

SGRP Frühlingsevent – 05. Mai 2010

"Risiko in der Cloud"

Neue Hacker-Attacken in der "Cloud"



Neue Hacker-Attacken in der "Cloud"

- Martin Rutishauser
 - Security Engineer, ISPIN AG Bern
 - SGRP Vorstandsmitglied
 - Referent HSLU CAS/MAS IS
- Agenda
 - Kurze Einführung Cloud Computing
 - Was sind die Top Risiken in der Cloud? (+ Massnahmen)
 - Praktisches Cloud Hacking
 - Cloud Orakel (Future Look)
 - Schutz und Verteidigung generell in der Cloud

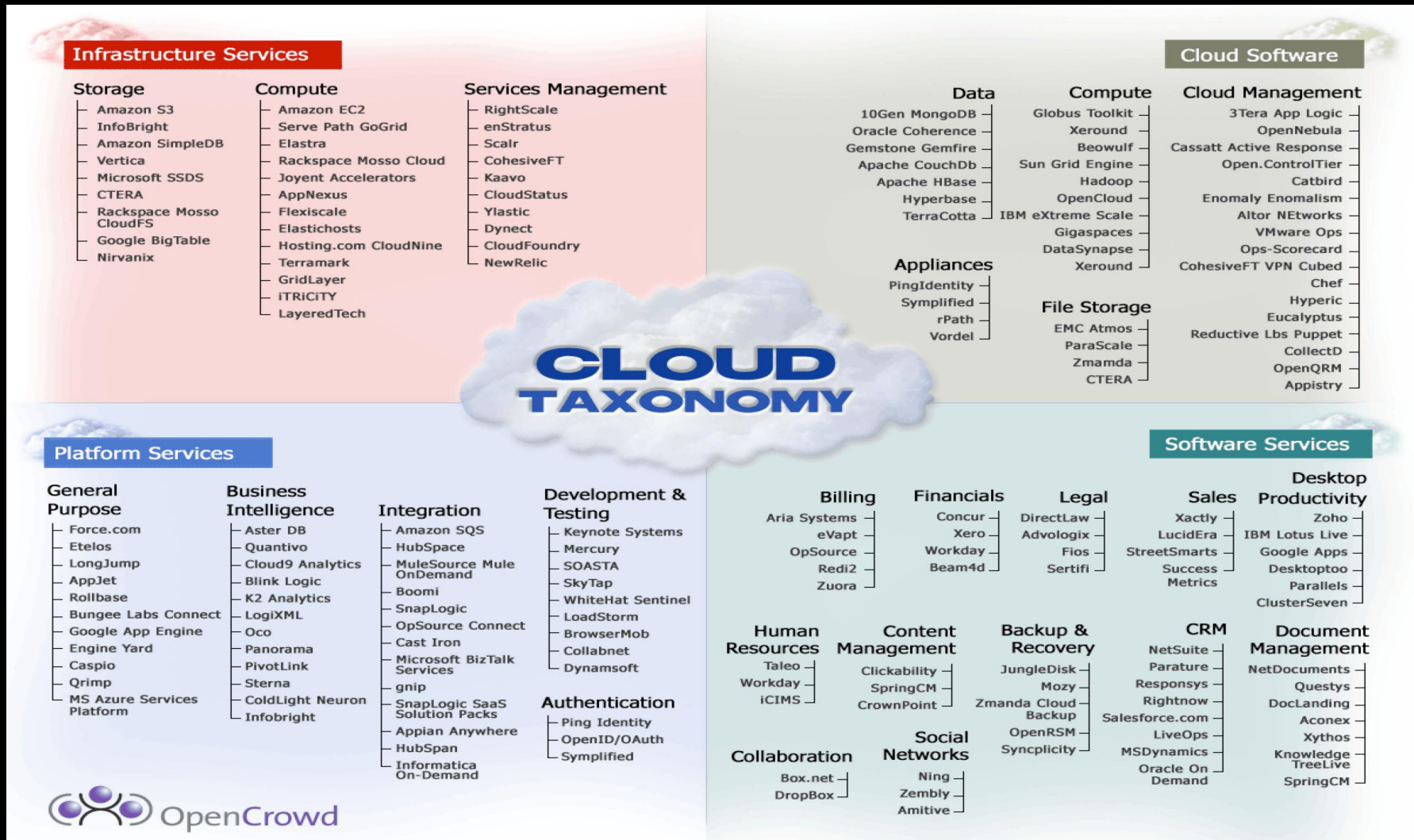
Neue Hacker-Attacken in der "Cloud"

- **Wer hat schon Daten/Dienste/Anwendungen in der Cloud?**



Neue Hacker-Attacken in der "Cloud"

- Cloud Taxierung (OpenCrowd)



Neue Hacker-Attacken in der "Cloud"

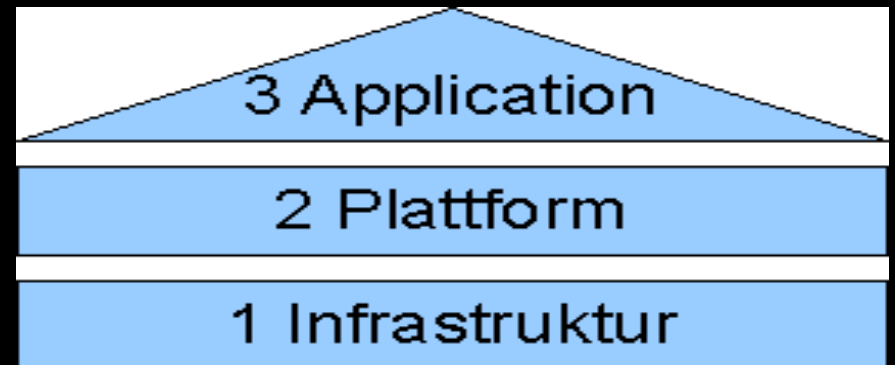
- **Was versteht man eigentlich unter Cloud Computing?**
- **Colocation Services**
 - Rack, Strom, Lüftung, Netzwerk
- **HaaS (Host as a Service) und IaaS (Infrastructure as a Service)**
 - Home für virtualisierte Maschinen
 - Amazon EC2 (XEN) / Rackspace / Terremark (vSphere)
 - Microsoft LiveMesh
- **CaaS (Computer as a Service) und DaaS (Desktop as a Service)**
 - Virtual Device Infrastructure
 - VMware View, Linux, Windows

Neue Hacker-Attacken in der "Cloud"

- **PaaS (Platform as a Service)**
 - Mit OS, Patching, Backend Interface für Apps
 - Microsoft Azure (.NET/PHP), Google App Engine (Java/Python), force.com (Business Logic, User Interface Design)
- **SaaS (Software as a Service)**
 - End Anwendung zum Benutzer
 - Microsoft Exchange/Sharepoint/Dynamics CRM, Salesforce CRM, IBM Lotus Live, Qualys VM, Evernote
- **Private Clouds**
 - VMware, XEN, Hyper-V, Citrix
- **Social Networking**
 - Flickr, Xing, LinkedIn, MySpace, Orkut, Buzz, Facebook, Hatebook, Baidu, Twitter, StudiVZ, Netlog, ...

Neue Hacker-Attacken in der "Cloud"

- **Weitere Unterscheidungen von Cloud Computing**
 - Private vs. Public
 - Open vs. Closed/Exclusive
 - Enterprise, Departmental, Exploratory
 - Hybrid Cloud (zB. Private → Failover Public)
- **Aufbau Cloud Computing**
 - 1) Infrastruktur
 - 2) Plattform
 - 3) Anwendung



Neue Hacker-Attacken in der "Cloud"

- Was sagt Gartner dazu? (2009)



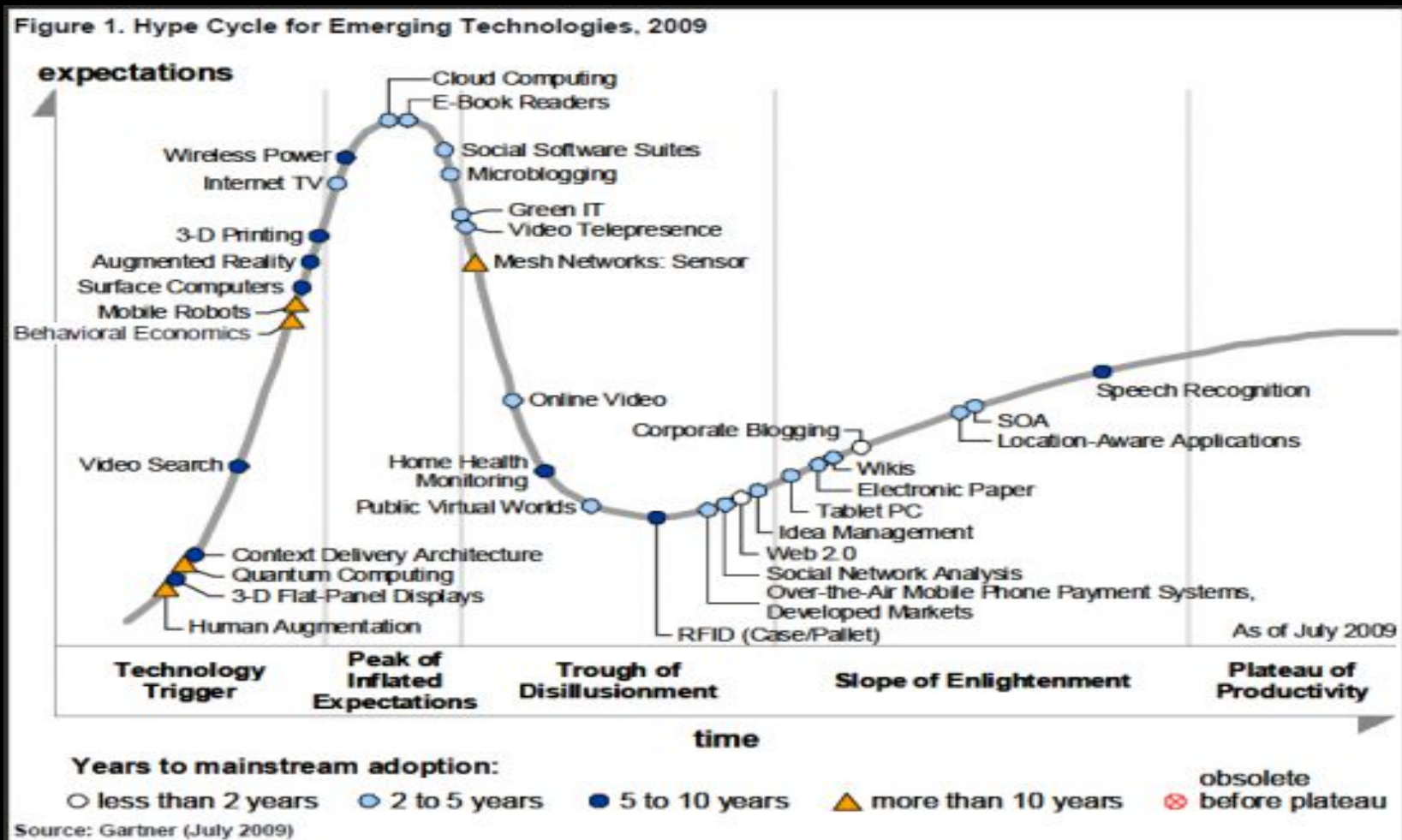
Neue Hacker-Attacken in der "Cloud"

- Gartner's Magic Quadrant (Cloud Hosting, June 2009)



Neue Hacker-Attacken in der "Cloud"

- Gartner's Hype-Cycle (July 2009)



Neue Hacker-Attacken in der "Cloud"

- An dieser Stelle Fokus auf...
 - **SaaS = Software as a Service**
 - Salesforce, Qualys, Evernote
 - **PaaS = Plattform as a Service**
 - Google App Engine, Microsoft Azure, force.com
 - **IaaS = Infrastructure as a Service**
 - Amazon EC2, Terremark, Rackspace

Neue Hacker-Angriffe in der "Cloud"

- SaaS = Software as a Service
 - Salesforce CRM (force.com = PaaS)

The screenshot shows the Salesforce website homepage. At the top, there is a navigation bar with the Salesforce logo, a 'Rate this page' link, 'Customer Login', 'Free Trial', and a search box. Below the navigation bar are links for 'Products', 'Services', 'Events', 'Community', and 'About Us'. The main content area features a large blue banner for 'chatter Collaboration Cloud' with the text 'The conversation starts here'. To the left of the banner is a screenshot of the Salesforce interface showing a user profile for 'Monica Lawrence'. To the right of the banner are three red-bordered buttons: 'contact manager \$5 per month', 'free trial Salesforce CRM for 30 days', and 'view demo'. Below the banner, there is a section titled 'The leader in customer relationship management (CRM) & cloud computing' with four columns: 'Sales Cloud™ 2 The world's #1 sales application.', 'Service Cloud™ 2 The future of customer service.', 'Custom Cloud™ 2 The platform for custom app', and 'Chatter Collaboration Cloud'. On the right side, there are links for 'Contact me', 'Editions & Pricing', and 'Cloud & CRM Resources'. At the bottom right, there is a 'Thank You!' section with the text 'Together we've raised over \$800,000 for relief agencies in Haiti'.

Neue Hacker-Angriffe in der "Cloud"

- SaaS = Software as a Service
 - Qualys Vulnerability Management



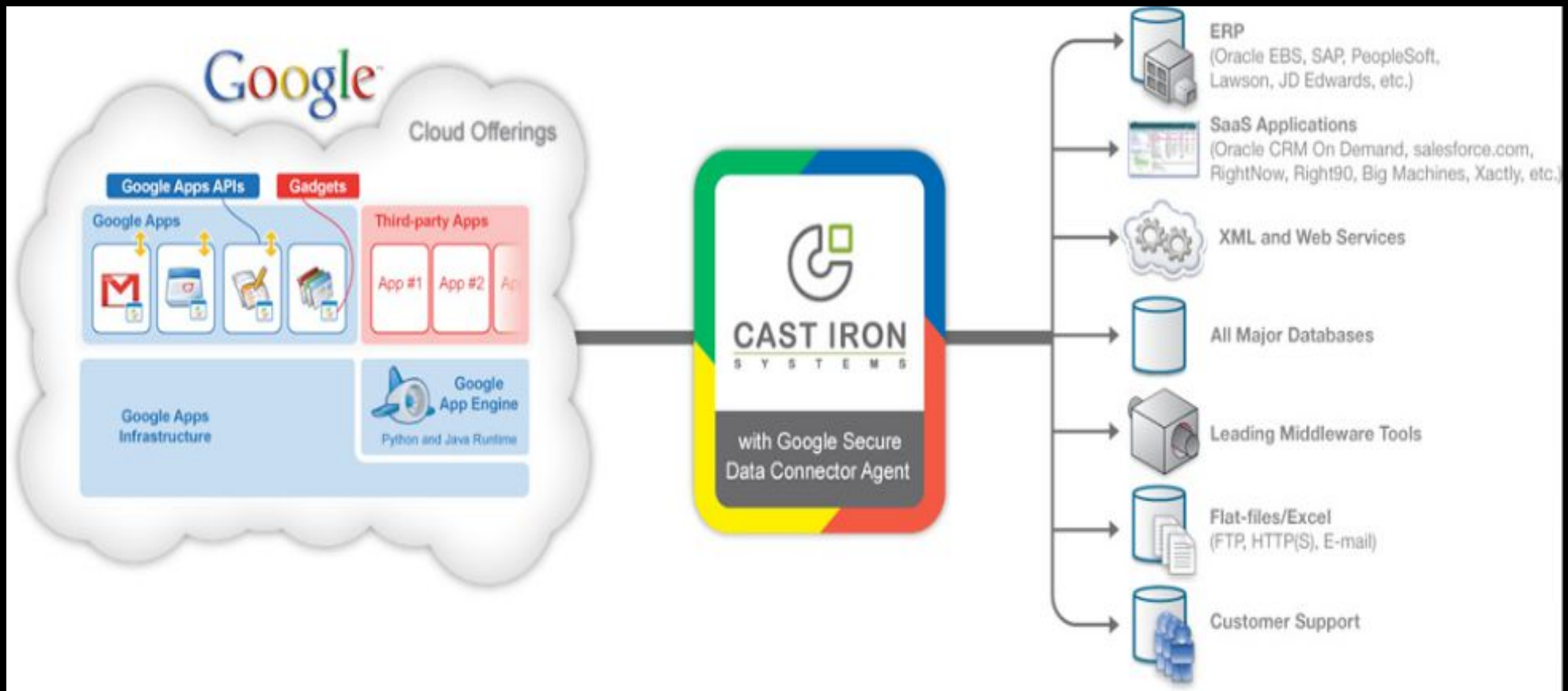
The screenshot shows the Qualys website homepage. At the top left is the Qualys logo. To its right are navigation links for "USA", "Contacts", and a "Login" button. A search bar is located on the far right of the top navigation. Below the logo is a horizontal menu with links for "PRODUCTS", "CUSTOMERS & AWARDS", "PARTNERS", "TRAINING & SUPPORT", "RESOURCES", and "COMPANY".

The main banner features a blue background with the text "Introducing QualysGuard® Malware Detection". A large red "X" is superimposed over the word "MALWARE". To the right of the "X" is the text "A Ground Breaking **FREE** Malware Detection Service". Below this are two bullet points: "• Prevent the Spread of Malware to Visitors" and "• Protect Web Sites from Malicious Activities". At the bottom right of the banner is a red button that says "It's Free SIGN UP TODAY!".

Below the banner are three sections: "QualysGuard Success Stories" with the text "40+ of the Global Fortune 100 use Qualys"; "Security Alerts" with a link to "March 9 — Microsoft March 2010 Security Update - 2 bulletins, 8 vulnerabilities"; and a red button labeled "Free Tools and Trials" with a biohazard icon and the text "QualysGuard Malware Detection".

Neue Hacker-Attacken in der "Cloud"

- PaaS = Plattform as a Service
 - Google App Engine



Neue Hacker-Attacken in der "Cloud"

- **PaaS = Plattform as a Service**
 - **Microsoft BPOS (Business Productivity Online Standard Suite)**
 - **Microsoft Azure**



Neue Hacker-Attacken in der "Cloud"

- IaaS = Infrastructure as a Service
 - Amazon EC2 / S3 / SQS, Terremark, Rackspace

The screenshot shows the Amazon Elastic Compute Cloud (Amazon EC2) product page. At the top left is the Amazon Web Services logo. To the right are links for "Sign in to the AWS Management Console" and "Create an AWS Account". Below the logo is a navigation bar with tabs for "AWS", "Products", "Developers", "Community", "Support", and "Account". A "Products & Services" dropdown menu is open, showing a list of links under "Amazon EC2 Details": "EC2 Overview", "EC2 FAQs", "EC2 Pricing", "Amazon EC2 SLA", "EC2 Instance Types", "EC2 Instance Purchasing Options", "Reserved Instances", "Spot Instances", and "Windows Instances". The main content area is titled "Amazon Elastic Compute Cloud (Amazon EC2)" and contains a description: "Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers." Below this is a paragraph: "Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios." To the right of the main text is a "Sign Up For Amazon EC2" button. At the bottom, there is a section titled "This page contains the following categories of information. Click to jump down:" with four links: "Amazon EC2 Functionality", "Service Highlights", "Pricing", and "Resources".

Neue Hacker-Attacken in der "Cloud"

- **TOP Risiken in der Cloud (Cloud Security Alliance +)**
 - **Sowie Massnahmenvorschläge**
 - Missbrauch und schamlose Nutzung Cloud Computing
 - Unsichere Interfaces und API's
 - Böartige Insider
 - Gemeinsame Benutzung von Technologien
 - Datenverlust oder Datenabfluss
 - Kunden- oder Dienst-Entführung (hijacking)
 - Unbekanntes Risikoprofil
 - Budget-Falle
 - Offline Cloud

Neue Hacker-Attacken in der "Cloud"

- **1. Missbrauch und Schamlose Nutzung Cloud Computing**
 - IaaS Providers haben einen (zu) nachsichtigen Registrierungsprozess => Registrierung mit Kreditkarte
 - Cyber-Kriminelle können Exploits und Malware hosten
- Massnahmen
 - Cloud Provider:
 - Strenger Registrierungsprozess
 - Monitoring Public Blacklists
 - Anonyme (?) Überwachung Netzwerkverkehr Kunden

Neue Hacker-Attacken in der "Cloud"

- **2. Unsichere Interfaces und API's**
 - Interfaces und API's müssen irrtümliche oder absichtliche Versuche zur Umgehung der Policy erkennen
 - Default Konfiguration oft ungenügend (!)
- Massnahmen
 - Cloud Provider:
 - Starke Authentisierung, Access Controls
 - Monitoring
 - Verschlüsselung
 - Benutzer:
 - Starke Authentisierung, Access Controls
 - Verschlüsselung

Neue Hacker-Attacken in der "Cloud"

- **3. Böartige Insider**
 - Risiko eines böartigen Insiders (Cloud Provider) hoch
 - Transparenz der Prozesse und Prozeduren Cloud Provider notwendig
- Massnahmen
 - Cloud Provider:
 - Transparenz schaffen
 - Benutzer:
 - Transparenz verlangen
 - Information Security und Management, Supplier Chain
 - Job Requirements (Handling meiner Daten!)
 - NDA erzwingen (?)

Neue Hacker-Attacken in der "Cloud"

- **4. Gemeinsame Benutzung von Technologien**
 - IaaS Providers können Infrastruktur-Komponenten einsetzen, welche nur unzulängliche starke Isolationsfähigkeit mandantenfähiger Architekturen unterstützen
 - Virtualisierung wird benutzt, um die Lücke zu schliessen
- **Massnahmen**
 - **Cloud Provider:**
 - Monitoring der Umgebung (unauthorisierte Änderungen)
 - Verfolgen Hacker-Aktivitäten (Hypervisor-Hacking!)
 - **Benutzer:**
 - Patch Management Reporting, Einsatz starker Authentisierung

Neue Hacker-Attacken in der "Cloud"

- **5. Datenverlust oder Datenabfluss**
 - Jederzeit möglich, Gefahr allgegenwärtig
- Massnahmen
 - Cloud Provider:
 - Starke Authentisierung für Zugriff auf API
 - Verschlüsselung der Daten (Transport), Starke Keys
 - Storage, Management, Destruction
 - Benutzer:
 - Klassifizierung Daten, Dateninventar
 - Verschlüsselung der Daten (Transport)
 - Logging/Audit von Aktionen/Changes
 - Data Loss Prevention (DLP)

Neue Hacker-Attacken in der "Cloud"

- **6. Kunden- oder Dienst-Entführung (Hijacking)**
 - Angreifer kann in Besitz von Account-Credentials gelangen
 - Einsicht in Aktivitäten
 - Image-Verlust (Umleitung Kunden, Angriffe)
 - Verlust von Vertraulichkeit, Integrität, Verfügbarkeit
- **Massnahmen**
 - **Benutzer:**
 - Kein Sharing von Account-Credentials für Benutzer oder Dienste
 - Nach Möglichkeit Verwendung starker Authentisierung

Neue Hacker-Attacken in der "Cloud"

- **7. Unbekanntes Risikoprofil**
 - Das eigene Risiko-/Sicherheitsprofil kennen
 - Softwareversionen
 - Verwundbarkeitsprofile
 - Einbruchversuche
 - Sicherheitsdesign
- Massnahmen
 - Cloud Provider/Benutzer:
 - Risikoanalyse erstellen (lassen)
 - Mitbenutzer der Infrastruktur herausfinden
 - IDS-Logging, Redirection-Versuche loggen

Neue Hacker-Attacken in der "Cloud"

- **8. Budget-Falle**

- Einer der Hauptgründe für die Cloud sind oft Budget-Sparmassnahmen

- Starke Authentisierung (nicht eingesetzt!)
- ESX Server Security Zones (1 pro Zone!)

- **Massnahmen**

- **Cloud Benutzer:**

- Die Cloud spart wahrscheinlich nur bei längerfristigem Einsatz wirklich Geld
- Verlockung "billigeres Angebot!" gut prüfen

Neue Hacker-Attacken in der "Cloud"

- 9. Offline Cloud
 - Ausfall der Internetanbindung

Uptime	Tag	Monat	Jahr
99.999%	00:00:00.4	00:00:26	00:05:15
99.990%	00:00:08	00:04:22	00:52:35
99.900%	00:01:26	00:43:49	08:45:56
99.000%	00:14:23	07:18:17	87:39:29

- Massnahmen
 - Cloud Provider/Benutzer:
 - Redundante Internet-Anbindung

Neue Hacker-Attacken in der "Cloud"

- Praktisches Cloud Hacking
 - 1) Nach Gold in der Cloud googlen
 - Salesforce (www.google.com/search?q=inurl:%22pw%3D%22+site:salesforce.com&hl=en&filter=0)

The screenshot shows the Salesforce.com user interface. At the top, there is a navigation bar with the Salesforce logo, a search bar, and a user profile dropdown showing 'セールス 2'. Below the navigation bar, there are several tabs: 'ホーム', '取引先', '取引先責任者', and 'プロジェクト'. The main content area is divided into several sections:

- Header:** '石田 参照(システム開発)' with a sub-header '次曜日 2010/02/23' and a link 'Winter '10の詳細はこちら'.
- Calendar:** A calendar view for February 2010. The current date is '今日 2010/02/23'. Below the calendar, it says '7日先までの行動予定はありません。' (No activities scheduled for the next 7 days).
- To-Do List:** A table with columns '完了', '期日', '件名', '名前', and '関連先'. The list contains several items, some with red exclamation marks indicating urgency or errors.

完了	期日	件名	名前	関連先
		リリースノートの確認 !		
		入門チュートリアル参照 !		
		個人設定の確認 !		
		見積書作成		新規CADシステム (モーリシャス)
		契約未承認		00000101

Neue Hacker-Attacken in der "Cloud"

- **Praktisches Cloud Hacking**
 - **2) Manipulationen in der Cloud**
 - Manipulierte AMI (Amazon Machine Images), der Community vertrauen?
 - **3) Informationsabfluss in der Cloud**
 - Informationsabfluss (Amazon EC2) durch Javascript (Side-Channel-Attack)
 - **4) Dokumentenabfluss in der Cloud**
 - "Hacker Croll" hackte Twitter-Admin (Juli 2009), beschaffte sich mit den Credentials Zugriff auf Google-Apps -> Dokumente leaked

Neue Hacker-Attacken in der "Cloud"

- **Orakel: Cloud Computing + Hacking + 1 Prise Ironie :) =**
 - **Zielkonflikt Datenschutz/Sicherheit und "Outsourcing" (Cloudsourcing?)**
 - **Vertrauen in den Cloud-Dienstleister (Cloudcontrolling?)**
 - **Die Cloud kann als Ausgangspunkt für Angriffe genutzt werden (böse, böse Cloud!)**
 - **Hochleistungs-Cracking wird auf einmal erschwinglich (10 Zeichen, nur kleine Buchstaben ~ 2000\$ -> Rainbowcloud? -> www.wpacracker.com)**
 - **Malware und Botnets in der Cloud (Hypervisor-Rootkits!)**
 - **Sicherheitsmassnahmen-NG (Next-Generation, !not Perimeter-based)?**

Neue Hacker-Attacken in der "Cloud"

- **Schutz und Verteidigung in der Cloud ganz allgemein**
 - **Begrenzung Cloud**
 - Risikobewusster Einsatz von Cloud-Technologien
 - **Sichere Passwörter**
 - Hohe Komplexität, oft wechseln, nie gleiches Passwort
 - **Sichere Programmierung**
 - PHP, Javascript, Ajax, etc. Härten/Limitieren
 - Benutzerinput/-output überprüfen
 - **Verschlüsselung wo möglich**
 - Transport und Ablage von Daten
 - **Solides Vertragswerk**
 - Insourcing-Option, Crypto, Forensic, Reporting

Neue Hacker-Attacken in der "Cloud"

- **Literatur und Links**

- ENISA Studie: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
- ISACA Whitepaper: www.isaca.org/cloud/
- O'Reilly: Hacking The Next Generation, Cloud Security and Privacy
- McGrawHill: Cloud Computing – A practical approach
- Cloud Security Alliance Top Threats and Security Guide
 - <http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
 - <http://cloudsecurityalliance.org/csaguide.pdf>
- Hacking Exposed: Virtualization and Cloud Computing (2010)
- MS BPOS: www.microsoft.com/online/business-productivity.msp

Neue Hacker-Attacken in der "Cloud"

Wem darf ich noch eine Frage beantworten?

Martin Rutishauser – [martin.rutishauser\(a\)ispin.ch](mailto:martin.rutishauser@ispin.ch)

