Secorvo Security News

August 2021

Dialektik

Man mag den Marxismus für eine Irrung oder eine mindestens wirtschaftlich gescheiterte Ideologie halten. Eines der drei von Engels in etwas freier Umdeutung von Hegels Dialektik aufgestellten Grundgesetze ist jedoch zweifellos eine zutreffende Beschreibung eines immer wieder zu beobachtenden Phänomens: Des Umschlags von Quantität in Qualität.

So sorgen nicht einzelne Staubkörner für eine Verschmutzung (von Reinsträumen einmal abgesehen), sondern erst deren große Zahl. Sandkörner bilden Strände und Schneeflocken Skipisten – aber nur, wenn sehr viele davon an einer Stelle zusammenkommen. Der Punkt, an dem dabei die Quantität zu einer neuen Qualität wird, ist nicht exakt auszumachen und liegt vielleicht auch im Auge des Betrachters. Irgendwann aber gibt es keinen Zweifel mehr, dass sie zu Dreck, Strand oder Skipiste geworden sind.

Unter demselben Phänomen leidet der Datenschutz – schon immer, aber seit der Entdeckung der Digitalisierung immer offensichtlicher. Einzelne Verarbeitungen personenbezogener Daten bedrohen selten die freie Entfaltung. Wohl aber deren viele. So mag eine einzige Videokamera auf einem öffentlichen Platz eine erträgliche Freiheitsbeschränkung sein. Eine auf jedem öffentlichen Platz schon weniger – und die nahtlose Aufzeichnung öffentlicher Bereiche sicher nicht.

Das ist ein Kernproblem des Datenschutzes. Gegen eine einzelne Verarbeitung mag wenig einzuwenden sein, doch im Kontext vieler weiterer wird sie irgendwann Teil einer potentiellen Überwachungsinfrastruktur.

Was dem Datenschutz daher fehlt ist ein Limit, das das Umschlagen in Überwachung verhindert. Wäre z. B. die Größe der durch Videokameras zulässig überwachbaren Fläche begrenzt oder die Datenmenge, die Webseiten und Apps „nach Hause“ schicken dürfen, würden sehr bald sinnvolle Prioritäten gesetzt – und ließen sich viele Verarbeitungen entspannter ertragen.

Security News

Der Schein darf trügen

Das Oberverwaltungsgericht Rheinland-Pfalz hat am 25.06.2021 entschieden, dass die DSGVO auf abgeschaltete Überwachungskameras nicht anwendbar ist. Die Aufsichtsbehörde hatte den Kläger aufgefordert, die Kamera zu beseitigen, dieser schaltete sie jedoch lediglich ab. Die Behörde stützte ihre Anordnung auf Art. 58 Abs. 2 lit. f) DSGVO. Nach Ansicht des Gerichts verarbeitet eine ausgeschaltete Kamera ebensowenig Daten wie eine Attrappe. Das ist sachlich richtig, denn wo keine Daten erhoben werden, findet auch keine Verarbeitung statt. In der Konsequenz bedeutet dies,

dass auch kein Hinweis auf die nicht stattfindende Videoüberwachung erfolgen muss und damit auch keine Kennzeichnungspflicht besteht. Die Entscheidung reiht sich in weitere, die einen Unterlassungsanspruch in solchen Fällen ablehnen (z. B. OLG Frankfurt a. M., Beschluss vom 12.10.2017 – 3 U 195/16). Zwar bleibt für den Betroffenen das „Überwachungserlebnis" dasselbe, da er eine Verarbeitung annehmen muss – aber ohne Daten auch kein Datenschutz.

Self-Assessment

Besonders für kleinere und mittlere Unternehmen ist es oft aufwendig, sich Grundkenntnisse der IT-Sicherheit als Beratung einzukaufen oder gar ein eigenes Security-Team aufzubauen. Da können Self-Assessment-Werkzeuge helfen. Sie ersetzen zwar kein externes Audit, geben jedoch einen ersten Überblick über die aktuell wichtigsten Themenbereiche und Sensibilisierungsmaßnahmen.

Bekannte Tools sind z. B. der ExPress Informationssicherheits Check (EPIC) des BSI, das Cyber Resilience Review (CRR) der CISA, der Cyber Aware Action Plan des GCHQ, der Sec-O-Mat der TISiM, das Cybersecurity Self-Assessment for SMEs von Cyberwatching oder auch das Security and Risk Self-Assessment von Brennan IT. Eine zusätzliche wertvolle Ressource liefert das CIS mit den CIS Controls.

Als Einstieg in die Informationssicherheit ist ein solches Self-Assessment jedenfalls keine schlechte Wahl. Mit dem CSIRT Maturity Self-Assessment Tool der ENISA lassen sich sogar mögliche Optimierungen für ein bereits bestehendes IT-Sicherheitsmanagement finden.

Druckereskalation

Am 19.05.2021 wurde von HP eine Schwachstelle im Druckertreiber diverser HP LaserJet Drucker veröffentlicht. Die gemäß HP mit einem CVSS-Score von 8.8 bewertete Schwachstelle CVE-2021-3438 ermöglicht über einen Buffer Overflow die Gewinnung von Berechtigungen im System-Kontext. Das ist ein gravierender Bug, sowohl hinsichtlich der möglichen Auswirkungen als auch wegen dessen weiter Verbreitung. Angreifer können sich darüber dauerhaft in einem System mit hohen Privilegien festsetzen.

Über die vom Hersteller bereitgestellten Updates (die zügig eingespielt werden sollten) hinaus stellen sich gleich mehrere Fragen: Warum erfolgt die Ausgabe von Dateien an einen Drucker heute noch mit hohen Privilegien? Warum geht das nicht im Benutzerkontext? Und: Warum benötigt ein Druckertreiber eine 25 MB große Installationsdatei, mit Utilities sogar oft über 100 MB? Sind bei diesem Umfang und dieser Komplexität nicht übersehene Schwachstellen zu erwarten? Welche technologische Entwicklung rechtfertigt eine solche Treiberkomplexität? Nicht zuletzt: Wurden (und werden) die Treiber vom Hersteller überhaupt gründlich auf Schwachstellen untersucht? Nach Auskunft der Forscher, die die Schwachstelle entdeckten, bestand sie seit mindestens 16 Jahren.

Ganz ähnliches gilt für Grafik-Treiber, die heute oft einen Umfang von über 700 MB mitbringen. Gerade Drucker- und Grafiktreiber-Programmierer sollten sich

professionell mit der Frage beschäftigen, wie die erforderlichen Funktionen kompakt und ohne Scheunentore bereitgestellt werden können. Helfen würde, wenn in Unternehmen und Behörden bei der Beschaffung von Hardware auch die Komplexität und Sicherheit der Treiber eine Rolle spielen würde (gemessen z. B. daran, wie viele Schwachstellen es bereits gab).

Better Hunting

Seit dem 02.08.2021 steht das forensische Werkzeug Autopsy in der neuen Version 4.19 zur freien Nutzung bereit. Sehr hilfreich ist das neue YARA-Ingest-Modul, das man mit eigenen Zusammenstellungen von Regeln für spezifische Fragestellungen (z. B. VBA-Macros in MS Office-Dokumenten) ablaufen lassen kann. Das Modul arbeitet problemlos mehrere tausend YARA-Regeln fehlerfrei ab, wenn man es z. B. zur Suche nach Schadsoftware auf eine Datenquelle anwendet.

Wesentlich beschleunigt wurde die Erstellung des Stichwort-Index, der nun nicht mehr versucht, eine Indexierung in mehreren Sprachen sowohl für unbekannte Dateiformate als auch für nicht belegten Speicherplatz eines Datenträgers (*unallocated space*) durchzuführen – für schnellere Triagen sehr hilfreich. Muss man als Incident Responder die „Nadel im Heuhaufen" suchen, kann die Suche zeitlich abgetrennt werden, indem der gesamte unallocated space zuerst mit Autopsy in eine separate Datei extrahiert wird.

Auch die Autopsy-Fallakte wurde verbessert, sodass unterschiedliche Datenquellen jeweils genau einem System oder einem Fundort zugewiesen werden können. Damit sind z. B. ein Desktop-PC, ein Laptop, ein Smartphone oder ein USB-Gerät als einzelne Entitäten logisch gruppierbar. So können z. B. auch logische Extraktionen von unterschiedlichen Volumenschattenkopien einer Windows-Installation zugeordnet werden. Ergänzt wird die Fallakte durch die optionale Zuordnung einer Datenquelle zu einem definierten Nutzer.

Die Einarbeitung in dieses Werkzeug erfordert etwas Zeit. Versteht man aber die Logik, dann lassen sich viele Detailspuren finden. Durch unterstützende Plugins wurde zuletzt auch die forensische Unterstützung für QNX (Echtzeitbetriebssystem im Bereich Automotive) realisiert.

Neue Mindeststandards des BSI

Am 07.07.2021 hat das BSI zwei überarbeitete Mindeststandards zur Nutzung externer Cloud-Dienste und für Schnittstellenkontrollen veröffentlicht. Ein Cloud-Dienst, z. B. eine Datenablage oder eine Kollaborationsplattform, ist schnell eingekauft. Aber passt der Dienst wirklich zur Unternehmensstrategie, wurde an den Datenschutz gedacht und wie sehen die Exit-Optionen aus? Zu diesen Fragen formuliert der Standard in strukturierter Form von der Planung bis zur Beendigung Anforderungen, an die definitiv gedacht werden sollte. Im Rahmen der Überarbeitung wurden die Mitnutzung von Cloud-Diensten integriert und die Inhalte an den IT-Grundschutz-Baustein sowie den Kriterienkatalog Cloud Computing angepasst.

Über Schnittstellen kann es zu Schadsoftwarebefall oder unerwünschtem Abfluss von Daten kommen.

Schnittstellen entstehen häufig „unkontrolliert“ mit einem neuen System oder einer Anwendung. Der Standard zeigt die wichtigsten Anforderungen im Lebenszyklus einer Schnittstelle und die zu ergreifenden Kontrollmaßnahmen.

Beide Standards gelten eigentlich nur für die Informationstechnik des Bundes, enthalten aber auch für andere Behörden und Unternehmen in kompakter Form wertvolle Hinweise. Sie können somit als Checklisten verstanden und genutzt werden. Systematisch und kostenlos – wenngleich die Umsetzung der Anforderungen (sinnvoll investierten) Aufwand verursacht.

One Face fits most

Am 01.08.2021 veröffentlichten israelische Forscher eine Studie mit dem Titel „Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution“. Darin stellen sie vor, wie sie mit KI-Werkzeugen sprichwörtliche „Allerweltsgesichter“ erzeugen können, die beim Vergleich mit Einträgen einer Referenzdatenbank für Gesichtserkennung (Labeled Faces in the Wild – LFW) zahlreiche „False Positives“ lieferten. Einzelne der synthetisierten Gesichter wurden mit bis zu 20% der Referenzdatensätze positiv abgeglichen; mit nur neun speziell erzeugten Gesichtern gelang das bei 40% aller Referenzgesichter.

Die Untersuchung lässt erwarten, dass eine Authentifizierung mittels biometrischer Gesichtserkennung auch zukünftig keine große Verlässlichkeit bieten wird. Zweifel an der Zuverlässigkeit biometrischer Identifikation sind demnach geboten. Und die Erfahrung lehrt: Angriffe werden über die Zeit besser, nicht schlechter.

Secorvo News

Seminare wieder möglich

Noch gibt es freie Plätze bei unseren Herbst-Seminaren – T.I.S.P., T.P.S.S.E., Live-Hacking und PKI. Wir empfehlen eine baldige Anmeldung unter https://www.secorvo.de/seminare.

Irren ist kryptografisch

Die Kryptoanalyse der ENIGMA ist eine der spannendsten Geschichten in der Kryptografie. Bis in die 70er Jahre wurde in der Öffentlichkeit – und nicht nur dort – angenommen, dass die wichtigste Verschlüsselungsmaschine des zweiten Weltkriegs nicht geknackt worden war. Ein Irrtum: Die ENIGMA wurde bereits in den 30er Jahren erfolgreich analysiert, und während des Krieges wurden in Bletchley Park (GB) Nachrichten deutscher U-Boote systematisch entschlüsselt.

Auf dem kommenden KA-IT-Si-Event am 30.09. 2021 wird Johann Grathwohl (IT-Security-Architekt bei CONITAS) die Entwicklung und die historischen Hintergründe der ENIGMA vorstellen und ihre Funktionsweise erläutern. Anschließend wird er die Kryptoanalyse skizzieren und auf Schwachpunkte und Fehler im Design des Verschlüsselungsverfahrens eingehen und daraus einige wichtige Erkenntnisse für den Entwurfsprozess ableiten.

Wir freuen uns darauf, unsere KA-IT-Si-Events nun wieder als Präsenzveranstaltungen durchführen und Ihnen unser „Buffet-Networking“ zum persönlichen Austausch anbieten zu können. Um die Vorträge auch weiterhin so vielen Interessenten wie in den vergangenen Monaten zugänglich zu machen, werden wir auch eine Teilnahme per Livestream ermöglichen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2021	
06.-10.09.	6th IEEE European Symposium on Security and Privacy (IEEE Computer Society, virtuell)
13.-16.09.	European Identity & Cloud Conference 2021 (KuppingerCole, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.09.-01.10.	Informatik 2021 (GI, Berlin)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
30.09.	Irren ist kryptografisch (KA-IT-Si, Karlsruhe/online)
Oktober 2021	
04.-07.10.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
12.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
12.-14.10.	it-sa 2021 (NürnbergMesse GmbH, Nürnberg)
17.-21.10.	Eurocrypt 2021 (IACR, Zagreb/HRV)

Fundsache

Am 18.07.2021 hat Amnesty International Security Lab ein forensisches Mobile Verification Toolkit veröffentlicht, mit dem auf mobilen Geräten nach Spuren der Pegasus-Spyware gesucht werden kann. Die Python-Quellen und eine Anleitung finden sich auf Github.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, 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