Zusätzliche Sicherheitsmaßnahmen in Zeiten von Prism & Co bieten neben der Separierung vom Windows-Betriebssystem der integrierte Smartcard-Leser und das PIN-Pad. Dadurch erfolgt die Eingabe der PIN für die Authentisierung mittels Smartcard nicht über die PC-Tastatur, sondern komfortabel über die Spezialtastatur auf der Box. Danach stehen dem Benutzer über LAN, WLAN oder 3G via Virtual Private Network (VPN) alle Anwendungen und Ressourcen aus dem zentralen Datennetz zur Verfügung. Eine integrierte Firewall schützt die VPN-Box und das angeschlossene Endgerät zusätzlich vor Angriffen aus dem Internet.

Weitere Informationen: *https://www.ncp-e.com/de/produkte/vpn-govnet-box.html* und *https://www.sit.fraunhofer.de/de/news/aktuelles/pressemitteilungen/details/news-article/abhoersicherheit-in-a-box/*

Rezensionen

Bücher

Marie-Theres Tinnefeld

Rieder, Stefan: Whistleblowing als interne Risikokommunikation. Ausgestaltung eines unternehmensinternen Whistleblowing-Systems aus arbeits- und datenschutzrechtlicher Sicht. Dike Verlag AG, Zürich St. Gallen 2013; ISBN 978-3-03751-490-0

Mit dem etwas reißerischen Titel „Bloß keine Helden" stellen Thomas Gröbner, Philipp Kurbel und Benedikt Winkel in der SZ (12./13.09 2013, V3/3) fest: „Sie werden versetzt, verklagt oder entlassen. Whistleblower decken am Arbeitsplatz auf, was verborgen bleiben sollte. Deshalb brauchen sie rechtlichen Schutz – und könnten so ihren Heldenstatus verlieren." Die Autoren der SZ dokumentieren die brisante und rechtlose Stellung von Whistleblowern in Deutschland. Rieder geht in seiner Dissertation der arbeits- und datenschutzrechtlichen Einordnung von Whistleblowern in der Schweiz mach. Er sieht durchaus die Folie, auf der Whistleblower in öffentlichen oder privaten Unternehmen als „Held oder Denunziant" apostrophiert zu werden. Der Autor kommt zu der Erkenntnis, dass „internes Whistleblowing ein „nutzenstiftendes Compliance-Instrument ist und als Programm für den Umgang mit Risiken im Unternehmen angesehen werden muss". In vier Teilen nähert er sich systematisch und praxisorientiert u.a. unter Heranziehung einer empirischen Untersuchung in 16 Unternehmen, darunter 9 Banken und 7 Versicherungen dem Thema. Im 1.Teil befasst er sich grundsätzlich mit dem Phänomen Whistblowing und erläutert sorgfältig Merkmale, die die Person eines Whistleblowers, der „Verantwortungsgefühl" zeigt, ausmachen. Er untersucht umfassend die Anforderungen, die für eine Offenlegung von Missständen zu sehen sind. Insbesondere grenzt er den Whistleblower auch vom investigativen Journalisten ab. Der Autor unterscheidet deutlich die Qualität von anonymen, vertraulichen und offenen Whistleblowing, die auch datenschutzrechtlich für Betroffene eine Rolle spielen, z.B. im Falle von etwaigen Rückfragen der „Angezeigten". Der Kampf mit offenen Visier kann aber auch gefährlich sein wie der aktuelle Fall des Whistleblowers E. Snowden zeigt. Im 2. Teil stellt der Autor die rechtlichen Grundlagen vor. Er stellt zunächst den Prozess dar, den der Whistleblower durchläuft bevor er tätig wird, er untersucht die Meldepflicht als Bestandteil seiner Treuepflicht als Arbeitnehmer und er betrachtet den Adressaten, grundsätzlich also den Arbeitgeber, den seinerseits eine Fürsorgepflicht trifft. Als Rechtsgrundlage des Melderechts hebt Rieder (so auch der EGMR) das Grundrecht auf Meinungsäußerungsfreiheit in Art. 10 EMRK hervor, an dem auch nationale Grundrechte in Europa zu messen sind. Sein besonderes Augenmerk richtet der Autor auf den Schutz des Whistleblowers vor einer missbräulichen Kündigung und Diskriminierung. Er beklagt einen effektiven Schutz, den es auch in Deutschland (noch) nicht gibt. Rieder leitet allerdings aus der Fürsorgepflicht des Arbeitgebers ab, eine unabhängige Whistleblowing-Stelle einzurichten, die „Meldungen vertraulich entgegennimmt und die Identität des Whistleblowers schont". Abschließend wird im 3. Teil nicht nur die empirische Untersuchung zum internen Whistleblowing, sondern auch die Nutzung von implementierten Whistleblowing-Systemen ausgewertet. Das Ergebnis sei grundsätzlich als positiv zu bezeichnen. Der Autor setzt auf eine Selbstregulierungsorganisation, die den Umgang mit Meldungen in Meldestellen für die Praxis aufbereitet. In einem zusammenfassenden 4. Teil stellt er Empfehlungen für Unternehmen auf der Basis seiner gewonnen Erkenntnisse auf und veröffentlicht eine themenbezogene Übersicht über das methodische Vorgehen bei der Untersuchung: Tabellarische Übersicht über die Meldepflichten (Anhang 1), Vor- und Nachteile eines Whistleblowing-Systems (Anhang 2), Implementierung eines Whistleblowing-Systems (Anhang 3), Checkliste Whistleblowing-Reglement (Anhang 4), Muster Whistleblowing-Reglement mit einschlägigen Datenschutzbestimmungen (Anhang 5), Fragebogen, Umfragen zum unternehmensinternen Whistleblowing (Anlage 6), Teilnehmer der Umfrage (Anhang 7). Begleitschreiben zur Umfrage (Anhang 8) und (detaillierte) Auswertung der Experteninterviews (Anhang 9). Zu Beginn der Besprechung wurde bereits die SZ zitiert, die zutreffend den arbeitsrechtlichen Notstand verantwortungsbewusster Whistlerblower anspricht. Die vorliegende Arbeit stellt das Problem sachgerecht dar und versucht, angemessene Lösungen voranzutreiben, die den arbeitsrechtlichen Interessen und den datenschutzrechtlichen Anforderungen Rechnung tragen. Die Ausführungen sind auch für die deutsche Praxis, insbesondere aber auch für den deutschen Gesetzgeber von Interesse. Die Forderung einer Selbstregulierungsorganisation ist zwar ein effektiver Ansatz zur Regelung des Whistleblowing. In jedem Fall sollte aber eine besondere Schutznorm in einem (noch) immer zu schaffenden deutschen Beschäftigungsdatenschutzgesetz erfolgen. Bei der vorliegenden Dissertation finden sich Eckpunkte für eine angemessene Regelung.