secorvo
security consulting

Secorvo Security News

Mai 2015

Wir regulieren uns zu Tode

Nicht immer kommt die Bürokratie so unübersehbar daher wie beim Mindestlohngesetz. Dokumentationspflichten, Erklärungen gegenüber Auftraggebern und Verpflichtungen von Auftragnehmern – 99% aller Unternehmen werden wegen einzelner schwarzer Schafe in kollektive Misstrauenshaft genommen.

Ganz Ähnliches ereilt Deutschland in Folge des Sarbanes-Oxley-Act: Die Skandale bei Enron und Worldcom hatten 2002 in den USA eine Welle der Compliance-Regulierung losgetreten. Seitdem sickern regulatorische Kontrollen unternehmerischen Wohlverhaltens in deutsche Unternehmen ein. Wirtschaftsprüfer stellen in wachsendem Umfang auch Anforderungen an den sicheren IT-Betrieb. Mit teilweise skurrilen Resultaten: Keine Prüfung, in der nicht für zentrale IT-Systeme ein regelmäßiger Passwortwechsel spätestens alle 90 Tage gefordert wird. Von dem eigentlichen Zweck (Begrenzung des Schadens, sollte ein Passwort kompromittiert sein) hat sich diese Regelung längst befreit – denn Benutzer wählen Passwörter, denen sie eine einfache Bildungsregel mitgeben, wie z. B. eine Ziffer am Ende. Ein Angreifer kennt daher mit einem Passwort auch alle folgenden – und wir quälen alle 90 Tage eine wahrscheinlich 8stellige Zahl von IT-Nutzern mit einem Sinn entleerten Ritual, das sogar die Passwortkomplexität senkt. Ähnliches könnte uns nun mit dem IT-Sicherheitsgesetz bevorstehen – und auch die Vorratsdatenspeicherung wird nicht ohne Auswirkungen auf die Compliance-Anforderungen in Unternehmen bleiben (siehe die Beiträge in diesen SSN).

Manchmal ist es unvermeidlich, dass politisch oder gesellschaftlich gewünschtes Verhalten gesetzlich erzwungen wird. Die durch Detailregulierung entstehenden Bürokratiekosten dürften jedoch – bei aller Sympathie für die IT-Sicherheit – die verhinderten Schäden um ein Vielfaches übersteigen. Wer in erster Linie wirtschaftlichen Schaden von Unternehmen abwenden will, sollte die IT-Sicherheit daher besser der Selbstregulierung und Haftung überlassen.

Inhalt

secorvo
security consulting

Security News

Das BAG und die Einwilligung

Dass die Einwilligung nur in speziellen Ausnahmefällen als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten taugt ist herrschende Meinung unter Datenschützern.

Das Bundesarbeitsgericht hat sich nun in einem Urteil vom 11.12.2014 – eher beiläufig – zu dieser Frage geäußert. So gebe der Arbeitnehmer mit Eingehen des Arbeitsvertrags nicht seine Persönlichkeitsrechte auf. Eine Benachteiligung aufgrund einer Einwilligungsverweigerung stelle einen groben arbeitgeberseitigen Nebenpflichtverstoß und einen Verstoß gegen das Maßregelungsverbot aus § 612a BGB (Verbot der Benachteiligungen wegen einer zulässigen Rechteausübung) dar. Arbeitnehmer könnten sich auch im Arbeitsverhältnis frei entscheiden, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben.

Eine Revolution steht trotzdem nicht bevor: Zwar stellt das BAG auch die Widerruflichkeit einer Einwilligung unter den Vorbehalt einer Interessensabwägung. Es verleiht damit aber der Einwilligung trotzdem nicht die praktisch notwendige Stabilität.

Zudem sind an der Argumentation des BAG Zweifel angebracht: Bereits die Befürchtung, der Arbeitgeber könne aufgrund der Verweigerung benachteiligen, ohne dass der Zusammenhang nachweisbar ist, kann die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis erheblich einschränken. Der Verweis auf späteren Rechtsschutz ist sehr formal und verkürzt den Schutz der Informationellen Selbstbestimmung erheblich.

Seiteneffekt der Vorratsspeicherung

Am 27.05.2015 hat das Bundeskabinett den Gesetzentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten – kurz: die Vorratsdatendatenspeicherung – beschlossen. Die Diskussion über die Verfassungsmäßigkeit des neuen Anlaufs ist nun in vollem Gange.

Aus Sicht der Informationssicherheit ist jedoch von Interesse, wie die Bundesregierung die Mahnung des Bundesverfassungsgerichts umgesetzt hat, den Schutz der Daten zu regeln. Der Entwurf kommt dieser Anforderung in den vorgeschlagenen §§ 113d ff TKG nach. Vorgesehen sind – in Ergänzung zu § 109 TKG – u. a. der Einsatz eines „besonders sicheren Verschlüsselungsverfahrens“, die Speicherung in getrennten Speichereinrichtungen, das „Vier-Augen-Prinzip“ für den Zugriff und eine Zugriffsprotokollierung von einem Jahr über Zeitpunkt, Akteure, Zweck und Art des Zugriffs.

Die Bundesnetzagentur soll in Abstimmung mit dem BSI und der Bundesdatenschutzbeauftragten einen ergänzenden Anforderungskatalog erstellen. Das Sicherheitskonzept der Provider nach § 109 Abs. 4 TKG ist entsprechend zu ergänzen. Ein mangelnder Schutz soll Geldstrafen bis zu 500.000 € nach sich ziehen.

Sollte der Entwurf Gesetz werden, könnte dies weit reichende Auswirkungen auf andere Verarbeitungen besonders schutzwürdiger Daten haben: Die Sicherheitsvorgaben setzen hier einen neuen Maßstab. Mit Spannung darf man daher den Anforderungskatalog der BNetzA erwarten – vor allem in Bezug auf die in § 113b Abs. 8 TKG n.F. geforderte irreversible Löschung oder die Kriterien für ein „besonders sicheres Verschlüsselungsverfahren“.

Wirkungen von Datensicherheit

Häufig sind es die Nebenfolgen, der die wahre Bedeutung eines Urteils ausmachen. So auch bei einem Urteil des Landesarbeitsgerichts Schleswig-Holstein vom 04.03.2015, das die Aufhebung einer Kündigung bestätigt, die gegen ein Betriebsratsmitglied wegen des Verstoßes gegen die Verschwiegenheitspflicht ausgesprochen worden war. Das Betriebsratsmitglied hatte Rechtsanwaltsrechnungen zu betriebsverfassungsrechtlichen und individualarbeitsrechtlichen Beratungen an den betroffenen Betriebsrat eines verbundenen Unternehmens weitergegeben.

Das Landesarbeitsgericht sah hierin keinen die fristlose Kündigung rechtfertigenden Verstoß. Denn die Zugriffsrechte des Gekündigten waren nicht eingeschränkt und es fehlte eine Kennzeichnung des Geheimhaltungsbedarfs an den Dokumenten.

Das Urteil verdeutlicht die rechtliche Bedeutung von IT-Sicherheitsmaßnahmen: Sie begründen bereits durch ihre Existenz rechtlichen Schutz und erzeugen auch rechtliche Wirkungen. Aus diesem Grund sollte selbst auf überwindbare technische und organisatorische Maßnahmen und eine Geheimhaltungsklassifizierung nicht verzichtet werden.

Schriftform bei Mitarbeiterfotos

Wollen Arbeitgeber Fotos oder Videos ihrer Mitarbeiter veröffentlichen, bedarf dies nach § 22 Kunsturhebergesetz (KUG) in der Regel der Einwilligung der Arbeitnehmer. Das Gesetz sieht für diese Einwilligung keine besondere Form vor. Tatsächlich setzen Unternehmen oft auf ein „lautes Nicken“ – die für einen Werksausweis angefertigten Fotos werden so oft wie selbstverständlich in das elektro-

nische Telefonverzeichnis aufgenommen und auf die Webseite gestellt.

Das Bundesarbeitsgericht (BAG) hat nun mit Urteil vom 11.12.2014 (Az. 8 AZR 1010/13) schärfer als die Forderung des KUG entschieden, dass eine ausdrückliche – also in der Regel schriftliche – Einwilligung der betroffenen Arbeitnehmer erforderlich ist. Anlass war ein Werbefilm im Internet, in dem Mitarbeiter einige Sekunden lang gezeigt wurden. Gleichzeitig stellte das BAG fest, dass eine formal korrekte Einwilligung nicht automatisch mit Beendigung des Arbeitsverhältnisses erlischt, sondern der Widerruf vielmehr eines plausiblen Grundes bedarf – zumindest dann, wenn nicht die Person des Mitarbeiters im Vordergrund steht.

Für die Fotos auf Werksausweisen wird man auch weiterhin von überwiegenden Sicherheitsinteressen des Unternehmens ausgehen können. In den meisten anderen Fällen der Veröffentlichung müssen Unternehmen schriftliche – und zweckbezogene – Einwilligungen einholen. Dies gilt für das Internet gleichermaßen wie für das Intranet. Eine unspezifische Generaleinwilligung in Arbeitsverträgen scheidet aus – solche Klauseln scheitern meist am AGB-Recht.

Security-Adventure

Die Spieler von „Gezielter Angriff – Das Spiel“, einem am 05.05.2015 veröffentlichten kostenlosen Online-Lernspiel des japanischen IT-Sicherheitsanbieters Trend Micro, schlüpfen in die Rolle des CIOs der fiktiven Firma „The Fugle“. Er hat ein beschränktes Budget und muss im Spiel das Geld in sinnvolle und angesichts der aktuellen Risiken angemessene Projekte investieren.

Seine Entscheidungen beeinflussen den weiteren Verlauf der Spiels, bis es schließlich zu einem gezielten Angriff kommt. Spieler, die den Angriff nicht mehr verhindern können, erhalten eine Analyse ihrer Handlungsschritte und Hinweise, wie sie das Spiel beim nächsten Mal in die richtige Richtung lenken können.

Ein interessanter Ansatz, um die Sensibilität für IT-Sicherheit zu steigern und zugleich ein gesundes Verständnis für angemessene Schutzmaßnahmen zu vermitteln. Das Spiel ist kostenlos, die Spieler müssen keine persönlichen Daten preisgeben.

Secorvo News

Kompetenz darf sich auszahlen

In diesen Tagen wird das 750ste T.I.S.P.-Zertifikat ausgestellt. Es belegt neben der mindestens dreijährigen Berufserfahrung im Gebiet IT-Sicherheit vertiefte Kenntnisse in allen relevanten Teilgebieten der Informationssicherheit – von rechtlichen Anforderungen über Public Key Infrastrukturen bis zur Sicherheit mobiler Endgeräte.

In unseren fünftägigen T.I.S.P. Schulungen erhalten Sie einen kompakten Überblick über alle für die Zertifizierung relevanten Wissensgebiete. Zur Vorbereitung schicken wir Ihnen vorab das von uns verfasste 700seitige Begleitbuch zum T.I.S.P. („Zentrale Bausteine der Informationssicherheit“, 2. Auflage 2014).

2015 geben wir Ihnen noch drei Mal die Gelegenheit das T.I.S.P.-Zertifikat zu erwerben: im Juni (**22.–26.06.**), September (**21.–25.09.**) und November (**23.–27.11.**). Sichern Sie sich Ihren Platz!

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Mehr Sicherheit im Mittelstand

Über 100 Verantwortliche für Datenschutz und IT-Sicherheit aus Unternehmen der TechnologieRegion Karlsruhe folgten am 19.05.2015 den Praxisberichten und Expertenvorträgen auf dem 7. Tag der IT-Sicherheit in Karlsruhe. Wer die Veranstaltung verpasst haben sollte, findet die Pressemitteilung und die Vortragsunterlagen (zu den Themen Risiko Mensch und Technik, Aktuelle Entwicklungen zu ‚Privacy by Design‘, Sicherheit im Always-On, Designprinzipien für sichere Systeme, Intrusion Prevention Systeme) ab sofort auf http://www.tag-der-it-sicherheit.de.

Das nächste Event der Karlsruher IT-Sicherheitsinitiative findet statt am **16.07.2015** im Panoramasaal der IHK Karlsruhe. Dort wird Dominik Schadow über Java-Security sprechen – wer ‚Java‘ sagt, sollte auch ‚sichere Softwareentwicklung‘ meinen …

Veranstaltungshinweise

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

Juni 2015	
08.-12.06.	Audit Challenge 2015 (Frankfurt School of Finance & Management, Frankfurt)
15.-16.06.	DuD 2015 (COMPUTAS Gisela Geuhs GmbH, Berlin)
19.06.	Workshop: Social Media Security (Fachgruppe SECMGT der Gesellschaft für Informatik e.V., Frankfurt)
22.-26.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)>
August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)

Fundsache

Am 12.01.2015 hat die ENISA einen 78seitigen Report „Privacy and Data Protection by Design" veröffentlicht. Darin versuchen die Autoren, die rechtlichen Anforderungen und technischen Möglichkeiten in Überdeckung zu bringen. Lesenswert sind die „Eight Privacy by Design Strategies" und der profunde Überblick über aktuelle Privacy Enhancement Technologies. 211 Referenzen belegen die breite fachliche Abdeckung.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, 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