Rechts-News von RA Mag. Stephan Novotny

Status Google-Fonts-Prozess, 5 kritische Sicherheitslücken, chinesische Hacker surfen mit.

Heute fassen wir für Sie kurz und prägnant **3 Rechts- & Sicherheits-Themen** zusammen, erklären die Hintergründe und geben Tipps für die Praxis.

a) 59 Sicherheitslücken in Windows müssen gestopft werden
Laut Computer-Zeitung Chip.de lieferte Microsoft kürzlich 59 Patches - auf Deutsch „Pflaster" - aus. Mit diesen Pflastern sollen Software-Fehler und ganz besonders Sicherheitslöcher „zugeklebt" werden.
Da einige dieser Sicherheitslücken bereits **„aktiv" für Attacken genutzt** werden, sollten Sie diese Updates rasch und laut Computer- und Datenschutz-Experten unbedingt einspielen und **nicht etwa verschieben oder unterbinden!**

5 „Löcher" werden als kritisch eingestuft, weitere 53 Sicherheitsprobleme tragen das Label "wichtig", eine Lücke ist als "moderat" gekennzeichnet. So fasst die Computer-Zeitung Chip die diversen Updates zusammen. **Und rät:** Egal, welche Version von Windows 10 oder 11 Sie einsetzen, die Updates sollten Sie zeitnah einspielen, weil fünf Sicherheitslücken bereits für Angriffe genutzt werden.

DSGVO – zum Erinnern!
Diese Warnungen und „Aufforderungen" das **Windows-Update nicht zu behindern,** dienen dazu, um Ihre EDV zu schützen, was heutzutage „lebenswichtig" geworden ist. Jedes Unternehmen, das 1, 2 oder mehr Tage lahmgelegt war, wird Ihnen das bestätigen.
Aber auch die **DSGVO – konkret die TOMs – verpflichtet Sie dazu,** alles Mögliche zu unternehmen, um die **Sicherheit Ihres Systems, Ihrer Daten,** etc. sicherzustellen. **Zum Erinnern:**

- http://www.b2b-projekte.at/files/bav-nl_08_2021_DSGVO_Megastrafe-wegen-Verletzung_TOMs_Was-daraus-lernen.pdf
- http://www.b2b-projekte.at/files/bav-nl_10_2021_aktuelles_dsgvo-update-zu-Google-Analytics_Datenaustausch-mit-UK.pdf
- http://www.b2b-projekte.at/files/BAV-NL-April-23_DSGVO-Update_1640-Mio-Strafen_Google-Fonts-Gerichtsverfahren-gestartet.pdf
- http://www.b2b-projekte.at/files/bav-nl_04_2022_google-analytics_verletzt_dsgvo_alternativen_gibt_es.pdf
- http://www.b2b-projekte.at/files/BAV-NL_06_21_DSGVO_Privacy-Shield-Out_Darf-man-ueberhaupt-noch-US-Software-oder-US-Dienstleister-nutzen.pdf

b) Chinesische Hacker surfen mit. Deutscher Verfassungsschutz warnt vor Angriffen.
Vorige Woche fand sich ein interessanter Beitrag in der Tageszeitung DER STANDARD (hier zum Nachlesen…).
Darin wird berichtet, dass das **deutsche Bundesamt für Verfassungsschutz (BfV)** eine **dringende Warnung** veröffentlicht hat. Zwei Hackergruppen, die für den chinesischen Staat arbeiten sollen, hätten eine **ausgeklügelte Strategie** entwickelt, um die Angriffe vorzubereiten: Sie nisten sich in die Geräte von Privat-Personen und mittelständischen Unternehmen ein (PC, Drucker, Modem, Router, sogar Smart-Home-Geräte).

Dieser **Missbrauch „passiere in großer Stückzahl" und „falle gar nicht auf".** In der Regel gebe es weder „Verbindungsabbrüche oder anderwärtige Auffälligkeiten". Alles funktioniere einwandfrei und die Hacker, die tausende Kilometer weit weg sitzen, surfen heimlich mit". Zitiert der Standard.

Ziel ist die Verschleierung. Denn die „echten Angriffe", z.B. auf Behörden oder Großunternehmen, erfolgen dann von diesen privaten und KMU-Geräten mit inländischen IP-Adressen, die von den Abwehrsystemen oftmals als harmlose Privatpersonen und KMUs eingestuft werden. Wodurch der Angriff oft unterschätzt wird.
Ob diese Hacker eine der oben im Chip-Beitrag erwähnten 59 Sicherheitslücken ausnutzen, wissen wir nicht.
Der **Tipp des deutschen Verfassungsschutzes, wie man verhindern könne,** dass die eigenen Geräte für Cyberangriffe verwendet werden: „Das Risiko lasse sich unter anderem dadurch minimieren, die Geräte auf dem aktuellen Stand zu halten und veraltete Geräte, die vom Hersteller nicht mehr unterstützt werden, durch neue auszutauschen."

Fakt ist: Es gilt, die EDV aktuell und damit möglichst sicher zu halten.
Denn sonst gefährden Sie nicht nur den Betrieb Ihres Unternehmens, sondern bekommen dann womöglich auch noch Schwierigkeiten von der bzw. durch die Datenschutzbehörde, weil man Ihnen vorwirft, dass Sie die DSGVO, konkret die TOMs, verletzt haben!

c) Abmahnanwalt und Klienten verlieren Google-Fonts-Prozess
Voriges Jahr ging ein DSGVO-Prozess durch fast alle Medien. Immerhin wurden rund **33.000** Webseiten-Betreiber mit einem **Abmahnschreiben** konfrontiert. Darin wurden diese aufgefordert 190 € zu zahlen, weil man Google Fonts (Schriften) auf der eigenen Webseite verwendet habe. **Der Vorwurf:** Durch die Nutzung von Google Fonts wären personenbezogene Daten (etwa die IP-Adresse des Computers) an Google in die USA übertragen worden, was zu einem „Unwohlsein" der Mandantin des Anwalts geführt hätte und ein Verstoß gegen die Datenschutzgrundverordnung sei.

Im Vorfeld des Urteils wurde dann via Krone.at bekannt, dass zwischen Anwalt und „Geschädigter" ein enges Verhältnis bestand, zumindest könnte man die Chat-Nachricht „Hase, es ist irre viel Money am Konto" so verstehen. Den Link zu diesen Beiträgen finden Sie unten in der Link-Sammlung.

Kürzlich berichtete **RA Dr. Brandl** im RisControl vom Ausgang des Prozesses und sprach von einer „wegweisenden Entscheidung". Tatsächlich konnte die Mandantin des Abmahnanwalts nicht beweisen, worin ihr Schaden bestanden habe und verzichtete auf alle ihre Ansprüche und muss die Verfahrenskosten tragen. Ein Grund für das Urteil könnte die Tatsache gewesen sein, dass die „Geschädigte" die 33.000 Webseiten nicht selbst geöffnet hatte, sondern ein Computerprogramm automatisch nach Webseiten suchen ließ, wo diese Schriften verwendet wurden.

Daher trotz positivem Urteil: Weiterhin VORSICHT walten lassen!
So erfreulich das Urteil in diesem Einzelfall ist: Nehmen Sie es nicht als Argument, um selbst alle Vorsicht fallen zu lassen. Fakt ist: Die **USA haben ganz andere Vorstellungen von Datenschutz,** ganz besonders, wenn es um die Daten von Europäern geht. Fakt ist weiters, dass Sie – ohne ausdrückliche und vorherige Zustimmung – keine Daten in die USA übertragen dürfen.

Denn **amerikanische Unternehmen sind verpflichtet,** aufgrund des „Patriot acts" den **US-Sicherheitsbehörden und Geheimdiensten Zugriff auf die in den Vereinigten Staaten gespeicherten Daten zu gewähren.**

Dennoch erklärten bereits **am 25. März 2022** EU-Kommissionspräsidentin Ursula von der Leyen und US-Präsident Joe Biden eine „grundsätzliche Einigung" über eine weitere Privacy-Shield-Vereinbarung**, ohne dass in den USA Überwachungsgesetze geändert worden wären.**

Datenschützer Max Schrems kritisierte sofort, dass die USA dem **Datenschutz eine andere Bedeutung** beimessen würden, als der EuGH. Außerdem stelle die Verletzung der Privatsphäre von Nicht-US-Bürgern kein Problem für die USA dar. Auch die vorgeschriebenen Rechtsbehelfe stimmen seiner Meinung nach nicht mit EU-Recht überein.

Und auf der **eigenen Webseite „noyb.eu"** findet sich bereits ein Beitrag, der ankündigt, dass er diesen neuerlichen Versuch, ein politisches Abkommen zu erreichen, wieder vor den Europäischen Gerichtshof bringen werde. Weil das neue Abkommen „weitgehend eine Kopie des gescheiterten Privacy-Shield-Abkommen" sei.

Daher: Verlassen Sie sich nicht auf politische Abkommen, sondern gehen Sie sorgfältig mit personenbezogenen Daten um und lassen Sie nicht zu, dass diese in die USA ohne vorherige Zustimmung übertragen werden.
Ja, es ist mühsam, wenn man als Unternehmen nicht weiß, wie man rechtskonform mit den USA zusammenarbeiten soll.

Frage: Darf man Google Fonts daher wieder nutzen?
Nein, das sagt das Urteil nicht aus. Aber es gab auch schon vorher die Möglichkeit, Google-Schriften zu nutzen. Und zwar derart, dass die **Google-Schriften lokal auf dem Webserver eingebettet** werden (Ihr EDV-Mann oder Webseiten-Spezialist weiß sicher, was wir meinen).

Wenn man das nicht kann oder will, also bei jedem Ansurfen der eigenen Webseite die Schriften vom Google-Server (nach-)geladen werden – was dazu führt, dass die personenbezogenen Daten jedes Besuchers Ihrer Webseite in die USA transferiert werden – dann muss man **VORHER vom Besucher eine ausdrückliche Zustimmung einholen**. Und: das **Häkchen** im entsprechenden Formular darf **nicht bei JA bereits vorgesetzt sein,** weil das wäre auch schon wieder ein Verstoß gegen die DSGVO….

Frage: Ganz allgemein: Darf man Produkte der US-Datenkraken nun wieder gedanken- und vor allem problemlos nutzen?

Nein. Hier rate ich – wie bisher – ganz bewusst ab. **Seien Sie auch weiterhin vorsichtig!** Jeder kann Facebook, WhatsApp und Co auf ausschließlich privat genutzten Geräten nutzen, wenn er /sie das möchte. Aber diese „sozialen" Medien haben auf beruflichen Geräten nichts zu suchen.

Auch **Google Fonts oder Google Analytics** sollte man ohne vorherige ausdrückliche Zustimmung keinesfalls nutzen! Zu Google Analytics gibt es bereits Urteile der Datenschutzbehörden in Österreich und Frankreich. Die bestätigen, dass **personenbezogene Daten,** wie etwa „eine einzigartige Nutzer-ID-Nummer, IP-Adresse und Browserparameter" **an Google in die USA übertragen und daraus ein eindeutiges User-Profil erstellt werden.**

Daher hat die österreichische Datenschutzbehörde – vereinfacht gesagt – entschieden, dass die Verwendung von Google Analytics auf Webseiten gegen die DSGVO verstößt, weil die **nötigen Schutzmaßnahmen** (der europäischen Daten gegenüber US-Behörden und Geheimdiensten) **nicht angemessen seien.**

Und der nächste Kläger gegen die Nutzung von Google Fonts **könnte vielleicht Recht bekommen,** wenn man nicht ein Computer-Programm zur Suche eingesetzt hat und daher die Schädigung wirklich nachweisen kann! **Denn die DSGVO ist da ganz eindeutig!**

Beste Grüße von RA Mag. Stephan Novotny und Mag. G.Wagner

Sollten Sie noch keinen Anwalt haben: **Mag. Stephan Novotny,** ein **auf Versicherungs- und Datenschutzrecht spezialisierter Fachanwalt** steht gerne zur Verfügung. Für Zurich-Newsletter-Leser sogar zum **Spezialpreis.**

RA Mag. Stephan Novotny
1010 Wien, Landesgerichtsstraße 16/12
kanzlei@ra-novotny.at
https://www.ra-novotny.at

Foto: Stephan Huger

Weitere **Lesetipps:**

- https://www.derstandard.at/story/3000000185002/chinesische-hacker-surfen-heimlich-bei-privatnutzern-mit
- https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_artikel.html
- https://www.msn.com/de-at/nachrichten/other/chinesische-hacker-surfen-heimlich-bei-privatnutzern-mit/ar-AA1g2Mcu
- https://www.zeit.de/digital/2023-03/verfassungsschutz-cyberspionage-warnung-suedkorea-kimsuky
- http://www.b2b-projekte.at/files/bav-nl_08_2021_DSGVO_Megastrafe-wegen-Verletzung_TOMs_Was-daraus-lernen.pdf
- http://www.b2b-projekte.at/files/bav-nl_10_2021_aktuelles_dsgvo-update-zu-Google-Analytics_Datenaustausch-mit-UK.pdf
- http://www.b2b-projekte.at/files/BAV-NL-April-23_DSGVO-Update_1640-Mio-Strafen_Google-Fonts-Gerichtsverfahren-gestartet.pdf

- http://www.b2b-projekte.at/files/bav-nl_04_2022_google-analytics_verletzt_dsgvo_alternativen_gibt_es.pdf
- http://www.b2b-projekte.at/files/BAV-NL_06_21_DSGVO_Privacy-Shield-Out_Darf-man-ueberhaupt-noch-US-Software-oder-US-Dienstleister-nutzen.pdf
- https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

Quellen: Computerzeitung Chip.de, DER Standard.at, DIE Zeit, RisControl, krone.at, msn.com, Webseite des IVVA, noyb.eu