Datenschutz und IT-Sicherheit

Harmonie des vermeintlich Unvereinbaren

Die gängige Vorstellung der meisten Datenschutzbeauftragten beziehungsweise IT-Sicherheitsbeauftragten ist, dass die beiden Aufgaben Datenschutz und IT-Sicherheit in einem Unternehmen oder in einer Behörde unvereinbar sind. Damit müssten die beiden entsprechenden Beauftragten ständig im Clinch liegen. Der Datenschutzbeauftragte predigt Datenvermeidung und kämpft gegen jede Art von Protokollierung – der IT-Sicherheitsbeauftragte fordert vollständige Überwachung und ist bestrebt, die „schwarzen Schafe" zu erwischen. Bei Beachtung einiger Punkte ist jedoch sehr wohl ein kollegiales Miteinander möglich [1].

Einer der Knackpunkte, die immer wieder für Zündstoff zwischen Datenschutz- und IT-Sicherheitsbeauftragtem sorgen, sind Datensammlungen in Form sogenannter Protokolldateien. Protokolldaten sind dabei in § 2 Abs. 8 BSI-Gesetz [2] präzise definiert als „Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind". Dabei können Protokolldaten Verkehrsdaten im Sinne des § 3 Nr. 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Abs. 1 des Telemediengesetzes enthalten. Die Protokolldaten sind dann besonders zu schützen.

Um an diesem Punkt ein besseres Verständnis für den IT-Sicherheitsbeauftragten zu bekommen, muss man sich sein Selbstverständnis nochmals genauer anschauen. Die IT-Sicherheit hat mehrere Ziele. Im Idealzustand will man Sicherheitsvorfälle verhindern. Dabei umfasst der Begriff „Sicherheitsvorfälle" ein weites Spektrum: Hackerangriffe, unberechtigter Zugriff auf Daten und unberechtigtes Kopieren von Daten, Sabotage der IT und vieles mehr. Nun wird man Sicherheitsvorfälle nicht immer verhindern können, wie aktuell leider immer wieder zu beobachten (zum Beispiel Sony, RSA, Rewe und andere), aber man möchte sie in dem Fall doch zumindest erkennen. „Im Jahr 2010 wurden allein 2108 ‚Elektronische Angriffe' auf Bundesbehörden festgestellt (2009: 1511)", heißt es dazu im Verfassungsschutzbericht 2010 [3]. Es ist aus dem Kontext leider nicht klar, ob hier „abgewehrt" oder nur „bemerkt" gemeint ist.

Das Abwehren eines Angriffs beziehungsweise das Verhindern eines Vorfalls kann – zumindest theoretisch – ohne das Erheben eines Protokolls erfolgen. In der Praxis wird man abgewehrte Angriffe trotzdem protokollieren, zum einen um die Wirksamkeit der Abwehrmaßnahmen zu belegen, zum anderen um einen Überblick zu bekommen, was im Netz vor sich geht. Fragen wie „Nimmt die Zahl der Angriffe zu?", „Welche Angriffe erfolgen?" etc. müssen beantwortet werden können. Dazu sind anonyme Protokolle völlig ausreichend.

Für das Erkennen des nicht abgewehrten Angriffs und das nachträgliche Erwischen des Übeltäters sind allerdings entsprechende personenbezogene Protokolle nötig. Der Angriff muss über die Protokolldateien dem Angreifer zugeordnet werden – dem Außentäter, um ihn der Strafverfolgung zuzuführen, dem Innentäter, um angemessen arbeitsrechtliche Maßnahmen ergreifen zu können.

Im Datenschutz gibt es die Vorgaben der Datenvermeidung und der Datensparsamkeit (§ 3a BDSG). Daraus wird oft schnell ein Protokollierungsverbot abgeleitet. Viele übersehen, dass das BDSG sogar Protokollierung fordert. Denn wenn es erforderlich ist, dass „nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind" (Nr. 5 der Anlage zu § 9 BDSG), ist dies nicht ohne entsprechende Protokollierung der Beschäftigtenaktivitäten möglich. Die „Protokollpflicht" wird durch die strenge Zweckbindung der Protokolldateien nach § 31 begleitet. Alle Protokolle, die im Rahmen der IT-Sicherheitsmaßnahmen eines Unternehmens oder einer Behörde erstellt werden, fallen unter diese Zweckbindung.

Dieses Konzept lässt sich hervorragend

Protokollierung dient der nachträglichen Erkennung und nicht der Verhinderung. Lediglich bei Innentätern (Bewertung in Klammern) kann die „Angst vor dem Erwischtwerden" eventuell zur Verhinderung durch Protokollierung beitragen.

Verhindern der privaten Nutzung	👎 (👍)
Verhindern von Straftaten	👎 (👍)
Urheberrechtsverstöße durch Verbreiten	👎 (👍)
Herunterladen (Kinder-)Pornographie	👎 (👍)
Abwehr von Hackern	👎
Abwehr von Wirtschaftsspionage	👎
Schutz vor Viren	👎

nutzen, um eine innerbetriebliche oder innerbehördliche Regelung zur Protokollierung im IT-Sicherheitsbericht zu schaffen, die den Interessen beider Seiten gerecht wird. Eine Regelung zur Protokollierung könnte beispielsweise so aussehen:

Die IT-Sicherheitsbeauftragte darf zur Abwehr von Gefahren für die Informations- und Kommunikationstechnik (IuK-Technik) des Unternehmens/der Behörde

1. Protokolldaten, die beim Betrieb der IuK-Technik des Unternehmens anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der IuK-Technik des Unternehmens oder von Angriffen auf die IuK-Technik des Unternehmens erforderlich ist,

2. die an den Schnittstellen nach außen der IuK-Technik des Unternehmens anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

Sofern nicht andere innerbetriebliche/innerbehördliche Regelungen eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen. Ferner müssen diese Daten nach erfolgtem Abgleich sofort und spurenlos gelöscht werden.

Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der gespeicherten Daten nur automatisiert erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der entsprechenden Regelungen zulässig.

Daten, die beim Betrieb aus diversen Gründen (Ordnungsmäßigkeit, Abrechnung etc.) erhoben werden, dürfen auch ausgewertet werden. Die Verarbeitung muss so gestaltet sein, dass das gewünschte Ergebnis so schonend wie möglich erreicht wird. Eine Maßnahme, dies zu gewährleisten, ist die Verpflichtung zur zeitnahen automatischen Auswertung. Der IT-Sicherheitsbeauftragte hat keinen Zugriff auf die Rohdaten, sondern er bekommt nur das Ergebnis der Auswertung. Ein manuelles Suchen in den Rohdaten unterbleibt und dubiose Erkenntnisse über das Einzelverhalten von Beschäftigten sind nicht möglich.

Der Regelungsvorschlag stammt im Übrigen aus dem von vielen extrem kritisierten BSI-Gesetz [2]. Die Änderungen zur Anpassung an die betriebliche oder behördliche Übung sind nur gering. Konkret handelt es sich um die Absätze 1 und 2 des § 5.

Eine weitere Möglichkeit zum datenschutzfreundlichen Umgang mit Protokollierung wurde vom Autor und einem Kollegen entwickelt [4]. In diesem Fall schreibt eine Firewall ein Protokoll, das nur einen unvollständigen Datensatz (nur die Quellinformationen der IP-Verbindung, die Zielinformationen fehlen) enthält. Erst mit zusätzlichen Informationen eines externen Beschwerdeführers (der die fehlenden Zielinformationen liefert) entsteht ein vollständiger Datensatz, der es erlaubt, konkrete Personen zu identifizieren.

Fazit

Der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte können konfliktfrei nebeneinander ihre Aufgaben erfüllen. Der Datenschutzbeauftragte ist zur Umsetzung technischer Schutzmaßnahmen auf das Fachwissen und die Technik des IT-Sicherheitsbeauftragten angewiesen und der IT-Sicherheitsbeauftragte benötigt die Fachkunde der Datenschutzschutzbeauftragten, denn nur (datenschutz-)rechtlich sauber erhobene und verarbeitete Daten können anschließend auch verwendet werden.

Im Rahmen von IT-Sicherheitsmaßnahmen darf gespeichert werden, was erforderlich ist. Dabei ist ein strenger Maßstab an das „erforderlich" anzulegen. Bei korrekter Beurteilung der Erforderlichkeit ist auch den Maßgaben des Datenschutzbeauftragten Genüge getan – gegebenenfalls ist sogar eine gemeinsame Festlegung der Erforderlichkeit denkbar. Auf alle Fälle gilt: Die Daten werden nur so lange gespeichert wie für den Zweck erforderlich – nach der Auswertung werden sie sofort gelöscht. ■

[1] R.W. Gerling, IT-Sicherheit und Datenschutz: Ein Widerspruch?, Datenschutz und Datensicherheit (DuD), 29 (2005) 338 – 339

[2] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI-Gesetz, vom 14. August 2009 (BGBl. I S. 2821).

[3] Bundesministerium des Innern, Verfassungsschutzbericht 2010, http://www.verfassungschutz.de, abgerufen am 24.7.2010.

[4] R.W. Gerling und Thomas Blaß, Diskrete Logs: Datenschutzfreundliche Protokollierung, ADMIN-Magazin, 04/2011, Seite 54 – 55.

Prof. Dr. Rainer W. Gerling,
Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft