secorvo
security consulting

Secorvo Security News

Oktober 2023

Herrschaftswissen

Der Philosoph *Max Scheler* (1874-1928) definierte in seiner Anthropologie Herrschaftswissen als das Wissen, das der Stabilisierung einer Herrschaft und deren Machtbestrebungen dient.

Im Kern ist darunter jeder Wissensvorsprung zu verstehen, der in diesem Sinne vorteilhaft für den Wissenden ist. Jede Herrschaft ist bestrebt, sich mit solchen exklusiven Wissensvorsprüngen zu stabilisieren – je prekärer die Legitimation, je geringer der Rückhalt bei den Beherrschten und je größer die äußere Bedrohung, desto stärker dieses Bestreben. Spionage, nach außen und nach innen, ist daher die logische Folge jeder Herrschaft – vor allem einer prekären.

Da Herrschaftswissen in der Hand der Herrschenden eine mächtige Waffe sein kann, versuchen Demokratien, Herrschaftswissen überall dort zu begrenzen, wo es der Exekutive Macht über den eigentlichen Souverän – das Volk – gibt. Aus dieser Perspektive lässt sich Datenschutz verstehen als eine systematische Begrenzung des Herrschaftswissens über Menschen: Die Forderung einer Rechtsgrundlage für die Verarbeitung, die strikte Zweckbindung und strenge Löschfristen sollen verhindern, dass solches Herrschaftswissen überhaupt erst entsteht.

Auch im sozialen Miteinander soll Datenschutz die Allokation von Herrschaftswissen zumindest erschweren, denn ein Airtag, der einem Stalker den Aufenthaltsort seines Opfers verrät, ist ein ähnlich starkes Machtinstrument wie eine Spionage-Drohne oder ein versteckter GPS-Sender. Daher sollte dem Verbot der anlasslosen Vorratsdatenspeicherung (BVerwG 6 C 6.22/7.22) nun auch bald ein Verbot der Nutzung von Informationstechnik zur heimlichen Feststellung des aktuellen Aufenthaltsorts von Personen folgen.

Auf kurze Löschfristen sollte man auch bei jeder App achten, die personenbezogene Daten speichert. In die falschen Hände geraten können auch sie – und damit zu Herrschaftswissen mutieren.

Inhalt

secorvo
security consulting

Security News

Konfigurationsfehler

Am 05.10.2023 stellten CISA und NSA eine gemeinsame Übersicht der Top Ten Cybersecurity Misconfigurations. Einige der aufgelisteten Konfigurationsfehler scheinen auf den ersten Blick ein alter Hut zu sein: In der Praxis ermöglichen aber offensichtlich eben diese alten Hüte immer wieder Einbrüche in IT-Infrastrukturen. Das Dokument enthält detaillierte Ursachenanalysen und Gegenmaßnahmen für die identifizierten Top Ten. Dabei wird immer wieder auf die hilfreichen Werkzeuge Mitre ATT&CK und Mitre D3FEND verwiesen.

Die Hartnäckigkeit der Schwachstellenmuster im Betrieb ähnelt der der Weaknesses in der Software-Entwicklung. Vielleicht sollten sie ähnlich exponiert und populär kommuniziert werden, wie es Mitre mit den CWE vormacht.

Schwachstellenschwemme

Die National Vulnerability Database des NIST weist für Oktober 2023 erneut über 2000 neu veröffentlichte Schwachstellen aus. Mindestens zehn dieser Verwundbarkeiten werden bereits aktiv ausgenutzt. Betroffen sind u. a. der Netscaler (Citrix) und Confluence (Atlassian). Besonders kritisch ist die mit dem Maximalscore 10.0 bewertete Cisco-IOS-XE-Lücke, da die Admin-Schnittstelle von Tausenden von Switches und Routern über das Internet erreichbar ist (siehe NET.3.1.A4, BSI-Grundschutz) und die Geräte daher ein leichtes Opfer sind. Dabei wären viele Lücken vermeidbar, etwa beim Cisco Emergency Responder, der mit einem Standard-Admin-Passwort ausgeliefert wurde.

Secure by Design – Joint Effort

Am 25.10.2023 hat die US-amerikanische CISA vor dem Hintergrund einer nicht nachlassenden Anzahl von Security-Schwachstellen in Produkten nachdrücklich auf die Handreichung Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software hingewiesen. Darin haben viele internationale Sicherheitsbehörden grundlegende Bausteine für sichere Software-Produkte übersichtlich zusammengestellt. Die Hinweise wurden im April 2023 vom BSI vorgestellt.

Wir empfehlen nachdrücklich, die darin vorgestellten Prinzipien ernst zu nehmen – auch vor dem Hintergrund der Anforderungen, die voraussichtlich mit dem Cyber-Resilience-Act an die Sicherheit von Software gestellt werden.

Das Thema Secure by Design Software ist auch ein Baustein im T.P.S.S.E.-Seminar, das sich umfassend mit Sicherheit in der Software-Entwicklung beschäftigt – die Bekämpfung von Schwachstellen also von der Wurzel aus angeht.

Meinungsmache

Am 04.09.2023 veröffentlichte die Mozilla Foundation eine „Studie", nach der moderne Autos ein „Datenschutz-Albtraum" seien. Mehrere Medien zitierten die Veröffentlichung, darunter der heise-Newsticker. Befasst man sich jedoch eingehender mit dem Text (vulgo: liest man ihn…), kommt man schnell zu dem Ergebnis, dass von einer systematischen Analyse keine Rede sein kann – die „Forschungsergebnisse" sind Resultat einer Durchsicht der Datenschutzerklärungen von 25 Herstellern und einer offenbar vorurteilsbeladenen und kompetenzbefreiten Sicht der Autoren. Zitat: „Automarken stellen mit Ihren persönlichen Daten oft alles Erdenkliche an, was noch irgendwie im rechtlichen Rahmen zulässig ist." Oder: „Am meisten Sorgen macht uns, dass wir nicht einmal wissen, ob überhaupt eine der geprüften Marken alle persönlichen, im Auto gespeicherten Daten verschlüsselt." Die anhängenden Vitae der Autoren lassen ebenfalls kein Expertenwissen im Datenschutz erkennen – die Autoren sehen sich selbst als „investigative Storyteller".

Undifferenzierte und inkompetente Positionspapiere dieser Art stiften mehr Schaden als Nutzen, machen sie es doch leicht, die Kritik als Scharlatanerie abzutun. Denn in einigen Punkten ist fundierte Kritik durchaus berechtigt – und tatsächlich sollten die Datenschutzerklärungen vieler Hersteller durchaus aussagekräftiger sein.

Auskunftsrecht

Das Recht eines jeden Menschen auf Auskunft über Verarbeitungen seiner personenbezogenen Daten ist in Art. 8 der EU-Grundrechtscharta verankert. In der Folge wurde 2013 das Recht auf Einsichtnahme in die eigene Patientenakte als § 630g ins Bürgerliche Gesetzbuch aufgenommen. Seitdem wurde allerdings immer wieder über die Frage gestritten, ob ein Patient die Kosten des Kopierens der Akte tragen muss.

Am 26.10.2023 hat nun der EuGH diese Frage abschließend höchstrichterlich beantwortet – mit einem klaren „Nein". Die Kosten der (ersten) Kopie einer Patientenakte sind vom Arzt bzw. der Klinik zu tragen (C-307/22). Das ist ein Sieg der Transparenz – der aber auch zu einer erheblichen Belastung medizinischer Einrichtungen werden kann, wenn viele Patienten eine Kopie anfordern.

Die Entscheidung des EuGH könnte daher die Digitalisierung im Gesundheitswesen beschleunigen, denn eine elektronische Gesundheitsakte würde nicht nur die Archivierung, sondern auch die Beauskunftung erheblich vereinfachen.

HSM-Restrisiko

Es ist immer eine gute Idee, wichtige Schlüssel in einem Hardware Security Modul (HSM) zu halten – beispielsweise solche, mit denen Zertifikate oder Authentication-Token signiert werden. Das alleine garantiert aber noch keine vollständige Sicherheit. Zu berücksichtigen ist auch, wer über die Schlüssel im HSM verfügen darf: Bei mindestens einem (verbreiteten) HSM-Modell darf das jeder Benutzer auf dem Windows-Server, an den das HSM angeschlossen ist.

Hans-Joachim Knobloch (Secorvo) erläutert diesen Schwachpunkt in seinem Blog-Artikel vom 06.10. 2023 und zeigt, wie man sich darüber ein Goldenes Zertifikat von einer Microsoft-CA erschleichen könnte – falls der CA-Server nicht so gehärtet ist, dass sich nur berechtigte Administratoren anmelden können. In der Tradition der einschlägigen Angriffsvektoren ESC1 bis ESC11 hat er diesen „ESC12“ getauft.

Website Evidence Collector

Bereits am 22.10.2019 wurde der Website Evidence Collector des Europäischen Datenschutzbeauftragten von der International Conference of Data Protection and Privacy Commissioners (ICDPPC) mit dem Global Privacy and Data Protection Award für Innovation ausgezeichnet. Das Tool für die automatische Überprüfung der Erhebung und des Schutzes personenbezogener Daten auf Websites kann Belege für die Verarbeitung personenbezogener Daten (wie Cookies) oder Anfragen an Dritte erzeugen.

Es lädt ohne weitere Benutzerinteraktion nacheinander alle im Besuch einer URL enthaltenen Webseiten. Dabei werden unter anderem Screenshots der Seiten angefertigt und Listen der http-Links, der besuchten Webseiten, der im lokalen HTML5-Speicher gehaltenen Informationen, aller Cookies, des http-Verkehrs sowie alle über Web Sockets ausgetauschten Nachrichten erzeugt.

Das unter der EU Public Licence (EUPL 1.2) veröffentlichte Tool ist auf GitHub für Linux, macOS und Windows zum Herunterladen verfügbar. Es ermöglicht eine schnelle und einfache Prüfung von Webseiten: Bleibt zu hoffen, dass es nicht für automatisierte Abmahnwellen missbraucht wird.

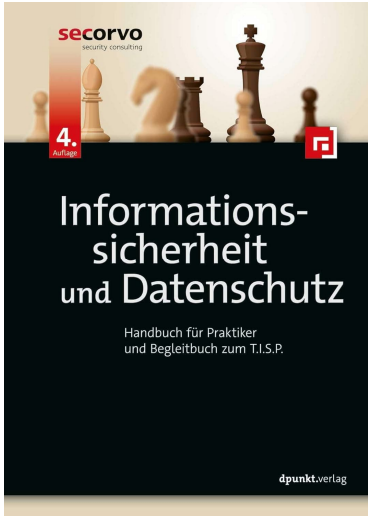
Secorvo News

Secorvo Seminare

Last but not least: Mit unserem neu konzipierten T.P.S.S.E.-Seminar beschließen wir vom **27. bis 30.11.2023** das Seminarjahr 2023: Vier Tage interaktive Workshops und jede Menge Inhalte mit Praxisbezug rund um die sichere Software-Entwicklung.

Die nächste Chance für Ihre T.I.S.P.-Zertifizierung bieten wir Ihnen auf unserem T.I.S.P.-Seminar vom **11. bis 15.03.2024**: Wissenstransfer aus über 20 Modulen des jüngst aktualisierten Curriculums. Dazu erscheint Anfang 2024 die **vierte Auflage** unseres T.I.S.P.-Begleitbuchs im dpunkt-Verlag.

Bevor wir Sie in die Adventszeit entlassen, werfen Sie doch noch einen Blick in unseren Seminarkalender 2024. Wir freuen uns auf Ihre Anmeldung!



Passe partout

Je mehr kryptografische Zertifikate als Authentifikationsmechanismus genutzt werden, desto kritischer sind Konfigurations- oder Implementierungsfehler, die es Angreifern ermöglichen, gefälschte Zertifikate als „Dietrich“ zu benutzen. Das hat erst kürzlich der Diebstahl eines „Generalschlüssels“ zur Microsoft Cloud gezeigt (siehe SSN 8/2023).

Beim Jahresabschlussevent 2023 der KA-IT-Si am **23.11.2023** werden Hans-Joachim Knobloch und Oliver Oettinger (Secorvo) aktuelle Angriffe auf das Active Directory mit solchen „Goldenen Zertifikaten“ demonstrieren und zeigen, wie man sich davor schützen kann. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum Networking am Buffet.

Wir freuen uns auf Sie im Haus der Wirtschaft der IHK Karlsruhe – und empfehlen (wie immer) eine schnelle Anmeldung...

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2023	
23.11.	Passe partout (KA-IT-Si, Karlsruhe)
26.-30.11.	ACM CCS 2023 (ACM/SIGSAC, Kopenhagen/DK)
27.-30.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2023	
04.-07.12.	Black Hat Europe 2023 (Blackhat, London/UK)
Januar 2024	
12.-14.01.	ShmooCon 2024 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2024 (in TIME berlin, Berlin)
30.-31.01.	31. DFN Konferenz (DFN-CERT, Hamburg)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, 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