Secorvo Security News

März 2022

Warnung

Am 15.03.2022 veröffentlichte das BSI eine Warnung vor dem Einsatz von Kaspersky-Virenschutzprodukten – und löste damit in den IT-Abteilungen vieler Unternehmen und Behörden hektische Betriebsamkeit aus.

Natürlich stimmt das Argument, dass die hohen lokalen Berechtigungen eines Virenschutzprodukts, das zudem regelmäßig große Datenmengen (Signaturdateien) nachlädt, sich für einen (nachrichtendienstlichen) IT-Angriff geradezu anbieten. Nur: Kein Geheimdienst der Welt, der einen solchen Angriff plant, würde damit wochenlang warten – vor „Cyberattacken" aus Russland hatte das BSI bereits im Februar gewarnt.

Die Empfehlung, Kaspersky-Produkte zu ersetzen, greift damit viel zu kurz. Wer solche Angriffe befürchtet, sollte sofort seine gesamte Infrastruktur analysieren – denn wenn sie geplant waren, muss man davon ausgehen, dass bereits Schadsoftware auf diesem Weg installiert wurde. Davon ist in der BSI-Warnung jedoch nichts zu lesen.

Auch ist unverständlich, warum sich die Warnung auf Kaspersky-Produkte beschränkt. Alle relevanten Geheimdienste der Welt bauen seit Jahr(zehnt)en Cybercrime-Abteilungen auf – und warten für ihre Attacken nicht auf einen begleitenden physischen Krieg. Neben Russland sind auch China, Israel und die USA sowohl technisch in der Lage als auch gesetzlich autorisiert, solche Angriffe in „Friedenszeiten" durchzuführen. Wer Kaspersky verbannt, darf auch keine Checkpoint-Firewalls, Huawei-Smartphones, Lenovo-Laptops, Intel-Prozessoren und Cisco-Router einsetzen – und sollte besser auf die Nutzung von Microsoft-Programmen, Apple-Apps und Google-Diensten verzichten.

Nicht möglich, sagen Sie? Richtig. Daher kommt es darauf an, bei der Angriffserkennung seine Hausaufgaben zu machen – damit man im Falle eines solchen Falles wenigstens zügig reagieren kann.

Security News

Behördliche Unterstützung

Am 24.02.2022 veröffentlichte das BSI einen „Maßnahmenkatalog Ransomware", in dem eine Vielzahl von ineinander greifenden Schutzmaßnahmen beschrieben wird. Das erste Kapitel enthält eine Checkliste mit konkreten Prüfpunkten zur Selbsteinschätzung und Beispiele, wie die Anforderungen des Maßnahmenkatalogs zu erfüllen sind.

Das ist wahrscheinlich hilfreich. Wie Behörden aber nicht nur Dokumente erzeugen, sondern auch konkrete Unterstützungsdienste erbringen können, zeigt die amerikanische Cybersecurity & Infrastructure Security Agency (CISA): Sie bietet Organisationen und Regierungseinrichtungen eine Reihe von kostenfreien

Services zum Schutz vor Angriffen. So kann man über das Internet erreichbare Netzbereiche und Webanwendungen einer automatisierten Überprüfung auf typische Schwachstellen unterziehen lassen oder mit dem auf GitHub zum Download bereitgestellten Cyber Security Evaluation Toll (CSET) ein Ransomware Readiness (Self-) Assessment (RRA) durchführen (siehe SSN 7/2021). Diese Angebote ersetzen keinen Penetrationstest, sind aber eine einfache Maßnahme, um offensichtliche Mängel zu identifizieren und abzustellen – und damit ein wichtiger Beitrag zu einer wirkungsvollen Prävention.

Interessenskonflikte des DSB

Am 16.12.2021 verhängte die belgische Datenschutzbehörde aufgrund eines Interessenskonflikts des Datenschutzbeauftragten einer Bank ein Bußgeld von 75.000 €. Der interne Datenschutzbeauftragte war zugleich Leiter von drei Abteilungen, die das operative Risikomanagement, das Informationsrisikomanagement sowie eine Sonderermittlungsstelle umfassten. In seiner Funktion sei er nicht nur beratend oder überwachend tätig geworden, sondern habe aufgrund seiner Befugnisse über die Verarbeitung personenbezogener Daten entscheiden können. Nach Auffassung der belgischen Behörde darf ein Datenschutzbeauftragter keine Position innehaben, die Mittel und Zweck der Verarbeitung von personenbezogenen Daten festlegen kann.

Interessenskonflikte können durch eine sorgfältige Zuweisung von Aufgaben und vertragliche Regelungen vermieden werden. Sobald sich ein Datenschutzbeauftragter selbst überwachen müsste, sind Interessenskonflikte unvermeidbar. Die Entscheidung der belgischen Behörde ist daher nicht überraschend und sollte zum Anlass genommen werden, die sonstigen Aufgaben und Befugnisse des internen Datenschutzbeauftragten zu überprüfen.

Kali Linux 2022

Pünktlich zum Valentinstag kündigte Kali das neue Release „Kali Linux 2022.1“ an. Neben visuellen Änderungen wie einheitlichen BIOS/UEFI Boot-Menus und „professionelleren“ Shell-Prompts ziehen neue Tools in die offiziellen Repositories ein – eine umfangreiche Ergänzung zum bisherigen Toolset und eine Alternative zu gängigen Tools in den Bereichen OSINT, Port- und Schwachstellenscannern sowie Proxies. Zusätzlich wurde das „Kali Everything Image“ als optionaler Download eingeführt, ein Komplettpaket mit allen möglichen vorinstallierten Tools. Für bestimmte Situationen ist dieses Angebot sicherlich nützlich – auch die Hacking-Distribution BlackArch Linux bietet seit 2020 ein derartiges Komplettpaket an. Mit rund der Hälfte der Download-Größe (ca. 9.4 GB) ist das „Kali Everything Image“ eine zumindest platzsparende Alternative zum „Black Arch Full ISO“ (ca. 18 GB).

Data-Act-Entwurf

Die Europäische Kommission hat am 23.02.2022 einen Vorschlag zur Data-Act-Verordnung vorgelegt. Die Verordnung ist Teil einer groß angelegten Datenstrategie der Europäischen Union, die unter Wahrung von Datenschutzstandards und Verbraucherrechten die

branchenübergreifende Nutzung von Daten fördern und die Vormachtstellung großer Konzerne zugunsten von KMUs und vor allem der Nutzer eindämmen soll.

Der Data Act ist bei der Verarbeitung personenbezogener Daten neben der DSGVO anwendbar, sodass Betroffene ihre Rechte aus beiden Verordnungen geltend machen können. Dabei sind die Rechte aus dem Data Act umfassender als die der DSGVO, da Daten nicht nur einmalig, sondern kontinuierlich in Echtzeit zur Verfügung gestellt werden sollen.

Die Zielsetzung des Entwurfs darf als gelungen, die Umsetzung muss aber als nicht ausreichend bewertet werden. Die Regelung des behördlichen Zugriffs ist schwammig und wird als rechtsstaatlich problematisch und als intensiver Eingriff in die Vertragsfreiheit sowie als eine Gefährdung der Wettbewerbsfähigkeit europäischer Unternehmen kritisiert. Auch wenn der Entwurf nachgebessert werden sollte, ist bereits jetzt erkennbar, dass die Auswirkungen der Verordnung auf die Wirtschaft in jedem Fall erheblich sein werden.

#airtagged

Seit dem 30.04.2021 verkauft Apple münzgroße Anhänger („AirTags"), die von Apple-Geräten im Umkreis von 10-50 m via Bluetooth und vom iPhone 11+ auf wenige cm genau geortet werden können. Das funktioniert über beliebige Distanzen weltweit: Entdeckt ein iPhone ein fremdes AirTag, schickt es die Geo-Koordinaten in die iCloud, wo sein Besitzer mit Apples „Find My"-App die Bewegung des AirTags auf einer Karte verfolgen kann. Die Idee ist bestechend: Einfach einen der rund 25 € teuren Anhänger am Hundehalsband, unter dem E-Bike-Sattel oder am Schlüsselbund befestigen, und Suchen ist Finden. Offenbar billigend in Kauf genommen hat Apple, dass sich damit auch fremde Habseligkeiten „markieren" lassen. So wurde z. B. am 15.12.2021 über AirTags berichtet, die an neuen Autos angebracht werden, um sie unbemerkt zu verfolgen – und einen guten Ort für einen Diebstahl abzupassen. Dass AirTags, in einer fremden Hand- oder Jackentasche versenkt, auch zu einem wertvollen Werkzeug für Stalker werden, ist inzwischen ebenfalls bekannt. Unterstützt wird der Missbrauch dadurch, dass die Identifikation des Eigners zu dessen Schutz technisch verhindert wird.

Zwar meldet sich ein AirTag mit einem Ton, wenn es acht bis 24 Stunden keinen Kontakt zum iPhone seines Besitzers hatte – aber das kann überhört oder mit einer einfachen Bohrung ausgeschaltet werden – auch werden inzwischen „Silent AirTags" mit deaktiviertem Lautsprecher angeboten. Die von Apple publizierte App zur Feststellung von längere Zeit in der Nähe befindlichen fremden AirTags warnt nach mehreren Stunden – befindet sich das „Opfer" aber mit Unterbrechungen in der Nähe des AirTags oder besitzt es kein iPhone, funktioniert der Alarm nicht. Offenbar fällt dieser Missbrauch sogar in eine „Strafbarkeitslücke", wie Lena Leffer und Michelle Weber in der DuD 3/2022 nachweisen.

Am 21.02.2022 veröffentlichte Fabian Bräunlein den Code für einen „Stealth AirTag Clone" auf Basis eines ESP32, der alle Schutzfunktionen des „Find My"-Protokolls von Apple umgeht. Und er macht klar, dass nicht

die AirTags das eigentliche Problem sind – sondern die Tracking-Infrastruktur, die Apple mit dem „Find My"-Netzwerk schon vor Jahren etabliert hat.

Signatur als werbefreie Zone

Am 15.09.2021 befand das Kammergericht Berlin den Zusatz in der E-Mail-Signatur eines Unternehmens „[...] Organisiert, denkt mit, erledigt. Nutzen Sie www.[...].de" als unerlaubte Werbung im Sinne des § 7 UWG und gestand dem Kläger einen Unterlassungsanspruch gegen das Unternehmen zu. Der geringe Umfang dieses Zweizeilers und die Positionierung am Ende der Nachricht seien hier unerheblich: „Nach der Rechtsprechung des BGH" könne dieser kleine Zusatz auch nicht durch den vorangestellten, legitimen Inhalt der E-Mail gerechtfertigt werden. Auch diese sehr geringfügige Beeinträchtigung sei generalpräventiv zu untersagen, um ein Um-sich-Greifen solcher Werbung durch Nachahmung zu verhindern.

In welchem Maß und Format Hinweise auf das eigene Unternehmen in der E-Mail-Signatur überhaupt zulässig sind, dazu bietet das rechtskräftige Urteil leider keine Anhaltspunkte. Immerhin sprach das Gericht der Sache eine „grundsätzliche Bedeutung" zu, d. h. das Gericht sieht eine endgültige Klärung durch den Bundesgerichtshof für zumindest wünschenswert an. Bis dahin sollten E-Mail-Signaturen kritisch auf eine mögliche Werbewirkung überprüft werden.

Secorvo News

BSI Vorfall-Experte

Die „Einschläge kommen näher" – daher gewinnt die Vorbereitung auf einen Sicherheitsvorfall als Teil des Sicherheitsmanagements an Bedeutung. Seit dem vergangenen Jahr bietet das BSI eine Zertifizierung zum „Vorfall-Experten" an. Voraussetzung ist die Teilnahme an einer Aufbau-Schulung auf der Grundlage des Leitfadens des BSI zur Reaktion auf IT-Sicherheitsvorfälle.

Die dreitägige Aufbauschulung zum BSI Vorfall-Experten bietet Secorvo erstmals vom **17. bis 19.05.2022** an. Wir freuen uns auf Ihre Anmeldung – natürlich auch zum PKI-Seminar (**25.–28.04.2022**) oder dem Vorbereitungsseminar auf die T.I.S.P.-Zertifizierung (**09.–13.05.2022**).

Wer besitzt mein Smartphone?

Auch wenn wir uns kaum noch daran erinnern können, wie wir ohne sie klarkamen: Smartphones gibt es erst seit 15 Jahren. Genauso alt wie das Smartphone ist die Geschichte der Smartphone Hacks – von den ersten Jailbreaks über die Celebrity Nudes bis hin zu kommerzieller und staatlicher Spyware.

Anhand von Attack Trees und Live-Hacking-Demos zeigen Ihnen Armin Harbrecht und Maximilian Stauß (aramido) beim kommenden KA-IT-Si-Event am **19.05.2022**, wie Smartphones angegriffen werden. Dieses Verständnis ist Voraussetzung für effektive Schutzmaßnahmen. Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – bei schönem

Wetter auf der herrlichen Dachterrasse von aramido (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
07.04.	„Geld oder Leben“ (KA-IT-Si, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)
Mai 2022	
03.-04.05.	Security Forum 2022 (Hagenberger Kreis, Hagenberg/AT)
05.05.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
09.-13.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.-13.05.	Blackhat Asia 2022 (Blackhat, hybrid)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)
10.-11.05.	BvD Verbandstage 2022 (BvD, Berlin)
16.-17.05.	23. Datenschutzkongress (EUROFORUM, Berlin)
16.-18.05.	Entwicklertag 2022 (VKSI, GI, ObjektForum, Karlsruhe)
17.-19.05.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
19.05.	„Wer besitzt mein Smartphone?“ (KA-IT-Si, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Nicolas Blum, Milan Burgdorf, Enes Erdoğan, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

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