secorvo
security consulting

Secorvo Security News

Oktober 2019

Rechenmagie

Wer die Liste der seit Inkrafttreten der DSGVO verhängten Datenschutz-Bußgelder durchsieht, wird von deren Spanne überrascht: Sie reicht von gerade einmal einhundert Euro bis zu deutlich dreistelligen Millionenbeträgen (Marriott, British Airways). Unvermeidlich drängt sich der Eindruck auf, dass die Bußgeldhöhe keiner einheitlichen Systematik folgt, sondern eher Beliebigkeit entspringt.

Bei genauerem Hinsehen wird deutlich, dass dies drei Ursachen haben dürfte: die noch geringe Erfahrung vieler europäischer Aufsichtsbehörden mit diesem gestärkten Sanktionsinstrument, die bisher eingeschränkte Abstimmung der Aufsichtsbehörden untereinander und die strukturell neue Ausrichtung der Bußgelder an der Leistungsfähigkeit des betroffenen Unternehmens.

Erkennbar ist, dass mit wachsender Erfahrung der Aufsicht auch die Höhe der Bußgelder steigt. Vor wenigen Wochen haben sich nun die deutschen Aufsichtsbehörden auf ein Berechnungsschema geeinigt, das die Bußgeldhöhe aus dem Unternehmensumsatz ableitet und mit einem Korrekturfaktor die Schwere des Verstoßes berücksichtigt sowie materielle Verstöße stärker als formelle ahndet.

Eine zu begrüßende Entwicklung zu mehr Transparenz und Nachvollziehbarkeit. Dennoch führen Rechenmodelle nicht automatisch zu gerechteren Ergebnissen. Daher ist der wichtigste Teil des Konzepts der letzte Punkt – die Berücksichtigung täterbezogener und wirtschaftlicher Umstände bei der endgültigen Bußgeldfestsetzung. Das ist keine Beliebigkeit durch die Hintertür, sondern räumt einen Ermessensspielraum ein, der bei besonnener Nutzung zu mehr Einzelfallgerechtigkeit führen kann als das Rechenschema.

Unternehmen müssen sich daran gewöhnen, dass derselbe Datenschutzverstoß zu verschiedenen Bußgeldern führen kann. Und die Aufsichtsbehörden müssen aufpassen, dass sie bei aller pseudo-objektiver Rechenmagie nicht das Augenmaß verlieren.

Inhalt

secorvo
security consulting

Security News

Unauffällige Erweiterungen

Auf der CS3STHLM-Konferenz in Stockholm zeigte der Sicherheitsforscher Monta Elkins am 24.10. 2019, wie es ihm mit einem Budget von nur $200 gelang, eine Cisco ASA 5505 Firewall um eine Hardware-Backdoor zu erweitern. Der von ihm aufgelötete ATtiny85 greift über die serielle Schnittstelle die Passwortrücksetzung an und richtet eine Hintertür mit Administrationsrechten ein. Der etwa fingernagelgroße Mikrocontroller ist ohne Schaltplan kaum als zusätzliches Bauteil erkennbar. Der Angriff erinnert stark an die von Edward Snowden und Glenn Greenwald 2014 aufgedeckten Manipulationen der NSA an Cisco-Routern auf dem Postweg und Gerüchte über chinesische Hacker, die 2018 auf Mainboards des Herstellers Supermicro einen reiskorngroßen Chip ergänzt haben sollen. Derartige Manipulationen zeigen eindrucksvoll, dass zur Herstellung sicherer Produkte auch eine sichere Lieferkette gehört. Präpariert ein Angreifer originale Firewalls oder Server und verkauft sie dann beispielsweise über Amazon Marketplace, kann er manipulierte Geräte mit geringem Aufwand verbreiten.

Freie Kekswahl

Ein kollektives Stöhnen und Wehklagen der online-Werbebranche erschallte am 01.10.2019, nachdem der EuGH in der Rechtssache C-673/13 - Planet49-GmbH entschieden hatte, dass beim Besuch einer Webseite nur technisch notwendige Cookies – so genannte Session-Cookies – ohne Einwilligung gesetzt werden dürfen. Das Urteil ist EU-weit unmittelbar umzusetzen und anzuwenden. Die deutsche Umsetzung der „Cookie-Richtlinie“ im Telemediengesetz ist nicht rechtskonform und muss angepasst werden. Voreingestellte Häkchen gehören nun ebenso der Vergangenheit an wie konkludente Einwilligungen durch Weiternutzung einer Webseite mit impliziter Duldung.

Wirksame Einwilligungen setzen voraus, dass der Seitenbetreiber die Nutzer über Third-Party-Cookies, die er zu setzen wünscht, informiert. Erst wenn Nutzer die Möglichkeit haben, eine freiwillige Entscheidung für oder gegen die Cookies zu treffen, entspricht die Einwilligung den gesetzgeberischen Anforderungen. Das bedeutet für (fast) alle Unternehmen Handlungsbedarf bei der Anpassung der Cookie-Banner auf ihren Webseiten. Ansonsten geht man das Risiko ein, in das Visier der Aufsichtsbehörden und etwaiger Abmahner zu geraten. Es ist nur ein schwacher Trost, dass auch der EuGH nach Veröffentlichung des Urteils den eigenen Cookie-Banner mehrfach anpassen musste, bis er den Vorgaben des eigenen Urteils entsprach.

In Code We Trust

Der Turing-Award-Preisträger Ken Thompson illustrierte schon 1984 in seiner Dankesrede „Reflections on Trusting Trust“, wie ein manipulierter Compiler Backdoors in Programme einbauen kann, ohne dass dabei Spuren im Quellcode zurückbleiben. Die am 24.10.2019 veröffentlichte Kombination einer XXE- und einer Directory Traversal Schwachstelle im XML Language Server (aka lsp4xml) erreicht zwar nicht ganz das Ausmaß eines manipulierten Compilers. Durch die Verwendung der Komponente in XML-Plugins diverser Entwicklungsumgebungen (Eclipse, VS-Code, ...) drängt sich allerdings immer noch die gleiche Frage auf wie vor 35 Jahren: Können wir dem Code oder der Software trauen, die wir einsetzen um neue Software zu erstellen?

Ken Thompson kam zu dem Schluss, dass dies nicht möglich ist: „*You can't trust code that you did not totally create yourself.*“ Den kompletten Code inklusive Tools und Compiler selbst zu erstellen ist heute allerdings in den seltensten Fällen überhaupt und nur mit unvertretbar hohem Aufwand möglich. Allerdings sollte es zu den Minimaltugenden gehören, nur etablierte Werkzeuge mit aktuellem Versionsstand einzusetzen und niemals „blind“ Code(schnipsel) aus unbekannten Quellen zu verwenden.

Entflammbarer Brandschutz

Immer noch fordern Auditoren, Virenschutzprodukte auf Servern einzusetzen. Aber funktionieren solche Lösungen tatsächlich effektiv als Brandschutz, oder werden sie beim nächsten Feuer nicht eher zu Brandbeschleunigern? Denn eine Virenschutzlösung, die mit erhöhten Privilegien arbeitet, kann selbst zur mächtigen Bedrohung werden. Das zeigen am 19.10.2019 und 21.10.2019 gemeldete Schwachstellen (Trend Micro Anti Threat Toolkit) und Einbrüche bei Herstellern von Sicherheitslösungen (NordVPN, Avast) sowie zahlreiche zurückliegende Fälle (SSN 3/2004, SSN 5/2014, SSN 5/2016). Deshalb sollte bei der Entscheidung für eine solche Lösung die mögliche Fehlbarkeit der eingesetzten Produkte in Risiko- und Bedrohungsanalysen sowie Sicherheitskonzepten berücksichtigt werden.

Rechenhilfe

Am 16.10.2019 präsentierte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ihr Modell zur Berechnung von Bußgeldern für Verstöße nach Art. 83 Datenschutz-Grundverordnung (DSGVO). Die Bußgeldbemessung soll damit transparent, systema-

tisch nachvollziehbar und innerhalb der EU harmonisiert werden. Das Konzept nimmt die Bußgeldzumessung in fünf Schritten vor:

- Zuordnung des Unternehmens zu einer von insgesamt 20 Größenklassen
- Bestimmung des mittleren Jahresumsatzes der jeweiligen Größenklasse
- Ermittlung eines wirtschaftlichen Grundwertes (entspricht dem durchschnittlichen Tagessatz)
- Multiplikation dieses Grundwertes mit einem von der Schwere der Tatumstände abhängigen Faktor (1-6 für formelle und 1-12 für materielle Verstöße)
- Anpassung des ermittelten Wertes unter Berücksichtigung täterbezogener und z. B. wirtschaftlicher Umstände

Nach Auffassung der DSK bestärkt dieses Konzept durch die Anknüpfung an den Unternehmensumsatz die Umsetzung des Wunschs des Europäischen Gesetzgebers nach Wirksamkeit, Verhältnismäßigkeit und abschreckender Wirkung gemäß Art. 83 Abs. 1 DSGVO. Das Bußgeldmodell ist also durchaus darauf ausgelegt, den Bußgeldrahmen möglichst umfassend auszuschöpfen.

Konkretisierungen

Der Europäische Datenschutzausschuss (EDSA) hat am 08.10.2019 Version 2.0 der Richtlinie zur „Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung von Online-Diensten“ veröffentlicht. Die Richtlinie enthält vor allem Vorgaben zur Abgrenzung der Erlaubnistatbestände im Bereich Marketing und Online-Dienste. Sie begrenzen die Verarbeitungserlaubnis „Vertrag“ strikt auf die Prozesse, die nach Erwartung des Betroffenen zur Vertragserfüllung erforderlich sind. Bereits die Aufbewahrung von vertragsbezogenen Unterlagen zu Buchhaltungszwecken soll bspw. vor allem nach Vertragsende transparent auf die gesetzliche Pflicht (Art. 6 Abs. 1 c) DSGVO) gestützt werden. Zwecke wie Service-Verbesserung, Werbung in Verbindung mit dem Vertragsgegenstand oder Betrugsabwehr können über das berechtigte Interesse des Verantwortlichen begründet werden, nicht jedoch über den Vertrag. Gewarnt wird davor, Verarbeitungen, die ein Vertrag erforderlich macht, auf Einwilligungen zu stützen, da sich die Rechtsfolgen bezüglich Widerspruch, Löschpflichten u. a. erheblich unterscheiden. Datenverarbeitung beispielsweise zum Zweck individualisierter Werbung als Gegenleistung für ein Leistungsangebot einzufordern ist nach Auffassung des EDSA unzulässig.

Die Richtlinie macht wie die Orientierungshilfe der Datenschutzkonferenz deutlich, dass innerhalb von Verarbeitungsvorgängen nach Zwecken und Rechtsgrundlagen sorgfältig differenziert werden muss, dass diese Differenzierungen Teil der Datenschutzinformationen sein sollen und dass die Rechtsgrundlagen nicht abhängig von der Darstellung austauschbar sind.

Secorvo News

Wissensauffrischung

Schnellentscheidern bieten wir noch zwei Gelegenheiten in diesem Jahr, ihre Kenntnisse in der Informationssicherheit aufzufrischen und zu erweitern: Bei unserem T.I.S.P.-Seminar (**25.–29.11.2019**) sowie dem viertägigen Intensivseminar PKI (**18.–21.11.2019**). Eine Übersicht über alle angebotenen Seminare, Programme und die Termine im Jahr 2020 sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Geliebter Feind – Enemy Mine

Fast täglich kann man in den Medien von Wirtschaftskriminalität, Wirtschaftsspionage und Cybercrime lesen. Was aber verbirgt sich konkret dahinter? Welche Tätertypen gibt es, und warum wird ein Mitarbeiter nach vielen Jahren Betriebszugehörigkeit auf einmal delinquent? Und was meinen Begriffe wie „wirtschaftskriminologisches Belastungssyndrom“ oder „Competitive Intelligence“? Wird man im eigenen Unternehmen mit einem solchen Vorfall konfrontiert, stellen sich viele Fagen: Was ist dem „internen Ermittler“ erlaubt und was nicht? Wann sollten Strafverfolgungsbehörden eingeschaltet werden? Und warum helfen Systeme wie ein IKS nur bedingt gegen Wirtschaftskriminalität?

Auf diese Fragen gibt Andreas Schäfer (VBK) auf dem nächsten KA-IT-Si-Event am **05.12.2019** Antworten und zeigt, wie Unternehmen sich im Vorfeld schützen und – im schlimmsten Fall – verteidigen können. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Alice und Bob im Wunderland

Zu einer Veranstaltung der ganz anderen Art laden wir Sie herzlich zusammen mit dem Forschungszentrum Informatik (FZI) am **14.11.2019** ein. Mit einem Vortrag von Tobias Schrödel über das Darknet und zahlreichen Live-Demos präsentiert Ihnen die IT-Sicherheitsregion Karlsruhe das „Wunderland der IT-Sicherheit“ im Karlsruher Palazzo. Lassen Sie sich von einem wunderbaren Abend verzaubern... Wir empfehlen eine schnelle Anmeldung, da die Zahl der Plätze begrenzt ist.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2019	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
05.-06.11.	9. Handelsblatt Jahrestagung – Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
11.-15.11.	ACM CCS 2019 (ACM/SIGSAC, London/UK)
18.-21.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.11.	43. DAFTA (GDD, Köln)
25.-29.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-29.11.	DeepSec In-Depth Security Conference Europe (DeepSec, Wien/AT)
Dezember 2019	
03.12.	Black Hat Europe 2019 (Blackhat, London/UK)
05.-06.12.	8. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Berlin)
10.12.	GERMAN OWASP DAY 2019 (OWASP Foundation, Karlsruhe)

Fundsache

Nachdem der Heise-Verlag im Frühjahr 2019 Opfer eines Emotet-Angriffs wurde, hat er nicht den Deckmantel des Schweigens über diesen Vorfall gebreitet, sondern ist sowohl mit einer Aufarbeitung als auch einer FAQ zu diesem Thema an die Öffentlichkeit gegangen. Die Erkenntnisse sind lesenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knöppler, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende

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