

Wie steht es um Ihre IT-Sicherheit?

Viele Angriffe bleiben lange Zeit unbemerkt. Die Täter installieren versteckt Schadsoftware und lassen diese einige Zeit schlummern. So können nach und nach Daten aus dem Unternehmen gesammelt werden, bis die Täter am Tag X zuschlagen.

Mit regelmäßigen Updates und maßgeschneiderten Sicherheits-Lösungen lassen sich die Risiken Ihrer IT auf ein Minimum begrenzen. Übersehene Kleinigkeiten können sich zu existenzbedrohenden Problemen und hohen Kosten entwickeln.

Basis-Security-Check: Testen Sie jetzt in nur 3 Minuten Ihre IT-Sicherheit!

Können Sie alle Fragen mit JA beantworten? Glückwunsch, dann haben Sie schon einen guten Grundstein in Richtung IT-Security gelegt. Hacker haben es nicht so leicht bei Ihnen sensible Daten zu klauen. Doch sollte bereits eine Frage mit NEIN beantwortet werden, ist es an der Zeit zu handeln. Gerne helfen Ihnen die Digital.Experts. von ProComp diese Lücke zu schließen.

Frage	Ja	Nein
Homeoffice		
Sind Festplatten und Daten verschlüsselt?		
Sind externe Geräte und Standorte angebunden?		
Gibt es eine Zweifaktorauthentifizierung für die VPN-Einwahl?		
Handelt es sich ausschließlich um firmeneigene Geräte?		
Befinden sich sensible Daten auf den Geräten (z.B. Emails, Adresslisten)?		
Firewall / Internetanbindung		
Ist eine professionelle Firewall im Einsatz?		
Wird die Firewall regelmäßig geprüft, gepatcht und gepflegt?		
Gibt es VPN-Tunnel? Sind hier Zugriffe klar geregelt und wird eine starke Verschlüsselung angewendet?		
Ist ein Content Filter implementiert? (Schutz vor gefährlichen Downloads, Sperren unerwünschter Websites > Jugendschutz)		
Gibt es eine Spamschutzlösung zum Schutz vor schadhaften E-Mails?		
Arbeitsplatz		
Werden installierte Anwendungen regelmäßig gepatcht?		

Arbeiten die Benutzer an Ihren Clients ohne lokale Administratorrechte?		
Werden Peripheriegeräte überwacht bzw. kontrolliert?		
Wird eine Virenschutzlösung nach neuestem Stand der Technik eingesetzt?		
Rechenzentrum		
Gibt es eine physikalische Zutrittskontrolle und Videoüberwachung?		
Werden Betriebssysteme und installierte Anwendungen regelmäßig gepatcht?		
Gibt es ein Offline-Backup?		
Mitarbeiter		
Werden Ihre Mitarbeiter regelmäßig zum Thema IT-Security sensibilisiert?		
Wird der Wissensstand regelmäßig kontrolliert?		
Sind Verhaltensregeln zur IT-Sicherheit definiert, schriftlich fixiert und den Mitarbeitern bekannt?		
Übergreifende Themen		
Gibt es Kennwortrichtlinien (komplexe Kennwörter, die regelmäßig geändert werden müssen) für alle Systeme?		
Gibt es ein durchgängiges Patchmanagement (Betrifft alle Systeme: Switches, Apps, Firewalls, Smartphones, Server, Firmware etc.)?		
Gibt es ein automatisiertes Managementsystem für Passwörter und Zugänge?		
Gibt es eine Dokumentation der gesamten IT-Infrastruktur?		

ACHTUNG! Dies ist nur ein Basis-Check.

Wie können Sie Ihr Unternehmen schützen?

- Bestandsaufnahme der aktuellen IT-Infrastruktur
- Bewertung der Lage
- Erfassung vorhandener Schutzmaßnahmen
- Ergänzung/Implementierung notwendiger Schutzmaßnahmen um das Risiko zu senken