Kreissparkasse Heinsberg

„Sicherer IT-Betrieb“

In nahezu jedem Unternehmen basieren existenzielle Geschäftsprozesse auf der Funktionsfähigkeit der IT. Wir geben Denkanstöße und informieren Sie über die häufigsten Versäumnisse der Unternehmen im Mittelstand und zeigen mögliche IT-Risiken auf:

Unzureichende Informationssicherheitsstrategie
Informationssicherheit wird lediglich als Kostentreiber und Behinderung gesehen. Besonders bei Neuanschaffungen werden Sicherheitseigenschaften häufig vernachlässigt. Ein Beispiel in diesem Zusammenhang ist die rasant wachsende Zahl völlig ungesicherter drahtloser Netze. Unzählige Firmen „veröffentlichen“ somit unfreiwillig ihre vertraulichen Daten.

Dauerhafte Prozesse zur Beibehaltung des Sicherheitsniveaus fehlen
Sicherheit wird häufig nur im Rahmen einzelner Projekte geschaffen. Häufig wird jedoch versäumt, zugleich verlässliche Prozesse zu definieren, die die im Projektverlauf erarbeiteten Ergebnisse und Ziele dauerhaft erhalten und fortschreiben.

Sicherheitsvorgaben sind nicht dokumentiert
Viele große Unternehmen verfügen über eine schriftlich fixierte Sicherheitsrichtlinie. In den meisten kleineren Unternehmen ist dies nicht der Fall. Viele Richtlinien sind darüber hinaus zu abstrakt formuliert und lassen zuviel Interpretationsspielraum.

Kontrollmechanismen und Aufklärung im Fall von Verstößen fehlen
Bestehende Sicherheitsrichtlinien und –vorgaben sind nur wirksam wenn ihre Einhaltung auch kontrolliert wird.

Die Rechtevergabe wird nicht restriktiv genug gehandhabt
Da PCs und Server einer Organisation in der Regel untereinander vernetzt sind, kann ohne geeignete Zugriffsbeschränkungen oftmals auf die Daten anderer Benutzer bzw. Rechner zugegriffen werden. Weitreichende Berechtigungen können so durch Unkenntnis oder beabsichtigt missbraucht werden.

IT-Systeme sind schlecht konfiguriert
Durch Fehler bei der Administration entstehen in der Praxis die mit Abstand meisten Sicherheitslücken - und nicht etwa durch Softwarefehler.

Systeme sind gegen offene Netze unzureichend abgeschottet
Informationen, Systeme und Teilnetze werden oftmals gar nicht oder nur unzureichend von offenen Netzen abgeschottet. Selbst die Existenz einer Firewall sagt nichts über den tatsächlichen Sicherheitszustand aus. Eine Überprüfung durch externe Sicherheitsspezialisten zeigt in vielen Fällen gravierende Sicherheitslücken auf.

Verfügbare Sicherheits-Updates werden nicht eingespielt
Administratoren spielen oftmals Sicherheits-Patches nicht rechtzeitig ein.

Räume und IT-Systeme sind ungenügend gegen Diebstahl oder Vandalismus geschützt
Gekippte Fenster über Nacht, unverschlossene IT-Räume, unbeaufsichtigte Besucher oder im Auto zurückgelassene Notebooks bieten ungebetenen Gästen vielfältige Möglichkeiten. Schwerer als der Verlust von Hardware durch Diebstahl wiegt im Allgemeinen der Verlust von Daten. Welche Risiken sind durch Ihre Versicherungen abgedeckt (z.B. Ersatz Hardware, Software, Schäden am Gebäude)?

Daten sind unzureichend vor Elementarschäden geschützt
Datensicherung wird in vielen Unternehmen sehr aufwendig betrieben. Aber was passiert, wenn Ihr Unternehmen einem Brand oder Hochwasser zum Opfer fällt? Haben Sie dann noch Zugriff auf eine externe Datensicherung? Verfügen Sie über eine Elektronikversicherung und Betriebsunterbrechungsversicherung? Ist die Entsorgung versichert?