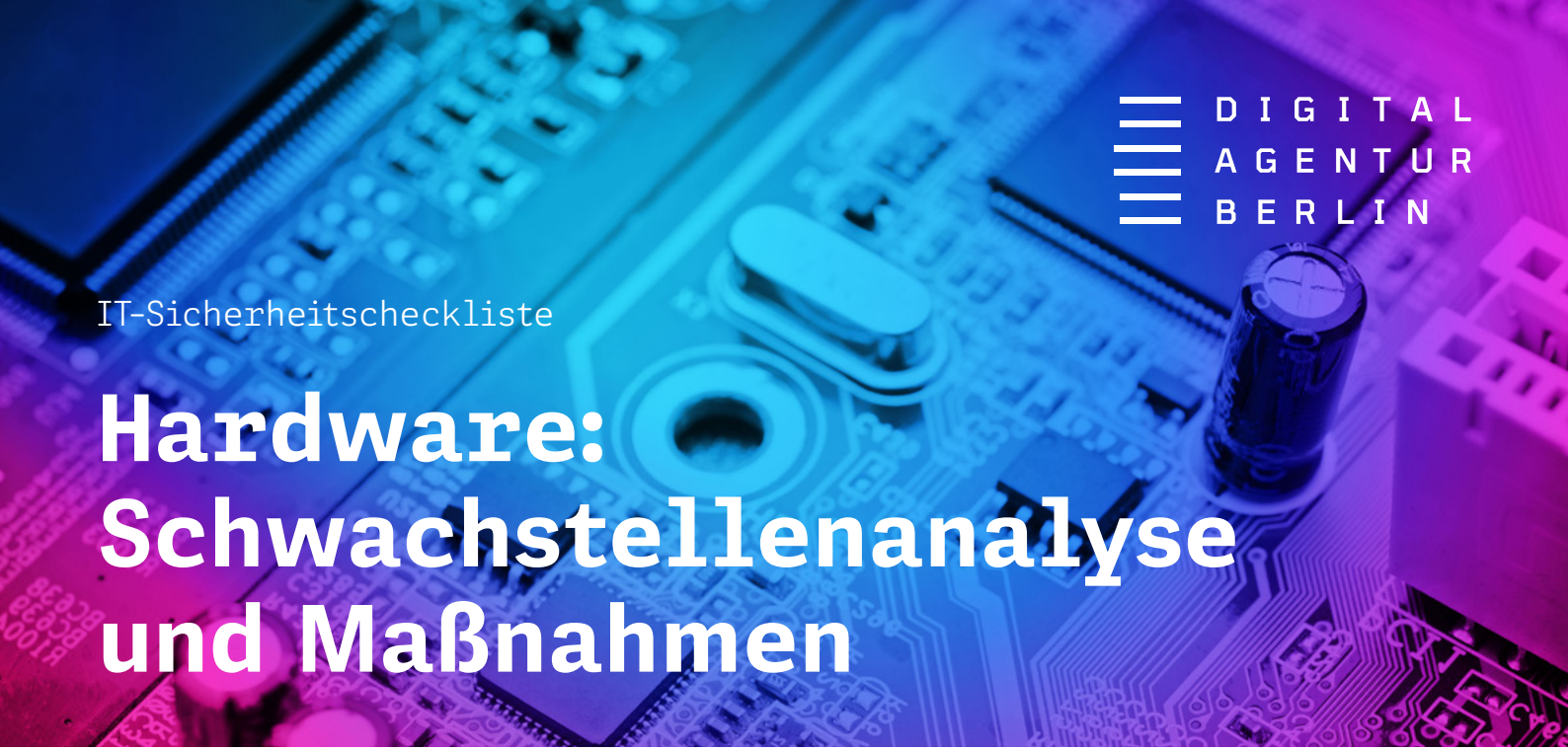

DIGITAL AGENTUR BERLIN

IT-Sicherheitscheckliste

Hardware: Schwachstellenanalyse und Maßnahmen

Der Begriff „**Hardware**“ wird im Folgenden für alle technischen Geräte verwendet, die zur Datenverarbeitung im Unternehmen, mobil, unterwegs oder am Heim-Arbeitsplatz verwendet werden. Z. B. PCs, Laptops, Tablet-Computer, Smartphones, Handys, USB-Sticks, externe Festplatten, Drucker, Bildschirme, Mikrophone, Kameras, Router, Server, usw.

Prüfen Sie anhand der folgenden 10 Fragen, wie Ihr Unternehmen in Bezug auf IT-Sicherheit aufgestellt ist. Wenn Sie eine Frage mit **Nein** beantworten, haben wir für Sie Beispiel-Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1. Haben Sie eine Liste aller datenverarbeitungsfähigen Geräte (Hardware), die im Unternehmen eingesetzt werden?	☐	☐	▪ Erstellen und regelmäßige Pflege einer Inventarliste ▪ Einsatz einer Inventarisierungssoftware je nach Umfang möglich
2. Gibt es für alle Mitarbeitenden eine Richtlinie, Anweisungen oder schriftliche Regelungen für die zulässige Nutzung von dienstlicher Hardware?	☐	☐	Verfassen von Anleitungen bzw. Anweisungen für den sicheren Umgang mit Hardware im Unternehmen, zuhause oder unterwegs
3. Gibt es einen schriftlichen Ablaufplan für die Aus- und Rückgabe von Arbeitsgeräten und Hardware (Eintritt, Versetzung, Austritt)?	☐	☐	▪ Dokumentieren, wer welche Geräte erhält und zurückgibt ▪ Einsatz einer Checkliste um Vollständigkeit sicherzustellen

Hardware: Schwachstellen-analyse und Maßnahmen

DIGITAL AGENTUR BERLIN

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
4.	**Sind Büroräume und ggf. Produktionsflächen (insbesondere Bereiche mit Hardware) gegen unbefugten Zutritt gesichert?**	☐	☐	▪ Schlüsselverwaltung ▪ eletronische Zutrittssysteme ▪ einbruchssichere Türen, Schlösser und Fenster ▪ alarmgesicherte Ein- und Ausgänge (auch Notausgänge) ▪ Videoüberwachung ▪ Zutritt nur für genehmigte Personen ▪ Besucherregistrierung
5.	**Wenn vorhanden: Sind Serverräume und IT-spezifische Lagerflächen (z. B. für Festplatten) mit erweitertem Zutritts- bzw. Einbruchsschutz gesichert?**	☐	☐	▪ Einrichtung eines Zwei-Faktor-Zuganges (Besitz eines Schlüssels und Kenntnis eines PIN-Codes) ▪ Zutritt nur für einen ausgewählten Personenkreis ▪ Serverraum nicht für andere Zwecke nutzen ▪ weitere Infos unter *berlin.de/polizei*[1]
6.	**Haben Sie präventive Maßnahmen für den Fall eines Diebstahls von Hardware getroffen?**	☐	☐	▪ Dokumentieren der Seriennummern der Geräte (z. B. IMEI-Nr. von Handys), SIM-Karten-Nr. samt Kunden-Nr. & Kundenkennwort zur Sperrung beim Netzanbieter ▪ Dokumentation über Inventarliste (siehe 1.) ▪ Aktivieren von Festplatten- und Geräteverschlüsselung (soweit vorhanden) ▪ Aktivieren von Fernortungsdiensten (soweit vorhanden) ▪ Infos unter *verbraucherzentrale.de*[2]
7.	**Sind die IT-Geräte insbesondere im Serverraum vor Stromausfall, Wasser, Überhitzung und Überspannung geschützt?**	☐	☐	▪ Rauchmelder ▪ geeigneter Feuerlöscher (z. B. CO2-Feuerlöscher) ▪ Notstromaggregat ▪ Videoüberwachung ▪ Hinweis: Prüfen Sie, ob ein ausreichender Versicherungsschutz besteht

Hardware: Schwachstellen-analyse und Maßnahmen

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
8.	**Findet eine ordnungsgemäße Instandhaltung und Wartung von IT-Betriebsmitteln durch Interne oder externe Dienstleister statt?**	☐	☐	▪ Regelmäßige protokollierte Updates der Betriebssysteme und Treiber (Windows, iOS, Linux) durchführen ▪ Regelmäßige Instandhaltung via Inventur (z.B. jährlich) oder via stetiger Wartung ▪ Elektrotechnische Prüfung regelmäßig durchführen
9.	**Werden nicht mehr benötigte Datenträger (z.B. Festplatten und USB-Sticks) sicherheitskonform entsorgt?**	☐	☐	▪ Sichere Löschprozeduren verwenden (z.B. mehrfaches Überschreiben) oder physisch Vernichten (gem. DIN-Norm 66399) ▪ Hinweis: Je höher die Sicherheits-Stufe der gespeicherten Daten, um so effektiver muss der Löschprozess sein
10.	**Gibt es einen Notfallplan, in dem Maßnahmen bei Zerstörung, Entwendung, Defekt von Hardware definiert werden?**	☐	☐	▪ Kommunikation des Notfallplans und von Meldewegen an Mitarbeitende ▪ Wesentliche Ersatzteile auf Lager haben ▪ Back-up im Notfall auf verschlüsselter Festplatte, NAS oder Tape (Daten-Band) ▪ Ggf. prüfen, ob es sich um einen Datenschutz-vorfall handelt

1 www.berlin.de/polizei/aufgaben/praevention/diebstahl-und-einbruch/artikel.125014.php
2 www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/handy-verloren-sperren-lassen-anzeige-erstatten-13870

Gerne unterstützen wir Sie bei der Umsetzung der Maßnahmen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Wir freuen uns auf Ihre Anfrage an **info@digitalagentur.berlin**.

Weitere Informationen finden Sie auch auf **digitalagentur.berlin** oder rufen Sie uns unter der **Cyberhotline 030 166 360 580** an.