E-NRW Kongress
Düsseldorf, den 17.11.2014

intetics
The Remote In-Sourcing® Company

WHERE SOFTWARE CONCEPTS COME ALIVE

Datensicherheit im Outsourcing / Near-Shoring

Bernard Weber, *Geschäftsführer Intetics GmbH, ehemalig NOKIA/HERE Outsourcing Manager*

ISO 9001 Certified
ISO 27001 Certified
Microsoft Partner Gold Software Development
ORACLE GOLD PARTNER
A MEMBER OF NOA NATIONAL OUTSOURCING ASSOCIATION
WWW.INTETICS.COM

AGENDA

- Übersicht Datensicherheit
- Datensicherheit im Outsourcing
- Intetics & NOKIA/HERE Fallstudie:
  - Übersicht
  - Risiken & Partnerschaftsmodell
  - Zertifizierung und Regelungen
  - Sicherheit & Praxis
  - Ergebnisse

INTETICS ÜBERSICHT

intetics
The Remote In-Sourcing® Company

- Gründung **1995**
- **450** Mitarbeiter
- **130** ‚Crowd' Vertragspartner
- Kunden in **30 Ländern**
- **200+** erfolgreiche Projekte

- Sitz: **Chicago, IL**
- Niederlassungen:
  - **Düsseldorf, Deutschland**
  - **Tokyo, Japan**
- Entwicklungszentren:
  - **Minsk, Weißrussland**
  - **Kiew, Ukraine**
  - **Charkow, Ukraine**

- 2011-2013 **#1 Outsourcing Rising Star**
- 2006-2013 **Top Outsourcing 100**
- 2007-2013 **Global Services 100**
- 2010 **European IT Excellence Award**
- 2014 **EOA Award**
- 2009-2014 **Software 500**
- 2008-2014 **Inc 500/5000**

ISO 9001 Certified
ISO 27001 Certified
Microsoft Partner Gold Software Development
ORACLE GOLD PARTNER

WWW.INTETICS.COM

Übersicht: Was ist IT Sicherheit?

Definitionen:

> *Eine Datenbank vor Zerstörung und unerwünschten Aktionen Unbefugter zu schützen.*
>
> *Die Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten.*

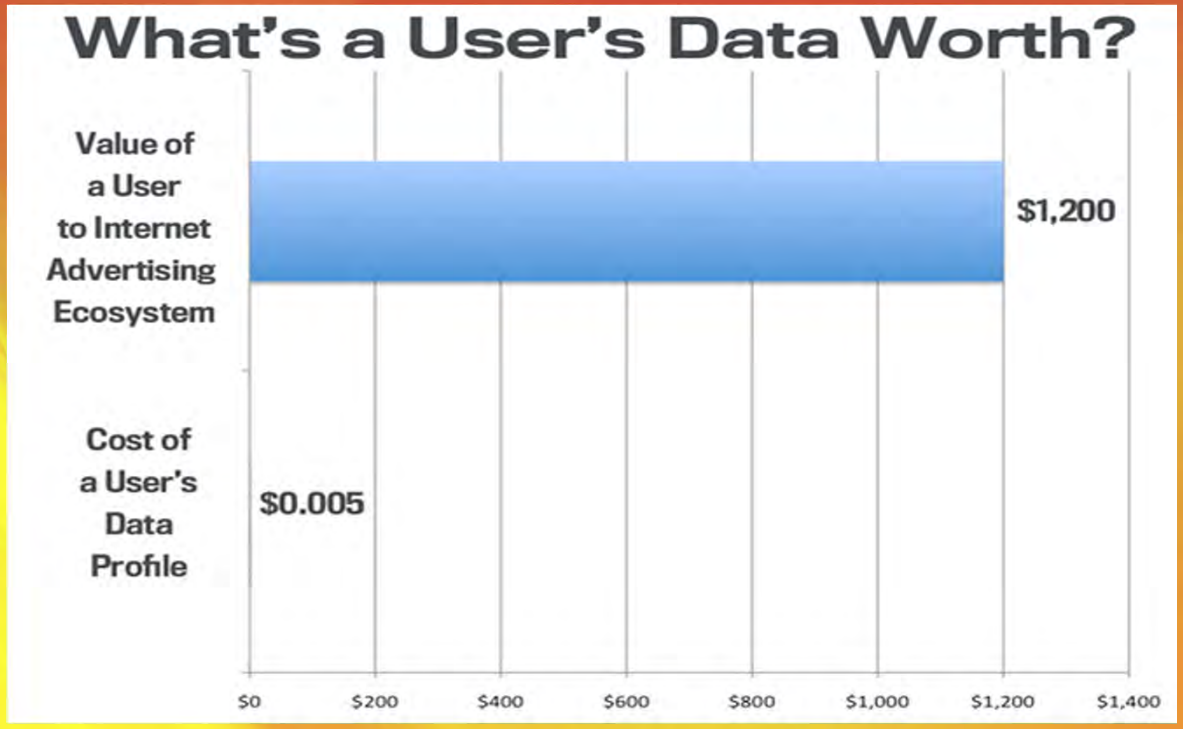
- **IT-Sicherheit:** Schutz der Daten vor böswilligen Angriffen und unbefugtem Zugriff
- **Informationssicherung:** Sicherstellung dass Daten nicht verloren gehen wenn Probleme auftreten
- **Jedermanns Business:** Benutzerschulung nicht nur für IT-Mitarbeiter; die Prozesskette ist nur so stark wie ihr schwächstes Glied
- **Neue Technologien:** Cloud Sicherheit funktioniert nach ähnlich Prinzipien wie physische Sicherheitsrichtlinien
- **Warum?** Was wollen wir verhindern?
  - Diebstahl von Geld oder Informationen
  - Datenschutzverletzungen
  - Datenverlust und Datenbeschädigung
  - Rufschädigung, Finanzielle Verluste

Übersicht: Was ist IT Sicherheit?

intetics
The Remote In-Sourcing® Company

Epsilon (2011) Millionen Kundendaten veröffentlicht (inklusive Daten der City Group)	**$ 4 Millionen Verlust**
Google & Silicon Valley (2009) Chinesische Regierung hackt sich in den Internet Explorer und kommt an Millionen IP Adressen	**Google zog sich aus dem China Geschäft zurück.**
Verisign (2010) Unklar was gestohlen wurde	**Verisign hat bis heute keine Einzelheiten veröffentlichen müssen.**
CardSystems Solutions (2005) 40 Millionen Kreditkartendaten gestohlen bzw. unbrauchbar gemacht	**CSS wurde aufgekauft**
Fidelity National Information Services (2007) 3,2 Millionen Kundendaten von einem Mitarbeiter gestohlen	**$20,000 pro Person Entschädigung gezahlt**

Übersicht: Wert von Daten



- Angenommen einen Datensatz kann man für $ 20 pro Satz verkaufen, dann hat eine Datenbank von 250.000 Einträgen einen Wert von $ 5 Millionen.

Übersicht: Derzeitiger Stand der Datensicherheit

intetics
The Remote In-Sourcing® Company

- 2013:
  - Gesamtkosten der Internetkriminalität: mehr als $ 400 Milliarden
  - 740 Millionen Datensätze exponiert (schlechtestes Jahr)
  - Nur 40% der größten Verstöße aufgedeckt
  - 91% aller Organisationen wurden Opfer einer Cyberattacke
- Was:
  - Kundendaten: Größte Gruppe mit 96% aller Attacken
  - Web Anwendungen: Größtes Ziel der Attacken im E-Commerce
- Wer:
  - Einzelhandel Non-Food (45%), Lebensmittelhandel (24%), Hotel und Gastgewerbe (9%)
- Wo:
  - USA= 73%; UK= 2%; Deutschland 1,6%
- Wie:
  - Viren und Spyware (66%)
  - Spam (61%)
  - Phishing (36%)

Mobile Malware: 400% Steigerung

Übersicht: Warum gibt es diese Probleme?

- Prozesse:
  - Prozesslücken: 89 % der Angriffe hätte mit grundlegenderen Sicherheitsmaßnahmen verhindert werden können
  - Häufigste Kennwort: Passwort1
- Verständnislücken:
  - 38 % wissen nicht was Big Data ist und 27 % haben nur eine partielles Verständnis
- Neue und schnelle Herausforderungen:
  - BYOD, Mitarbeiter Remote, immer online, Cloud
- Personalmangel:
  - 85% der IT Manager wünschen sich mehr Personal
- Druck:
  - 50% der IT Manager unter Innovationsdruck
  - 80% der IT Projekte unter Zeitdruck und Sicherheitsbedenken angegangen
  - Cloud und Mobile Einführung in Organisationen obwohl Sicherheitsrisiko bekannt ist

Datensicherheit & Outsourcing

intetics
The Remote In-Sourcing® Company

> Datensicherheit ist ein Prozess.

"OpenSSL was not developed by a responsible team."

— criticism of Heartbleed & OpenSSL

- Partnerschaftsmodelle
  - Zusammenarbeit unter Partnern
  - Bewährte & zertifizierte Sicherheitsprozesse
  - Nachhaltige Prozesse
- Verständnis der Sicherheitsverfahren & Vorschriften
- Klare Verantwortlichkeiten:
  - Fehlende Nachhaltigkeit bei der Überprüfung von Sicherheitsmängeln
  - Transparenz bei Sicherheitsproblemen: Vermeidung von ‚nicht unser Problem gewesen'
- Benutzerschulung
- *82 % der Unternehmen planen verwenden bereits Drittunternehmen zur Datensicherheit*

Fallstudie: INTETICS - NOKIA/HERE Partnerschaft

Historie:

- NAVTEQ: Anbieter von GIS-Daten und GPS-Navigations-Lösungen
- Kooperation begann 2008
- Kartenexpansion noch Osteuropa – Cyrillisch
- Gründung der Intetics GEO
- Weiterführung der Partnerschaft nach Übernahme durch Nokia und Namenswechsel zu HERE

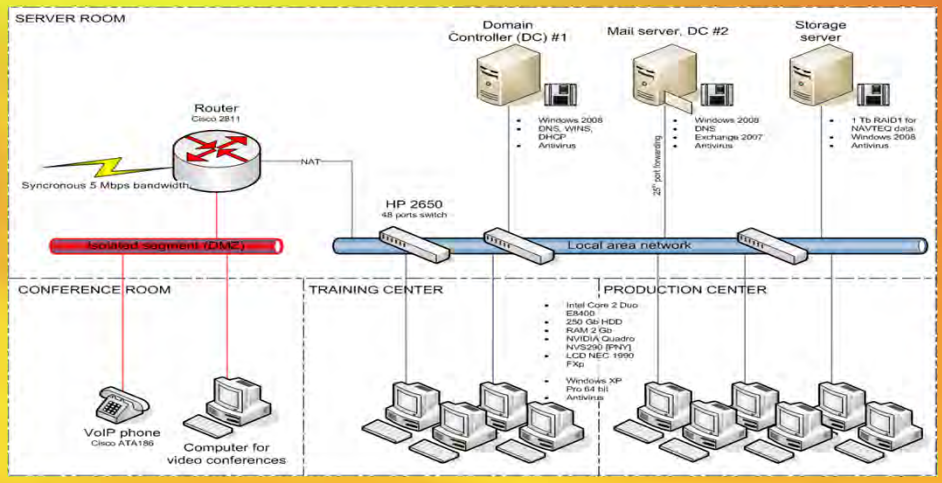
- Zielsetzung: Sichere Flexibilität
  - Ressourcen in Osteuropa
  - Sichere Datenerfassung & Verarbeitung von GIS-Daten
  - Team musste flexibel & skalierbar sein
- Herausforderungen:
  - Sicherheit & Qualität der Datenverarbeitung
  - Datenverarbeitung findet direkt auf dem Core Server des Kunden statt – Verbindung über VPN
  - Daten mussten separat von anderen Projekten und Kunden verarbeitet werden
  - Sicherheitssystem für die Mitarbeiter
- Lösungen:
  - 100% kundenspezifisches Team an Mitarbeitern
  - Biometrische Sicherheitskennung und räumliche Trennung
  - Sichere in-sich geschlossene Systemkonfiguration

NOKIA/HERE Anforderungen:

Spezifische Anforderungen:

- Vertraulichkeitserklärungen mit allen Mitarbeitern
- Haftung
- IT Security Policy Document
- Physische Zugangssicherung – Biometrische Kennung
- Point to Point Cisco IPsec VPN Verbindung
- Keine Transfer Devices auf den Rechnern – kein aktives USB Port
- Internetverbindung nur für White-List
- Sichere Kennwörter und Verschlüsselungen

- NOKIA/HERE Daten und Software
- Direkter Zugang zu Daten durch VPN Tunnel
- Nachhaltigkeit:
  - Recht zur Überprüfung - Audit
  - Trennung der VPN-Verbindung im Sicherheitsfall
- Netzwerkdiagramm:

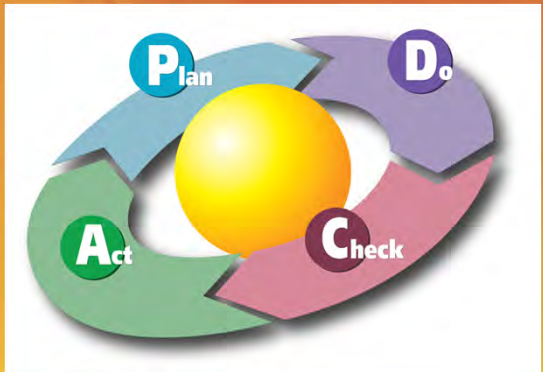


Fallstudie: Partnerschaftsmodell

Remote In-Sourcing® ist ein auf den Kunden zugeschnittenes Modell welches sich vom klassischen Outsourcing in folgenden Punkten unterscheidet:

- Aufbau einer Organisation – kein Projektteam im klassischem Sinn
- 100% Einbeziehung des Kunden in die Teamzusammenstellung
- erlaubte und gewollte Identifikation mit dem Kundenprodukt – Co-Branding
- Echte Partnerschaft – mehr als nur Zulieferer
- Aufbau einer echten, effektiven Organisation mit den richtigen Prozessen – mehr als nur Personalvermittlung
- Teilnahme und Unterstützung der strategischen Entwicklung des Kunden – mehr als Projektarbeit

Fallstudie: Zertifizierung und Regulierungen



- **ISO 27001**: *Informations- und Sicherheits-Managementsystem*
  - Verliehen bei Einhaltung von Sicherheits-garantien für Kunden
  - Basiert auf Plan-Do-Check-Act Prinzip
  - Richtlinien für sichere Daten-Management-Prozesse (z.B. Passwörter muss stärker als "Passwort1" sein..)

U.S.•EU SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE

Compliant with EUDPD
EU Data Protection Directive

- **US Safe Harbor Zertifizierung**
  - Identifiziert Unternehmen, die den EU-Privatsphäre-Schutz-Standards entsprechen
  - Compliance ermöglicht eine effizientere Datenübertragung zwischen USA und Europa
  - Jährliche Auswertung und Anreiz zur Weiterentwicklung (Eigenerklärung)
  - Belegt die Einhaltung der EU-Datenschutzgesetze und die europäischen Datenschutz-Richtlinien

intetics
The Remote In-Sourcing® Company

Vielen Dank
für Ihre Aufmerksamkeit.

intetics
The Remote In-Sourcing® Company

Mehr über uns:

Intetics GmbH
Fritz-Vomfelde-Strasse 34
40547 Düsseldorf
Tel : +49 (211) 53883-229
Fax : +49 (211) 53883-112
Email : contact@intetics.de

ISO 9001 Certified
ISO 27001 Certified
Microsoft Partner Gold Software Development
ORACLE GOLD PARTNER
A MEMBER OF NOA NATIONAL OUTSOURCING ASSOCIATION

WWW.INTETICS.COM

SOURCES

In order of use:

Armerding, T. (2012, February 15). The 15 Worst Data Breaches of the 21st Century. *CSO Online.* Retrieved from http://www.csoonline.com/article/2130877/data-protection/the-15-worst-data-security-breaches-of-the-21st-century.html

McCandless, D. (n.d.). World's Biggest Data Breaches. *Information is Beautiful.* Retrieved June 9, 2014, from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Madrigal, A. C. (2012, March 19). How Much Is Your Data Worth? *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730

The Value Of A Business Contact Database. *Ready Contacts.* Retrieved June 9, 2014, from http://www.readycontacts.com/the-value-of-a-business-contact-database-how-much-is-yours-worth/

2014 Data Protection & Breach Readiness Guide. (2014, April 7). *Online Trust Alliance.* Retrieved from https://otalliance.org/system/files/files/best-practices/documents/2014otadatabreachguide4.pdf (PDF)

Data Security Statistics. *Gazzang.* Retrieved June 9, 2014, from http://www.gazzang.com/resources/data-security-statistics

SOURCES (Continued)

2014 Trustwave Security Pressures Report. *Trustwave*. Retrieved June 9, 2014, from http://www2.trustwave.com/rs/trustwave/images/2014%20Trustwave%20Security%20Pressures%20Report.pdf (PDF)

2013 Global Security Report. *Trustwave.* Retrieved June 9, 2014, from http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf (PDF)

Kontsevoi, B., & Kontsevaia, D. (2013, May 1). Hitting the Right Balance of "In" and "Out": A Closer Look at Evolving Sourcing Models. *Pulse Magazine*, Issue *5*, pp 22-23. http://www.intetics.com/custom-software-development-company/white-papers/download-white-paper/?wpid=43 (PDF)

Kontsevoi, B. (2012, November 8). Evolution of sourcing models during the last decade: hands on experience of a 20 year old outsourcing company. *CIO-CEE Conference*. Lecture conducted in Prague, Czech Republic. http://www.intetics.com/custom-software-development-company/white-papers/download-white-paper/?wpid=35 (PDF)

ISO 27001: Information Security Management. *ISO.org.* Retrieved June 9, 2014, from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

US-EU Safe Harbor. (2013, December 18). *Export.gov*. Retrieved from http://export.gov/safeharbor/eu/eg_main_018365.asp