Selbsttest -Potentielle Gefährdungen für meinen Handwerksbetrieb

	Selbsttest mit 25 Fragen	Zufrieden-stellend in meinem Betrieb geregelt	Weiß ich nicht	Trifft zu
1	Die Datensicherung wird unvollständig und unregelmäßig durchgeführt. Die Datensicherungsmedien werden nicht ausreichend sicher aufbewahrt. Das Zurückspielen des Backups wird kaum getestet.			
2	Auf den Arbeitsplatzrechnern, Notebooks, Tablets und Smartphones werden nur unregelmäßig Sicherheitspatches und Updates eingespielt. Das Virenmanagement findet nur unregelmäßig statt.			
3	Bei den restlichen IT-Systemen, z. B. Netzdrucker oder NAS findet ein Patchmanagement nur unregelmäßig statt.			
4	Die Mitarbeiter verwenden für den Zugriff auf die IT-Systeme und Anwendungen triviale Kennwörter.			
5	Der DSL-Router (z. B. Fritz!Box) hat ein einfaches Zugangskennwort. Die Firmware wird nur unregelmäßig auf eine aktuellere Version geupdatet. Die Fernadministration auf den DSL-Router ist aktiviert.			
6	Die Arbeitsplatzrechner haben keinen besonderen „Surf-Schutz". Die Systempflege von PCs und Notebooks erfolgt unregelmäßig.			
7	Die Mitarbeiter können selbstständig Programme /Apps installieren.			
8	Fremdpersonen können ungehindert ins Gebäude gelangen und sich ohne Aufsicht bewegen.			
9	Welchen Mitarbeitern welche Berechtigungen auf IT-Komponenten, Anwendungen und Daten zugewiesen wurden, können „Datenverantwortliche" nicht nachvollziehen.			
10	Die Standardkennwörter wurden bei der Installation der IT-Systeme nicht geändert.			
11	Die Administrationskennwörter für die einzelnen IT-Komponenten sind einheitlich und allen Administratoren und IT-Dienstleistern bekannt.			
12	In meinem Betrieb können ohne Einschränkungen private Speichermedien, z.B. USB-Sticks, an Arbeitsplatzrechnern, Notebooks oder Tablets angeschlossen werden.			

13	Geschäftsdaten auf Datenträgern werden nur logisch gelöscht und können deshalb mit einfachen Tools wiederhergestellt werden.			
14	Datenträger, Notebooks oder USB-Sticks, die außerhalb des Firmengeländes genutzt werden, sind nicht verschlüsselt.			
15	Auf der Festplatte des Digitalkopierers werden alle Kopier- und Druckaufträge dauerhaft gespeichert, sodass nach Ablauf des Leasingzeit das Gerät mit allen Daten den Handwerksbetrieb verlässt.			
16	Bei E-Mail und Webnutzung können uneingeschränkt Dateien auf Smartphones gespeichert und genutzt werden.			
17	Webseiten mit aktiven Inhalten werden beim Anklicken automatisch ohne vorherige Nachfrage ausgeführt.			
18	Ein Schlüsselbestandsbuch für Büro und Funktionsräume wird nicht geführt, sodass nicht nachvollziehbar ist, wer über welche Zutrittsbefugnisse verfügt.			
19	Einen Überblick über den Bestand und die Ausgabe der (General-)Schlüssel besteht nicht.			
20	Der Reinigungsdienst verfügt über Generalschlüssel und reinigt außerhalb der Geschäftszeiten, wenn alle Mitarbeiter abwesend sind.			
21	Externe IT-Dienstleister haben aus der Ferne uneingeschränkten und unkontrollierten Zugang zu betrieblichen IT-Systemen.			
22	Die Sicherheitseinstellungen auf der Firewall sind nur dem IT-Dienstleister bekannt und können von ihm ohne Absprache mit dem Handwerksbetrieb geändert werden.			
23	Die Mitarbeiter dürfen ihre privaten Geräte (ob Smartphone, Tablet oder Notebook) mit dem Firmen-WLAN verbinden.			
24	Auf dem Firmen-Smartphone sind sowohl dienstliche Daten gespeichert als auch WhatsApp installiert.			
25	In unserem Betrieb fühlt sich niemand zuständig für das Thema Informationssicherheit. Keiner informiert sich regelmäßig über die aktuelle „Sicherheitslage“.			
25 + 1	Das Firmen-WLAN ist mit WPA2 verschlüsselt und hat ein einfaches WLAN-Kennwort mit 8 Zeichen Länge. Das WLAN-Kennwort wird kaum geändert.			

Fazit:
Je mehr Kreuze sich in den beiden rechten Spalten befinden, um so höher wird die Wahrscheinlichkeit eines Datenlecks.