Secorvo Security News

Juni 2024

Impertinent

Die Vertraulichkeit der Kommunikation ist ein seit Jahrhunderten umstrittenes Grundrecht. Die Möglichkeit vermeintlich geschützte Nachrichten heimlich mitzulesen brachte eine Königin aufs Schafott, die USA in den ersten Weltkrieg und 1943 die Entscheidung im U-Boot-Krieg. Nach dem Scheitern des Clipper Chip unter Clinton 1996 und dem vergeblichen Versuch der Nachrichtendienste, die Exportverbote für Verschlüsselungslösungen ins neue Jahrtausend zu retten, verlegte sich die NSA aufs Tricksen und Täuschen, wie Edward Snowden 2013 nachwies – von der Analyse des transatlantischen Datenverkehrs bis zum Einbau von Hintertüren in Router und standardisierte Verschlüsselungsverfahren.

Doch starke Verschlüsselung verbreitet sich: Technisch ist sie in vielen Bereichen inzwischen Standard. Terrorismusbekämpfern und Strafverfolgern ist das ein Dorn im Auge: Online-Durchsuchungen sind nur in seltenen Ausnahmefällen zulässig, die Technik der IMSI-Catcher funktioniert nicht in 5G- und 6G-Netzen und die umstrittene Chat-Kontrolle der EU ließ sich bisher nicht durchsetzen.

In einem am 10.06.2024 publizierten 56-seitigen „First Report On Encryption" der EU-Bedarfsträger werden nun die Herausforderungen zunehmender Verschlüsselung für die Arbeit von Ermittlungsbehörden beschworen, die nach Ansicht der Autoren regulative Eingriffe zur Verhinderung unumgehbarer Verschlüsselung erfordern.

Wie so oft wird dabei behauptet, es gehe um das Spannungsverhältnis von „privacy of individuals and collective security" – was suggeriert, dass hier Individualwohl mit Gemeinwohl kollidiert.

Tatsächlich ist es umgekehrt: Für eine technische Möglichkeit zur Aufklärung von Straftaten, deren Wirksamkeit bis heute nicht nachgewiesen ist, soll das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme der gesamten Gesellschaft beschränkt werden – eine Posse.

Security News

Und wieder die Supply Chain

Am 25.06.2024 warnte Sansec, dass die vom Web-Team der Financial Times im Oktober 2014 initiierte Open-Source-Bibliothek polyfill.io (zur Unterstützung neuer JavaScript APIs in älteren Browsern) Malware verteilt. Die Domäne und das Github Repository der von einer mindestens sechsstelligen Anzahl Hosts genutzten Bibliothek hatte der chinesische Content-Delivery-Network-Betreiber (CDN) Funnull im Februar

2024 erworben. Daher riet der ursprüngliche Autor Andrew Betts schon am 24.02. 2024 dringend davon ab, sie noch zu verwenden.

Der Registrar Namecheap, bei dem Polyfill.io registriert war, hat nach dem Bekanntwerden des Angriffs die DNS-Einträge gelöscht. Webseitenanbieter können auf alternative Implementierungen der CDNs Cloudflare oder Fastly zurückgreifen; Cloudflare ersetzt gefährliche polyfill.io-Links automatisch durch Links auf die eigene Implementierung. In Browsern kann der Adblocker uBlockOrigin helfen; bei ihm sind die betroffenen URLs in den Blocklisten enthalten.

Schutz vor derartigen Supply-Chain-Angriffen kann Subresource Integrity bieten: Damit erkennen Browser manipulierte Bibliotheken am Hashwert. In diesem Fall ist es allerdings nicht praktikabel, da Polyfill für jeden Useragent individuell zusammengestellt wird. Schon im September 2017 berichteten wir über solche Supply-Chain-Angriffe, die sich seitdem angesichts der zunehmenden Nutzung fremder Bibliotheken wachsender Beliebtheit bei Angreifern mit Zeit und Ressourcen erfreuen – höchste Zeit also, dass sich Unternehmen mit sicherer Software-Entwicklung beschäftigten.

Maskerade

Moderne Malware installiert sich häufig nicht, wenn sie Sandboxen oder Analysesoftware entdeckt – beides Hinweise auf Systeme von Sicherheitsforschern. Das Windows-Tool Cyber Scarecrow nutzt diese Eigenschaft, um Malware abzuschrecken, indem es ein Analysesystem vortäuscht. Der Code ist allerdings nicht offengelegt und die Autoren verraten von sich nur, dass sie „cybersecurity researcher living in UK“ seien.

Die Idee ist nicht neu: Auch das schon ein wenig in die Jahre gekommene Fake-Sandbox-Artifacts (April 2020) simuliert eine virtualisierte Umgebung. Im Unterschied zu Cyber Scarecrow ist es jedoch Open Source.

Leider ist der Nutzen solcher Tools eher gering: 2019 schätzte Symantec den Anteil an Malware, die virtuelle Maschinen erkennt, auf 15-20%. Zudem verwenden die meisten dieser Malware-Varianten ein schwer zu täuschendes Fingerprinting. Und schließlich würde eine Verbreitung solcher Tools sehr bald dazu führen, dass Malware ihrerseits die Maskerade entlarvt.

Gefunden im Netz

Das LAG Düsseldorf hat am 10.04.2024 entschieden, dass Arbeitgeber Bewerber informieren müssen, wenn sie potentielle neue Mitarbeiter „googeln“ und die daraus gewonnenen Erkenntnisse im Bewerbungsprozess nutzen. Wird er nicht darüber informiert, kann der Bewerber Anspruch auf eine Entschädigung nach Art. 82 DSGVO fordern. Unternehmen sollten daher ihre Datenschutzinformationen für Bewerber um den Hinweis ergänzen, dass sie Informationen, die im Internet und in sozialen Netzwerken zu finden sind, im Rahmen des Bewerbungsprozesses nutzen. Rechtsgrundlage dieser Verarbeitung ist Art. 6 Abs. 1 b) DSGVO.

Apple setzt Privacy-Maßstäbe

Apple hat auf der Entwicklerkonferenz WWDC am 10.06.2024 „Private Cloud Compute“ vorgestellt – Apples Confidential Computing zur Auswertung von AI-Modellen in der Cloud, quasi als Koprozessor für das iPhone.

Dabei soll die Privatsphäre der Anwender geschützt werden. Kern der Umsetzung sind Rechenknoten, die Apple-eigene Hardware mit einem angepassten Apple-Betriebssystem verwenden und Sicherheitstechnologien wie Secure Boot, Secure Enclave, Code Signing, remote Attestation und Sandboxing nutzen. Nutzeranfragen werden bei der Übertragung zum Knoten Ende-zu-Ende verschlüsselt, in der Secure Enclave verarbeitet und dann gelöscht.

Netzwerkseitig werden Metadaten minimiert; die Autorisierung verwendet Blind Signatures. Mit Oblivious HTTP werden IP-Adressen versteckt. Die Software der Knoten soll veröffentlicht werden; Endgeräte senden ihre Anfragen nur an Knoten, die eine veröffentlichte Version der Software ausführen und gültige Zertifikate besitzen. Forscher, die die Sicherheitsversprechen prüfen und Fehler finden, belohnt Apple im Rahmen des Bug-Bounty-Programms.

Apple setzt damit Maßstäbe für Privacy by Design. Zwar „erkundet“ OpenAI Vergleichbares, bietet AWS mit AWS Nitro eine Plattform, die ähnliche Anwendungen ermöglichen könnte und setzt Azure sogar auf Hardwareunterstützung durch Nvidia Confidential Computing – es ist aber nicht bekannt, dass ein AI-Betreiber diese Technologie bereits einsetzt.

Der Sicherheitsforscher Matthew Green fasst es so zusammen: „Indeed, if you gave an excellent team a huge pile of money and told them to build the best ‘private’ cloud in the world, it would probably look like this.“

Hersteller, die AI-Funktionen in ihre Software integrieren, möchten ihre AI-Modelle zunehmend auf den Geräten der Nutzer auswerten. Die von Apple eingesetzten Techniken können auch helfen, die AI-Modelle auf diesen Endgeräten zu schützen.

Sprachdisharmonie

Eines der Ziele der EU ist die Harmonisierung des europäischen Rechts. Häufig ist dabei jedoch die Sprachvielfalt eine Hürde. So veröffentlichte der Europäische Datenschutzausschuss am 17.05.2024 eine Orientierungshilfe für kleine und mittlere Unternehmen zum Datenschutz in deutscher Sprache. Eine gute Sache, würden darin nicht sprachliche Fehler den EU-Bürgern gänzlich neue Rechte verschaffen: das „Recht auf Information“ (Art. 13) und das „Recht auf Zugang“ (Art. 15). Wer die offizielle deutsche Fassung der DSGVO zur Hand nimmt, wird darin beides vergeblich suchen. Höchstwahrscheinlich wurde hier die englische Fassung (mittels Maschine?) fehlerhaft übersetzt.

Übersetzungsfehler finden sich nicht nur in abgeleiteten Dokumenten, sondern sogar in den Gesetzestexten selbst, wie beispielsweise in der NIS-2-Richtlinie: „Human resources security“ (Art. 21 i) hat mit der „Sicherheit des Personals“ wenig zu tun.

Um Fehlinterpretationen zu vermeiden sollte man sich daher bei juristischen Texten nicht auf automatische (z. B. KI-gestützte) Übersetzungen verlassen, sondern kritisch prüfen, was im Originaltext steht und überlegen, worauf der Gesetzgeber abzielen wollte.

Kein Anschluss unter dieser Nummer

Nicht selten werden bei Tiefbauarbeiten Telekommunikationskabel beschädigt. Sind davon Gerichte betroffen, wie am 26.06.2024 das Bundesverfassungsgericht, können Verfahrensbeteiligte es nicht mehr per Fax erreichen und sind auf den Postweg angewiesen. Die Einführung der digitalen Verfassungsbeschwerde zum 01.08.2024 dürfte das Problem etwas entschärfen. Zwar wirkt eine „Wiedereinsetzung in den vorigen Stand" fristwahrend (§ 93 Abs. 4 BVerfGG); zu Entscheidungsverzögerungen in Eilverfahren könnte es bei einem Verbindungsausfall jedoch auch bei digitalen Einreichungen kommen – mit ggf. unangenehmen Folgen für die Beschwerdeführer.

Redundante Standortanbindungen, die zwei Faserpaare oder Kabel in derselben Trasse verwenden oder vom gleichen Provider versorgt werden, beseitigen das Risiko jedoch nicht. Da viele Provider zudem die Infrastruktur der Deutschen Telekom verwenden, ist eine echte Risikostreuung gar nicht einfach. Vor Gericht und auf hoher See ist man eben auch IT-technisch in Gottes Hand.

Secorvo News

Wissen ist Macht

Buchen Sie sich neben Ihrem wohlverdienten Urlaub doch noch schnell Ihre Weiterbildung für das 2. Halbjahr 2024. Nach der Sommerpause können Sie sich mit unseren kompakten IT Security Insights vom **10.** bis **11.09.2024** in der Informationssicherheit und im Datenschutz updaten. Auf das T.I.S.P.-Zertifikat bereiten wir Sie vom **23.** bis **27.09.2024** vor. Und im November machen wir Sie vom **25.** bis **28.11.2024** zum Experten in sicherer Software-Entwicklung. Wir freuen uns auf Ihre Anmeldung.

14. Tag der IT-Sicherheit

Am **18.07.2024** bietet Ihnen der Karlsruher Tag der IT-Sicherheit zum 14. Mal die Möglichkeit, sich über aktuelle IT-Sicherheitsthemen wie AI oder NIS2 und Präventionsmaßnahmen für Unternehmen zu informieren. Die Keynote hält Ralf Wigand, National Security and IT-Compliance Officer von Microsoft Deutschland. Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Hier finden Sie das Programm und die Möglichkeit zur Anmeldung.

Wer die Wahl hat...

Beim nächsten KA-IT-Si-Event am **19.09.2024** gibt Prof. Melanie Volkamer (KIT) einen Überblick zu den Sicherheitsherausforderungen bei Internet-Wahlen und -Abstimmungen. Anschließend erwartet Sie der beliebte Erfahrungsaustausch beim „Buffet-Networking".

Merken Sie sich den Termin schon vor, der Sommer vergeht schneller als man denkt... Wir freuen uns auf Sie – und empfehlen Ihnen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2024	
15.-20.07.	PETS 2024 (University of Bristol, Bristol/UK)
18.07.	14. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, KASTEL, Karlsruhe)
August 2024	
03.-08.08.	Black Hat USA 2024 (Black Hat, Las Vegas/US)
08.-11.08.	DEFCON 32 (Las Vegas/US)
11.-13.08.	SOUPS 2024 (usenix, Philadelphia/US)
14.-18.08.	33rd USENIX Security Symposium (usenix, Philadelphia/US)
18.-22.08.	Crypto2024 (IACR, Santa Barbara/US)
September 2024	
10.-11.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
19.09.	KA-IT-Si-Event "Wer die Wahl hat..." (KA-IT-Si, Karlsruhe)
23.-27.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
25.-26.09.	heise devSec 2024 (dpunkt.verlag, heise, Köln)

Fundsache

Als Hilfestellung für Beschwerden zum EU-US Data Privacy Framework hat die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Formulare bereitgestellt.

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