ASV testy - podmínky služby

Část I. Podmínky provozu služby

Služby QualysGuard

Služba QualysGuard Service umožňuje zákazníkovi automatizovat proces řízení bezpečnosti a řízení IT, včetně zjišťování sítí, mapování a prioritizace IT prostředků IT; vyhodnocování zranitelnosti sítí a webových aplikací, posuzování shody politik; správa úloh pro nápravu. Služba QualysGuard je produkt třetích stran, který je zákazníkovi dodáván společností Diebold Nixdorf na základě licence společnosti Qualys, Inc. Služba QualysGuard neposkytuje servis, údržbu ani opravy pro žádný nebo skutečný nebo osobní majetek.

Některé prvky služby QualysGuard vyžadují síťové skenování. Síťové skenování pro externí adresy IP se provádí pomocí vzdálených skenerů z centra SOC (Security Operation Centre). Síťové skeny budou provedeny na definovaných IP adresách.

Platforma QualysGuard. Platforma QualysGuard využívá modul dodávání softwaru jako služby. Platforma QualysGuard se skládá z následujících komponent: webový portál, SOC a databáze znalostí o zranitelnostech.

1.2.1 Webový portál

Webový portál umožňuje zákazníkovi spravovat IP adresy, které byly pro něj do systému zadány. Zákazník může prostřednictvím portálu nakonfigurovat provádění síťových skenů, nastavit profily možností síťových prověřování, šablon zpráv, seznamy vyhledávání, zásady shody, ovládací prvky IT a nastavení pracovních postupů. Jakmile jsou dokončeny síťové skeny, je možné v rámci webového portálu vizualizovat zprávy výsledků síťových skenů. V rámci zobrazovaných sestav je možné si nechat zobrazit předdefinované výsledky: například datum, název aplikace pod danou IP adresou, popis nalezené zranitelnosti a úroveň závažnosti. Reporty zranitelností mohou být zobrazeny jako seznamu nebo v grafickém formátu a mohou být nadefinovány s ohledem na míru podrobnosti, tj. techničtější pro správce systému a přehlednější úroveň pro management. V rámci vizualizací je možné zobrazit i trendové informace za určité časové období.

Pouze uživatelé autorizovaní zákazníkem s aktivním přihlašovacím pověřením mohou přistupovat k webovému portálu. Každý zákazník musí poskytnout informace o jedné osobě, která bude působit jako primární kontakt pro daného zákazníka. Je možné nastavit oprávnění

pro přístup do WEBového portálu pro další autorizované uživatele. Webový portál umožňuje přidělování uživatelských oprávnění založených na rolích.

1.2.2 SOC (Security Operation Centre)

Jsou datová centra s technologií a infrastrukturou pro provozování platformy QualysGuard. Infrastruktura SOC se používá pro ukládání a zpracování dat zákazníků, stejně jako pro hostování znalostní báze zranitelností a pro provoz vzdálených skenerů provádějících skeny prostřednictvím internetu.

1.2.3 Databáze zranitelností (Vulnerability KnowledgeBase)

Databáze zranitelností obsahuje znalosti ohledně zranitelností, které se vyskytují v rámci sítí a nástroje a postupy jak tyto zranitelnosti odhalit v rámci síťových skenů. Databáze zranitelností je využívána k identifikaci IT komponent, zranitelností IP adres a webových aplikací, služeb TCP / IP a operačních systémů. Databáze zranitelnosti se čas od času aktualizuje signaturami pro nové chyby zabezpečení, ověřené opravy, opravy false positive nálezů a další data protokolu TCP / IP.

2. Popis modulu QualysGuard PCI

Modul Compliance Module QualysGuard PCI ("Modul PCI") umožňuje zákazníkovi provádět síťové kontroly pro zjištění informací o konfiguraci operačního systému a informací o řízení přístupu k aplikacím. Modul PCI používá tyto informace k hlášení míry souladu s PCI DSS. Modul PCI byl schválen Radou pro bezpečnostní standardy PCI (PCI Security Standards Council), aby mohl být využít jako schválený dodavatel skenování (approved Scanning Vendor) pro posouzení souladu s PCI DSS standardem. Modul PCI poskytuje zákazníkům tipy na dodržování předpisů detailní manuály jak postupovat v rámci procesu dodržování předpisů PCI DSS. Modul PCI je přístupný prostřednictvím portálu PCI a splňuje podmínky uvedené v rámci tohoto portálu. Modul PCI je přístupný z internetu prostřednictvím PCI portálu.
Modul PCI má následující funkce:

- Modul PCI je použitelný pro externí síťové skeny.
- Síťové skeny mohou být naplánovány tak, aby se prováděly automaticky opakovaně.
- Jednotlivé testy v rámci síťových skenů používají znalostní databázi pro zjištění zranitelnosti.
- Logy aktivit ukazují činnosti uživatele a systému.
- V rámci skenování zranitelností je rovněž zahrnuta funkce vyhledávání IT komponent.
- Modul PCI umožňuje Zákazníkovi automaticky odeslat stav ASV skenů a jejich souladu s PCI přímo na acquiringovou banku.

Část II: Podmínky poskytování služeb

Minimální doba užívání služby a ukončení služeb.

1. Služba je poskytována na dobu neurčitou s 3 měsíční výpovědní lhůtou.
    1.1 Datum aktivace služby. Po objednání služby QualysGuard odběratelem obdrží zákazník email od zaměstnance Diebold Nixdorf, který zákazníkovi oznámí, že služba QualysGuard je připravena k provozu. E-mail bude obsahovat uvítací dopis s přihlašovatelem a heslem zákazníka QualysGuard. Datum tohoto e-mailu je datum aktivace služby.
    1.2 Ukončení. Zákazník může smlouvu ukončit doručením výpovědi. Služba bude ukončena do konce třetího měsíce po doručení výpovědi.

2. Uživatelské jméno a heslo. Zákazník je zodpovědný za důvěrné uchování svého uživatelského jména a hesla a ochranu přihlašovacích údajů uživatelů. Zákazník musí okamžitě informovat společnost Qualys (support@qualys.com) o tom, že se dozví o neoprávněném použití přihlašovacích údajů. V takovém případě Qualys deaktivuje kompromitované přihlašovací údaje a vydá nové přihlašovací údaje. Zákazník zodpovídá za veškeré aktivity a náklady, které vzniknou při používání kompromitovaných přihlašovacích údajů, dokud nebudou kompromitované přihlašovací údaje deaktivovány.

3. Licenční podmínky a omezení.
    3.1 Zákazníkovi je udělena nepřevoditelná, nevýhradní licence na používání integrovaného softwaru a webového portálu pouze v souvislosti s použitím služby QualysGuard od zákazníka. Pokud zákazník jinak nepovoluje, zákazník chápe a souhlasí s tím, že není povoleno distribuovat dále dodaný software v žádné podobě nebo používat dodaný software jinak než prostřednictvím portálu. Zákazník souhlasí s tím, že nesmí a neumožňuje žádné třetí straně, aby se pokoušela z jakéhokoli důvodu zpětně rekonstruovat vývoj, dekompilaci nebo dekompozici dodaného softwaru, s výjimkou případů, kdy to výslovně povoluje příslušné právo bez ohledu na omezení v těchto podmínkách poskytování služeb nebo je to povoleno podle licenčních podmínek (např. licenční podmínky pro Open Source).
    3.2 Některé komponenty dodaného software podléhají GNU General Public License verze 2 (dále jen "GPL") a tyto komponenty se zde označují jako "Open Source Software". Zákazník je oprávněn používat, upravovat a distribuovat Open Source Software, který je v souladu s GPL, pokud zákazník splňuje podmínky GPL (k dispozici na adrese http://www.gnu.org/copyleft/gpl.html#SEC1).
    3.3 Zákazník souhlasí, že jeho práva smluvně poskytnutá podléhají níže uvedeným omezením:

(a) Zákazník může používat službu QualysGuard

(i) pouze pro skenování IP adres a / nebo mapování názvů domén vlastněná a registrovaná zákazníkovi, nebo pro kterou má zákazník úplné právo, moc a pravomoc souhlasit s tím, aby měl

QualysGuard Service scan a / nebo mapu a
(ii) pouze do počtu IP adres nebo počtu skenování, které jsou zahrnuty v rámci služby zákazníkovi.

(b) Zákazník musí informovat společnost Qualys s použitím webového portálu o všech změnách v IP adresách nebo názvech domén, které mají být skenovány. Navýšení počtu IP adres může představovat nutnost zaplacení dodatečných poplatků za služby. Zákazník bere na vědomí, že služba QualysGuard je poskytována v souvislosti s PCI DSS včetně případných přizpůsobených přehledů a individualizované pomoci pouze jako nástroj umožňující zákazníkovi vyhodnotit jeho shodu s PCI DSS. Pravidla souladu s PCI DSS nejsou definována acquirerskou bankou ani společnostmi Qualys a Diebold Nixdorf. Karetní asociace a další subjekty sdružené v rámci Rady pro bezpečnostní standardy PCI stanoví bezpečnostní kritéria a další podmínky shody s PCI DSS. Zákazník bere na vědomí, že společnost Qualys může zveřejnit zprávu týkající se shody s PCI DSS s acquirerskou bankou, společností Diebold Nixdorf a s organizací PCI Security Standards Council, LLC nebo obdobnými subjekty.

4. Definované IP adresy.

Vzhledem k citlivé povaze provádění bezpečnostních skenů na IP adresách zákazník objednáním služby potvrzuje, že má pravomoc povolit službě QualysGuard, aby byla otestována zranitelná místa ("scan") definovaných IP adres nebo domén určených pro skenování. Sken je prováděn elektronicky a může být proveden po prvotním objednání služby nebo později. Zákazník tímto souhlasí se skenováním IP adres a domén z třetích zemí (včetně přenosů uvnitř skupiny a převody subjektům v zemích, které neposkytují zákonné ochrany osobních údajů) za účelem použití nebo zpracování podle podmínek smlouvy. Zákazník také bere na vědomí a souhlasí s tím, že skenování IP adres a/nebo domén může ohrozit zranitelná místa a za určitých okolností může mít za následek i narušení služeb na skenovaných stránkách. Zákazník bere na vědomí a přijímá rizika spojená se službou QualysGuard, která zahrnuje skenování a podpisem objednávky autorizuje výkon služby QualysGuard. Zákazník souhlasí s tím, že je jeho povinností provést zálohování všech dat obsažených v zařízeních připojených k IP adresám zákazníka a/nebo doménám, které jsou určeny pro skeny a to předtím, než začne být služba QualysGuard používána. Zákazník souhlasí s tím, že společnost Global Payments a její přidružené společnosti a subdodavatelé jsou vyjmuti ze zodpovědnosti za škody, které mohou vzniknout v souvislosti s prováděním skenů. V případě datového úniku u zákazníka i přes dosažení shody v rámci služby ASV skenu, nepřijímá společnost Global Payments odpovědnost za tento datový únik a případné pokuty s tím související.

5. Důvěrnost

Veškerá data týkající se IP adres zákazníků, domén nebo charakteristik sítě (včetně údajů získaných v důsledku poskytnutí služby QualysGuard podle této smlouvy) se považují za důvěrné informace zákazníka a veškerá data a informace obsažené v rámci služby QualysGuard

včetně informací týkajících se síťových prvků budou považovány za důvěrné informace společností Global Payments a všemi jejími subdodavateli. Bez ohledu na výše uvedené, zákazník souhlasí s tím, že některé informace generované v souvislosti s testy zranitelnosti mohou být použity v agregované, anonymizované podobě pro sledování trendů zranitelností. Údaje v "agregovaném, anonymizovaném tvaru" představují všeobecná data, která nezahrnují informace týkající se konkrétního zákazníka, žádné specifické informace o adresaci nebo nastavení sítě Zákazníka včetně informací o jménu zákazníka, týkajících se jména Zákazníka nebo společnosti Global Paments, tržní vertikály, na které Zákazník působí, specifické IP adresy, názvy síťových prvků, podsítě, MAC adresy, identifikátory obvodů nebo jakákoli jiná síťová komponenta specifická pro zákazníky nebo data specifická pro uživatele.