secorvo
security consulting

Secorvo Security News

November 2020

Unter den Wolken

Luftaufnahmen haftet etwas Magisches an. Vielleicht, weil sie aus einer Perspektive aufgenommen werden, die wir Menschen aus eigener Kraft nicht einnehmen können – es grüßt der ewige Traum vom Fliegen. Diese Faszination ist es wohl auch, die Menschen auf Türme, Berge und zu Ballonfahrten und Fallschirmsprüngen treibt.

Doch diese bislang seltenen Bilder werden selbstverständlicher: Dank leistungsstarker Servo-Motoren, verbesserter Batterie-, Funk- und Kameratechnik sowie hochwertiger GPS-, Beschleunigungs- und Gyro-Sensoren liefern mit Videokameras bestückte Drohnen heute Aufnahmen, die zuvor bestenfalls aus Hubschraubern möglich waren.

Und das weckt Begehrlichkeiten. Drohnenflüge kosten nur einen mikroskopischen Teil eines Hubschrauberflugs, können fast überall gestartet werden und liefern Bilder in Echtzeit – perfekte Voraussetzungen für eine großflächige Überwachung des öffentlichen Raums. Im April wurden in Düsseldorf Drohnen zur Überwachung der Einhaltung der Corona-Kontaktbeschränkung eingesetzt.

Mitte November brachte die Firma DJI die Kamera-Drohne „mini 2“ auf den Markt: Mit nur 239 g darf sie von jedermann geflogen werden, überträgt Full-HD-Aufnahmen über eine Distanz von bis zu 10 km und erreicht eine Fluggeschwindigkeit von über 57 km/h. Bei einer Flugdauer von bis zu 30 Minuten und einer maximalen Flughöhe von 4.000 m ist der Wirkungskreis gewaltig. Die Motoren sind schon aus wenigen Metern Entfernung nicht mehr zu hören – und die nur 14 cm lange Drohne kaum noch zu erkennen.

Die Anschaffung eines Polizeihubschraubers kostet rund 5,8 Mio. €, Betriebs- und Flugkosten sowie die Pilotenausbildung nicht gerechnet. Für diesen Betrag erhält man – ohne Preisverhandlung – rund 13.000 Mini-Drohnen: für jeden vierten Bundespolizisten eine.

Schöne neue Überwachungswelt.

Inhalt

secorvo
security consulting

Security News

Vorsicht bei Gesundheits-Apps

Neben sogenannten „Medical Apps“ aus dem Lifestyle- und Wellness-Bereich wurden am 06.10.2020 die ersten „Gesundheits-Apps“ zugelassen, die es vom Arzt auf Rezept gibt und deren Kosten von den gesetzlichen Krankenversicherungen übernommen werden. In das DiGA-Verzeichnis aufgenommen werden die Apps ohne weitere sicherheits- und datenschutzrechtliche Prüfung durch die zuständigen Behörden nach einem an die CE-Kennzeichnung angelehnten „Fast-Track“-Verfahren: Die Hersteller geben eine Erklärung ab, in der sie versichern, dass sie die gesetzlichen Vorgaben einhalten. Dieses kursorische Verfahren bewertet der Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz kritisch – bei den ersten angebotenen „Apps auf Rezept“ wurden bereits erhebliche Sicherheits- und Datenschutzlücken festgestellt. Eine Überprüfung durch die zuständige Aufsichtsbehörde, das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), fand erst im Nachgang statt. Wer solche Apps verschrieben bekommt oder freiwillig nutzen möchte, sollte sich zuvor genauer mit den Einstellungen beschäftigen. Blindes Vertrauen in solche Anwendungen ist jedenfalls nicht zu empfehlen.

Spurenarm Surfen

Wer im Internet „surft“ hinterlässt Spuren – unvermeidlich beim Anbieter der aufgerufenen Seite und fast immer zusätzlich bei eingebundenen Trackern, Werbeseitenanbietern, Diensten, Icons von Social Networks oder Schriftarten. Zwar dürfen IP-Adresse und Zugriffszeitpunkt nur mit Einwilligung der Betroffenen übermittelt und von den Empfängern zu eigenen Zwecken wie der Gewinnung von Werbe-Profilen genutzt werden – aber darum kümmern sich viele Anbieter wenig.

Schutz gegen solcherart unerwünschtes Tracking bieten nicht nur die Datenschutz-Grundverordnung, sondern auch Browser-Einstellungen und die Nutzung von Browser-Erweiterungen. Sie begrenzen das Tracking auf den Seitenanbieter, sperren lästige Werbeeinblendungen aus und verkürzen so, ganz nebenbei, die Ladezeiten von Webseiten merklich. Aber Achtung: Man sollte nur Browser-Erweiterungen installieren, denen man vertraut, sonst holt man sich leicht statt eines Privatsphärenschützers einen Spionagehelfer in den Browser (SSN 04/2020).

Bei den Browser-Einstellungen empfiehlt es sich, zumindest so genannte „Third-Party Cookies“ zu deaktivieren. Empfehlenswerte Browser-Erweiterungen sind beispielsweise der Privacy Badger oder HTTPS Everywhere der EFF. ClearURLs entfernt Tracking-Bestandteile aus URLs. Mit Decentraleyes werden lokale Ressourcen statt solcher von einem zentralen Content Delivery Network (CDN) injiziert. uBlock Origin blockiert nicht nur lästige Werbeeinblendungen sondern auch bösartige und gefährliche Domänen. Und wer sein Netzwerk bereits auf DNS-Ebene von einem dedizierten Gerät aus filtern möchte, dem empfiehlt sich Pi-hole. Zu guter Letzt kann man über „Cover Your Tracks“ (ehemals Panopticlick) prüfen, wie eindeutig der „Fingerprint“ des eigenen Browsers ist und was man dagegen tun kann.

Verräterische Uploads

Am 18.05.2020 berichtete die Investigativ-Journalismus-Webseite „bell¿ngcat“, wie mittels einer Bier-Bewertungs-App Militärpersonal identifiziert und vertrauliche Dokumente gefunden werden können: Manche der in Untappd hochgeladenen und mit einer Örtlichkeit (wie z. B. einer Bar) verknüpften Fotos des getrunkenen Bieres zeigen neben dem Bierglas Militärausweise, Kreditkarten und Militärdokumente. Jedes Besucher-Profil besitzt zudem eine „Timeline“ der Örtlichkeiten, an denen die Person bereits ein Foto hochgeladen hat. So konnten sogar geheime oder inoffizielle Militärbasen identifiziert und chronologische Abläufe von Reisen zwischen Militärbasen und privaten Aufenthaltsorten rekonstruiert werden.

Ähnliches erlaubt die „Heatmap“ der Fitness-App Strava: Wie Nathan Ruser bereits am 27.01.2018 erkannte, kann diese genutzt werden, um Militärbasen zu erkennen und detailliert zu kartographieren. Bereits am 08.07.2018 berichtete bell¿ngcat, wie dank der Fitness-App von Polar das Haus und die Jogging-Gewohnheiten eines hochrangigen Militäroffiziers einer Nuklearwaffenbasis herauszufinden waren – samt vollem Namen.

Auch Bewertungen auf Google Maps oder Amazon bieten Einblick in Aufenthaltsorte, Vorlieben und Gewohnheiten von Personen. Wenn diese Angaben z. B. über die Suche nach Benutzernamen, Aufenthaltsorten, Freunden, Bekannten oder Verwandten mit Daten anderer sozialer Netzwerke wie Swarm korreliert werden, ergibt sich schnell ein aussagekräftiges Gesamtbild.

Für Sammelpunkte, die Ernennung zum „Local Guide“ oder „Top Reviewer“ machen Menschen ihr Leben öffentlich und sich selbst zum freiwillig gläsernen Menschen. Beim nächsten Joggen, Biertrinken oder Bewerten sollte man vielleicht darüber nachdenken, ob man diese Spuren wirklich hinterlassen möchte.

secorvo
security consulting

Github Code Scanning

Nachdem Github am 18.09.2019 das Code-Analyse-Unternehmen Semmle übernommen hat, bietet Github auf Basis der CodeQL-Technologie seit dem 30.09.2020 auf Github automatisierte Code Scans an. Diese Funktionen wie Scans auf Schwachstellen im Code und den Abhängigkeiten oder auch die Suche nach hartkodierten Geheimnissen sind sowohl für Enterprise-Modelle als auch über öffentliche Repositories verfügbar. Sobald Änderungen am Code in ein Repository hochgeladen werden, können entsprechende Code Scans automatisch durchgeführt und Schwachstellen zeitnah ausfindig gemacht werden. Eine einfache Möglichkeit, Schwachstellen aufzudecken ohne in komplexe Technologien oder teure Werkzeuge investieren zu müssen. Insbesondere für finanziell häufig klamme Open-Source-Projekte ist dieses Angebot ein Mehrwert. Erste Erfahrungsberichte bestätigen das: Durch die Anpassungsmöglichkeiten an die jeweiligen Anwendungsumgebungen war es im Jenkins-Projekt möglich, sieben Schwachstellen in verschiedenen Plug-Ins zu identifizieren, die generische Code Scanner nicht finden konnten.

Datenschutz in Videokonferenzsystemen

Mit der zunehmenden Nutzung von Web- bzw. Videokonferenzen seit Beginn der Corona-Pandemie haben sich viele Datenschutzaufsichtsbehörden zu deren Zulässigkeit und zu den an diese zu stellenden Datenschutzanforderungen geäußert. Mit der neuen Orientierungshilfe der Datenschutzkonferenz (DSK) vom 23.10.2020 fassen die Aufsichtsbehörden nun (endlich) ihre Auffassung zusammen. Darin wird weiterhin von einem Auftragsverarbeitungsverhältnis zum Anbieter ausgegangen; dafür führt das Papier als neue Rolle die des „Veranstalters“ als Verantwortlichem ein. Für den Austausch von bspw. Gesundheitsdaten soll zuvor eine Einwilligung eingeholt werden, der Kommunikationskanal wird zur eigenständigen Inhaltsverarbeitung erklärt.

Mit der Checkliste zur Orientierungshilfe können Unternehmen überprüfen und dokumentieren, ob das von ihnen eingesetzte Tool den Anforderungen der Aufsichtsbehörden entspricht oder ob Nachbesserungsbedarf besteht, etwa bzgl. der vertraglichen Nutzungsgrundlagen, Betroffeneninformationen oder der technischen Einstellungen. Dabei erscheinen die Antworten auf die Checkpunkte durch die bekannten Einschätzungen der DSK bereits determiniert, sodass die Verantwortlichen lediglich zum bereits vorbestimmten Ergebnis (Unzulässigkeit) geführt werden. Die in ersten Stellungnahmen teilweise eklatanten Begründungsmängel setzen sich auch in den gemeinsamen Papieren abgeschwächt fort, daher ist der tatsächliche Nutzen leider begrenzt.

Hallo Admin

Am 10.11.2020 berichtete der Sicherheitsforscher Kevin Backhouse vom Github Security Lab, wie man mit einer einfachen Methode Administrator-Privilegien in der Desktop-Variante von Ubuntu 20.04 erlangen konnte. Hierfür leitete der Sicherheitsforscher die Datei „.pam_environment“ auf „/dev/zero“ um. Nach Änderung einer Benutzereinstellung (wie z. B. der genutzten Sprache) versucht der Hintergrunddienst „accounts-daemon“ die umgeleitete Datei einzulesen und landet in einer Endlosschleife. Danach kann der Dienst (durch ein eingebautes Sicherheits-Feature, das den Zugriff auf sensible Dateien verhindern soll) von einem normalen Benutzer zum Absturz gebracht werden.

Bei der nächsten Anmeldung wird der Benutzer dann von GNOME mit dem Dialog zur erstmaligen Einrichtung eines Administrator-Accounts begrüßt – da der Login-Manager nicht mit dem „accounts-daemon“ kommunizieren kann, nimmt er an, es gäbe keine Benutzer auf dem System.

Die Sicherheitslücke zeigt eindrucksvoll, wie sämtliche Schutzmaßnahmen sehr einfach durch das Versetzen des Systems in einen Ausnahmezustand umgangen werden konnten. Eine schöne Metapher für viele Sicherheitslücken – sind es doch oft Sonderfälle, die ausgenutzt werden können. Diese funktionieren übrigens auch beim Menschen: Versetzt man jemanden durch Zeitdruck, Androhung von Konsequenzen, Schmeicheleien o. ä. in einen Ausnahmezustand, fällt er auf Social Engineering herein.

Secorvo News

Adventsrätsel

Am 01.12.2020 startete die sechste Staffel des Adventsrätsels „Krypto im Advent“, einer Initiative von Secorvo in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe. Sie führt jährlich rund 4.000 Kinder und Jugendliche spielerisch an Verschlüsselungstechniken heran. Dabei gilt es, über 24 Tage spannende Verschlüsselungs-Rätsel zu lösen, um einen der über 250 Sachpreise zu gewinnen.

Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind auch nach dem 01.12. noch möglich (Krypto-im-Advent.de); die Teilnahme ist kostenlos.

Erzählen Sie es weiter – und rätseln Sie gerne mit!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
01.-02.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)
März 2021	
03.-04.03.	Future Security 2021 (Fraunhofer VVS, Nürnberg)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Europol veröffentlichte am 05.10.2020 den Bericht "Internet Organised Crime Threat Assessment" (IOCTA): aktuelle Bedrohungen durch die organisierte Kriminalität auf gut 60 Seiten. Aufgeführt werden konkrete Beispiele wie die „Versteigerung“ geraubter Daten und Schwierigkeiten, z. B. auch in Deutschland die Infrastruktur von „Bulletproofed“-Hostern zu stören. Durchaus empfehlenswert, um sich einen Überblick über die aktuelle Bedrohungslage zu verschaffen und gegebenenfalls die eigenen Schutzmaßnahmen anzupassen.

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