Checkliste: EDV-Infrastruktur und Verfügbarkeit absichern

1 **Relevanz und Thema positionieren.**
Ihre Aufgaben:
1-1 Eignen Sie sich IT-Grundwissen an.
1-2 Vertrauen Sie einem IT-Dienstleister, der Sie unabhängig berät.
1-3 Machen Sie konkrete Pläne, welche IT-Maßnahmen Sie bis wann umsetzen.

2 **Analysieren Sie, wo Risiken lauern.**
Ihre Aufgaben:
2-1 Erstellen Sie eine Liste, welche IT-Geräte im Unternehmen im Einsatz sind. Achten Sie dabei auch darauf, was miteinander vernetzt ist – und sich eventuell durch Segmentierung trennen ließe.
2-2 Erfassen Sie auch die Software und welche Beschäftigten die einzelnen Programme nutzen.
2-3 Achten Sie darauf, wo Ihre Systeme besonders angreifbar sind.

3 **Die „Kronjuwelen" Ihres Unternehmens identifizieren**
Ihre Aufgaben:
3-1 Überlegen Sie, welche die zentralen Daten und Prozesse im Unternehmen sind.
3-1 Kümmern Sie sich als Erstes um die Sicherheit dieser „Kronjuwelen".

4 **Zugriffsrechte beschränken und Software aktualisieren**
Ihre Aufgaben:
4-1 Dokumentieren und beschränken Sie die Zugriffs- und Administratorenrechte innerhalb der Belegschaft.
4-2 Bestimmen Sie eine Person, die dafür zuständig ist, dass Software-Updates und -Aktualisierungen durchgeführt werden.

5 **Firewall und Virenscanner checken**
Ihre Aufgaben:
5-1 Stellen Sie sicher, dass an jeder Schnittstelle vom Unternehmensnetzwerk zum Internet eine Firewall den Zugang kontrolliert.
5-2 Kontrollieren Sie, dass auf jedem Gerät, das auf das Internet zugreifen kann, ein Virenschutz-Programm installiert ist.

6 **Schutz für den DNS der Internetseite überprüfen**
Ihre Aufgabe:
6-1 Informieren Sie sich, wie Ihr DNS-Provider seine Server schützt.

7 **Gefahr im Mailpostfach minimieren**
Ihre Aufgaben:
7-1 Richten Sie einen Spamfilter ein, der eingehende E-Mails vorsortiert.
7-2 Stellen Sie die E-Mail-Postfächer so ein, dass Bilder nicht automatisch heruntergeladen werden.

Checkliste: EDV-Infrastruktur und Verfügbarkeit absichern

8 **Das Team zur menschlichen Firewall ausbilden**
Ihre Aufgaben:
8-1 Geben Sie regelmäßige Schulungen in IT-Sicherheit.
8-2 Sorgen Sie dafür, dass Mitarbeiter die Regeln zur IT-Sicherheit jederzeit nachlesen können.

9 **Datenverlust mit Backups vermeiden**
Ihre Aufgaben:
9-1 Machen Sie einen Plan, welche Daten wie häufig gesichert werden müssen.
9-2 Testen Sie, ob Ihre Backups funktionieren.

10 **Richtlinien für die Qualität von Passwörtern erstellen**
Ihre Aufgabe:
10-1 Erstellen Sie Richtlinien für sichere Passwörter in Ihrem Unternehmen.

11 **2-Faktor-Authentifizierung für wichtige Dienste einrichten**
Ihre Aufgabe:
11-1 Sichern Sie Nutzerkonten für wichtige Online-Dienste per 2-Faktor-Authentisierung.

12 **Schutz im Homeoffice gewähren und verlangen**
Ihre Aufgaben:
12-1 Erstellen Sie einen Leitfaden für sicheres Arbeiten im Homeoffice.
12-2 Installieren Sie auf jedem Gerät, das auf das Internet zugreifen kann, ein Virenschutzprogramm.

13 **Zugriff von extern nur mit VPN-Client ermöglichen**
Ihre Aufgabe:
13-1 Richten Sie ein VPN ein, wenn Beschäftigte von extern auf sensible Firmendaten zugreifen müssen.

14 **Eine Cloud auswählen, die Sie wieder verlassen können**
Ihre Aufgaben:
14-1 Achten Sie bei Cloud-Anbietern darauf, wo die Daten liegen und dass sie exportiert werden können.
14-2 Legen Sie fest, welche Daten in die Cloud sollen.

15 **Einen Plan für den Ernstfall und die Tage danach machen**
Ihre Aufgaben:
15-1 Bereiten Sie eine Notfallkarte vor, auf der steht, was bei einem IT-Notfall zu tun und wer zu informieren ist. Die Informationen müssen regelmäßig aktualisiert werden.
15-2 Legen Sie fest, welche Abteilungen nach einem Angriff als erste wieder arbeiten können müssen.

BEARBEITET VON _____ AM _____ | NÄCHSTE BEARBEITUNG: _____

Quellen: Impulse 10/2021 (Auszugsweise Verwendung) | www.bsi.de | www.uz-online.com