FSDZ RECHTSANWÄLTE & NOTARIAT AG
ZUGERSTRASSE 76b
CH-6340 BAAR
Tel. ++ 41 41 727 60 80
Fax.++ 41 41 727 60 85
praktikanten@fsdz.ch

CHECKLISTE FÜR HOMEOFFICE UND CYBERSICHERHEIT FÜR MEDIZINISCHE EINRICHTUNGEN

29.10.2020

file:///Volumes/homes/DISKs-Public/03 ORGANISATION/99 Urteile zur Publikation/Checklisten - Endversion - 29-10-2020.docx

Quelle: BayLDA

Interne Verfasserin: RA Lukas Fässler, BLaw Alessio Frongillo

Das BayLDA hat Checklisten für Homeoffice und für die Cybersicherheit für medizinische Einrichtungen publiziert. Hier das Wichtigste in Kürze:

Datenschutzrechtliche Regelung bei Homeoffice:

Checkliste mit Prüfkriterien nach DS-GVO

1. **Arbeitsumgebung:**
   Die Vertraulichkeit und Verfügbarkeit der Daten sollte wie im Büro sichergestellt sein.

2. **Genutzte Hardware:**
   Es sollten nur dienstlichen Geräten genutzt werden, private Geräte sollten nur im Ausnahmefall zur Anwendung kommen.

3. **Umgang mit Papierdokumenten:**
   Wo Betriebe noch nicht komplett digitalisiert wurden, sollte der Umgang mit Papierdokumenten vorsichtig sein. Etwa die Entsorgung sollte nicht durch den Hausmüll erfolgen, sondern durch einen Aktenvernichter.

4. **Nutzung von Konferenzsystemen:**
   Bei der Wahl der Videokonferenzlösung sollten bestimmte Anforderungen beachtet werden. So sollte u.a. der Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO abgeschlossen sein oder Verwendung einer Transportverschlüsselung (z.B. TLS) verwendet werden.

5. **Sicherheit:**
   Wie etwa die Anbindung an das Firmennetz durch eine verschlüsselte VPN-Verbindung, die Nutzung heimischer WLAN mit starken Passwörtern oder das Durchführen von täglichen Updates der Virensignaturen auf dem Homeoffice-Notebook wie die Pin-Sperre bei dienstlichen Smartphones.

6. **Nutzung von Cloud-Diensten:**
   Zu beachten gilt u.a., dass der Vertrag nach Art. 28 DS-GVO abgeschlossen ist, dass die Nutzer starke Passwörter nutzen und dass sie in Bezug auf Risiken durch Phishing-Attacken auf Cloud-Konten sensibilisiert werden.

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt,
BSc Wirtschaftsinformatik
Tel.: ++41 41 541 79 60
roman.boehni@boehnilaw.ch
www.boehnilaw.ch

de la cruz beranek Rechtsanwälte AG
Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin
delacruz@delacruzberanek.com

Nicole Beranek Zanon
Rechtsanwältin und Notarin[1,2]
beranek@delacruzberanek.com

Industriestrasse 7
CH-6300 Zug
Tel.: ++41 41 710 28 50
Fax: ++41 41 710 90 76
www.delacruzberanek.com
UID: CHE-389.928.945 MWST

Lichtsteiner Rechtsanwälte und Notare
Urs Lichtsteiner
lic. iur. Rechtsanwalt[1,2], MSc (Stanford)
lichtsteiner@lilaw.ch

Zugerstrasse 76B,
CH-6340 Baar
Tel.: +41 41 726 90 00
Fax: +41 41 726 90 05
www.lilaw.ch
info@lilaw.ch
UID: CHE-404.805.335 MWST

Anwaltskanzlei Dr. Weltert
Hans M. Weltert
Dr. iur. Rechtsanwalt[1,4]
hans.weltert@raweltert.ch

Matthias Heim
lic.iur. Rechtsanwalt[1,4]
matthias.heim@raweltert.ch

Michael Heim
lic.iur. Rechtsanwalt[1,4]
michael.heim@raweltert.ch

Bahnhofstrasse 10
CH-5001 Aarau
Tel.: +41 62 832 77 33
Fax: +41 62 832 77 34
www.raweltert.ch
info@raweltert.ch
UID: CHE-100.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug
[3] Eingetragen im Anwaltsregister des Kantons Zürich
[4] Eingetragen im Anwaltsregister des Kantons Aargau

7. **Nutzung von Messenger-Diensten:**
   Damit die Unternehmenskommunikation gewährleistet ist, ist die Nutzung von Messenger-Diensten unabdingbar. Beachtet werden sollte, dass die Kommunikation der Inhalte Transport und Ende- zu Ende-Verschlüsselt erfolgt. U.a. auch dass keine Verwendung oder Weitergabe der Verkehrsdaten an den Anbieter für Zwecke wie Werbung oder Profiling weitergegeben werden.

8. **Allgemeine organisatorische Regelungen:**
   Stets einen Überblick über die Mitarbeiter, die im Homeoffice arbeiten behalten oder über die Geräte die ins Homeoffice gebracht werden. Auch das Weiterleiten von betrieblichen E-Mails an privaten Konten sollte unterlassen werden. Es wird zudem eine schriftliche Verpflichtung der Mitarbeiter empfohlen, dass sich diese an die Regelungen halten.

   Die detaillierte Checkliste finden sie hier.

Cybersicherheit für medizinische Einrichtungen:

Checkliste mit Prüfkriterien nach Art. 32 DS-GVO

1. **Patch Management:**
   Eingesetzte Softwares sollten durch regelmässigen Sicherheitsupdates aktuell gehalten werden.

2. **Malware-Schutz:**
   Ein wirksamer Antivirenschutz ist einzusetzen.

3. **Ransomware-Schutz:**
   Proaktive Massnahmen zum Schutz gegen Verschlüsselungstrojaner sind unabdingbar, damit früh genug drohende Risiken (wie Lösegeldforderungen) abgefangen werden können.

4. **Passwort-Schutz:**
   Es sollten starke Passwörter eingesetzt werden.

5. **Zwei-Faktor-Authentifizierung:**
   Schützenswerte Zugänge sollten nebst einem Passwort durch eine Zwei-Faktor-Authentifizierung gesichert sein.

6. **E-Mail Sicherheit:**
   Regelungen, um den E-Mail Verkehr zu sichern, wie die «Nur-Text-Format» Einstellung, damit werden manipulierte Links sichtbar gemacht.

7. **Backups:**
   Regelmässige Backups sind wichtig, um bei einem IT-Ausfall wichtige Datenbestände zu sichern.

8. **Home-Office:**
   Dazu kann auf die Checkliste oben verwiesen werden.

9. **Externe Abrufmöglichkeit für Laborergebnisse:**
   Um Hackerangriffe zu verhindern sollten Schutzmassnahmen eingesetzt werden, wie die kryptografisch angemessene Absicherung der Zugriffe oder sichere und für jeden Einsender unterschiedliche Zugangsdaten auszugeben.

10. **Fernwartung:**
    Für Dienstleistern, die sich durch Fernwartung auf Systeme einschalten sind eingespielte Sicherheitsabläufe besonders wichtig. Etwa durch die vollständige Protokollierung von Fernwartungszugriffe.

11. **Administratoren:**
    Administratorenkoten sollten nur gezielt eingesetzt werden, da falls Cyberkriminelle in Besitz Administratorenkoten kommen sehr leichten Zugriff auf die restliche Konten haben.

12. **Notfall-Konzept:**
    Um den reibungslosen Betriebsalltag zu gewährleisten ist ein Notfall-Konzept beim Ausfall der medizinischer Geräte, Kommunikationsprogramme oder grundlegende Daten relevant.

13. **Netztrennung:**
    Wenn der eigene IT-Netz strikt mit Netzwerkkomponente voneinander getrennt werden, kann die Auswirkung der Angriffe miniert werden.

14. **Firewall:**
    Firewall-Regelwerke sind wichtig, um Zugriffsversuche möglichst gut zu blockieren.

15. **Datenschutzbeauftragter (DSB):**
    Es ist wichtig nicht nur IT-Verantwortliche sondern auch Datenschutzbeauftrage bei der Umsetzung von Sicherheitsfragen einzubinden.

16. **Social Engeneering:**
    Alle Beschäftigte sollten geeignete Schulungen zum «Sicherheitsfaktor-Mensch» erhalten.

Die detaillierte Checkliste finden sie hier.

Bei Fragen kontaktieren Sie unsere Kanzlei.

29.10.2020