Predstavitev slovenskega odseka Cloud Security Alliance

Damir Savanović, CISA, CISM
predsednik odseka

Agenda

Predstavitev slovenskega odseka Cloud Security Alliance

1. Predstavitev
2. Področja delovanja
3. GRC knjižnica
4. Primeri CAI in CCM – Aplikacijska varnost
5. CCSK
6. Zaključek

Cloud Security Alliance

Predstavitev

- *Globalna, neprofitna organizacija*
- *23,000+ članov, 100 korporativnih članov, 50 odsekov*
- *Gradimo najboljše prakse in zaupanja vreden ekosistem*
- *Agilna filozofija, hiter razvoj uporabnih raziskav*
  - GRC: Uravnoteževanje skladnosti z upravljanjem tveganji
  - Referenčni modeli: z uporabo obstoječih standardov
  - Identiteta: osnova za delovanje oblačnega trga
  - Zagovarjanje združljivosti
  - Omogočanje inovacij
  - Zagovarjanje preudarne javne politike

"Promocija uporabe najboljših praks za zagotovljanje varnosti znotraj računalništva v oblaku in izobraževanje o uporabi računalništva v oblaku z namenom zaščite vseh ostalih oblik računalništva."

Cloud Security Alliance

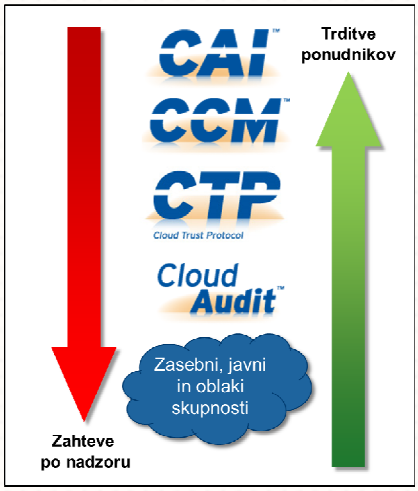
Področja delovanja (v2.1)

Arhitektura oblaka	Upravljanje v oblaku	Delovanje v oblaku
Arhitekturni okvir računalništva v oblaku	Korporativno upravljanje in upravljanje organizacijskih tveganj	Tradicionalna varnost, neprekinjeno poslovanje in okrevanje po katastrofi
	Pravna in elektronska razkritja	Odziv na incidente, obveščanje in odprava
	Skladnost in revizija	Aplikacijska varnost
	Upravljanje življenjskega cikla informacij	Enkripcija in upravljanje s ključi
	Prenosljivost in združljivost	Upravljanje z identitetami in dostopi
		Virtualizacija
		Varnost kot storitev (predlog)

Cloud Security Alliance

GRC knjižnica

- *Družina 4 raziskovalnih projektov*
  - *Cloud Controls Matrix*
  - *Consensus Assessments Initiative*
  - *Cloud Audit*
  - *Cloud Trust Protocol*
- *Orodja za korp. upravljanje ter upravljanje tveganj in skladnosti*
- *Omogoča avtomatizacijo in neprekinjen nadzor GRC*



Cloud Security Alliance

GRC knjižnica

Government	Specs	Extensions	Commercial
??? Deliver "continuous monitoring" required by A&A methodologies	Continuous monitoring ... with a purpose	CTP Cloud Trust Protocol	Common technique and nomenclature to request and receive evidence and affirmation of controls from cloud providers
???	Claims, offers, and the basis for auditing service delivery	Cloud Audit The A6 Working Group	• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
FedRAMP DIACAP Other C&A standards	Pre-audit checklists and questionnaires to inventory controls	CAI Consensus Assessments Initiative	• Industry-accepted ways to document what security controls exist
NIST 800-53, HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPAA, SOX, GLBA, STIG, NIST 800-144, SAS 70, ...	The recommended foundations for controls	CCM Cloud Controls Matrix	• Fundamental security principles in assessing the overall security risk of a cloud provider

Cloud Security Alliance

Primer CAI in CCM – Aplikacijska varnost

Control Area	Control ID	Consensus Assessment Questions (Cloud-Specific Control Assessment)
Security Architecture - Application Security	SA-04	SA-04a - Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc) to "build-in" security for your Systems/Software Development Lifecycle (SDLC)? SA-04b - Do you utilize an automated source-code analysis tool to detect code security defects prior to production? SA-04c - Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?

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
Security Architecture - Application Security	SA-04	Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and comples with applicable regulatory and business requirements.	No Change	X	X	X	X		COBIT 4.1 AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SC-6 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-10 NIST SP800-53 R3 SC-11 NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-14 NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-18	NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SC-6 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-7 (1) NIST SP800-53 R3 SC-7 (2) NIST SP800-53 R3 SC-7 (3) NIST SP800-53 R3 SC-7 (4) NIST SP800-53 R3 SC-7 (5) NIST SP800-53 R3 SC-7 (7) NIST SP800-53 R3 SC-7 (8) NIST SP800-53 R3 SC-7 (12) NIST SP800-53 R3 SC-7 (13)	PCI DSS v2.0

CCSK

Predstavitev

- Prvi certifikat na področju varnosti v oblaku
- Temelji na osnovi dveh gradiv:
  - CSA vodilo
  - ENISA Cloud Computing Risk Assessment
- Dve vrsti delavnic:
  - CCSK Osnovni (1 dan)
  - CCSK Napredni (2 dni)

Cloud Security Alliance

Zaključek

- CSA Application Security Whitepaper:
  - https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide-dom10-v2.10.pdf
- Članstvo v slovenskem odseku
  - Brezplačno
  - Včlanitev preko LinkedIn skupine *Cloud Security Alliance, Slovenia Chapter* (http://goo.gl/t7G25)
- Za vsa morebitna vprašanja in sodelovanje pišite:
  - dsavanovic@cloudsecurityalliance.si

cloud CSA security alliance℠

HVALA