



DATACOLLECTION  
Systemhaus GmbH

# DATACOLLECTION

DATACOLLECTION

## IT-Security Workshop

29.10.2002

WIFI Wien

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 10 min)
- Berechnung von Ausfallkosten (ca. 15 min, T. Pamperl)
- Datensicherung (ca. 25 min, F. Pakr)
- Virenschutz (ca. 30 min, W. Preier)
- Zugriffsschutz (ca. 30 min, W. Preier)
- Überwachung (ca. 20 min, F. Pakr)
- Interne Gefahren (ca. 15 min, T. Pamperl)
- Security Management (ca. 15 min, T. Pamperl)
- Standardeinstellungen (ca. 20 min, P. Hartl)
- Fragen & Antworten

DATA  
COLLECTION

# Referent: Thomas Pamperl



DATACOLLECTION  
Systemhaus GmbH

- Ausbildung: HTL Elektrotechnik, FH Unternehmensführung
- Technische Qualifikationen: Novell CNE, Oracle Database Administrator, Microsoft MCP
- Organisatorische Qualifikationen: Trainer- und Lektorentätigkeit, Projektmanagement im techn. Bereich
- Coaching im technischen und Organisatorischen Bereich

DATA  
COLLECTION

# Referent: Wolfgang Preier



DATACOLLECTION  
Systemhaus GmbH

- Ausbildung: HTL Elektrotechnik
- Qualifikationen: Alle Protokolle und Netzwerktypen seit X.25 (Datex/P)
- Systems Engineer bei Radio Austria und Ericsson Austria
- Spezialisierung auf Internet, Security und Systems Management (Micromuse Netcool)

DATA  
COLLECTION

# Referent: Franz Pakr



DATACOLLECTION  
Systemhaus GmbH

- Spezialaufgaben im Bereich Audio und Video (Harddiskrecording-Videoschnitt, div. Einbindungen)
- Programmierung und Grafik im WEB-Bereich (php,asp,java und Coldfusion)
- Programmierung im kaufmännischen und industriellen Bereich (Testplätze etc.) sowie Audio und Video in Visual Basic Visual C.
- Installation und Einrichtung im Bereich Desktop-Publishing (Scanner, Belichter, Plotter, Schnittplotter).

DATA  
COLLECTION

# Referent: Peter Hartl



DATACOLLECTION  
Systemhaus GmbH

- Ursprünglich verschiedene Tätigkeiten im Speditionsbereich
- Seit 1999 EDV Technik
- Support, Installation und Schulungen im Software- und Netzwerkbereich
- Seit 2001: Pre-Sales Consultant im Multimedia-Bereich

DATA  
COLLECTION

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten (15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- Interne Gefahren (ca. 15 min)
- Security Management (ca. 15 min)
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Einflussfaktoren



DATACOLLECTION  
Systemhaus GmbH

- Zeit für Fehlersuche
- Produktivitätsausfall
- Ansehensverlust
- Datenrekonstruktionskosten
- Umsatzausfälle
- EDV Techniker
- Hardwarekosten
- Softwarekosten
- Installationskosten
- Wartung
- Laufende Prüfung

DATA  
COLLECTION

# Bewertung



DATACOLLECTION  
Systemhaus GmbH

- Klassische Systeme nicht geeignet
  - Finanzbuchhaltung
  - Kostenrechnung
- Prozesskostenrechnung möglicher Ansatz

DATA  
COLLECTION

# Beispiele Teil 1



DATACOLLECTION  
Systemhaus GmbH

- Tandberg: ([http://www.tandbergdata.de/home\\_de/profile/archive/info/whyback.html](http://www.tandbergdata.de/home_de/profile/archive/info/whyback.html))

Was kostet es für verschiedene Abteilungen, 20 MByte Daten zu rekonstruieren?

| Abteilung:              | Kosten:    | Zeit:   |
|-------------------------|------------|---------|
| Vertrieb und Marketing  | 25.000 DM  | 19 Tage |
| Rechnungswesen          | 29.000 DM  | 21 Tage |
| Produktion              | 40.000 DM  | 32 Tage |
| Forschung & Entwicklung | 147.000 DM | 42 Tage |

(Basiert auf 300 Anschlägen/Minute und Kosten von 35 DM/Stunde)

# Beispiele Teil 2

Annahme: 100 PCs infiziert



DATA COLLECTION  
Systemhaus GmbH

## TYPISCHE KOSTEN, DIE BEI DER ENTDECKUNG, SÄUBERUNG UND WIEDERHERSTELLUNG NACH EINEM VIRENANGRIFF ANFALLEN

| <i>Aktion</i>  | <i>Kosten</i> |
|--|---------------|
| Informieren eines IT-Managers und dessen Aktion gegen einen Virenvorfall | 550 Euro      |
| Stoppen, Suchen des Virus und Säubern einer Workstation                  | 110 Euro      |
| Entdecken und lokales Säubern einer Vireninfection auf einer Workstation | 110 Euro      |
| Durchschnittliche Anzahl von Hackangriffen auf ein Netz pro Monat        | 2             |

## KOSTENVERGLEICH EINES TYPISCHEN VIRENAUSBRUCHS

| <i>Firma A (keine eMail-Schutz)</i>  |               | <i>Firma B (mit eMail-Virenschutz)</i>           |               |
|--|---------------|--|---------------|
| <i>Aktion</i>  | <i>Kosten</i> | <i>Aktion</i>                                    | <i>Kosten</i> |
| 20% der Benutzer geschützt, dennoch wird IT zu Hilfe gerufen               | 9.000 €       | IT-Manager alarmiert, ergreift notwendige Aktion | 550 €         |
| 5% der Benutzer ungeschützt, IT wird benötigt für Virensuche und Säuberung | 5.500 €       |  |               |
| 75% der Benutzer entdecken und säubern Infektionen selbst                  | 8.250 €       |  |               |
| Gesamtkosten des Vorfalls  | 24.750 €      | Gesamtkosten des Vorfalls                        | 550 €         |

DATA COLLECTION

# Kostenberechnung

[http://germany.trendmicro.de/free\\_tools/edoctor/default.asp](http://germany.trendmicro.de/free_tools/edoctor/default.asp)



DATA COLLECTION  
Systemhaus GmbH

- Annahme: 10 Client PCs, 1 File/Print Server, 1 Mailserver, 1 Gateway
  - Ohne Virenschutz
  - Mit Virenschutz „dezentral“
  - Nur 2 Virenfälle pro Jahr !!!
  - Produktivitätswert je Mitarbeiter und Jahr \$ 80.000,--

DATA COLLECTION

# Schaden im Falle einer Infektion



DATACOLLECTION  
Systemhaus GmbH

| MIS Tasks                              | Arbeitsaufwand           |                 |                          |                 |
|--|--------------------------|-----------------|--------------------------|-----------------|
|  | Ohne zentrale Verwaltung |                 | Mit zentraler Verwaltung |                 |
|  | Stunden                  | Kosten          | Stunden                  | Kosten          |
| Help Desk                              | 4                        | \$153.85        | 4                        | \$153.85        |
| Situation eines Virenangriffs erkennen | 4                        | \$153.85        | 0.167                    | \$6.42          |
| infizierte Dateien feststellen         | 1                        | \$38.46         | 0.167                    | \$6.42          |
| Informationen über den Virus einholen  | 1                        | \$38.46         | 1                        | \$38.46         |
| Interne Reports erstellen              | 2                        | \$76.92         | 0.5                      | \$19.23         |
| jeden Server scannen                   | 3                        | \$115.39        | 0.167                    | \$6.42          |
| <b>Gesamt</b>                          | <b>15</b>                | <b>\$576.93</b> | <b>6.001</b>             | <b>\$230.81</b> |

DATACOLLECTION

# Aufwand für den Endbenutzer



DATACOLLECTION  
Systemhaus GmbH

| Aufgaben<br>des End-<br>benutzers                   | Arbeitsaufwand              |          |                             |        |
|---|-----------------------------|----------|-----------------------------|--------|
|   | Ohne zentrale<br>Verwaltung |          | Mit zentraler<br>Verwaltung |        |
|   | Stunden                     | Kosten   | Stunden                     | Kosten |
| Scannen<br>eines jeden<br>Client-PC (30<br>min./PC) | 5                           | \$192.31 | Echtzeit                    | \$0.00 |
| Status-<br>mitteilungen                             | 0.167                       | \$6.42   | N/A                         | \$0.00 |
| <b>Gesamt</b>                                       | 5.167                       | \$198.73 | 0                           | \$0.00 |

DATACOLLECTION

# Gesamtaufwand



DATACOLLECTION  
Systemhaus GmbH

## Gesamtschaden pro Vireninfection

| Ohne zentrale Verwaltung |          | Mit zentraler Verwaltung |          |
|--------------------------|----------|--------------------------|----------|
| Stunden                  | Kosten   | Stunden                  | Kosten   |
| 20.167                   | \$775.66 | 6.001                    | \$230.81 |

## Veranschlagter Gesamtschaden pro Jahr

| Ohne zentrale Verwaltung |            | Mit zentraler Verwaltung |          |
|--------------------------|------------|--------------------------|----------|
| Stunden                  | Kosten     | Stunden                  | Kosten   |
| 40.334                   | \$1,551.33 | 12.002                   | \$461.62 |

Nicht berücksichtigt: Umsatzausfälle, Imageschaden,  
Datenrekonstruktion...

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten(15min)
- **Datensicherung (ca. 25 min)**
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- Interne Gefahren (ca. 15 min)
- Security Management (ca. 15 min)
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Fragen zur Datensicherung



DATACOLLECTION  
Systemhaus GmbH

- Wie lange dauert ein gesamter Wiederherstellungsvorgang?
- Sichern Sie alle Datenbanken (Active Directory, DNS, DHCP...)?
- Haben Sie ein Wiederherstellungskonzept für Client PCs?
- Prüfen Sie regelmäßig, ob Ihre Medien noch lesbar sind?

DATA  
COLLECTION

# Datensicherung



DATACOLLECTION  
Systemhaus GmbH

- Restorekonzept führt zu Backupkonzept
- Restore/Backup von
  - Dateien
  - Betriebssystem
  - Datenbank (DNS, DHCP, Active Directory, SQL, Progress, Oracle)
  - Server, Server & Clients, Server & Clients & Exoten
- Rotationsalgorithmen (Großvater-Vater-Sohn, Tower of Hanoi)
- Test der Restorefunktion

DATA  
COLLECTION

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten(15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- Interne Gefahren (ca. 15 min)
- Security Management (ca. 15 min)
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Virenschutz



DATACOLLECTION  
Systemhaus GmbH

- Viren, Trojaner und Würmer
- Störungsarten (Löschung von Dateien, versenden von emails & Passwörtern, übernehmen von Systemfunktionen)
- Abwehrmechanismen und Software

DATACOLLECTION



DATACOLLECTION  
Systemhaus GmbH

# Viren, Trojaner, Würmer

- Virus (Bugbear)
- Trojaner (mirc)
- Wurm (Reeezak.A)
- IIS-Angriffe (Code-Red)
- Script-Kiddies
- HOAX-Viren

DATA  
COLLECTION

# Störungen durch Viren



DATACOLLECTION  
Systemhaus GmbH

- Virus oder Nicht?
- Gelöschte Dateien
- Aufruf von Programmen
- Fernsteuerung des PC
- Ausspionieren von Kreditkarten

DATA  
COLLECTION

# Virenabwehr



DATACOLLECTION  
Systemhaus GmbH

- Security-Patches
- Mails
- Antivirensoftware
  - Für den PC
  - Für den Server
  - Für das Internet Gateway (Firewall)

DATA  
COLLECTION

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Was passiert wenn Sie Ihre Daten verlieren? (15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- Interne Gefahren (ca. 15 min)
- Security Management (ca. 15 min)
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Zugriffsschutz I



DATACOLLECTION  
Systemhaus GmbH

- Proxy oder Firewall
- Mailscanner und Webscanner
- Kontrolle
- IDS – Intrusion Detection
- Prüfung
- Protokolle

DATA  
COLLECTION

# Proxy



DATACOLLECTION  
Systemhaus GmbH

- Was ist ein Proxy
- Unterschiede zur Firewall
- Einsatzmöglichkeiten und Grenzen
- Personal Firewall

DATA  
COLLECTION

# Firewall



DATACOLLECTION  
Systemhaus GmbH

- Was ist eine Firewall
- Welche Firewalls gibt es
- Was ist eine sichere Firewall
- Kaufen oder selber machen?
- Kommerzielles Produkt oder Open Source (Linux)?
- Load-Sharing, Load-Balancing, Failover

DATA  
COLLECTION



- Was sind SPAM (UCE) Mails
- Wie schützt man sich vor SPAM-Mails
- Was ist ein Webscanner
- Selber machen oder kaufen?

# Kontrolle



DATACOLLECTION  
Systemhaus GmbH

- Wie kontrolliert man Zugriffe
- Wann kontrolliert man Zugriffe
- Rechtliche Hintergründe
- Melden oder Verschweigen?
- BSI, DuD, CERT, Microsoft, Linux, SANS Institute, Bruce Schneier u.a.

DATACOLLECTION

- Was ist ein IDS
- Funktion Einsatz und Grenzen von IDS
- Beispiel SNORT in der Firewall
- Maßnahmen bei Warnungen
- Updates, Prüfung und Kontrolle

# Prüfung



DATACOLLECTION  
Systemhaus GmbH

- Wie prüft man einen Internetzugang
- Einbruchversuch = Vergehen?
- Einfache Prüfungsmöglichkeit mit nmap
- Kontrolle
- Pflichten und Rechte – Gesetzliche Rahmen

DATA  
COLLECTION

# Protokolle



DATACOLLECTION  
Systemhaus GmbH

- WLAN – SSID, MAC, WEP, EAP-TLS
- Secure-DNS, TLS
- Proprietäre Protokolle
- GSM Sicherheit

DATA  
COLLECTION

# Zugriffsschutz II



DATACOLLECTION  
Systemhaus GmbH

- Von Innen
  - Firewall oder Proxy, Zugriffsrechte
  - Passwörter
  - Alternative Systeme (Biometrik, Secure-Card)
  - Kontrolle
  - Prüfung

DATA  
COLLECTION

# Firewall und Proxy



DATACOLLECTION  
Systemhaus GmbH

- Firewall oder Proxy was ist besser?
- Zugriffsrechte und Rechtevergabe
  - Im Proxy – MS ISA Server
  - Im Proxy – SQUID
  - In der Firewall
- Abrechnung/Kostenkontrolle

DATA  
COLLECTION

# Passwörter



DATACOLLECTION  
Systemhaus GmbH

- Sichere und unsicher Passwörter
- Passwortcracker im Einsatz
- Gesperrtes Konto was tun?
- Administrator ausgesperrt?
- Trojaner und Passwort-Diebe

DATA  
COLLECTION

# Alternative Systeme



DATACOLLECTION  
Systemhaus GmbH

- Zugangskontrolle mit Chip-Card
- Biometrische Zugangskontrolle
- Dongle Zugangskontrolle
- RSA SecurID
- LDAP, RADIUS, KERBEROS
- X.500 – Single Sign On

DATA  
COLLECTION

# Zugriffsschutz III



DATACOLLECTION  
Systemhaus GmbH

- VPN
- SSL (HTTP-S), TLS, SSH
- S/MIME, PGP
- PKI/X.509

DATA  
COLLECTION

# VPN



DATACOLLECTION  
Systemhaus GmbH

- Client-Server/Server-Server
  - Shared Secret oder Public Key?
- PPTP, L2TP, IPSEC, SSH
  - Microsoft RAS
  - Linux Free S/WAN
  - Checkpoint Firewall-1
  - Cisco
- Einsatz im Internet
- Sicherung eines WLAN

DATA  
COLLECTION

# SSL



DATACOLLECTION  
Systemhaus GmbH

- SSL – Das Protokoll
- Einsatz von SSL mit Private Keys
- Einsatz von SSL mit Public Keys
- SSL-Beschleuniger
- TLS
- SSH

DATA  
COLLECTION

# S/MIME, PGP



DATACOLLECTION  
Systemhaus GmbH

- S/MIME oder PGP?
- Signatur und Gesetz
- Funktionsweise S/MIME
- Funktionsweise PGP

DATA  
COLLECTION

# PKI/X.509



DATACOLLECTION  
Systemhaus GmbH

- PKI – Public Key Infrastructure
- Rolle der tkc in Österreich
- Wer kann eine PKI „bauen“
- Warum PKI – Warum keine Passwörter
- PKI und Passport Was ist der Unterschied?

DATA  
COLLECTION

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten(15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- **Überwachung (ca. 20 min)**
- Interne Gefahren (ca. 15 min)
- Security Management (ca. 15 min)
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Überwachung



DATACOLLECTION  
Systemhaus GmbH

- Sicherheitsrelevante Vorgänge
  - Dateizugriff von vertraulichen Dateien
  - Remote Zugriffe
- Geschäftskritische Funktionen
  - Backup
  - Mailverkehr

DATA  
COLLECTION

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten(15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- **Interne Gefahren (ca. 15 min)**
- Security Management (ca. 15 min)
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Frage:



DATACOLLECTION  
Systemhaus GmbH

- Wie „funktioniert“ ein Mitarbeiter?
  - Wissen
  - Motivation
  - Methoden
  - Sonstiges

DATA  
COLLECTION

# Interne Gefahren



DATACOLLECTION  
Systemhaus GmbH

- Eigene Mitarbeiter
  - Vorsätzlich z.B. bei Kündigung
  - Fahrlässig z.B. keine/bekannte Kennwörter
- Social engineering
- Ungesicherte wireless LANs

DATA  
COLLECTION

# Vorsätzliche Schädigung



DATACOLLECTION  
Systemhaus GmbH

- Mögliche Maßnahmen
  - Effiziente Accountverwaltung (→ sofortige Sperrung bei Kündigung, Account-Sperrungs Richtlinien)
  - Laufende Kontrolle der Zugriffslogs
  - Internetverhalten (Vorsicht!!!); gesetzliche Normierungen beachten
    - Proxylogs
    - Maillogs

DATA  
COLLECTION



DATACOLLECTION  
Systemhaus GmbH

# Fahrlässige Schädigung

- Gelebte Kennwortrichtlinien
- Schulungen
- Rechteverwaltung (z.B. Löschungsrecht für Verteilerlisten nur für Power User...)
- Vorsicht bei temporären Benutzern (Ferialpraktikanten...)
- Webmail... (Adresse und Kennwort im Verlauf des Internet Cafe PCs)

DATA  
COLLECTION

# Social Engineering



DATACOLLECTION  
Systemhaus GmbH

- Jedes Kennwort ist „in Erfahrung“ zu bringen
- Einziges Gegenmittel: Regelmäßige Änderung (auch Administrator!)
- Regelmäßige Prüfung der Accountdaten (am Besten über „Auditing“ Funktionalität)

DATA  
COLLECTION

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten (ca. 15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- Interne Gefahren (ca. 15 min)
- **Security Management (ca. 15 min)**
- Standardeinstellungen (ca. 20 min)
- Fragen & Antworten

DATA  
COLLECTION

# Security Management



DATACOLLECTION  
Systemhaus GmbH

- Normiert in ISO 17799
- Management ist mit ISO 9000/14000/EMAS vergleichbar
- Sicherheitsmanagement ist ein stetiger Support-Prozess
- Bewertung der Einzelrisiken nach
  - Eintrittswahrscheinlichkeit
  - Auswirkung auf Geschäftsprozesse
  - Multiplikation ergibt Gewichtungsfaktor
- Führt zu einem „IT Security Handbuch“

DATA  
COLLECTION

# ISO 17799 Teil1

vgl: <http://enterprisesecurity.symantec.de/article.cfm?articleid=1414&PID=13106146&EID=0>



DATACOLLECTION  
Systemhaus GmbH

- Richtlinien
- Verteilung der Sicherheitsaufgaben
- Klassifizierung und Kontrolle unternehmenskritischer Daten
- Mitarbeitersicherheit
- Physikalische Sicherheit und Schutz der IT-Sicherheit

DATA  
COLLECTION

# ISO 17799 Teil 2



DATACOLLECTION  
Systemhaus GmbH

- Communication und Operation Management
- Zugriffskontrolle
- Systementwicklung und Wartung
- Geschäftskontinuitätsmanagement
- Richtlinieneinhaltung

DATA  
COLLECTION

# Risikobewertung



DATACOLLECTION  
Systemhaus GmbH

| Risiko                   | Eintrittswahrsch. | Auswirkung | Bewertung |
|--------------------------|-------------------|------------|-----------|
| Datenverlust             |                   |            |           |
| Unbeabsichtigte Löschung | 90%               | 10%        | 9%        |
| Hardwaredefekt           | 2%                | 100%       | 2%        |
| HW-Tausch nach defekt    | 2%                | 100%       | 2%        |
| Softwarefehler           | 1%                | 100%       | 1%        |
| Virus                    | 100%              | 50%        | 50%       |
| Eindringling             | 90%               | 5%         | 45%       |

DATACOLLECTION

# Dokumentation



DATACOLLECTION  
Systemhaus GmbH

- Jeder Patch/Update muss auf jedem Computer dokumentiert werden
  - „Logbuch“ je Computer
  - Sicherstellung, dass an alle Computer verteilt wird (→ Problem: unterschiedliche Betriebssysteme, Anwesenheit...)
- Stichprobenartige Prüfung laut „IT Security Handbuch“

DATA  
COLLECTION

# Security Handbuch



DATACOLLECTION  
Systemhaus GmbH

- Datensicherung (Beispiel)
  - Jeden Tag wird gesichert und das Logfile (manuell) kontrolliert
  - Bandrotation nach dem GFS Prinzip
  - Einmal wöchentlich wird das Bandlaufwerk gereinigt (Reinigungsband)
  - Einmal im Quartal wird eine Datei rückgesichert
  - Alle 50 Schreibvorgänge werden die Bänder getauscht

DATA  
COLLECTION

- Rechtliche Aspekte
  - Was ist erlaubt
  - Betriebsvereinbarung
  - Arbeitsanweisung
- Soziale Aspekte
  - Überwachungsangst
  - Unterschiedliche Behandlung von Mitarbeitern

# Agenda



DATACOLLECTION  
Systemhaus GmbH

- Überblick (ca. 15 min)
- Berechnung von Ausfallkosten(15min)
- Datensicherung (ca. 25 min)
- Virenschutz (ca. 30 min)
- Zugriffsschutz (ca. 30 min)
- Überwachung (ca. 20 min)
- Interne Gefahren (ca. 15 min)
- Security Management (ca. 15 min)
- **Standardeinstellungen (ca. 20 min)**
- Fragen & Antworten

DATA  
COLLECTION

# Standardeinstellungen



DATACOLLECTION  
Systemhaus GmbH

- Trend Micro „Handbuch zum sicheren Umgang mit Computern“
- Symantec „Die 10 goldenen Regeln“
- Dienste (IIS) deaktivieren
- Shares deaktivieren (ggf. nur auf Internetseite)
- Sichere Kennwörter

DATA  
COLLECTION

# Handbuch zum sicheren Umgang (Trend Micro)



DATACOLLECTION  
Systemhaus GmbH

- Funktion "Windows Scripting Host" deaktivieren
- Optionen zum Ausblenden der Dateierweiterungen bekannter Dateitypen deaktivieren
- Internet Explorer-Sicherheitsstufe mindestens auf "Mittel" einstellen
- eMail-Programm so einstellen, dass vor dem Öffnen von eMail-Anhängen eine Bestätigung angefordert wird
- Makroviren-Warnung aktivieren
- Aufforderung vor dem Speichern von Änderungen in der globalen Vorlage anzeigen
- Alle aktuellen Microsoft Security Updates anwenden

DATA  
COLLECTION

# Goldene Regeln (Symantec)



DATACOLLECTION  
Systemhaus GmbH

- Aktueller Virens Scanner
- Virens Scanner einschalten
- E-Mail Dateianhänge
- Schlechte Scherze
- Software aktuell halten
- Newsgroups
- Wissen ist Macht
- Weniger ist mehr
- Kennwort Disziplin
- Dezentrale Netze

DATA  
COLLECTION

# Sichere Kennwörter



DATACOLLECTION  
Systemhaus GmbH

- Mindestens 8 Zeichen
- Ziffern und Zeichen gemischt
- Groß- und Kleinschreibung
- Algorithmen
  - Regelmäßige Änderung (z.B. monatlich)
  - Zahlenkombinationen: Sozversnr., Tel.Nr., Kalenderwoche der Änderung...
  - Namen ohne Vokale, Namen umgekehrt, Kombinationen (Auto-Name)

DATA  
COLLECTION

# Beispiel



DATACOLLECTION  
Systemhaus GmbH

- Änderung jeden 2. Dienstag im Monat
- Summer der letzten beiden Ziffern der Telefonnummer und aktuellen Kalenderwoche und Kombination AutoVorname, in ungeraden Monaten Kombination AuVo einer anderen Person
- November: 66VoyTom
- Dezember: 70GoAlf

DATA  
COLLECTION

# Microsoft Security Bulletin MS02-060 (17.10.2002)



DATACOLLECTION  
Systemhaus GmbH

- Fehler im Windows Support Center
  - ...da eine Datei, die eigentlich ausschließlich für das System benutzbar sein sollte auch von jeder Webseite benutzt werden kann.
  - Dieses Problem kann es einem Angreifer ermöglichen Dateien auf dem System eines anderen Benutzers zu löschen – entweder über eine Webseite oder ein E-Mail.
  - Voller Wortlaut:  
[http://technet.microsoft.at/News\\_Showpage.asp?newsid=3029&secid=122](http://technet.microsoft.at/News_Showpage.asp?newsid=3029&secid=122)

# Fragen & Antworten

---



DATACOLLECTION  
Systemhaus GmbH

DATA  
COLLECTION