Secorvo Security News

Juni 2026

Smarte Spione

Vor 14 Jahren überraschte Google die Welt mit seinem Projekt „Google Glass“: einem tragbaren Computer in Brillenform, der mit einer kleinen Kamera ausgestattet war, über Mikrofon, Kopfbewegungen und ein Touchpad gesteuert wurde und durch ein Prisma ausgewählte Informationen auf das rechte Brillenglas projizierte. Die Reaktionen waren teilweise heftig – und trugen dazu bei, dass es in den vergangenen Jahren leise wurde um diese Überwachungsbrillen. Doch Nachfolger Meta entwickelte sie weiter.

Heute sind sie kaum noch von einer regulären Brille zu unterscheiden: Marken wie Ray-Ban oder Oakley bieten sie als Designer-Version an. Sie verbinden sich via Bluetooth mit dem Smartphone und „kommunizieren“ mit dem Träger über einen Over-Ear-Kopfhörer und ein Mikrofon. Die Spracherkennung, mit der Apps, Recherchen und Funktionen des Smartphones gesteuert werden können, übernimmt Metas KI Gemini. Der Auftragsfertiger EssilorLuxottica spricht von allein 7 Mio. verkauften Exemplaren im Jahr 2025 – Tendenz steigend.

Die Brillen sind Ausdruck einer neuen Dimension der Bedrohung der Privatsphäre. Zwar sind Kameras (in Smartphones) schon zum ständigen Begleiter des Menschen geworden, doch Smart Glasses ermöglichen völlig unbemerkte Bildaufzeichnungen – die sich in Sekunden mit Rechercheergebnissen verknüpfen, weitergeben und veröffentlichen lassen. Wem es an Fantasie mangelt, sich vorzustellen, was daraus entstehen kann, dem seien Marc Elsbergs Dystopie „ZERO“ aus dem Jahr 2014 ans Herz gelegt – oder aktuelle US-Nachrichten.

Überwachungstechnik, die vor Jahrzehnten Science Fiction war, steckt heute in Alltagsgeräten: Telefone, Drohnen, Brillen. Der 1973 verstorbene Politiker Karl-Hermann Flach hat diese Entwicklung auf den Punkt gebracht: „Die Freiheit stirbt immer zentimeterweise.“ Dasselbe gilt für unsere Privatsphäre – nur gab es 1973 weder Drohnen noch Meta-Brillen. Nicht einmal PCs.

Security News

Hilfe vom Höllenhund

Auf ihrer Build-Konferenz kündigte Microsoft am 02.06.2026 an, noch im Juni die Kerberos-Erweiterungen IAKerb und LocalKDC in die Preview-Versionen von Windows 11 und Windows Server aufzunehmen. Beide Features sollen helfen, das veraltete und unsichere (siehe z. B. die SSN 7/2021) Authentifizierungsverfahren NTLM abzuschaffen: IAKerb ermöglicht Kerberos-Anmeldungen auch dann, wenn ein Client keinen direkten Kontakt zu einem Domänencontroller

hat; in solchen Fällen kann der Server als Proxy dienen. Und LocalKDC ermöglicht die Verwendung von Kerberos mit lokalen statt mit Domänenkonten.

Beide Lösungen sind nicht neu. IAKerb stammt aus dem Jahr 1997 und war jahrelang – wie auch ein lokaler KDC – Teil von Apples Dienst Back to My Mac. Ungelöst bleibt allerdings der dritte Grund für die Nutzung von NTLM: Anwendungen, die NTLM fest integriert haben. Darunter finden sich auch Programme von Microsoft selbst.

Das Unternehmen rät seinen Kunden seit Jahren, NTLM abzuschalten. Es kündigte im Januar an, das Verfahren in künftigen Windows-Versionen schrittweise zu deaktivieren. Mit IAKerb und LocalKDC rückt dieses Ziel näher. Wann die Features allgemein verfügbar sein werden, ist noch nicht bekannt, evtl. bereits mit der Version 26H2.

Frankreich treibt PQC-Einführung

Auf der France Quantum 2026 am 16.06.2026 kündigte Samih Souissi, Leiter der französischen Cybersicherheitsbehörde ANSSI an, dass ab 2027 nur noch Sicherheitsprodukte zertifiziert werden, die quantenresistente Verschlüsselung (PQC) aufweisen.

Frankreich geht damit entschiedener voran als die EU-Roadmap vom 11.06.2025, die die Einführung von PQC-Verfahren in Hochrisikoanwendungen bis spätestens Ende 2030 vorsieht (siehe SSN 6/2025). In Frankreich dürfen Behörden und KRITIS-Einrichtungen nur Produkte mit ANSSI-Zertifizierung beschaffen; ab 2030 sollen Organisationen nur noch Produkte kaufen, die quantenresistente Kryptografie verwenden.

Die Ankündigung kommt nicht überraschend. Bereits Anfang 2022 veröffentlichte ANSSI erste Empfehlungen, die sie 2023 weiter ausarbeiteten. Ein Grund für die Entscheidung ist die Sorge vor „Harvest Now, Decrypt Later": Wer heute klassisch verschlüsselte Daten speichert, könnte sie später entschlüsseln, sobald ein Quantencomputer verfügbar ist, der in polynomieller Zeit faktorisieren kann.

Ob es einen solchen Computer je geben wird, ist weiterhin umstritten. Die Folgen des Ereignisses wären jedoch so gravierend, dass die Entscheider lieber auf Nummer sicher gehen. Wer in einigen Jahren nicht in Zeitnot geraten will, sollte sich heute schon mit der Migration zu PQC-Verfahren befassen. Secorvo unterstützt dabei gerne.

Sisyphos lässt grüßen

Unerwünschte Prompts und Antworten von LLMs werden unter anderem von Guardrails bereinigt – Filtern, die Halluzinationen erkennen, diskriminierende und beleidigende Formulierungen ersetzen und personenbezogene Daten schwärzen. Doch Guardrails werden immer wieder ausgetrickst. So erging es auch Anthropic mit seinem neuen Modell Claude Fable 5: Binnen Tagen meldete Pliny the Liberator, Fables Guardrails umgangen zu haben.

Am 09.06.2026 veröffentlichte Apostol Vassilev vom US-amerikanischen NIST einen mathematischen Beweis mit unbequemer Botschaft: Vollständige Sicherheit gegen manipulative Eingaben ist bei KI-Systemen

prinzipiell unmöglich. Darin überträgt er den ersten Unvollständigkeitssatz von Kurt Gödel auf KI-Schutzmechanismen. Sein Kernsatz: Kein endliches Regelwerk an Guardrails ist universell robust gegen bösartige Prompts: Es gibt immer einen Weg, ein Modell zum Bruch seiner Regeln zu bewegen – man muss ihn nur finden („Robust AI Security and Alignment: A Sisyphean Endeavor?", IEEE Security & Privacy 05/2026). Bruce Schneier kommt in seinem Essay vom 19.06.2026 zu demselben Schluss: „There is no foolproof way to prevent people from using AI models to complete harmful tasks."

Auch Anthropic räumt ein, dass seine Constitutional Classifiers nicht gegen alle Angriffe gefeit sind und bündelt deshalb unvollkommene Schutzschichten (Defense in Depth). Vassilev empfiehlt denselben Weg – weg vom „einmal absichern, dann ist Ruhe" hin zu fortlaufendem Red-Teaming, stetigem Härten und Resilienz, bis Angriffe schlicht zu aufwändig werden. Wer KI einführt (siehe SSN 03/2026 „Agents of Chaos") sollte also nicht versuchen, deren Restrisiko zu eliminieren, sondern es angemessen reduzieren. Sicherheit ist kein Zustand, den man endgültig erreicht – sondern eine Daueraufgabe.

„Nein Danke" auf Knopfdruck

Seit dem 19.06.2026 ist die EU-Verbraucherrichtlinie in § 356a BGB umgesetzt. Danach müssen Fernabsatzverträge von Verbrauchern so einfach widerrufen werden können wie Einwilligungen im Datenschutzrecht, etwa bei Newsletter-Abos. Unternehmen im B2C-Bereich **müssen** dies sofort umsetzen, sonst drohen Abmahnungen und Klagen.

Betroffenenrechte nach dem *„Privacy by Design"-Prinzip der DSGVO* ziehen damit in weitere Rechtsgebiete ein.

Wie souverän ist souverän?

Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) hat am 21.05.2026 den Zuschlag für eine souveräne KI-Cloud an Konsortien um T-Systems und SAP vergeben. Die KI-Cloud soll als Basis für die digitale Verwaltung dienen. Doch die behauptete Souveränität erscheint fragil, denn der CLOUD Act und FISA 702 erlauben US-Behörden den Zugriff auf Daten amerikanischer Unternehmen, auch wenn die Server in Europa stehen – und sowohl T-Systems als auch SAP unterhalten Tochtergesellschaften in den USA, die dort wirtschaftlich stark verwurzelt sind. Damit erscheint nicht ausgeschlossen, dass US-Behörden den Zugriff auf deutsche Verwaltungsdaten durchsetzen können.

Bundesminister Wildberger betont zu Recht die Bedeutung einer selbst kontrollierten nationalen Verwaltungsinfrastruktur. Doch ohne zweifelsfreie Abschottung von US-Einfluss bleibt die Wahl der KI-Cloud ein Kompromiss zwischen Souveränität und wirtschaftlicher Leistungsfähigkeit. Wie souverän die gewählte Plattform tatsächlich ist, wird die Praxis zeigen – sobald US-Behörden Daten anfordern.

Sicherere Zertifikatserneuerung

Nach Entscheidung des CA/Browser-Forums vom 11.05.2026 (Ballot SC098v2) müssen Zertifizierungsstellen ab dem 15.03.2027 vor der Ausstellung öffentlich vertrauter TLS-Zertifikate prüfen, ob der verwendete (ACME-)Account und die verwendete Validierungsmethode per CAA-Record im DNS zugelassen sind. Ein weiterer Schritt zu mehr Sicherheit im Netz.

CAA wird bislang vor allem als eine Liste zugelassener Zertifizierungsstellen verstanden, die für eine Domäne TLS-Zertifikate ausstellen dürfen. Mithilfe der nun verpflichtend auszuwertenden zusätzlichen Parameter „accounturi" und „validationmethods" lässt sich dies weiter einschränken. Da bei der Erstbeantragung eines Zertifikats z. B. bei Let's Encrypt ein ACME-Account erzeugt wird, und der ACME-Client mit dem Server gleich einen öffentlichen Schlüssel zur Authentifizierung aller kommenden Anfragen aushandelt, ist die Festlegung der „accounturi" via CAA ein zusätzlicher Authentifizierungs-Faktor: Ohne den geheimen Schlüssel, der dem Account zugeordnet ist, kann kein Zertifikat beantragt werden.

Die Hürde für (versehentlich oder absichtlich) falsche Zertifikatsausstellungen wird somit sinnvoll erhöht. Besonders stark schützt die Einschränkung, wenn das Unternehmen seine Zone zusätzlich mit DNSSEC absichert, also den eigenen DNS-Eintrag signiert. Das schützt gleich doppelt, wenn DNS auch als ACME-Validierungsmethode gewählt wird.

Secorvo News

Qualifikationen

In unserer vierstündigen NIS-2-Schulung nach BSIG vermitteln wir am **15.10.2026** Geschäftsleitungen die erforderlichen Grundlagen zur Erkennung und Bewertung von Informationssicherheitsrisiken.

Unsere fünftägige T.I.S.P.-Schulung (**28.09.–02.10.** und **16.–20.11.2026**) bereitet Sie auf die Online-Prüfung vor – mit 20jähriger Erfahrung und hunderten erfolgreichen Zertifizierungen. Referenten sind die Autoren des T.I.S.P.-Begleitbuchs „Informationssicherheit und Datenschutz" (4,9 ✶ bei Amazon).

Die vertiefenden Seminare ISMS verstehen und planen (**12.–13.10.2026**) und PKI – Grundlagen, Vertiefung, Realisierung (**23.–26.11.2026**) vermitteln Ihnen Praxiswissen für den Aufbau und Betrieb eines wirksamen Sicherheitsmanagements und von Public-Key-Infrastrukturen.

Gemeinsam mit andrena objects und über 25 Jahren Erfahrung in Informationssicherheit und Softwareentwicklung führen wir auf dem T.P.S.S.E.-Seminar (**05.–08.10.2026** und **02.–05.11.2026**) in die Grundlagen der sicheren Softwareentwicklung ein – und bereiten Sie auf die Zertifizierung als Secure Software Engineering Professional vor.

Planen Sie jetzt Ihre Weiterbildung für das 2. Halbjahr 2026 und sichern Sie sich den Frühbucherrabatt. Alle Seminarangebote und die Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

16. Tag der IT-Sicherheit

Welche Lehren zieht man aus dem ersten und bisher einzigen Cyberkatastrophenfall in Deutschland? Wie gelingt ein wirksames ISMS? Wie erreicht man sichere Software mit Hilfe eines Dependency Tracks? Antworten auf diese Fragen gibt es am **23.07.2026** auf dem 16. Tag der IT-Sicherheit in den Räumen der IHK Karlsruhe – ein Networking-Event der Karlsruher IT-Sicherheitsinitiative, des CyberForum, der IHK Karlsruhe und KASTEL.

Hier geht's zur Anmeldung – wir freuen uns auf Sie.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

Juli 2026	
06.-10.07.	11th IEEE European Symposium on Security and Privacy (IEEE Computer Society, Lissabon/PT)
20.-25.07.	PETS 2026 (University of Calgary, Calgary/CA)
23.07.	16. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, Karlsruhe)
27.-30.07.	DFRWS USA 2026 Conference (DFRWS, Arlington/US)
August 2026	
01.-06.08.	Black Hat USA 2026 (Black Hat, Las Vegas/US)
03.-05.08.	IEEE Internation Conference on Cyber Security and Resilience (IEEE CSR 2026) (IEEE, LogosRI, Lissabon/PT)
06.-09.08.	Defcon 34 (DEF CON Communications, Inc., Las Vegas/US)
12.-14.08.	35th USENIX Security Symposium (usenix, Baltimore/US)
17.-20.08.	Crypto 2026 (IACR, Santa Barbara/US)
23.-26.08.	SOUPS 2026 (usenix, Hannover)
24.-25.08.	SAC 2026 (IACR, Ottawa/CA)
24.-25.08.	SAC Summer School (IACR, Toronto/CA)
September 2026	
09.-10.09.	Annual Privacy Forum 2026 (PLUS, Goethe Universität, Plattform Privatheit, Salzburg/AT)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Michael Schrempp, Liza Trace.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Bahnhofplatz 8
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