SWITCH-CERT report on the latest IT security and privacy trends

November/December 2018

SWITCH

I. SiSyPHuS gives Windows 10 low marks for data protection and security

As a national cyber security authority, Germany's Federal Office for Information Security (BSI) has responsibilities which, according to its own description, include 'helping users in government, business, and society to use IT products and software securely'. Because Windows 10 is the most widely used PC operating system, the BSI considers it especially relevant to the security of IT systems in Germany. This and the fact that Germany's Federal Office of Administration uses Windows 10 motivated the BSI to commission the respected Karlsruhe-based cyber security company ERNW in to conduct a major study on the security of the operating system.

The title: *SiSyPHuS Win 10*. Its scope: a thorough security analysis of the telemetry components as well as Trusted Platform Modules (TPM), VBS/DeviceGuard, Windows PowerShell, Application Compatibility Infrastructure, driver management and PatchGuard. The first results in the category of telemetry in the OS have now been published (for details, see the links to the bsi.bund.de below). The initial conclusion: Windows 10 does exactly what users have always feared, namely it collects data on system crashes and device use and sends it to the servers of the maker of Windows 10, Microsoft. According to the report, this includes 'data about how the machine is used with Windows 10 and connected devices, data about system performance, data collected

from errors such as software and system crashes, as well as data from Windows Defender and the Malicious Software Removal Tool (MSRT).' The report also criticises the fact that advanced IT knowledge is required to suppress or at least reduce the telemetry service's voraciousness for data in Windows 10. But there are two good reasons for doing so. From the perspective of data protection, it helps to better protect privacy; from the perspective of data security, a constant flow of data offers hackers a gateway for launching attacks. For this reason, the BSI has prepared a PDF including specific recommendations for procedures and configurations to disable or restrict the telemetry service. The document can be downloaded below.

The exact procedure for blocking communication between the PC sitting on your desk and the servers in Richmond, however, also depends on the other Microsoft programs installed on your device. This is because Office 365 and Internet Explorer send data to Microsoft servers without making use of the telemetry service in Windows 10. A Dutch government report on Office Pro Plus concluded that this puts Microsoft in violation of the European General Data Protection Regulation (GDPR). Microsoft could face hefty fines of more than 10 million euros if the matter goes to court. The software maker has now committed to developing an improvement plan to resolve these violations, which it will submit by April 2019.

Read more:

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 suffering from multiple diseases: security researchers uncover several vulnerabilities in the patient data app

In mid-September, a partnership incorporating 16 German health insurers unveiled its prestige project, Vivy. The new app is designed to give around 13.5 million customers the ability to set up and manage their patient data in a digital patient file. Because the developers included a whole range of tracking tools from the outset, they were eventually forced to make some improvements after data protection activists intervened. And although the makers of Vivy had focused their advertising efforts on the app's security features, major improvements were required in that area as well. This came after several serious flaws were discovered by the security experts at Modzero. After fixing the vulnerabilities, they published a list of the app's problems.

According to Modzero, sloppy programming of the end-to-end encryption function had made it possible for potential hackers to get their hands on doctors' keys and decrypt the data with them. This is because the document could be accessed on the domain vivy.com using an identifier consisting of five lower-case letters. For would-be hackers, it would be easy to crack and access these document URLs. What's more, URLs were automatically sent from the app to four third-party providers in the United States and Singapore. To make matters worse, hackers had managed to plant a public decryption key with the doctor for whom the document was intended and could use it to unlock all of the encrypted data.

Researchers also found faults in the app's error-prone E2E encryption which were embedded in the fundamental design of the platform. The Vivy developers attempted to reassure users by claiming that the app was built on a 'multi-layered, state-of-the-art security architecture', but this was debunked by the security experts at Modzero, who showed that the cipher block chaining used for encryption represents a technique that is no longer up-to-date and does not protect encrypted data against malicious tampering.

To the credit of the app developers, they did respond quickly to the Modzero report and, according to their own statements, closed the security gaps. The affair still left a bad aftertaste, however. You might have thought the developers would have been grateful to receive the information before they encountered even worse problems with the insecure app. Instead, they accused netzpolitik.org and others of 'making false claims and

painting a one-sided picture'. So it was all the more awkward when the writers they were targeting managed to find contradictions and false statements in the account given by Vivy's developers. Is this a healthy way to build trust?

Read more:

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. Facing court: Chinese facial recognition unfairly lands big entrepreneur in hot water

Any pedestrian who crosses the street on red in China should be aware that they are being filmed and identified using facial recognition, and are legally subject to punitive action – at least in the form of public display of a large format photo of the offender, with name, along with a description of the offence – a digital rendering of the medieval pillory. Recently, authorities 'nabbed' one of the best-known entrepreneurs in China – Dong Mingzhu, CEO of air conditioner manufacturer Gree Electric who has been called China's 'Aircon Queen'. The New York Times even referred to her as 'one of the toughest businesswomen in China'.

Her picture was recently put up on the digital pillory in Ningpo, because she had allegedly crossed the street on red. The image, which was later published, did indeed show Dong Mingzhu – but not crossing the street as a pedestrian, but rather on an advertisement on the side of a bus driving through the intersection. The story quickly made the rounds on Chinese social media. The police in Ningpo also responded immediately and apologised to the entrepreneur, who thanked law enforcement officials and reminded citizens to respect traffic rules and regulations.

Read more:

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. Not exactly cuddly: data protection authority imposes first GDPR fines after hacking attack

Knuddels.de (a name derived from the German word for 'cuddle') is one of the largest German-speaking chat communities on the web. Founded in 1999, the Karlsruhe-based company had more than four million users in the mid-2000s. In 2018, there were still more than 300,000 active users on the platform each month. In early September 2018, Knuddels reported to the data protection authority that it had fallen victim to a criminal cyberattack. Hackers had stolen around 808,000 email addresses and more than 1.8 million user pseudonyms. Because some of these passwords were left unencrypted and stored in plain text, the hackers were able to make off not only with the chat names but also their passwords, email addresses, and information about their real names and home addresses. The company responded quickly, announcing that it had improved its security standards, and immediately notifying the data protection authority.

The company was praised for its exemplary cooperation but admonished for unencrypted storage of personal data – a clear breach of the GDPR, which went into effect in May 2018. This marks the first time that fines for infringement of the regulation have been imposed. The GDPR stipulates that violations may be subject to fines of up to 20 million euros or a maximum of 4% of annual turnover. The fine for Knuddels was set at 20,000 euros.

Read more:

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

This SWITCH-CERT security report was written by Dieter Brecheis and Frank Herberg.