secorvo
security consulting

Secorvo Security News

März 2024

Voyeure überall

Am 15.03.2024 veröffentlichte Kaspersky den Stalkerware Report 2023. Unter Stalkerware werden kommerzielle Apps verstanden, die eine Überwachung des Smartphones einer anderen Person aus der Ferne ermöglichen. Rund 31.000 Fälle hat Kaspersky im Jahr 2023 allein bei Nutzern von Kaspersky-Lösungen gezählt. Die Gesamtzahl dürfte deutlich höher liegen, zumal Apps wie beispielsweise Ortungsdienste gar nicht unter die Definition von Stalkerware fallen, aber zum Stalking missbraucht werden können.

Weit aussagekräftiger als die absoluten Zahlen sind die Ergebnisse der 21.000 Online-Interviews, die Kaspersky Mitte Januar 2024 zusammen mit Arlington Research in 21 Ländern weltweit durchgeführt hat. Darin gaben 23% der Befragten an, dass sie bereits Online-Stalking durch einen Partner erlebt haben, 10% berichteten, dass ihr Standort verfolgt wurde und 7% hatten festgestellt, dass Stalker-Software auf ihren Geräten installiert worden war.

Am meisten erschüttert jedoch die Erosion des Anstands: Waren im Jahr 2021 noch 70% der Befragten der Auffassung, dass die Überwachung eines Partners ohne dessen Wissen völlig inakzeptabel ist, sank dieser Anteil 2024 auf 54%. Offenbar zählt die heimliche Beobachtung anderer Menschen zunehmend zu den üblichen Gepflogenheiten – zur Befriedigung der Neugier oder der subtilen Freude an der Macht, die intimes Wissen verschafft.

Von Menschen, die keinerlei Hemmungen verspüren, andere Menschen aus ihrem persönlichen Umfeld zum Gegenstand verdeckter Kontrolle zu machen, wird man wohl kaum erwarten dürfen, dass sie davor zurückschrecken, das Verhalten von ihnen Unbekannten zu überwachen. Vor dem Hintergrund der exponentiellen Zunahme digitaler Spuren kann einem angesichts dieser Entwicklung angst und bange um die Zukunft werden.

Inhalt

Voyeure überall

Security News

Generalüberholtes CSF

Consent Framework rechtswidrig

Features-by-Default

Auskunft bei Hackerangriff

Fehlerhafte Einwilligungen

Freier Normenzugang?

Secorvo News

Verstärkung

Seminare

14. Tag der IT-Sicherheit

Veranstaltungshinweise

secorvo
security consulting

Security News

Generalüberholtes CSF

Am 26.02.2024 stellte das amerikanische NIST das inzwischen verbreitete Cybersecurity Framework (CSF) in einer überarbeiteten Version 2.0 vor – fast genau zehn Jahre nach der Erstveröffentlichung. Sogar der ISO/IEC 27002:2022 verweist inzwischen auf den CSF (v1.1). Zielgruppe des Managementsystems für Cybersicherheitsrisiken sind nicht mehr nur kritische Infrastrukturen, sondern alle öffentlichen und privatwirtschaftlichen Einrichtungen.

In der jüngsten Fassung wird der neue Ansatz des Frameworks, Sicherheitsmaßnahmen nach den Zielen „Identify", „Protect", „Detect", „React" und „Recover" zu strukturieren (und damit zu verdeutlichen, dass ausschließlich präventive Maßnahmen zu kurz greifen), durch die Ebene „Govern" ergänzt: Sicherheit erfordert auch Steuerung.

Die sehr hilfreichen „Informal References" mit Querbezügen zu anderen Standards (auch dem ISO 27001) werden künftig dynamisch im National Online Informative References Program (OLIR) gepflegt; bisher sind darin noch nicht alle Referenzen des CSF 2.0 enthalten.

Auf der Webseite des Projekts findet man alle Materialien zum CSF. Das Framework selbst steht als PDF-Dokument, online sowie als JSON- oder Excel-Export zur Verfügung. Die Online-Version wurde in das Cybersecurity and Privacy Reference Tool (CPRT) integriert, über das weitere Standards zugänglich sind. Für Einsteiger sind die diversen Quick-Start-Guides ein guter Ausgangspunkt.

Consent Framework rechtswidrig

Anfang 2022 haben wir berichtet, dass die belgische Datenschutzaufsichtsbehörde ADP das Transparency and Consent Framework (TCF) von IAB Europe als rechtswidrig einstuft (SSN 02/2022): Willigt ein Nutzer innerhalb des TCF ein, wird auf der Endeinrichtung ein Transparency and Consent String (TC-String) gespeichert und an alle Werbepartner übermittelt. Unter Bezugnahme auf den TC-String und die IP-Adresse des Betroffenen erfolgt dann eine Echtzeit-Werbeauktion durch IAB Europe, das Real Time Bidding (RTB) (siehe auch SSN 05/2022).

Gegen die Entscheidung hatte IAB Europe Rechtsmittel eingelegt. Der EuGH folgte nun im Urteil vom 07.03.2024 der Auffassung der ADP, dass der TC-String ein personenbezogenes Datum darstellt und daher für das RTB eine Einwilligung erforderlich ist – ein klares Votum für den Datenschutz. Außerdem sei IAB Europe möglicherweise „gemeinsam Verantwortlicher" und damit für die Einhaltung der DSGVO zusammen mit den Werbetreibenden haftbar – ein schwerer Schlag für das Geschäftsmodell des „Real Time Bidding", aber ein großer Fortschritt bei der Begrenzung der Nutzer-Überwachung im Internet.

Features-by-Default

Microsoft-Cloud-Anwender können sich mit einem Entra Device Code auch von Geräten ohne echte Tastatur (wie z. B. Smart-TVs) anmelden. Ein Microsoft-Artikel vom 27.02.2024 erläutert nun, wie man dieses Feature mit neuen Conditional-Access-Funktionen schützen kann – denn schon im Oktober 2020 wurde es als Phishing-Einfallstor ausgemacht.

Das ist ein gutes Beispiel dafür, dass die Nutzung einer Cloud-Lösung nicht davon entbindet, sich eingehend mit deren Konfiguration zu befassen. Auch wenig bekannte oder nicht genutzte Features des Cloud-Dienstes sollte man kennen und ggf. deaktivieren, um Risiken zu minimieren. Security-by-Default (oder nach der DSGVO Privacy-by-Default) würde bedeuten, dass solche Features explizit aktiviert werden müssen. Aber das werden wir vermutlich genauso wenig erleben wie nach der Standard-Installation automatisch gehärtete On-Premise-Betriebssysteme – oder das schon lange versprochene papierlose Büro.

Auskunft bei Hackerangriff

Das Landgericht Berlin hatte mit Urteil vom 24.03.2023 entschieden, dass ein durch einen Hackerangriff betroffenes Unternehmen nicht auskunftspflichtig gemäß Art. 15 Abs. 1 DSG-VO hinsichtlich der durch den Hackerangriff erbeuteten (personenbezogenen) Daten ist. Verantwortliche Stelle für die im Rahmen des Hackerangriffs verarbeiteten Daten sei der Hacker, nicht dessen Opfer. Das gehackte Unternehmen trifft aber eine Benachrichtigungspflicht gemäß Art. 34 DSGVO: So muss es betroffene Personen über den Angriff bzw. die abgezogenen Daten informieren, wenn daraus ein hohes Risiko für die Rechte und Freiheiten der Betroffenen entsteht. Am 22.11.2023 wies das KG Berlin die gegen das Urteil eingelegte Berufung zurück: Zu den Gründen des Landgerichts komme hinzu, dass der Auskunftsanspruch persönlich und nicht abtretbar sei. Für einen Schadensersatz nach Art. 82 DSGVO müsse ein Betroffener zudem einen tatsächlichen (immateriellen) Schaden darlegen – Hackerangriffe sind keine Gelegenheit für Trittbrettfahrer.

Fehlerhafte Einwilligungen

Auf Webseiten und in Apps eine rechtskonforme Einwilligung in die Verarbeitung der Nutzungsdaten einzuholen ist für eine Vielzahl von Unternehmen offenbar eine nicht zu bewältigende Herausforderung, wie das Bayerische Landesamt für Datenschutzaufsicht am 09.02.2024 feststellte. So muss nach Auffassung der deutschen Datenschutzaufsichtsbehörden (DSK) die Möglichkeit, keine Einwilligung zu erteilen, zwingend auf der ersten Ebene eines Cookie Banners angeboten werden, sofern die Webseite nicht ohne Interaktion mit dem Einwilligungs-Banner beeinträchtigungsfrei genutzt werden kann – eine Eigenschaft mit Seltenheitswert.

Unternehmen, die sich bislang mit fehlender Rechtsprechung entschuldigen, sollten besser das Urteil des OLG Köln vom 19.01.2024 lesen: Wenn dem Seitenbesucher durch die Gestaltung des Cookie-Banners „weder auf der ersten noch auf der zweiten Ebene eine gleichwertige, mithin auf klaren und umfassenden Informationen beruhende Ablehnungsoption angeboten“ und dieser deshalb „zur Abgabe der Einwilligung hingelenkt und von der Ablehnung der Cookies abgehalten wird“, so kann „die erteilte Einwilligung nicht“ im Sinne von § 25 Abs. 1 TTDSG und Art. 4 DSGVO „als freiwillig und hinreichend aufgeklärt angesehen werden“ – sprich: Die Datenverarbeitung ist in diesem Fall rechtswidrig und es drohen Bußgelder und Schadensersatzforderungen.

Wer dieses Risiko vermeiden will, findet konkrete Hinweise zur rechtskonformen Einholung einer Einwilligung z. B. in den FAQ des LfDI Baden-Württemberg.

Freier Normenzugang?

Am 05.03.2024 hat der EuGH abweichend von der bisherigen Rechtsprechung des EuG (Urteil vom 14.07.2001) entschieden, dass EU-Bürger das Recht haben, auf solche technischen Normen zuzugreifen, die Bestandteil europäischer Verordnungen und Richtlinien und damit Teil des Unionsrechts sind. Damit gewähre das Unionsrecht jeder natürlichen oder juristischen Person mit Wohnsitz oder Sitz in der EU den (kostenlosen) Zugang zu im Amtsblatt der EU veröffentlichten harmonisierten Normen. Da deren Rechtswirkung für Wirtschaftsteilnehmer von wesentlicher Bedeutung sei, müsse es jeder durch ein Gesetz geschützten Person möglich sein zu prüfen, ob ein Produkt die gesetzlichen Regeln einhalte.

Dieses öffentliche Interesse überwiege den (einem freien Zugang zu Normen normalerweise entgegenstehenden) Schutz der berechtigten geschäftlichen Interessen und des geistigen Eigentums der Rechteinhaber. Das Urteil erstreckt sich nach Einschätzung des DIN vom 15.03.2024 auf rund 3.000 harmonisierte EU-Normen – darunter wahrscheinlich auch einige IEC- und ETSI-Standards zur Informationssicherheit, soweit deren Einhaltung verbindlich vorgeschrieben ist.

Secorvo News

Verstärkung

Seit dem 01.03.2024 verstärkt Markus Toran (M.Sc. Informatik mit Schwerpunkt Information Security) unser Beratungsteam. Herzlich willkommen!

Seminare

Kurzentschlossene können noch einen Platz für das Seminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) vom **22. bis 25.04.2024** buchen: vier Tage spannende Vorträge und interaktive Workshops rund um die sichere Software-Entwicklung mit der Möglichkeit zur anschließenden Zertifizierung als T.P.S.S.E.

Mit dem Wissens-Booster IT-Security Insights – T.I.S.P.-Update vom **14. bis 15.05.2024** bringen Sie sich im Bereich der IT-Sicherheit auf einen aktuellen Stand.

Und das fünftägige T.I.S.P.-Seminar bereitet Sie vom **24. bis 28.06.2024** auf die Zertifikatsprüfung zum TeleTrusT Information Security Professional vor. Ein Exemplar der gerade erschienenen 4. Auflage des Begleitbuchs zum T.I.S.P. schicken wir Ihnen nach Ihrer Anmeldung zu.

Alle drei genannten Seminare haben bereits die Mindestteilnehmerzahl erreicht und werden stattfinden.

14. Tag der IT-Sicherheit

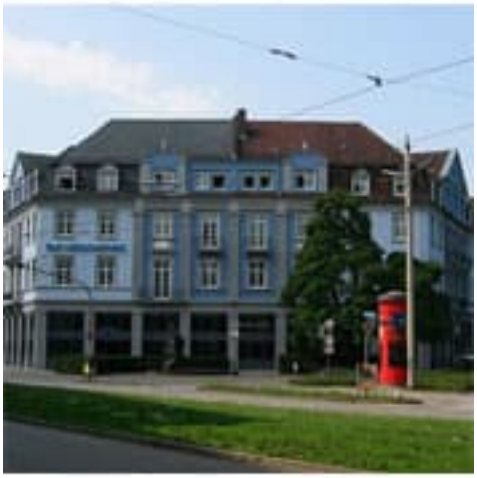
Zum Vormerken: Am **18.07.2024** findet der 14. „Tag der IT-Sicherheit“ in der IHK Karlsruhe statt. Das Programm wird in Kürze veröffentlicht – so viel sei aber schon einmal verraten: Die Keynote hat Ralf Wigand übernommen, National Security & IT-Compliance Officer von Microsoft Deutschland.

Es erwarten Sie zahlreiche weitere Vorträge zu aktuellen Themen der Informationssicherheit – und natürlich der anschließende Erfahrungsaustausch beim „Buffet-Networking“.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2024	
09.-11.04.	GI Sicherheit 2024 (Gesellschaft für Informatik, Worms)
11.04.	KA-IT-Si-Event "No risk, no fun." (KA-IT-Si, Karlsruhe)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/ASE)
22.-25.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2024	
07.-08.05.	20. Deutscher IT-Sicherheitskongress (BSI, virtuell)
14.-15.05.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
14.-16.05.	Datenschutztage 2024 (WEKA Akademie, Niedernhausen hybrid)
22.-24.05.	25. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2024 (IACR, Zürich/CH)
28.-29.05.	BvD Verbandstage 2024 (BvD, Berlin)
Juni 2024	
03.-05.06.	Entwicklertag 2024 (VKSI, GI, ObjektForum, Karlsruhe)
04.-07.06.	European Identity & Cloud Conference 2024 (KuppingerCole, Berlin)



Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

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