SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

November/Dezember 2018

SWITCH

I. SiSyPHuS stellt Windows 10 bezüglich Datenschutz und -sicherheit kein gutes Zeugnis aus

Das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI sieht sich nach eigenen Angaben als nationale Cyber-Sicherheitsbehörde, das unter anderem die Aufgabe hat, "Anwender in Staat, Wirtschaft und Gesellschaft dabei zu unterstützen, IT-Produkte und Software sicher einsetzen zu können." Windows 10 sieht das BSI als das am weitesten verbreitete Betriebssystem auf PCs mit besonderem Einfluss auf die Sicherheit vieler IT-Systeme in Deutschland. Dies und die Tatsache, dass die deutsche Bundesverwaltung Windows 10 einsetzt, hat das BSI dazu motiviert, bei der renommierten Cyber-Security-Firma ERNW in Karlsruhe eine grosse Studie zur Sicherheit des Betriebssystems in Auftrag zu geben.

Ihr Titel: SiSyPHuS Win 10. Ihr Inhalt: Eine komplette Sicherheitsanalyse von Telemetriekomponenten sowie Trusted Platform Modulen (TPM), VBS/DeviceGuard, Windows Powershell, Application Compatibility Infrastructure, Treiber-Management und PatchGuard. Erste Ergebnisse zum Bereich Telemetrie wurden nun veröffentlicht (im Detail nachzulesen unter den nachstehenden Links zu bsi.bund.de). Erstes Fazit: Windows 10 macht genau das, was Anwender schon immer befürchtet haben: Daten über die Systemabstürze und die Nutzung des Geräts sammeln und auf Server von Windows 10-Hersteller Microsoft übermitteln. Laut Bericht sind dies "Daten über die

Nutzung des Computers unter Windows 10 und der an ihn angeschlossenen Geräte, Daten über die Performance des Systems, Daten, die bei Fehlern wie Programm- oder Systemabstürzen erhoben werden, sowie Daten des Windows Defenders und des Malicious Software Removal Tools (MSRT).“ Zudem bemängelt der Bericht, dass es vertiefte IT-Kenntnisse voraussetze, den Sammel- und Sendeeifer des Telemetriedienstes in Windows 10 abzustellen oder zumindest einzudämmen. Dies zu tun macht aus zwei Gründen Sinn. Aus Sicht des Datenschutzes kann damit die Privatsphäre besser geschützt werden. Aus Sicht der Datensicherheit öffnet der permanente Datenfluss Hackern ein Einfallstor zum System. Daher hat das BSI auf der unten angegebenen Webseite ein PDF mit konkreten Handlungs- und Konfigurationsempfehlungen zum Abschalten bzw. Eingrenzen des Telemetriedienstes zum Download bereit gestellt.

Inwieweit dadurch die Kommunikation zwischen dem PC auf dem Schreibtisch und den Servern in Richmond unterbunden wird, hängt aber auch davon ab, welche Microsoft-Programme noch auf dem Gerät installiert sind: Office 365 und der Internet Explorer schicken nämlich Daten auch ohne den Telemetriedienst von Windows 10 auf die Microsoft-Server. Ein holländischer Regierungsbericht über Office Pro Plus kommt zu der Bewertung, dass Microsoft damit gegen die Europäische Datenschutzgrundverordnung DSGVO verstösst. Microsoft droht im Falle einer Anklage und Verurteilung ein happiges Bussgeld von mehreren 10 Millionen Euro. Der Hersteller hat sich inzwischen verpflichtet einen Verbesserungsplan, der die Verstösse verhindern soll, zu erarbeiten und diesen bis April 2019 vorzulegen.

Nachzulesen unter:

https://www.chip.de/news/Experten-durchleuchten-Windows-10-Und-bestaetigen-leider-was-alle-Nutzer-schon-lange-wissen_153496607.html
https://www.heise.de/newsticker/meldung/BSI-untersucht-Sicherheitseigenschaften-von-Windows-10-4227139.html
https://winfuture.de/news,106207.html
https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf?__blob=publicationFile&v=2
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Analyse_Telemetriekomponente.pdf?__blob=publicationFile&v=4
https://www.pcwelt.de/a/regierungsbericht-microsoft-office-verstoesst-gegen-dsgvo,3463053

II. Vivy-App mit multiplem Krankheitsbild: Sicherheitsforscher entdecken eine Reihe von Sicherheitslücken in Patientendaten-App

Mitte September ging mit Vivy-App ein Prestigeobjekt von 16 Krankenversicherern in Deutschland an den Start, mit dem ca. 13.5 Millionen Kunden ermöglicht werden soll, ihre Patientendaten in einer digitalen Krankenakte anzulegen und zu verwalten. Weil die Entwickler gleich eine ganze Reihe von Tracking-Tools eingebaut hatten, mussten sie nach Intervention von Datenschützern nachbessern. Und obwohl die Vivy-Macher die Sicherheit der App in den Fokus der Werbung gestellt hatten, waren auch dort erhebliche Nachbesserungen fällig. Denn die zeigte gleich an mehreren Stellen schwerwiegende Mängel, wie die Security-Experten der Firma Modzero herausfanden. Nachdem die Schwachstellen behoben wurden, veröffentlichten sie die Mängelliste der App.

Ihr zufolge ermöglichte es die unsaubere Programmierung der Ende-zu-Ende-Verschlüsselung potenziellen Angreifern, die geheimen Ärzteschlüssel auszulesen und damit die Daten zu entschlüsseln. Denn das Dokument wurde unter einer Kennung aus fünf Kleinbuchstaben unter der Domain vivy.com öffentlich erreichbar gemacht. Für mögliche Angreifer wäre es ein leichtes, solche Dokumenten-URLs zu knacken und abzurufen. Zudem wurden die URLs automatisch von der App aus an 4 Drittanbieter in den USA und in Singapur geschickt. Als noch problematischer erwies sich, dass Angreifer dem Arzt, für den das Dokument bestimmt war, einen öffentlichen Decodierschlüssel unterschieben konnten, mit dem sie alle verschlüsselten Daten hätten auslesen können.

Desweiteren bemängelten die Forscher, dass die E2E-Verschlüsselung der App schon vom Plattform-Design fehleranfällig angelegt sei. Die Beschwichtigung seitens der Vivy-Entwickler, dass die App auf einer "vielschichtigen Sicherheitsarchitektur, die auf dem neuesten Stand der Technik beruht" aufbaue, widerlegten die Sicherheitsforscher von Modzero mit dem Hinweis, dass bei der Verschlüsselung mit Cipher Block Chaining eine Technik verwendet wird, die nicht mehr auf der Höhe der Zeit ist und verschlüsselte Daten nicht vor bösartiger Manipulation schützt.

Zugute halten muss man den App-Entwicklern, dass sie auf den Bericht der Modzero-Forscher schnell reagiert und die Sicherheitslücken nach eigener Aussage inzwischen geschlossen haben. Allerdings bleibt ein bitterer Nachgeschmack: Denn eigentlich hätten die Macher um die Hinweise froh sein können, bevor es zu ernsteren Problemen mit der unsicheren App gekommen wäre. Statt dessen warfen sie u.a. netzpolitik.org "falsche

Tatsachenbehauptungen und einseitige Darstellung" vor. Peinlich nur, dass die angegriffene Redaktion in den Aussagen der Vivy-App-Macher Widersprüche und unwahre Aussagen nachweisen konnte. Ob so ein gesunder Vertrauensaufbau möglich ist?

Nachzulesen unter:

https://www.heise.de/security/meldung/Vivy-Gravierende-Sicherheitsmaengel-in-Krankenkassen-App-aufgedeckt-4207260.html
https://www.modzero.ch/modlog/archives/2018/10/30/sicherheitsm_aumlngel_in_e-health_anwendungen/index.html
https://www.modzero.ch/static/vivy-app-security-final.pdf
https://www.zm-online.de/news/nachrichten/it-experten-finden-zahlreiche-sicherheitsluecken-bei-vivy
https://netzpolitik.org/2018/gesundheits-app-vivy-macher-versuchen-berichterstattung-zu-korrigieren
https://www.iphone-ticker.de/gesundheits-app-vivy-auf-sicherheits-folgt-kommunikationsdebakel-133394

III. Vom Werbegesicht zum Amtsgericht: Chinesische Gesichtserkennung stellt prominente Unternehmerin fälschlicherweise an den Pranger

Wer in China eine rote Fussgängerampel überquert, sollte sich bewusst sein, dass er oder sie dabei von Kameras erfasst, per Gesichtserkennung identifiziert und nach geltenden Regeln gebüsst werden kann – zumeist in der Form, dass das Foto mit Namensnennung und dem Hinweis auf das Fehlverhalten auf Grossdisplays öffentlich zur Schau gestellt wird – die digitalisierte Form des mittelalterlichen Prangers. Nun hat es eine der bekanntesten Unternehmerinnen des Riesenreichs erwischt: Dong Mingzhu ist Vorstandsvorsitzende des Klimageräteherstellers Gree Electric und wird auch schon mal als "Air-Con-Queen" Chinas bezeichnet. Die New York Times nannte sie auch schon "one of the toughest businesswomen in China".

In Ningpo erschien ihr Bild am öffentlichen Pranger, weil sie angeblich trotz roter Ampel einen Fussgängerübergang benutzt hatte. Das Bild, das kurze Zeit später veröffentlicht wurde, zeigte denn auch Dong Mingzhu – aber nicht beim Überqueren des Zebrastreifens, sondern beim Vorbeifahren als Werbeaufdruck auf der Seite eines Linienbusses. In den sozialen Netzwerken Chinas machte die Geschichte schnell die Runde. Und auch die Polizei von Ningpo reagierte unverzüglich und entschuldigte sich bei der Unternehmerin, die ihrerseits den Ordnungshütern dankte und die Bürger aufforderte, sich an die Verkehrsregeln zu halten.

Nachzulesen unter:

https://www.scmp.com/tech/innovation/article/2174564/facial-recognition-catches-chinas-air-con-queen-dong-mingzhu
https://www.independent.co.uk/news/world/asia/china-police-facial-recognition-technology-ai-jaywalkers-fines-text-wechat-weibo-cctv-a8279531.html
https://www.iottechnews.com/news/2018/nov/28/chinese-facial-recognition-ad-jaywalking
https://www.nytimes.com/2011/01/27/world/asia/27iht-dong27.html?pagewanted=all

IV. Alles andere als zum Knuddeln: Datenschutzbehörde verhängt nach Hackerangriff erstmalig Bussgeld wegen DSGVO-Verstoss

Knuddels.de ist eine der grössten deutschsprachigen Chatcommunities im Internet. 1999 gegründet, verzeichnete die Karlsruher Firma Mitte der 2000er Jahre mehr als 4 Millionen Nutzer. 2018 waren immerhin noch mehr als 300.000 Nutzer monatlich auf der Plattform aktiv. Anfang September 2018 meldete Knuddels der Datenschutzbehörde einen Hackerangriff, bei dem Cyber-Kriminelle ca. 808.000 Mailadressen sowie mehr als 1.8 Millionen Pseudonym-Nutzernamen erbeuteten. Weil ein Teil dieser Passwörter nicht verschlüsselt, sondern als Klartext abgespeichert wurden, fielen den Hackern neben dem Chatnamen auch Passwort, Mailadresse sowie Angaben zum echten Vornamen oder zum Wohnort in die Hände. Das Unternehmen reagierte rasch, erhöhte nach eigenen Angaben die Sicherheitsstandards und informierte sofort die Datenschutzbehörde.
Die lobte denn auch, dass das Unternehmen in vorbildlicher Weise kooperiert habe, monierte aber, dass die unverschlüsselte Speicherung personenbezogener Daten ein klarer Verstoss gegen die seit Mai 2018 geltende Datenschutzgrundverordnung DSGVO darstelle und verhängte dafür erstmalig ein Bussgeld. Die DSGVO sieht Strafen bis zu 20 Millionen oder maximal 4% des Jahresumsatzes vor. Die Busse für Knuddels wurde auf 20.000.- Euro festgesetzt.

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/Passwoerter-im-Klartext-20-000-Euro-Bussgeld-nach-DSGVO-gegen-Knuddels-de-4229798.html
http://www.spiegel.de/netzwelt/web/knuddels-de-von-hackern-angegriffen-a-1227170.html
https://www.golem.de/news/knuddels-leak-datenschuetzer-verhaengen-erstmalig-bussgeld-nach-dsgvo-1811-137857.html
https://www.basicthinking.de/blog/2018/11/28/knuddels-dsgvo-bussgeld
https://www.datenschutz.org/dsgvo-strafe-fuer-knuddels-ein-echo-aus-der-vergangenheit

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.