Sicherheit ist ein Grundbedürfnis des Menschen - und damit unserer Gesellschaft. Gerade in Zeiten von Globalisierung, steigender Mobilität und wachsender Abhängigkeit der Unternehmen von Informations- und Kommunikationstechnik nimmt das Sicherheitsbedürfnis immer mehr zu.

Wachsende Komplexität und die damit verbundene **Gefahr massiver wirtschaftlicher Schäden in Folge von IT-Risiken** erhöhen den Handlungsdruck, durch
aktives IT-Sicherheitsmanagement
Schäden zu verhindern und das Restrisiko zu minimieren. Die Verantwortung beschränkt sich keineswegs auf die jeweiligen IT-Fachabteilungen. Vielmehr gilt:
Sicherheit ist Chefsache!
Dem hat auch der Gesetzgeber Rechnung getragen. Verschiedene Gesetze und Regelungen, wie z.B. die
EU Datenschutz Grundverordnung (EU-DSGVO),
und die damit verbundenen hohen Geldbußen bei Verstößen gegen deren Richtlinien (bis zu 20 Mio. Euro oder 4% des Gesamtumsatzes), haben auch Auswirkungen auf Geschäftsführungs- bzw. Vorstandsebene im Falle von Versäumnissen.

Eine weit verbreitete Ansicht ist, dass **IT-Sicherheitsmaßnahmen** zwangsläufig mit hohen Investitionen in Sicherheitstechnik und der Beschäftigung von hoch qualifiziertem Personal verknüpft sind. Dem ist jedoch nicht so. Die wichtigsten Erfolgsfaktoren sind gesunder Menschenverstand, durchdachte organisatorische Regelungen und zuverlässige - gut informierte Mitarbeiter, oder, wenn man sich diese nicht leisten kann, kompetente IT Dienstleister, die Sicherheitserfordernisse kompetent und routiniert umsetzen.

Die Erstellung und Umsetzung eines wirksamen und effektiven **IT-Sicherheitskonzeptes** ist daher dringend zu empfehlen und muss auch nicht unbedingt teuer sein. Im Rahmen dieses Sicherheitskonzepts werden die bestehenden Sicherheitsmaßnahmen analysiert und diese auf die Erfordernisse einer modernen Sicherheitsarchitektur adaptiert bzw. erweitert, sodass ein
gesamtheitlicher Schutz gegenüber Sicherheitsbedrohungen
unterschiedlicher Art, wie z.B. Datendiebstahl, Datenverlust, Malware, Ransomware und Viren gewährleistet wird.

Eine andere **weit verbreitete Fehleinschätzung betrifft den eigenen Schutzbedarf**. Oft stößt

man auf die folgenden Aussagen:

„Bei uns ist noch nie etwas passiert“. Diese Aussage ist mutig. Vielleicht hatten Sie bisher nur Glück oder es hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt!

„*Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.“* Diese Aussage ist sehr unbedacht. Bei sorgfältiger Betrachtung von möglichen Schadensszenarien zeigt sich schnell: es gibt eine Vielzahl an Dokumenten und Informationen, die persönliche Daten oder wichtige Geschäftsinformationen enthalten und die somit vielfältigen Missbrauch ermöglichen, wenn sie in die falschen Hände fallen - sowohl intern als auch extern. Vorallem ist hier anzumerken, dass gerade die EU Datenschutzgrundverordnung einen Verlust bzw. Missbrauch von personenbezogenen Daten mit sehr hohe Geldstrafen ahndet.

„Unser Netz ist sicher.“ Die Fähigkeiten potentieller Angreifer - egal ob es sich hierbei um Viren, Hacker oder vielleicht sogar eigene Mitarbeiter handelt - werden oft unterschätzt. Hinzu kommt, dass selbst ein erfahrener Netz- oder Sicherheitsspezialist nicht alles wissen und gelegentlich Fehler machen kann. Externe Überprüfungen decken nahezu immer ernste Schwachstellen auf und sind ein guter Schutz vor „Betriebsblindheit“.

„Unsere Mitarbeiter sind vertrauenswürdig.“ Es ist zwar gut, wenn man Vertrauen in die eigenen Mitarbeiter hat, aber verschiedene Statistiken zeichnen ein anderes Bild: Die Mehrzahl der Sicherheitsverstöße wird durch eigene Mitarbeiter verursacht. Dabei muss nicht immer Vorsatz im Spiel sein. Auch durch Versehen, Unachtsamkeit, Übereifer oder Neugierde gepaart mit mangelndem Problembewusstsein entstehen manchmal große Schäden

Jeder sollte sich bewusst machen: **Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess** . Stellen Sie sich daher immer wieder die folgenden Fragen:

- Welche Formen von Missbrauch wären möglich, wenn vertrauliche Informationen Ihres Unternehmens oder Ihrer Organisation in die Hände Dritter gelangten?
- Welche Konsequenzen hätte es für Sie, wenn wichtige Informationen, durch welche Umstände auch immer, verändert würden oder verloren gingen? Als Ursache kann nicht nur böse Absicht unbekannter Dritter, sondern auch technisches Versagen in Frage kommen.

- Was würde geschehen, wenn in Ihrer Organisation wichtige Computer oder andere IT-Komponenten plötzlich ausfielen und einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr nutzbar wären? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden?

Es gibt drei **Grundwerte der IT-Sicherheit**: Vertraulichkeit, Verfügbarkeit und Integrität

- **Vertraulichkeit**: vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden
- **Verfügbarkeit**: dem Benutzer stehen Daten, Dienste und Applikationen zum geforderten Zeitpunkt zur Verfügung
- **Integrität**: die Daten sind vollständig und unverändert

Ein gut durchdachtes IT-Sicherheitskonzept schützt Sie vor folgenden **potentiellen Gefahren**:

- **Datenverlust** - durch regelmäßige Datensicherung können die Daten jederzeit wieder hergestellt werden
- **Datendiebstahl** - Nichtbefugten wird der Zugriff auf die Daten verweigert
- **Virenbefall** - intelligente und aktuelle Virenscanner bieten entsprechenden Schutz
- **Hacker** - sorgsam konfigurierte Firewalls blockieren alle unerlaubten Zugriffe von außen
- **Ransomware -** Intelligente Firewalls, Backups und Servervirtualisierung schützen vor Verschlüsselung Ihrer Unternehmensdaten
- **Administratorausfall** - Notfallplan, Vertretungsregeln und gute Dokumentation beugen vor
- **Systemausfall** - Redundanzkonzept, Datensicherung und Notfallplan reduzieren das Risiko
- **Rechtlichen Konsequenzen** - ein sorgsam geplantes und umgesetztes Sicherheitskonzept beugt vor

Sparen Sie daher nicht am falschen Ende. Erstellen Sie mit Spezialisten ein solides **IT-Sicherheitskonzept**
und setzen Sie dieses so rasch wie möglich um.

Wir unterstützen Sie gerne dabei. Folgende Dienstleistungen und Produkte können wir Ihnen anbieten:

- **Beratung**
- **Erstellung Sicherheitskonzept**
- Implementierung einer **maßgeschneiderten Sicherheitslösung**
- **Softwarelösungen zum Schutz von Endusergeräten** (PCs, Smartphones) **und Servern** betreffend Viren, Malware, Threats und Ransomware

- **NextGeneration Firewallsysteme** als primärer Schutz gegen Bedrohungen von außerhalb
- **Backup-Lösungen** um sich hinsichtlich Datenverlust und Ransomware zu schützen
- **Server-Virtualisierungs-Lösungen von Microsoft und Proxmox** für Server-Konsolidierung und für die schnelle Wiederherstellung/Rücksicherung gesamter Serversysteme im Ernstfall

Kontaktieren Sie uns, wir beraten Sie gerne bei einem unverbindlichen, kostenlosen Erstgespräch.