Checkliste für Datenschutz und Compliance

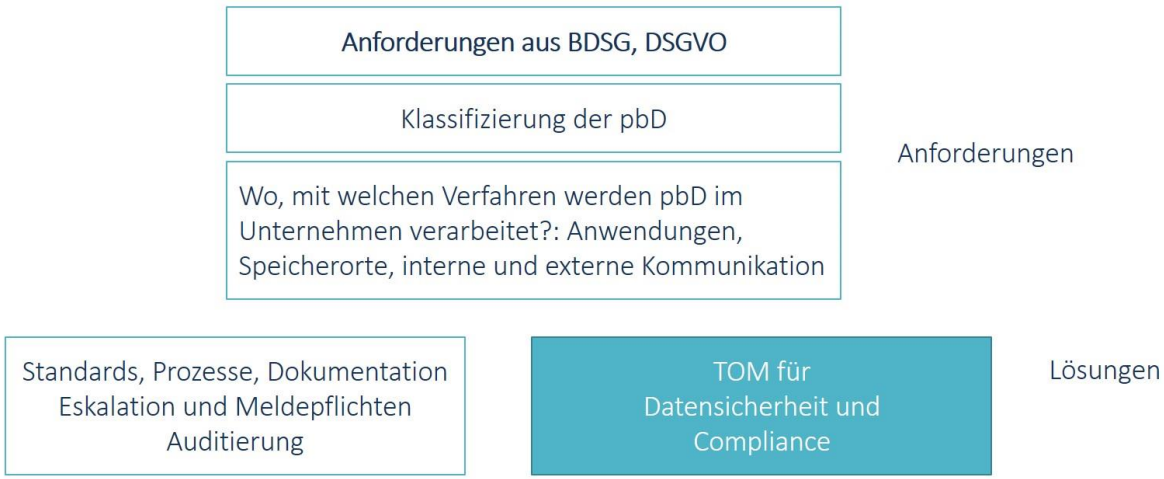
Version vom 9.2.2018 Kontakt: Dr. Lutz Netik, lnetik@netik.de

Die aktuellen Anforderungen an Datenschutz und Compliance sind vor allem aus dem Bundesdatenschutzgesetz (BDSG neu) und aus der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union abzuleiten.

DSGVO
BDSG (neu)
zur Erinnerung BDSG 1990
Gute Zusammenfassungen:
DSGVO aufbereitet
Bitkom FAQ zur Grundschutzverordnung

Dr. Netik & Partner GmbH
17034 Neubrandenburg
Feldmark 1
Fax: +49 395 43017-90
18273 Güstrow
Grabenstraße 16
Fax: +49 3843 7245-55
Internet: www.netik.de
Mail: info@netik.de

Deutsche Bank PGK AG · IBAN: DE07 1307 0024 0400 2515 00 · SWIFT: DEUTDEDBROS
Ust-IdNr.: DE 137267922 · Steuernr.: 072/107/00476 . Gerichtsstand: Amtsgericht Neubrandenburg, HRB 1699
Geschäftsführer: Dr. Lutz Netik, Heimon Hinze, Bernd Scheller, Frank Seefeld, Alexander Henkel



Netik kann nicht die Rolle des Datenschutzbeauftragten oder Compliance-Beraters für Ihr Unternehmen übernehmen.

Wir unterstützen unsere Kunden durch Lösungen und Technisch-Organisatorische Massnahmen (TOM) für die Entwicklung und Schärfung Ihrer Cybersecurity-Strategie.

Als Managed Service Provider sorgen wir für IT-Sicherheit im Rechenzentrum.

Im Fall von Datenpannen und Verletzung des Datenschutzes unterstützen wir Sie bei der Aufklärung und Beseitigung der Ursachen.

In dieser Checkliste werden Technisch-Organisatorische Maßnahmen für Datensicherheit und Compliance vorgelegt.

Konkrete Lösungen finden Sie auf unseren Webseiten – oder fragen Sie einfach bei uns nach.

1 „Bedrohungen abwehren“: Sicherheit für die Verbindung zwischen Unternehmensnetz und Internet

Hier sind bereits bewährte Lösungen im Einsatz. Prüfen Sie, ob Sie up-to-date sind!

Thema	TOM	Status
Internet Firewall	Solide "richtige" Firewall zwischen Unternehmensnetz und Internet: mit leistungsfähigen Funktionen für Gateway-Antivirus, Intrusion Prevention, Anti-Spyware und Capture ATP Korrekte Einstellungen, aktuelle Software (Wartungsvertrag) keine "Hintertüren" im Netz Ausreichend Performance für die geforderte Bandbreite. Redundante Internetverbindungen mit automatischem Failover bei erhöhten Anforderungen an die Verfügbarkeit der Internetverbindung.	
	Lassen sich eingehenden Verbindungen aus dem Internet generell vermeiden (bzw. welche)? z.B. durch Outsourcing von E-Mail, öffentlicher Website u.a.	
Stationäre VPN-Verbindungen	zwischen Standorten sowie zwischen Unternehmen und Outsourcer bzw. wichtigen Partnern.	

Access Gateway	Definierter externer Zugriff über das Internet Access Gateway und verschlüsselte SSL-Verbindung für die Anbindung mobiler Mitarbeiter, Home Office, Externe u.ä.	
E-Mail Security durch Appliance oder durch Cloud-Lösung	Überwachung der ein- und ausgehender Kommunikation, Schutz gegen Angriffe durch infizierte E-Mails und Webseiten: Emailsecurity Appliance mit Spam-, Spoofing-, Phishing-, Virenschutz und Capture ATP oder cloudbasierte E-Mail Protection und ATP	
Content Filter	Schutz gegen illegale Inhalte auf Webseiten	

2 „Ausbreitung verhindern“: Sicherheit im internen Netz

2.1 Identity Management

Anscheinend altbekannte Themen! Allerdings liegen hier auch die Haupt-Einfallstore für Angreifer. In vielen Fällen ist wesentlich mehr Disziplin, Akkuratesse und Energie für die Durchsetzung angesagt. (und Fachwissen!). Es gibt neue Aspekte und Lösungsansätze.

Thema	TOM	Status
Windows Active Directory Benutzer- und Ressourcenmanagement	Konsequente Trennung von Benutzerkonten, Administratorkonten, Dienstbenutzerkonten Dienst-Konten für automatisierte Anwendungen Gruppenbasierte Administration von Berechtigungen und Richtlinien	
	normale Benutzerkonten ohne lokale Admin-Rechte	
	AD Management AD Audit	
Berechtigungen	auf das Dateisystem, auf Clientlaufwerke, USB-Sticks, Cloud Speicher usw.	
Sichere Passwörter!	Kennwortrichtlinien, Kontosperrungsrichtlinien, Kerberosrichtlinien	

	Solide, strenge Passwortrichtlinien einschließlich Passwortwechsel 2-Faktorauthentifizierung mindestens für externen Zugriff über Access Gateway	
Dateiausführungsrichtlinien	Freigabe (nur) für erlaubte betriebliche Anwendungen	
PKI	für sensible Verbindungen zwischen Geräten - Server, AD u.ä. Authentifizierung von Geräten - speziell Mobilgeräten im internen WLAN E-Mail Verschlüsselung	

2.2 Management und Security der zentralen IT

Auch hier sind bereits bekannte, bewährte Lösungen im Einsatz. Prüfen Sie, ob Sie up-to-date sind!

Thema	TOM	Status
Management der zentralen IT	Netzwerkmanagement Servermanagement Updatemanagement Virenschutzmanagemt	
aktuelle Server Betriebssysteme	Windows Server 2012, 2016	
Proaktives Systemmonitoring	für alle wichtigen Geräte und deren Parameter Warnung bzw. Alarm bei Grenzwertüberschreitung Systemlog	

2.3 Clientmanagement und -security

Die Absicherung der Clients für den Fall, dass doch eine Schadsoftware ins Netz gelangt, muss wesentlich verbessert werden. Clientmanagement war bisher ein Stiefkind gegenüber dem Management der zentralen IT. Hier gibt es neue Ansätze und Lösungen.

Thema	TOM	Status
Zentrales Clientmanagement	cloud-basiertes Clientmanagement für mobile und stationäre Windows Clients: Updatemanagement Virenschutzmanagement / Endpoint Threat Protection Softwareausbringung und -standardisierung	
Zentrales Mobilgeräte-management	cloud-basiertes Mobilgerätemanagement: Softwareausbringung und -standardisierung, Unternehmens App Store Daten von verlorenen Geräten sicher löschen	
Aktuelle Client Betriebssysteme	Windows 10 Pro/Ent. mit Windows Defender und Bitlocker	
Windows Firewall	Aktivieren! + Ausnahmeregeln	
Intrusion Detection	Windows Defender Advanced Threat Protection	

2.4 Netzwerksegmentierung

Beschränkung der Verbindung zwischen Subnetzen und Geräten untereinander auf das Notwendige

Thema	TOM	Status
Virtuelle LANs	Netzwerksegmentierung auf Switch-Ebene	
Zugriff auf das Unternehmensnetz absichern und kontrollieren	Trennung von öffentlichem und internem WLAN Zugriffssteuerung für registrierte Geräte und Benutzer	
Interne Firewall	Zugriffssteuerung zwischen Netzwerksegmenten und Gerätegruppen	

4 "Wiederherstellung ermöglichen"

Für Backup und Redundante Auslegung von Ressourcen sind bewährte Lösungen im Einsatz. Prüfen Sie, ob Sie up-to-date sind!

Vor allem testen Sie regelmäßig, ob die Wiederherstellung von Funktionen und Daten tatsächlich in der erwarteten Frist gelingt!

Thema	**TOM**	**Status**
Backup und Recovery Management	Backup to Disk to Tape ← vs. → Cloud Backup für Server Fileserver und Datenbanken für Clients für Virtuelle Maschinen	
Virtualisierung und Provisionierung	für Server für Clients	
Images	Systemwiederherstellungspunkte	

5 „Dokumente kategorisieren, Zugriff regeln“: Richtlinien für Dokumente

Data-Governance-Werkzeuge für mehr Transparenz, Kontrolle und Reporting:

Wo werden personenbezogene und allgemein sensible Daten gespeichert, wie werden sie genutzt, wann und wie werden sie gelöscht?

Thema	TOM	Status
Kontrolle, Steuerung und Reporting des Zugriffs auf Anwendungen und Daten	Active Directory Management	
Dokument Klassifizierung und dokumentbasierter Zugriffsschutz	Azure Information Protection Rights Management Services Data Loss Prevention	
E-Mail Archivierung	Compliance Pflichten erfüllen! Mailstore Exchange Online Archivierung	
Sicherer Datenaustausch	Enterprise File Sharing	
Dateiverschlüsselung	Bitlocker	
E-Mail Verschlüsselung	Zertifikatsinfrastruktur, PKI	

6 "Sichere Prozesse einrichten und überwachen"

Organisatorische Standards und Prozesse für die Verwaltung und Dokumentation sensibler Daten, für Eskalation und Erfüllung der Meldepflichten, für die Datenschutz-Auditierung

Thema	TOM	Status
Dokumentation	IT-Inventarisierung, Visualisierung, Berechtigungsanalyse, Lizenzmanagement Systemdokumentation Betriebshandbuch Notfallhandbuch Neue DSGVO Berichte	
Inventur und Test	Management- und Kontrollprozesse Test Redundanz/Recovery und Wiederanlauf Checkin-/Checkout-Prozesse Update- und Erneuerungsprozesse	
Monitoring	Monitoring von Systemen, Diensten und Anwendungen: u.a. Inhalt von Ordnern, Dateien überwachen, Protokolle und Berichte Automatisierte Eskalation und Meldung von Störfällen	

Mehr Information auf den Netik Webseiten:

Datenschutz und Compliance

TOM für Datensicherheit und Compliance

www.netik.de/fokus/dsgvo

Weiterführende Links (auf Microsoft Seiten):

Microsoft Trust Center

Ein neues Zeitalter der Datenschutzbestimmungen

Compliance-Lösungen in Office 365

Kontakt:

Dr. Netik & Partner GmbH

Dr. Lutz Netik	Frank Seefeld
lnetik@netik.de	fseefeld@netik.de
+49 (395) 4307 13	+49 (03843) 7245 12