In vielen größeren Unternehmen und Behörden gibt es sie: IT-Sicherheitsbeauftragte. Aber was bedeutet dieser Titel konkret?

1. *Müssen Unternehmen/Behörden bestimmter Größe einen IT-Sicherheitsbeauftragten haben? Welche (gesetzlichen) Regelungen/Empfehlungen gibt es?*

   Gesetzlich vorgeschrieben ist die Bestellung eines IT-Sicherheitsbeauftragten nur für Telekommunikationsunternehmen. Eine entsprechende Bestimmung findet sich in § 166 Abs. 1 Nr. 1 TKG. Für alle übrigen Unternehmen und Behörden gelten nur die allgemeinen Vorschriften, wonach die Vorstände und Geschäftsführer, die Dienststellenleiter und die sonstigen Verantwortlichen für die Sicherheit der IT zu sorgen haben. Verhindert werden sollen dabei nicht nur unbefugte Zugriffe durch Dritte (die ggf. Betriebsgeheimnisse auskundschaften wollen). Vielmehr geht es insbesondere um die Abwehr von Angriffen, die das System lahmlegen und so die weitere Arbeit unmöglich machen wollen. Besonders bedeutsam ist dies für die sog. kritische Infrastruktur: Wenn Saboteure das Wasserwerk oder das E-Werk lahmlegen, können die Konsequenzen für die Bevölkerung verheerend sein. Insoweit gibt es Regelwerke des BSI (=Bundesamt für die Sicherheit in der Informationstechnik), die auch für andere Unternehmen von Interesse sind, die aber keine rechtliche Verbindlichkeit besitzen. Weiter kann man sich gegen „Datenklau“ und „Attacken“ nur versichern, wenn bestimmte Voraussetzungen erfüllt sind, die von der Versicherungswirtschaft aufgestellt wurden. In allen diesen „Regelwerken“ ist auch die Schaffung eines IT-Sicherheitsbeauftragten vorgesehen.

2. *Wer kann/sollte IT-Sicherheitsbeauftragter sein? (Bestimmte Qualifikation, Ausbildung, Zertifizierung)*

   IT-Sicherheitsbeauftragter, auch ISB (=Informationssicherheitsbeauftragter) genannt, sollte eine Person sein, die sich in der IT auskennt und die insbesondere auch Kenntnisse über mögliche Sicherheitslücken mitbringt. Woher ein Kandidat sein Wissen hat, muss nicht weiter interessieren, sofern an seiner persönlichen Zuverlässigkeit keinerlei Zweifel bestehen. Es muss sich um einen loyalen Mitarbeiter handeln, der weiß, was auf dem Spiel steht. Eine spezifische Ausbildung oder eine besondere staatliche Zertifizierung gibt es nach meiner Kenntnis nicht – was nicht ausschließt, dass private Einrichtungen derartige Bescheinigungen ausstellen, über deren Bedeutung man ggf. Erkundigungen einziehen muss.

3. *Was sind die Aufgaben eines IT-Sicherheitsbeauftragten?*

   Die Aufgaben werden meist in „anfängliche“ und „laufende“ aufgeteilt. Die aufwendigeren sind die anfänglichen: Es muss eine Risikoanalyse erstellt und auf dieser aufbauend ein Sicherheitskonzept entwickelt werden. Weiter ist ein „Notfallplan“ auszuarbeiten, der dann greift, wenn die Sicherheitsmaßnahmen versagen: Was kann man z. B. tun, wenn Hacker das betriebliche System lahmlegen und versprechen, es wieder verfügbar zu machen, wenn sie eine bestimmte Summe an Bitcoins erhalten? Gegen Erpressungen dieser Art kann man sich schützen, wobei die vorgesehenen Maßnahmen möglichst wenigen Personen bekannt sein sollten. Die „laufenden“ Aufgaben bestehen in einer regelmäßigen Überwachung der IT und insbesondere in der „Feindbeobachtung“; Angreifer entwickeln häufig neue Methoden, auf

die man sich rechtzeitig einstellen sollte. Auch kann es kleinere „Sicherheitsvorfälle“ geben, die man untersuchen muss, um Wiederholungen zu vermeiden.

4. *Wie bestimmt sich das Verhältnis von IT-Sicherheitsbeauftragten und Datenschutzbeauftragten? Ist eine Personalunion möglich/sinnvoll?*

   Die Aufgaben des betrieblichen Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten überschneiden sich zum Teil: Beide ziehen etwa an einem Strang, wenn es darum geht, den Zugriff durch Unbefugte zu verhindern. Wenn es um die Erarbeitung und Überwachung eines Sicherheitskonzepts geht, haben sie jedoch verschiedene Rollen: Der IT-Sicherheitsbeauftragte braucht möglichst umfassende Informationen über alle betrieblichen Abläufe, der Datenschutzbeauftragte muss dafür sorgen, dass möglichst wenige Personen Zugriff auf die vorhandenen Daten haben. Dies schließt es im Allgemeinen aus, dieselbe Person mit beiden Aufgaben zu betrauen, weil sonst Interessenkollisionen entstehen können.

   Aus der Praxis kommt außerdem der Rat, den IT-Sicherheitsbeauftragten nicht zum Teil der IT-Abteilung zu machen. Dies deshalb, weil Sicherheitsanforderungen häufig mehr Arbeit verursachen und außerdem die Alltagstätigkeit komplizierter machen können, was dem „Eigeninteresse“ der IT-Abteilung widerspricht. Deshalb sollte der IT-Sicherheitsbeauftragte verselbständigt und direkt einem Vorstandsmitglied oder Geschäftsführer unterstellt werden. Dies würde ihm ein wenig mehr Unabhängigkeit geben. Freilich hat er auch dann immer noch eine sehr viel schwächere Stellung als der betriebliche Datenschutzbeauftragte: Mangels gesetzlicher Regelung gibt es keine Bestimmung, die ihn bei der Ausübung seiner „Fachkunde“ unabhängig von Weisungen macht oder die ihm gar einen besonderen Kündigungsschutz verleiht. Der Schutz von personenbezogenen Daten wird offensichtlich als wichtiger angesehen als der Schutz gegen die Lahmlegung ganzer IT-Systeme – aus meiner Sicht eine ziemlich verquere Herangehensweise, die vielleicht ein wenig mit der deutschen Tradition zusammenhängt, die Persönlichkeit der „Dichter und Denker“ in besonderem Maße zu hegen und zu pflegen. Dass ohne Wasser und Strom auch der Persönlichkeitsschutz leidet, sollte man etwas mehr ins Bewusstsein rücken.

5. *Dürfen IT-Sicherheitsbeauftragte in den BR/PR gewählt werden? (Interessenkonflikt? Doppelrolle? Ist das sinnvoll?)*

   Bisher ist nach meiner Kenntnis dieser Fall nicht aufgetreten. Das BAG hat ja vor nicht allzu langer Zeit die Unvereinbarkeit der Rolle eines Datenschutzbeauftragten mit der eines Betriebsratsvorsitzenden angenommen: Der Datenschutzbeauftragte müsse mitberaten, wenn es um die datenschutzrechtliche Zulässigkeit von Auskunftsersuchen des Betriebsrats gehe. Insoweit müsse er sich selbst kontrollieren, was nicht hinnehmbar sei. Der IT-Sicherheitsbeauftragte hat zwar eine andere Aufgabe, doch kann auch hier das Problem auftauchen, dass er aus Gründen der IT-Sicherheit Bedenken gegen die Weitergabe einer Information an den Betriebsrat hat. Von daher ist damit zu rechnen, dass im Streitfalle genauso wie beim Betriebsratsvorsitzenden entschieden und eine Unvereinbarkeit angenommen wird.

6. *Welche Rechte haben die Gremien bezüglich des IT-Sicherheitsbeauftragten?*

   Hier muss man unterscheiden. Handelt es sich um eine Person, die schon bisher im Unternehmen beschäftigt ist, so liegt in der Übertragung der Aufgaben eines IT-Sicherheitsbeauftragten in der Regel eine Versetzung im Sinne des § 95 Abs. 3 BetrVG. Diese löst die Rechte aus § 99 BetrVG aus: Der Betriebsrat kann aus bestimmten, in § 99 Abs. 2 BetrVG aufgeführten Gründen der Versetzung widersprechen, doch liegen diese Gründe in der Praxis nur selten vor. Genauso ist die Situation, wenn ein von außen Kommender als Beauftragter eingestellt wird; auch dann greift § 99 BetrVG ein. Wäre der IT-Sicherheitsbeauftragte ein leitender Angestellter, so wäre nach § 105 BetrVG der Betriebsrat lediglich zu informieren. Dies würde aber voraussetzen, dass der Beauftragte selbst unternehmerische Teilaufgaben in eigener Verantwortung erfüllt, was nur ganz ausnahmsweise der Fall sein wird.

7. *Dürfen IT-Sicherheitsbeauftragte die Gremien kontrollieren?*

   Die Frage ist im Verhältnis zwischen Betriebsrat und betrieblichem Datenschutzbeauftragtem in § 79a BetrVG nicht mit letzter Klarheit entschieden. Beim IT-Sicherheitsbeauftragten fehlen – wie immer – gesetzliche Bestimmungen. Insoweit muss man auf allgemeine Prinzipien zurückgreifen. Wichtig ist dabei der Grundsatz der Unabhängigkeit des Betriebsrats vom Arbeitgeber: Sie darf nicht dadurch in Gefahr geraten, der ein Beauftragter des Arbeitgebers in die Daten des Betriebsrats Einsicht nimmt und so dessen Überlegungen und Strategien der Gegenseite zur Kenntnis kommen können. Soweit diese Eigensphäre des Betriebsrats nicht berührt ist, bestehen keine Bedenken, dass Sicherheitsvorkehrungen auch für den Betriebsrat obligatorisch gemacht werden. Der IT-Sicherheitsbeauftragte kann daher z. B. überprüfen, ob die im Betrieb als verbindlich angeordnete Verschlüsselungstechnologie auch vom Betriebsrat durchgehend benutzt wird. Dies muss allerdings in einer Weise geschehen, dass der Beauftragte keine Kenntnis von den Inhalten der vom Betriebsrat ausgehenden und der an ihn gesandten Sendungen erhält. Bei gutem Willen lassen sich IT-Sicherheit und Datenschutz sowie Unabhängigkeit des Betriebsrats durchaus in Einklang bringen.

   Interview mit Prof. Dr. Wolfgang Däubler, Universität Bremen