SV-Büro für Elektrotechnik & Informationstechnologie
Dipl.-Ing. Reinhold J. H. Steinberger
Consultant, IT-Architekt, Gerichtssachverständiger

✉Rastbühelstr. 164
8301 Laßnitzhöhe
☎ 0316-491764

Email: office@microtool.at
www.microtool.at

Das Erreichen einer EDV-BASIS-KOMPETENZ wird immer dringlicher

Meldungen über Internet-Erpressung häufen sich. Zeitungen berichten über Cyberaktivitäten von kriminellen Hackern, die sich übers Internet den Zugang zu sensiblen bzw. pekuniär verwertbaren Daten erschlichen haben und durch entsprechende Maßnahmen wie z.B. mittels Verschlüsselung, wichtige Bereiche einer Computeranlage lahmlegen - mit dem Ziel Lösegeld von den Cyber-Opfern zu fordern. Speziell im Bereich der Hotelerie – aber nicht nur bei Unternehmen, sondern vermehrt auch bei Privatpersonen ist diese äußerst unangenehme Art der Erpressung im Vormarsch.

In meinen Seminaren zeige ich Basis-Maßnahmen über den Umgang mit sensiblen Daten, um den Schutz eines Unternehmens, aber auch von Privatpersonen zu gewährleisten und darüber hinaus wie man mit einfachen Mitteln die Produktivität dramatisch steigern kann.

Für ein maßgeschneidertes Seminar haben sie die Möglichkeit für ihre Institution, eine Firma bzw. ihre geschätzten Kunden aus nachfolgenden brisanten Themenbereichen eine Auswahl für einen Vortrag zu wählen.

1. Effiziente IT-Sicherheit im Büro, notwendige Basismaßnahmen in der EDV

Die **IT-Sicherheit** umfasst Eigenschaften von informationsverarbeitenden Systemen, die Daten vor unbefugtem Zugriff von außen schützen. Die Maßnahmen zum Schutz von IT-Infrastrukturen sind vielfältig. Im Wesentlichen umfassen sie Datensicherung, Verschlüsselung, Zugriffskontrollen und eingeschränkte Nutzerkonten.

a. Die sieben Security-Todsünden
b. EDV-Rahmenbedingungen
c. EDV-Security-Tipps
d. Passwort, Passwortalternativen
e. Checkliste Basisschutz
f. Vorsicht bei brisanten Daten
g. Recherchieren sie anonym?
h. Einkauf im Internet
i. Versenden sicherer Briefe
j. Airbag für die Datensicherung

2. Wie man Daten sicher vernichtet

Unbemerkte Weitergabe von brisanten Daten durch gefährliche Datenspeicher mit Sicherheitslücken, sowie Unachtsamkeit gepaart mit fehlendem Sicherheitsbewußtsein, das ist nur ein kleiner Ausblick, wie Dokumente die dem Datenschutz unterliegen in fremde Hände gelangen können.

a. Firmenwechsel
b. Computertausch
c. Auslandsreisen
d. Löschantrag bei Suchmaschinen
e. Todesfall

3. Zukunft Blockchain – Bedeutung der Kryptowährung Bitcoin

Blockchain ist eine dezentrale Datenbank mit stetig wachsenden Transaktionsdatensätzen, die gegen nachträgliche Manipulation durch Speicherung von Prüfsummen des vorigen Datensatzes im jeweils nachfolgenden gesichert ist.

Kryptowährung nennt man digitales Geld (ohne Münzen und Scheine).

Bitcoin ist eine rein digitale Währung, die auf einem dezentralen Bezahl-Netzwerk basiert und die Blockchain Technologie als technisches Hilfsmittel benötigt.

a. Blockchaintechnologie
b. Anwendungsbeispiele
c. Visionen

4. Der richtige Umgang mit Zertifikaten

Signieren von Rechnungen, unterzeichnen von Schriftstücken, Verträgen oder Gutachten nach dem Signaturgesetz, Zugang zu E-Government, Justiz und Finanzamt über das Internet ist heute Standard und sollte sich im Portfolio von Unternehmen oder Privatpersonen befinden.

a. Handy-Signatur
b. Zertifikate auf Karte
c. Installation der Software/Treiber
d. PDF-Dokumente signieren
e. Dokumente verschlüsseln

5. IT-Infrastruktur anwendungsorientiert prüfen

Die IT-Infrastruktur umfasst die gesamte Hardware, Software und Netzwerkumgebung eines Büros, die für den Betrieb und das Management eines Unternehmens erforderlich sind.

Es werden IT-Lösungen und Dienstleistungen Angestellten, Partnern und/oder Kunden zur Verfügung gestellt, daher hat eine praxisgerechte und leicht nachvollziehbare Darstellung des Potenzials für Kosteneinsparung durch die Identifikation eventueller Wartungsmängel, durch sinnvolle Erneuerung von Hardware/Software bzw. praxisnaher Optimierung bestehender Arbeitsabläufe oberste Priorität.

a. Hardwareüberblick vom Server, Router/WLAN bis zu den mobilen Geräten.
b. Betriebssysteme
c. Anwendungsprogramme
d. Green-IT
e. Cloud-Systeme

6. Optimierung des Arbeitsablaufes

Am Arbeitsplatz liegt häufig großes Potenzial, um Arbeitsprozesse zu optimieren. Optimierung der Arbeitsabläufe durch Automatisierung und Standardisierung kann die Effizienz sofort und spürbar gesteigert werden.

a. Fehlerhäufigkeiten
b. EDV Einrichtung
c. Aufwertung der Arbeitsumgebung
d. Analyse des Arbeitsablaufes
    i. Zeitgewinn durch Optimierung
e. Effizienz schlagartig steigern
    i. Daten strukturiert verwalten
    ii. Formatvorlagen erleichtern die Arbeit
f. Operative Daten effizient konvertieren
    i. Bild- , Video- u. Tondateien – Datenmengen verkleinern, je nach Anwendung in andere Formate konvertieren
g. Tipps & Tricks für den Arbeitsalltag

7. Gefahren des Social-Engineering

Social Engineering eigentlich ein Begriff aus der angewandten Sozialwissenschaft, zeigt im Bereich der IT-Sicherheit, dass durch zwischenmenschliche Beeinflussungen Personen zur Preisgabe von vertraulichen Informationen animiert werden.

Dieses Seminarmodul beleuchtet die heute üblichen Arbeitsweisen wie unauffällig platzierter Hardware durch Fremdpersonal oder von gezielten externen Anrufen um Spionage und Identitätsdiebstahl zu betreiben und skizziert eingehend das Schadenspotenzial die durch *Pharming, Phishing, Skimming, Sholdersurfen* oder installierter *Bloat*- und *Ransomware*, sowie dem Ausnutzen von *Social Networks* oder *Tailgating* – um nur einige zu nennen - entstehen können.

8. Persönliches Wissensmanagement schlank und effektiv

Persönliches Wissensmanagement integriert Beiträge aus unterschiedlichsten Fachgebieten zu übergeordneten Konzepten und Methoden, um Wissensbestände und Lernprozesse eigenverantwortlich und effektiv zu verwalten.

Eingebunden in diesen Prozess sind neben Zeitmanagement, unter anderen auch Informations-, Stress- und Fehlermanagement die einen enormen Anteil an der Informationssammelwut haben und unweigerlich zu Datenredundanz führen. Informationssammelwut führt zum Datenfriedhof.

9. Wie man lästige Zeitfresser eliminiert

„Zeitfresser“ finden sie nicht nur im Büro, sondern auch unterwegs z.B. bei Kunden oder Lieferanten, auf Baustellen oder bei Befundaufnahmen.

a. Zeitdiebe
b. Zeitfallen

10. Security-Audit mit Risiko- und Schwachstellenanalyse

Als **IT-Sicherheitsaudit** werden Maßnahmen zur Risiko- und Schwachstellenanalyse eines IT-Systems oder Computerprogramms bezeichnet. Bedrohungen für die Sicherheit können von kriminellen Angriffen, von organisatorischen Mängeln aber auch von technischen Unfällen oder höherer Gewalt ausgehen.

a. Konzeption
b. Implementierung
c. Design- oder Konstruktionsfehler
d. Menschliches Fehlverhalten
e. Standortsicherheit