Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)
Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Cybersicherheit für medizinische Einrichtungen

Best-Practice-Prüfkriterien Art. 32 DS-GVO

Stand: 27. Mai 2020

Ziel und Inhalt dieses Papiers

Diese Handreichung ermöglicht einen Überblick einiger Praxismaßnahmen zur Cybersicherheit für medizinische Einrichtungen – inklusive eines Themenblocks speziell für Labore – entsprechend den geltenden gesetzlichen Datenschutzvorgaben. Im Sinne einer gezielten Prävention soll damit eine gesteigerte Sensibilisierung für sicherheitsrelevante Themen erreicht und aktiv ein störungsfreier Betrieb dieser Einrichtungen unterstützt werden. Der Fokus des Dokuments liegt auf der **Verfügbarkeit** der Daten bzw. Dienste bezüglich Angriffe aus dem Internet und weniger auf deren Vertraulichkeit und Integrität, die aus Datenschutzsicht jedoch ebenfalls zu beachten sind. Die aufgeführten Maßnahmen sind selbstverständlich nicht als abschließend zu betrachten, sondern stellen einen **Best-Practice-Ansatz** dar, der einen effektiven Schutz gegen aktuelle Cybersicherheitsbedrohungen unterstützen kann. Auf Grund der individuellen Gegebenheiten jedes Betriebs ist es nicht zwingend erforderlich, jede genannte Maßnahme zur Einhaltung der datenschutzrechtlichen Sicherheitsanforderungen umzusetzen. Werden einzelne Maßnahmen nicht umgesetzt, ist zu prüfen, wie andere (ggf. bestehende) Maßnahmen ein vergleichbares angemessenes Schutzniveau bieten können.

Bei diesem Papier handelt sich um eine Hilfestellung zur schnellen Überprüfung der eigenen Sicherheit hinsichtlich der Verfügbarkeit der eigenen Datenverarbeitung im Sinne von Art. 32 DS-GVO. Der Anwendungsbereich umfasst sowohl den nicht-öffentlichen als auch den öffentlichen Bereich. Das Werk entstand in einer Zusammenarbeit des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) und des Bayerischen Landesbeauftragten für den Datenschutz (BayLfD). Weiterführende Links zu vertrauenswürdigen Websites helfen bei der eigenen Umsetzung. Bei Fragen stehen das BayLDA und der BayLfD beratend zur Seite.

Selbst-Check: Cybersicherheit in medizinischen Einrichtungen

1 Patch Management

Veraltete Softwarestände bergen ein erhöhtes Angriffsrisiko wegen potentieller Schwachstellen. Die eingesetzte Software muss daher durch regelmäßige Sicherheitsupdates aktuell gehalten werden.

- ☐ Konzept zum Patch Management vorhanden (u. a. Update-Plan mit Übersicht der eingesetzten Software)
- ☐ Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software, Fachanwendungen und medizinische Geräteumgebung (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)
- ☐ Ausschließlicher Einsatz von Desktop-Betriebssystemen, für die der Hersteller/Maintainer beim Bekanntwerden von Schwachstellen Sicherheitsupdates zur Verfügung stellt
- ☐ Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server
- ☐ Automatische Updates der Desktop-Betriebssysteme (direkt vom Hersteller oder durch zentrale Verteilung)
- ☐ Geregelter Prozess für Updates der Browser (Empfehlung: Automatisch, sofern möglich)
- ☐ Geregelter Prozess für Updates von Basiskomponenten wie z. B. Java, PDF-Reader (Empfehlung: Automatisch, sofern möglich)

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_3_Patch... (BSI)

2 Malware-Schutz

Ein Befall mit Schadcode führt oft zu einer erheblichen IT-Störung. Durch Antiviren-Programme werden zwar nicht alle Schadcode-Varianten erkannt, aber viele Standardangriffe abgefangen. Ein wirksamer Anti-Malware-Schutz ist folglich einzusetzen.

- ☐ Endpoint Protection auf jedem Arbeitsplatzrechner
- ☐ Tägliche automatische Aktualisierung der Antivirensignaturen
- ☐ Zentrale Erfassung von Alarmmeldungen durch die IT-Administration
- ☐ Klare Anweisungen an Beschäftigte zum Umgang mit Alarmmeldungen
- ☐ Ablaufplan der IT-Administration bei Malware-Befall
- ☐ Antivirenlösung mit als „hoch" konfigurierter lokaler heuristischer Erkennung
- ☐ Sandboxing-Verfahren oder Advanced Endpoint Protection and Response (EDR) nur unter strenger Berücksichtigung datenschutzrechtlicher Vorschriften

>> Weitere Informationen:

www.lda.bayern.de/de/thema_schadcode.html (LDA)

3 Ransomware-Schutz

Trojaner, die Daten gezielt verschlüsseln, um Lösegeld zu erpressen, können den Betriebsablauf zum Stillstand bringen. Proaktive Maßnahmen zum Schutz gegen Verschlüsselungstrojaner sind essentiell, um drohende negative Auswirkungen frühzeitig abzufangen.

- ☐ Weitestgehender Verzicht auf Makros in Office-Dokumenten im Betriebsalltag
- ☐ Zulassen ausschließlich signierter Microsoft Office-Makros oder (regelmäßige) Information, bspw. einmal pro Jahr, der Beschäftigten über Risiken einer Makro-Aktivierung (z. B. in Microsoft Word)
- ☐ Verhinderung einer automatischen Ausführung von heruntergeladenen Programmen (z. B. Software Restriction Policy und Sandboxing)
- ☐ Deaktivierung von Windows Script Hosts (WSH) auf Clients (sofern nicht zwingend benötigt)
- ☐ Prüfung, ob die Einschränkung von Powershell-Skripten mit dem „ConstrainedLanguage Mode“ auf Windows-Clients sinnvoll durchführbar ist
- ☐ Nutzen eines Web-Proxys mit (tages-)aktuellen Sperrlisten von Schadcode-Download-Seiten (IOCs)
- ☐ Notfallplan für den Umgang mit Verschlüsselungstrojanern auf Papier
- ☐ Überprüfung der Backup- und Recovery-Strategie (vgl. Punkt 7), die sicherstellt, dass Backups durch die Ransomware nicht verschlüsselt werden können

>> Weitere Informationen:

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf (BSI)

4 Passwort-Schutz

Der Zugang zu personenbezogenen Daten jeglicher Art ist Unbefugten, insbesondere Cyberkriminellen, durch geeignete Maßnahmen zu erschweren. Starke Passwörter helfen dabei im Alltag, die Logins von Beschäftigten wirksam abzusichern.

- ☐ Bewusstsein bei Beschäftigten, was starke Passwörter sind und wie mit diesen umzugehen ist (z. B. keine Haftnotizen am Arbeitsplatz, niemals weitergeben, …)
- ☐ Vorgabe bei Anwendungen zur Verhinderung der Auswahl sehr schwacher Passwörtern (z. B. über Richtlinien oder, soweit möglich, technisch erzwungen über das Identity-Management-System)
- ☐ Mindestlänge bei genutzten Passwörter von zehn Stellen
- ☐ Empfehlung zur Vermeidung leicht zu erratender Passwörter oder Passwortbestandteile
- ☐ Regelung zur Sperrung und Neuvergabe von Passwörtern nach einem Vorfall
- ☐ Starke Passwörter gemäß Passwort-Richtlinien auch auf internen Systemen verwenden, sofern diese nicht bereits über das Identity Management System erzwungen werden
- ☐ Überprüfung der Regel, dass Passwörter nach kurzen Zeiträumen (z. B. 60 Tage) geändert werden müssen – falls die Passwörter stark und ausreichend lang sind (z. B. mind. zwölf Stellen), kann das Passwortwechselintervall deutlich länger sein (z. B. einmal pro Jahr)

>> Weitere Informationen:

www.stmd.bayern.de/service/passwort-check/online-anwendung-passwort-check/ (StMD)

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/ORP/ORP_4_Ident... (BSI)

5 Zwei-Faktor-Authentifizierung

Sicherheitskritische Bereiche liegen längst im Fokus von Angreifern. Neben klassischen Passwörtern sind daher weitere Zugangsfaktoren erforderlich, um diese besonders schützenswerten Zugänge angemessen abzusichern.

- ☐ Zwei-Faktor-Absicherung für Administratorzugänge – zumindest für Internetdienste (z. B. Cloud Mail Hosting[2])
- ☐ Grundsätzliche Absicherung von verschlüsselten VPN-Verbindungen mit kryptographischen Zertifikaten oder Einmalpasswörtern
- ☐ Falls Chipkarten als Mitarbeiterausweise eingesetzt werden, prüfen, ob diese für Standardauthentifizierungen (z. B. Windows-Login) verwendet werden können

>> Weitere Informationen:

www.bsi.bund.de/SharedDocs/Videos/DE/BSIFB/2FA-zwei-faktor-authentisierung.html (BSI)

6 E-Mail-Sicherheit

Der E-Mail-Verkehr verursacht große Sicherheitsrisiken und ist oft Ausgangspunkt eines erfolgreichen Angriffs. Unternehmensweite Regelungen zum E-Mail-Verkehr helfen, diesen Risiken rechtzeitig zu begegnen.

- ☐ Anzeige von E-Mails im „Nur-Text-Format“, um manipulierte Links sichtbar zu machen
- ☐ Verwendung von einer Security-Komponente, um Links in E-Mails vor Aufruf zu prüfen
- ☐ Prüfung eingehender E-Mails mittels Anti-Malwareschutz
- ☐ Blockieren von gefährlichen Anhänge (z. B. .exe, .doc, .cmd)
- ☐ Information der Beschäftigten über die Gefahren verschlüsselter E-Mail-Anhänge[1] (z. B. Zip-Datei mit Passwort)
- ☐ Information der Beschäftigten zur Erkennung gefälschter E-Mails (z. B. Absenderadressen, Auffälligkeiten, eingebettete Links)
- ☐ Regelmäßige Information der Beschäftigten über aktuelle Angriffsvarianten per E-Mail (z. B. Emotet, CEO-Fraud), z. B. einmal pro Jahr
- ☐ Deaktivieren von pauschalen Weiterleitungsregelungen bei Cloud-Hosting[2]

[1] Hinweis: Eine Verschlüsselung ist insbesondere bei personenbezogenen medizinischen Daten erforderlich. Dies kann jedoch dazu führen, dass der Inhalt nicht vorab auf Schadcode geprüft werden kann. Daher ist vor bzw. beim Öffnen besondere Sorgfalt anzuwenden.

[2] Hinweis: Für Labore und andere medizinische Einrichtungen in bayerischen Krankenhäusern kann ein Cloud Hosting von medizinischen Daten aufgrund von Art. 27 Abs. 4 Bayerisches Krankenhausgesetz (BayKrG) unzulässig sein, siehe hierzu den

- ☐ Einsatz von kryptographisch signierten E-Mails (z. B. mit S/MIME) bei interner Kommunikation zur Erkennung von gefälschten internen E-Mails im Rahmen von Angriffsversuchen prüfen

>> Weitere Informationen:

www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Email/email_node.html (Allianz für Cybersicherheit)

7 Backups

Ausfälle von Datenträgern, sei es durch Störungen oder Cyberattacken, können nachhaltige Schäden bis hin zum Totalausfall eines Betriebs führen. Regemäßige Sicherungen wichtiger Datenbestände sind daher Voraussetzung, um einen IT-Ausfall möglichst schadlos zu überstehen. Zu beachten bleibt, dass Trojaner je nach Ausgestaltung auch auf Backups übergreifen können.

- ☐ Vorhandensein eines schriftlich fixiertes Backup-Konzepts
- ☐ Durchführung von Backups nach der 3-2-1 Regel: 3 Datenspeicherungen, 2 verschiedene Backupmedien (auch „Offline" wie Bandsicherungen) und 1 davon an einem externen Standort
- ☐ Geeignete physische Aufbewahrung von Backupmedien (z. B. Tresor, unterschiedliche Brandabschnitte, Gefahr von Wasserschäden, ...)
- ☐ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird
- ☐ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert
- ☐ Mindestens ein Backup-System ist durch Schadcode nicht verschlüsselbar (z. B. spezielles Datensicherungsverfahren wie Pull-Verfahren des Backup-Systems oder Air-Gap-getrennt (offline) nach Abschluss des Backup-Prozesses

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/CON/CON_3... (BSI)

8 Home Office

Verlagern Beschäftigte die Arbeit ins eigene Zuhause, entstehen völlig neue Sicherheitsprobleme, die als Einfallstor für tiefgreifende Cyberangriffe fungieren können. Die Anbindung von Beschäftigten im Zu-Hause-Modus muss daher durchdacht und sicher ausgestaltet werden.

- ☐ Überblick über Beschäftigte, die die grundsätzliche Möglichkeit haben, im Home Office zu arbeiten
- ☐ Überblick über Beschäftigte, die aktuell Home Office nutzen
- ☐ Überblick über Geräte der Beschäftigten im Home Office
- ☐ Gewährleistung der Erreichbarkeit der Beschäftigten im Home Office über verschiedene Kommunikationskanäle im Falle eines Angriffs (z. B. Ausweichen auf Telefon)
- ☐ Festplattenverschlüsselung mobiler Endgeräte per starker Kryptographie (z. B. AES 256 Bit)
- ☐ Absicherung der Home-Office-Zugänge zum Unternehmensnetz mit VPN-Verbindungen sowie einer Zwei-Faktor-Authentifizierung
- ☐ Regelungen zur Nutzung von privaten Endgeräten in Ausnahmefällen (z. B. ausschließlich Verbindungen zu Terminalservern)
- ☐ Bei Bedarf Containerlösungen zur Trennung von dienstlichen und privaten Bereichen
- ☐ Information zum Umgang mit Videokonferenzen
- ☐ Regelungen zur Mitnahmen und Entsorgung sensibler Papierdokumente (z. B. Sicherheitskonzepte, Policies, Netzpläne, ...)

>> Weitere Informationen:

www.datenschutz-bayern.de/corona/sonderinfo.html (BayLfD)

www.lda.bayern.de/best_practice_homeoffice (BayLDA)

www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html (BSI)

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenz... (BSI)

9 Externe Abrufmöglichkeit für Laborergebnisse

Möglichkeiten zum Online-Abruf von Laborergebnissen für Einsender, z. B. über eine Website, bieten neue Angriffsflächen, da diese über das Internet zugänglich sind und somit Ziel für Hackerangriffe werden können. Folglich müssen umfangreiche Schutznahmen eingesetzt werden.

- ☐ Kryptographisch angemessene Absicherung der Zugriffe (z. B. SSL)
- ☐ Sichere und für jeden Einsender unterschiedliche Zugangsdaten
- ☐ Regelmäßiges Update der verwendeten Software, insbesondere zügiges Schließen von bekanntgewordenen Sicherheitslücken
- ☐ Vollständige Protokollierung der Zugriffe
- ☐ Regelmäßige Kontrolle der Protokolle
- ☐ Sicherheitstechnische Trennung von Abrufseiten und internen IT-Systemen
- ☐ Regelmäßige (automatische) Löschung der bereitgestellten Daten nach Abruf durch die Einsender
- ☐ Regelmäßige Penetrationstests

10 Fernwartung

Möglichkeiten zum Fernzugang eines Systems bieten neue Angriffsflächen. Im Umgang mit Dienstleistern, die sich per Fernwartung auf Systeme schalten, sind eingespielte Sicherheitsabläufe im Betrieb besonders wichtig.

- ☐ Begrenzung der Fernwartungszugänge nur auf die konkret zu wartenden Systeme statt auf komplette Netzwerksegmente, ggf. zusätzlich abgesichert durch sog. „Jumpserver"

---

gemeinsamen Leitfaden zur Auftragsdatenverarbeitung des BayLDA und des BayLfD.

- ☐ Freischaltung der Fernwartungszugriffe nur für konkrete Zwecke und Dauer
- ☐ Deaktivierung der Übertragungen von Dateien – sofern für die Fernwartung nicht erforderlich
- ☐ Vollständige Protokollierung der Fernwartungszugriffe
- ☐ Regelmäßige Kontrolle der Protokolle zur Fernwartung
- ☐ Kryptographisch angemessene Absicherung der Fernwartungszugriffe (z. B. VPN, TLS)
- ☐ Sperren bzw. Unterbinden von Fernwartungszugriffen nach Beendigung eines Dienstleistungsvertrags

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_2_5_Fernwartung.html (BSI)

www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html (BSI)

11 Administratoren

Cyberkriminelle haben leichtes Spiel, wenn sie im Besitz privilegierter Nutzerkonten sind. Auch wenn die Rolle der Administratoren mit ihren weitreichenden Berechtigungen in Notfällen besonders wichtig ist, sind Administratorenkonten nur gezielt einzusetzen.

- ☐ Nicht-privilegierte Standardkonten auch für Administratoren für die sonstige Arbeit außerhalb der administrativen Tätigkeit
- ☐ Regelung, dass nicht mit Administrator-Rechten im Internet gesurft oder E-Mails gelesen/versendet werden
- ☐ Sehr starke Passwörter für lokale Admin-Konten (z. B. mind. 16-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden PC)
- ☐ Soweit möglich konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung bei Anwendungen, die dies insbesondere für Administratoren unterstützen
- ☐ Keine Abhängigkeit des gesamten Betriebs von einzelnen Beschäftigten mit Administratorenkennungen
- ☐ Gewährleistung, dass bei einem Ausfall (z. B. Krankheit) von mehreren Beschäftigten der IT-Administration die Arbeitsfähigkeit des Betriebs aufrechterhalten werden kann
- ☐ Bestellung eines Informationssicherheitsbeauftragten oder eines Verantwortlichen für die Informationssicherheit mit klar geregelter Kompetenzzuweisung

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_2_... (BSI)

12 Notfall-Konzept

Die Verfügbarkeit wichtiger medizinischer Geräte, von Kommunikationsprogrammen und grundlegenden Daten, ist für einen reibungslosen Betriebsalltag von Bedeutung. Ein Notfall-Konzept ist daher relevant, um bei einem Ausfall vorbereitet zu sein.

- ☐ Vorhandensein eines Notfallkonzepts, das auch tatsächlich für die relevanten Personengruppen in Papierform greifbar ist
- ☐ Regelmäßige Prüfung der Aktualität des Notfallkonzepts und ggf. Anpassung
- ☐ Ermöglichung der Wiederaufnahme des Betriebs durch verschiedene bereits im Voraus geplante und getestete Ablaufstufen im Notfallplan
- ☐ Vorhandensein von Notfall-Reserve-Hardware, um Ausfälle zu kompensieren (z. B. ausgemusterte Geräte, Ersatzbeschaffungen)
- ☐ Rasche Aufbaumöglichkeit einer Ausweichinfrastruktur (z. B. externe Server, mobile Kommunikation, Notfall-E-Mail-Adressen)
- ☐ Vorhandensein eines gut strukturierten und aktuellen Netzplans
- ☐ Information der Beschäftigten über die Ansprechpartner bzw. internen Kontaktpersonen bei Sicherheitsvorfällen
- ☐ Gewährleistung der Erreichbarkeit der internen Kontaktperson(en) für Sicherheitsvorkommnisse
- ☐ Angabe der relevanten zuständigen Behörden und Meldeverpflichtungen im Notfallplan
- ☐ Sichere Aufbewahrung zentraler Administrationszugangsdaten (z. B. im Tresor) und Zugangsmöglichkeiten im Notfall

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Schulung/Webkurs1004/Webkurs1004_node.html (BSI)

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/DER/DER_2_1_Behandlung... (BSI)

www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_128.pdf?__blob... (Allianz für Cybersicherheit)

13 Netztrennung

Befinden sich Angreifer erst einmal im eigenen Netzwerk, scannen sie u. a. nach Datenschätzen, angebundenen Geräten und Ausbreitungsmöglichkeiten. Wenn die eigenen IT-Netze, z. B. zum medizinischen Bereich, zur Verwaltung und zum Internet, strikt mit Netzwerkkomponenten voneinander getrennt sind, werden die Auswirkungen des Angriffs minimiert.

- ☐ Restriktive (physikalische) Trennung medizinischer Netze von Verwaltungsnetzen (mittels Firewall-Systemen)
- ☐ Betrieb der über das Internet erreichbaren Server in einer demilitarisierten Zone (DMZ) (z. B. E-Mail-Server, Webserver, VPN-Endpunkte)
- ☐ Geregelter Prozess zur ordnungsmäßigen Konfiguration der Firewalls und regelmäßige Überprüfung der selbigen (z. B. zu der Notwendigkeit von Freigaben)
- ☐ Protokollierungen auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren
- ☐ Automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen

>> Weitere Informationen:

www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/NET/NET_1_1_Netzarchitektur... (BSI)

14 Firewall

Zugriffsversuche von außen auf den eigenen Betrieb sind nicht zu verhindern. Wichtig ist es, diese bestmöglich durch ein Firewall-Regelwerk zu blockieren und zu protokollieren, um Gefahren zu erkennen und Sicherheitsmaßnahmen bedarfsgerecht zu gestalten.

- ☐ Abschottung aller internen Server, PCs und am internen Netz angebundenen medizinischen Geräte vom Internet durch eine Firewall gegenüber dem Internet; „Air Gap", also die Trennung vom Netzwerk, sollte bei kritischen Systemen, sofern verhältnismäßig möglich, umgesetzt werden
- ☐ Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IP-Adressen von extern und periodischer Pentests)
- ☐ Einsatz von ausreichend qualifiziertem Personal/Dienstleister zur Konfiguration der Firewall
- ☐ Monitoring, um Zugriffsversuche zu erkennen

>> Weitere Informationen:

www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/Routenplaner/NET/net_d.html?cms_pos=5 (Allianz für Cybersicherheit)

www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_134.pdf?__blob... (Allianz für Cybersicherheit)

15 Datenschutzbeauftragter (DSB)

Mangelhafte Sicherheitsstrukturen in einer Organisation können den Betriebsablauf gefährden. Wichtig ist es daher, bestehende Kompetenzen zu nutzen und nicht nur IT-Verantwortliche, sondern auch den DSB bei der Umsetzung von Sicherheitsfragen einzubinden.

- ☐ Konsequente Einbindung des DSB bei Sicherheitsfragen
- ☐ Ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema
- ☐ Durchführung von regelmäßigen Audits des DSB nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung
- ☐ Kenntnis der zuständigen Datenschutzaufsichtsbehörde
- ☐ Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DS-GVO (Verletzung der Sicherheit)
- ☐ Unterstützung der Zusammenarbeit des DSB mit dem Informationssicherheitsbeauftragten (ISB) durch die Unternehmensleitung (Info: bei der Auswahl und Umsetzung der technisch-organisatorischen Maßnahmen nach Art. 32 DS-GVO können Synergien durch den DSB und den ISB genutzt werden)

>> Weitere Informationen:

www.lda.bayern.de/de/thema_datenschutzbeauftragter.html (BayLDA)

www.datenschutz-bayern.de/docs/verwaltung/aufgaben_bdsb.html (BayLfD)

16 Social Engineering

Kriminelle erschleichen sich durch Social-Engineering-Angriffe wichtige Informationen für nachgelagerte Cyberattacken. Entsprechend ist es wichtig, allen Beschäftigten den „Sicherheitsfaktor Mensch" in geeigneten Schulungen zu erläutern.

- ☐ Regelmäßige Schulung der Beschäftigten bezüglich aktueller und häufiger Cyberangriffe (z. B. einmal pro Jahr)
- ☐ Konsequente Einweisung neuer Beschäftigter zum fachgerechten Umgang mit den IT-Komponenten und Verhalten bei Social-Engineering Angriffen
- ☐ Sensibilisierung neuer Beschäftigter bezüglich IT-Risiken vor der Aufnahme der Datenverarbeitung (z. B. auch bei Aushilfskräften)
- ☐ Darstellung des Ablaufs von Social-Engineering-Angriffen zur Sensibilisierung der Beschäftigten (z. B. Möglichkeit der Manipulation von Telefonnummern)
- ☐ Informationen an die Mitarbeiter über Meldewege (z. B. durch den ISB oder DSB) und Zuständigkeiten

>> Weitere Informationen:

www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Social_Engineering/social... (Allianz für Cybersicherheit)

www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Awareness/awareness... (Allianz für Cybersicherheit)

Aktuelle Version zum Download:

www.lda.bayern.de/best_practice_medizin
www.datenschutz-bayern.de/best_practice_medizin

Hier finden sich auch nochmals die Links zu den weiteren Informationen.

Herausgeber und Kontakt:

Der Bayerische Landesbeauftragte für den Datenschutz
(BayLfD) | Wagmüllerstraße 18 | 80538 München
www.datenschutz-bayern.de | Tel.: 089 212672-0
poststelle@datenschutz-bayern.de

Bayerisches Landesamt für Datenschutzaufsicht
(BayLDA) | Promenade 18 | 91522 Ansbach
www.lda.bayern.de | Tel.: 0981 180093-100
poststelle@lda.bayern.de