ETALON MINIMÁLNÍ BEZPEČNOSTI PRO DODAVATELE

Statutární město Brno

Obsah

1 Úvodní ustanovení

1. **Etalon minimální bezpečnosti pro dodavatele** statutárního města Brna (dále též SMB) tvoří soubor pravidel a postupů, který vymezuje způsob a požadovanou úroveň bezpečnosti, vymezení aktiv a způsob jejich zajištění, týkající se firem a organizací se smluvním vztahem ke statutárnímu městu Brnu.
2. Dodržování pravidel uvedených v tomto dokumentu je povinné pro všechny partnery spolupracující na smluvní bázi se statutárním městem Brno, kterých se dotýká problematika bezpečnosti.
3. Používané i nově zaváděné informační systémy v rámci SMB musí být upraveny, vyvíjeny a vybírány a spravovány tak, aby splňovaly zásady bezpečnosti podle této směrnice.
4. Tento dokument je pro smluvní partnery statutárního města Brna veřejný.

1.1 Cíle dokumentu

1. Bezpečnost je ochrana informací, systémů a služeb proti živelním událostem, lidským omylům a úmyslné manipulaci s cílem snížit pravděpodobnost a dopad bezpečnostních incidentů na minimum.
2. Cílem **Etalonu minimální bezpečnosti pro dodavatele** statutárního města Brno je obecně:
   a) specifikovat jasné zásady bezpečnosti SMB pro dodavatele
   b) zabránit porušení platných právních předpisů ČR ,
   c) zamezit, příp. minimalizovat možnost finanční a majetkové újmy,
   d) zabránit neautorizovanému přístupu k informacím SMB,
   e) umožnit provádění kontroly přístupu k informacím,
   f) zajistit dostupnost informací pro oprávněné uživatele i procesy,
   g) zabránit neautorizované modifikaci či zneužití dat nebo jiných aktiv a umožnit ověření původu informací,
   h) definovat základní pravidla rozvoje a výběru nových používaných prostředků a technologií (vývoj zabezpečovacích prostředků, vlastnosti používaných aplikací a operačních systémů),
   i) umožnit sledování a hodnocení stavu bezpečnosti.

2 Obecné povinnosti

Mezi zodpovědnosti zaměstnanců smluvních partnerů patří zejména:

a) dodržování platných bezpečnostních ustanovení a právních předpisů,

b) využívání uživatelských systémů tak, jak bylo stanoveno vlastníkem informací,

c) používání informačních aktiv statutárního města Brna pouze v souladu s rozsahem přístupových oprávnění a pouze ke schváleným účelům,

d) zajištění ochrany svých autentizačních údajů, (login, heslo, identifikační předmět)

e) odpovědnost za každý přístup k informacím, provedený prostřednictvím jejich autentizačních údajů,

f) respektování všech bezpečnostních opatření a procedur určených vlastníkem informací,

g) nerozšiřování dat bez souhlasu vlastníka informací nebo jeho nadřízeného.

3 Bezpečnost HW, SW a komunikace

Smluvní partneři SMB musí chránit aktiva SMB, která používají ke své práci či výkonu pro SMB, a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití nebo odcizení.

3.1 Pracovní stanice, notebooky

Při práci na koncových uživatelských pracovištích SMB musí být splněny nejméně následující bezpečnostní zásady:

a) Použití počítače SMB musí být umožněno pouze oprávněné osobě.

b) Je zakázáno připojovat vlastní počítače do vnitřní sítě SMB bez vědomí správce informační bezpečnosti.

c) Pracovní stanice nesmí být ponechány bez dozoru zapnuté a s přihlášeným uživatelem. Je třeba přinejmenším použít heslem chráněného spořiče obrazovky.

d) Počítač smluvního partnera, který má být připojen do vnitřní sítě SMB, musí mít instalován a spuštěn systém pro ochranu před škodlivými programy (antivirový program) v nejnovější verzi programu i virové databáze.

e) Smluvní partner je povinen chránit vybavení SMB, udržovat okolo sebe bezpečné pracovní prostředí; v blízkosti výpočetní techniky je zakázáno jíst, pít a kouřit.

f) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému, aby se zamezilo zneužití jeho přístupových práv.

3.2 Využívání internetu

1. Systémy v SMB vztahující se k počítačové síti, internetu a intranetu, včetně počítačového vybavení, programů, operačních systémů, medií pro ukládání dat, schránek elektronické pošty SMB, možností prohlížení internetových stránek a zdrojů přístupných na FTP jsou vlastnictvím SMB. Tyto systémy jsou používány pro pracovní účely tak, aby sloužily zájmům SMB a jejím klientům a partnerům při normální činnosti.

2. Zaměstnanci smluvních partnerů mají dovoleno používat internetové připojení do a z vnitřní sítě SMB pouze za účelem pracovních záležitostí. Způsob připojení do vnitřní sítě SMB a autentizace musí být předem dohodnuta s manažerem informační bezpečnosti SMB. Poskytovatel vede provozní deník, kde je jednoznačně zaznamenáno datum a čas přihlášení k vnitřnímu prostředí a následně ukončení práce ve vnitřním prostředí. Poskytovatel je povinen provozní deník předložit na vyžádání objednatele.

4 Bezpečnost systémů IT

U vyvíjených, dodávaných a spravovaných informačních systémů musí být zajištěna níže uvedená pravidla.

4.1 Používání hesel

a) Aplikace musí být vytvářeny tak, aby znemožnily přístup bez zadání hesla.

b) Uživatel aplikace musí být nucen si heslo pravidelně měnit.

c) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezeno. Po třech neúspěšných pokusech o přihlášení musí být další zadávání dočasně ochromeno nebo spojení rozpojeno.

d) Pokud je při přihlašování do aplikace některá část chybná, nesmí být uživateli poskytnuta informace, ve kterém z údajů je chyba.

e) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností autora aplikace vynutit si změnu tohoto inicializačního hesla.

f) Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor (přihlašovací jméno) tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti.

g) Zaměstnanci dodavatele smí používat jedno přihlašovací jméno pro několik svých zaměstnanců, přičemž dodavatel odpovídá za veškeré úkony provedené v informačním systému SMB pod těmito identifikátory.

h) Systém správy hesel musí být podpořen efektivním a interaktivním vybavením, které prosazuje kvalitu hesel.

4.2 Monitorování používání a přístupu k systému

V informačních systémech musí být pořizovány auditní záznamy obsahující:

a) identifikaci uživatele,

b) datum a čas přihlášení a odhlášení,

c) identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné),

d) záznamy o přístupu (úspěšném i neúspěšném).

4.3 Řízení přístupu k informačnímu systému

a) Před umožněním přístupu musí být každý uživatel identifikován a autentizován.

b) Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.

c) Po určitém množství neúspěšných autentizačních pokusů (doporučeno 3) se musí ukončit přihlašovací procedura.

d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informaci o tom, která část autentizace je chybná.

e) Pro každého uživatele systému musí být možno identifikovat, jaká má přístupová práva.

f) Pro každý protředek musí být možno vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.)

g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

5 Bezpečnost dat

5.1 Data vstupující do IS SMB

Data vstupující do systémů musí být kontrolována, aby byla zajištěna jejich správnost. V aplikacích se musí evidovat identifikátor uživatele nebo procesu, který změny nebo pořízení provedl.

Pro kontrolu dat je nezbytné aplikovat opatření:

a) Vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost…),

b) kontrola vnitřního zpracování dat,

c) kontrola oprávněnosti běhu programů,

d) kontrola integrity dat,

e) kontrola obsahu generovaných dat.

Opatření musí zahrnovat i popis postupu při zjištění chyby.

Pokud SMB usoudí, že vytvářená aplikace by měla podporovat kryptografii, je nezbytné, aby byly podporovány mezinárodně uznávané standardy a dodrženy právní předpisy České republiky.

5.2 Data předávaná smluvním partnerům

Jedná se o informace předávané ze SMB smluvnímu partnerovi na jakémkoliv nosiči, zejména jakékoliv listiny, interní dokumenty SMB, CD-ROM, diskety, pevné disky počítačů a jiné nebo zasílané e-mailem. Smluvní partner musí nakládat s předávanými daty dle tohoto dokumentu.

a) Předávání dat musí být vymezeno ve smlouvě (struktura dat, způsob předávání, způsob ochrany, periodicita, oprávněné osoby atd.) a musí probíhat bezpečným způsobem.

b) Uchovávání a případné zpracování dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich dostatečná ochrana před neoprávněným přístupem a aby bylo znemožněno jejich zneužití.

c) Zodpovědnost za dostatečnou ochranu předávaných dat má smluvní partner

d) Je nutno dbát na bezpečnost likvidace již nepotřebných dat, případně médií s daty. Pro likvidaci medií nesoucích neveřejné informace musí být zvolena metoda, která zaručuje, že takto zlikvidované informace není možno běžně dostupnými prostředky obnovit (skartovačka, SW skartovačka).

e) Každé nové předávání dat na smluvním základě je vhodné již při tvorbě smlouvy konzultovat s Manažerem informační bezpečnosti.

f) Smluvní partner si nesmí sám stahovat žádná data z IS SMB; vytváření souborů musí provést oprávněný zaměstnanec SMB a teprve takto vytvořená data smí být (na smluvním základě) předána partnerovi.

6 Bezpečnost dodávek a služeb

6.1 Vývoj software smluvními partnery

1. Vývoj software musí probíhat:
    a. legálním software,
    b. na testovacím prostředí odděleném od prostředí produkčního,
    c. na testovacích datech, která nejsou převzata z provozní databáze. Pokud je nutno použít data z provozní databáze, je nutno je anonymizovat,
    d. tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení.
2. Přístup dodavatele do IS SMB
    a. Vzdálený přístup dodavatele může být povolen pouze do vývojového a testovacího prostředí za podmínek dohodnutých se Správcem informační bezpečnosti. Výjimky může povolit pouze Manažer informační bezpečnosti.
    b. Lokální přístup dodavatele do provozního prostředí musí být zcela výjimečný a bude povolen pouze v odůvodněných případech. Tento přístup musí probíhat ve zvláštním režimu dohledu ze strany administrátorů nebo oprávněných uživatelů, vždy ale až po povolení administrátorem SMB na základě zdůvodnění dodavatele.
    c. Přístup dodavatele do IS SMB (testovacího i provozního prostředí) může být použit pouze pro zpracování zadané oprávněným pracovníkem SMB.

6.2 Dodávka software

1. Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována.
2. U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice.

3. Každý nový software musí být otestován, než bude akceptován a zařazen do produkčního prostředí.

6.3 Dodávka hardware

1. Dodávka hardware musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. O každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný dodavatelem a odběratelem. Způsob předání závisí na konkrétním produktu a na smlouvě s dodavatelem.
2. Každé nové zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí.

6.4 Dodávka služeb

Dodávka služeb musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Způsob předání závisí na konkrétní službě a na smlouvě s dodavatelem.

6.5 Servis HW a SW

Smluvní partneři, zajišťující servis hardware nebo software, jsou na základě smlouvy oprávněni pohybovat se v neveřejných lokalitách SMB pouze s vědomím administrátora SMB.

6.6 Ostatní služby

Smluvní partneři zajišťující ostatní služby, např. úklid, ostrahu atd. jsou na základě smlouvy oprávněni pohybovat se v neveřejných lokalitách SMB. Při svém pohybu musí dbát bezpečnostních pravidel a pokynů pracovníků SMB.

6.7 Dokumentace o provedené práci

Nedílnou součástí dodávky hardware, software nebo služeb tam, kde to má smysl, je projektová a bezpečnostní dokumentace. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s dodavatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v krajním případě odstoupení od smlouvy z důvodu jejího nenaplnění ze strany dodavatele.

6.8 Akceptace

Každý dodaný hardware, software nebo služba musí být plně a široce otestován zda splňuje očekávané a smluvně definované parametry a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika. Než bude systém předán do rutinního provozu, musí být formálně akceptován managementem a specialisty.

6.9 Outsourcing

Outsourcing musí být řádně smluvně zajištěn a průběžně kontrolován a dokumentován. Všechna externí zpracování neveřejných informací SMB musí být smluvně ošetřena tak, aby byla zachována úroveň ochrany ve všech aspektech informační bezpečnosti podle požadavků SMB a platných právních předpisů.

7 Poskytování informací třetím stranám (mlčenlivost)

1. Smluvní partneři jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při výkonu své činnosti v souladu s uzavřenou smlouvou v SMB. Tato skutečnost musí být ošetřena smlouvou, ve které může být udělena výjimka např. pro účely reference.
2. Každé veřejné použití neveřejných informací SMB (např. na veřejných vystoupeních, do publikací) musí být schváleno vlastníkem těchto informací.

8 Závěrečná ustanovení

Závažné porušení bezpečnostních standardů zavedených v SMB, bude klasifikováno jako porušení smlouvy a SMB může od smluvního partnera požadovat náhradu vzniklé škody s ohledem na okolnosti vzniku škody.