Empfehlungen zum Datenschutz

Datenschutz ist im Zeitalter der Digitalisierung unerlässlich. Ob es sich um persönliche Informationen, Geschäftsdaten oder sensible finanzielle Informationen handelt, die Sicherheit dieser Daten sollte immer oberste Priorität haben. Nachfolgend einige Empfehlungen, wie Unternehmen ihre Daten schützen können.

1. Probleme gar nicht erst entstehen lassen

- **Datenverarbeitung minimieren:** Daten sollten nur dort gespeichert und verarbeitet werden, wo es unbedingt notwendig ist. Dies verringert die Angriffsfläche für potenzielle Sicherheitsverletzungen.
- **Keine unverschlüsselten Daten als E-Mails:** Verzichten Sie darauf, datenschutzrelevante Daten unverschlüsselt per E-Mail zu versenden. Verwenden Sie stattdessen sichere Übertragungsmethoden wie vertrauenswürdige Filetransfer-Dienste über die Sie die Kontrolle haben. Notwendige Daten für Tickets können sie direkt in xpectoPro/aifExpert als Datei an die Tickets anhängen und so verschlüsselt übertragen.
- **Datendefinition:** Legen Sie klare Richtlinien fest, welche Daten wie behandelt werden müssen.
- **Information und Aufklärung:** Es ist wichtig, alle Mitarbeiter über die Bedeutung des Datenschutzes zu informieren und sie entsprechend zu schulen.

2. Angriffspunkte minimieren

- **Mail-Sicherheit:** Investieren Sie in Schulungen zur Erkennung von Phishing-E-Mails und setzen Sie Filterungssysteme ein, um unsichere Nachrichten und Anhänge (alte Office-Dateien ...) zu blockieren. Schützen Sie ihre E-Mail-Domäne vor Absenderfälschung mittels SPF (idealerweise "-all"), DKIM und DMARC.
- **Gerätesicherheit:** Verwenden Sie immer die aktuellsten Geräte und Software-Updates, und achten Sie auf optimale Sicherheitseinstellungen.
- **Schulung der Mitarbeiter:** Bilden Sie Ihre Mitarbeiter fortlaufend im Bereich Sicherheit aus und sorgen Sie für eine regelmäßige Aufklärung über potenzielle Gefahren.
- **Zugriffsrechte:** Gewähren Sie den Benutzern nur exakt so viel Zugang, wie sie für ihre Arbeit benötigen.
- **Zugangsdatensicherheit:** Achten Sie darauf, dass Passwörter und andere Zugangsdaten gut geschützt und für jeden Anwendungsfall individuell sind. Ein Passwortmanager kann hilfreich sein.
- **Gefahr in der Chefetage und Verwaltung:** Oftmals ist die Geschäftsführung, sowie die Verwaltung (Rechnungsstelle, Buchhaltung, Info-Postfach) ein Hauptziel für Angreifer, da sie Zugriff auf wichtige Informationen haben, bzw. gewöhnt sind Anweisungen von Vorgesetzten zu erhalten. Hier sollte besonders hohe Vorsicht gelten.
- **Keine lokalen Administratorrechte**: Auf Arbeitsplatz-PCs sollte ein User keine Administratorrechte erhalten. Als Alternative bieten sich Windows LAPS oder manuell gepflegte zusätzliche lokale "local-administrator"-Konten an.

3. Schaden begrenzen

- **Backupkonzept:** Implementieren Sie ein robustes Backup-System, das Daten an mindestens zwei verschiedenen Orten oder auf verschiedene Arten sichert.
- **Langzeitsicherung:** Halten Sie mindestens ein Backup bereit, das nicht zerstörbar oder überschreibbar ist und bewahren Sie dieses für mindestens 12 Monate auf.
- **Backup-Überprüfung:** Prüfen Sie regelmäßig mit Stichproben, ob die Backups wiederherstellbar sind.
- **Datenzentralisierung:** Bewahren Sie alle Daten auf zentralen Fileservern auf und verzichten Sie darauf, Endgeräte zu sichern.
- **Sofortige Reaktion:** Bei Sicherheitsverstößen oder -bedrohungen sofort reagieren: Trennen Sie das betroffene System vom Internet und Netzwerk, lassen Sie den Rechner laufen und ziehen Sie Experten zu Rate.