standards (u. a. WPA2 und WPA3) sowie Geräte zahlreicher Hersteller.

Die Design-Schwachstellen sind schwierig auszunutzen, da sie u. a. die Mitwirkung des Benutzers voraussetzen. Die Lücken in den Implementierungen sind vom praktischen Standpunkt aus schwerwiegender: Sie sind leichter ausnutzbar und erlauben es, Systeme in internen Netzen anzugreifen, ohne die Verschlüsselung brechen zu müssen. Hierzu bedienen sich die Forscher fragmentierter Authentisierungspakete. Der fehlerfreie Umgang mit fragmentierten Daten ist ein komplexes Problem und verursacht immer wieder Schwachpunkte in Kommunikationsprotokollen.

In einem neunmonatigen Disclosure-Prozess wurden die Schwachstellen an die Hersteller kommuniziert. Die meisten Hersteller sind derzeit noch mit der Behebung der Schwachstellen beschäftigt, wobei in vielen Fällen Updates der Firmware notwendig sind. Einzelne Hersteller haben bereits Patches veröffentlicht.

Wer die Angriffe nachvollziehen und eigene Geräte auf Verwundbarkeit testen will, findet entsprechende Tools auf Github. Sofern für eingesetzte Komponenten noch keine Patches verfügbar sind, sollte – bspw. unter Berücksichtigung der Funkausleuchtung – die Relevanz für die eigene Organisation geprüft und entschieden werden, wie man mit der Schwachstelle umgeht. Eine Vorstellung weiterer Details zu den Angriffen ist auf der Konferenz Black Hat USA zu erwarten.

IT-Sicherheitsgesetz 2.0

Am 07.05.2021 hat der Bundesrat den Gesetzesentwurf des Bundestages zur Überarbeitung des IT-Sicherheitsgesetzes angenommen. Nach Veröffentlichung im Bundesgesetzblatt wird das Gesetz aller Kritik zum Trotze in Kraft treten. Neben einigen gravierenden, das BSI betreffenden Änderungen gibt es nun größeren Handlungsbedarf bei den Betreibern Kritischer Infrastrukturen. So werden die Einführung von „Systemen zur Angriffserkennung“ sowie detailliertere Meldungen zur Pflicht und die „Siedlungsabfallentsorgung“ zu einem neuen Sektor der Kritischen Infrastrukturen.

Um in dem Paragrafendschungel den Überblick zu behalten empfehlen wir einen Blick in die Plattform OpenKRITIS, die neben anderem eine gute Übersicht über die Änderungen anbietet.

Auslegungssache

Ist die Übermittlung personenbezogener Daten in Drittstaaten zulässig, wenn die Betroffenen informiert eingewilligt haben oder die Übermittlung zur Erfüllung eines Vertrags erforderlich ist? Art. 49 DSGVO sieht solche Ausnahmetatbestände vor, die jedoch von den Aufsichtsbehörden mit Verweis auf eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) vom 25.05.2018 bislang sehr restriktiv ausgelegt werden.

Im Zweifel ist jedoch immer der Wortlaut des Gesetzes maßgeblich. So sind nach Prof. Thomas von Danwitz, Richter am Europäischen Gerichtshof (EuGH) und Berichterstatter für das „Schrems-II“-Urteil, die Ausnahmeregelungen des Art. 49 DSGVO „noch nicht hinreichend ausgelotet“ (siehe seine Stellungnahme auf dem Europäischen Datenschutztag vom 28.01.2021).

Damit ist Art. 49 DSGVO jedoch kein „Freibrief“ für jede Datenübermittlung: Für jeden Fall, in dem weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, ist die Erforderlichkeit zu prüfen – beispielsweise also, ob keine Dienstleister aus der EU die Verarbeitung übernehmen können.

IT-Grundschutz-Kompendium

Das BSI verkündete am 19.05.2021 im IT-Grundschutz-Newsletter die Veröffentlichung weiterer Umsetzungshinweise zur Edition 2021 des IT-Grundschutz-Kompendiums. Darin wird aufgezeigt, wie die Anforderungen aus dem jeweiligen IT-Grundschutz-Baustein des Kompendiums erfüllt werden können.

Die Ergänzungen betreffen insbesondere die Schicht "IND" (Industrielle IT): IND.1 Prozessleit- und Automatisierungstechnik, IND.2.1 Allgemeine ICS-Komponente, IND.2.2 Speicherprogrammierbare Steuerung (SPS), IND.2.4 Maschine und IND.2.7 Safety Instrumented Systems.

Für die praktische Umsetzung der Bausteine wird die Lektüre der Hinweise wärmstens empfohlen.

Volatility v3

Bereits am 01.02.2021 wurde Volatility, das Standardwerkzeug für die forensische Hauptspeicheranalyse, nach einer eineinhalbjährigen Betaphase in einer stabilen Version 3 (Release V3-1.0.1) auf

GitHub veröffentlicht. In den seither vergangenen Monaten wurden weitere Fehler behoben und die Stabilität der neuen Funktionen verbessert.

Die Grundausstattung an Plugins ist im Vergleich mit der bisherigen Version V2.6.1 allerdings noch deutlich reduziert. So unterstützt Volatility V2.61 allein für Windows 113 Plugins, das Release V3-1.0.1 umfasst lediglich 44. Dennoch empfiehlt sich der Einsatz der neuen Version: Mit der Umstellung auf Python 3 wurden parallele Threads eingeführt, wodurch bisher sehr zeitintensive Plugins wie z. B. „strings" (Mapping von Strings auf Speicheradressen) oder „yarascan" (Prüfung des Hauptspeichers mit YARA-Regeln) wesentlich schneller abgearbeitet werden. Das ersparte z. B. bei der Untersuchung 64-GB-großer Hauptspeicherabzüge von MS Exchange im Kontext des APT-HAFNIUM-Angriffs im März 2021 z. T. mehrstündige Laufzeiten – bei einem akuten, kritischen Angriff ein echter Gewinn für die Verteidiger in den Unternehmen.

Eine weitere wichtige Funktion ist die automatisierte Unterstützung der Generierung spezifischer Windows-Profiles, die sich häufig nach NTOS-Kernel-Subversion unterscheiden. Bisher konnten lediglich Fachleute neue Profile erstellen.

Secorvo News

Live Hacking – Grundlagen von Pentests

Online-Formate können lebendige Seminare mit direktem Erfahrungsaustausch nur begrenzt ersetzen. Dafür haben sie große Stärken bei Demonstrationen und praktischen Übungen: Da bieten sie ein unmittelbareres Erleben und die Möglichkeit zum Training am gewohnten eigenen System.

Der große Erfolg einer Abendveranstaltung zum gleichen Thema im April hat uns daher motiviert, ein Ein-Tages-Online-Mitmach-Seminar für Sie zu entwickeln: In unserem „Live-Hacking-Lab" weisen unsere Penetrationstest-Experten Sie in die Grundlagen der Schwachstellensuche ein. Dabei führen Sie unter unserer Anleitung an realitätsnah konfigurierten, verwundbaren Laborsystemen gängige Methoden zur Identifikation von Schwachstellen praktisch durch – ganz bequem an Ihrem eigenen Arbeitsplatz.

Neben diesem Einblick in die Praxis des „Ethical Hackings" zeigen wir Ihnen die Möglichkeiten und Grenzen von Penetrationstests. Das Schulungskonzept spiegelt die langjährige Erfahrung der Referenten wider – von Praktikern für Praktiker.

Das Seminar bieten wir an am **23.06.2021** und am **14.07.2021**. Programm und Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

KA-IT-Si für alle

Erstmals haben wir in diesem Jahr Veranstaltungen der Karlsruher-IT-Sicherheitsinitiative (KA-IT-Si) in einem Online-Format durchgeführt. Die Resonanz war überwältigend: Mehr als 650 Datenschutz- und Datensicherheitsexperten haben an den bisherigen vier Abendveranstaltungen teilgenommen.

Auch wenn wir so bald wie möglich zu unseren Präsenzveranstaltungen mit lebendigem Buffett-Networking zurückkehren werden: Wir wollen auch zukünftig eine Möglichkeit zur „virtuellen" Teilnahme bieten, nicht zuletzt um die Veranstaltungen bundesweit „besuchbar" zu machen. Wenn Sie interessiert sind, freuen wir uns, wenn Sie sich in den Einladungsverteiler eintragen.

12. Tag der IT-Sicherheit

Auch der jährliche "Karlsruher Tag der IT-Sicherheit", eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V., wird in diesem Jahr als virtuelle Veranstaltung stattfinden, verteilt auf drei Abende. Den Einstieg bildet jeweils ein kurzer Blick in die Forschungs- und Gründerszene der Informationssicherheit, gefolgt von einem vertiefenden Fachvortrag:

1. Abend – Donnerstag, **01.07.2021**, 18 Uhr

10 Jahre Kompetenzzentrum KASTEL – ein Ausblick auf die IT-Sicherheit der Zukunft.
Prof. Dr. Jörn Müller-Quade (KIT)

Aus der Sicht eines Hackers. *Tim Schmidt (KIT)*

2. Abend – Donnerstag, **08.07.2021**, 18 Uhr

Einfach.Sicher.Machen. Transferstelle IT-Sicherheit im Mittelstand. *Stephanie Ziegler (KIS)*

Modernes DNS: Datenschutz mit Nebenwirkungen.
Prof. Dr. Rainer W. Gerling

3. Abend – Donnerstag, **15.07.2021**, 18 Uhr

Elevator Pitch: StartUps IT-Security.
Jun.-Prof. Dr. Christian Wressnegger (Poison Ivy) und *Mirko Ross (asvin)*

Cookies, Tracking, Analysen.
Friederike Schellhas-Mende (Secorvo)

Im Anschluss an die Vorträge bieten wir die Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit den Referenten und anderen Teilnehmern. Wir freuen uns auf drei kurzweilige und interessante Abende mit Ihnen! (Anmeldung)

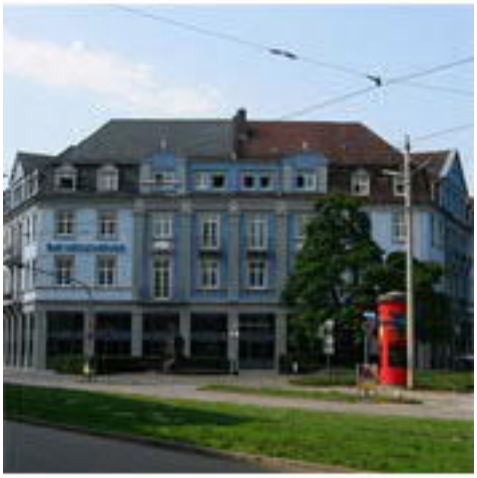
Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2021	
08.06.	Datenschutztag 2021 (COMPUTAS, Berlin)
09.-11.06.	Entwicklertag 2021 (VKSI, GI, ObjektForum , virtuell)
14.-15.06.	DuD 2021 (COMPUTAS, Berlin)
17.-18.06.	Annual Privacy Forum 2021 (ENISA, DG Connect, Católica University of Portugal, virtuell)
23.06.	Live Hacking Lab – Grundlagen Penetrationstest (Secorvo, virtuell)
Juli 2021	
01.07.	12. Tag der IT-Sicherheit, 1. Abend (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
08.07.	12. Tag der IT-Sicherheit, 2. Abend
12.-14.07.	PETS 2021 (University of Minnesota, virtuell)
12.-16.07.	DFRWS USA 2021 (DFRWS, virtuell)
14.07.	Live Hacking Lab – Grundlagen Penetrationstest (Secorvo, virtuell)
15.07.	12. Tag der IT-Sicherheit, 3. Abend
31.07.-05.08.	Blackhat USA 2021 (Blackhat, Las Vegas/US)

Fundsache

Am 15.04.2021 veröffentlichte der LfDI Baden-Württemberg ein Video zum Löschen von Daten samt Musterverzeichnis von Verarbeitungstätigkeiten mit integriertem Löschkonzept. Ein guter Einstieg.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

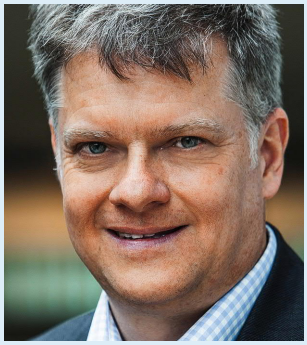
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Juni 2021



Erpressbar

Ransomware-Angriffe, bei denen die Daten der Opfer verschlüsselt und erst nach Zahlung eines Lösegelds wieder zur Entschlüsselung freigegeben werden, sind in den vergangenen Monaten zu einem beachtlichen Unternehmensrisiko herangewachsen. So hat nicht nur die Zahl der Angriffe, sondern auch die Höhe der Lösegeldforderungen erheblich zugenommen.

Seit etwa zehn Jahren sind Ransomware-Angriffe verbreitet. Da die Angreifer häufig genug Lösegeldzahlungen von den betroffenen Unternehmen erhalten, sind die Angriffe nicht nur finanziell sehr attraktiv, sondern werden auch erhebliche Summen in die Weiterentwicklung der Angriffssoftware investiert.

Die von einem Angriff betroffenen Unternehmen und Institutionen sind dabei allerdings nicht nur Opfer eigener Versäumnisse wie unzureichender Schutzmaßnahmen, fehlender Updates oder lückenhafter Backup- und Notfall-Konzepte, sondern auch der Schwachstellen in erworbener Software: Gäbe es diese Lücken nicht, wären Ransomware-Angriffe vergleichsweise selten erfolgreich.

Dennoch sind Schadensersatzforderungen an diese „Mitverursacher“ schwierig, denn die Angreifer verwischen ihre Spuren: Meist ist nicht oder nur mit sehr viel forensischem Aufwand feststellbar, auf welchem Weg das Eindringen in die Systeme gelungen ist. Kein Wunder, wollen die Täter ihr technisches Vorgehen doch noch bei weiteren Opfern erfolgreich praktizieren – und obendrein die von ihnen entwickelte Angriffssoftware vor „Piraterie“ schützen.

Damit bleibt Unternehmen und Behörden nur eines: Sich darauf einzustellen, dass – allen Schutzmaßnahmen zum Trotz – ein Ransomware-Angriff passieren kann. Und dafür zu sorgen, dass Angriffe schnell erkannt werden, Backups nicht verschlüsselt werden und ein Neuaufsetzen der Infrastruktur in kurzer Zeit gelingt. Diesen Weg sollte nur scheuen, wer über ausreichend Rücklagen verfügt.

Inhalt

secorvo
security consulting

Security News

Konzertierte Aktion

Die deutschen Datenschutz-Aufsichtsbehörden haben am 02.06.2021 die Durchführung einer koordinierten Prüfung internationaler Datentransfers personenbezogener Daten angekündigt. Damit soll den Anforderungen des Europäischen Gerichtshofs aus seiner Schrems-II-Entscheidung vom 16.07.2020 zur Durchsetzung verholfen werden: So dürfen weder das „Privacy Shield" noch die Standardvertragsklauseln ohne „wirksame zusätzliche Maßnahmen" als Rechtsgrundlage herangezogen werden.

Dazu werden ausgewählte Unternehmen zunächst mit abgestimmten Fragebögen zu Bewerberportalen, konzerninternem Datenverkehr und Tracking angeschrieben; außerdem stehen Mailhoster und Webhoster auf der Liste der Aufsichtsbehörden. Auch wenn zunächst nur ein (geringer) Teil der rund 3,3 Mio. deutschen Unternehmen angeschrieben werden wird, lohnt ein Blick in die Fragebögen, die u. a. von der Webseite des virtuellen Datenschutzbüros abgerufen werden können: Sie zeigen, welche Prüfpunkte im Fokus der Aufsichtsbehörden stehen.

Parallel-Welten-Netze

Seit einiger Zeit werden über "LoRaWAN" (Long Range Wide Area Network) IoT-Geräte über Funkverbindungen mit kleiner Reichweite zu Weitverkehrsnetzen mit geringer Bandbreite zusammengeschlossen. Am 08.06.2021 aktivierte Amazon USA ein bereits 2019 angekündigtes neues Feature von Amazon-Echo- und -Ring-Geräten, das diese LoRaWAN-Technik in Kombination mit BLE (Bluetooth Low Energy) nutzt: Bei schlechter Verbindung zum eigenen WLAN verbinden sich Amazon-Geräte via Amazon Sidewalk nun automatisch mit anderen Amazon-Geräten in der Umgebung, um eine Netzverbindung zu erhalten. Konkret redet der eigene Amazon-Lautsprecher oder die Ring-Kamera dann nicht mehr mit dem gerade schlecht verfügbaren WLAN-Router, sondern z. B. mit dem Echo-Gerät des Nachbarn. Dieses fungiert als „Bridge" zum Internet und stellt dafür 80 kbit/s seiner Bandbreite zur Verfügung.

Ähnliche Ansätze gab es bereits in der Vergangenheit mit Hotspots einiger ISPs. Dabei stellten private Router zusätzlich ein Gastnetzwerk zur Verfügung, über das andere Kunden desselben Providers Zugriff zum Internet erhielten. Der große Unterschied liegt allerdings darin, dass derartige Hotspots durch ein dediziertes Netzwerk-Gerät aufgespannt werden (Router), das über entsprechend segmentierende Sicherheitsfunktionen dafür sorgt, dass die Nutzer des Hotspots den eigenen Geräten nichts anhaben können.

Ob sich Lautsprecher und Kameras als Netzwerk-Barrieren eignen, sollte trotz ggf. sogar guter Spezifikation gründlich getestet werden. Und selbst dann stellt die reine Bereitstellung der Schnittstelle einen neuen Angriffsweg dar. Sobald die Funktion auch in Deutschland aktiviert wird, sollte man daher entscheiden, ob man Pioniernutzer dieser neuen Lösungen sein möchte – oder die Option in der Konfiguration lieber deaktivieren.

Alles auf Anfang

Von der Europäischen Kommission wurden am 04.06.2021 neue Standardvertragsklauseln für die DSGVO-konforme vertragliche Regelung des internationalen Austauschs personenbezogener Daten beschlossen und vom Europäischen Parlament verabschiedet. Darin wurde der durch die Cookies-II-Rechtsprechung entstandene Änderungsbedarf berücksichtigt.

Auch wenn die bisher gültigen Standardvertragsklauseln noch bis Ende September 2021 abgeschlossen werden können, ist es wichtig zu wissen, dass diese nur noch bis Ende Dezember 2022 verwendet werden dürfen. Bis dahin müssen sämtliche Verträge auf die neuen Standardvertragsklauseln umgestellt sein.

Zoom-Benchmark

Das Center for Internet Security (CIS) ist bekannt für Hardening Guides/Benchmarks zu Betriebssystemen, Webservern oder Datenbanken. Inzwischen gibt es auch Guides für Anwendungen und Cloud-Lösungen wie Zoom oder Azure – denn auch Cloud-Dienste sollte man restriktiv konfigurieren. Die Benchmarks sind in der Regel recht ausführlich und unterscheiden die Anforderungen u. a. nach Level 1 und Level 2. Einstellungen des Level 1 sollten in den meisten Fällen problemlos umsetzbar sein; bei Level 2 ist ggf. je Einstellung im Einzelfall eine Prüfung erforderlich.

Zur automatisierten Prüfung werden vom CIS mit Kosten verbundene Werkzeuge bereit gestellt: für den regelmäßigen Einsatz und wiederholte Compliance-Prüfungen eine gute Lösung. Testen kann man dies bspw. für Zoom über Test-Skripte, die Ende Mai 2021 auf Github zur Verfügung gestellt wurden.

Bann für Banner

Am 31.05.2021 hat die Stiftung noyb (my privacy is None of YOur Business) von Datenschutzaktivist Max Schrems den Cookie-Bannern pressewirksam den Kampf angesagt. Allen Cookie-Bannern? Nein,

nur solchen, die genervten Nutzern nicht die richtigen Auswahlmöglichkeiten lassen. noyb will über 500 Unternehmen anschreiben, bei denen nicht rechtmäßige Cookie-Banner festgestellt wurden, und droht mit einer Datenschutzbeschwerde bei der zuständigen Aufsichtsbehörde.

Da Webseiten nur selten korrekte Cookie-Banner verwenden, könnte eine beträchtliche Anzahl von weiteren Beschwerden die (von Schrems sicher erhoffte) Folge sein. In der Regel werden mindestens die Anforderungen an den Widerspruch für erteilte Einwilligungen (genauso einfach wie die Erteilung) gar nicht oder nicht korrekt umgesetzt.

Dabei kann man in den Leitlinien des European Data Protection Board nachlesen, wie es richtig geht. Großen Nachbesserungsbedarf sieht auch das ULD bei der länderübergeifenden Datenschutz-Prüfung von Medien-Webseiten. Wer es genau wissen will, dem sei der Vortrag „Cookies, Tracking, Analysen“ von RAin Friederike Schellhas-Mende (Secorvo) auf dem kommenden Karlsruher Tag der IT-Sicherheit am 15.07.2021 ans Herz gelegt (siehe unten).

E-Privacy-Richtlinie umgesetzt

Das schon lange erwartete „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) wurde endlich am 28.05.2021 im Bundestag und tags darauf im Bundesrat beschlossen. Mit diesem Gesetz, das zusammen mit dem novellierten Telekommunikationsgesetz (TKG) am 01.12.2021 in Kraft tritt, wird die E-Privacy-Richtlinie der EU vor allem hinsichtlich der Cookies umgesetzt. Geregelt werden der digitale Nachlass und insbesondere das Thema Cookies und Einwilligungen. Das Gesetzt enthält in § 25 die Vorgabe, dass eine Einwilligung in das Setzen von Cookies immer dort notwendig ist, wo es sich nicht um technisch notwendige Cookies handelt, die beispielsweise zum Betrieb der Webseite erforderlich sind. Interessant ist § 26, in dem die Grundlage für Einwilligungsverwaltungsdienste gelegt wird. Diese Regelung muss aber noch mittels einer Verordnung konkretisiert werden.

Bei der Umsetzung sollte beachtet werden, dass nicht alles, was für den Nutzer komfortabler auch besser ist: Die Möglichkeit zur zentralen Speicherung und Verwaltung von Einwilligungen bei Treuhändern erscheint verlockend, bringt aber neue Risiken mit sich. Auch die Einwilligung über Voreinstellungen des Internetbrowsers sollte sehr kritisch betrachtet werden, wenn man eine Eindämmung der Bannerflut erreichen will. Völlig außer Acht geblieben sind leider die Anforderungen an die Gestaltung der Cookie-Banner; hier ist erster Nachbesserungsbedarf erkennbar.

Secorvo News

Teamverstärkung

Seit dem 01.07.2021 verstärkt Milan Burgdorf, Diplom-Jurist mit mehrjähriger Berufserfahrung als Informationssicherheitsbeauftragter das Secorvo-Team. Herzlich willkommen!

Secorvo Seminare

Nachdem die Infektionszahlen erwarten lassen, dass im Spätsommer die Durchführung von Präsenzseminaren wieder möglich sein wird, bieten wir das erfolgreiche T.I.S.P.-Seminar vom **20.09. bis 24.09.2021** (schnelle Buchung empfohlen) und vom **22.11. bis 26.11.2021** an. Das Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

12. Tag der IT-Sicherheit

Der jährliche "Karlsruher Tag der IT-Sicherheit", eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V., findet in diesem Jahr als virtuelle Veranstaltung statt – verteilt auf drei Abende. Der erste Abend mit Prof. Dr. Jörn Müller-Quade (Leiter der Forschungsgruppe „Kryptografie und Sicherheit“ am KIT) und dem White-Hat-Hacker Tim Schmidt am 01.07. stieß bereits auf großen Zuspruch. Es folgen:

2. Abend – Donnerstag, **08.07.2021**, 18 Uhr

Einfach.Sicher.Machen. Transferstelle IT-Sicherheit im Mittelstand. *Stephanie Ziegler (KIS)*

Modernes DNS: Datenschutz mit Nebenwirkungen. *Prof. Dr. Rainer W. Gerling*

3. Abend – Donnerstag, **15.07.2021**, 18 Uhr

Elevator Pitch: StartUps IT-Security.
Jun.-Prof. Dr. Christian Wressnegger (Poison Ivy) und *Mirko Ross (asvin)*

Cookies, Tracking, Analysen.
Friederike Schellhas-Mende (Secorvo)

Im Anschluss an die Vorträge bieten wir die Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit den Referenten und anderen Teilnehmern. Wir freuen uns auf drei kurzweilige und interessante Abende mit Ihnen! (Anmeldung)

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2021	
01.07.	12. Tag der IT-Sicherheit, 1. Abend (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
08.07.	12. Tag der IT-Sicherheit, 2. Abend
12.-14.07.	PETS 2021 (University of Minnesota, virtuell)
12.-16.07.	DFRWS USA 2021 (DFRWS, virtuell)
15.07.	12. Tag der IT-Sicherheit, 3. Abend
31.07.-05.08.	Blackhat USA 2021 (Blackhat, Las Vegas/US)
August 2021	
05.-09.08.	DEF CON 29 (DEFCON, Las Vegas/US)
08.-10.08.	SOUPS 2021 (usenix, Vancouver/CAN)
11.-13.08.	30th USENIX Security Symposium (usenix, Vancouver/CAN)
15.-19.08.	Crypto 2021 (IACR, Santa Barbara/US)
September 2021	
07.-09.09.	6th IEEE European Symposium on Security and Privacy (IEEE, Wien/AUT)
14.-15.09.	D•A•CH Security (Institut für Verteilte Intelligente Systeme, syssec, München))
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)

Impressum

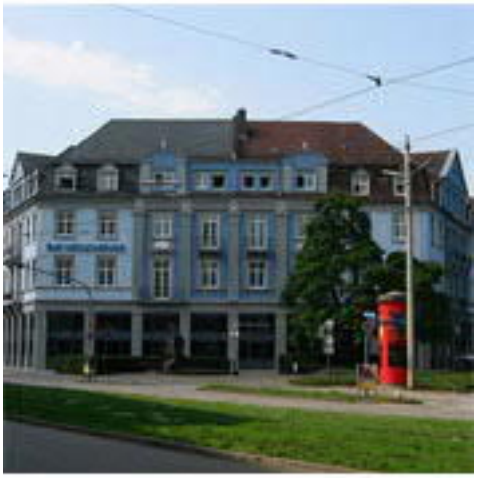
Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

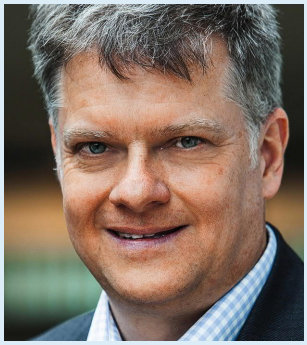
Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

Juli 2021



Die Bäume und der Wald

Je tiefer wir in den Schutz der immer komplexeren Informationstechnik eintauchen, desto eher laufen wir Gefahr das große Bild aus den Augen zu verlieren. Treten wir also einen Schritt zurück.

Besonders zwei Entwicklungslinien sind es, die sich gerade deutlich abzeichnen. Die eine: Mit der zunehmenden Digitalisierung entstehen zahlreiche neue Risiken, die oft erst nach einem Vorfall erkannt werden, so wie Anfang Juli beim Ransomware-Vorfall im Landratsamt Anhalt-Bitterfeld. Der Landrat rief den Katastrophenfall aus: Wochenlang konnten im Landkreis weder Wohngeld noch Sozialhilfe gezahlt, Mitarbeitergehälter überwiesen oder Fahrzeuge angemeldet werden.

Die zweite Entwicklungslinie zeigt, wie wenig wir bisher der ersten gewachsen sind – und wie unverstanden der Zusammenhang noch ist. Denn wie in einer Parallelwelt zeigte die CDU die Forscherin Lilith Wittmann beim LKA an, nachdem diese am 11.05.2021 eine hoch kritische Sicherheitslücke in der CDU-Connect-App entdeckt und dem CERT-Bund gemeldet hatte. Schon am 18.05.2009 wies das BVerfG eine Beschwerde gegen den „Hackerparagrafen" § 203c StGB zurück, der immer wieder die bspw. datenschutzrechtliche Ahndung der Verbreitung von Programmen mit Sicherheitslücken verhindert –wie sollte man auch eine solche Lücke dokumentieren, ohne ein Programm zu verwenden, das sie ausnutzt? Und am 08.06.2021 lehnte es eine Beschwerde gegen die Geheimhaltung von Zero-Day-Exploits durch deutsche Sicherheitsbehörden ab – genau damit entwickelt die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) seit 2017 Software zur Telekommunikationsüberwachung.

Klar ist: Unsere Zukunft wird digital sein. Funktionieren wird sie nur, wenn sie sicher ist. Daher muss die systematische Beseitigung von Sicherheitslücken unser aller Ziel sein. Auch das der Sicherheitsbehörden. Die Geheimhaltung und Verbreitung solcher Lücken gehört geahndet – nicht deren Aufdeckung oder Dokumentation.

Inhalt

secorvo
security consulting

Security News

UK ist sicheres Drittland

Aufatmen in vielen Unternehmen: Entgegen den Bedenken des EU-Parlaments hat die EU-Kommission am 28.06.2021 den Angemessenheitsbeschluss für Großbritannien (UK) angenommen. Damit gilt UK nun als sicheres Drittland mit angemessenem Datenschutzniveau, obwohl der Investigatory Powers Act dem britischen Geheimdienst ähnlich viele Befugnisse einräumt wie den US-amerikanischen Diensten der FISA 702, der EO 12333 und der CLOUD Act. Die UK-GDPR basiert auf den europäischen Standards und übernimmt wesentliche Teile der DSGVO. Darin enthalten sind aber auch Ausnahmeregelungen zu Zwecken der Einwanderungskontrolle, was neben den unkontrollierten Zugriffen durch die Geheimdienste für Bedenken gesorgt hat.

Der Angemessenheitsbeschluss hat eine Laufzeit von sechs Jahren, kann aber durch die Kommission jederzeit eingeschränkt oder auch komplett aufgehoben werden.

Ransomware-Hotfix

Am 02.07.2021 gelang es Angreifern der Ransomware-Gruppe REvil mittels einer Zero-Day-Schwachstelle zahlreiche Installationen der Softwareverteilungsplattform Kaseya VSA zu kompromittieren. Die Cloud-Plattform des Herstellers konnte offenbar rechtzeitig abgeschaltet werden; die On-Premise-Instanzen diverser Kunden wurden jedoch übernommen und lieferten eine als Hotfix getarnte Ransomware an die verwalteten Systeme aus. Die Erpresser forderten anschließend von Kaseya die Rekordsumme von 70 Mio. Dollar für die Entschlüsselung der betroffenen Systeme. Bei vielen Unternehmen kam es zu Einschränkungen des IT-Betriebs.

Der Angriff veranlasste US-Präsident Joe Biden, Wladimir Putin am 09.07.2021 aufzufordern, gegen die mutmaßlich aus Russland stammende Gruppe REvil vorzugehen. Offenbar gerieten die Angreifer unter Druck: Am 05.07.2021 senkten sie ihre Forderung überraschend auf 50 Mio. Dollar, und am 13.07.2021 verschwanden ihre Webseiten. Ob die Gruppe untergetaucht ist oder ob es sich um eine Aktion der Ermittlungsbehörden oder der Geheimdienste handelt, ist nicht bekannt. Allerdings teilte Kaseya am 23.07.2021 mit, dass man von einer „vertrauenswürdigen Drittpartei" einen Generalschlüssel erhalten habe.

In den vergangenen Jahren erfolgen vermehrt Angriffe über die „Supply Chain", so wie der Solarwinds-Hack vom vergangenen Dezember. Bei solchen Angriffen werden mit einer Schwachstelle zahlreiche Kunden gleichzeitig kompromittiert, trotz ansonsten angemessener Schutzmaßnahmen. Daher sollte für administrative Werkzeuge ein besonders hohes Schutzniveau greifen.

Ransomware Readiness

Am 30.06.2021 veröffentlichte die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) ein neues Modul für das Cyber Security Evaluation Tool (CSET). CSET ist eine Desktop-Software für Windows, die umgesetzte Schutzmaßnahmen im Netzwerk prüft. Mit dem neuen Modul Ransomware Readiness Assessment (RRA) wird überprüft, wie gut eine Organisation technisch und organisatorisch vor Ransomware-Vorfällen geschützt ist und ob sie sich von einem Vorfall absehbar erholen kann.

In einem ersten Test machte das Modul einen guten Eindruck – es eignet sich auch für Organisationen, die einen ersten Überblick gewinnen wollen, da sie noch nicht so genau wissen, was beim Thema „Schutz vor Ransomware" zu beachten ist. Vorausgesetzt, man scheut die Installation einer 1 GB großen EXE-Datei nicht, die einen kompletten Microsoft IIS Express zum Anzeigen einer Webseite mitbringt. Nehmen Sie vorsichtshalber eine virtuelle Maschine – denn auch bei Tests kann man sich etwas einfangen.

Grenzen des One-Stop-Shop

Bisher konnten nationale Aufsichtsbehörden bei angezeigten Verstößen gegen die DSGVO nicht direkt gegen Unternehmen mit Firmensitz in einem anderen europäischen Mitgliedsstaat vorgehen, weil entsprechend Art. 56 DSGVO die Federführung einer solchen Untersuchung bei der Aufsichtsbehörde des Sitzlandes liegt. Im unternehmens- oder steuerrechtlichen Kontext ist dieses Zuständigkeitsprinzip als „One-Stop-Shop" bekannt.

In der Vergangenheit stellte dieses Prinzip beispielsweise die deutschen Aufsichtsbehörden vor erhebliche Probleme, wenn sie mögliche Verstöße von großen Internet-Konzernen untersuchen wollten, die ihren Sitz in Irland haben.

Der EuGH hat nun am 15.06.2021 bestätigt, dass nach Art. 55 DSGVO eine nationale Aufsichtsbehörde einen Verstoß gegen die DSGVO selbst verfolgen kann, sofern sie das Verfahren der Zusammenarbeit und Kohärenz nach Art. 60 DSGVO eingehalten hat. Allerdings – und das ist neu – stellt der EuGH klar, dass die nationale Behörde zur wirksamen Anwendung der DSGVO den angeblichen Verstoß weiter untersuchen darf, wenn die federführende Aufsichtsbehörde nicht mit ihr zusammenarbeitet.

Eine lesenswerte Zusammenfassung des Urteils findet sich in der EuGH-Pressemitteilung.

MS PKI under attack

Via Advisory warnte Microsoft am 23.07.2021 vor einem „PetitPotam" getauften NTLM-Angriff auf den Zertifikatsdienst der Microsoft-PKI, mit dem ein Angreifer sich Nutzer-Berechtigungen verschaffen kann. Die Ursache ist – wieder einmal – übertriebene Abwärtskompatibilität: Da Microsoft NTLM per Default-Einstellung unterstützt, dürften von der Schwachstelle sehr viele Microsoft-PKIs betroffen sein. Die wirksamste (und simpelste) Schutzmaßnahme ist daher auch, die NTLM-Authentifikation mindestens auf Domain-Controllern zu deaktivieren – ohnehin eine gute Idee, um sich vor weiteren noch unentdeckten Bugs zu schützen. Falls das nicht gewünscht ist, sollte man zumindest den Web-Enrollment-Dienst der Windows-PKI deaktivieren oder ihm, wenn er gebraucht wird, NTLM verbieten. Der PKI-Experte Hans-Joachim Knobloch (Secorvo) beschreibt nach seiner ausführlichen Untersuchung des Angriffs vom 28.07.2021 was dafür zu tun ist.

Dabei entdeckte er einige weitere beunruhigende Varianten. Denn Zertifikate können auch über den Network Device Enrollment Service (NDES) angefordert werden. Dabei kann es einem Angreifer je nach Konfiguration der PKI gelingen, ein Kerberos-Ticket zur Anmeldung am Domain-Controller mit administrativen Berechtigungen zu erschleichen. Hans-Joachim Knobloch listet in seinem Blog-Beitrag vom 30.07.2021 zahlreiche Maßnahmen, die vor dieser Attacke wirksam schützen.

Ersatz für Cookie-Banner?

In Kooperation mit den Sustainable Computing Labs der Wirtschaftsuniversität Wien möchte die NGO noyb die allgegenwärtigen Cookie-Banner durch Advanced Data Protection Control (ADPC) ersetzen. Die Idee veröffentlichte Max Schrems am 14.06.2021: Durch ein automatisches Browser-Signal soll der Nutzer eine Einwilligung erteilen oder verweigern, eine bereits erteilte Einwilligung widerrufen oder einer Verarbeitung aus einem berechtigten Interesse widersprechen können.

Dafür soll eine hersteller- und browserunabhängige standardisierte Schnittstelle eingeführt werden. Statt eines reinen Ja-Nein-Mechanismus' sollen Nutzer einerseits nach Art der Daten entscheiden und andererseits Entscheidungen für mehrere Webseiten treffen können. So soll auch ein „Opt In" möglich sein, das ein differenziertes Einwilligungsmanagement bietet. Dieser Ansatz sollte auch beim Einwilligungsmanagement nach § 26 TTDSG berücksichtigt werden (siehe SSN 6/2021). Für Firefox und Chromium-basierte Browser existieren bereits Prototypen.

Secorvo News

Septemberseminare

Endlich sind Präsenzseminare wieder ohne Bedenken möglich. Daher können wir Sie vom **20. bis 24.09.2021** wieder auf die berufsqualifizierende, angesehene T.I.S.P.-Zertifizierung vorbereiten. Nach Ihrer Anmeldung erhalten Sie vorab unser T.I.S.P.-Buch zugesandt (Amazon-Rating: 4,8).

Da wir während der Pandemie gelernt haben, dass Online-Formate sich besonders für eintägige Hands-On-Seminare eignen, bieten wir erneut am **15.09.2021** unser Live-Hacking-Lab online an. Und vom **28. bis 30.09.2021** stellen wir Ihnen mit IT Security Insights aktuelle Themen der IT-Sicherheit vor (als T.I.S.P.-Update anerkannt).

Alle Programme und die Möglichkeit zur Online-Anmeldung finden Sie auf unseren Webseiten.

Irren ist kryptografisch

Die Kryptoanalyse der ENIGMA ist eine der spannendsten Geschichten in der Kryptografie. Bis in die 70er Jahre wurde in der Öffentlichkeit – und nicht nur dort – angenommen, dass die wichtigste Verschlüsselungsmaschine des zweiten Weltkriegs nicht geknackt worden war. Ein Irrtum: Die ENIGMA wurde bereits in den 30er Jahren erfolgreich analysiert, und während des Krieges wurden in Bletchley Park (GB) Nachrichten deutscher U-Boote systematisch entschlüsselt.

Auf dem kommenden KA-IT-Si-Event am 30.09.2021 wird Johann Grathwohl (IT-Security-Architekt bei CONITAS) die Entwicklung und die historischen Hintergründe der ENIGMA vorstellen und ihre Funktionsweise erläutern. Anschließend wird er die Kryptoanalyse skizzieren und auf Schwachpunkte und Fehler im Design des Verschlüsselungsverfahrens eingehen und daraus einige wichtige Erkenntnisse für den Entwurfsprozess ableiten.

Wir freuen uns darauf, unsere KA-IT-Si-Events ab September wieder als Präsenzveranstaltungen durchführen und Ihnen unser „Buffet-Networking" zum persönlichen Austausch anbieten zu können. Um die Vorträge auch weiterhin so vielen Interessenten wie in den vergangenen Monaten zugänglich zu machen, werden wir auch eine Teilnahme per Livestream ermöglichen (zur Anmeldung).

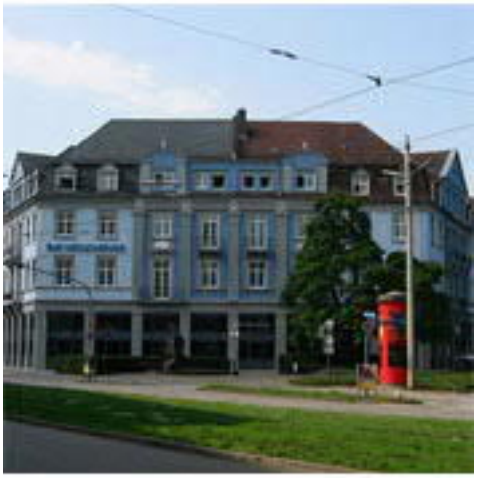
Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2021	
05.-09.08.	DEF CON 29 (DEFCON, Las Vegas/US)
08.-10.08.	SOUPS 2021 (usenix, Vancouver/CAN)
11.-13.08.	30th USENIX Security Symposium (usenix, Vancouver/CAN)
16.-20.08.	Crypto 2021 (IACR, virtuell)
September 2021	
06.-10.09.	6th IEEE European Symposium on Security and Privacy (IEEE Computer Society, virtuell)
13.-16.09.	European Identity & Cloud Conference 2021 (KuppingerCole, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.09.-01.10.	Informatik 2021 (GI, Berlin)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
30.09.	Irren ist kryptografisch (KA-IT-Si, Karlsruhe/online)

Fundsache

Am 17.07.2021 hat der Landesbeauftragte für Datenschutz-und Informationsfreiheit in Baden-Württemberg eine Handreichung zur Durchführung von Online-Prüfungen veröffentlicht, nachdem er festgestellt hatte, dass bei zahlreichen Prüfungen von Hochschulen die räumliche und technische Privatsphäre von Studierenden verletzt worden war.



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

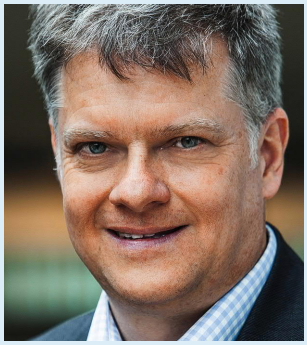
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

August 2021



Dialektik

Man mag den Marxismus für eine Irrung oder eine mindestens wirtschaftlich gescheiterte Ideologie halten. Eines der drei von Engels in etwas freier Umdeutung von Hegels Dialektik aufgestellten Grundgesetze ist jedoch zweifellos eine zutreffende Beschreibung eines immer wieder zu beobachtenden Phänomens: Des Umschlags von Quantität in Qualität.

So sorgen nicht einzelne Staubkörner für eine Verschmutzung (von Reinsträumen einmal abgesehen), sondern erst deren große Zahl. Sandkörner bilden Strände und Schneeflocken Skipisten – aber nur, wenn sehr viele davon an einer Stelle zusammenkommen. Der Punkt, an dem dabei die Quantität zu einer neuen Qualität wird, ist nicht exakt auszumachen und liegt vielleicht auch im Auge des Betrachters. Irgendwann aber gibt es keinen Zweifel mehr, dass sie zu Dreck, Strand oder Skipiste geworden sind.

Unter demselben Phänomen leidet der Datenschutz – schon immer, aber seit der Entdeckung der Digitalisierung immer offensichtlicher. Einzelne Verarbeitungen personenbezogener Daten bedrohen selten die freie Entfaltung. Wohl aber deren viele. So mag eine einzige Videokamera auf einem öffentlichen Platz eine erträgliche Freiheitsbeschränkung sein. Eine auf jedem öffentlichen Platz schon weniger – und die nahtlose Aufzeichnung öffentlicher Bereiche sicher nicht.

Das ist ein Kernproblem des Datenschutzes. Gegen eine einzelne Verarbeitung mag wenig einzuwenden sein, doch im Kontext vieler weiterer wird sie irgendwann Teil einer potentiellen Überwachungsinfrastruktur.

Was dem Datenschutz daher fehlt ist ein Limit, das das Umschlagen in Überwachung verhindert. Wäre z. B. die Größe der durch Videokameras zulässig überwachbaren Fläche begrenzt oder die Datenmenge, die Webseiten und Apps „nach Hause“ schicken dürfen, würden sehr bald sinnvolle Prioritäten gesetzt – und ließen sich viele Verarbeitungen entspannter ertragen.

Inhalt

secorvo
security consulting

Security News

Der Schein darf trügen

Das Oberverwaltungsgericht Rheinland-Pfalz hat am 25.06.2021 entschieden, dass die DSGVO auf abgeschaltete Überwachungskameras nicht anwendbar ist. Die Aufsichtsbehörde hatte den Kläger aufgefordert, die Kamera zu beseitigen, dieser schaltete sie jedoch lediglich ab. Die Behörde stützte ihre Anordnung auf Art. 58 Abs. 2 lit. f) DSGVO. Nach Ansicht des Gerichts verarbeitet eine ausgeschaltete Kamera ebensowenig Daten wie eine Attrappe. Das ist sachlich richtig, denn wo keine Daten erhoben werden, findet auch keine Verarbeitung statt. In der Konsequenz bedeutet dies, dass auch kein Hinweis auf die nicht stattfindende Videoüberwachung erfolgen muss und damit auch keine Kennzeichnungspflicht besteht. Die Entscheidung reiht sich in weitere, die einen Unterlassungsanspruch in solchen Fällen ablehnen (z. B. OLG Frankfurt a. M., Beschluss vom 12.10.2017 – 3 U 195/16). Zwar bleibt für den Betroffenen das „Überwachungserlebnis" dasselbe, da er eine Verarbeitung annehmen muss – aber ohne Daten auch kein Datenschutz.

Self-Assessment

Besonders für kleinere und mittlere Unternehmen ist es oft aufwendig, sich Grundkenntnisse der IT-Sicherheit als Beratung einzukaufen oder gar ein eigenes Security-Team aufzubauen. Da können Self-Assessment-Werkzeuge helfen. Sie ersetzen zwar kein externes Audit, geben jedoch einen ersten Überblick über die aktuell wichtigsten Themenbereiche und Sensibilisierungsmaßnahmen.

Bekannte Tools sind z. B. der ExPress Informationssicherheits Check (EPIC) des BSI, das Cyber Resilience Review (CRR) der CISA, der Cyber Aware Action Plan des GCHQ, der Sec-O-Mat der TISiM, das Cybersecurity Self-Assessment for SMEs von Cyberwatching oder auch das Security and Risk Self-Assessment von Brennan IT. Eine zusätzliche wertvolle Ressource liefert das CIS mit den CIS Controls.

Als Einstieg in die Informationssicherheit ist ein solches Self-Assessment jedenfalls keine schlechte Wahl. Mit dem CSIRT Maturity Self-Assessment Tool der ENISA lassen sich sogar mögliche Optimierungen für ein bereits bestehendes IT-Sicherheitsmanagement finden.

Druckereskalation

Am 19.05.2021 wurde von HP eine Schwachstelle im Druckertreiber diverser HP LaserJet Drucker veröffentlicht. Die gemäß HP mit einem CVSS-Score von 8.8 bewertete Schwachstelle CVE-2021-3438 ermöglicht über einen Buffer Overflow die Gewinnung von Berechtigungen im System-Kontext. Das ist ein gravierender Bug, sowohl hinsichtlich der möglichen Auswirkungen als auch wegen dessen weiter Verbreitung. Angreifer können sich darüber dauerhaft in einem System mit hohen Privilegien festsetzen.

Über die vom Hersteller bereitgestellten Updates (die zügig eingespielt werden sollten) hinaus stellen sich gleich mehrere Fragen: Warum erfolgt die Ausgabe von Dateien an einen Drucker heute noch mit hohen Privilegien? Warum geht das nicht im Benutzerkontext? Und: Warum benötigt ein Druckertreiber eine 25 MB große Installationsdatei, mit Utilities sogar oft über 100 MB? Sind bei diesem Umfang und dieser Komplexität nicht übersehene Schwachstellen zu erwarten? Welche technologische Entwicklung rechtfertigt eine solche Treiberkomplexität? Nicht zuletzt: Wurden (und werden) die Treiber vom Hersteller überhaupt gründlich auf Schwachstellen untersucht? Nach Auskunft der Forscher, die die Schwachstelle entdeckten, bestand sie seit mindestens 16 Jahren.

Ganz ähnliches gilt für Grafik-Treiber, die heute oft einen Umfang von über 700 MB mitbringen. Gerade Drucker- und Grafiktreiber-Programmierer sollten sich professionell mit der Frage beschäftigen, wie die erforderlichen Funktionen kompakt und ohne Scheunentore bereitgestellt werden können. Helfen würde, wenn in Unternehmen und Behörden bei der Beschaffung von Hardware auch die Komplexität und Sicherheit der Treiber eine Rolle spielen würde (gemessen z. B. daran, wie viele Schwachstellen es bereits gab).

Better Hunting

Seit dem 02.08.2021 steht das forensische Werkzeug Autopsy in der neuen Version 4.19 zur freien Nutzung bereit. Sehr hilfreich ist das neue YARA-Ingest-Modul, das man mit eigenen Zusammenstellungen von Regeln für spezifische Fragestellungen (z. B. VBA-Macros in MS Office-Dokumenten) ablaufen lassen kann. Das Modul arbeitet problemlos mehrere tausend YARA-Regeln fehlerfrei ab, wenn man es z. B. zur Suche nach Schadsoftware auf eine Datenquelle anwendet.

Wesentlich beschleunigt wurde die Erstellung des Stichwort-Index, der nun nicht mehr versucht, eine Indexierung in mehreren Sprachen sowohl für unbekannte Dateiformate als auch für nicht belegten Speicherplatz eines Datenträgers (*unallocated space*) durchzuführen – für schnellere Triagen sehr hilfreich. Muss man als Incident Responder die „Nadel im Heuhaufen" suchen, kann die Suche zeitlich

abgetrennt werden, indem der gesamte unallocated space zuerst mit Autopsy in eine separate Datei extrahiert wird.

Auch die Autopsy-Fallakte wurde verbessert, sodass unterschiedliche Datenquellen jeweils genau einem System oder einem Fundort zugewiesen werden können. Damit sind z. B. ein Desktop-PC, ein Laptop, ein Smartphone oder ein USB-Gerät als einzelne Entitäten logisch gruppierbar. So können z. B. auch logische Extraktionen von unterschiedlichen Volumenschattenkopien einer Windows-Installation zugeordnet werden. Ergänzt wird die Fallakte durch die optionale Zuordnung einer Datenquelle zu einem definierten Nutzer.

Die Einarbeitung in dieses Werkzeug erfordert etwas Zeit. Versteht man aber die Logik, dann lassen sich viele Detailspuren finden. Durch unterstützende Plugins wurde zuletzt auch die forensische Unterstützung für QNX (Echtzeitbetriebssystem im Bereich Automotive) realisiert.

Neue Mindeststandards des BSI

Am 07.07.2021 hat das BSI zwei überarbeitete Mindeststandards zur Nutzung externer Cloud-Dienste und für Schnittstellenkontrollen veröffentlicht. Ein Cloud-Dienst, z. B. eine Datenablage oder eine Kollaborationsplattform, ist schnell eingekauft. Aber passt der Dienst wirklich zur Unternehmensstrategie, wurde an den Datenschutz gedacht und wie sehen die Exit-Optionen aus? Zu diesen Fragen formuliert der Standard in strukturierter Form von der Planung bis zur Beendigung Anforderungen, an die definitiv gedacht werden sollte. Im Rahmen der Überarbeitung wurden die Mitnutzung von Cloud-Diensten integriert und die Inhalte an den IT-Grundschutz-Baustein sowie den Kriterienkatalog Cloud Computing angepasst.

Über Schnittstellen kann es zu Schadsoftwarebefall oder unerwünschtem Abfluss von Daten kommen. Schnittstellen entstehen häufig „unkontrolliert“ mit einem neuen System oder einer Anwendung. Der Standard zeigt die wichtigsten Anforderungen im Lebenszyklus einer Schnittstelle und die zu ergreifenden Kontrollmaßnahmen.

Beide Standards gelten eigentlich nur für die Informationstechnik des Bundes, enthalten aber auch für andere Behörden und Unternehmen in kompakter Form wertvolle Hinweise. Sie können somit als Checklisten verstanden und genutzt werden. Systematisch und kostenlos – wenngleich die Umsetzung der Anforderungen (sinnvoll investierten) Aufwand verursacht.

One Face fits most

Am 01.08.2021 veröffentlichten israelische Forscher eine Studie mit dem Titel „Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution“. Darin stellen sie vor, wie sie mit KI-Werkzeugen sprichwörtliche „Allerweltsgesichter“ erzeugen können, die beim Vergleich mit Einträgen einer Referenzdatenbank für Gesichtserkennung (Labeled Faces in the Wild – LFW) zahlreiche „False Positives“ lieferten. Einzelne der synthetisierten Gesichter wurden mit bis zu 20% der Referenzdatensätze positiv abgeglichen; mit nur neun speziell erzeugten Gesichtern gelang das bei 40% aller Referenzgesichter.

Die Untersuchung lässt erwarten, dass eine Authentifizierung mittels biometrischer Gesichtserkennung auch zukünftig keine große Verlässlichkeit bieten wird. Zweifel an der Zuverlässigkeit biometrischer Identifikation sind demnach geboten. Und die Erfahrung lehrt: Angriffe werden über die Zeit besser, nicht schlechter.

Secorvo News

Seminare wieder möglich

Noch gibt es freie Plätze bei unseren Herbst-Seminaren – T.I.S.P., T.P.S.S.E., Live-Hacking und PKI. Wir empfehlen eine baldige Anmeldung unter https://www.secorvo.de/seminare.

Irren ist kryptografisch

Die Kryptoanalyse der ENIGMA ist eine der spannendsten Geschichten in der Kryptografie. Bis in die 70er Jahre wurde in der Öffentlichkeit – und nicht nur dort – angenommen, dass die wichtigste Verschlüsselungsmaschine des zweiten Weltkriegs nicht geknackt worden war. Ein Irrtum: Die ENIGMA wurde bereits in den 30er Jahren erfolgreich analysiert, und während des Krieges wurden in Bletchley Park (GB) Nachrichten deutscher U-Boote systematisch entschlüsselt.

Auf dem kommenden KA-IT-Si-Event am 30.09. 2021 wird Johann Grathwohl (IT-Security-Architekt bei CONITAS) die Entwicklung und die historischen Hintergründe der ENIGMA vorstellen und ihre Funktionsweise erläutern. Anschließend wird er die Kryptoanalyse skizzieren und auf Schwachpunkte und Fehler im Design des Verschlüsselungsverfahrens eingehen und daraus einige wichtige Erkenntnisse für den Entwurfsprozess ableiten.

Wir freuen uns darauf, unsere KA-IT-Si-Events nun wieder als Präsenzveranstaltungen durchführen und Ihnen unser „Buffet-Networking“ zum persönlichen Austausch anbieten zu können. Um die Vorträge auch weiterhin so vielen Interessenten wie in den vergangenen Monaten zugänglich zu machen, werden wir auch eine Teilnahme per Livestream ermöglichen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2021	
06.-10.09.	6th IEEE European Symposium on Security and Privacy (IEEE Computer Society, virtuell)
13.-16.09.	European Identity & Cloud Conference 2021 (KuppingerCole, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.09.-01.10.	Informatik 2021 (GI, Berlin)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
30.09.	Irren ist kryptografisch (KA-IT-Si, Karlsruhe/online)
Oktober 2021	
04.-07.10.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
12.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
12.-14.10.	it-sa 2021 (NürnbergMesse GmbH, Nürnberg)
17.-21.10.	Eurocrypt 2021 (IACR, Zagreb/HRV)

Fundsache

Am 18.07.2021 hat Amnesty International Security Lab ein forensisches Mobile Verification Toolkit veröffentlicht, mit dem auf mobilen Geräten nach Spuren der Pegasus-Spyware gesucht werden kann. Die Python-Quellen und eine Anleitung finden sich auf Github.

Impressum

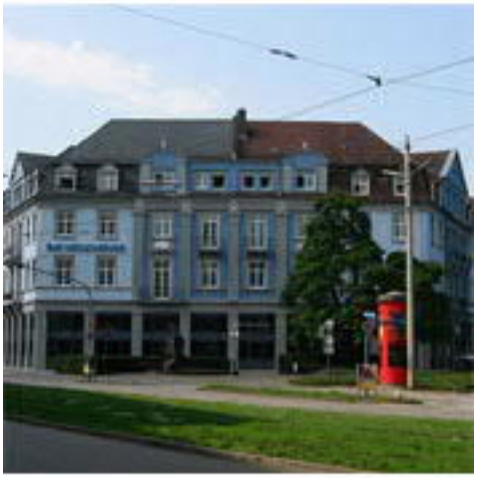
Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

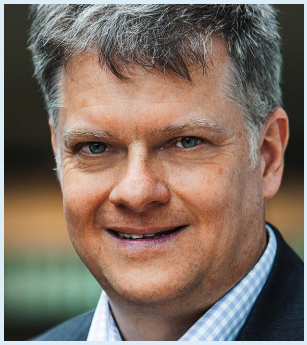
Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de



secorvo
security consulting

Secorvo Security News

September/Oktober 2021



Aufgelöste Verantwortung

Schneller als gedacht sind Cloud-Dienste zum neuen Standard geworden. Doch unsere Vorstellung, dass es dabei im Wesentlichen auf die Wahl eines vertrauenswürdigen Anbieters ankäme, ist zu kurz gesprungen.

Denn tatsächlich bestehen viele Cloud-Lösungen selbst wieder aus zahlreichen Einzeldiensten, die über die Cloud eingebunden werden: Ticketsystem, E-Mail-Services, Zahlungssystem, Benutzersupport, Shopsystem, Chat, Telefonie, Adressdatenbank, Tracking, Videostreaming ... – warum sollte ein Anbieter das auch neu implementieren, wenn er es günstig hinzukaufen kann?

Das Ergebnis ist – zumindest aus der Perspektive eines Datenschützers – fatal. Die Auftragsverarbeitungsverträge der Lösungsanbieter lesen sich wie das Who-is-who einschlägiger Cloud-Dienstleister: seitenlange Tabellen mit Unterauftragnehmern. Und schaut man sich deren AV-Verträge an, finden sich dort weitere Listen. Viele Unterauftragnehmer haben ihren Sitz im nichteuropäischen Ausland; wenn nicht, dann nutzen sie selbst nichteuropäische Dienstleister. Dass alle Verträge in dieser Kette korrekt geschlossen und die dokumentierten Schutzmaßnahmen sowie die Listen der Unterauftragnehmer der Wirklichkeit entsprechen, ist wenig wahrscheinlich – und praktisch nicht mit vertretbarem Aufwand überprüfbar.

Die Idee der Auftragsverarbeitung wird damit ad absurdum geführt. Denn im zerstückelten „Klein-Klein“ atomarer Cloud-Dienste bleibt die Verantwortung auf der Strecke. Wie sollte der Anbieter, dessen Sub-Sub-Sub-Auftragsverarbeiter seine Tickets in den USA verarbeiten lässt, den datenschutzkonformen Umgang sicherstellen?

Das erinnert ein wenig an die Finanzkrise 2008. Damals wurden die Ausfallrisiken von Immobilienkrediten durch Zerstückelung und Verteilung auf Investitionspapiere marginalisiert. Bis sie sich durch das Platzen der Immobilienblase plötzlich wirkungsvoll manifestierten.

Inhalt

secorvo
security consulting

Security News

Augen überall

Am 24.08.2021 berichtete das ZDF Magazin „frontal“, dass die von Tesla-Fahrzeugen regelmäßig in die Cloud des Herstellers hochgeladenen Daten auch die Bilddaten der am Auto verbauten acht hochauflösenden Kameras umfassen. Ob dafür der Hersteller (weil das Auto ohne die Übermittlung nicht vollumfänglich funktioniert) oder der Halter (da er der Übermittlung zugestimmt hat) die datenschutzrechtliche Verantwortung trägt, ist ungeklärt. Nach Auffassung der Aufsichtsbehörden sind Aufzeichnungen mit Dashcams nur in sehr engen Grenzen zulässig. Die niedersächsische Aufsichtsbehörde hält eine Speicherung nur bis maximal 30 Sekunden für rechtmäßig. Ähnliches gilt für die Video Doorbell von Ring, einer Amazon-Tochter, über die der SWR am 05.10.2021 berichtete. Über die mit Mikrofon ausgestattete Kamera können Hausbesitzer auf dem Mobilgerät verfolgen, was sich vor der heimischen Haustür so tut – und mit Besuchern Kontakt aufnehmen.

In beiden Fällen muss der Verantwortliche die Betroffenen nach Art. 12 ff. DSGVO über Art und Zweck der Verarbeitung informieren; dabei darf keine Erfassung des öffentlichen Raums erfolgen.

Die ggf. heimliche Tonübertragung der Video Doorbell kann zudem eine strafrechtlich relevante Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) darstellen. Auch sind die Geräte vor einiger Zeit durch Schwachstellen aufgefallen.

Bis zu einer datenschutzkonformen Lösung muss man wohl empfehlen, um Teslas und Video Doorbells einen großen Bogen zu machen.

ISO-Leitlinie Löschkonzept

Als praxisbewährte Hilfestellung für die Entwicklung von Löschkonzepten wurde bis 2016 unter der Federführung von Secorvo und mit Unterstützung der Unternehmen Blancco, DATEV, Deutsche Bahn und Toll Collect die „Leitlinie Löschkonzept“ entwickelt und schließlich als DIN 66398 verabschiedet (SSN 4/2016). 2018 startete die DIN das Projekt ISO/IEC 27555 zur Überführung der Leitlinie in einen internationalen Standard (SSN 7/2018). Jetzt ist es so weit: Am 08.10.2021 wurde die ISO/IEC 27555:2021 (Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion) publiziert. Die Vorgehensweise entspricht der DIN 66398; im Detail gibt es einige wenige Unterschiede. Der Text wurde redaktionell überarbeitet und deutlich gekürzt. Die DIN 66398 wurde im Juni 2021 vom zuständigen Arbeitskreis bestätigt und wird zunächst beibehalten.

Bad Practice 1FA

Wie u. a. im SANS-Newsletter vom 30.08.2021 gemeldet, hat die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) die Single-Factor-Authentifizierung auf die Liste der Bad Practices gesetzt. Aus unserer Sicht eine sinnvolle Ergänzung, nicht nur Best Practices sondern auch verbreitete „No Gos“ als Bad Practice zu „brandmarken“.

In internen Netzen und geschlossenen Umgebungen kann ein Kennwort als einziger Faktor ggf. noch angemessen sein. Bei über das Internet genutzten (Cloud-) Diensten ist das aufgrund der zahlreichen mit Kennworten verbundenen Gefährdungen wie Brute-Force-Angriffen, Phishing oder der Wiederverwendung von Kennworten nicht zu empfehlen.

One Time Token und Zertifikate haben sich in der Praxis bewährt. Wer darauf verzichtet, sollte sich darüber im Klaren sein, dass er bei einer Kompromittierung zu Recht eine Tasse mit Aufschrift „Das kannste schon so machen, aber dann isses halt …“ auf den Tisch gestellt bekommt. Auch die weiteren Anti-Empfehlungen der CISA Bad Practices lohnen einen genaueren Blick.

Willkommen 2FA

Viele Dienste bieten zur Verbesserung der Sicherheit zusätzlich eine Zwei-Faktor-Authentifizierung an. Ursprünglich waren dies TAN-Listen auf Papier. Mittlerweile werden die zusätzlichen Geheimnisse in Hardware-Token oder in Smartphone-Apps gespeichert wie die Authenticator-Apps von Google und Microsoft.

Privatanwendern wird nun für das Microsoft-Konto eine kennwortlose App-Authentifikation angeboten, die sie in den Sicherheitseinstellungen aktivieren können. Unternehmen und Bildungseinrichtungen steht diese Funktion bereits länger zur Verfügung. Statt der App kann z. B. auch ein FIDO2-Key verwendet werden. Angriffe auf gut zu merkende, aber zu einfache Passwörter sollen so der Vergangenheit angehören.

Prinzipiell kann das Verfahren als 2FA angesehen werden: Der Zugang erfordert den physischen Besitz des Smartphones, und beim iPhone ist die Authentikator-App zusätzlich durch einen Fingerabdruck gesichert. Damit das Entsperren des Smartphones dauerhaft nur dem Besitzer möglich ist, sind regelmäßige Sicherheitsupdates und eine komplexe PIN (oder gute Biometrie) essentiell. Damit zukünftig nicht jeder Dienst eine eigene Authentikator-App benötigt, bleibt zu hoffen, dass sich Standards wie FIDO2 durchsetzen.

Faxen unter der DSGVO

Nach der Bayrischen, der Niedersächsischen und der Bremischen Aufsichtsbehörde hat am 14.09.2021 auch der Hessische Datenschutzbeauftragte den Faxversand als unsicheres Übermittlungsverfahren eingestuft. Zwar verneint er die Zulässigkeit einer Fax-Übertragung personenbezogener oder auch besonders schutzbedürftiger Daten nicht generell, begrenzt sie jedoch auf dringliche Ausnahmefälle.

Der Vergleich der Aufsichtsbehörde mit dem E-Mail-Versand hinkt jedoch. Denn nach wie vor gilt (SSN 03/2021): Ein Fax ist genauso sicher wie ein Telefonat – beide nutzen heute TCP/IP-basierte Paketvermittlung. Und beide Übertragungen unterliegen dem Telekommunikationsgeheimnis, das die TK-Provider durch geeignete Schutzmaßnahmen sicherstellen müssen.

Die Technik der Faxübermittlung ist nicht unsicherer geworden. Die besonderen Gefahren beim Faxversand schützenswerter Daten liegen schon immer auf der „Benutzerebene", wie Zahlendreher bei der Fax-Nummer, Nutzung der Wahlwiederholungstaste oder ein Empfangsgerät, das Unberechtigten zugänglich ist. Daher ist die Empfehlung der Aufsichtsbehörde zutreffend, nach Möglichkeit alternative Übertragungstechniken zu wählen.

Transnationale Verhaltensregeln

Noch immer herrscht große Unsicherheit, wie die Anforderungen aus dem EuGH-Urteil Schrems II an internationale Datentransfers zu erfüllen sind. Ein Weg ist die Auswahl von Dienstleistern, die sich zur Einhaltung von der EU anerkannter transnationaler Verhaltensregeln verpflichten. Am 20.05.2021 wurden die Beschlussvorlagen zum EU Cloud Code of Conduct und zum Code of Conduct for Cloud Infrastructure Service Providers in der Version 2.11 als erster Transnational Code of Conduct vom Europäischen Datenschutzausschuss angenommen und damit deren DSGVO-Konformität bestätigt.

Datentransfer-Folgenabschätzung

Die am 04.06.2021 von der EU-Kommission verabschiedeten neuen Standardvertragsklauseln verlangen, dass im Hinblick auf internationale Datentransfers in Drittstaaten ohne anerkanntes angemessenes Datenschutzniveau sog. Transfer Impact Assessments (TIA) durchgeführt werden (Klauseln 14 a) - d)). Dabei ist eine mehrstufige Prüfung durchzuführen, die den besonderen Umständen der Datenübermittlung, also z. B. der Länge der Verarbeitungskette, den beabsichtigten Übertragungskanäle, den Kategorien und dem Format der übermittelten personenbezogenen Daten Rechnung tragen soll. Die relevanten Rechtsvorschriften des Bestimmungslandes müssen geprüft, die erforderlichen technischen und organisatorischen Schutzmaßnahmen (TOMs) müssen festgelegt werden.

Um hier eine Hilfestellung zu geben, hat die non-profit-Organisation iapp am 01.09.2021 ein Muster zur Durchführung eines solchen TIAs bereitgestellt, das für Übermittlungen in die USA hilfreich ist.

Secorvo News

Secorvo Seminare

Auf unserem letzten Seminar in diesem Jahr gibt es noch wenige freie Plätze: IT Security Insights, unser T.I.S.P.-Update (**30.11.–02.12.2021**). Natürlich freuen wir uns auch über Anmeldungen für unsere im kommenden Jahr geplanten Seminare. Eine Übersicht aller Termine und Seminarangebote finden Sie unter www.secorvo.de/seminare.

Schwarzer Gürtel

Unser Penetrationstester Enes Erdoğan hat jetzt ebenfalls den „schwarzen Gürtel" – seine OSCP-Zertifizierung. Herzlichen Glückwunsch!

Pilze und Sicherheitsstandards...

In den vergangenen Jahren ist die Zahl der Standards, Checklisten und Best Practices zur Informationssicherheit ständig gewachsen. Auf dem kommenden KA-IT-Si-Event am **18.11.2021** zeigt Ihnen Milan Burgdorf interessante Gebiete auf der Landkarte der Informationssicherheitsstandards und -frameworks. Dabei werden bekannte (ISO 2700x und IT-Grundschutz) und unbekannte Gegenden erkundet, damit Sie sich auf diesem unübersichtlichen Territorium besser zurecht finden. Wir freuen uns auf einen interessanten Abend mit Ihnen – diesmal wieder als Online-Event (zur Anmeldung).

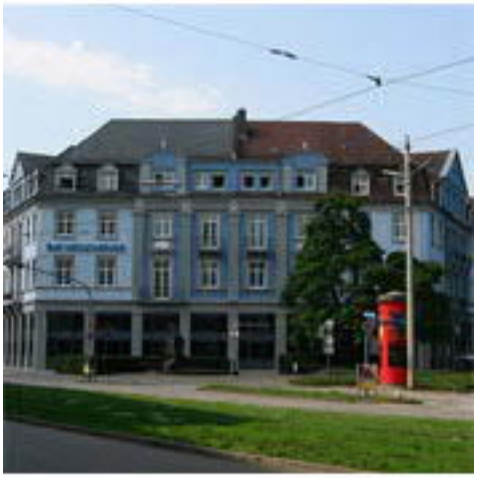
Krypto im Advent

Mit unserem interaktiven Online-Adventskalender „Krypto im Advent" lernen Schülerinnen und Schüler (3.-9. Klasse) seit 2015 auf spielerische Weise Verschlüsselungstechniken kennen und können dabei attraktive Sachpreise gewinnen. Zusammen mit der PH Karlsruhe haben wir uns auch diesmal wieder spannende Kryptografie-Rätsel ausgedacht. Schulklassen und Profis können ebenfalls „miträtseln", letztere allerdings außer Konkurrenz. Anmeldungen sind ab dem 01.11.2021 auf Krypto-im-Advent.de möglich (Teilnahme kostenlos).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2021	
14.-19.11.	ACM CCS 2021 (ACM/SIGSAC, Seoul/KOR)
17.-19.11.	45. DAFTA (GDD, virtuell)
18.-19.11.	DeepSec 2021 (DeepSec, Wien/AT)
30.11.-02.12.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Januar 2022	
24.-26.01.	Omnisecure 2022 (in TIME berlin, Berlin)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

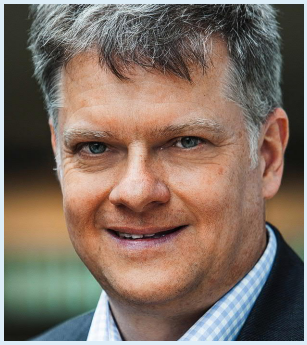
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

November 2021



Keks-Transparente

Sie nerven. Kaum eine Webseite, die noch ohne Mausklick zu erreichen wäre: Zuerst muss man den „Cookie-Banner" hinter sich bringen. Schlimmer noch: Seltenst kann man das Tracking mit einem einzigen Klick ablehnen – erst auf einer weiteren Seite, oft nach längerem Scrollen und manchmal erst nach mühseligem Deaktivieren der (rechtswidrig) voreingestellten ungewünschten Datenerhebungen. Dabei versuchen Text, Hervorhebung und Farbe der „Knöpfe" den Besucher zu einem vorschnellen „Einverstanden" zu bewegen – „Nudging" heißt dieser neue Wettlauf zwischen Werbestrategen und genervten Seitenbesuchern.

Die gewählte Cookie-Einstellung wird gespeichert – in einem Cookie natürlich, das bei einer datensparsamen Browser-Konfiguration beim Schließen sorgsam von der Festplatte gelöscht wird. Und beim nächsten Seitenbesuch geht alles wieder von vorne los. Bleiben die Webseiten ohne Banner. Sie sind fast noch schlimmer, denn wer einen Tracker-Alarm in seinem Browser installiert hat, weiß, dass die meisten dieser Seiten einfach ohne Einwilligung tracken. So nagt unvermeidlich der Gedanke im Hinterkopf, dass man diese Seiten eigentlich sofort verlassen müsste.

Kein Wunder, dass viele Menschen ein Ziel für ihren Ärger suchen – und es in der DSGVO finden: einem weiteren Beispiel für ausufernde Brüsseler Regelungsbürokratie. Der britische Kultusminister Oliver Dowden dürfte vielen aus dem Herzen gesprochen haben, als er im August die „Abschaffung der endlosen Cookie-Hinweise" forderte.

Alles verständlich. Und dennoch Unsinn. Das ist, als würde man fordern, allen Autofahrern, die auf fremden Grundstücken parken wollen, das Fragen um Erlaubnis zu erlassen – weil so viele fragen.

Verursacher der Cookie-Banner ist nicht der Datenschutz. Sondern die hemmungslose Aufdringlichkeit, mit der Webseitenbetreiber unser Nutzerverhalten protokollieren und auswerten.

Inhalt

secorvo
security consulting

Security News

Ja, ich will!

Der Bayerische Beauftragte für Datenschutz hat am 01.09.2021 eine Orientierungshilfe zum Thema Einwilligung herausgebracht. Diese ist all denjenigen zur Lektüre zu empfehlen, die sich bei der Verarbeitung personenbezogener Daten auf Einwilligungen stützen. Besonders relevant ist dies bei der Gestaltung von Webseiten, die mehr als nur technisch notwendige Cookies verwenden. Unberücksichtigt bleibt darin leider das am 01.12.2021 in Kraft getretene TTDSG, in dem Einwilligungsmanagement und Einwilligungstreuhänder vorgesehen sind. Dazu sollte man sich zeitnah anderweitig informieren.

Ransomware: Never Ending Story

Am 08.11.2021 schaffte es wieder einmal ein Angriff mit Ransomware in die Tagespresse. Dass es sich bei dem Angriff auf den Media-Saturn-Konzern nicht um einen Einzelfall handelt, kann man live auf der Cyberbedrohung Echtzeitkarte von Kaspersky beobachten oder dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland des BSI entnehmen.

Neben einem angemessenen Schutz vor Ransomware und anderer Schadsoftware sollte es auch selbstverständlich sein, Vorkehrungen für die Schadensbegrenzung im Fall einer Infektion zu treffen: Verzicht auf unnötige administrative Berechtigungen, Virenschutz, Einschränkungen von Programmausführungen, Makrosicherheit und ein Backup nach der 3-2-1-Regel gehören dazu. Für dunkle Wintertage empfehlen wir die ausführliche Publikation des BSI zum Thema Ransomware mit sinnvollen weitergehenden Maßnahmen zur Lektüre.

Ich sehe was, was Du nicht siehst

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) hat am 27.10.2021 Hinweise und eine Handreichung zur praktischen Nutzung von Videokonferenzsystemen veröffentlicht. Gemäß Pressemitteilung will der LfDI keine „detaillierten Hinweise zu allen möglichen Konfigurationen und Vertragsgestaltungen geben", sondern bei der Auswahl und Einrichtung des „richtigen" Systems unterstützen.

Leider gelingt dies der Handreichung nicht. Die einführenden Rahmenbedingungen und Empfehlungen sind möglicherweise für den einen oder anderen Nutzer hilfreich. Problematisch sind jedoch die Hinweise zu den verschiedenen Anbietern: Hier fehlt es an einer einheitlichen Darstellung und an der Bewertung des aktuellen Stands der datenschutzrelevanten Dokumente. Es wird erkennbar, dass keine neutrale Beurteilung stattgefunden hat. Daher sollte man zur Auswahl weitere Dokumente wie etwa den Mindeststandard des BSI zu Videokonferenzdiensten als Checkliste hinzuziehen (s. u.).

Videokonferenz-Mindeststandard

Am 07.10.2021 hat das BSI einen Mindeststandard für Videokonferenzdienste veröffentlicht. Obwohl die BSI-Mindeststandards unmittelbar nur für die Informationstechnik des Bundes gelten, enthalten sie häufig praxisorientierte Hinweise in kompakter Form, die auch für andere Behörden und Unternehmen hilfreich sind. Ohne auf bekannte Videokonferenzprodukte einzugehen, werden typische Sicherheits- und Funktionsanforderungen wie ein Rollenkonzept, Verschlüsselung, Dateiablagen, das Teilen von Bildschirminhalten oder Sicherheitsupdates vorgestellt. Zusätzlich wird darauf aufmerksam gemacht, nicht benötigte Funktionen abzuschalten und die Beschäftigten in die Verwendung und Moderation des Videokonferenz-Tools einzuweisen. Bei Einführung oder Betrieb eines Videokonferenzdienstes kann der Mindeststandard somit als Checkliste verwendet werden, um Informationssicherheitsanforderungen an einen Videokonferenzdienst systematisch umzusetzen.

Kontextfreie MFA

Dass auch eine Multi-Faktor-Authentifikation (MFA) ohne vernünftiges „User-Interface" schief gehen kann, illustrierte Roger Grimes am 20.10.2021 anhand einiger Beispiele. Darunter ist das eines Vice Präsidenten, der ein Login mehrfach mit einem zugesandten zweiten Faktor bestätigte, obwohl er sich nirgends anmelden wollte – und so Angreifer in die Firma ließ.

Solche Fehler darf man nicht allein dem Nutzer vorwerfen, denn oft fehlt bei der Zusendung des zweiten Faktors der Kontext. Einen Sicherheitsexperten wird eine kontextfreie MFA sicherlich Verdacht schöpfen lassen – einen an „kryptische" E-Mails von der IT gewöhnten Mitarbeiter aber vielleicht nicht. Verständlichkeit und Nachvollziehbarkeit sind für einen wirksamen Schutz unverzichtbar.

Einmal keine Updates eingespielt...

Im Tätigkeitsbericht der niedersächsischen Aufsichtsbehörde für 2020 wird von einem Bußgeld in Höhe von 65.000 Euro gegen einen Onlineshop-Betreiber berichtet, der seine Shop-Anwendung fünf Jahre lang nicht aktualisierte, obwohl der Softwarehersteller auf erhebliche Sicherheitslücken hingewiesen und eine neue Version bereitgestellt hatte. Wesentlich für die Aufsichtsbehörde war, dass nach Art. 24 Abs. 1 DSGVO Schutzmaßnahmen vom Verarbeiter überprüft und aktualisiert werden

müssen und dass die Verwendung aktueller, um Sicherheitslücken bereinigter Software für das Unternehmen nicht unverhältnismäßig gewesen wäre. Auch im Tätigkeitsbericht der baden-württembergischen Aufsichtsbehörde für 2020 findet sich ein Bericht über ein Bußgeld in Höhe von 1,2 Mio. Euro gegen eine Krankenkasse, die Maßnahmen zum Schutz der Daten von Gewinnspielteilnehmern nur unzureichend umgesetzt hatte.

Zur Handlungspflicht bei Kenntnis einer Schwachstelle gibt die Pressemitteilung der baden-württembergischen Aufsichtsbehörde Hinweise, was sie beispielsweise bei der Exchange-Lücke von den Betreibern erwartete.

Die Aufsichtsbehörden tolerieren eine nachlässige Umsetzung von technischen und organisatorischen Maßnahmen nicht, erwarten regelmäßige oder anlassbezogene Überprüfungen und insbesondere das zügige Einspielen von Sicherheitsupdates. Sofern personenbezogene Daten verarbeitet werden, ist Informationssicherheit nach Stand der Technik Pflicht.

Top Hardware-Schwachstellen

Die OWASP Top 10 sind mittlerweile jedem ein Begriff, wenn es um die verbreitetsten Schwachstellen in Web-Anwendungen geht. Dass Sicherheit jedoch gerade im Kontext von IoT auch weit mehr als klassische Web-Anwendungen umfasst, griff am 26.10.2021 die MITRE auf und veröffentlichte die 2021 CWE Most Important Hardware Weaknesses bestehend aus den zwölf bedeutendsten Schwachstellenklassen von Hardware. Dazu zählen beispielsweise schlechte kryptographische Implementierungen, unzureichender Schutz gegen Debugging oder fehlende Funktionen für Firmware-Updates.

Insgesamt haben sich die Common Weakness Enumeration (CWE) in den vergangenen Jahren immer weiter durchgesetzt und sind auch bei uns insbesondere im Pentesting zum Standard für die Kategorisierung von Schwachstellen geworden. So liefert die Datenbank nicht nur allgemeine Informationen zur Schwachstelle und Beispiele, sondern auch Gegenmaßnahmen und Referenzen zu Vorkommen der Schwachstelle in Form von CVEs. Für verschiedenste Anwendungsfälle bietet die Datenbank Mappings und Ansichten an, welche die Navigation signifikant erleichtern.

Secorvo News

Schwarze Gürtel

Im November haben Mitglieder des Secorvo-Teams drei weitere Zertifizierungen erhalten: Enes Erdoğan bestand die 24stündige Prüfung zum „Offensive Security Certified Professional“ (OSCP) und ist jetzt Träger des ‚schwarzen Gürtels‘ für Pentester. André Domnick erwarb in einer 48stündigen Prüfung den bereits dritten DAN und darf sich nun „Offensive Security Experienced Penetration Tester“ (OSEP) nennen. Und Milan Burgdorf erhielt die Zertifizierung zum ISO/IEC 27001-Auditor – die ‚Lizenz zum Prüfen‘. Herzlichen Glückwunsch!

White Paper „Penetrationstests”

Viele Unternehmen führen regelmäßig technische Sicherheitsprüfungen der IT-Infrastruktur in Form von externen Penetrationstests durch. Für solche Tests haben wir aus unserer langjährigen Erfahrung eine standardisierte Vorgehensweise entwickelt, die eine wiederholbare und modularisierte Durchführung erlaubt.

Am 11.11.2021 haben wir eine überarbeitete und erweiterte Version unseres White Papers „Penetrationstests“ veröffentlicht, in dem wir die Vorgehensweise von Secorvo vorstellen und konkrete Empfehlungen zur erfolgreichen Durchführung von Penetrationstests geben. Gerne finden wir auch für Sie die zu Ihrem Unternehmen passende Vorgehensweise.

Seminare

Mit sehr positiver Resonanz haben wir das Seminar „IT Security Insights“ erstmals online durchgeführt: praktische Übungen und aktuelle Themen der IT-Sicherheit als ‚Update‘ für IT-Sicherheitsbeauftragte und -Experten. Die nächste Gelegenheit zur Teilnahme, die hoffentlich wieder in Präsenz möglich sein wird, haben Sie vom **15. bis 17.03.2022**. Davor bieten wir Ihnen vom **07. bis 11.03.2022** die Möglichkeit, sich zum T.I.S.P. zu zertifizieren, unterstützt von unserem T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“. Weitere Termine, Programme und die Möglichkeit zur Anmeldung finden Sie unter secorvo.de/seminare.

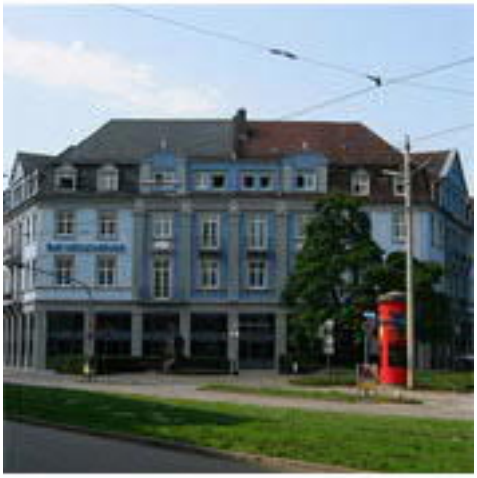
Rätseln mit Lerneffekt

Es ist wieder so weit: Mit dem interaktiven Online-Adventskalender „Krypto im Advent“ lernen Schülerinnen und Schüler (3.-9. Klasse) vom 1. bis 24.12. auf spielerische Weise Verschlüsselungstechniken kennen und können dabei attraktive Sachpreise gewinnen. Die PH Karlsruhe und die KA-IT-Si haben sich für die siebte Auflage des Adventskalenders wieder spannende Kryptografie-Rätsel ausgedacht. Ein Einstieg ist auch nach dem 1.12. noch möglich. Auch Schulklassen und Profis dürfen miträtseln, letztere allerdings außer Konkurrenz (zur kostenfreien Registrierung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2022	
14.-16.01.	ShmooCon2022 (The Shmoo Group, Washington/US)
Februar 2022	
01.-02.02.	18. Deutscher IT-Sicherheitskongress (BSI, virtuell)
03.02.	KA-IT-Si-Event „Willkommen bei den Quanten“ (KA-IT-Si, hybrid)
03.-04.02.	29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
März 2022	
07.-11.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.-17.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, Darmstadt)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de