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.

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 fest-

stellbar 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, 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