Secorvo Security News

April 2022

Cyber, Cyber, Cyberagentur

Mit der von der Bundesregierung 2020 gegründeten „Agentur für Innovation in der Cybersicherheit“ soll Deutschland „bei der Cybersicherheit im internationalen Vergleich die Führung, zumindest eine Spitzenposition übernehmen.“ Um das zu erreichen, soll sie Forschung und bahnbrechende Innovationen im Bereich der Cybersicherheit vorantreiben (Strategie 2022-2025). Bis 2023 stehen ihr dafür zunächst 280 Mio. € Steuergeld zur Verfügung. Wem hilft das? Seit 1991 gibt es das BSI mit inzwischen über 1.300 Mitarbeitern (Jahresetat 200 Mio. €), es forschen das Horst-Görtz-Institut für IT-Sicherheit in Bochum, das Helmholtz-Zentrum für Informationssicherheit in Saarbrücken, die KASTEL Security Research Labs am Karlsruher KIT und seit 2004 das Fraunhofer Institut für Sichere Informationstechnologie an der TU Darmstadt sowie die Lehrstühle für IT-Sicherheit an 50 deutschen Hochschulen und Universitäten und die Kompetenzzentren für IT-Sicherheit der 16 Bundesländer. An Institutionen und Agenturen mangelt es nun wirklich nicht.

Die Herausforderungen der Informationssicherheit liegen jedoch nicht in fehlenden Technologien, die auf zauberhafte Weise Sicherheit produzieren: Es mangelt an der Umsetzung bekannter Schutzmaßnahmen. Schließlich ist in der ISO 2700x, dem BSI IT-Grundschutz und vielen weiteren Standards ordentlich definiert, wie Unternehmen sich wirksam schützen können. Doch es fehlen nicht zuletzt Experten für die Umsetzung. Wie sinnvoll ist es, weitere Technologien am Ende der Fahnenstange zu erforschen, wenn die Stange selbst wackelig im Morast steckt? Wenn Hersteller mangels Produkthaftung Security Engineering und sichere Softwareentwicklung nicht ernst nehmen? Ein Auto braucht kein Radar zur Fußgängererkennung, wenn nicht mal die Bremsen zuverlässig funktionieren. Da könnte schon helfen, wenn Kinder bereits in der Grundschule lernen würden, besser nicht auf jeden Anhang zu klicken.

Security News

Cloud-Ausfallerscheinungen

Den meisten Verantwortlichen, die Dienste und Anwendungen „in die Cloud“ auslagern, dürfte klar sein, dass man damit Risiken verlagert: Der Ausfall eigener Systeme wird weniger relevant, und eigene Maßnahmen zur Absicherung von Systemen und Räumlichkeiten können eingespart werden.

Im Gegenzug begibt man sich in eine Abhängigkeit: Bei Ausfall der Internetanbindung oder des Cloud-Anbieters selbst können die Dienste nicht genutzt werden.

In den meisten Fällen wird man dieses Risiko tragen und in Kauf nehmen, dass ein Anbieter mal einzelne Stunden bis hin zu ein oder zwei Tagen nicht zur Verfügung steht.

Wie sieht es aber aus, wenn Dienste – wie am 05.04.2022 bei Atlassian – für bis zu zwei Wochen ausfallen? Welche Auswirkungen hat das auf die Geschäftsprozesse? Müssen Entwickler nach Hause geschickt werden, da sie ohne ihre Cloud-Werkzeuge keine Software entwickeln können? Gibt es zeitkritische Prozesse, die nicht mehr funktionieren, wenn ein Dienst länger nicht zur Verfügung steht? Werden möglicherweise Sicherheitsprobleme übersehen, wenn Alarmierungen aus der Cloud nicht mehr eingehen?

Gerade versteckte Abhängigkeiten in immer stärker miteinander verzahnten digitalen Prozessen werden bei einer oberflächlichen Risikobewertung leicht übersehen – je mehr Cloud-Dienste in Anspruch genommen werden, desto genauer und häufiger sollte die Risiko-Prüfung wiederholt werden. Zur Sicherheit sollte man außerdem „analoge" Ersatzprozesse vorsehen, um größere Ausfall-Schäden zu verhindern.

Drum prüfe, wer prüfen lässt

Der von Google angebotene Dienst VirusTotal überprüft hochgeladene Dateien kostenlos mit etwa 70 verschiedenen Antiviren-Programmen. Doch nur wenige Nutzer dürften zuvor die Benutzerhinweise gelesen haben, in denen darauf hingewiesen wird, dass keine personenbezogenen Daten hochgeladen werden sollen.

Am 15.03.2022 warnte das BSI vor möglichen Datenabflüssen bei VirusTotal, wenn statt Datei-Hashwerten beispielsweise unternehmensinterne Dokumente oder E-Mails hochgeladen werden. Neben den unternehmenseigenen Vorgaben zu Datenschutz und Informationssicherheit sind bei der Nutzung das Geschäftsgeheimnisgesetz und die DSGVO zu beachten.

Das kann auch für Antiviren-Programme gelten, bei denen die Virenerkennung cloudbasiert erfolgt. Hat der Hersteller seinen Sitz außerhalb der EU, müssen die hohen rechtlichen Anforderungen an eine Übermittlung personenbezogener Daten in Drittstaaten (wie bspw. die USA) erfüllt sein.

Cookie-Banner

Auf heutigen Webseiten sind (nervtötende) Cookie-Banner allgegenwärtig. Wer keine Cookies möchte, dem wird die Ablehnung meist obendrein durch „Dark Pattern"-Techniken erschwert, mit denen Besucher durch entsprechende Gestaltung der Banner dazu bewegt werden sollen, gegen ihren Willen eine Einwilligung zu erteilen. Um dieser Entwicklung entgegenzuwirken hat das European Data Protection Board (EDBP) am 15.03.2022 Richtlinien zur korrekten Bannergestaltung beschlossen.

Zuvor hatte die französische Datenschutzaufsicht CNIL am 31.12.2021 wegen eines zu umständlichen Verfahrens zur Cookie-Ablehnung ein 150-Mio.-€-Bußgeld gegen Google verhängt. In dieselbe Kerbe schlägt jetzt auch die Hamburgische Datenschutzaufsicht. Am

05.04.2022 forderte Thomas Fuchs (HmbBfDI) für Cookie-Banner einen „Alles ablehnen"-Knopf: Eine wirksame Einwilligung läge nur dann vor, wenn Zustimmung und Ablehnung gleichermaßen schnell und einfach zugänglich seien.

Doch auch diese Forderung greift noch zu kurz. Denn tatsächlich sind Cookie-Banner eine absurde Degeneration der datenschutzrechtlichen Einwilligung. Stellen Sie sich vor, in Ihrem örtlichen Supermarkt lägen ab sofort mehrere Packungen Kekse in jedem Einkaufswagen, die Sie vor Einkaufsbeginn aus dem Wagen herausnehmen müssten, wenn Sie sie nicht kaufen wollen. Genauso zwingen Cookie-Banner Seitenbesucher den Aufwand einer aktiven Ablehnung auf – anstatt bei Ignorieren des Banners automatisch von einer nicht erteilten Einwilligung auszugehen. Tatsächlich ist zu wünschen, dass die Aufsichtsbehörden bei Cookie-Bannern noch eine deutlich härtere Gangart wählen.

Bike Scamming

Schon am 07.08.2021 hatte die New York Post über Scamming-Angriffe auf das Buchungsverfahren der in New York verbreiteten City Bikes berichtet, nachdem der Angriff kurz zuvor bei Reddit beschrieben worden war. Die Attacke ist geradezu trivial und kommt gänzlich ohne IT aus: Zum Freischalten des Mietrads muss der Nutzer den auf dem Rad aufgeklebten QR-Code mit der Buchungs-App einscannen. Klebt man den QR-Code eines Rads auf ein anderes, kann man „sein" Rad durch einen anderen Kunden (auf dessen Kosten) freischalten lassen.

Dieser simple Scamming-Angriff funktioniert bei allen Sharing-Systemen, bei denen die Identifikation des Fahrzeugs über einen aufgebrachten Code erfolgt – eine verbreitete Methode übrigens auch bei E-Scootern. Es lohnt also, sich vor Freischalten des Fahrzeugs davon zu überzeugen, dass der aufgebrachte Code nicht überklebt oder ausgetauscht wurde.

Der geschilderte Angriff ist ein eindrückliches Beispiel dafür, dass die Optimierung des Benutzerkomforts schnell auf Kosten der Sicherheit geht. Da lohnt es, sich gelegentlich Einsteins Bonmot in Erinnerung zu rufen: „Mache die Dinge so einfach wie möglich. Aber nicht einfacher."

Neuer Auskunftsanspruch

Das am 01.12.2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) regelt in §§ 21 ff. verschiedene Auskunftsansprüche. Neu ist § 21 Abs. 2 TTDSG, der Betreiber von Social-Media-Plattformen verpflichtet, Betroffenen mitzuteilen, wer als Verursacher einer Persönlichkeitsverletzung in Betracht kommt. Der Anspruch ist auch gegen Anbieter von Telemedien durchsetzbar, die zwar keinen Sitz in Deutschland haben, aber ihre Dienste auch in Deutschland erbringen.

Allerdings begrenzte das Schleswig-Holsteinische Oberlandesgericht am 23.03.2022 die Auskunft auf Bestandsdaten; Nutzungsdaten sind nicht mitzuteilen. Da die Verletzung der Auskunftspflicht nicht strafbewehrt ist und ohne Nutzungsdaten kein Nachweis für die Täterschaft vorliegt, ist der Anspruch in der

Praxis eher ein stumpfes Schwert. Um wenigstens mittelbar an die Nutzungsdaten zu gelangen, bleibt den Betroffenen daher auch weiterhin nur der Weg über eine Strafanzeige.

Post-Corona-Aufräumarbeiten

Während der Corona-Pandemie wurden an vielen Orten – in Restaurants, Schulen, Krankenhäusern, Pflegeheimen und bei den Gesundheitsämtern – personenbezogene Daten von Bürgern erhoben und gespeichert. Nach Ablauf der jeweiligen Löschfrist, spätestens aber mit dem Wegfall der Rechtsgrundlagen wie den Corona-Verordnungen und dem Infektionsschutzgesetz sind diese Daten zu löschen.

Der Baden-Württembergische Landesdatenschutzbeauftragte Dr. Stefan Brink hat die wichtigsten Verarbeitungen in seiner Pressemitteilung vom 08.04.2022 („Zurück zur Freiheit“) aufgelistet. Darin weist er auch darauf hin, dass Arbeitgeber (bis auf die Heil- und Pflegebranche) alle erhobenen Daten über den Impfstatus der Mitarbeiter unverzüglich löschen müssen – und kündigt stichprobenartige Überprüfungen an.

NEO-Innovationspreis

Die TechnologieRegion Karlsruhe hat den diesjährigen Innovationspreis NEO2022 dem Thema „Cybersecurity“ gewidmet. Für den mit 20.000 € dotierten Preis können sich Unternehmen bundesweit bis zum 19.05.2022 online bewerben. Die Preisverleihung wird am 21.10.2022 in Karlsruhe stattfinden.

Secorvo News

Der frühe Vogel …

… fängt den Wurm: Das gilt auch für die Buchung Ihrer Weiterbildung. Melden Sie sich bereits jetzt zum T.I.S.P.-Seminar im September an (**19.–23.09.2022**) und bereiten Sie sich mit dem T.I.S.P.-Buch von Secorvo, das wir Ihnen nach Ihrer Anmeldung zusenden, entspannt darauf vor.

Bereits zertifizierten T.I.S.P.-Absolventen und erfahrenen Sicherheitsexperten bieten wir das Seminar IT Security Insights mit ausgewählten vertieften Beiträgen zu aktuellen Themen der IT-Sicherheit (**27.–29.09.2022**).

Wer eine gründliche Einführung in Theorie und Praxis von Public Key Infrastrukturen sucht, sollte sich unser viertägiges PKI-Seminar (**04.–07.11.2022**) im Kalender vermerken. Und Ende November bietet sich die nächste Möglichkeit, sich zum BSI Vorfall-Experten ausbilden zu lassen (**29.11.–01.12.2022**).

Die ausführlichen Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Wer besitzt mein Smartphone?

Auch wenn wir uns kaum noch daran erinnern können, wie wir ohne sie klarkamen: Smartphones gibt es erst seit 15 Jahren. Genauso alt wie das Smartphone ist die Geschichte der Smartphone Hacks – von den

ersten Jailbreaks über die Celebrity Nudes bis hin zu kommerzieller und staatlicher Spyware.

Anhand von Attack Trees und Live-Hacking-Demos zeigen Ihnen Armin Harbrecht und Maximilian Stauß (aramido) beim kommenden KA-IT-Si-Event am **19.05.2022** um 18 Uhr, wie Smartphones angegriffen werden. Dieses Verständnis ist Voraussetzung für effektive Schutzmaßnahmen.

Die Veranstaltung führen wir hybrid durch. Die Vor-Ort-Plätze bei aramido sind bereits ausgebucht, aber für eine Online-Teilnahme können Sie sich noch anmelden (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2022	
10.-13.05.	Blackhat Asia 2022 (Blackhat, hybrid)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)
10.-11.05.	BvD Verbandstage 2022 (BvD, Berlin)
16.-17.05.	23. Datenschutzkongress (EUROFORUM, Berlin)
16.-18.05.	Entwicklertag 2022 (VKSI, GI, ObjektForum, Karlsruhe)
19.05.	Wer besitzt mein Smartphone? (KA-IT-Si, Karlsruhe)
30.05.-03.06.	Eurocrypt 2022 (IACR, Trondheim/NOR)
Juni 2022	
06.-10.06.	7th IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/I)
06.-08.06.	OWASP Global AppSec (OWASP Foundation, Dublin/IRL)
20.-21.06.	DuD 2022 (COMPUTAS, Berlin)

Fundsache

Am 31.03.2022 wurde Version 4.0 des PCI DSS Standards veröffentlicht. Der Standard legt umfangreiche technische und organisatorische Anforderungen an Zahlungssysteme und Dienstleistungen fest. Diese wurden konkretisiert und verschärft. Die Änderungen zur Vorgängerversion 3.2.1 sind ebenso wie der Standard selbst auf Englisch, Deutsch und Portugiesisch verfügbar. Einige neue Anforderungen müssen PCI-kompatible Anbieter bis spätestens 31.03.2025 umsetzen.

Impressum

Secorvo Security News – ISSN 1613-4311

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

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