**Testy ASV – podmienky služby**

**Časť I. Podmienky prevádzky služby**

Služby QualysGuard

Služba QualysGuard Service umožňuje zákazníkovi automatizovať proces riadenia bezpečnosti a riadenia IT vrátane zisťovania sietí, mapovania a prioritizácie prostriedkov IT; vyhodnocovanie zraniteľnosti sietí a webových aplikácií, posudzovanie zhody politík; správa úloh pre nápravu. Služba QualysGuard je produkt tretích strán, ktorý zákazníkovi dodáva spoločnosť Diebold Nixdorf na základe licencie spoločnosti Qualys, Inc. Služba QualysGuard neposkytuje servis, údržbu ani opravy pre žiadny alebo skutočný alebo osobný majetok.

Niektoré prvky služby QualysGuard vyžadujú sieťové skenovanie. Sieťové skenovanie pre externé IP adresy prebieha pomocou vzdialených skenerov z centra SOC (Security Operation Centre). Sieťové skeny budú vykonané na definovaných IP adresách.

Platforma QualysGuard. Platforma QualysGuard využíva modul dodávania softvéru ako služby. Platforma QualysGuard sa skladá z nasledujúcich komponentov: webový portál, SOC a databáza znalostí o zraniteľnostiach.

1.2.1 Webový portál

 Webový portál umožňuje zákazníkovi spravovať IP adresy, ktoré boli preňho do systému zadané. Zákazník môže prostredníctvom portálu nakonfigurovať vykonávanie sieťových skenov, nastaviť profily možností sieťových preverovaní, šablón správ, zoznamy vyhľadávania, zásady zhody, ovládacie prvky IT a nastavenie pracovných postupov. Hneď ako sú dokončené sieťové skeny, je možné v rámci webového portálu vizualizovať správy výsledkov sieťových skenov. V rámci zobrazovaných zostáv je možné si nechať zobraziť preddefinované výsledky: napríklad dátum, názov aplikácie pod danou IP adresou, opis nájdenej zraniteľnosti a úroveň závažnosti. Reporty zraniteľností je možné zobraziť ako zoznam alebo v grafickom formáte a nadefinovať s ohľadom na mieru podrobnosti, t. j. technickejšie pre správcu systému a prehľadnejšia úroveň pre manažment. V rámci vizualizácií je možné zobraziť aj trendové informácie za určité časové obdobie.

Iba používatelia autorizovaní zákazníkom s aktívnym prihlasovacím poverením môžu pristupovať k webovému portálu. Každý zákazník musí poskytnúť informácie o jednej osobe, ktorá bude pôsobiť ako primárny kontakt pre daného zákazníka. Je možné nastaviť oprávnenie na prístup do webového portálu pre ďalších autorizovaných používateľov. Webový portál umožňuje prideľovanie používateľských oprávnení založených na rolách.

1.2.2 SOC (Security Operation Centre)

Sú dátové centrá s technológiou a infraštruktúrou na prevádzkovanie platformy QualysGuard. Infraštruktúra SOC sa používa na ukladanie a spracovanie dát zákazníkov, rovnako ako na hosťovanie znalostnej bázy zraniteľností a na prevádzku vzdialených skenerov vykonávajúcich skeny prostredníctvom internetu.

1.2.3 Databáza zraniteľností (Vulnerability KnowledgeBase)

 Databáza zraniteľností obsahuje znalosti týkajúce sa zraniteľností, ktoré sa vyskytujú v rámci sietí, a nástroje a postupy ako tieto zraniteľnosti odhaliť v rámci sieťových skenov. Databáza zraniteľností sa využíva na identifikáciu IT komponentov, zraniteľností IP adries a webových aplikácií, služieb TCP/IP a operačných systémov. Databáza zraniteľnosti sa z času na čas aktualizuje signatúrami pre nové chyby zabezpečenia, overené opravy, opravy false positive nálezov a ďalšie dáta protokolu TCP/IP.

2. Opis modulu QualysGuard PCI

Modul Compliance Module QualysGuard PCI (Modul PCI) umožňuje zákazníkovi vykonávať sieťové kontroly s cieľom zistiť informácie o konfigurácii operačného systému a informácie o riadení prístupu k aplikáciám. Modul PCI používa tieto informácie na hlásenie miery súladu s PCI DSS. Modul PCI bol schválený Radou pre bezpečnostné štandardy PCI (PCI Security Standards Council), aby sa mohol využiť ako schválený dodávateľ skenovania (Approved Scanning Vendor) pre posúdenie súladu so štandardom PCI DSS. Modul PCI poskytuje zákazníkom tipy na dodržiavanie predpisov, detailné manuály ako postupovať v rámci procesu dodržiavania predpisov PCI DSS. Modul PCI je prístupný prostredníctvom portálu PCI a spĺňa podmienky uvedené v rámci tohto portálu. Modul PCI je prístupný z internetu prostredníctvom portálu PCI.

Modul PCI má nasledujúce funkcie:

* Modul PCI je použiteľný na externé sieťové skeny.
* Sieťové skeny môžu byť naplánované tak, aby sa vykonávali automaticky opakovane.
* Jednotlivé testy v rámci sieťových skenov používajú znalostnú databázu na zistenie zraniteľnosti.
* Logy aktivít zobrazujú činnosti používateľa a systému.
* V rámci skenovania zraniteľností je zahrnutá aj funkcia vyhľadávania IT komponentov.
* Modul PCI umožňuje zákazníkovi automaticky odoslať stav skenov ASV a ich súladu s PCI priamo na acquiringovú banku.

**Časť II: Podmienky poskytovania služieb**

Minimálne obdobie využívania služby a ukončenie služieb.

1. Služba je poskytovaná na dobu neurčitú s 3-mesačnou výpovednou lehotou.
	1. Dátum aktivácie služby. Po objednaní služby QualysGuard odberateľom dostane zákazník e-mail od zamestnanca spoločnosti Diebold Nixdorf, ktorý zákazníkovi oznámi, že služba QualysGuard je pripravená na prevádzku. E-mail bude obsahovať uvítací list s prihlasovacím menom a heslom zákazníka QualysGuard. Dátum tohto e-mailu je dátum aktivácie služby.
	2. Ukončenie. Zákazník môže zmluvu ukončiť doručením výpovede. Služba bude ukončená do konca tretieho mesiaca po doručení výpovede.
2. Meno používateľa a heslo. Zákazník je zodpovedný za dôverné uchovanie svojho mena používateľa a hesla a ochranu prihlasovacích údajov používateľov. Zákazník musí okamžite informovať spoločnosť Qualys (support@qualys.com) o tom, že sa dozvie o neoprávnenom použití svojich prihlasovacích údajov. V takom prípade Qualys deaktivuje kompromitované prihlasovacie údaje a vydá nové prihlasovacie údaje. Zákazník zodpovedá za všetky aktivity a náklady, ktoré vzniknú pri používaní kompromitovaných prihlasovacích údajov, pokým nebudú kompromitované prihlasovacie údaje deaktivované.
3. Licenčné podmienky a obmedzenia
	1. Zákazníkovi je udelená neprevoditeľná, nevýhradná licencia na používanie integrovaného softvéru a webového portálu iba v súvislosti s použitím služby QualysGuard od zákazníka. Ak zákazník inak nepovoľuje, zákazník chápe a súhlasí s tým, že nie je povolené distribuovať ďalej dodaný softvér v žiadnej podobe alebo používať dodaný softvér inak než prostredníctvom portálu. Zákazník súhlasí s tým, že nesmie a neumožňuje žiadnej tretej strane, aby sa pokúšala z akéhokoľvek dôvodu spätne rekonštruovať vývoj, dekompiláciu alebo dekompozíciu dodaného softvéru, s výnimkou prípadov, keď to výslovne povoľuje príslušné právo bez ohľadu na obmedzenia v týchto podmienkach poskytovania služieb alebo je to povolené podľa licenčných podmienok (napr. licenčné podmienky pre Open Source).
	2. Niektoré komponenty dodaného softvéru podliehajú GNU General Public License, verzii 2 (ďalej len GPL) a tieto komponenty sa tu označujú ako „softvér Open Source“. Zákazník je oprávnený používať, upravovať a distribuovať softvér Open Source, ktorý je v súlade s GPL, ak zákazník spĺňa podmienky GPL (k dispozícii na adrese http://www.gnu.org/copyleft/gpl.html#SEC1).
	3. Zákazník súhlasí, že jeho práva zmluvne poskytnuté podliehajú nižšie uvedeným obmedzeniam:

(a) Zákazník môže používať službu QualysGuard

1. iba na skenovanie IP adries a/alebo mapovanie názvov domén vlastnených a registrovaných zákazníkovi, alebo na ktoré má zákazník úplné právo, moc a právomoc súhlasiť s tým, aby mal

QualysGuard Service sken a/alebo mapu a

1. iba do počtu IP adries alebo počtu skenovaní, ktoré sú zahrnuté v rámci služby zákazníkovi.

(b) Zákazník musí pomocou webového portálu informovať spoločnosť Qualys o všetkých zmenách v IP adresách alebo názvoch domén, ktoré sa majú skenovať. Navýšenie počtu IP adries môže predstavovať nutnosť zaplatiť dodatočné poplatky za služby. Zákazník berie na vedomie, že služba QualysGuard je poskytovaná v súvislosti s PCI DSS vrátane prípadných prispôsobených prehľadov a individualizovanej pomoci iba ako nástroj umožňujúci zákazníkovi vyhodnotiť jeho zhodu s PCI DSS. Pravidlá súladu s PCI DSS nie sú definované acquirerskou bankou ani spoločnosťami Qualys a Diebold Nixdorf. Kartové asociácie a ďalšie subjekty združené v rámci Rady pre bezpečnostné štandardy PCI stanovujú bezpečnostné kritériá a ďalšie podmienky zhody s PCI DSS. Zákazník berie na vedomie, že spoločnosť Qualys môže zverejniť správu týkajúcu sa zhody s PCI DSS s acquirerskou bankou, spoločnosťou Diebold Nixdorf a s organizáciou PCI Security Standards Council, LLC alebo obdobnými subjektmi.

1. Definované IP adresy.

Vzhľadom na citlivú povahu vykonávania bezpečnostných skenov na IP adresách zákazník objednaním služby potvrdzuje, že má právomoc povoliť službe QualysGuard, aby boli otestované zraniteľné miesta (sken) definovaných IP adries alebo domén určených na skenovanie. Sken prebieha elektronicky a môže byť vykonaný po prvotnom objednaní služby alebo neskôr. Zákazník týmto súhlasí so skenovaním IP adries a domén z tretích krajín (vrátane prenosov vnútri skupiny a prevodov subjektom v krajinách, ktoré neposkytujú zákonnú ochranu osobných údajov) na účel použitia alebo spracovania podľa podmienok zmluvy. Zákazník taktiež berie na vedomie a súhlasí s tým, že skenovanie IP adries a/alebo domén môže ohroziť zraniteľné miesta a za určitých okolností môže mať za následok aj narušenie služieb na skenovaných stránkach. Zákazník berie na vedomie a prijíma riziká spojené so službou QualysGuard, ktorá zahŕňa skenovanie, a podpisom objednávky autorizuje výkon služby QualysGuard. Zákazník súhlasí s tým, že je jeho povinnosťou zazálohovať všetky dáta obsiahnuté v zariadeniach pripojených k IP adresám zákazníka a/alebo doménam, ktoré sú určené na skeny, a to pred tým, ako sa začne služba QualysGuard používať. Zákazník súhlasí s tým, že spoločnosť Global Payments a jej pridružené spoločnosti a subdodávatelia sú vyňatí zo zodpovednosti za škody, ktoré môžu vzniknúť v súvislosti s vykonávaním skenov. V prípade dátového úniku u zákazníka aj napriek dosiahnutiu zhody v rámci služby ASV skenu, neprijíma spoločnosť Global Payments zodpovednosť za tento dátový únik a prípadné pokuty s tým súvisiace

1. Dôvernosť

Všetky dáta týkajúce sa IP adries zákazníkov, domén alebo charakteristík siete (vrátane údajov získaných v súvislosti s poskytovaním služby QualysGuard podľa tejto zmluvy) sa považujú za dôverné informácie zákazníka a všetky dáta a informácie obsiahnuté v rámci služby QualysGuard vrátane informácií týkajúcich sa sieťových prvkov bude spoločnosť Global Payments a všetci jej subdodávatelia považovať za dôverné informácie. Bez ohľadu na vyššie uvedené zákazník súhlasí s tým, že niektoré informácie generované v súvislosti s testami zraniteľnosti je možné použiť v agregovanej, anonymizovanej podobe na sledovanie trendov zraniteľností. Údaje v „agregovanom, anonymizovanom tvare“ predstavujú všeobecné dáta, ktoré nezahŕňajú informácie týkajúce sa konkrétneho zákazníka, žiadne špecifické informácie o adresovaní alebo nastavení siete Zákazníka vrátane informácií o mene zákazníka, týkajúcich sa mena Zákazníka alebo spoločnosti Global Payments, trhovej vertikály, na ktorej Zákazník pôsobí, špecifických IP adries, názvov sieťových prvkov, podsietí, MAC adries, identifikátorov obvodov alebo akéhokoľvek iného sieťového komponentu špecifického pre zákazníkov alebo dát špecifických pre používateľa.