secorvo
security consulting

Secorvo Security News

Juni 2018

Panik 4.0

Unter Panik verstehen wir eine durch eine plötzliche, echte oder vermeintliche Gefahr hervorgerufene, übermächtige Angst, die zu unüberlegten Reaktionen führt. Sie kann sich zur kollektiven oder Massenpanik entwickeln, wenn in „eng stehenden Gruppen“ Menschen ihre Handlungen gegenseitig beobachten und darauf reagieren – und dabei ihre Selbstkontrolle verlieren.

In Zeiten allgegenwärtiger Digitalisierung kann auch Panik digital werden: Verursacht im digitalen Kontext und verstärkt durch die Verbreitung über verzugsfreie digitale Kommunikationsmedien wie Instant Messaging oder Social Networks entsteht so schnell eine Massenpanik 4.0. Dabei zeigen sich die fatalen Folgen des zunehmenden Fast-Food-Gebarens bei der Erzeugung und Verbreitung von Informationen: Publizierte Nachrichten sind immer nachlässiger recherchiert und werden allerorten ungeprüft kopiert – die Empfänger haben sich bereits so daran gewöhnt, dass sie den Wahrheitsgehalt nicht mehr aus der Seriosität einer Quelle (gibt es das noch?) sondern aus der Anzahl der Nachrichten ähnlichen Inhalts ableiten.

Erleben konnte man das in den vergangenen Wochen im Zusammenhang mit dem Inkrafttreten der DS-GVO. Bestenfalls halbrichtige Darstellungen der Anforderungen in den Medien ließen den Verdacht aufkeimen, es kämen völlig neue Herausforderungen auf Unternehmen, Vereine und Verbände zu – und es sei mit Ordnungsgeldern in Höhe von 4% des Jahresumsatzes zu rechnen.

Zu den Panik-Reaktionen auf dieses Halbwissen zählen E-Mails von Vereinen, die eine Einwilligung der Mitglieder für die erforderliche Verarbeitung personenbezogener Mitgliederdaten erbitten, Kühlschränke mit Datenschutzerklärung oder Tageszeitungen, die den Webauftritt abschalten. Blenden wir den volkswirtschaftlichen Schaden aus, so bleibt ein sehr bitterer Nachgeschmack: Dem Schutz unserer Persönlichkeitsrechte hat das mehr geschadet als genutzt.

Inhalt

Panik 4.0

Security News

Alte Zöpfe

Stand der Technik

Unter der Gürtellinie

Gezahnter Papiertiger

Bulk-Forensik

Secorvo News

Teamverstärkung

Secorvo@itsa

Secorvo Seminare

Freiwild im Cyberspace

Veranstaltungshinweise

secorvo
security consulting

Security News

Alte Zöpfe

Nachdem sich seit März 2018 Version 1.3 des Protokolls Transport Layer Security (TLS) in den letzten Zügen der Standardisierung befindet, gibt es zunehmend Bestrebungen, alte Zöpfe abzuschneiden. Gemeint sind insbesondere die Protokollversionen TLS 1.0 (1999) und 1.1 (2006). Die alten Protokollversionen weisen kryptografische Schwächen auf und sind im Vergleich mit TLS 1.2 und 1.3 nicht mehr zeitgemäß. Diese Erkenntnis ist auch im Standard PCI DSS angekommen: Ab dem 01.07.2018 sind TLS 1.0 und 1.1 nicht mehr erlaubt.

In den meisten Fällen sollte eine Deaktivierung der alten Versionen keine merkbaren Folgen nach sich ziehen: TLS 1.2 ist bereits seit 10 Jahren standardisiert und wird dementsprechend auch von allen gängigen Browsern und Bibliotheken unterstützt. Diverse aktuelle Browser unterstützen übrigens bereits TLS 1.3. – sind Sie schon dabei?

Stand der Technik

Am 14.06.2018 veröffentlichte TeleTrusT die deutlich überarbeitete Fassung der „TeleTrusT-Handreichung zum Stand der Technik“ nach IT-Sicherheitsgesetz und DSGVO. Die Erstfassung von 2016 wurde um Erklärungen zur Bestimmung des Technologiestandes und um eine Methode zur Bewertung der Maßnahmen ergänzt. Die Beiträge wurden gründlich überprüft und ggf. gestrichen oder überarbeitet. Eine Bewertung soll transparent machen, warum Maßnahmen aufgrund von „Grad der Anerkennung“ und „Grad der Bewährung in der Praxis“ als Stand der Technik aufgeführt sind. Zusätzlich wurden die Struktur verbessert und neue Maßnahmen und Prozesse ergänzt.

Ein weiterer schöner Meilenstein für die Pioniere der IT-Sicherheit und eine hilfreiche Grundlage zur Positionsbestimmung, wenn es um die Konzeption von Maßnahmen und Prozessen geht.

Unter der Gürtellinie

Traditionell setzten viele Bedrohungsanalysen und Sicherheitskonzepte auf der Ebene des Betriebssystems an. Durch zunehmende Virtualisierung kommt u. U. noch ein unterliegendes Hypervisor-System mit ins Bild. Seit ein paar Monaten gerät nun die Sicherheit unterhalb der Betriebssystem-Ebene zusehends ins Blickfeld: Seit der Entdeckung der Spectre- und Meltdown-Schwachstellen finden Forscher immer neue Varianten, um Informationen über Prozessgrenzen hinweg auszuspähen. So veröffentlichte OpenBSD am 05.06.2018 einen Patch gegen eine Prozessor-Schwachstelle – das zugehörige Advisory wurde von Intel erst am 13.06.2018 veröffentlicht.

Und auch auf der proaktiven Seite gibt es Aktivitäten: Microsoft hat – experimentell und unabhängig von Schwachstellen durch spekulative Ausführung von Befehlen – bereits Windows 10 auf eine Prozessor-Architektur portiert, bei der der Compiler die optimierte Abarbeitungsfolge vorgibt. Und am 18.06.2018 veröffentlichten Forscher einen Vorschlag für eine „Leak“-freie spekulative Ausführung.

Derweil holen uns wieder totgehoffte Altlasten ein: So wurde am 19.06.2018 gemeldet, dass sich die Anmeldung an HPs iLO4 Management-System mittels eines simplen Pufferüberlaufs übertölpeln lässt.

Wer heute neue Sicherheitskonzepte erstellt, tut gut daher daran, in die Bedrohungsanalyse auch die relevanten Ebenen unterhalb des Betriebssystems einzubeziehen.

Gezahnter Papiertiger

„Lieber offline als abgemahnt“, „Was Ihr Chef jetzt verbieten kann“ oder „Selbst Anwälte sind ratlos über die neuen Datenschutzregeln“ sind nur einige der Headlines, welche dieser Tage in den Medien zum Thema Datenschutz gestreut werden. Nach Ablauf der zweijährigen Übergangsfrist gelten seit dem 25.05.2018 die Vorgaben der Datenschutz-Grundverordnung (DS-GVO). Den Aufsichtsbehörden wird nun eine wesentlich höhere Bedeutung zugemessen als bisher. Wer sich nicht datenschutzkonform verhält, riskiert Bußgelder bis zu 20 Mio. € oder 4% des weltweit erzielten Jahresumsatzes. Zahlen, die mittlerweile durch die Medien Omnipräsenz erlangt haben und einen Großteil der Angst und Unsicherheit verantworten, die sich in den letzten Monaten ausgebreitet haben.

Seit Inkrafttreten des Gesetzes ist nun ein Monat vergangen. Haben die Unternehmen nun überreagiert, oder wurden sie gerechtfertigt dazu gedrängt, in hektische Tätigkeit zu verfallen, um DS-GVO-konform zu werden? Sicher ist: Vieles, was bereits im nun von der DS-GVO verdrängten Bundesdatenschutzgesetz (BDSG) gefordert wurde, behält seine Gültigkeit. Und angesichts der Übergangsfrist von zwei Jahren hatten Unternehmen ausreichend Zeit, sich auf die neuen Anforderungen vorzubereiten.

Die Verantwortung sollte jedoch nicht allein den betroffenen Unternehmen zugeschoben werden. Denn es bestehen gerechtfertigt Unsicherheiten, die aufgrund dehnbarer DS-GVO-Bestimmungen

noch ausgelegt und geklärt werden müssen. Nicht zuletzt auch aufgrund der noch im Entwurfsstadium befindlichen E-Privacy-Verordnung für den Bereich der elektronischen Kommunikation, deren „go live" nicht vor 2019 zu erwarten ist, und von welcher erwartet wird, dass sie konkretisierende und ergänzende Anforderungen zu den Vorgaben der DS-GVO formuliert.

Doch was bedeutet diese aktuelle Rechtslage für Unternehmen konkret: Soll man sich von dem aktuellen Hype mitreißen lassen? Ist mit einem Abflachen des Datenschutz-Aktivismus zu rechnen, sobald sich die Unruhe etwas gelegt hat?

Tatsächlich wäre es ratsam, sich auf die (Weiter-) Entwicklung des Grundgerüsts der Datenschutz-Organisation und deren Implementierung zu konzentrieren. Denn mit entsprechender Dokumentation der Prozesse und kontinuierlicher Verbesserung ist nicht nur ein nachhaltigerer Datenschutz-Reifegrad zu erreichen – es ist auch der beste Schutz vor behördlichen Maßnahmen.

Bulk-Forensik

Lange Zeit war es recht still um die Weiterentwicklung des forensischen Carving-Werkzeuges bulk_extractor. Dies hat sich aber am 30.12.2017 geändert: Die hilfreiche Scanner-Komponente „scan_ntfsusn" wurde integriert, mit der USN-Journal-Metainformationen (Zeitstempel und Schreibtransaktionen für Dateien und Verzeichnisse) in einem NTFS-Dateisystem von Windows parallel ausgewertet werden können.

Da bulk_extractor tatsächlich jeden CPU-Core und Thread nutzt, kann mit Nutzung von scan_ntfsusn ein erheblicher Zeitgewinn bei der vollautomatischen Datenaufbereitung erzielt werden. Dazu kommt seit 28.01.2018 eine Weiterentwicklung namens bulk_extractor-rec, die nicht der offiziellen Entwicklung folgt, aber dafür aus den verschiedenen internen NTFS-Logdaten noch die Record-Typen INDX, RSTR/RCRD und FILE durch zusätzliche Scanner-Komponenten extrahiert. Wer also schnell Informationen braucht und nicht auf Plaso warten möchte, den werden diese Funktionen freuen.

Secorvo News

Teamverstärkung

Dank der zunehmenden Nachfrage nach Unterstützung benötigt auch Secorvo personelle Verstärkung. Und wir freuen uns, in den vergangenen Wochen mit Michael Knöppler und Thomas Maus zwei sehr kompetente IT-Sicherheitsexperten für unser Team gewonnen zu haben.

Secorvo@itsa

In diesem Jahr werden wir vom 09. bis 11.10.2018 auf der IT-Security-Messe it-sa in Nürnberg vertreten sein und dort am Stand 10.1-628 unsere Datenschutz- (DSMSready2go) und Informationssicherheits-Management-Lösungen (ISMSready2go) zeigen. Sie sind herzlich eingeladen, bei Interesse vorab einen Termin mit uns zu vereinbaren.

Secorvo Seminare

Nach der Sommerpause startet die Herbst-Seminarserie von Secorvo im Oktober mit den beiden Zertifizierungsseminaren T.I.S.P. (15.-19.10.2018) und T.P.S.S.E. (12.-15.11.2018). Wir freuen uns auf Ihre Teilnahme – und empfehlen für das T.I.S.P.-Seminar eine frühzeitige Anmeldung.

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

Freiwild im Cyberspace

Die Anforderungen an die Mobilität von Arbeitnehmern steigen beständig - unterstützt von immer kleineren und leistungsfähigeren Endgeräten. Wie aber lässt sich diese Flexibilität mit Sicherheitsanforderungen vereinbaren? Bei unserem kommenden KA-IT-Si-Event am **12.07.2018** stellt Dirk Fox (Secorvo) in seinem Vortrag wichtige Anforderungen und technische Möglichkeiten für sicheres mobiles Arbeiten vor. Anschließend geht Holger Bajak (ophelis) in seinem Vortrag "Mobil und vernetzt" auf das Arbeiten in neuen Strukturen ein. Arbeiten ist im digitalen Zeitalter überall und jederzeit möglich. Das Büro gewinnt dadurch eine neue Bedeutung: Es ist weit mehr als ein Arbeitsraum. Das Büro wird zum Treffpunkt, dient dem Austausch und der Zusammenarbeit. Es erzeugt Zugehörigkeit und bietet den Mitarbeitern Heimat.

Die Veranstaltung findet in Kooperation mit feco-feederle und ophelis statt. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2018	
12.07.	Freiwild im Cyberspace (KA-IT-Si Karlsruhe)
24.-27.07.	PETS 2018 (University of Minnesota, Barcelona/ES)
August 2018	
04.-09.08.	Blackhat USA 2018 (Blackhat, Las Vegas/US)
09.-12.08.	DEF CON 26 (DEFCON, Las Vegas/US)
14.08.	SOUPS 2018 (usenix, Baltimore/US)
15.-17.08.	27th USENIX Security Symposium (usenix, Baltimore/US)
15.-18.08.	DFRWS USA 2018 (DFRWS, Providence/US)
19.-23.08.	Crypto 2018 (IACR, Santa Barbara/US)
September 2018	
04.-05.09.	D • A • CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter (ULD, Kiel)
24.09.	Datenschutztag 2018 (COMPUTAS Gisela Geuhs GmbH, Köln)
28.-30.09.	FIfFKon 2018 (FIfF e.V., Berlin)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Hans-Joachim Knobloch, Sarah Niederer, Jochen Schlichting

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