Secorvo Security News

Dezember 2024

Gotcha

Einer Kleinen Anfrage im Bundestag und Recherchen von netzpolitik.org ist die Information zu verdanken, dass mit dem Gesichtserkennungssystem des Bundeskriminalamts (BKA) jährlich rund 3.500 Personen identifiziert werden. Referenzbilder von 5 Mio. Menschen seien in der Datenbank des Systems erfasst; Jahr für Jahr kämen rund 10% hinzu. Bemerkenswert ist offenbar die Erkennungsrate des KI-unterstützten BKA-Systems, bei dem eine menschliche „Endkontrolle" inzwischen verzichtbar sei.

Nun mag man der Strafverfolgung leistungsfähige Erkennungssysteme zubilligen. Doch ist die Technik inzwischen allgemein zugänglich – z. B. über das polnische Unternehmen pimEyes (SSN 7/2020), das ein hochgeladenes Bild mit über 1 Mrd. aus dem Internet gesammelten Personenfotos vergleicht. Wie sich darüber ein privates Erkennungssystem konstruieren lässt, demonstrierten die Harvard-Studenten AnhPhu Nguyen und Caine Ardayfio am 02.10.2024 in einem Youtube-Video: Ihr Projekt I-XRAY nutzt die verborgene Kamera einer Ray-Ban Meta-Brille, um (sprachgesteuert) Fotos von beliebigen Personen mit Bildern aus dem Internet zu vergleichen und über die zugehörigen Webseiten deren Namen, Adressen und Telefonnummern zu finden. Auf dem Smartphone werden dann die Kontaktdaten und alle zu der Person gefundenen Webseiten angezeigt – innerhalb von Sekunden.

Noch vor wenigen Jahren war unser Name das Identifikationsmerkmal: Wer ihn kannte, konnte auf Informationen über uns zugreifen, die wir (in der Regel willentlich) online verfügbar gemacht hatten. Niemand musste aber damit rechnen, auf der Straße erkannt zu werden. Das änderte Google mit der Bildersuche. Dank biometrischer Erkennungsverfahren genügt heute ein Foto, um alles Veröffentlichte über uns zu erfahren. Und vielleicht bald schon ein einziger gesprochener Satz. On the internet, everybody knows you're a dog.

Security News

Unsichere Anker

Das Domain Name System (DNS) ist einer der wichtigsten Vertrauensanker des Internet. Daher wurde vor 25 Jahren DNSSEC entwickelt und 2005 als RFC 4033-4035 standardisiert: Damit wird die Richtigkeit der Angaben mit digitalen Signaturen bestätigt.

Viele Registrare und DNS-Provider unterstützen den Standard allerdings bis heute nicht. In seiner am 28.11.2024 veröffentlichten Bachelorarbeit analysierte Felix Wotschofsky von der Berliner CODE University die Verbreitung von DNSSEC: Lediglich 6% der von ihm untersuchten 171 Millionen Domänen nutzen es; Dänemark und Schweden sind mit über 60% rühmliche

Ausnahmen. Dabei überprüfen allein in Deutschland über 80% der DNS-Resolver DNSSEC-Signaturen – sofern vorhanden. Zumindest in Deutschland wäre die Vertrauenswürdigkeit von DNS-Auskünften daher leicht zu erreichen.

Leicht zugängliche Firewalls

Selbst IT-Administratoren neigen zu der Annahme, dass bei besonders sicherheitsrelevanter Software auch deren Qualität entsprechend hoch ist. Dieses Vertrauen ist leider häufig unberechtigt, wie aktuelle Berichte über gravierende Schwachstellen in den Firewalls von Fortinet (15.10.2024) und Palo Alto (19.11.2024) zeigen. Bei der US-amerikanischen Cyber Defense Agency CISA kann man nachlesen, dass Angreifer diese Schwachstellen bereits ausnutzen (27.12.2024).

Den Zugriff auf administrative Zugänge – insbesondere den von Firewalls – sollte man immer durch besonders starke Authentifikationsmechanismen schützen und auf Systeme im internen Netz beschränken. Suchmaschinen wie Shodan oder CriminalIP zeigen, dass solche elementaren Schutzmaßnahmen häufig nicht ergriffen werden – und damit die Ausnutzbarkeit von Schwachstellen auch noch fahrlässig erleichtert wird.

Auch andere goldene Regeln werden bei Firewalls regelmäßig verletzt: Dienste wie E-Mail-Filterung oder VPN-Gateways gehören nicht auf die Firewall, sondern auf ein separates System in der DMZ. Wer auf einer Firewall zusätzliche Dienste betreibt, vergrößert unvermeidlich die Angriffsfläche – und damit die Wahrscheinlichkeit eines erfolgreichen Angriffs. Wie bei allen kritischen Systemen gilt auch hier das KISS-Prinzip: Keep it simple and stupid.

Ross Andersons Vermächtnis

Am 03.11.2024 teilte ein Mitarbeiter des im März 2024 viel zu früh verstorbenen Ross Anderson mit, dass nun auch die dritte Auflage des Standardwerks "Security Engineering – A guide to building dependable distributed Systems" als PDF frei zum Download verfügbar ist. Wir nutzen die Gelegenheit, um dieses hervorragende Grundlagenwerk wärmstens zur Lektüre zu empfehlen.

Ausgeschaltete Geräte aufspüren

Mit Googles "Find-My-Device"-Netzwerk (FMD) können sogar ausgeschaltete Android-Geräte geortet werden, sofern sich der Bluetooth-Chip nach dem Ausschalten als Beacon verhält – wie bei den aktuellen Pixel-Modellen. Eine am 13.02.2024 in Android eingeführte Schnittstelle ermöglicht es, beim Herunterfahren berechnete Ephemeral Identifier (EIDs) in den Bluetooth-Chip zu laden. Empfangen andere Android-Geräte diese EIDs, senden sie ihren damit verschlüsselten Standort an Google. Nur der Besitzer des Geräts kann diese Daten entschlüsseln und so sein Gerät orten.

Zum Schutz der Privatsphäre aller Beteiligten kommen verschiedene Techniken zum Einsatz: Befindet man sich an seiner hinterlegten „Zu-Hause"-Adresse, sendet Android keine Standortdaten. Außerdem werden

mehrere Standorte aggregiert, sodass die Standorte einzelner Netzwerkteilnehmer nicht bekannt werden. Durch Rate-Limiting soll die missbräuchliche Nutzung zur Personenverfolgung in Echtzeit ausgeschlossen werden. Außerdem kann die Funktion deaktiviert werden. Es wird sogar die derzeit noch in der Entwicklung befindliche IETF-Spezifikation zur Erkennung unerwünschter Tracker (dult) unterstützt. Hier hat Google offenbar aus den Erfahrungen Apples mit deren AirTags (SSN 3/2022) gelernt.

Sichere Anker

Am 03.12.2024 erläuterte Senior Product Manager Steven Hosking, warum Microsoft für Windows 11 das Vorhandensein eines Trusted Platform Module (TPM) 2.0 fordert. Zahlreiche spontane Kommentare (allein 630 bei Heise) unterstellen Microsoft, damit den Verkauf neuer Hardware ankurbeln zu wollen – und loben Linux, das sich auch ohne TPM installieren lässt.

Tatsache ist aber: Ohne sichere Hardware gibt es kein sicheres Betriebssystem. Das TPM ist der Vertrauensanker für sicheres Booten und Festplattenverschlüsselung – anwenderfreundlich und mit einem hohen Sicherheitsniveau. Das gilt auch für Linux. Ein TPM bietet außerdem einen sicheren Ablageplatz für Passkeys und ähnliche Anmeldeschlüssel, auch ohne FIDO-Key. Smartphones nutzen ähnliche Vertrauensanker. Kein Wunder, dass Smartphones bisher von Schadsoftwarewellen verschont wurden. Auch dafür benötigen die Betriebssysteme passende Hardwareunterstützung. Im Übrigen: Worüber reden wir eigentlich? TPMs in Version 2.0 werden seit 2017 in nahezu jedem neuen PC verbaut…

Durch Nachbars Garten

Die Forensiker von Volexity berichteten am 22.11.2024 ausführlich, wie russische Hacker in ein Unternehmensnetzwerk eingebrochen sind, indem sie zunächst Computer benachbarter Firmen kaperten. Anschließend nutzten sie deren WLAN, um in das schlecht gesicherte WLAN des Zielunternehmens einzudringen. Volexity taufte diese bisher eher hypothetische Angriffsmethode treffend als „Nearest Neighbour Attack".

Die Annahme, dass ein Angreifer sich in unmittelbarer Nähe eines WLANs aufhalten müsste, um es zu kompromittieren, übersieht diesen Angriffsvektor: Benachbarte Netzwerkinfrastrukturen können von einem Angreifer als Proxy genutzt werden.

Messbare Fortschritte

Am 02.12.2024 veröffentlichte das National Institute of Standards and Technology (NIST) die überarbeiteten Versionen seiner Leitfäden zu Messungen in der Informationssicherheit. Teil 1 der Special Publication SP 800-55 legt den Schwerpunkt auf die Auswahl und Bewertung von Sicherheitsmaßnahmen, Teil 2 behandelt die Integration dieser Messmethoden in ein ISMS. Ziel ist, den Erfolg von Schutzmaßnahmen nicht isoliert zu bestimmen, sondern damit Entscheidungen und das Risikomanagement zu unterstützen.

Die Neuauflagen ersetzen die Versionen von 2008 und berücksichtigen aktuelle Standards wie das NIST Cybersecurity Framework 2.0. Beide bieten wertvolle Anregungen zur Umsetzung eines der meistgescheuten Themen der Informationssicherheit.

Secorvo News

Secorvo Seminare

Werfen Sie doch einen Blick in unseren Seminarkalender, damit Sie Ihre Weiterbildung 2025 nicht aus den Augen verlieren. So bereiten wir Sie im März gerne auf die T.I.S.P.- und die T.P.S.S.E.-Zertifizierung vor.

Programm und Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Wer zahlt die Zeche?

Risiken kann man ignorieren, reduzieren – oder transferieren. Mit der Zunahme erfolgreicher Cyberangriffe steigt daher auch die Nachfrage nach Cyber-Versicherungen. Im Februar 2024 widmete die BaFin diesem Thema sogar einen Fachartikel.

Aber wie das so ist im Leben: Erst im Ernstfall zeigt sich, was eine Vereinbarung wert ist. Denn nicht jeder Vorfall ist automatisch auch ein Versicherungsfall – angesichts der wachsenden Vorfallszahlen und sinkender Margen im Cyber-Versicherungsgeschäft wird aus einem Vorfall schnell ein Streitfall. Welche Fragen dabei zu klären sind und was Versicherungsnehmer schon bei Vertragsabschluss beachten sollten, erläutert anschaulich und spannend an realen Beispielen Dr. Christian Förster (Bartsch Rechtsanwälte) beim Jahresauftakt-Event 2025 der Karlsruher IT-Sicherheitsinitiative am **27.02.2025** um 18:00 Uhr im Saal Baden (IHK Haus der Wirtschaft). Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking".

Wir freuen uns auf Ihr Kommen – und empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2025	
10.-12.01.	ShmooCon 2025 (The Shmoo Group, Washington DC/US)
20.-22.01.	Omnisecure 2025 (in TIME berlin, Berlin)
Februar 2025	
11.-12.02.	32. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
12.-14.02.	IT-Defense 2025 (cirosec, Stuttgart)
19.-20.02.	ID:SMART Workshop 2025 (CAST e.V., Darmstadt)

27.02.	KA-IT-Si-Event „Wer zahlt die Zeche?“ (KA-IT-Si, Karlsruhe)
März 2025	
10.-14.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (heise Medien, Hannover)
24.-27.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2025	
01.-04.04.	DFRWS EU 2025 (DFRWS, Brno/CZW hybrid)
01.-04.04.	Black Hat Asia 2025 (Black Hat, Singapur/ASE)
07.-10.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, 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