SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Veřejné cloudy z pohledu bezpečnosti

Dominik Pintér

Kentico software s.r.o

Představení

- MCPD .NET 3.5
- ASP.NET – 4 roky
- Windows Azure – 2 roky
- Amazon WS – 0,5 roku
- Bezpečnost – 1,5 roku

Kentico software

- Česká mezinárodní firma
- Kentico CMS for ASP.NET

Agenda

- Veřejné cloudy
  - Z pohledu zákazníka
    - Přehled
    - Správa
    - Jednotlivé služby
  - Z pohledu útočníka
    - Faktory umožňující zneužití
    - Typy útoků

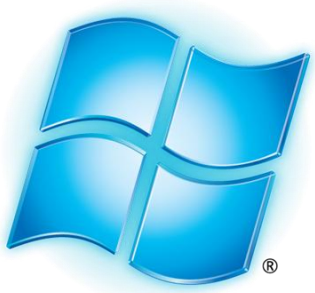
Modelový případ

Cíl: webová aplikace v cloudu

Požadavky:

- Webový server pro běh aplikace
- Úložiště souborů s podporou CDN
- Databázový server

Veřejné cloudy



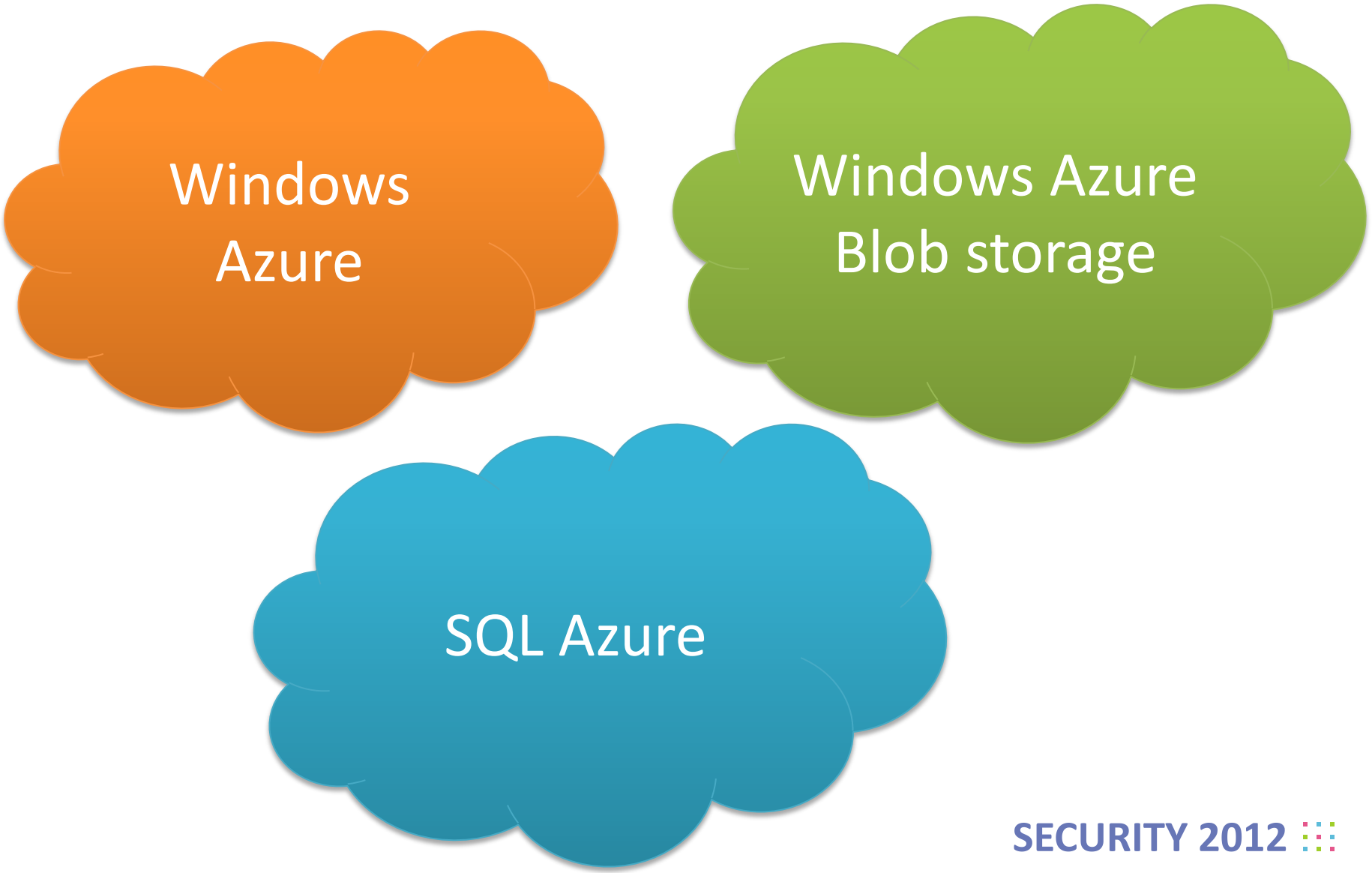
Windows Azure™

amazon web services™

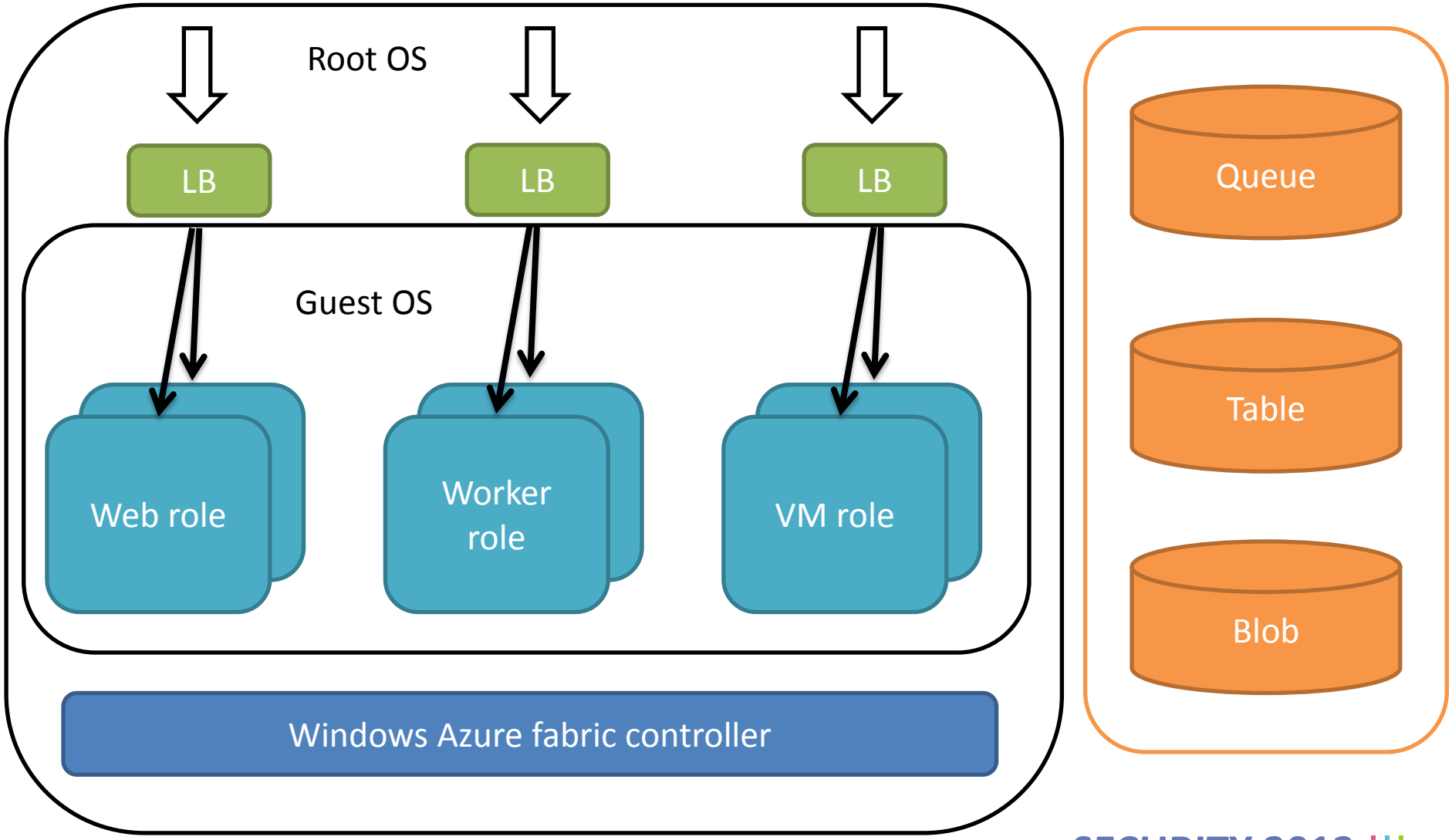
Veřejné cloudy

- Fyzická bezpečnost
  - Velmi omezený přístup osob, Více zdrojů energie
  - Kamery, biometrické systémy, čipové karty, …
  - Windows Azure - MS Global foundation services [1]
- Zkušenosti
  - Microsoft - 18 let zkušeností (MSN, LiveID, Office 365, …)
  - Amazon - Amazon.com, AWS GovCloud
- Průmyslové standarty
  - Windows Azure - ISO 27001, Safe harbor, SAS 70 TYPE I a TYPE II
  - Amazon – ISO 27001, PCI DSS Level 1, FISMA moderate, … [2]
- Platební model „Pay as you go“
- DNS systém
- Přístup z internetu
- Interní komunikace v cloudu

Windows Azure



Windows Azure



Amazon web services

Správa Windows Azure

- Management portál
  - Autentizace pomocí Live ID

    „Windows Live ID is one of the longest-running Internet authentication services available, and thus provides a rigorously tested gatekeeper for Windows Azure.“ [3]
  - Není malých rolí
- Management API
  - Autentizace pomocí self signed private/public klíčů,
  - Registrace klíčů přes portál PKCS#12 (.PFX)
  - Požadavky management API přes SSL
- Speciální konfigurační soubory
  - Nastavování komunikačních bodů

Správa Amazon Web services

- Striktní rozdělení na služby
- Management portál
  - Autentizace pomocí jména a hesla
  - Možnost multifaktorové autentizace [4]
- Management API – komunikace přes HTTP/HTTPS
  - REST
  - SOAP
- Typy – Access credentials, Sign-in credentials, Account identifiers
  - AWS Identity and access management
  - REST, X.509 – SOAP, Pár klíčů – EC2, CloudFront
- Veřejný PGP klíč pro komunikaci
- Penetrační testování
- Reportování bezpečnostních chyb

Výpočetní služba – Windows Azure

- Omezená práva – Windows Azure trust level
- Remote desktop
- Integrovaný firewall – public a internal endpointy
- Web role a Worker role
  - Předkonfigurované
  - Automaticky záplatované
  - Nelze na ně nainstalovat vlastní software (IDS/IPS, Firewall)
- Virtual machine role
  - Deployment jako obraz
  - Musí se manuálně záplatovat
  - Možnost instalace vlastního sw

Výpočetní služba - Amazon EC2

- Virtuální stroje - plný přístup má pouze majitel
- Amazon Machine Image (AMI)
  - Vytváření vlastních obrazů [5]
  - Použití sdílených obrazů
- Vlastní správa
  - Manuální zabezpečení virtuálního stroje
- Integrovaný firewall v „denny all“ módě – není součástí Guest OS

Úložiště – Windows Azure

- Fyzické uložení dat- 3 zálohy v různých nodech
- Logické uložení - blob a container – bez ACL
- Autentizace - 2 druhy klíčů
- Připojení přes SSL
- Public přístup je pouze pro čtení
- Shared access signature – autorizace na úrovní blobu – url obsahuje access token, lze specifikovat čas, práva, …
- Šifrování pomocí .NET Crypthography service providers [6]

Úložiště – Amazon S3

- Autentizace pomocí dvojice key, secret
- Logické uložení - bucket a object
  - ACL pro oba typy objektů
- Neautentizovaný přístup pro čtení/zápis
- Připojení přes SSL
- Před uploadem je doporučené data šifrovat
- Ukládání dat na EC2 – není zalohované, lze šifrovat standartními nástroji OS

SQL Azure

- Bezpečnostní prvky – generovaný DNS název, firewall, zákaz admin jmen pro přístup, připojení přes pouze SSL
- Firewall – nefiltruje IP adresy uvnitř cloudu
- Důvěra SSL certifikátu – Man in the middle
- Nepodporuje transparent data encryption

Amazon RDS

- MySQL nebo Oracle databáze
- Integrovaný firewall (security groups)
- Připojení přes SSL – není vynucené - certifikát automaticky generuje Amazon
  - Dostupné pouze pro MySQL
- Automatické zálohy a updaty

Veřejné cloudy - pro a proti

- Proti:
  - (Zákony, certifikace, firemní politika)
  - IPS/IDS, záplaty
    - Windows Azure - „Hash collision“ útok – veřejně známá chyba od 28.12.2011, záplatované - 1.1.2012
  - Bezpečnostní chyby u cloud providera [7]
- Pro:
  - Fyzická bezpečnost, infrastruktura
  - Méně starostí
  - Certifikace
- Amazon – nastavitelná míra bezpečnosti
- Windows Azure – důvěra v poskytovatele

Možnosti zneužití

- Faktory:
  - Snadný a rychlý přístup
  - Anonymita – kreditní karta a e-mail adresa (live id)
  - Výpočetní síla
  - Větší důvěra uvnitř cloudu
  - Nelze nastavit Firewall/IPS/IDS pro všechny zákazníky optimálně

Možnosti zneužití

- Útoky na jiné cloudové služby
- Provedení útoku z relativně bezpečného prostředí cloudu
- DoS, DDoS – výpočetní síla a síťové připojení
- Spam – Amazon Simple e-mail service
- Crackování hesel – Windows HPC podporuje Windows Azure

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Dominik Pintér
Kentico software s.r.o
dominikp@kentico.com

Reference

[1]http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf

[2]http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf

[3]http://www.globalfoundationservices.com/security/documents/WindowsAzureSecurityOverview1_0Aug2010.pdf

[4]http://aws.amazon.com/mfa/

[5]http://www.trust.informatik.tudarmstadt.de/fileadmin/user_upload/Group_TRUST/PubsPDF/BNPSS11.pdf

[6]http://msdn.microsoft.com/en-us/magazine/ee291586.aspx

[7]https://aws.amazon.com/security/security-bulletins/reported-soap-request-parsing-vulnerabilities-reso/