Deloitte.

Deloitte Advisory s.r.o.
Nile House
Karolinská 654/2
186 00 Praha 8 - Karlín
Česká republika

Tel: +420 246 042 500
Fax: +420 246 042 555
DeloitteCZ@deloitteCE.com
www.deloitte.cz

zapsána Městským soudem
v Praze, oddíl C, vložka 113225
IČO: 27582167
DIČ: CZ27582167

REPORTING.CZ, s.r.o.
Zastoupena Ing. Michalem Rozehnalem
U Elektry 203/8
198 00 Praha 9 – Hloubětín
Česká republika

18. 6. 2015

Závěrečné prohlášení

Věc: Závěry z provedení posouzení bezpečnosti aplikace Reporting.cz

Společnost Deloitte Advisory s.r.o. (dále jen „Deloitte") v souladu se smlouvou o poskytování služeb provedla v období dubna 2015 až června 2015 posouzení zabezpečení aplikace Reporting.cz provozované společností REPORTING.CZ, s.r.o. (dále jen „REPORTING.CZ").

Posouzení zabezpečení zahrnovalo zejména následující oblasti:

- Posouzení zabezpečení aplikační vrstvy Reporting.cz, které zahrnovalo posouzení autentizačních mechanismů, řízení přístupu k aplikaci a logování činností uživatelů.
- Revize komponent IT infrastruktury - posouzení konfigurace řešení na úrovni síťové infrastruktury, firewallu, operačních a databázových systémů a aplikačního serveru.
- Posouzení fyzického a environmentálního zabezpečení serverů a technického vybavení, které je hostováno v datovém centru ve Stodu u Plzně.
- Posouzení zabezpečení rozhraní aplikace, včetně posouzení zachování důvěrnosti a integrity přenášených dat od klientů.
- Posouzení úrovně správy IT systémů — posouzení úrovně procesů provozního a bezpečnostního monitoringu, zálohování, řízení přístupů, změnového řízení, vztahů s externími dodavateli a plánování kontinuity podnikání a havarijního plánování.
- Posouzení smlouvy o správě a provozu virtuálních a fyzických serverů, která je uzavřena mezi REPORTING.CZ a společností Bluepeople s.r.o.
- Posouzení interní řídící dokumentace týkající se interních IT procesů a poskytnutí návrhů na zlepšení.

Na základě zjištění v rámci posouzení bezpečnosti aplikace Reporting.cz ve výše uvedeném rozsahu byly společnosti REPORTING.CZ doporučeny úpravy týkající se zvýšení celkové úrovně bezpečnosti aplikace, související technické infrastruktury a jednotlivých procesů souvisejících se zabezpečením provozu a správy aplikace. Pro všechny zásadní doporučení byl společností REPORTING.CZ stanoven implementační plán, kterým bude zajištěno odstranění většiny identifikovaných rizik. Detaily zjištění a doporučení jsou uvedeny v závěrečné zprávě „Posouzení zabezpečení aplikace Reporting.cz", která může být jakýmkoliv třetím osobám předložena, a to pouze po předchozím písemném souhlasu společnosti Deloitte.

Naše služby nepředstavovaly účetní audit, sběr dat, prověrku ani služby zaměřené na poskytnutí ujištění o dodržení příslušných požadavků dle popisu ve vyjádřeních k odborným standardům vydaným institutem AICPA, a ve spojitosti s účetní závěrkou REPORTING.CZ či jeho systémem interních kontrol, tudíž nevydáváme výrok ani neposkytujeme žádnou jinou formu ujištění. Společnost Deloitte neprováděla žádné činnosti spojené s výkonem řídicích funkcí, nepřijímala manažerská rozhodnutí ani nepůsobila na postu zaměstnance REPORTING.CZ. Naše zpráva a závěry vycházejí z části z informací, které nám poskytl REPORTING.CZ, a naše společnost nepřebírá žádnou odpovědnost za úplnost a správnost těchto informací.

S pozdravem

Ing. Zdeněk Křížek
Partner, oddělení Poradenských služeb

Deloitte Advisory s.r.o.
Karolinská 654/2
186 00 Praha 8

ŘÍZENÍ RIZIK

1. DOSTUPNOST

1.1. Umístění
- a. Provoz zajištěn z technologie umístěné ve dvou nezávislých lokalitách;
- b. Sekundární technologie plně nahrazuje primární v případě jeho nedostupnosti;

Dopad rizika nedostupnosti – vysoký
Pravděpodobnost rizika – nízká

1.2. Připojení k internetu
- a. primární i sekundární lokalita je připojena 3 nezávislými přípojkami do internetu;
- b. V případě výpadku jednoho ze spojení, je využita další, technologicky rozdílné připojení (optické, bezdrátové, kabelové);

Dopad rizika nedostupnosti – vysoký
Pravděpodobnost rizika – nízká

1.3. Napájení
- a. Elektrické napájení je plně zálohováno;
- b. V případě výpadku elektrického proudu je využito náhradní zdroj energie z baterie a generátoru s trvalou dodávkou paliva;

Dopad rizika nedostupnosti – střední
Pravděpodobnost rizika – nízká

1.4. Data
- a. Data jsou zálohována mimo fyzické umístění primární i sekundární technologie;
- b. V případě nedostupnosti lze data obnovit z kompletní maximálně 1 den staré zálohy;

Dopad rizika nedostupnosti – nízký
Pravděpodobnost rizika – nízká

1.5. Služba
- a. Provoz aplikace je umožněn z obou lokalit;
- b. V případě nedostupnosti, je služba obnovená na sekundární technologie do 1 hodiny;

Dopad rizika nedostupnosti – nízký
Pravděpodobnost rizika – nízká

1.6. Chlazení
- a. Technologie je chlazena aktivně klimatizací a vhodnou stavební dispozicí pasivně;
- b. V případě nedostupnosti aktivního chlazení, pasivní plně pokryje potřeby chlazení;

Dopad rizika nedostupnosti – nízký
Pravděpodobnost rizika – nízká

RISK MANAGEMENT

1. AVAILABILITY

1.1. Location:
- a. The operation is ensured with technology located at two independent location;
- b. Secondary technology is fully able replace primary while it is unavailable;

Level of risk - High
Probability of risk - Low

1.2. Internet connection
- a. Primary and secondary location is connected via 3 independent connection to internet;
- b. In case of failure, the others technologically independent connection is used (optical, wireless, cable);

Level of risk – High
Probability of risk – Low

1.3. Power Supply
- a. Electrical power is fully backup;
- b. In case of failure of primary electrical source, there are available batteries and diesel generator with continuous supply of fuel;

Level of risk – Middle
Probability of risk – Low

1.4. Data
- a. Data are backup to two physical locations which are out of primary or secondary site;
- b. In case of unavailability all data shall be recovered from backup one day old;

Level of risk – Low
Probability of risk – Low

1.5. Service
- a. Application can be served from 2 locations;
- b. In case of unavailability, service can be restored at second site during 1 hour;

Level of risk – Low
Probability of risk – Low

1.6. Air condition
- a. Technology is cooled by air condition as well as passively by building disposition;
- b. In case of failure of air condition, building disposition fully cover all cooling needs;

Level of risk – Low
Probability of risk – Low

2. BEZPEČNOST

2.1. Fyzický přístup
a. Technologie je fyzický zabezpečená proti přístupu 3. osob;
b. Každá lokalita je monitorována kamerovým systémem a alarmem;

Dopad rizika - vysoký
Pravděpodobnost rizika – nízká

2.2. Osoby
a. Přístup k technologiím je omezen pouze na vybrané osoby poskytovatele hostingových služeb;
b. Všechny vybrané osoby jsou občany ČR, s čistým trestním rejstříkem a jejich zodpovědnost je smluvně vázána;

Dopad rizika - střední
Pravděpodobnost rizika – nízká

2.3. Administrativní přístup
a. Administrativní přístup k serverům je omezen na vybrané osoby poskytovatele hostingových služeb a osoby poskytovatele služby Reporting.cz;
b. Přístup na servery je monitorován, historie aktivit logována, úroveň práv je omezena na vybrané úkony dle zodpovědnosti dané osoby;

Dopad rizika - střední
Pravděpodobnost rizika – nízká

2.4. Připojení
a. Připojení je na server a na poskytované služby je šifrováno;
b. Přenos dat je zabezpečen SSL certifikátem, všechna spojení jsou šifrována pomocí SSL či VPN IPsec, přihlášení je možné nezávisle ověřovat emailem;

Dopad rizika - střední
Pravděpodobnost rizika – nízká

2.5. Zálohování
a. Bezpečnost záloh je řízena umístněním a šifrováním;
b. Data jsou lokálně šifrována symetrickým klíčem AES-256 a následně zabezpečeným SSL spojením přenesena do datového uložiště, přístup do uložiště je omezen dle bodu c). Uložiště záloh je pod kontrolou poskytovatele služby Reporting.cz;

Dopad rizika - střední
Pravděpodobnost rizika – nízká

2. SECURITY

2.1. Physical access
a. Technology is physically secured in order to avoid access by 3rd party;
b. Each location is monitored by camera as well as by alarm;

Level of risk – High
Probability of risk – Low

2.2. Osoby
a. Access at the site is limited only to selected employees of the partner responsible for hosting;
b. All selected employees are citizens of CR with clean criminal record and their responsibility is covered by agreement;

Level of risk – Middle
Probability of risk – Low

2.3. Administration
a. Administration access to the server is limited to selected employees of hosting partner and employees of service provider Reporting.cz;

b. Access is monitored, history of activities is logged, level of access is individually setup according to responsibilities for maintain and support of service;

Level of risk – Middle
Probability of risk – Low

2.4. Připojení
a. Connection to server and to all services is encrypted;
b. Data transfer is secure by SSL certificate, all connections are encrypted by SSL or VPN IPsec, login to service can be independently verified via e-mail;

Level of risk – Middle
Probability of risk – Low

2.5. Zálohování
a. Security of backup is managed by physical location and encryption;
b. Data are locally encrypted by symmetrical key AES-256 and then transfer to storage via encrypted connection, access to backup storage is limited as paragraph c). Storage is under responsibility and control of service provider Reporting.cz

Level of risk – Middle
Probability of risk – Low

2.6. Data
a. Přístup k datům je omezen;
b. Přístup k datům je omezen dle bodu b) a c), data jsou anonymizována dle klíčů v maximální možné míře už na úrovni aplikace;

Dopad rizika - nízký
Pravděpodobnost rizika – nízká

2.7. Bezpečnosti OS
a. Bezpečnost operačního systému vychází z nejnovějších bezpečnostních standardů;
b. Systém je chráněn službou ESET EndPoint Security a firewally ZyXEL USG (certifikace ICSA);

Dopad rizika - nízký
Pravděpodobnost rizika – nízká

2.8. Přístup třetích osob
a. Veškerá technologie, data, zálohy a interní i externí služby jsou umístěny v neveřejných prostorech na území České Republiky;
b. Přístup je striktně omezen pouze na povinnosti vyplývajících ze zákonů ČR;

Dopad rizika - nízký
Pravděpodobnost rizika – nízká

2.9. Komunikace - emaily
a. Emaily jsou hostovány na vlastním firemním MS Exchange serveru;
b. Data a komunikace jsou uloženy privátním, nesdíleném a neveřejném poštovním serveru, sdílení jakékoliv komunikace je striktně omezeno pouze na povinnosti vyplývajících ze zákonů ČR;

Dopad rizika - nízký
Pravděpodobnost rizika – nízká

2.6. Data
a. Data access is limited;
b. Data access is limited according paragraph b) and c), data are got anonymous by keys at the maximum possible level in the application;

Level of risk – Low
Probability of risk – Low

2.7. Security of OS
a. Security of operation system is aligned with the newest security standards
b. System is secure by service ESET EndPoint Security and firewalls ZyCEL USG (Certificated by ICSA)

Level of risk – Low
Probability of risk – Low

2.8. 3rd party access
a. All technology, data, backup and internal as well as external services are located at the private location in the Czech Republic;
b. Access is strictly limited according obligation by law of CR;

Level of risk – Low
Probability of risk – Low

2.9. Communication – e-mails
a. E-Mails are hosted on the private MS Exchange server;
b. Data and communication is stored on private, unshared, non-public email server, share of any communication is strictly limited according obligation by law of CR;

Level of risk – Low
Probability of risk – Low