Secorvo Security News

Juni 2023

Die IT frisst ihre Kinder

Es war wohl der IBM PC, der vor über 40 Jahren den Siegeszug der Informationstechnik auslöste. Das Versprechen: Computer machen unser Leben leichter. Und tatsächlich: Wer zuvor Schreibmaschine und Stift für die Korrespondenz benutzt hatte, konnte seinen Durchsatz mit Tastatur und E-Mail leicht verzehnfachen.

Als rund 20 Jahre später Internet-Portale Bankgeschäfte, Einkäufe, Musikgenuss, Videoverleih und Behördengänge von zuhause ermöglichten, steigerte auch das unsere Lebensqualität. Die Ersetzung des transportresistenten PC durch Laptops und Smartphones, auf denen Kommunikation, Portale, Unterhaltung und Nachrichten per Fingertipp verfügbar sind, krönte diese Entwicklung und festigte die Überzeugung, dass IT unser Leben verbessert. Doch stimmt das noch?

Selbst wenn man verödende Innenstädte, erhöhtes Verkehrsaufkommen durch individuelle Warentransporte, die Verlagerung von „Tippdiensten" (Stichwort Grundsteuer) auf die Bevölkerung und den Energieverbrauch von IT-Geräten (inzwischen fast 30% des Strombedarfs) als unvermeidliche Nebeneffekte hinnimmt, macht uns die Digitalisierung zunehmend das Leben schwer. Wer sich durch eine Telefon-Hotline „durchgeklickt", seine Steuererklärung mit digitalen Rechnungen gemacht, einen Smartphone-Modellwechsel durchgezogen, versucht hat, an einer Kasse mit leerem Handy-Akku zu bezahlen oder sich gerade wieder beim Online-Banking per Transaktion neu authentifizieren muss, obwohl er erst am Vortag eine Überweisung getätigt hat, kann davon ein Lied singen.

Dabei ist ein großer Teil der Komplexität hausgemacht. Das gilt nicht zuletzt für Schutzmechanismen – in sehr vielen Fällen sind Authentifikationen überflüssig, in anderen Fällen ließen sie sich durch Nutzung der 2021 eingeführten eID-Funktion des Personalausweises vereinfachen. Und: Im Biergarten kann man nach wie vor sicher und anonym mit Bargeld bezahlen. Solange man noch einen Geldautomaten findet.

Security News

Cloud Supply Chain Security

Ein Satz wie „Der Angriff erfolgte ausschließlich auf den Dienstleister" (Kommentar der Barmer Ersatzkasse vom 17.06.2023 nach einem Hackerangriff auf den Dienstleister des Bonussystems) ist für Kunden keine Beruhigung. Vor allem: Ein Unternehmen wird die Verantwortung für die Datenverarbeitung durch die Verlagerung in die Cloud nicht los – häufig aber den Überblick.

Am 01.06.2023 veröffentlichte TeleTrusT einen Leitfaden zum Thema Cloud Supply Chain Security, der

kompakt zusammenfasst, worauf es beim Einsatz von Cloud-Lösungen in der Supply Chain ankommt. Durch Maßnahmen wie „SBOM“ (*Software Bill of Materials*) erfahren Auftraggeber, welche konkreten Frameworks und Software-Komponenten in den gebuchten Cloud-Diensten zum Einsatz kommen. Damit kann für die genutzten Cloud-Dienste im Incident Handling ein temporäres Abschalten bei der Identifikation ungepatchter Software-Komponenten vorgesehen werden.

Harmonie

Am 24.05.2023 hat der europäische Datenschutzausschuss (EDPB) die fast 50-seitigen Richtlinien zur einheitlichen Bemessung von Bußgeldern bei Verstößen gegen die DSGVO nach einjähriger öffentlicher Kommentierungsmöglichkeit (SSN 5/2022) verabschiedet. Das Vorgehen umfasst fünf Schritte von der Identifizierung bis zur finalen Bewertung. Besonders relevant für die Bußgeldhöhe ist die Festlegung des Ausgangspunktes. Dazu werden die Schwere (bezogen auf den Einzelfall), die Art und die Dauer des Verstoßes sowie die maximale Bußgeldhöhe herangezogen, die vom Umsatz des Unternehmens bestimmt wird. Erscheint der Verstoß schwerer als gleichartige Verstöße, soll das Bußgeld höher ausfallen. Bewertet wird auch das Verhalten des Verantwortlichen in Vergangenheit und Gegenwart; je nachdem erhöht oder vermindert sich das Bußgeld.

Die Richtlinien schaffen durch viele Beispielfälle mehr Transparenz bei der Bemessung von Bußgeldern. Sie liefern allerdings keine mathematische Formel, nach der Verantwortliche das Bußgeld berechnen könnten. Der Ermessenspielraum der einzelnen Aufsichtsbehörden bleibt trotz aller Vereinheitlichung erhalten – und das ist auch gut so.

Don´t roll your own crypto

Sichere Verschlüsselung ist schwierig umzusetzen. Schwachstellen können über fehlerhaft entworfene Protokolle (SSN 12/2022) oder auch schwache Komponenten, wie beispielsweise Zufallszahlen-generatoren (SSN 03/2023) entstehen.

Am 13.06.2023 veröffentlichten Forscher der Universität des Negev in Israel einen Seitenkanalangriff, der in der Lage ist, einen geheimen Schlüssel von einem Smartphone oder aus einer Smartcard auszulesen. Dafür wurde eine Variante der „Poweranalysis“ verwendet, bei der der Stromverbrauch des Prozessors während einer Krypto-Operation zeitlich hoch aufgelöst aufgezeichnet und daraus der geheime Schlüssel abgeleitet wird.

Die Besonderheit bei dem neuen Angriff: Der Stromverbrauch des Prozessors wurde aus dem Flackern der Power-LED des Smartcard-Lesers bestimmt. Dafür war keine spezielle Kamera nötig: Der Angriff wurden mit einem handelsüblichen iPhone 13 durchgeführt. Das Geheimnis: Beim technisch bedingten „Rolling-Shutter“ wird das Bild zeilenweise ausgelesen – die Zeilen des Bildes entstehen daher nicht zeitgleich. Füllt das Licht der Power-LED das gesamte Bild, so liefert jede Zeile eines Bildes Informationen über einen anderen Zeitpunkt. Wird durch den „Rolling-Shutter“ das

einzelne Bild beispielsweise in 1000 Schritten ausgelesen, so kann aus einem Video mit 60 Bildern pro Sekunde eine Messreihe mit 60.000 Messpunkten pro Sekunde abgeleitet werden. Diese Auflösung ist für eine „Poweranalysis" ausreichend. Allerdings benötigt der Angriff gut eine Stunde Videomaterial mit kontinuierlichen Krypto-Operationen, was einen realen Angriff mit dieser Methode stark erschwert. Der Angriff zeigt aber wieder einmal, dass (wie McGraw und Vega schon vor über 20 Jahren aufzeigten) bei der Implementierung von Kryptoverfahren viel schief gehen kann – auch an unerwarteten Stellen.

Verpfiffen

Der deutsche Gesetzgeber hat mit Verspätung zum 31.05.2023 das deutsche Hinweisgeberschutzgesetz beschlossen. Es tritt am 02.07.2023 in Kraft und beinhaltet für Unternehmen ab 50 Mitarbeitern die Pflicht, eine interne Meldestelle einzurichten. Unternehmen ab 250 Mitarbeiter müssen die Meldestelle mit Inkrafttreten errichtet haben; für kleinere Unternehmen gilt eine Umsetzungsfrist bis zum 17.12.2023.

In ihrer Orientierungshilfe zu Whistleblowing-Hotlines vom 14.11.2018 haben die Datenschutzaufsichtsbehörden darauf hingewiesen, dass die Meldungen von Hinweisgebern auch für die durch den Hinweis belasteten Personen ein hohes Risiko für deren Rechte und Freiheiten darstellen. Deshalb verlangen sie zu Recht die Durchführung einer Datenschutz-Folgenabschätzung vor der Einführung von technischen Systemen zur Umsetzung der Meldestellenpflicht. Auch müssen die Mitarbeiter über etwaige Datenverarbeitungen informiert werden.

Wer dies vermeiden möchte, kann die Meldestelle bei einer Anwaltskanzlei einrichten – das spart nicht nur die Kosten für ein hoffentlich selten eingesetztes System, sondern auch dessen Pflege und Wartung.

Brute-Force-Biometrie-Attacke

Am 18.05.2023 veröffentlichten zwei chinesische Forscher einen BrutePrint getauften neuen Angriff auf die Fingerabdruck-Erkennung diverser Smartphone-Modelle. Anders als die meisten derartigen Angriffe versucht BrutePrint jedoch nicht, den Fingerabdruck zu fälschen: Die Forscher hängen nach Öffnen des Gehäuses ein eigenes Gerät in die SPI-Bus-Verbindung vom Fingerabdrucksensor zum Smartphone – ähnlich einem Hardware-Keylogger, der in die Tastaturleitung eingeschleift wird. Darüber kann der Angreifer übertragene Fingerabdruck-Samples mitlesen oder als Man-in-the-Middle eigene einspielen und durchprobieren. Daher auch der Name des Angriffs: *Brute*-Force-Finger-*Print*. Unter den getesteten Smartphones waren nur die (noch mit Touch-ID ausgestatteten) iPhones weitgehend resistent gegen den Angriff, da Apple als einziger Hersteller die SPI-Bus-Verbindung kryptographisch sichert.

Zwar haben alle Geräte einen Fehlbedienungszähler, der nach mehreren falschen Fingerpints eine Pause erzwingen soll, um Angreifer auszubremsen. Aber sogar bei iPhones war es möglich, den Vorgang über den SPI-Bus abzubrechen, bevor der Fehlbedienungszähler erhöht wird. Bei vielen Geräten war außerdem während

der erzwungenen Pause zwar keine Anmeldung möglich, aber eingespielte Fingerabrücke wurden dennoch weiterhin ungebremst geprüft. Ein Lehrbeispiel dafür, wie man biometrische Sensoren nicht integrieren sollte.

Trau keinem Trust-Center

Zur einfachen Beantragung und automatisierten Erneuerung von TLS-Serverzertifikaten wird das ACME-Protokoll (zu Recht) immer populärer. Dabei verbindet sich ein ACME-Client (wie Certbot oder acme.sh) mit dem Trust-Center, das die Zertifikate ausstellt. Allerdings sollte sich das Vertrauen in das Trust-Center nur auf die ausgestellten Zertifikate und Sperrinformation beziehen, wie der am 08.06.2023 bekannt gewordene Vorfall bei einem chinesischen Trust-Center zeigt: Der Betreiber hatte eine unbekannte Remote-Code-Injection-Schwachstelle in acme.sh ausgenutzt, um während des Zertifikats-Enrollments zusätzliche Kommandos auf dem beantragenden Server auszuführen.

Zwar wurde schon am 09.06.2023 eine korrigierte Version von acme.sh veröffentlicht, aber da amce.sh manchmal auch in die Firmware von Appliances, Firewalls o. ä. integriert ist, kann es eine Weile dauern, bis nur noch gefixte Versionen im Einsatz sind. Eine Vorsichtsmaßnahme wäre, auf betroffenen Appliances ACME temporär zu deaktivieren und in den sauren Apfel des manuellen Enrollments zu beißen. Dann muss sich auch der Betreiber der chinesischen CA etwas Neues ausdenken...

Secorvo News

Aus dem Secorvo-Team

Mit Jochen Schlichting hat seit Juni ein weiteres Mitglied unseres Beratungsteams als „ISO/IEC 27001:2022 Lead Auditor" die Lizenz zum Prüfen. Und seit Anfang Juli unterstützt uns unser neuer Kollege Paul Blenderman mit seiner über 20-jährigen Erfahrung mit IT-Sicherheit in Produktionsumgebungen. Willkommen im Secorvo-Team!

Seminare nach der Sommerpause

Bevor Sie Ihre Urlaubskoffer packen, werfen Sie doch noch einen Blick in unser Seminarangebot für das 2. Halbjahr. Wir starten mit unserem T.I.S.P.-Seminar vom **18. bis 22.09.2023** in den Herbst – noch gibt es freie Plätze.

Das Seminar IT-Security-Insights (**26.–27.09.2023**) aktualisiert Ihren Wissenstand zur Informationssicherheit. Wer sich mit Public-Key Infrastrukturen auskennen möchte, ist bei unserem PKI-Seminar (**09.–12.10.2023**) genau richtig. Und mit der Teilnahme am BSI-Seminar (**17.–19.10.2023**) bereiten Sie sich auf die Zertifizierung zum BSI-Vorfall-Experten vor. Wir freuen uns auf Ihre Anmeldung.

13. Tag der IT-Sicherheit

Endlich wieder im bewährten Format: Der 13. Tag der IT-Sicherheit findet am **20.07.2023 ab 14 Uhr** im Saal Baden der IHK Karlsruhe statt. Es erwarten Sie Fachvorträge zur Bedrohung durch Quanten-

computer, den Herausforderungen durch die gestiegene Leistungsfähigkeit von KIs und zum Patchmanagement – sowie ein intensives Buffet-Networking. Hier geht's zum vollständigen Programm und zur Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2023	
10.-15.07.	PETS 2023 (Université de Lausanne, Lausanne/CH)
20.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL, Karlsruhe)
August 2023	
05.-10.08.	Blackhat USA 2023 (Blackhat, Las Vegas/US)
06.-08.08.	SOUPS 2023 (usenix, Anaheim/US)
09.-11.08.	32nd USENIX Security Symposium (usenix, Anaheim/US)
10.-13.08.	DEF CON 31 (DEFCON, Las Vegas/US)
19.-24.08.	Crypto 2023 (Santa Barbara/US)
September 2023	
11.-13.09.	heise devSec 2023 (dpunt.verlag, heise, Karlsruhe)
18.-22.09.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-27.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
27.-29.09.	Informatik 2023 (GI, Hamburg)

Fundsache

Das Bayerische Landesamt für Datenschutzaufsicht hat sich der vom EDSA angekündigten Prüfaktion zu Stellung und Aufgaben von Datenschutzbeauftragten angeschlossen. Die Fragen zur Prüfung kann man u. a. bei IITR Datenschutz GmbH herunterladen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

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