secorvo
security consulting

Secorvo Security News

Februar 2016

Trägheitsprinzip

Das Trägheitsprinzip ist ein zentrales Axiom der Physik *Sir Isaac Newtons* (1642-1726), auch bekannt als das im Jahr 1687 publizierte „Erste Newtonsche Gesetz". Formuliert wurde es bereits im Jahr 1638 von *Galileo Galilei* (1564-1641): Jeder Körper behält seinen Ruhe- oder Bewegungszustand bei, solange keine auf ihn einwirkende Kraft ihn zur Änderung dieses Zustands zwingt.

Wie wir heute wissen, lassen sich mit diesem Prinzip nicht nur die Bewegungen der Himmelskörper erklären, sondern auch das Verhalten von elektromagnetischen Feldern. Verfolgt man aufmerksam die Nachrichten, kann man sich außerdem des Eindrucks nicht erwehren, dass auch das menschliche Verhalten diesem Prinzip gehorcht.

Wie anders ließe es sich auch erklären, dass nach einer Analyse von 35 Millionen Authentifikationsdaten durch das Hasso-Plattner-Institut im Jahr 2015 das meistgenutzte Passwort der Welt „123456" lautet? Dass gut 15 Jahre nach dem I-Love-You-Virus noch immer angeklickte E-Mail-Anhänge das Haupteinfallstor für Schadsoftware sind? Dass auch heute noch Mitarbeiter ihre Rechner am Arbeitsplatz in der Regel ohne Aktivierung einer Zugangssperre verlassen? Dass Mitarbeiter sich mit Händen und Füßen gegen den Entzug von Administratorrechten für ihren lokalen Rechner wehren?

Sicherheit könnte viel einfacher sein – etwas mehr Einsicht bei den „Gurtmuffeln" des 21. Jahrhunderts vorausgesetzt. Derweil üben sich die Verantwortlichen in Selbsttäuschung: Nach dem am 17.11.2015 veröffentlichten „Cyber Security Report" des Instituts für Demoskopie Allensbach (im Auftrag der Deutschen Telekom) halten die befragten Führungskräfte deutscher Unternehmen das Schadensrisiko durch einen Hackerangriff für eher gering (60 %) und sehen ihr Unternehmen „so gut wie möglich vorbereitet" (60 %).

Offenbar müssen wohl auch hier erst externe Kräfte einwirken, damit sich der Zustand ändert.

Inhalt

secorvo
security consulting

Security News

Und Krypto funktioniert doch ...

... zumindest bei aktuellen Erpressungs-Trojanern (*Ransomware*) wie Teslacrypt. Ließen sich von Teslacrypt 2 verschlüsselte Dateien noch mit dem TeslaDecoder wiederherstellen, weil der verwendete AES-Schlüssel rekonstruierbar im Header der Datei versteckt wurde, ist dies bei dem am 12.01.2016 in Umlauf gebrachten Teslacrypt 3 nicht mehr möglich. Auch ältere Erpressungs-Trojaner wie Cryptowall (seit 01.11.2014 bekannt) setzen inzwischen so gute kryptographische Verfahren ein, dass das FBI empfiehlt, die erpresste Summe zu zahlen.

Gegen derartige Angriffe hilft eine Kombination aus technischen und Sensibilisierungs-Maßnahmen für die Benutzer. Werden E-Mail-Anhänge abgefangen oder solche mit Schadsoftware gar nicht erst geöffnet, wird damit die Infektion unterbunden – das ist wirkungsvoller als ein Virenschutz, der neue Varianten der Trojaner ohnehin zunächst nicht erkennt. Um den Schaden einer Infektion zu begrenzen helfen restriktive Berechtigungen, sodass nur wenige (Benutzer-) Dateien und nicht komplette Netzlaufwerke unerwünscht verschlüsselt werden. Und eine angepasste und strikte Backup-Strategie hilft im Fall der Fälle bei der Wiederherstellung der Daten.

Minimierung per Verordnung

Das Bundesinnenministerium hat am 13.01.2016 einen Referentenentwurf der Verordnung (BSI-KritisV) zum am 25.07.2015 in Kraft getretenen IT-Sicherheitsgesetz vorgelegt, der insbesondere näher festlegt, welche Anlagen als kritische Infrastrukturen gelten und damit dem Gesetz unterfallen.

Der Entwurf zählt die Anlagenkategorien aus den Bereichen Energie, Wasserversorgung, Telekommunikation und Ernährung auf und umfasst einen Anhang mit branchenspezifischen Schwellenwerten. Beispielsweise fallen Stromerzeugungsanlagen ab 420 MW installierter Leistung und Serverfarmen mit im Jahresdurchschnitt mindestens 25.000 laufenden Instanzen unter die Regelungen.

Der Aspekt des Gefährdungspotentials für die öffentliche Sicherheit (§ 2 Abs. 10 Nr. 2 BSI-Gesetz) wird dabei vollständig ausgeblendet. Auch die im Gesetzestext enthaltenen Sektoren Gesundheit, Transport und Verkehr oder Finanz- und Versicherungswesen sind (bis Ende 2016) ausgespart. Nach der Begründung sind in Deutschland insgesamt 650 Anlagen betroffen, deren Betreiber jährlich mit einem Aufwand von sieben Vorfallsmeldungen à 660 Euro pro Anlage rechnen müssen. In der Gesetzesbegründung war noch von 2000 Betreibern und einem nicht quantifizierbaren Aufwand für die Maßnahmenumsetzung die Rede. Offenbar ist ein ISMS in Deutschland zurzeit günstig zu haben.

Arbeitnehmerkontrolle

Das Landesarbeitsgericht Berlin-Brandenburg hat am 14.01.2016 entschieden, dass Arbeitgeber die Internetnutzung ihrer Mitarbeiter – auch bei in Pausen ausnahmsweise gestatteter privater Nutzung – ohne Einwilligung der Betroffenen anhand der Browserprotokollierung überprüfen dürfen. Die Protokolle haben zudem Beweiskraft im Streit über eine außerordentliche Kündigung wegen exzessiver Internetnutzung.

Die Datenschutz-Aufsichtsbehörden sehen dies v. a. bei erlaubter Privatnutzung kritischer und haben ihre Einschätzung gerade erst in einer am 30.01. 2016 veröffentlichten Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz dargestellt.

Das Landesarbeitsgericht Berlin-Brandenburg hat bereits im Jahr 2011 vertreten, dass der Arbeitgeber selbst bei erlaubter Privatnutzung nicht zum Telekommunikationsdiensteanbieter wird. Ob dieses jüngste Urteil in ähnlicher Weise rechtliche Streitstände vertieft, wird jedoch erst die Urteilsbegründung verraten.

Transparenz ist Pflicht

Fast jede Webseite verfügt heute über eine Anbieterkennzeichnung gem. § 5 TMG, meist zu finden unter dem Link „Impressum“. Eine korrekte Datenschutzerklärung nach § 13 TMG fällt vielen Seitenbetreibern schon viel schwerer. Dabei hatte das OLG Hamburg bereits im Juli 2013 entschieden, dass fehlende oder fehlerhafte Datenschutzerklärungen einen abmahnfähigen Wettbewerbsverstoß darstellen.

Dieser Entscheidung folgt das LG Köln mit seinem Beschluss vom 26.11.2015 und erließ eine entsprechende einstweilige Verfügung gegen einen Webseitenbetreiber. Unter anderem wurde auf der Seite das Remarketing-Tool Google Adwords eingesetzt. Webseitenbetreiber sollten den Beschluss als Ermahnung nehmen, ihre Datenschutzerklärung auf Aktualität und Vollständigkeit zu überprüfen – oder umgehend eine zu erstellen.

Grünes Licht für Cookie-Opt-out

Das OLG Frankfurt hat am 17.12.2015 entschieden, dass eine Opt-out-Möglichkeit beim Einsatz eines Webanalyse-Dienstes ausreicht. In dem Urteil über die Klage eines Verbraucherschutzverbands ging es um eine Gewinnspiel-Einwilligung, die aufgrund

undifferenzierter Verlinkung auf 59 Kooperationspartner nicht rechtswirksam war.

„Nebenbei" beantwortet das Urteil jedoch die Frage, ob die so genannte Cookie-Richtlinie der EU und deren Vorgabe zur Einwilligung beim Einsatz von Cookies in Deutschland unmittelbar anwendbar ist. Diese Frage ist seit Jahren heiß diskutiert und umstritten. Das OLG hat nun klargestellt, dass die entsprechenden datenschutzrechtlichen Vorschriften keine Einwilligung (in Gestalt eines Opt-in-Verfahrens) vorschreiben. Die Zustimmung gilt als erteilt, wenn der Nutzer einen bereits gesetzten Haken nicht entfernt (Opt-out-Verfahren).

Grenzen der Werbeflut

In seiner Urteilsbegründung zu der bereits am 15.12.2015 ergangenen Entscheidung über Werbung in Eingangsbestätigungs-E-Mails ist der Bundesgerichtshof (BGH) auf die Reichweite der von ihm angenommenen Persönlichkeitsrechtsverletzung eingegangen. Im verhandelten Fall hatte der Kläger auf einen Werbewiderspruch eine automatische Eingangsbestätigungs-E-Mail mit Werbeinhalt erhalten. Der § 7 UWG war in diesem Fall nicht anwendbar, da es sich beim Kläger um einen Verbraucher, nicht um einen Wettbewerber handelte. Ein elektronisches Postfach sei jedoch Teil der Privatsphäre, das allgemeine Persönlichkeitsrecht vermittle das Recht „in Ruhe gelassen zu werden".

Ob das Einwilligungserfordernis aus Art. 13 Abs. 1 der EU-Datenschutzrichtlinie für elektronische Kommunikation bei Verstößen stets zu einem Eingriff in das Persönlichkeitsrecht mit resultierendem Unterlassungsanspruch führt, ließ der BGH jedoch offen. Dies gelte jedenfalls regelmäßig für einen Werbewiderspruch.

Werbezusätze in E-Mails dürfen nach dieser Rechtsprechung nur noch bei Einwilligung oder bei bestehender Geschäftsbeziehung eingesetzt werden – vom E-Mail-Server automatisch angehängte Marketing-Footer können zukünftig teuer werden.

Secorvo News

Call for Paper für die T.I.S.P.-Community

Vom **10. bis 11.11.2016** treffen sich in Frankfurt Absolventen des T.I.S.P.-Zertifikats auf dem „10. T.I.S.P. Community Meeting" zum Erfahrungsaustausch. Von TeleTrusT wurde ein Call for Paper für diese Veranstaltung veröffentlicht: Bis zum 18.04. 2016 können Sie Beitragsvorschläge einreichen.

Das CPSSE-Zertifikat

Werden bei der Entwicklung von Software-Sicherheitsanforderungen systematisch berücksichtigt, dann ist das nicht nur ein wichtiger Schritt zu einer höheren Softwarequalität, sondern auch ein Gewinn für die IT-Sicherheit aller Kunden. Wie das gelingt, zeigt die Schulung zum Certified Professional for Secure Software Engineering (CPSSE) vom **11. bis 14.04.2016** in Karlsruhe. Ein Teilnehmer schrieb uns dazu: „*Secure Software Engineering: alles andere als nur Theorie: Informatives und interaktives Seminar mit einem sehr guten Verhältnis von Theorie und Praxis.*"

PKI für die Praxis

Über 300 PKI-Experten haben sich bisher auf einem unserer PKI-Seminare mit aktuellem Know-how versorgt. Eine Teilnehmerstimme: „*Das gesamte Seminar war beeindruckend strukturiert aufgebaut und umfasste alle wesentlichen Themen wie Grundlagen, Standards und praktische Umsetzung. Unter kompetenter Begleitung durch spezialisierte Dozenten hat mich der abschließende Workshop für die schrittweise Vorgehensweise sensibilisiert […]. Eine wohltuende Atmosphäre um das Seminar […].*" Die nächste PKI-Schulung, die Expertise und Erfahrung aus 20 Jahren aktiver Gestaltung von PKIs bündelt, findet vom **19. bis 22.04.2016** in Karlsruhe statt.

Detaillierte Seminarinhalte, weitere Angebote und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite.

Dumm. Dümmer. DAU?

In der IT gilt die alte Weisheit, stets den „Dümmsten Anzunehmenden User" (DAU) im Blick zu behalten. Doch was heißt das eigentlich? Und warum verhält sich der DAU so „dumm"? Und was kann man daraus lernen?

In seinem Vortrag „Psychologie der Sicherheit: Ist der DAU wirklich dumm?" beim nächsten KA-IT-Si-Event am **21.04.2016** um 18 Uhr erläutert Christoph Schäfer (Secorvo Security Consulting GmbH), wie Entscheidungsprozesse im menschlichen Gehirn ablaufen und welchen systematischen Fehlern Menschen bei der Entscheidungsfindung unterliegen.

Dabei wird deutlich, welche Bedeutung dem „Faktor Mensch" in der IT-Sicherheit zukommt – und was man daraus lernen sollte. Anschließend haben Sie wie gewohnt die Gelegenheit zum „Buffet-Networking". Anmeldung unter www.ka-it-si.de.

Save the Date: APP #4

Merken Sie sich bereits den 29.04.2016 vor – den Termin unserer vierten Anti-Prism-Party im Karlsruher ZKM.

Veranstaltungshinweise

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

März 2016	
14.-15.03.	9. GDD-Fachtagung „Datenschutz International“ (Gesellschaft für Datenschutz und Datensicherung e.V., Berlin)
21.-24.03.	1st IEEE European Symposium on Security and Privacy (IEEE, Saarbrücken)
April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.04.	Dumm. Dümmer. DAU? (KA-IT-Si, Karlsruhe)
27.-28.04.	17. Datenschutzkongress (EUROFORUM, Berlin)
29.04.	Anti-Prism-Party 4. Staffel (KA-IT-Si, Karlsruhe)
Mai 2016	
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)

Fundsache

Am 28.01.2016 hat der Rat der Europäischen Union die deutschsprachige Fassung der am 15.12.2016 beschlossenen Datenschutz-Grundverordnung veröffentlicht, die die EU-Richtlinie aus dem Jahr 1995 ablöst.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Michael Knopp, Christoph Schäfer

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