Secorvo Security News

Dezember 2020

Beweislastumkehr

Am 26.11.2020 hat die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) einen Beschluss zur Datenschutzkonformität von Windows 10 Enterprise gefasst. Das Dokument liest sich – selbst (oder gerade) für einen „in der Wolle gewaschenen" Datenschützer – äußerst befremdlich.

In aller Ausführlichkeit wird zunächst festgehalten, dass Microsoft mehrfach versichert hat, dass Windows 10 bei Konfiguration der Telemetrie-Stufe „Security" keine Telemetriedaten (Daten über das Nutzungsverhalten) an Microsoft übermittelt. Mit Bezugnahme auf eine (dem Beschluss beiliegende) BSI-Untersuchung vom Januar 2020 kommt die DSK zu dem Ergebnis, dass „Verantwortliche nicht abschließend von ihrer (...) Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten" entlastet werden können. Dabei kommt die referenzierte BSI-Untersuchung zu dem Schluss, dass „sich keine Hinweise ergeben, dass Windows 10 Enterprise (...) Daten an Microsoft übertragen hat, die aus h. S. ein Risiko oder das Offenlegen vertrauenswürdiger Informationen darstellen. Insbesondere konnte keine Übertragung von Telemetriedaten an Microsoft beobachtet werden."

Für ihr Urteil genügte der DSK, dass eine bestimmte Verbindung „nicht im Klartext analysiert werden konnte" – mithin die Möglichkeit besteht, dass Microsoft entgegen der anderslautenden Zusicherungen darüber doch Telemetriedaten übermitteln *könnte*. Das Verdikt wirkt wie eine merkwürdige Gemengelage aus Skepsis, Vorurteilen und Unterstellungen – und wird viel Unsicherheit hervorrufen. Warum sich die Aufsichtsbehörden hier so in Stellung bringen, während zeitgleich Millionen Webseiten und Milliarden Apps offensichtlich rechtswidrig Nutzerdaten erheben und (nicht nur) in die USA übermitteln, dürfte auch Datenschützern schwer zu vermitteln sein.

Security News

Besenrein

Am 07.07.2020 veröffentlichte The Register einen exklusiven Artikel darüber, wie Cyberkriminelle mehr als 240 Subdomänen existierender Organisationen übernehmen konnten. Ursächlich dafür waren Subdomänen mit verwaisten DNS-Einträgen, die auf zwischenzeitlich aufgegebene Azure-Ressourcen zeigten. Die Angreifer erstellten Ressourcen mit denselben Namen neu und empfingen anschließend den gesamten Datenverkehr, der für die noch im DNS hinterlegte Subdomäne bestimmt war.

Offensichtlich ist das Problem so groß, dass Microsoft am 29.09.2020 in der Netzwerksicherheitsdokumentation für Azure einen Artikel zur Verhinderung von Subdomain-Übernahmen ergänzte.

Merke: Auch in der Cloud betriebene Assets sollten einem kontrollierten Lebenszyklus unterliegen – Stichwort „Cloud Asset Management" – und am Ende „besenrein" abgeschlossen werden. Außerdem sollte man nicht davon ausgehen, dass in der Cloud betriebene Ressourcen „auto-magisch" sämtliche Konfigurationen selbst vornehmen und „einfach funktionieren". Bester Beweis dafür sind die seit Jahren immer wieder entdeckten falsch konfigurierten und damit für die ganze Welt zugänglichen AWS S3 Buckets.

Cookie-Einsatz im Fokus

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat am 25.11.2020 seinen Bericht zur Prüfung des Einsatzes von Cookies und Drittdiensten auf niedersächsischen Webseiten veröffentlicht. Die geprüften Webseiten genügten – wenig überraschend – nicht den Anforderungen der DSGVO, der Gerichte und der Aufsichtsbehörden. Häufig kommen so genannte „Consent Tools" zum Einsatz, die die Lage eher verschlimmern als verbessern: Einwilligungen werden häufig nicht wirksam eingeholt, Widerrufsmöglichkeiten fehlen ganz und die zur Verfügung gestellten Informationen zum Tracking sind mangelhaft. Dabei blieb bei der Prüfung gänzlich unbeachtet, dass es neben Cookies auch andere Tracking-Technologien gibt, an die die gleichen Anforderungen zu stellen sind.

Das Risiko, wegen unzureichender „Consent Banner" mit einem Bußgeld belegt zu werden, steigt: Europaweit häufen sich die Berichte über entsprechende Verfahren der Aufsichtsbehörden. Die Handreichung der niedersächsischen Aufsichtsbehörde gibt verständliche Hinweise, was möglich und erlaubt ist.

Gefährliche Ignoranz

Am 06.12.2020 veröffentlichte der Sicherheitsforscher Oskars Vegeris Details zu einer am 31.08.2020 an Microsoft gemeldeten kritischen Schwachstelle in Microsoft Teams. Sie konnte zur Ausführung beliebigen Codes aus der Ferne genutzt werden – plattformübergreifend. Nötig war dafür allein eine bösartige Chat-Nachricht. Die Schwachstelle war „wurmbar", d. h. es konnte Schadcode geschrieben werden, der sich selbstständig weiter verbreitet. Sie wurde Ende Oktober 2020 geschlossen – still und heimlich, da es sich bei Teams um ein sich „selbst aktualisierendes Produkt" handelt, und ohne CVE-Eintrag. Belohnt wurde der Sicherheitsforscher nicht für seinen Fund, da der Desktop-Client nicht Teil des Bug-Bounty-Programms ist – die Schwachstelle also „out of scope" war.

Ein beliebtes, aber gefährliches Vorgehen, da es die Finder kritischer Schwachstellen künftig motivieren könnte, solche Funde direkt auf dem Schwarzmarkt zu verkaufen oder zu veröffentlichen. Das sollte Microsoft eigentlich wissen: 2018 hatte die Sicherheitsforscherin „SandboxEscaper" nach einer ähnlichen Erfahrung mit Microsoft mehrere Zero-Day-Schwachstellen samt Exploit-Code auf Twitter und GitHub veröffentlicht.

Neue Datenschutzklauseln

Die Europäische Kommission hat am 13.11.2020 einen Entwurf für neue Standardvertragsklauseln, die zugehörige Angemessenheitsentscheidung und Leitlinien zur Verwendung zur öffentlichen Konsultation vorgelegt. Die Neugestaltung war bereits durch sich verändernde Übermittlungskonstellationen, vor allem aber durch das Schrems-II Urteil erforderlich geworden.

Der vorgelegte Entwurf ersetzt und vereinheitlicht die bisherigen drei Varianten der Standardvertragsklauseln. Dafür werden innerhalb der Entwurfsklauseln vier Module gebildet: Modul 1 für die Übermittlung zwischen Verantwortlichen, Modul 2 für Auftragsverarbeiter, Modul 3 für Unterbeauftragungen durch Auftragsverarbeiter und Modul 4 für die Zusammenführung von personenbezogenen Daten, die der EU-Auftragsverarbeiter erhebt, mit Daten des Verantwortlichen aus einem Drittstaat. Die anwendbaren Regelungen ergeben sich aus der anfänglichen Festlegung der Konstellation. Die Umsetzungsfrist für den Übergang zu den neuen Klauseln soll ein Jahr ab Verabschiedung betragen.

Dem Schrems-II Urteil wird durch die verankerte Pflicht zur Prüfung der Umsetzbarkeit, entsprechende Meldepflichten und Kündigungsvorbehalte Rechnung getragen. Die Erneuerung der in die Jahre gekommenen Standardvertragsklauseln war überfällig. Ansätze zur Lösung der Problematik von zu weit gehenden oder ungenügend kontrollierten staatlichen Zugriffen (Stichwort „US CLOUD Act“) enthalten die Klausel-Entwürfe jedoch nicht.

Spy in the Middle

Am 08.12.2020 veröffentlichte Cloudflare, wie der Konzern künftig durch Einsatz von „Oblivious DNS over HTTPS“ (ODoH), einem in Kooperation mit Apple und Fastly entwickelten Protokoll, die Anonymität von Anfragen mittels DNS over HTTPS (DoH) verbessern will. DoH ermöglicht die Namensauflösung über TLS-gesicherte HTTP-Verbindungen und war wegen der Nachvollziehbarkeit des Surfverhaltens durch Cloudflare in die Kritik geraten (SSN 09/2019). Bei ODoH ist die DNS-Anfrage verschlüsselt, sodass der Proxy-Anbieter den Inhalt nicht mitlesen kann. Weder der DNS-Anbieter noch der Betreiber des Proxy-Servers kann eine Anfrage einem Nutzer zuordnen – solange der Proxy-Betreiber nicht mit dem DNS-Anbieter kooperiert.

Dass DNS dringend Sicherheits- und Privatsphären schützende Funktionen wie Verschlüsselung benötigt, steht außer Frage. Mit welcher Technologie dies erfolgen wird, ist jedoch noch offen. TLS und HTTPS liegen zwar aus konzeptioneller Sicht auf dem falschen OSI-Layer, aber eine in der Praxis getestete und weit verbreitete Technologie ist erfahrungsgemäß sicherer als die Entwicklung eines neuen Protokolls. Auch ist die großflächige Änderung der bestehenden DNS-Infrastruktur z. B. in Form von Erweiterungen wie DNSSEC in der Praxis schwierig. Ähnlich der Entwicklung von Programmierbibliotheken ist es einfacher, bei den Nutzern eine neue „Bibliothek“ (ODoH) zu installieren, als eine bestehende Infrastruktur zu ändern.

Identifikation bei Auskunftsanfrage

Das Verwaltungsgericht Berlin entschied am 31.08.2020, dass bei einem Auskunftsersuchen eine „qualifizierte Form" der Identifikation nur dann verlangt werden kann, wenn „begründete Zweifel" an der Identität des Antragstellers bestehen. So sehen es auch § 59 BDSG und Art. 12 Abs. 6 DSGVO vor. Dem BayObLG genügt jedoch laut Beschluss vom 18.11.2020 bei einem schriftlichen Antrag auf Auskunft nicht, dass sich der Antragsteller mit vollständigem Namen und Geburtsdatum identifiziert. Dass auch die korrekte Adresse bekannt war, wie der Schriftwechsel mit den Gerichten zeigt, half auch nicht weiter. Vor Gericht und auf hoher See – ist man in Gottes Hand.

Windows 10 und die Daten

Am 26.11.2020 hat die Datenschutzkonferenz einen Beschluss zur Datenschutzkonformität der Telemetriefunktionen von Windows 10 Enterprise gefasst. Die Bewertung geht auf eigene Laboruntersuchungen einer DSK-Arbeitsgruppe und eine Analyse des BSI vom Januar 2020 zurück.

Die Übermittlung der Telemetrie-Daten an Microsoft kann auch personenbezogene Daten zum Nutzungsverhalten beinhalten, deren Übermittlung durch das verantwortliche Unternehmen v. a. gegenüber Arbeitnehmern einer Rechtsgrundlage und bei Übermittlung in Drittstaaten gesonderter Regelungen bedarf. Die Untersuchungen kommen zu dem Ergebnis, dass die geprüften Windows-Versionen die Deaktivierung der Telemetrieübermittlung grundsätzlich ermöglichen. Die DSK sieht die Microsoft-Kunden als Verantwortliche in der Nachweispflicht bzgl. der sicheren Unterbindung von Übermittlungen. Probleme bereitet hier die Ansteuerung eines Microsoft-Endpunktes in allen Einstellungsvarianten, der möglicherweise für eine dynamische Konfiguration der Telemetrieeinstellungen verwendet werden kann. Die diesbezüglichen Zusicherungen von Microsoft werden als nicht ausreichend angesehen. Für Windows Pro und Home besteht derzeit keine Deaktivierungsmöglichkeit.

Es drängt sich die Frage auf, wie Verantwortliche auch bei vergleichbaren Anwendungen regelmäßig eigenständig über die Zusicherungen der Anbieter hinaus nachweisen sollen, dass keine derartigen Übermittlungen an die Software-Anbieter stattfinden.

Vorsatz 2021: Keine unnötigen Risiken

Meldungen wie die vom 19.11.2020 über eine Sicherheitslücke im Server-Backend der Corona-Warn-App lassen sich unterschiedlich interpretieren: Laut Projekt belegt sie, dass „der Open-Source- sowie Community-Prozess einwandfrei funktioniert"; nach der Beschreibung der Entdeckung auf GitHub war es hingegen ein Zufallsfund. Sie fiel auf, als ein Scanner auf Basis des (in SSN 11/2020 beschriebenen) GitHub-integrierten Scanners trainiert wurde. Eines jedenfalls zeigt der Fall: Selbst kritisch in der Öffentlichkeit stehende Software kann Fehler enthalten. Daher empfehlen wir für 2021 einen grundlegenden Sicherheitsmechanismus: Unnötige Risiken vermeiden! Wer sein Auto öffnen lassen

möchte, indem das Auto das Handy fragt, ob der Fahrzeughalter gerade vor ihm steht – bitte. Für sicherheitsbewusste Technik-Nutzer sollte aber eine Möglichkeit bestehen, einen solchen potenziell fehlerhaften Zugangsmechanismus zu deaktivieren.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
01.-04.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)
März 2021	
03.-04.03.	Future Security 2021 (Fraunhofer VVS, Nürnberg)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, 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