Kybernetická bezpečnost - podmínky
obchodní společnosti ENERGETIKA TŘINEC, a.s.

pro práce nebo služby,
realizované na základě smluvního vztahu uzavřeného mezi objednatelem a dodavatelem.

Platné od 01.05.2023

1.1 Požadavky na bezpečnost objektů

ENERGETIKA TŘINEC, a.s. (dále jen „ET“) stanovila fyzické bezpečnostní okruhy týkající se ochrany objektů, v nichž jsou umístěna primární či podpůrná aktiva (prostředky ICT nebo informace), a ve kterých musí být v souladu s typem objektu dodržovány minimální požadavky a prvky fyzického zabezpečení.

- V případě fyzického přístupu pracovníků dodavatele do objektů ET musí tito pracovníci dodržovat požadavky na objektovou bezpečnost ve fyzicky zabezpečených oblastech, kam mají v rámci plnění smluvních závazků a schválené žádosti oprávněn fyzický vstup.
- V případě ICT a informací umístěných, spravovaných nebo poskytovaných mimo objekty ET, musí vlastníci nebo jiní uživatelé těchto objektů zajistit adekvátní naplnění požadavků na prvky objektové bezpečnosti tak, aby nemohlo dojít k neoprávněnému fyzickému přístupu k ICT a informacím ET.

1.2 Požadavky na bezpečnost zařízení

Zařízení a vybavení, které slouží k zajištění provozu podpůrných aktiv (ICT nebo podpůrných služeb), musí být chráněno před fyzickými hrozbami, jako jsou přírodní události (oheň, voda, mráz, vítr) nebo působení lidského činitele, jejichž výsledkem může být havárie, porucha, poškození, zničení, krádež apod. Mezi zařízení a vybavení, která musí být chráněna v objektech ET i dodavatele, a na kterých je závislá provozuschopnost ICT, patří:

- výpočetní technika, switch / router, přístupové zařízení (AP), kabeláž, tiskárna, skener, kopírka
- zdroje energie, jističe, UPS, agregáty.

Všichni pověření, resp. oprávnění pracovníci dodavatele jsou povinni zabezpečit fyzický přístup k zařízení a vybavení ve všech lokalitách, kde jsou umístěny ICT, IS nebo jejich komponenty (v elektronické i tištěné podobě), před výše uvedenými fyzickými hrozbami jak v mimopracovní době, tak i v případě krátkodobého opuštění pracoviště v pracovní době, zejména těmito opatřeními:

- dodržování zásady „čistého stolu“, tzn. bezpečné ukládání dokumentů v listinné podobě a nosičů dat a médií podle citlivosti obsažených informací (v souladu s klasifikací informací) - do uzamykatelných schránek (zásuvka, skříň, trezor)
- důsledné zamykání kanceláře
- fyzická ochrana klíčů, vstupních / čipových karet apod.
- zákaz kouření a práce s nebezpečnými látkami na pracovišti.

Povinnosti fyzické ochrany (tj. zvýšená opatrnost a používání prostředků fyzické bezpečnosti) se vztahují i na mobilní zařízení, jako jsou např. přenosné počítače, notebooky, tablety, mobilní telefony, nosiče dat a média, pokud fyzicky opouštějí zabezpečené oblasti ET a jsou používány v objektech nechráněných bezpečnostními perimetry[1] .

1.3 Požadavky na kontrolu fyzického přístupu

Fyzický vstup návštěvníků a pracovníků dodavatele do zabezpečených oblastí objektů ET musí být kontrolován. K prostředkům ICT, které jsou umístěny v zabezpečených oblastech ET nebo dodavatele, je fyzický přístup vyhrazen pouze povolaným a oprávněným osobám, kterými mohou být:

- zaměstnanci ET na základě jim přidělených oprávnění, nebo
- pracovníci dodavatele na základě smluvních ujednání.

Všem ostatním osobám je fyzický přístup a používání ICT ET zakázáno.

[1] Perimetr = hraniční prvek objektu, jako např. budova / zdi, uzamykatelné dveře, schránka / trezor apod.

1.4 Požadavky na řízení přístupu k informacím

Základními požadavky při řízení tzv. „logického“ přístupu, tedy přístupu externího uživatele na základě přihlášení uživatelským účtem s přístupovým oprávněním k informacím zpracovávaným v ICT, jsou:

- maximální omezení všech práv; postupné rozšiřování a přidělování práv je možné pouze:
  - se souhlasem administrátora nebo Manažera kybernetické bezpečnosti ET, který posuzuje oprávněnost přístupu
  - na základě písemného požadavku externí odpovědné osoby, která posuzuje potřebnost přístupu externího uživatele
- každá organizace (dodavatel a jeho pracovníci) musí mít přidělen svůj vlastní (jmenovitý) externí uživatelský účet pro každou fyzickou osobu
- zákaz sdílení jednoho administrátorského přístupu (účtu) více fyzickými osobami
- každý pracovník dodavatele (externí uživatel) musí být odpovědný za ochranu jemu přidělených přihlašovacích údajů (jméno, heslo, PIN, další autentizační údaje).

1.4.1 Standardy pro přidělování přístupu

Každému externímu uživateli je na základě schváleného požadavku přidělován přístup, jehož rozsah určuje garant aktiva. Nadstandardní rozšíření přístupu a výjimky jsou řešeny individuálně:

- podle specifických potřeb určovaných garantem aktiv
- v souladu s interní klasifikací informací.

Pracovníci dodavatele s přidělenou možností hlásit se k IS zvenčí musí používat zabezpečený způsob přístupu a autentizace dle aktuálně používaných metod přístupu pro dodavatele.

1.4.2 Používání privilegovaného přístupu

Za privilegovaný přístup je považován takový přístup (např. administrátorský), který umožňuje uživateli spravovat systém, tzn. zasahovat do jeho konfigurace, provádět změny, vytvářet či rušit účty a přístupy dalším uživatelům apod. Privilegované (administrátorské a podobné) účty přidělené pracovníkům dodavatele je dovoleno používat pouze pro správu systémů, nikoliv k běžné činnosti těchto externích uživatelů. Jeden účet nesmí být sdílen více administrátory, pokud je to technicky / provozně možné.

Pro dodavatele jsou uplatňovány následující požadavky:

- Přidělení privilegovaného (resp. administrátorského) přístupu k ICT ET dodavateli musí schválit Manažer kybernetické bezpečnosti.
- Uživatelé bez oprávnění administrace systému ET musí mít systémově odepřen přístup k těmto činnostem a nesmí jim být dovoleno svévolně vytvářet další účty a přístupy k operačnímu systému počítače, z nějž přistupují k ICT a informacím ET.
- Na všech počítačích s přístupem k ICT a informacím ET je povolen výskyt pouze administrátorem předem definovaných účtů a musí být povinně zrušeny / zakázány všechny obecné účty vytvářené např. při instalaci OS s přednastaveným přístupem (typu „guest“, „anonymous“ apod.).
- Každý externí uživatel se musí korektně přihlašovat k danému systému svým jedinečným identifikátorem (jménem a heslem) příp. jiným povoleným způsobem identifikace a autentizace, tj. ověření uživatele vůči systému, využití schválených autentizačních prostředků, HW tokenů, čipových karet, digitálních certifikátů apod.
- Pokud aplikace využívají vlastní omezení přístupu k informacím zpracovávaným jejich prostřednictvím, pak tato omezení nesmějí být v rozporu se stanovenou politikou přístupových práv a úrovní přístupu (zejména ke klasifikovaným informacím) pro konkrétní externí uživatele či jimi zastávané funkce.

1.5 Požadavky na hesla

Pro oprávněný přístup dodavatele musí být používána přístupová hesla, která splňují stanovená kvalitativní kritéria:

- vygenerované prvotní heslo musí být uživateli předáváno bezpečným způsobem,
- přidělené heslo k uživatelskému účtu musí být při prvním přihlášení uživatelem změněno,
- musí být uplatňována vícefaktorová autentizace, nebo:
  - heslo musí být dlouhé minimálně:
    - 12 znaků (pro běžné uživatele)
    - 17 znaků (pro privilegované účty)
- heslo musí mít nastaveno datum expirace,
- heslo musí být změněno každých 18 měsíců,
- opakované použití stejného hesla musí být omezeno, tj. že systém si musí pamatovat nejméně 12 hesel

v historii,
- systém musí limitovat počet neúspěšných pokusů o přihlášení, tj. zablokovat přístup po 5 pokusech,
- heslo nesmí být nikde ukládáno v čitelné (nechráněné) podobě, a to jak ve fyzické, tak v elektronické podobě,
- heslo může být změněno nejdříve za 30 minut po předchozí změně.

1.6 Požadavek čistého stolu a obrazovky

V případě fyzického opuštění pracoviště v ET nebo v místě, odkud se pracovník dodavatele přihlašuje k ICT ET, je povinností externího uživatele zabezpečit pracoviště i pracovní stanici před neoprávněným fyzickým i logickým přístupem jiných osob takovým způsobem, který je přiměřený délce nepřítomnosti, jako např.:

- odhlášení uživatele
- uzamknutí stanice
- aktivace spořiče obrazovky chráněného kvalitním heslem
- bezpečné uložení nosičů dat a výtisků klasifikovaných informací
- uzavření oken, uzamčení místnosti
- aktivace zabezpečovacího systému / EZS apod.

Jedná-li se o nepřetržitý provoz, při němž se nelze odhlásit ze systému a stanice či konzola serveru musí zůstat v provozu např. i v nočních hodinách, je nezbytné zamezit přístupu k systému nepovolaným osobám jinými vhodnými opatřeními, která stanoví Manažer kybernetické bezpečnosti.
Všechny neaktivní stanice či terminály musí být po definovaném čase nečinnosti automaticky zablokovány.

1.7 Požadavky na ochranu mobilních prostředků při práci na dálku

ET uplatňuje politiku ochrany přístupu k mobilním prostředkům používaným vně (tzn. mimo chráněné prostředí počítačové sítě) ET, jako jsou např. notebooky, „chytré“ mobilní telefony, SD-karty a další zařízení či média fungující jako nosiče dat, kde mohou být potenciálně ohroženy klasifikované informace.
Používá-li pracovník dodavatele mobilní prostředky, v nichž se nacházejí chráněné informace ET klasifikované vyšší než „nízkou“ úrovní (veřejné informace), je povinen takové prostředky zabezpečit některým ze stanovených způsobů:

- ochrana zařízení (dle typu mobilního prostředku)
- ochrana přístupu k informacím v zařízení (dle typu např. PIN, gesto, biometrika, vícefaktorová autentizace)
- šifrování dat (šifrovací nástroj a použití kvalitního hesla viz kapitola 4.5)
- příp. fyzická ochrana mobilního prostředku (přenosná schránka chráněná zámkem s kódem).

Dostatečnost zabezpečení mobilních prostředků používaných k práci na dálku s ICT a informacemi v ET posuzuje, případně vhodné metody ochrany konkrétních mobilních prostředků stanovuje správce systému (administrátor) ve spolupráci s Manažerem kybernetické bezpečnosti.

1.8 Požadavky na IT procesy

Všechny důležité nebo kritické IT-procesy v rámci podpůrných aktiv (dále jen „podpůrné IT-procesy“) týkající se provozu, zpracování dat a služeb poskytovaných dodavatelem, na kterých jsou závislá primární aktiva, musí být definovány, popsány a spravovány podle potřeby tak, aby:

- bylo možno je zabezpečit
- bylo možno zajistit zastupitelnost jednotlivých výkonných rolí.

1.8.1 Garant IT-procesu

Podpůrné IT-procesy mají přiřazeného garanta (vlastníka procesu), který je zodpovědný za jejich správné provádění. Správce systému (administrátor) je garantem podpůrných IT-procesů a odpovídá za jejich identifikaci, přidělení priorit a kontrolu výkonu smluvně dohodnutých IT-procesů a souvisejících činností pracovníků dodavatele.
Garant podpůrných IT-procesů odpovídá za jejich dokumentaci, popis postupů, jejich aktuálnost a evidenci.
Garantem procesu může být stanoven i zástupce dodavatele, jedná-li se o zajištění podpůrných IT-služeb externím dodavatelem. V takovém případě může být zpracování dokumentovaných postupů smluvně vyžadováno po dodavateli takové služby.
Manažer kybernetické bezpečnosti je oprávněný zajišťovat nezávislou kontrolu podpůrných IT-procesů – revizi postupů dodavatele z hlediska dostatečnosti IT-procesů, aktuálnosti, schválených přístupů a ochrany dat odpovídající jejich klasifikaci.

1.8.2 Hlášení incidentů podpůrných IT-procesů

Definování, popis a určení priority podpůrných IT-procesů slouží pro stanovení odpovídající reakce na pravděpodobné bezpečnostní incidenty v těchto procesech. Řízení incidentů obecně přísluší Manažerovi kybernetické bezpečnosti.
V případě zajišťování podpůrných IT-procesů dodavatelem musí být aplikovány následující kontrolní mechanismy vzájemné komunikace s odpovědnými osobami ET, zejména pro:

- hlášení závad a selhání podpůrných IT-procesů
- hlášení bezpečnostních incidentů a zranitelných míst (slabin) systémů
- kontrolu ztráty nebo porušení důvěrnosti informací v systémech spravovaných dodavatelem
- pravidelné sledování a vyhodnocování auditních záznamů systémů spravovaných dodavatelem.

1.8.3 Zajištění zastupitelnosti

V případě podpůrných IT-procesů realizovaných dodavatelem je uplatňován požadavek na zachování kontinuity. Dodavatel musí zajistit zastupitelnost pracovníků v době jejich nepřítomnosti. Pro tyto případy musí být v dokumentaci dodavatele uvedena podrobná pravidla (např. pro ukládání, resp. obnovu hesel a přístupových kódů pro mimořádné události, prokazatelné přidělení příslušných oprávnění zastupujícím pracovníkům, požadavky přesměrování komunikace apod.).

1.9 Požadavek na oddělení procesů vývoje od ostrého provozu

Vývoj programového vybavení je řešen dodavatelsky. Pokud dochází k implementaci SW-nástrojů či k úpravám systémů dodavatelem, musí být zajištěno, aby proces testování nového systému či SW nemohl negativně ovlivnit provozuschopnost podpůrných IT-procesů nebo bezpečnost „ostrých dat“. Migrace do ostrého provozu musí respektovat stanovené bezpečnostní zásady a pravidla ET zajišťující, že nedojde k neplánovanému přerušení činnosti nebo kompromitaci dat.

1.9.1 Změnové řízení

Implementace změn v systému realizovaných dodavatelem podléhá formalizovanému procesu změnovému řízení, v jehož rámci jsou změny autorizovány odpovědnými osobami. Požadované změny musí být ještě před implementací technicky přezkoumány správcem systému (administrátorem).
Dodavatel je povinný u programového vybavení, OS a IS, jejichž správu a provoz zajišťuje:

- omezit modifikace programových balíků (customizace ap.) na nezbytné minimum
- kontrolovat opravné „balíčky“ před jejich implementací do ostrého provozu, s ohledem na ochranu před možnými hrozbami, skrytými kanály a trojskými koni
- v případě vývoje nového SW externím dodavatelem je nutno zajistit příslušné bezpečnostní kontroly a smluvně ošetřit rizika.

1.10 Požadavky na ochranu před škodlivým SW

Informační systémy dodavatele, z nichž se v rámci oprávnění připojují pracovníci k systémům ET, musí být chráněny před škodlivými kódy pomocí vhodného SW. Antivirová ochrana obecně musí plnit jak detekční funkce, tak podle možností a potřeby i preventivní opatření k zabránění průniku nebo rozšíření škodlivého SW do systémů ET. Jsou uplatňovány následující minimální požadavky:

- všechny počítačové stanice, včetně mobilních zařízení, s přístupem k informacím ET jsou kontrolovány na přítomnost škodlivého kódu a musí mít povinně zapnutou rezidentní AV ochranu
- na všech počítačových stanicích a mobilních zařízeních musí být zakázáno vypnout či omezit tuto ochranu uživatelem
- pro všechny pracovníky dodavatele platí zákaz zasahovat do HW a SW konfigurace počítače, k němuž jim byl přidělen přístup, pokud to nevyžaduje plnění smluvních závazků
- správnost, aktuálnost a účinnost nastavení AV ochrany musí být pravidelně kontrolována a ověřována
- zveřejněné opravné balíky (záplaty) jsou po nezbytném ověření funkčnosti neprodleně aplikovány na ohrožené systémy či aplikace.

1.11 Zálohování

Zálohování informací v ET je řešeno centrálně. Požadavky na zálohování a zálohovací mechanismy jsou na základě dokumentovaných podpůrných IT-procesů definovány jejich garanty. Dodavatel musí zajistit, aby:

- byla zálohována všechna důležitá data nezbytná pro zajištění kontinuity provozu jimi spravovaných systémů nebo v rámci jimi poskytovaných IT-služeb, a to vhodnou definicí požadavků na zálohy (dle

stanovených RTO / RPO)
- se na lokálních počítačových stanicích nevyskytovaly žádné informace určené ke sdílení a podléhající centrálnímu zálohování.

Vyžaduje-li to charakter zpracování, jsou individuální zálohy dat na lokálních PC (např. u specifických lokálních agend) řešeny jednotlivě dle požadavků garantů těchto procesů pověřenými zástupci ET a dodavatele.
Pokud na straně externích dodavatelů existují záložní kopie důležitých informací musí být:
- zabezpečeny před neoprávněným přístupem
- fyzicky uloženy odděleně od provozního prostředí (v jiné lokalitě).

1.12 Požadavky na bezpečnost elektronické komunikace

Při elektronické komunikaci s ET musí dodavatel posuzovat bezpečnostní rizika, která s sebou přináší komunikace prostřednictvím elektronické pošty tak, aby nemohla způsobit přerušení provozu ET či pád systému nebo služeb, ztrátu nebo kompromitaci neveřejných klasifikovaných informací, infikovat počítačovou síť ET viry nebo jiným škodlivým SW. Z těchto důvodů jsou u dodavatele uplatňovány následující bezpečnostní požadavky:
- obsah elektronické pošty, včetně příloh v různých formátech přijímaných zpráv, musí být chráněn proti škodlivým kódům účinným antivirovým programem
- neveřejné klasifikované informace ET musí být při přenosu prostřednictvím elektronické pošty (nebo obdobné formy komunikace prostřednictvím internetu) chráněny, jinak nesmí být v nezabezpečené formě posílány elektronickou poštou.

Vhodným způsobem ochrany je např. šifrování a použití elektronického podpisu, příp. ukládání dokumentů do určeného zabezpečeného úložiště s chráněným přístupem.

1.13 Požadavky na kryptografická opatření

Neveřejné klasifikované informace ET v elektronické podobě nesmí opustit chráněné prostředí počítačové sítě v otevřené formě. K jejich zabezpečení a přenosu mezi ET a dodavatelem musí být určeny smluvně nebo jinou vzájemně dohodnutou formou stanovené vhodné systémy, nástroje nebo kryptografické prostředky (dle aktuální metodiky – doporučení NÚKIBu).