



# Informatik und Sicherheit in KMUs



**Romain Roubaty**  
Verantwortlicher CINC

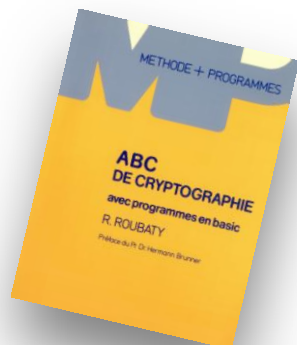
3. November Bern

# Romain Roubaty

**ROUBATIC Sàrl**

cinc - centre d'investigation  
numérique et de cryptologie  
ILCE Institut de lutte contre la criminalité économique

**arc**



## ILCE

- Das ILCE wurde 2000 gegründet
  - Angebot an Nachdiplom-Ausbildungen (MAS, CAS)
  - Breites Angebot an Weiterbildung
  - Forschung , R&D (inkl. Publikationen)
  - Übernimmt Einzelaufträge in Ausbildung und Begutachtung
  - Sein Ermittlungszentrum in Daten und Kryptologie (CINC) bietet Höchstleistungen in Datenermittlung und Bekämpfung der Computerkriminalität



# ILCE

## • 2010 in Zahlen

- Führungsstab: 10 Personen
- Permanent Mitarbeitende: 8 Personen – 4,8 Vollzeitposten
- 150 GastvorleserInnen
- 47 Studierende in Nachdiplom-Ausbildung
- 550 Teilnehmende an Tagungen oder Bausteinkursen
- Nationale und internationale Partner
- R&D-Umsatz: etwa. 30 % des R&D-Umsatzes des IMSI (Institut für Management der Informationssysteme), das Forschungsinstitut der FHW-Arc

# Nachdiplom Studiengänge am ILCE

- **MAS in Economic Crime Investigation (MAS ECI)**

- MAS in Bekämpfung der Wirtschaftskriminalität (MAS LCE)
  - o seit 2001 – zur Zeit 9. und 10. Jahrgang

**o a o**  
**evaluated 08**

- **CAS in Financial Investigation (CAS FI)**

- CAS in Finanzermittlung (CAS IF)
  - o seit 2008 – 5. Jahrgang

- **CAS in Computer Forensics (CAS CF)**

- CAS in Datenermittlung (CAS IN)
  - o seit 2009 – 2. Jahrgang; 3. Jahrgang ab Januar 2012 geplant

- ***In Vorbereitung: CAS in Cybersecurity (ab 2012)***

# Forschungsaktivitäten und Publikationen

- **DB-ECML:** *Data Base of Economic Crime and Money Laundering* - Datenbank in Sachen Wirtschaftskriminalität und Geldwäsche
- **ISCIA:** *Internet Surveillance for Criminal Intelligence Analysis*
  - Projekt in Zusammenarbeit mit der HEIG-VD
- **SURVEY ILCE 2011:** Umfrage bei den Kandidatinnen und Kandidaten zu den Bundeswahlen
- Publikation zahlreicher Artikel und Fachbücher, hauptsächlich im juristischen Bereich

**KMU**

Business  
Intelligence



Geistiges Eigentum

Unternehmensdaten



**Unternehmensdaten**



**Risiko**



Kundendaten

Personalwesen (HR)



Löhne



Finanzen

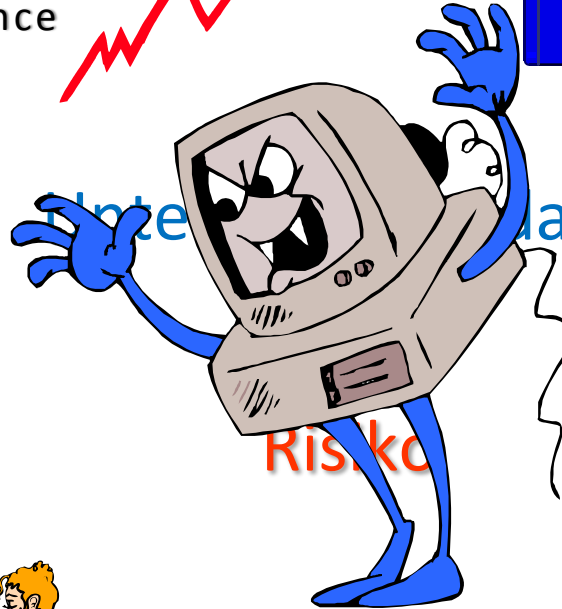
# KMU

Business  
Intelligence

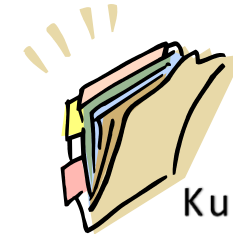


Geistiges Eigentum

Unternehmensdaten



Informations



Kundendaten

Personalwesen (HR)



Löhne



Finanzen

# Risiken für die Daten

- Viren und Schadprogramme (Malware)
- Betrügerische E-Mails
- Piraterie
- Industriespionage
- Veruntreuung
- Verlust von Informationen
- Offenlegung von vertraulichen Informationen
- Bedienungsfehler
- Naturkatastrophe, Umweltproblem
- Materialausfall, Netzausfall
- Unterbrechung der Stromversorgung
- Programmfehler, Netzproblem

# Internet, Mobilité, Virtualität



# Informatiksicherheit



$$Risiko = \frac{Drohung * Verletzbarkeit}{Gegenmassnahme}$$

- **Drohung**
  - Jegliche Aktivität hat das Potenzial zu schaden
- **Verletzbarkeit**
  - Inwieweit ist man der Drohung ausgesetzt ?
  - Schwachstelle, Lücke
- **Gegenmassnahme**
  - Präventionsmassnahme
  - Technische Massnahme
  - Ausbildung, Sensibilisierung, Funktionsregeln



# Ziel der Informatiksicherheit

- Datenintegrität
- Datenvertraulichkeit
- Datenverfügbarkeit
- Unwiderruflichkeit
- Authentifizierung

# Datenintegrität

- Kommunikation
- In der Datenbank
  
- Lösungen
  - Digitaler Abdruck
  - Transaktionstagebuch
  - Datensicherung



# Datenvertraulichkeit

- Daten ausserhalb des Unternehmens
- In der Datenbank
- Vor internem und externem Diebstahl schützen
  
- Lösung
  - Kodierung

# Datenverfügbarkeit

- Sicherheit der Server
- Redundanz

|     |         |        |        |
|-----|---------|--------|--------|
| 365 | 80      | 73     | Tage   |
| 365 | 90      | 36.5   | Tage   |
| 365 | 95      | 18.25  | Tage   |
| 365 | 99      | 3.65   | Tage   |
| 365 | 99.5    | 1.825  | Tage   |
| 365 | 99.9    | 8.76   | Stunde |
| 365 | 99.99   | 52.56  | Min.   |
| 365 | 99.999  | 5.256  | Min.   |
| 365 | 99.9999 | 31.536 | Sek.   |



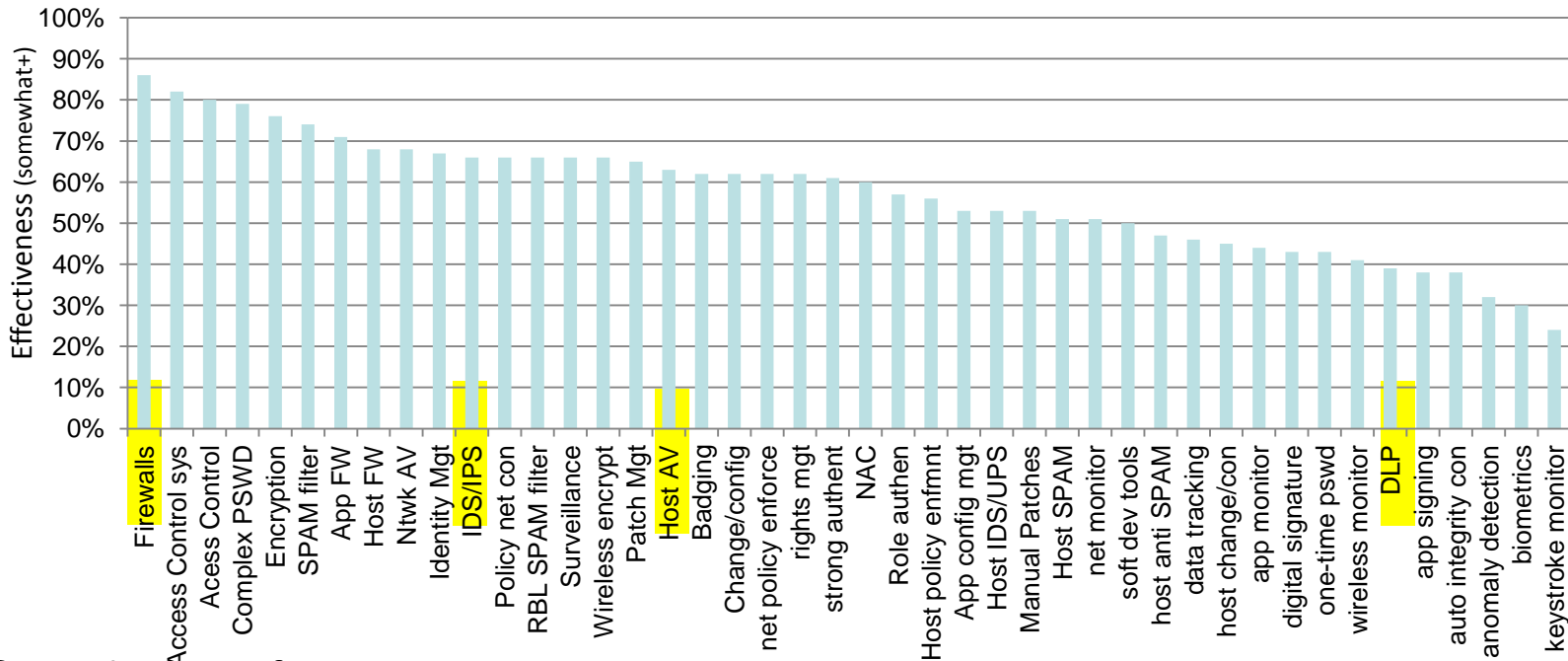
# Unwiderruflichkeit

- Herkunft und Empfang
- Lösungen
  - Signatur, Zertifikat
  - Zeitstempel

# Authentifizierung

- Zugriffsrechte
- Probleme
  - Tastaturschnüffler
  - Vor sehr langer Zeit erteilte Zugriffsrechte
  - Naivität

# Effizienz der Schutzmassnahmen



## Proaktive Haltung

- Die Funktionsweise des Unternehmens verstehen
- Eine Risikoanalyse durchführen
- Das digitale Aktivvermögen identifizieren
- Das digitale Aktivvermögen schützen
- Verletzbarkeiten identifizieren und vermindern
- Sicherheitsregeln erstellen und einsetzen
- Benutzer ausbilden

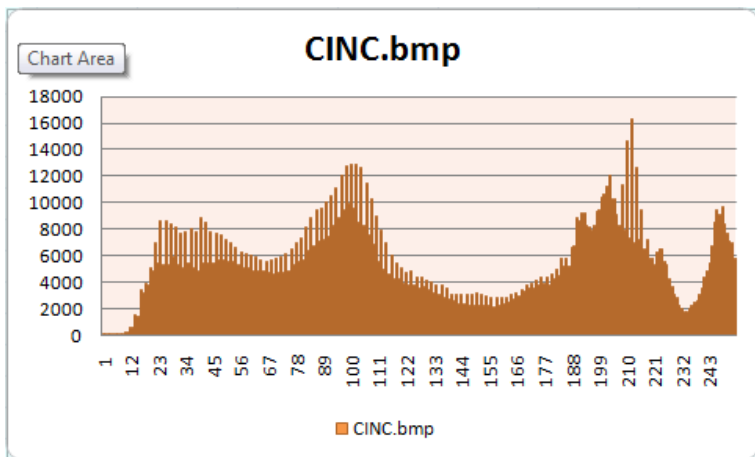
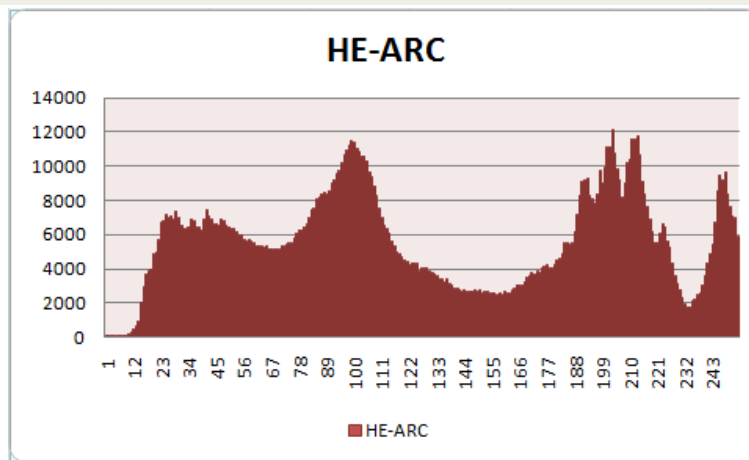
## Was ist zu tun ?

- Den Zugang zum Internet schützen
- Das Informatiknetz schützen
- Den Inhalt Ihrer Website überprüfen
- Ihre Daten sichern
- Software und Betriebssysteme warten (updaten)
- Elektronische Post filtern
- Benutzer sensibilisieren
- Zwischenfälle vorhersehen

## Ein Beispiel ...



# Steganographie





## Unsere Dienstleistungen

- **Ausbildung**
  - CAS in Cybersecurity
- **Beratung, Audit**
- **Password Wiederauffinden**