Penetrační testování

1.1. Penetračními testy (dále jen „Testování“) se rozumí činnost související s otestováním možného průniku do počítačového systému nebo sítě (dále jen „Počítačové systémy“) zákazníka a za účelem zjištění jejich zranitelnosti či jejich zabezpečení, ověření účinnosti interních bezpečnostních opatření, popř. poskytnutí poradenství k zabezpečení předmětných Počítačových systémů.

1.2. Testování bude prováděno sdružením CZ.NIC vzdáleně prostřednictvím sítě internet. V případě, že v průběhu testování vyvstane potřeba provést Testování na místě (místem se rozumí sídlo zákazníka či jiné jím určené místo v České republice), může část Testování v nezbytném rozsahu proběhnout po předchozí dohodě stran tímto způsobem.

1.3. Sdružení CZ.NIC se zavazuje poskytnout Testování ve sjednaných termínech. Závěrečná zpráva bude zpřístupněna zabezpečeným komunikačním kanálem dle dohody. Odesláním závěrečné zprávy je Testování dokončeno.

1.4. Sdružení CZ.NIC je povinno:

1.4.1. při provádění Testování postupovat s veškerou odbornou péčí, dodržovat obecně závazné právní předpisy, normy a další předpisy a pokyny zákazníka;

1.4.2. informovat zákazníka o všech okolnostech, které mohou zabránit a/nebo omezit průběh Testování, pokud jsou mu tyto skutečnosti známy předem. Jedná se především o poruchy nebo odstávky zařízení třetích stran (zejména přerušení dodávky elektrické energie, telekomunikačního spojení apod.

1.4.3. zdržet se jakéhokoliv úmyslného nakládání s údaji, daty, nebo informacemi zákazníka jinak, než pro účely provedení Testování, pokud k nim v průběhu Testování a v přímé souvislosti s Testováním získá přístup. Sdružení CZ.NIC odpovídá zákazníkovi v plném rozsahu za újmu vzniklou úmyslným porušením této povinnosti (pro vyloučení pochybností – o úmysl se nejedná v případě, pokud dojde např. k modifikaci či poškození dat v průběhu Testování, viz výčet rizik dále, jakožto předpokládaného rizika; odpovědnost sdružení CZ.NIC je dána v případech úmyslného zneužití Testováním získaného přístupu k datům).

1.5. Zákazník se zavazuje poskytnout sdružení CZ.NIC nezbytnou součinnost, zejm. vytvořit takové podmínky, aby Testování mohlo být provedeno řádně a včas, a poskytnout sdružení CZ.NIC veškeré informace nezbytné k provedení Testování, včetně přístupu do sítě a zajištění potřebného HW (PC) pro potřeby provedení Testování. O dobu prodlení zákazníka s poskytnutím součinnosti se sdružení CZ.NIC prodlužuje doba k provedení Testování.

1.6. Zákazník prohlašuje, že je výlučným vlastníkem či oprávněným uživatelem Počítačových systémů, které jsou předmětem Testování, případně jedná na základě pověření vlastníka či provozovatele Počítačových systémů či jiné oprávněné osoby.

1.7. Sdružení CZ.NIC je oprávněno odmítnout provést Testování nebo přerušit jeho poskytování i v jeho průběhu, a to zejména v případě, kdy bude zjištěno, že zákazník nebyl oprávněn objednat či zajistit provedení Testování nebo pokud má sdružení CZ.NIC důvod se domnívat, že tak zákazník nebyl oprávněn učinit.

VYLOUČENÍ ODPOVĚDNOSTI

1.8. Zákazník výslovně prohlašuje, že si je plně vědom, že Testování představuje simulaci reálného kybernetického útoku na Počítačové systémy zákazníka a také možnosti zneužití zranitelností za použití ofenzivních technik, které mohou reálně ohrozit fungování nebo provoz testovaných Počítačových systémů a mohou dále negativně ovlivnit i fungování a provoz dalších souvisejících systémů.

1.9. Zákazník bere na vědomí, že prostřednictvím Testování nemusejí být odhaleny všechny nedostatky zabezpečení či zranitelnosti testovaných Počítačových systémů. Zákazník rovněž bere na vědomí, že ne všechny výsledky zjištěné Testováním musejí být skutečnými nedostatky zabezpečení či zranitelnostmi. Testování je určeno jako pomůcka pro zákazníka a jeho provedení nepředstavuje žádné potvrzení o bezvadnosti, bezrizikovosti, dostatečném zabezpečení či nezranitelnosti testovaných Počítačových systémů. Zákazník není oprávněn výsledky Testování uveřejňovat, ani není oprávněn užívat výsledky Testování či fakt, že jeho Počítačové systémy prošly Testováním, pro své reklamní, marketingové nebo PR aktivity. Povinnost zákazníka stanovená v předchozí větě platí obdobně i pro sdružení CZ.NIC, s výjimkou zpracování informací o Testování dle bodu 1.14. Výsledky Testování se vztahují pouze ke konfiguraci testovaných Počítačových systémů a jejich konfiguraci a prostředí v okamžiku provádění Testování. Poskytovatelem není poskytována na výsledky Testování žádná záruka.

1.10. Zákazník prohlašuje, že byl ve smyslu bodu 1.8. a v souladu s ustanovením § 2896 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, upozorněn sdružením CZ.NIC na možná rizika související s Testováním. Demonstrativní výčet rizik a jejich popis je uveden dále. Zákazník potvrzuje, že se důkladně seznámil a je plně srozuměn s možnými riziky, které v souvislosti s Testováním existují.

1.11. Sdružení CZ.NIC neodpovídá za újmu vzniklou zákazníkovi či třetím osobám v souvislosti s provedením Testování, zejména pak za újmy způsobené poškozením Počítačových systémů zákazníka, nebo způsobením výpadku (nedostupnosti) jeho Počítačových systémů, ledaže byla tato újma způsobena úmyslně či hrubou nedbalostí, a to nejvýše do limitu uhrazené ceny za Testování. Sdružení CZ.NIC neodpovídá ani za nepřímou újmu vzniklou zákazníkovi či třetím osobám, zejména pak za případný ušlý zisk způsobený výpadkem či poškozením Počítačových systémů zákazníka.

1.12. Smluvní strany se zavazují vyvinout úsilí, které po nich lze spravedlivě požadovat, k předcházení škodám a k minimalizaci vzniklých škod. Sdružení CZ.NIC je povinno upozornit zákazníka na rozumně předvídatelné skutečnosti, které by mohly vést ke vzniku újmy. Zákazník je povinen sdělit sdružení CZ.NIC veškeré relevantní informace k předejití škodám či k jejich minimalizaci.

1.13. Zákazník odpovídá za újmu způsobenou sdružení CZ.NIC zejména tím, že uvedl nepravdivé, neúplné nebo zavádějící údaje, porušením smlouvy (užití Testování v rozporu se smlouvou, resp. touto přílohou smlouvy) či práv třetích osob.

1.14. Zákazník výslovně souhlasí s tím, že sdružení CZ.NIC je oprávněno zpracovat informace získané v průběhu Testování, a to i důvěrné informace, tak, že tyto informace budou anonymizovány a statisticky zpracovány tak, aby jejich dalším užitím nebyl přímo identifikován Zákazník ani jeho Počítačové systémy, které byly testovány („anonymizovaná data“). Anonymizovaná data je sdružení CZ.NIC oprávněno uchovávat, zpracovávat, uveřejňovat, spojovat je s dalšími informacemi a poskytovat je třetím osobám, a to bez omezení území, času, formy uchování a způsobu zpracování. Za poskytnutí tohoto oprávnění nenáleží zákazníkovi odměna.

DEMOSTRATIVNÍ VÝČET RIZIK V SOUVISLOSTI S PROVEDENÍM TESTOVÁNÍ

Během testování může docházet

- Při provádění automatizovaných testů k odmítnutí služby (zablokování, nedostupnost; Denial of Service) nebo k omezení provozu;
- Při testování autentizace k zablokování uživatelských účtů;
- K nabourání do systémů a k zpřístupnění či získání dat z tohoto systému;
- K nestandardnímu chování aplikace;
- K aktivaci bezpečnostních mechanismů aplikace/firewallu (může dojít k zaslání oznámení administrátorovi);
- K zaplnění logovacího systému;
- K poškození systému/sítě;
- Ke ztrátě dat;
- K tvorbě fiktivních dat;
- K tvorbě fiktivních registrací.