KRASNI NOVI SVET
STANDARDIZIRANJA, SKLADNOSTI IN CERTIFICIRANJA
VARNOSTI V OBLAKIH

Stanka Šalamun, ACROS d.o.o.

19.4.2011, DSI 2011

acros

PENETRACIJSKI PREIZKUSI

VARNOSTNE ANALIZE

hp invent

IBM

vmware

bea

PGP

NASDAQ

macromedia

Microsoft

RSA SECURITY

NETSCAPE Communicator

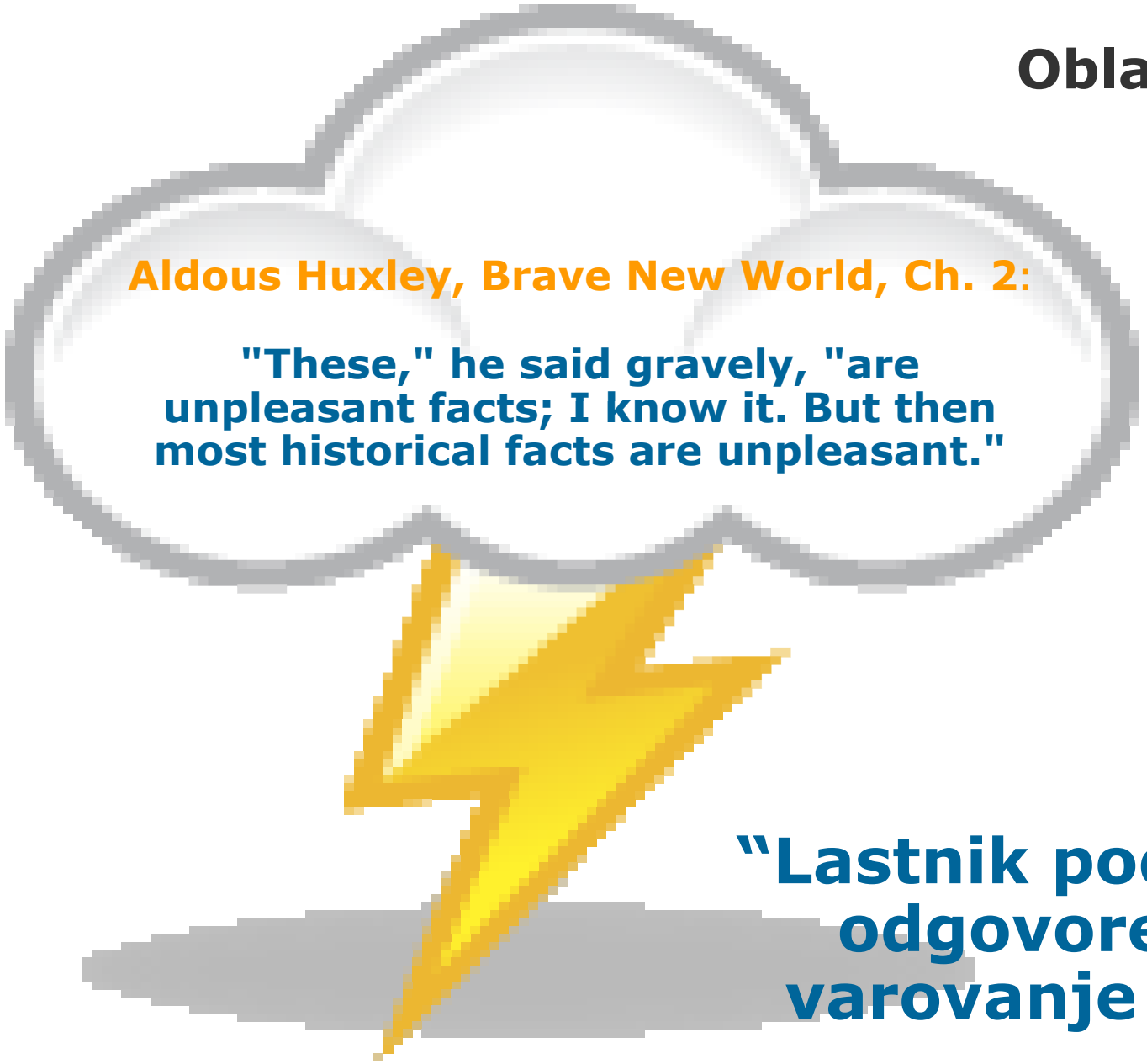
Oblačni izzivi

- **Podatki v oblaku – privlačna tarča – finančna motivacija**

- "Je pametno hraniti pomembne ali občutljive podatke v oblakih?"
- "Ali lahko živimo z izgubo nadzora nad pomembnimi podatki?"
- "Kje vse so razpršeni naši podatki v oblaku? V koliko kopijah? Vemo za vse? "
- "Kje (geografsko) so naši podatki, kateri zakonodaji so podvrženi?"
- "Nočemo biti v istem oblaku kot konkurenca!"
- "Lahko k nam lahko vdrejo z izkoriščanjem napak drugih oblačnih stanovalcev?"

"Lastnik podatkov" odgovoren za varovanje le-teh

Oblačni izzivi



"Lastnik podatkov" odgovoren za varovanje le-teh

Koliko so vredna naša informacijska sredstva?

- **Ključen premik v ocenjevanju vrednosti:**
  - Podjetja se bolj sprašujejo po dejanski vrednosti svojih ključnih informacijskih sredstev
  - Več konkretnega ocenjevanja potrebnosti informacijskih sredstev ("kaj bo, če podatek ne bo dostopen", "kaj bo, če mi bo kdo spreminjal podatke")
  - Kdo bo kriv za morebitno izgubo/razkritje podatkov?
  - Ponudniki v oblakih ne morejo poznati prave vrednosti podatkov svojih strank

Katere podatke v oblak?

Podatki:

- Spletne trgovine
- Kadrovske in CRM/prodajne evidence
- Projektne pisarne
- Elektronska pošta
- Varnostne kopije
- Male eBolnišnice
- Davčne storitve
- ...

Različne potrebe po varnosti:

ISO2700x

ZVOP

PCI-DSS

Sarbanes-Oxley

HIPAA

COBIT

FISMA

NIST

...

Varnostne zahteve:

- Varnostne funkcije
- Dostopnost
- Javna varnostna poročila
- Redni pregledi
- Šifriranje
- Replikacije in varnostne kopije
- Usklajenost s standardi
- Terminalni pogoji

Oblaki bodo po varovanju zelo različni in nudili različno drage storitve!

Ključni igralci standardizacije varnosti oblakov

- **CSA:** https://cloudsecurityalliance.org/
- **ENISA:** http://www.enisa.europa.eu/
- **Eurocloud:** http://www.eurocloud.org/
- **NIST:** http://www.nist.gov/index.html

Cloud Security Alliance: CCSK certifikat

CSA CCSK: Certificate of Cloud Security Knowledge

- Prvi od industrije priznani certifikat obvladovanja oblačne varnosti za **posameznike**
- Osnova:
  - CSA: "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" (dec 2009)
  - ENISA: "Cloud Computing: Benefits, Risks and Recommendations for Information Security" (nov 2009)
- Izpit: po spletu, 295$ (2 poskusa)

Cloud Security Alliance: "GRC Stack"

- **GRC (Governance, Risk Management and Compliance) stack:**
  - **osnova: Cloud Controls Matrix**
  - CloudAudit: "Automate the Audit, Assertion, Assessment, and Assurance"
  - Vprašalnik Consensus Assessment Questions ("Cloud-Specific Control Assessment")

CCM™ Cloud Controls Matrix

Cloud Audit The A6 Working Group

CAI™ Consensus Assessments Initiative

CSA Cloud Controls Matrix v1.1

- **Dec 2010, preko 50 sodelujočih strokovnjakov informacijske varnosti**

- **Tabela po usklajenostih:** COBIT 4.1, HIPAA, ISO 27001-2005, NIST SP 800-53, PCI-DSS v2.0, FedRAMP
- Obvladovanje področij nadzora po plasteh (IaaS, PaaS, SaaS)
- Obvladovanje področij nadzora po načinu uporabe (stanovalec, ponudnik)

- **99 področij nadzora, po 11 skupinah:**

CO – Compliance	OP - Operations Management
DG - Data Governance	RI – Risk Management
FS - Facility Security	RM - Release Management
HR - Human Resources Security	RS – Resilience
IS - Information Security	SA - Security Architecture
LG – Legal	

CSA Cloud Controls Matrix v1.1

Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability		Compliance Mapping					
				SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53	FedRAMP	PCI DSS v2.0
Security Architecture - Segmentation	SA-09	System and network environments are separated by firewalls to ensure the following requirements are adhered to: • Business and customer requirements • Security requirements • Compliance with legislative, regulatory, and contractual requirements • Separation of production and non-production environments • Preserve protection and isolation of sensitive data	No Change	X	X	X	X	X	COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7	PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4
Security Architecture - Wireless Security	SA-10	Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.). • Logical and physical user access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	No Change	X	X	X	X	X	COBIT 4.1 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) (New) 45 CFR 164.312(e)(1) (New) 45 CFR 164.312(e)(2)(ii) (New)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 CM-6 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-18 (1) NIST SP800-53 R3 AC-18 (2) NIST SP800-53 R3 AC-18 (3) NIST SP800-53 R3 AC-18 (4) NIST	PCI DSS v2.0 1.2.3 PCI DSS v2.0 2.1.1 PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.011.1 PCI DSS v2.0 9.1.3
Security Architecture - Shared Networks	SA-11	Access to systems with shared network infrastructure shall be restricted to authorized personnel in	No Change	X	X	X	X	X		45 CFR 164.312 (a)(1)	A.10.8.1 A.11.1.1 A.11.6.2	NIST SP800-53 R3 PE-4 NIST SP800-	NIST SP800-53 R3 PE-4	PCI DSS v2.0 1.3.5 PCI DSS

"EuroCloud Star Audit Certification"

- **"maturitetni" model: od ★ do ★★★★★**
- **EuroCloud Star Audit SaaS**
  - **"SaaS Ready" – za ponudnike podatkovnih centrov** (pogodbene zaveze, varovanje podatkov, operativni in varnostni opravki)
  - **"SaaS App" – za ponudnike storitev na certificirani "SaaS Ready" platformi** (izvedba aplikacije in integracija v oblak, usklajenost z zakonodajo in standardi, lahko samo "delta" pregled glede na "SaaS Ready" certifikat)
  - **EuroCloud Star Audit "PaaS":** napovedan za leto 2011
  - **EuroCloud Star Audit"IaaS":** napovedan za leto 2011
- **Prvi certifikat: marec 2011, Pironet NDH, za "web MS Office" rešitev, 5 zvezdic**
- **Proces**: obvezna delavnica, NDA, 6-8 tedenska revizija, certifikat velja 2 leti

"Eurocloud Star Audit (SaaS) Certification (2)"

★ ali ★★ **"Less Reliability and Security"**

★★★ **"Trusted Cloud Service"**

- podatkovna varnost in zasebnost, pogodbene obveze in izhodni pogoji, zanesljivost

preverjanje SLA, tehnične podpore, dokumentov

TESTNA PODROČJA:

- **Profil ponudnika**
- **Pogodba in skladnosti**
- **Podatkovna varnost**
- **Infrastrukturne operacije**
- **Procesi**
- **Aplikacije**
- **Izvedba**

★★★★ **"Trusted Cloud Service Advanced"**

- *** in dodatni nadzor kvalitete

preverjanje šifriranja podatkov, upravljanja incidentov, poročanja, uporabniških vlog, infrastrukture

★★★★★ **"Trusted Cloud Service Advanced High Available"**

- **** in redundanca podatkovnega centra

penetracijski testi, preverjanje redundance, 99.99% dostopnost

NIST: SP 800-144

- **NIST: SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing (draft)**

  28. jan 2011

  http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

- **NIST: SP 800-145: The NIST Definition of Cloud Computing (draft)**

  28. jan 2011

  http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Drugi pomembni igralci ("splošne" oblačne dobre prakse)

- **Cloud Industry Forum ("CIF"), UK:**

  - splošen oblačni "code of practice"
  - samocertifikacija (200-8000 GBP na leto)

- **ISACA**

  - Cloud Computing Management Audit/Assurance Program

Zaključek

- **Zaradi prehoda v oblake se več sprašujemo o vrednosti podatkov**
- **Oblaki prihodnosti bodo zaradi zahtev certificiranja (tudi varnosti) superspecializirani**
- **V oblakih lahko ravno zaradi zahtev varnostnih standardov (ponekod) dvignemo varnostne nivoje**
- **Certificiranje varnosti v oblakih bi moralo prispevati k povečanju zaupanja uporabnikov**

- **Ampak:**
  - Vsak "lastnik podatkov" je še vedno sam odgovoren za svoje podatke.
  - So nivoji certificiranja uporabnikom (kupcem) dovolj jasni?
  - So revizije za pridobitev certifikatov dovolj tehnično poglobljene?
  - Je "samocertifikacija" za varnost v oblakih pravi način zagotavljanja varnosti?

Ključno vprašanje:

Bodo certificirane oblačne rešitve vzdržale napade?