secorvo
security consulting

Secorvo Security News

Februar 2021

Die schlechte gute Nachricht

Der 13.05.2019 dürfte in die Annalen des Heise-Verlags eingegangen sein. An diesem Montag schlug „Emotet“ im Verlagsnetz ein und bewies, dass auch ein technisch kompetentes und sicherheitsbewusstes Unternehmen zum Opfer werden kann. Anders als die meisten Emotet-Geschädigten ging der Verlag an die Öffentlichkeit und berichtete in schonungsloser Offenheit über den Vorfall, die eigenen Fehler und seine „Lessons learned“. Was dabei deutlich wurde: Die Hacker nutzten jeden Fehler und jede noch so kleine Nachlässigkeit, um sich nach ihrem Eindringen im Netz festzusetzen.

2014 hatte „Emotet“ begonnen, seine Trojaner-Infrastruktur zu einer Art „Cloud-Service für Angreifer“ auszubauen. Mit gut gemachten Spear-Phishing-Angriffen, die aus den E-Mails anderer Opfer konstruiert wurden, und bösartigen Makros in angehängten Office-Dateien hatte sich die Gruppe Zugang zu zigtausend IT-Systemen von Privatpersonen, Unternehmen und Behörden verschafft und „vermietete“ die Zugänge an Kriminelle zur Einschleusung von Online-Banking-Malware oder Verschlüsselungstrojanern.

Am 27.01.2021 meldete das Bundeskriminalamt, das seit 2018 gegen Emotet ermittelt hatte, dass es zusammen mit Europol deren Infrastruktur „ausgehoben“ habe. Die Zerschlagung stelle „eine wesentliche Verbesserung der Cybersicherheit in Deutschland dar“. Also „Ende gut, alles gut“? Ist das wirklich so? Seit Anfang Februar wertet das BSI die auf den Emotet-Servern entdeckten Credentials aus, die die Trojaner bei ihren Opfern „eingesammelt“ hatten, und informiert die betroffenen Unternehmen. Dabei zeigt sich, dass das erfolgreiche „Einnisten“ von Emotet in tausenden Unternehmen offenbar nicht einmal bemerkt worden war – zigtausend „Schläfer“-Rechner warteten noch immer auf ihren Einsatz.

Das ist keine gute Nachricht. Denn durch das Ausschalten eines einzelnen Angreifers verbessert sich die Cybersicherheit natürlich nicht. Sondern nur durch einen wirksameren Schutz der IT-Systeme.

Inhalt

secorvo
security consulting

Security News

„Human Supply Chain" Attack

Am 05.02.2021 versuchten Angreifer, in einer Wasseraufbereitungsanlage in Oldsmar (Florida) die chemische Zusammensetzung des Wassers zu verändern. Der Angriff wurde von einem Mitarbeiter erkannt, der die Mauszeigerbewegungen und eine Misstrauen erweckende Veränderung des Natriumhydroxid-Anteils bemerkte. Daraufhin setzte er diesen zurück und meldete den Vorfall. Einem Advisory des Massachusetts Department of Environmental Protection zufolge erfolgte der Angriff über einen TeamViewer-Zugang; drei Tage zuvor hatte es Datenleaks gegeben, die auch Credentials für die Wasseraufbereitungsanlage in Oldsmar enthielten.

Der Vorfall macht deutlich, wie wichtig es ist, dass kritische Industrial Control Systems nicht nur erfahrenes Personal und bspw. Intrusion-Detection-Systeme oder SIEM einsetzen, sondern auf diversitären Architekturen basieren. Eine Infrastruktur, die an verschiedenen Stellen getrennte Systeme verwendet, erlaubt es, gefälschte Werte, die (ähnlich wie bei Stuxnet) über ein kompromittiertes System eingespielt werden, auf Plausibilität zu prüfen und Abweichungen zu erkennen.

Zusätzlich empfehlen wir allen Betreibern kritischer Systeme die Beachtung gängiger Best Practices: So sollten Management-Schnittstellen nicht nach außen exponiert und Remote-Zugänge – falls überhaupt erforderlich – bestmöglich abgesichert werden. Hierzu gehört das Erzwingen starker Authentifizierungsmechanismen bspw. über eine Multi-Faktor-Authentifizierung und die strenge Kontrolle des Ursprungs der Authentifizierungs-Anfrage (Einschränkung auf IP-Bereiche und Geräte). Auch eine bedarfsabhängige Aktivierung des Remote-Zugangs verringert die Angriffsfläche. Passwörter sollten zudem nicht nur stark sein, sondern dürfen auch nicht geteilt werden, da sonst eine Zuordnung zu Benutzern und ein differenziertes Berechtigungsmanagement unmöglich sind.

Troja-X

Das 2019 gestartete europäische Projekt Gaia-X soll eine europäische Dateninfrastruktur der Zukunft entwickeln, die eine europaweite „digitale Souveränität" von Unternehmen und Geschäftsmodellen ermöglicht. Es soll sich an sieben Leitprinzipien ausrichten, zu denen insbesondere der „europäische Datenschutz" und „Offenheit und Transparenz" zählen. Bislang haben sich dem Projekt über 300 Organisationen aus ganz Europa angeschlossen.

Ob das Projekt mehr ist als politisches Marketing muss sich jedoch noch erweisen. So löste am 18.11.2020 eine Mitteilung der Nachrichtenagentur Dow Jones News über die Beteiligung des amerikanischen Big-Data-Unternehmens Palantir, der Cloud-Anbieter Microsoft, Amazon und Google sowie des chinesischen Unternehmens Huawei Diskussionen aus – sollte Gaia-X europäische Unternehmen und Behörden doch gerade von Anbietern unabhängig machen, deren Sicherheits- und Datenschutzniveau aufgrund staatlicher Eingriffsbefugnisse wie dem US-CLOUD Act in Zweifel stehen. Mit zu viel Offenheit wird aus Gaia-X jedenfalls bald ein Troja-X.

Rechtmäßigkeit der Verarbeitung

In einem am 11.01.2021 veröffentlichten Beschluss stellt das Verwaltungsgericht (VG) Wiesbaden fest, dass bei der Bearbeitung eines Löschbegehrens immer „erneut" die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DSGVO zu prüfen sei. Die ist sowohl vor Beginn einer Datenverarbeitung als auch anschließend regelmäßig zu prüfen; dasselbe gilt für die Angemessenheit der festgelegten Löschfrist.

Erreicht eine verantwortliche Stelle ein Löschbegehren, hat sie nach Auffassung des VG zunächst zu prüfen, ob die Voraussetzungen für eine rechtmäßige Datenverarbeitung noch vorliegen – und erst dann, ob diese dem Löschersuchen entgegenstehen. Anderenfalls ist die Verarbeitung ohnehin zu beenden und sind die Daten zu löschen.

Grundschutz-Kompendium 2021

Am 01.02.2021 veröffentlichte das BSI die jährliche Überarbeitung und Erweiterung des IT-Grundschutz-Kompendiums. Auf den ersten Blick überrascht der neue Baustein „INF.11 Allgemeines Fahrzeug". Da moderne Fahrzeuge eher einem Rechenzentrum mit vier Rädern ähneln, ist es jedoch sinnvoll, daran IT-Sicherheitsanforderungen zu stellen.

Nicht in diese Edition geschafft hat es der Baustein „SYS.1.2.3: Windows Server 2019", der bereits als Community Draft vorliegt. Die Verschiebung des Bausteins „APP.6 Allgemeine Software", der bisher auf anderer Ebene (CON.4) angesiedelt war, ist zu begrüßen; daraus ergeben sich Vorteile bei der Modellierung und den Soll-Ist-Vergleichen. Und der ehemalige Katalogbaustein „B 5.25 Allgemeine Anwendungen" hat nun einen Nachfolger; das hilft bei Migrationen.

Wie gewohnt sind alle im Kompendium vorgenommenen Verbesserungen systematisch in einem Änderungsdokument zusammengefasst. Das vereinfacht die Fortschreibung von IT-Sicherheitskonzepten. Fazit: Klasse.

Verzagte Neuregelung

Das Bundeskabinett beschloss am 10.02.2021 nach Eingang von 31 Stellungnahmen einen Entwurf für ein „Gesetz zur Regelung des Datenschutzes [...] in der Telekommunikation und bei Telemedien“ (TTDSG). Das Gesetz soll die bislang im Telekommunikationsgesetz (TKG) geregelten Datenschutzbestimmungen in einem Gesetz mit dem teilweise neu zu regelnden Datenschutz des Telemediengesetzes (TMG) zusammenführen. Die Anpassung des TKG setzt (verspätet) die europäische Richtlinie 2018/1972 über einen Kodex für elektronische Kommunikation vom 11.12.2018 um.

Der Entwurf enthält in § 24 eine neue Einwilligungsregelung zur Verwendung von Cookies und bereits im Endgerät gespeicherten Informationen. Die bisherigen Regelungen zum technischen und organisatorischen Datenschutz aus § 13 TMG werden teilweise gekürzt, dafür wird ein Auskunftsverfahren für Bestands- und Nutzungsdaten von Telemediendiensten umfangreich neu geregelt.

Was der Entwurf versäumt ist die Abgrenzung und Neuaufteilung der Pflichten zwischen Telekommunikations- und Telemediendiensten, für die die neuen Begriffsbestimmungen des Kodex für elektronische Kommunikation einen Ansatzpunkt bieten. So ist es beispielsweise an der Zeit, E-Mail-, Messenger- und Videokonferenzdienste als interpersonelle Kommunikationsdienste neu einzuordnen. Stattdessen kreist der Entwurf um neue Eingriffsbefugnisse und Datenschutzeinschränkungen.

Selbstverständliche Best Practices

Über Sinn und Unsinn von (immer wieder neuen) IT-Sicherheits-Checklisten kann man trefflich streiten. Das trifft auch auf die vom Bayrischen Landesdatenschutzbeauftragten bereits am 27.05.2020 veröffentlichte fünfseitige Checkliste zur „Cybersicherheit für medizinische Einrichtungen“ zu.

Sie ist eine übersichtliche Zusammenstellung geeigneter Schutzmaßnahmen. Allerdings sollte nicht der Eindruck entstehen, dass die Liste alle, nicht einmal alle wesentlichen Anforderungen abdeckt. Wie in der Einleitung angemerkt liegt der Fokus auf der Verfügbarkeit der verarbeiteten (personenbezogenen) Daten und weniger auf den in diesem Kontext mindestens ebenso wichtigen Zielen Integrität und Vertraulichkeit.

Die zahlreichen Verweise auf das IT-Grundschutz-Kompendium sind zweifellos sinnvoll, werfen aber die Frage auf, ob die Checkliste eher als „Lesehilfe“ für medizinische Einrichtungen gedacht ist, die sich die Mühe einer gründlichen Auseinandersetzung mit dem IT-Grundschutz ersparen möchten. Viele der in der Checkliste aufgeführten Punkte sind zudem simple Selbstverständlichkeiten („Empfehlung zur Vermeidung leicht zu erratender Passwörter oder Passwortbestandteile“), andere muten etwas merkwürdig an („Kenntnis der zuständigen Datenschutzaufsichtsbehörde“ – die sollte spätestens beim Lesen der Checkliste bekannt sein).

Hilfreicher erscheint die vom TeleTrusT Bundesverband IT-Sicherheit e. V. am 04.02.2021 in erweiterter Fassung (v1.8) veröffentlichte Handreichung zum „Stand der Technik in der IT-Sicherheit“ – mit 98 Seiten deutlich umfangreicher als die bayerische Checkliste, aber dafür eine umfassendere Zusammenstellung geeigneter technisch-organisatorischer Maßnahmen (TOMs).

Secorvo News

PKI, T.P.S.S.E. und T.I.S.P.

Unsere beiden Zertifizierungsseminare zum „TeleTrusT Information Security Professional“ (**03.–07.05.2021**) und zum „TeleTrusT Professional for Secure Software Engineering“ (**26.–29.04.2021**) sowie das Vertiefungsseminar zu Public-Key Infrastrukturen (**19.–22.04.2021**) hoffen wir wieder in bewährter Form und unter Einhaltung der Abstandsregelung als Präsenzveranstaltung durchführen zu können. Das Programm und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite. Teilnehmer des T.I.S.P.-Seminars erhalten nach Anmeldung zur Vorbereitung das T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“ zugesandt.

Lesen bildet

Der Ausfall zahlreicher Abendveranstaltungen hat die Bücherkäufe ansteigen lassen. Da wollen wir Sie nicht alleine lassen und laden Sie herzlich ein zum „1. Literarischen Kabinett“ der Karlsruher IT-Sicherheitsinitiative am 25.03.2021 um 18 Uhr (Teams). Sie werden zahlreiche Werke der Weltliteratur kennenlernen, die Sicherheits- und Datenschutzexperten gelesen haben müssen. Fünf Bücher werden wir etwas ausführlicher vorstellen – und freuen uns nicht nur auf Ihre Anmeldung, sondern auch über eine persönliche Rückmeldung: Welche Bücher gehören unbedingt auf diese Liste? Und: Haben Sie Lust, Ihr eigenes Lieblingsbuch, das Sie im Hinblick auf IT-Sicherheit oder Datenschutz nachdenklich oder betroffen gemacht hat, kurz in 10 Minuten vorzustellen? Dann schreiben Sie uns.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2021	
15.-18.03.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz/virtuell)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2021	
03.-07.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)
12.05.	SecurityCruise (Connecting Media, Karlsruhe)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)

Fundsache

Datenschutz-Unterstützung für Vereine: Mit DS-GVO.clever bietet der LfDI Baden-Württemberg seit kurzem eine effiziente und effektive Hilfestellung für Vereine bei der Erstellung ihrer Datenschutzhinweise.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, 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