secorvo
security consulting

Secorvo Security News

Mai 2021

Zweck verfehlt

Am vergangenen Samstag erhielt ich im Zusammenhang mit einer Erbschaftsangelegenheit ein Schreiben von einem Finanzinstitut, bei dem ich bisher kein Kunde war. Betreff: „Datenschutzhinweise“. Sie ahnen, was beilag: Fünf eng bedruckte Seiten „zur Kenntnisnahme und für Ihre Unterlagen“. Immerhin nur fünf, dachte ich fast erleichtert.

Ähnliche Schreiben wurden seit Inkrafttreten der DSGVO millionenfach versandt. Sie dienen der Erfüllung der Informationspflicht aus Art. 13 DSGVO: Danach müssen Betroffene zu Beginn einer Verarbeitung erfahren, welche personenbezogenen Daten zu welchen Zwecken verarbeitet werden.

Ein wichtiges Prinzip des Datenschutzes: Transparenz. Nur: In dieser Umsetzung degeneriert es zur Farce, zu einer gigantischen Vergeudung von Ressourcen – denn gelesen werden solche Seiten wohl von den wenigsten Empfängern. Das sehen offenbar auch die Absender so: Das Schreiben beginnt mit den Worten „... aufgrund rechtlicher Bestimmungen der Datenschutz-Grundverordnung erhalten Sie ...“. Nicht etwa: „... mit diesem Schreiben möchten wir Sie über die Verarbeitung Ihrer folgenden personenbezogenen Daten informieren.“ Oder gar: „... für die Abwicklung unseres Vertrags müssen wir personenbezogene Daten von Ihnen verarbeiten. Der folgenden tabellarischen Übersicht können Sie entnehmen, zu welchen Zwecken wir welche Angaben erheben – und wann wir sie löschen.“

Darüber hätte ich mich tatsächlich gefreut: Eine übersichtliche Darstellung auf einer Seite, der ich auf einen Blick entnehmen kann, welche Daten konkret erfasst werden – und wann sie wieder aus den Systemen verschwinden. Stattdessen: Reichlich allgemeine Formulierungen über mögliche Verarbeitungen, die dem Art. 13 formal genügen mögen – mich aber weitgehend im Unklaren darüber lassen, welche Daten denn nun konkret von mir verarbeitet werden.

Aber vielleicht weiß das ja auch dort niemand so ganz genau.

Inhalt

secorvo
security consulting

Security News

Fragmentation meets Exploitation

Am 11.05.2021 veröffentlichte das Team um den Sicherheitsforscher Mathy Vanhoef (bekannt von den KRACK- oder Dragonblood-Angriffen) mit FragAttacks eine neue Gruppe von Schwachstellen in Wi-Fi-Netzen. Bei den neuen Schwachstellen handelt es sich um drei Design- sowie diverse Implementierungsfehler. Betroffen sind allen relevanten Wi-Fi-Standards (u. a. WPA2 und WPA3) sowie Geräte zahlreicher Hersteller.

Die Design-Schwachstellen sind schwierig auszunutzen, da sie u. a. die Mitwirkung des Benutzers voraussetzen. Die Lücken in den Implementierungen sind vom praktischen Standpunkt aus schwerwiegender: Sie sind leichter ausnutzbar und erlauben es, Systeme in internen Netzen anzugreifen, ohne die Verschlüsselung brechen zu müssen. Hierzu bedienen sich die Forscher fragmentierter Authentisierungspakete. Der fehlerfreie Umgang mit fragmentierten Daten ist ein komplexes Problem und verursacht immer wieder Schwachpunkte in Kommunikationsprotokollen.

In einem neunmonatigen Disclosure-Prozess wurden die Schwachstellen an die Hersteller kommuniziert. Die meisten Hersteller sind derzeit noch mit der Behebung der Schwachstellen beschäftigt, wobei in vielen Fällen Updates der Firmware notwendig sind. Einzelne Hersteller haben bereits Patches veröffentlicht.

Wer die Angriffe nachvollziehen und eigene Geräte auf Verwundbarkeit testen will, findet entsprechende Tools auf Github. Sofern für eingesetzte Komponenten noch keine Patches verfügbar sind, sollte – bspw. unter Berücksichtigung der Funkausleuchtung – die Relevanz für die eigene Organisation geprüft und entschieden werden, wie man mit der Schwachstelle umgeht. Eine Vorstellung weiterer Details zu den Angriffen ist auf der Konferenz Black Hat USA zu erwarten.

IT-Sicherheitsgesetz 2.0

Am 07.05.2021 hat der Bundesrat den Gesetzesentwurf des Bundestages zur Überarbeitung des IT-Sicherheitsgesetzes angenommen. Nach Veröffentlichung im Bundesgesetzblatt wird das Gesetz aller Kritik zum Trotze in Kraft treten. Neben einigen gravierenden, das BSI betreffenden Änderungen gibt es nun größeren Handlungsbedarf bei den Betreibern Kritischer Infrastrukturen. So werden die Einführung von „Systemen zur Angriffserkennung“ sowie detailliertere Meldungen zur Pflicht und die „Siedlungsabfallentsorgung“ zu einem neuen Sektor der Kritischen Infrastrukturen.

Um in dem Paragrafendschungel den Überblick zu behalten empfehlen wir einen Blick in die Plattform OpenKRITIS, die neben anderem eine gute Übersicht über die Änderungen anbietet.

Auslegungssache

Ist die Übermittlung personenbezogener Daten in Drittstaaten zulässig, wenn die Betroffenen informiert eingewilligt haben oder die Übermittlung zur Erfüllung eines Vertrags erforderlich ist? Art. 49 DSGVO sieht solche Ausnahmetatbestände vor, die jedoch von den Aufsichtsbehörden mit Verweis auf eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) vom 25.05.2018 bislang sehr restriktiv ausgelegt werden.

Im Zweifel ist jedoch immer der Wortlaut des Gesetzes maßgeblich. So sind nach Prof. Thomas von Danwitz, Richter am Europäischen Gerichtshof (EuGH) und Berichterstatter für das „Schrems-II“-Urteil, die Ausnahmeregelungen des Art. 49 DSGVO „noch nicht hinreichend ausgelotet“ (siehe seine Stellungnahme auf dem Europäischen Datenschutztag vom 28.01.2021).

Damit ist Art. 49 DSGVO jedoch kein „Freibrief“ für jede Datenübermittlung: Für jeden Fall, in dem weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, ist die Erforderlichkeit zu prüfen – beispielsweise also, ob keine Dienstleister aus der EU die Verarbeitung übernehmen können.

IT-Grundschutz-Kompendium

Das BSI verkündete am 19.05.2021 im IT-Grundschutz-Newsletter die Veröffentlichung weiterer Umsetzungshinweise zur Edition 2021 des IT-Grundschutz-Kompendiums. Darin wird aufgezeigt, wie die Anforderungen aus dem jeweiligen IT-Grundschutz-Baustein des Kompendiums erfüllt werden können.

Die Ergänzungen betreffen insbesondere die Schicht "IND" (Industrielle IT): IND.1 Prozessleit- und Automatisierungstechnik, IND.2.1 Allgemeine ICS-Komponente, IND.2.2 Speicherprogrammierbare Steuerung (SPS), IND.2.4 Maschine und IND.2.7 Safety Instrumented Systems.

Für die praktische Umsetzung der Bausteine wird die Lektüre der Hinweise wärmstens empfohlen.

Volatility v3

Bereits am 01.02.2021 wurde Volatility, das Standardwerkzeug für die forensische Hauptspeicheranalyse, nach einer eineinhalbjährigen Betaphase in einer stabilen Version 3 (Release V3-1.0.1) auf

GitHub veröffentlicht. In den seither vergangenen Monaten wurden weitere Fehler behoben und die Stabilität der neuen Funktionen verbessert.

Die Grundausstattung an Plugins ist im Vergleich mit der bisherigen Version V2.6.1 allerdings noch deutlich reduziert. So unterstützt Volatility V2.61 allein für Windows 113 Plugins, das Release V3-1.0.1 umfasst lediglich 44. Dennoch empfiehlt sich der Einsatz der neuen Version: Mit der Umstellung auf Python 3 wurden parallele Threads eingeführt, wodurch bisher sehr zeitintensive Plugins wie z. B. „strings" (Mapping von Strings auf Speicheradressen) oder „yarascan" (Prüfung des Hauptspeichers mit YARA-Regeln) wesentlich schneller abgearbeitet werden. Das ersparte z. B. bei der Untersuchung 64-GB-großer Hauptspeicherabzüge von MS Exchange im Kontext des APT-HAFNIUM-Angriffs im März 2021 z. T. mehrstündige Laufzeiten – bei einem akuten, kritischen Angriff ein echter Gewinn für die Verteidiger in den Unternehmen.

Eine weitere wichtige Funktion ist die automatisierte Unterstützung der Generierung spezifischer Windows-Profiles, die sich häufig nach NTOS-Kernel-Subversion unterscheiden. Bisher konnten lediglich Fachleute neue Profile erstellen.

Secorvo News

Live Hacking – Grundlagen von Pentests

Online-Formate können lebendige Seminare mit direktem Erfahrungsaustausch nur begrenzt ersetzen. Dafür haben sie große Stärken bei Demonstrationen und praktischen Übungen: Da bieten sie ein unmittelbareres Erleben und die Möglichkeit zum Training am gewohnten eigenen System.

Der große Erfolg einer Abendveranstaltung zum gleichen Thema im April hat uns daher motiviert, ein Ein-Tages-Online-Mitmach-Seminar für Sie zu entwickeln: In unserem „Live-Hacking-Lab" weisen unsere Penetrationstest-Experten Sie in die Grundlagen der Schwachstellensuche ein. Dabei führen Sie unter unserer Anleitung an realitätsnah konfigurierten, verwundbaren Laborsystemen gängige Methoden zur Identifikation von Schwachstellen praktisch durch – ganz bequem an Ihrem eigenen Arbeitsplatz.

Neben diesem Einblick in die Praxis des „Ethical Hackings" zeigen wir Ihnen die Möglichkeiten und Grenzen von Penetrationstests. Das Schulungskonzept spiegelt die langjährige Erfahrung der Referenten wider – von Praktikern für Praktiker.

Das Seminar bieten wir an am **23.06.2021** und am **14.07.2021**. Programm und Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

KA-IT-Si für alle

Erstmals haben wir in diesem Jahr Veranstaltungen der Karlsruher-IT-Sicherheitsinitiative (KA-IT-Si) in einem Online-Format durchgeführt. Die Resonanz war überwältigend: Mehr als 650 Datenschutz- und Datensicherheitsexperten haben an den bisherigen vier Abendveranstaltungen teilgenommen.

Auch wenn wir so bald wie möglich zu unseren Präsenzveranstaltungen mit lebendigem Buffett-Networking zurückkehren werden: Wir wollen auch zukünftig eine Möglichkeit zur „virtuellen" Teilnahme bieten, nicht zuletzt um die Veranstaltungen bundesweit „besuchbar" zu machen. Wenn Sie interessiert sind, freuen wir uns, wenn Sie sich in den Einladungsverteiler eintragen.

12. Tag der IT-Sicherheit

Auch der jährliche "Karlsruher Tag der IT-Sicherheit", eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V., wird in diesem Jahr als virtuelle Veranstaltung stattfinden, verteilt auf drei Abende. Den Einstieg bildet jeweils ein kurzer Blick in die Forschungs- und Gründerszene der Informationssicherheit, gefolgt von einem vertiefenden Fachvortrag:

1. Abend – Donnerstag, **01.07.2021**, 18 Uhr

10 Jahre Kompetenzzentrum KASTEL – ein Ausblick auf die IT-Sicherheit der Zukunft.
Prof. Dr. Jörn Müller-Quade (KIT)

Aus der Sicht eines Hackers. *Tim Schmidt (KIT)*

2. Abend – Donnerstag, **08.07.2021**, 18 Uhr

Einfach.Sicher.Machen. Transferstelle IT-Sicherheit im Mittelstand. *Stephanie Ziegler (KIS)*

Modernes DNS: Datenschutz mit Nebenwirkungen.
Prof. Dr. Rainer W. Gerling

3. Abend – Donnerstag, **15.07.2021**, 18 Uhr

Elevator Pitch: StartUps IT-Security.
Jun.-Prof. Dr. Christian Wressnegger (Poison Ivy) und *Mirko Ross (asvin)*

Cookies, Tracking, Analysen.
Friederike Schellhas-Mende (Secorvo)

Im Anschluss an die Vorträge bieten wir die Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit den Referenten und anderen Teilnehmern. Wir freuen uns auf drei kurzweilige und interessante Abende mit Ihnen! (Anmeldung)

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2021	
08.06.	Datenschutztag 2021 (COMPUTAS, Berlin)
09.-11.06.	Entwicklertag 2021 (VKSI, GI, ObjektForum , virtuell)
14.-15.06.	DuD 2021 (COMPUTAS, Berlin)
17.-18.06.	Annual Privacy Forum 2021 (ENISA, DG Connect, Católica University of Portugal, virtuell)
23.06.	Live Hacking Lab – Grundlagen Penetrationstest (Secorvo, virtuell)
Juli 2021	
01.07.	12. Tag der IT-Sicherheit, 1. Abend (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
08.07.	12. Tag der IT-Sicherheit, 2. Abend
12.-14.07.	PETS 2021 (University of Minnesota, virtuell)
12.-16.07.	DFRWS USA 2021 (DFRWS, virtuell)
14.07.	Live Hacking Lab – Grundlagen Penetrationstest (Secorvo, virtuell)
15.07.	12. Tag der IT-Sicherheit, 3. Abend
31.07.-05.08.	Blackhat USA 2021 (Blackhat, Las Vegas/US)

Fundsache

Am 15.04.2021 veröffentlichte der LfDI Baden-Württemberg ein Video zum Löschen von Daten samt Musterverzeichnis von Verarbeitungstätigkeiten mit integriertem Löschkonzept. Ein guter Einstieg.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Sarah Niederer, 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