1. Record Nr. UNINA9910557238003321

Autore	Bittner Marc-Philipp
Titolo	Cybersecurity als Unternehmensleitungsaufgabe / Marc-Philipp Bittner, Anabel Guntermann, Christoph Benedikt Muller, Darius Rostam . Volume 2
Pubbl/distr/stampa	Baden-Baden, : Nomos Verlagsgesellschaft mbH & Co. KG, 2021 [s.l.] : , : Nomos Verlagsgesellschaft mbH & Co. KG, , 2021
ISBN	9783748927679 3748927673
Edizione	[1st ed.]
Descrizione fisica	1 online resource (156 p.)
Collana	Schriften zum IT-Sicherheitsrecht
Soggetti	Computers / Security Computers
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Cybersecurity und Unternehmensleitung -- A. Einleitung -- B. Grundlagen: Cybersecurity und Bedrohungspotentiale -- I. Unbefugte Eingriffe in Systeme (Hacking) -- II. Schadsoftware -- III. Systemfehler, Fehlbedienung, Falschberatung -- IV. Ausspähen von Informationen -- C. Rechtliche Rahmenbedingungen für Cybersecurity -- D. Pflichten der Unternehmensleitung -- I. Grundlagen der Sorgfaltspflicht -- II. Business Judgment Rule -- 1. Ausreichende Informationsgrundlage -- 2. Höchstpersönliche Vorstandspflicht -- 3. Bewertung und Abwägung -- II. Legalitätspflicht der Geschäftsleitung -- 1.Grundlagen -- a. Interessenabwägungen und unbestimmte Rechtsbegriffe -- b. Anforderungen an Organmitglieder -- c. Schaffung ausreichender Entscheidungsgrundlage -- 2. Beurteilungsspielräume? -- 3. Beachtung ausländischen Rechts -- E. Pflicht zur Einrichtung eines IT-Riskmanagementsystems -- I. Organisations- und Überwachungspflichten, insbesondere Compliance -- 1. Grundsätze -- 2. IT-spezifische Compliance-Felder -- a. Datenschutzrechtliche Compliance -- b. IT-Sicherheit -- aa. Risikoanalyse -- bb. Maßnahmen -- cc. Überwachung -- c. Rolle von Zertifizierungen -- II. Handlungsfelder in concreto (Auwahl) -- 1. Pflicht zur Einrichtung eines CISO (Chief Information Security Officer)? -- 2. Pflicht zum Abschluss

von Cyberrisk-Versicherungen? -- 3. Technische Maßnahmen -- F. Anforderungen an Überwachungsorgane (Aufsichtsrat) -- G. Fazit -- Cybersecurity als Unternehmensleitungsaufgabe - Neue Aspekte der Organhaftung -- I. Haftungsrisiko des Unternehmens -- 1. Haftungsreduzierung kaum möglich -- 2. Überwälzung des Schadens auf Dritte -- II. Haftungsrahmen der Geschäftsleitung für Cybersecurity -- 1. Haftungsmaßstab -- 2. Enthaftung möglich? -- a. Horizontale Delegation -- b. Enthaftung durch vertikale Delegation -- c. Enthaftung durch Zertifizierung?.
d. Enthaftung durch Versicherungslösung? -- III. Fazit -- Offenlegungspflichten bei Cyberangriffen -- I. Einleitung -- II. BSIG -- 1. Regelungszweck -- 2. Meldepflichtige Unternehmen -- 3. Auslöser der Meldepflicht -- a. 8b Abs. 4 BSIG -- b. 8c Abs. 3 BSIG -- 4. Inhalt der Meldepflicht -- 5. Sanktionen -- III. DSGVO -- 1. Regelungszweck -- 2. Personeller Anwendungsbereich -- 3. Auslöser der Meldepflicht -- a. Art. 33 DSGVO -- b. Art. 34 DSGVO -- 4. Verfahren und Inhalt der Meldung -- a. Art. 33 DSGVO -- b. Art. 34 DSGVO -- 5. Sanktionen -- IV. MAR -- 1. Regelungszweck -- 2. Meldepflichtige Unternehmen -- 3. Auslöser der Meldepflicht -- a. Insiderinformation gem. Art. 7 Abs. 1 lit. a) MAR -- b. Unmittelbare Betroffenheit -- c. Keine Saldierung -- 4. Aufschubbefugnisse gem. Art. 17 Abs. 4 MAR -- a. Berechtigte Interessen des Emittenten -- b. Keine Irreführung der Öffentlichkeit -- c. Sicherstellung der Geheimhaltung -- 5. Verfahren und Inhalt der Mitteilung -- 6. Sanktionen -- V. Schlussfolgerungen -- Unternehmerische IT-Compliance in China: Cybersecurity und Künstliche Intelligenz -- A. Einführung -- B. Regelungssystematik und politische Strategien -- C. Chinese Cybersecurity Law -- D. Chinese Cryptography Law -- E. Chinese Data Security Law -- F. Fazit und Ausblick -- IT-Sicherheitssysteme und Mitbestimmung des Betriebsrats -- A. Der Mitbestimmungstatbestand: „technische Einrichtungen" -- B. Reformvorschläge -- C. Gesetzliche Vorgaben begrenzen die Mitbestimmung -- D. Entscheidungsspielraum für die Unternehmensleitung als Korridor für mitbestimmungspflichtige Entscheidungen -- E. Einschätzungsprärogative des Arbeitgebers zu regulatorischen Vorgaben und technischen Details? -- F. Verfahrensablauf in der Mitbestimmung -- I. Innerbetriebliche Verhandlungen -- II. Spruch der Einigungsstelle und dessen gerichtliche Überprüfung.
III. Einstweiliger Rechtsschutz -- 1. Verfügungsanspruch -- 2. Anforderungen an den Verfügungsgrund -- 3. Keine Ausnahme von den Anforderungen an Verfügungsanspruch und -grund -- G. Fazit -- IT-Sicherheit: ein verfassungsrechtlicher Zugang -- A. Die verfassungsrechtliche Relevanz von IT-Sicherheit -- B. Der Begriff der IT-Sicherheit - ein Zugang über Schutzziele -- I. Fragmentiertheit rechtlicher Anforderungen an die IT-Sicherheit -- II. Ein Zugang über Schutzziele -- 1. Vertraulichkeit -- 2. Verfügbarkeit -- 3. Integrität und Authentizität -- 4. IT-Sicherheit und der Gedanke der Vorsorge -- C. IT-Sicherheit und Verfassungsrecht -- I. IT-Sicherheit in privater Hand und die Rolle des Gewährleistungsstaates -- II. IT-Sicherheit als Staatsaufgabe und der Gedanke der Vorsorge -- III. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme -- 1. Positiv-rechtliche Aussagen des Grundgesetzes zur IT-Sicherheit -- 2. Rechtsfortbildungen durch das Bundesverfassungsgericht hin zur IT-Sicherheit -- 3. Die Rolle des Staates über die Abwehrdimension hinaus? -- D. Der Mehrwert eines intra- und interdisziplinären Blicks auf verfassungsrechtliche Fragen der IT-Sicherheit -- I. Interdisziplinäre Möglichkeiten: IT-Sicherheit als Public Good -- II. Ein intradisziplinärer Blick auf den

verfassungsrechtlicher Konkretisierungsbedarf zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme -- E. Fazit: von der Nützlichkeit eines verfassungsrechtlichen Kompasses für Fragen der IT-Sicherheit -- Cybersecurity in der unternehmerischen Praxis des Mittelstandes -- A. Cyberangriffe und -risiken in mittelständischen Unternehmen -- I. Cyberangriffe und -risiken von außen -- 1. Cyberangriffe durch Dritte -- a. Ransomware -- b. Phishing -- c. Spear-Phishing -- d. Whaling. 2. Cybersecurity in Zeiten der Coronapandemie -- II. Cyberangriffe und -risiken von innen -- 1. Disgruntled employees -- 2. Cyberrisiken durch geteilte Zugriffsrechte und Remote Devices -- a. Zugriffsrechte -- b. Mobile Endgeräte -- B. Lösungsansätze und Präventionsstrategien -- I. Lösungsansätze für Risiken von außen -- 1. Prävention gegen Ransomware -- 2. Prävention gegen Phishing -- 3. Prävention gegen Whaling -- 4. Passwörter und Passwortmanager -- 5. Zwei-Faktor-Authentisierung -- 6. Firewall und Antivirenprogramme -- 7. Haftung und Cyberversicherungen -- II. Lösungsansätze für Risiken von innen -- 1. Mitarbeiterschulungen und -sensibilisierungen -- 2. Clean-Desk-Policy -- 3. Weitere Policies -- 4. Zugriffsrechte -- 5. Equipment -- C. Fazit -- Verzeichnis der Autoren und Herausgeber.

Sommario/riassunto

Cybersecurity is a central challenge for many companies. On the one hand, companies have to protect themselves against cyberattacks; on the other hand, they have special obligations towards third parties and the state in critical infrastructures or when dealing with personal data. These responsibilities converge with company management. This volume examines the duties and liability risks of management in connection with cyber security from the perspective of corporate, constitutional and labour law. The volume is based on a conference of the same name, which took place in cooperation with the Friedrich Naumann Stiftung fur die Freiheit on 23 and 24 October 2020 at Bucerius Law School in Hamburg. With contributions by Andreas Beyer, Marc Bittner, Alexander Bruggemeier, Anabel Guntermann, Katrin Haußmann, Dennis-Kenji Kipker, Christoph Benedikt Muller, Isabella Risini, Darius Rostam, Sarah Schmidt-Versteyl and Gerald Spindler.