Vereinbarkeit Beruf und Familie – was bedeutet das für die IT?

ECOS Technology GmbH

Paul Marx

Über ECOS Technology

- **Bestehen**
  - Seit 1983 als Ingenieursbüro tätig
  - 1999 Gründung der ECOS Technology GmbH
- **Niederlassungen**
  - Zentrale und Entwicklung: Oppenheim (bei Mainz)
  - Vertrieb: Eschborn
- **Historie**
  - Entwicklung von Hardware-basierenden UTM-, PKI- und OTP-Appliances
- **Heutige Ausrichtung**
  - Lösungen für einen hochsicheren Datenfernzugriff
  - Virtuelle UTM-, PKI- und OTP-Appliances

Win-Win-Situation

Arbeitgeber

- Geringere Fehlzeiten
- Motivierte Arbeitskräfte
- Größere Bewerberauswahl
- Reduzierte Bürokosten

Arbeitnehmer

- Bessere Arbeitseinteilung
- Weniger Stressfaktoren
- Bessere Karrierechancen
- Reduzierte Fahrtkosten

In Zahlen

- **Fehlzeitenquote -41%**
- **Krankheitsquote -39%**
- **Motivation der Beschäftigten +32%**
- **Produktivität der Beschäftigten +23%**
- **Bewerberqualität +26%**

Quelle: Studie aus 2013, Forschungszentrum Familienbewusste Personalpolitik

Was bedeutet das für die IT?

- Datenschutz & IT-Sicherheit
- Administration und Wartung externer Geräte
- Investitionen und laufende Betriebskosten

Mögliche Optionen

- **Firmennotebook**
- **Privat-PC**

Die Bayerische Landesbank überlässt ihren Mitarbeitern für Heimarbeitsplätze die frei Wahl zwischen einem Firmennotebook oder der unentgeltlichen Nutzung des eigenen PCs.

Über 50% entscheiden sich für ein Arbeiten mit dem privaten PC.

Bundesdatenschutzgesetz

- §9 Technische und organisatorische Maßnahmen
  - Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
- Anlage (zu § 9 Satz 1)
  - …

1. Zutrittskontrolle

- **Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren,**

- **Abschließbarer Arbeitsbereich**

2. Zugangskontrolle

- **zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können,**

- **Sicheres Authentisierungsverfahren: 2-Faktor-Authentisierung**
- **Keine lokale Datenhaltung, wegen**
  - **Wartung und Reparatur privater Geräte**
  - **Nutzung durch Familienangehörige**

3. Zugriffskontrolle

- **zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,**

- **Nutzerspezifische Rechtevergabe**
- **Schutz vor dem Zugriff durch Malware**
- **Schutz vor dem Abgreifen von Daten oder Bildschirminhalten durch Trojaner**
- **Schutz vor unberechtigtem Kopieren, Drucken oder Screendumps**

4. Weitergabekontrolle

- **zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,**

- **Sichere VPN-Verbindung**
- **Keine lokale Datenhaltung, wegen**
  - **Möglichem Verlust oder Diebstahl der Geräte**
  - **Gewährleistung der Datenlöschung bei Ausscheiden eines Mitarbeiters**
- **Detaillierte Übersicht der Rechtevergaben**

5. Eingabekontrolle

- **zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,**

- **Detaillierte Logfiles und Reporting-Tools**

6. Auftragskontrolle

- **zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können,**

- **Keine lokale Datenhaltung**

7. Verfügbarkeitskontrolle

- **zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind,**

- **Keine lokale Datenhaltung, wegen**
  - **Möglichem Verlust oder Diebstahl der Geräte**
  - **Durchsetzbarkeit regelmäßiger Backups**

8. Trennung nach Zweck

- **zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.**

- **Berechtigungsabhängiger Zugang auf unterschiedliche Fachanwendungen**

Verschlüsselung

- **Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.**

- **Sichere VPN-Verbindung**
- **Keine lokale Datenhaltung, wegen**
  - **der Notwendigkeit der Festplattenverschlüsselung**

Kontrollrecht

- **Zugriff auf geschäftliche Daten seitens des Unternehmens, muss zu jeder Zeit gewährleistet sein.**
- **Verantwortung für die Sicherheit personenbezogener Daten liegt beim Unternehmer.**
- **Zugriff auf private Daten ist gemäß §88 TKG auszuschließen.**

- **Keine lokale Datenhaltung**
- **Zugriff auf private Dateien technisch ausschließen**

Schutzstufenkonzept

gemäß des saarländischen Datenschutzbeauftragten

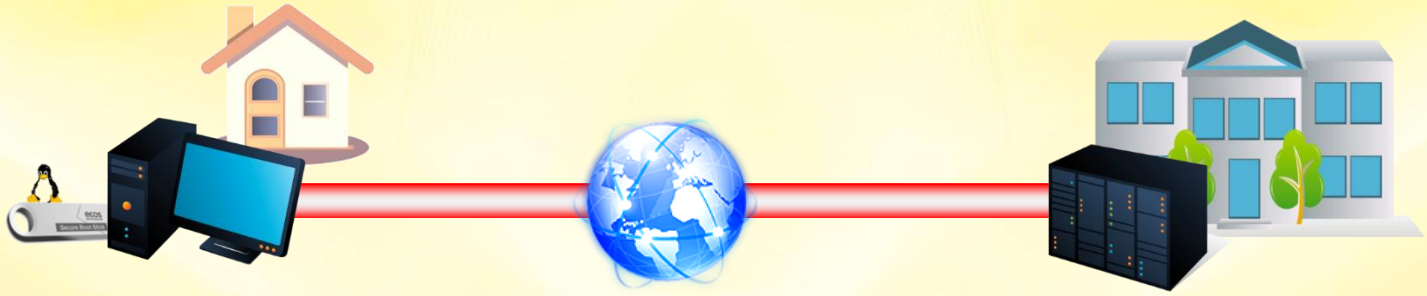
- **Schutzstufe A: Frei zugängliche Daten**
  Frei zugängliche Daten, die keinen Schutz erfordern, sind z.B.
  - Mitgliederverzeichnisse
  - Adressbücher
  - Benutzerkataloge in Bibliotheken
  - Nicht dazu gehören z.B. Wählerverzeichnisse, die nur ausnahmsweise und für kurzen Zeitraum frei zugänglich sind.
- **Schutzstufe B: Belästigung**
  Der Missbrauch dieser Daten lässt keine besondere Beeinträchtigung schutzwürdiger Belange erwarten. Solche Daten sind z.B.
  - Anschriftendateien (für Zwecke der Öffentlichkeitsarbeit), Verteiler für Unterlagen, Informationen Dateien mit folgendem Inhalt:
  - Name, akademischer Grad, Berufsbezeichnung, Anschrift, Telefonnummer, Ordnungsmerkmale (z.B. Aktenzeichen), Bankverbindung, Veranlagungsdaten für: Hundesteuer Erschließungs- und Anliegerbeiträge
- **Schutzstufe C: Gesellschaftliche Stellung**
  Der Missbrauch dieser Daten kann Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen (= Ansehen) beeinträchtigen.
  - Familienstand, Geburtsdaten, Religion, Staatsangehörigkeit, Wehrdienstzeit, Daten des Melderegisters, Schulzeugnisse, Prüfungsnoten, Ergebnisse von Beurteilungen, Personaldaten aus Beschäftigung (soweit nicht Schutzstufe D), Einkommen inkl. Abzüge, Sozialleistungen, Zugehörigkeit zu Vereinen, Verbänden, Zugehörigkeit zu gesetzlichen oder privaten Versicherungen, Grundsteuer, Ordnungswidrigkeiten leichterer Art, Verkehrsordnungswidrigkeiten, Verwarnungen, Erwerbsminderungsgrade (ohne medizinische Angaben)
- **Schutzstufe D: Wirtschaftliche Verhältnisse**
  Missbrauch dieser Daten kann den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich (= Existenz) beeinträchtigen:
  - Gesundheitliche Verhältnisse, Unterbringung in Anstalten, Straffälligkeit, auch Disziplinarverfahren, Ordnungswidrigkeiten, schwerwiegender Art, dienstliche Beurteilungen, psychologisch- medizinische Untersuchungsergebnisse (z. B. beim Führerschein), wirtschaftliche Verhältnisse (wenn sensibler als bei Schutzstufe C), Vermögen, Umsatz, Schulden, Pfändungen, Konkurse, Offenbarungseide
- **Schutzstufe E: Leben, Gesundheit oder Freiheit**
  Missbrauch dieser Daten kann für den Betroffenen lebensbedrohlich sein, seine Gesundheit gefährden oder seine Freiheit beeinträchtigen. Solche Daten, wie z.B:
  - Zugehörigkeit zu Geheimdiensten, Polizeispitzeltätigkeit, Mitglieder von Sonderkommandos, usw.

ECOS SECURE BOOT STICK

Hochsicherer Zugriff bei einer absoluten Trennung zwischen privater und betrieblicher Nutzung eines PCs, auf

Windows Server · CITRIX · vmware · Webserver

ECOS Secure Boot Stick



- 100 %ige Trennung behördliche/private Nutzung durch das Booten eines eigenen Betriebssystems
- Sämtliche Software auf dem Stick
  - ECOS Secure Linux, VPN-Client, RDP-Client, Citrix Receiver, Firefox
- Starke 2-Faktor-Authentifizierung
- Gesicherte VPN-Verbindung
- Integrierte Firewall schützt vor Angriffen im externen Netz

Anforderungen BDSG erfüllt

1. Zutrittskontrolle	• /
2. Zugangskontrolle	• 2-Faktor-Authentisierung • Keine lokalen Daten
3. Zugriffskontrolle	• Benutzerspezifische Zugriffsrechte • Schreibgeschützte Partition für Firmware und Client-Software • Drucken und Kopieren von Daten nur nach Freigabe
4. Weitergabekontrolle	• Sichere VPN-Verbindung
5. Eingabekontrolle	• Detaillierte Logfiles und Reporting-Möglichkeiten
6. Auftragskontrolle	• Keine lokale Datenhaltung
7. Verfügbarkeitskontrolle	• Keine lokale Datenhaltung
8.Trennung nach Zweck	• Benutzerspezifische Zugriffsrechte
Verschlüsselung	• Sichere VPN-Verbindung
Kontrollrecht	• Interne Festplatte deaktiviert

IT-Sicherheit

Firmen-PC

- Private Nutzung möglich
- Windows anfällig für Malware
- Kein Schutz im (W)LAN

Privat-PC
mit ECOS SECURE BOOT Stick

- Private Nutzung 100% getrennt
- Gekapselte Linux-Umgebung
- Integrierte Firewall

Administration und Wartung

Firmen-PC

- Automatisierter Rollout
- Aktualisierung aufwendig
- Regelmäßige Supportfälle
- Stets aktuelle AV-Software

Privat-PC
mit ECOS SECURE BOOT Stick

- Keine Installation / Konfiguration
- Automatische Aktualisierung
- Support einmalig für USB-Boot
- AV-Schutz nur für privat

Investitionen und Betriebskosten

Firmen-PC

- Hardware
  - Anschaffung
  - Wartung
- Anti-Viren-Software
- Festplattenverschlüsselung
- OTP-Token o.Ä.
- Endanwender-Support

- ca. 2.500 € auf 3 Jahre

Privat-PC
mit ECOS SECURE BOOT Stick

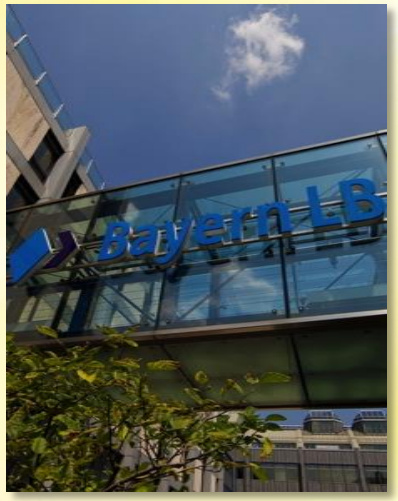
- ECOS Secure Boot Stick
  - Up-to-Date

- ca. 350 € auf 3 Jahre

Das sagen unsere Kunden:

Der ECOS SECURE BOOT Stick im Einsatz bei der Bayerischen Landesbank

Für den Fernzugriff steht den Mitarbeitern mit dem ECOS SECURE BOOT Stick eine Alternative zum Firmennotebook zur Verfügung



„Die Lösung ist einfach anzuwenden und erfüllt ihren Zweck ohne weiteren Aufwand. Die gekapselte, in sich geschlossene Technik, die auf den Rechnern keine speziellen Updates oder Patches voraussetzt, lässt mich und meine IT-Kollegen wesentlich ruhiger schlafen."

Florin Comanici
RAS-Servicemanager bei der BayernLB

Zum Lesen der gesamten Case Study klicken Sie hier.

Alle Prozesse abgesichert - Der ECOS SECURE BOOT STICK im Einsatz beim hessischen Justizministerium

In vielen Behörden wird Telearbeit aktiv gefördert. Das hessische Justizministerium ermöglicht Mitarbeitern mit Lösungen von ECOS Technology von ihren privaten Computern aus Fernzugriff auf die zentralen IT-Systeme und wichtige Anwendungen. Das Resultat: Maximale Flexibilität und Zufriedenheit bei höchster Sicherheit.

„Der Secure Boot Stick von ECOS ist fester Bestandteil unserer Strategie für die alternierende Telearbeit und den technischen Zugang zur Heimbeschäftigung. Er ermöglicht unseren Mitarbeitern größtmögliche Flexibilität und Produktivität bei der Arbeit von zu Hause oder unterwegs. Gleichzeitig sind sensible Daten optimal geschützt.“

Holger Hofmann
Regierungsdirektor und Referatsleiter
Informationstechnik des Hessischen Justizministeriums

Zum Lesen der gesamten Case Study klicken Sie hier.

Ihre Ansprechpartner

Paul Marx

Geschäftsführer

Tel.: 06133/ 939- 250

Fax: 06133/ 939- 334

E-Mail: paul.marx@ecos.de

Vielen Dank für Ihr Interesse