Einführung

Durch die zunehmende Nutzung von IT für Geschäftsprozesse in Unternehmen ist hängt der Geschäftserfolg zunehmend auch von der sicheren Nutzung unserer IT-Systeme ab. Gemeinsam mit ihnen möchten wir den schwere Verluste für das Unternehmen abwenden, wie z.B.

- Durch einen Virenbefall können wichtige Geschäftsdaten unwiederbringlich verloren gehen
- Durch einen unsicheren Netzwerkzugang wird es Wirtschafspionen - die heutzutage von den zahlreichen Auslandsgeheimdiensten ihrer jeweiligen Länder unterstützt werden - ermöglicht zentrale Geschäftsgeheimnisse zu entwenden und sich dadurch die von uns mühsam erarbeiteten und erforschten Ergebnisse zu eigen zu machen. Stellen sie sich vor, unsere unnachahmlichen Stutenwecken würden morgen aus China zum halben Preis geliefert werden!
- In Folge eines unsachgemäßen Gebrauches der Speicherumgebung haben Betrüger Zugriff auf unsere Kontodaten erhalten und so einen sechsstelligen Betrag ins Ausland überwiesen

In unserer Netzwerkumgebung ist es jedem Mitarbeiter gestattet, mit seinem eigenen Computer auf die IT-Services zuzugreifen (BYOD). Das bedeutet auch, dass wir nur mit ihrer Hilfe dafür sorgen können, dass wir auch morgen alle noch ein Unternehmen haben, dass unsere Kunden - und so auch unsere Familien - ernährt.

Was muss ich tun?

- **M 2.138 Strukturierte Datenhaltung**
  - Speichern sie Programm- und Arbeitsdaten in getrennten Verzeichnissen. Dies erleichtert die Übersichtlichkeit und Datensicherung.
  - Richten sie für verschiedene Aufgaben und Projekte getrennte Verzeichnisse ein
  - Legen sie so wenig Dateien wie möglich in personenbezogenen Verzeichnissen ab. Nutzen sie statt dessen Gruppenablagen oder die Ablage für den allgemeinen Zugriff.
- **M 2.160 Regelungen zum Schutz vor Schadprogrammen**
  - Aufgrund der dezentralen Verwaltung der Clients ist jeder Anwender für ein aktuelles Virenschutz-Programm auf seinem Client selbst verantwortlich
  - Melden sie Schadprogramm-Infektionen dem Benutzerservice

- **M 2.224 Vorbeugung gegen Schadprogramme**
  - Alle von Dritten erhaltenen Dateien und Programme sollten vor der Aktivierung auf möglicherweise enthaltene Schadprogramme überprüft werden.
  - Daten und Programme sollten grundsätzlich nur von vertrauenswürdigen Quellen geladen werden, also insbesondere von den Original-Web-Seiten oder Original-Datenträgern des Erstellers
  - Arbeiten sie mit einem Benutzerkonto ohne lokale Administrator-Rechte
  - Stellen sie alle Programme, welche Makros ausführen können (MS Office, Adobe Acrobat, etc.) so ein, dass diese Makros nicht automatisch ausgeführt werden können
- **M 3.21 Sicherheitstechnische Einweisung der Telearbeiter**
  - Halten sie dienstliche und private Daten konsequent getrennt
- **M 5.155 Datenschutz-Aspekte bei der Internet-Nutzung**
  - Konfigurieren sie ihren Browser so, dass er Cookies aus dem Internet nicht automatisch akzeptiert
  - Konfigurieren sie ihren Browser so, dass er die Historie nach jeder Sitzung automatisch löscht. Führen sie dienstliche und private Nutzung nicht über die gleiche Sitzung durch oder nutzen sie für dienstliche und private Zwecke verschiedene Browser
  - Speichern sie im Browser keine dienstlich sensiblen Angaben wie Passwörter, Unternehmen-Kredikartendaten, Telefonnummern usw.
- **M 5.51 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution**
  - Achten sie beim Surfen im Intranet auf eine abgesicherte Verbindung (Schloss-Symbol im Browser)
- **M 2.46 Geeignetes Schlüsselmanagement**
  - Verwenden sie für jeden Login ein anderes Passwort
  - Verwenden sie KeePass zum Managen ihrer Passwörter und um neue sichere Passwörter zu erzeugen
  - Ändern sie ihre verwendeten Passwörter mindestens einmal im Quartal
  - Besteht der Verdacht, dass eines ihrer Passwörter kompromittiert wurden, dann informieren sie bitte den Benutzerservice
- **M 4.448 Einsatz von Verschlüsselung für Speicherlösungen**

  - Verschlüsseln sie Daten, die einen hohen Schutzbedarf bezüglich Vertraulichkeit aufweisen, mit einem aktuellen Verschlüsselungsprogramm (etwa VeraCrypt) auf dem Netzlaufwerk. Teilen sie das Passwort nur mit Gruppenmitgliedern, die zwingend Zugriff auf diese Daten benötigen.

- **M 4.63 Sicherheitstechnische Anforderungen an den Telearbeitsrechner**
  - Schützen sie ihr Client-Benutzerkonto mit einem sicheren Passwort. Sperren sie ihren Computer, wenn sie den Raum verlassen.
  - Verschlüsseln sie ihre gesamte Festplatte mittels Bitlocker oder Truecrypt
  - Verwenden sie nur Passwörter, die mindestens 8 Zeichen lang sind
- **M 4.433 Einsatz von Datenträgerverschlüsselung**
  - Verschlüsseln sie alle Datenträger, die sie mobil nutzen, etwa Laptop-Festplatten oder USB-Sticks (Werkzeuge: Bitlocker, TrustedDisk, TrueCrypt)
- **M 5.69 Schutz vor aktiven Inhalten**
  - Konfigurieren sie ihren Browser so, dass aktive Inhalte nur auf Rückfrage ausgeführt werden
  - Führen sie aktive Inhalte, bei deren Herkunft sie sich nicht sicher sind, nur in einer virtuellen Maschine, oder auf einem Computer der nicht an unsere IT angeschlossen ist, aus
- **M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren**
  - Wenn sie ein Programm zur Passwortverwaltung oder Verschlüsselung von Daten benutzen, denken sie bitte daran auch dieses Programm auf dem Dateiserver abzulegen