ViCoTec
IT-Sicherheit & Datenschutz

12 goldene Regeln für mehr

Datenschutz & IT-Sicherheit

in kleinen Firmen

ViCoTec
IT-Sicherheit & Datenschutz

"Datenschutz & Datensicherheit sind überhaupt nicht HIP - für Unternehmen aber lebensnotwendig!"

Viele unangenehme Risiken

- Die Anzahl an Hackerangriffen nimmt stetig zu
- IT-Ausfälle sind für Unternehmen oft sehr teuer
- Virenangriffe legen komplette Firmen lahm
- Mitarbeiter sind verunsichert
- Die DSGVO zwingt zum Einsatz aktueller Technik, zu Datenschutzmaßnahmen und zu Backups
- Bei Pannen droht erheblicher Reputationsverlust

Es ist jetzt an der Zeit zu handeln

Mit einfach umzusetzenden Maßnahmen können Sie für Ihre Firma das Sicherheitsniveau um ein Vielfaches steigern.
Dafür haben wir diese 12 Regeln zusammengestellt.

Die 12 Regeln gelten für jedes Unternehmen - reichen aber in manchen Fällen bei weitem nicht aus.

ViCoTec
IT-Sicherheit & Datenschutz

1. Betriebssystem & Software

Nutzen Sie aktuelle Software und spielen Sie regelmäßig Updates und Patches ein - am besten automatisch!

2. Antivirus-Software

Auf dem Server und allen Arbeitsplatzrechnern gehört eine Antivirensoftware, die sich täglich aktualisiert.

3. Firewall

Ihr Internetzugang muss durch eine Firewall geschützt sein!

4. Mitarbeiter

Mitarbeiter müssen regelmäßig zur IT-Sicherheit geschult werden und sie müssen wissen, was im Schadensfall zu tun ist.

5. Passwörter

Jeder Mitarbeiter braucht ein eigenes Passwort. Passwörter müssen mindestens 8 Zeichen mit Groß- und Kleinschreibung und mind. eine Zahl beinhalten. Es dürfen keine Namen oder einfache Wörter benutzt werden. Passwörter müssen in regelmäßigen Abständen gewechselt werden.
Zugänge von ausgeschiedenen Mitarbeitern werden gesperrt!

6. Notfallplan

Im Notfall müssen alle wissen, was zu tun ist oder kurz auf dem Notfallplan nachsehen. Legen Sie fest was zu tun ist, wenn ein Hackerangriff stattfindet.

ViCoTec
IT-Sicherheit & Datenschutz

7. Rechner sperren

Rechner müssen sich nach max. 10 Minuten selber sperren. Beim Verlassen des Arbeitsplatzes wird der Rechner grundsätzlich händisch gesperrt (Windows-Taste + L).

8. Administrator Rechte

Nur der Administrator sollte Administratorrechte haben. Alle anderen Mitarbeiter dürfen auf dem jeweiligen PC nicht als Administrator angemeldet sein.

9. Backups

Machen Sie täglich ein Backup. Lagern Sie ein wöchentliches Backup an einem anderen Ort. Testen Sie regelmäßig die Rücksicherung!

10. E-Mails & Internet

Unbekannte oder unerwartete Anhänge dürfen nicht geöffnet werden. Excel, Word, Powerpoint oder ausführbare Dateien dürfen nicht geöffnet werden. Links werden nur geklickt, wenn es gar nicht anders geht und wenn die Email erwartet wurde. Browser werden aktuell gehalten. Daten werden nur bei SSL Verschlüsselung in den Browser eingegeben und wenn die URL bekannt ist.

11. Mobile Geräte

Laptops benötigen eine explizite Festplattenverschlüsselung und ein starkes Passwort. Handys benötigen Passwort oder PIN.

12. WLAN

Gäste müssen sich über ein Gast-WLAN einwählen - niemals ins Haupt-WLAN. Passwörter müssen stark sein und regelmäßig gewechselt werden. WLANs müssen verschlüsselt sein.

ViCoTec
IT-Sicherheit & Datenschutz

Sogar HELDEN brauchen Datenschutz.

Digitale Selbstverteidigung für Unternehmen, die digitale Chancen nutzen und Risiken begrenzen wollen.

Datenschutz

- Datenschutzberatung
- Datenschutzbeauftragter

IT-Sicherheit

- Sicherheitsaudits
- IT-Sicherheitsberatung

Schulungen

- Datenschutz für Mitarbeiter
- IT-Sicherheit am Arbeitsplatz
- Datenschutz Crashkurs für Geschäftsführer

ViCoTec IT-Sicherheit und Datenschutz GmbH & Co. KG
August-Wilhelm-Kühnholz Str. 5
26135 Oldenburg

0441 2057 2220
info@vicotec.de

www.vicotec.de
www.datenschutz-oldenburg.de