SPIRIT LEGAL®

Datenschutz in der Praxis

NGFW
und der Zielkonflikt mit dem Datenschutz

Institut für Rechtsinformatik, Uni Saarland //
31.01.2023

Anna Cardillo

- Rechtsanwältin @Spiritlegal
- Datenschutzrecht
- Beratung, Audits

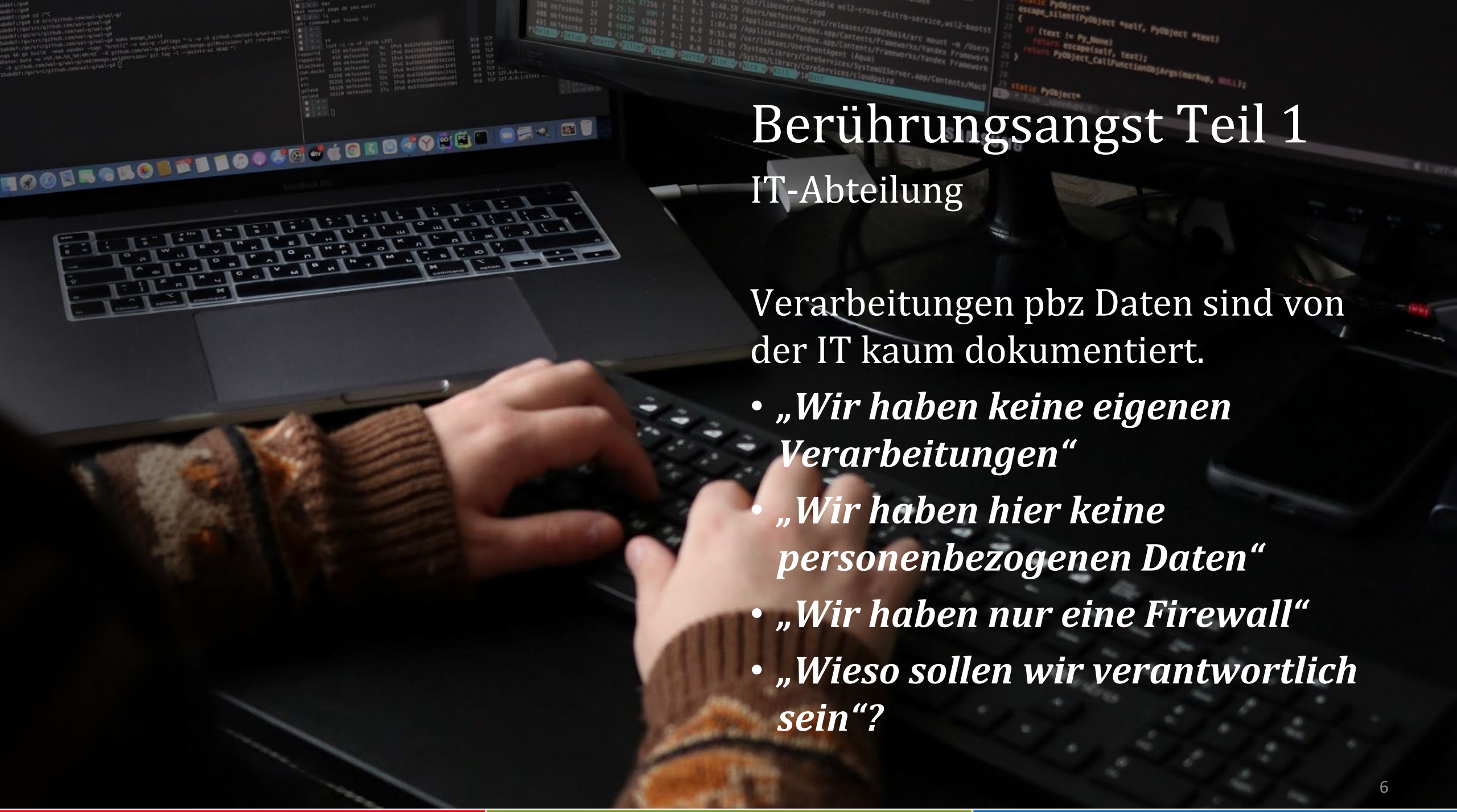
Worum es heute nicht geht

1. Rechtstheorie, tiefe Schutzgutdebatte ☺
2. Produktempfehlungen

Worum es heute geht

1. Kurzer Einblick in meine Auditwelt – Verarbeitungen personenbezogener Daten in der IT
2. Aufwachen, wachrütteln, miteinander sprechen
3. Praktische Empfehlungen

1. Kurzer Einblick in meine Auditwelt – Verarbeitungen personenbezogener Daten in der IT



Berührungsangst Teil 1

IT-Abteilung

Verarbeitungen pbz Daten sind von der IT kaum dokumentiert.

- ***„Wir haben keine eigenen Verarbeitungen“***
- ***„Wir haben hier keine personenbezogenen Daten“***
- ***„Wir haben nur eine Firewall“***
- ***„Wieso sollen wir verantwortlich sein“?***

Berührungsängste Teil 2

Datenschutzbeauftragte

- werden nicht einbezogen
- fragen nicht nach
- hinterfragen nicht
- verstehen oft die Technologie nicht
- verstehen die Technologie zwar, kennen die rechtlichen Anforderungen nicht
- erkennen daher manchmal die Brisanz nicht

Berührungsängste Teil 3

Betriebsrat und HR

- Betriebsvereinbarungen (BV) veraltet, neue werden erstellt, alte BV mit den selben Regelungsgegenständen (zum Beispiel Protokollierung und Kontrolle der E-Mail und Internetnutzung) nicht ersetzt, obwohl neue Technologien eingeführt. BV benötigen Management!
- Betriebsvereinbarungen werden einfach unterzeichnet, obwohl weder Systeme, Prozesse, Datenkategorien, Zwecke, Rechtsgrundlagen, Protokollierungs-, Zugriffs- und Löschkonzept vernünftig erfasst und bewertet sind.
- Besonders oft: IT-Abteilungen kennen die in der BV geregelten Zugriffsregelungen, Löschfristen etc nicht. Regelungen werden daher nicht eingehalten, Löschfristen i.Ü. auch nicht synchron beim Cloudanbieter…
- Sowohl BR als auch HR sind dabei oft im Unklaren über tatsächliche Abläufe, weil… ja, weil Berührungsangst Teil 1 und Teil 2.

2. Aufwachen, wachrütteln, miteinander sprechen

Praxisbeispiel: Next Generation Firewall

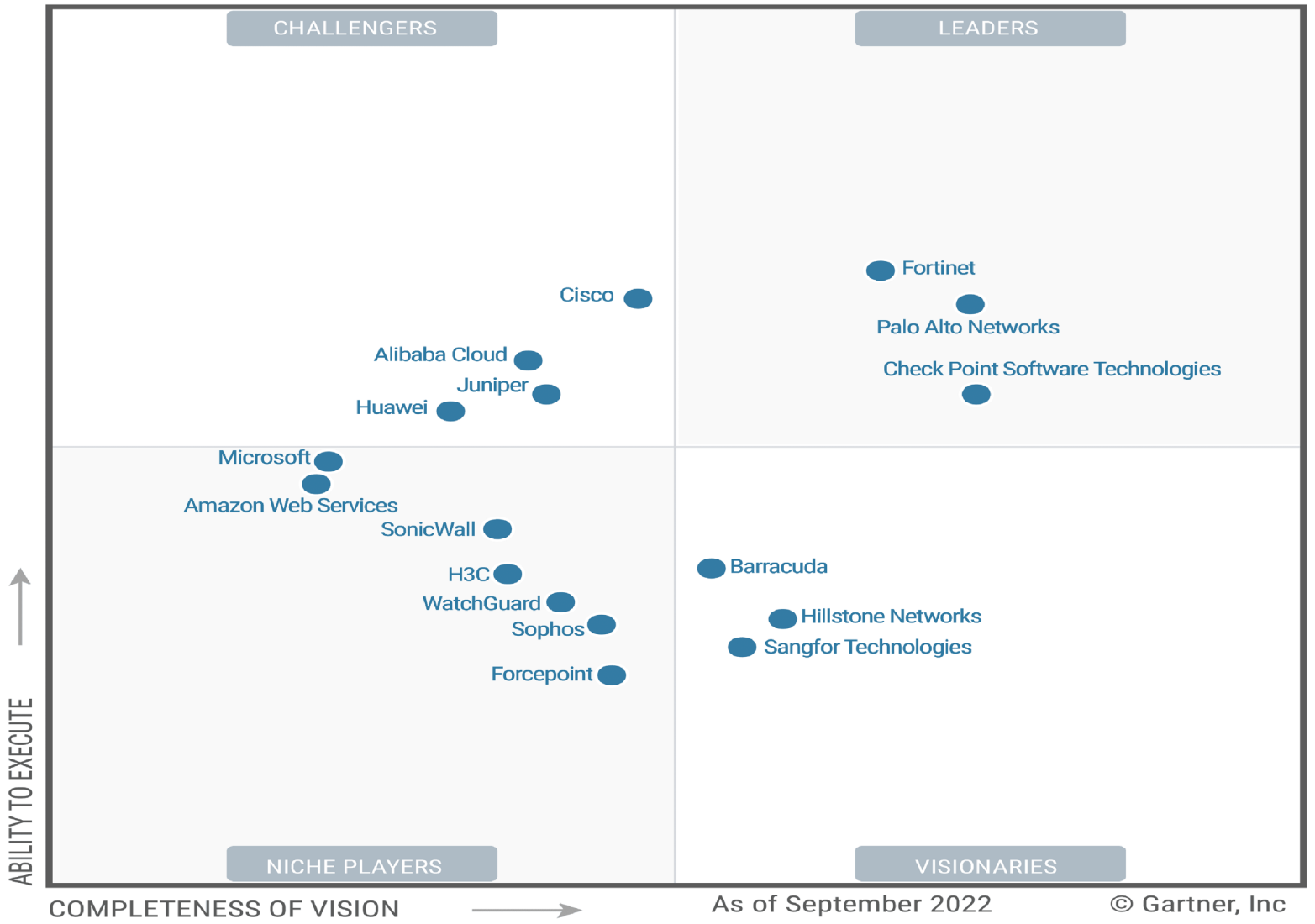
- **Firewall war gestern.**
- **Enormes Paket von einzelnen Filter - und Analysetools. Deep Packet Inspection, SSL Decryption, Sandboxing, IPS, IDS, DLP, CASB, UEBA, SIEM, etc.**
- **In der Regel Cloudbasiert**
- **Schnittstellen zu anderen Systemen**
- **„Machine learning“ ?**
- **Oft 3rd-party Lösungen – ebenfalls meist Drittlandsbezug und ebenfalls cloudbasiert**
- **Protokolldaten, Protokolldaten, Protokolldaten everywhere…**
- **Umfangreiche Analyse- und Reportmöglichkeiten „User Risk Report“**

What could possibly go wrong???

„… verschwimmen die Grenzen zwischen IT-Sicherheit, Betrugs- und Diebstahlprävention, Schutz von Kundendaten und Geschäftsgeheimnissen („Data Loss Prevention“, abgekürzt „DLP“ oder etwa der Sicherstellung der Einhaltung von Gesetzen, Richtlinien und sonstiger Verhaltensregeln im Unternehmen („ Compliance“) zunehmend. Systeme für die Abwehr von Cyberangriffen, die Verwaltung von Zugriffsberechtigungen oder für die Fernwartung von Geräten greifen ineinander und werden auch genutzt, um Fehlverhalten zu verhindern – ob fahrlässig, unabsichtlich oder in anderer Weise unerwünscht. Die gleiche Software, die das Abrufen auf virenverseuchte Websites verhindern soll, wird auch zur Sperrung des Zugriffs auf betrieblich unerwünschte Internetseiten eingesetzt und liefert Daten über Verhaltensmuster“.

Wolfie Christl, Digitale Überwachung am Arbeitsplatz, Cracked Labs, 2021, S. 101

Figure 1: Magic Quadrant for Network Firewalls

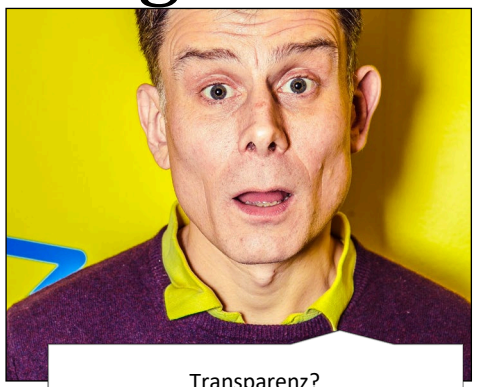


Source: Gartner (December 2022)

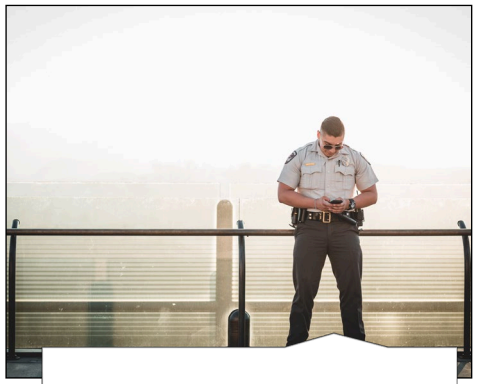
Komplexe Fragestellungen/Herausforderungen

Rechtsgrundlage für die jeweilige Datenverarbeitung/Beschränkung durch § 3 TTDSG?

Wie sind die verschiedenen Akteure (Cloud-Anbieter) datenschutzrechtlich zu bewerten? Art. 26 oder 28 oder eigenständige Verantwortliche?



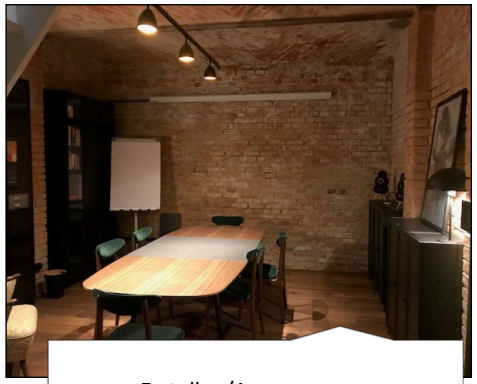
Transparenz? Betroffeneninformationen? Ausnahmen?



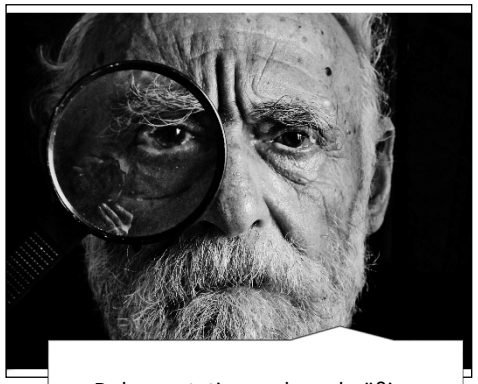
Drittlandsbezug, SCC, TIA

Protokollierungskonzept

DSFA, vgl. MUSS-Listen der Aufsichtsbehörden, aber auch so voraussichtlich hohes Risiko zu bejahen



Erstellen/Anpassen von Betriebsvereinbarungen



Dokumentation und regelmäßige Evaluierung

3. Praktische Empfehlungen

Ganzheitlicher Ansatz

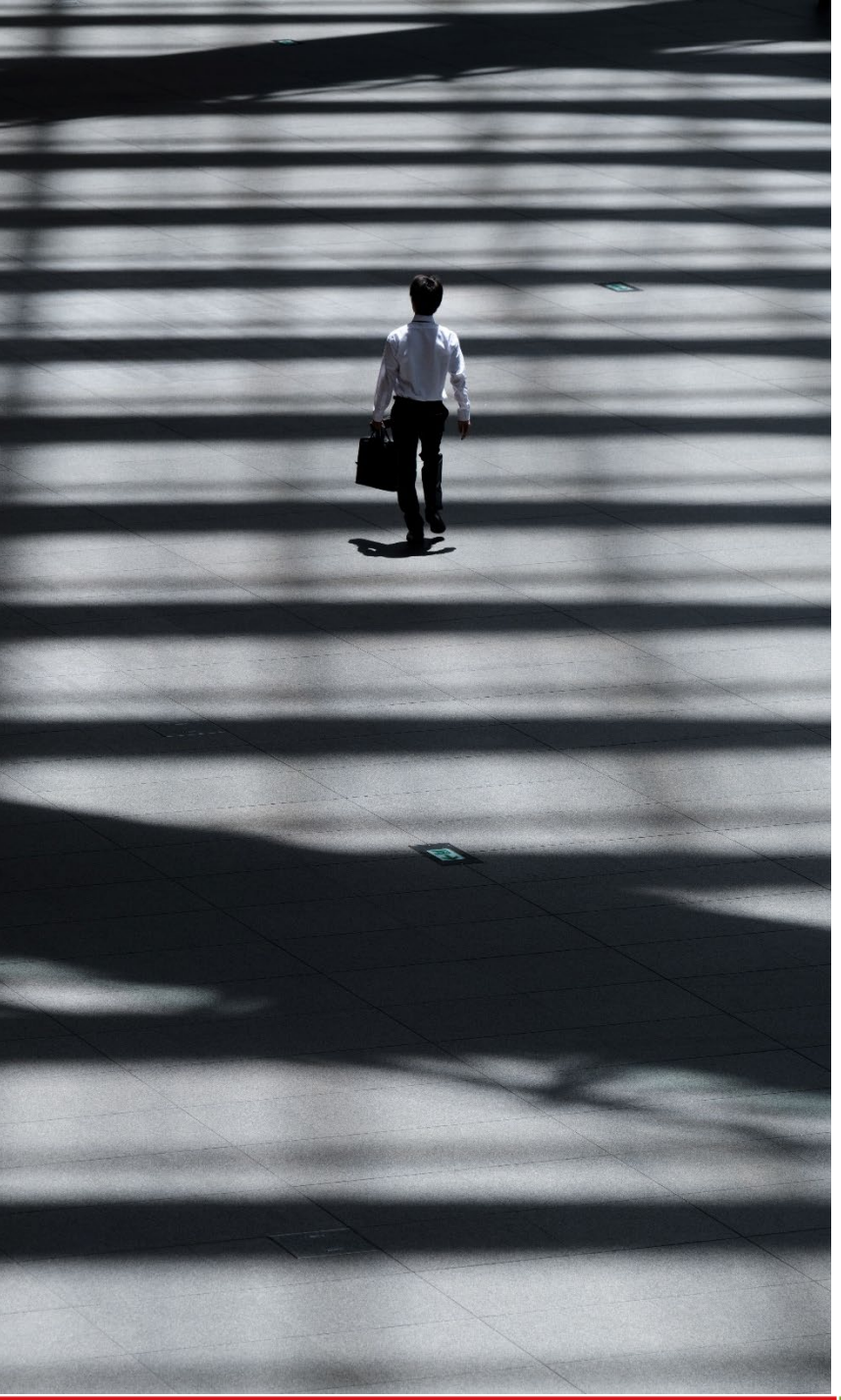
Gute Technik

Gute Datenschutz – und Sicherheits-konzepte

Gutes TEAM

Projektmanager?

Jemand muss den Hut aufhaben, um alle Fäden zusammen zu halten



Mühsamer Weg, ja – aber notwendig

- Ohne technische Sachverhaltserfassung keine Verhältnismäßigkeitsprüfung möglich => individuelle Betrachtung der einzelnen Lösungen erforderlich! Anbieter veröffentlichen oft hilfreiche White paper, die Hinweise geben können (Marketing-Sprech wegdenken). Visualisierungen der Anbieter nutzen!
- Zwecke sauber festlegen => Was kommt in Betracht? Bitte nicht nur „ Zur Sicherheit unserer IT-Systeme“
- Erforderlichkeit => Was genau wird an Daten benötigt? Einschränkung nicht immer möglich, dann höhere organisatorische Anforderungen
- Achtung: Berufsgeheimnisträger/BR/DSB
- Sauberes Zugriffskonzept, welches mit (legitimen) Zwecken korrespondiert. Auch innerhalb IT-Abteilung müssen Zugriffsrechte differenziert betrachtet werden. Nicht alle benötigen den Zugriff auf Protokolldaten (Helpdesk, IT-Betrieb ungleich SOC)
- Vernünftiges Protokollierungskonzept erstellen
  - damit kann ein Wirr-Warr in den BV vermieden werden, maßgeblich ist das jeweils aktuelle (!) Protokollierungskonzept. Dieses muss dann natürlich mit BR abgestimmt werden
  - Sollte auch Löschfristen regeln
  - Bekanntgabe und Schulung der Zuständigen

SPIRIT LEGAL®

Welche Zwecke kommen zum Beispiel in Betracht bzw. sollten berücksichtigt werden (je nach Einzellösung)?

- Umsetzung gesetzlicher Vorgaben (z.B. Jugendschutz: Blockierung unpassender Inhalte)
- Blockierung von ungewünschtem Internet-Datenverkehr
- Automatisierte Analyse auf Schadcode / Malware
- Erkennung und Abwehr von Web-basierten Cyber-Angriffen; Gewährleistung der Sicherheit von Systemen und Informationen, einschließlich personenbezogener Informationen
- Identifizierung von Sicherheitsvorfällen
- Forensische Analyse von Sicherheitsvorfällen
- Optimierung der Computer-Systeme
- Optimierung des Netzes
- Überprüfung der Einhaltung der Bestimmungen der DSGVO (Audits DSB oder sonstigen Sachverständiger)
- Überprüfung der Einhaltung von Betriebsvereinbarungen (Audits BR)
- Zur Missbrauchskontrolle usw.

Leseempfehlungen

- **Laura Schulte, Tim Wambach**, *Zielkonflikte zwischen Datenschutz und IT-Sicherheit im Kontext der Aufklärung von Sicherheitsvorfällen,* DuD 7/2020, 462-468 (Beispiele **Log-files** und **SIEM**)
- **Florian Deusch, Tobias Eggendorfer**, ***Intrusion Detection*** *und DSGVO*, DSRITB 2018, 741
- **Tina Krügel,** *Der Einsatz von* ***Angriffserkennungssystemen*** *im Unternehmen*, MMR 2017, 795
- **Hendrik Schlegel**, *Software zur verdachtslosen Kontrolle* ***Data-Loss-Prevention(DLP)*** *ausgehender E-Mails,* ZD 2020,243
- **Wolfie Christl**, *Digitale Überwachung und Kontrolle am Arbeitsplatz,* abrufbar unter https://crackedlabs.org/dl/CrackedLabs_Christl_UeberwachungKontrolleArbeitsplatz.pdf
- **Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V**, *Protokollierung und Protokollierungskonzept –Eine Einführung in die Thematik* abrufbar unter https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php (letzter Aufruf 31.01.23)

Kontakt

Anna Cardillo

anna.cardillo@spiritlegal.com

www.spiritlegal.com