Minimálny rozsah a špecifikácia bezpečnostných opatrení pre dodávateľa

# Všeobecné zásady

Minimálny rozsah a špecifikácia bezpečnostných opatrení v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj "**IaKB**“) pre Dodávateľa v prostredí Prevádzkovateľa pri plnení Hlavnej zmluvy je stanovený v týchto Pravidlách. Dodávateľ je povinný opatrenia uvedené v týchto Pravidlách uplatniť ako minimálne bezpečnostné štandardy a tieto opatrenia musia byť uplatňované po celú dobu plnenia Zmluvy, a to aj v prípade ak je plnenie zabezpečované na základe Zmluvy s dodávateľom alebo prostredníctvom tretích osôb.

Pravidlá a v nich uvedené opatrenia pokrývajú rôzne aspekty IaKB a vzťahujú sa na Plnenia uvedené v Zmluve (ďalej aj „**Plnenia**“), v závislosti od povahy takých Plnení ako je definované nižšie.

Tieto opatrenia môžu byť navyše posilnené o dodatočné bezpečnostné opatrenia, ktoré budú dohodnuté medzi Zmluvnými stranami v dokumentoch priložených k Zmluve, a/alebo Objednávke, alebo akoukoľvek inou súvisiacou zmluvou, ktorá takéto bezpečnostné opatrenia bude riešiť (napr. zmluva uzatvorená podľa Zákona o kybernetickej bezpečnosti).

Ak Dodávateľ v rámci svojho Plnenia zistí akúkoľvek nezhodu s bezpečnostnými opatreniami uvedenými v týchto Pravidlách, potom Dodávateľ Prevádzkovateľovi bezodkladne predloží analýzu situácie a plán pre zabezpečenie nápravy. Ak bude plán pre zabezpečenie nápravy Prevádzkovateľom schválený, bude Dodávateľom implementovaný bez akýchkoľvek nákladov pre Prevádzkovateľa a Dodávateľ poskytne dôkaz o účinnosti plánu pre zabezpečenie nápravy.

Ak nedodržanie požiadaviek pretrváva po dobu viac ako 30 dní, ak nebude v konkrétnom prípade dohodnutá iná lehota a/alebo plán pre zabezpečenie nápravy nebude schválený Dodávateľom alebo taký plán nezaistí nápravu, bude taký stav automaticky považovaný za podstatné porušenie zmluvy, pričom Prevádzkovateľ je v takom prípade oprávnený odstúpiť od Zmluvy.

# PRIORITA DOKUMENTOV

Pravidlá sa vzťahujú na všetky zmluvy uzatvorené s Dodávateľom, v ktorých je uvedený odkaz na tieto Pravidlá.

Ak nebude v Zmluve stanovené iné poradie priorít dokumentov, budú mať ustanovenia Zmluvy prednosť pred ustanoveniami týchto Pravidiel.

# DODRŽIAVANIE ZMLUVY A NORIEM (ODPORÚČANÝCH TECHNICKÝCH ŠTANDARDOV)

Hodnotenie bezpečnosti Plnenia

Na žiadosť Prevádzkovateľa poskytne Dodávateľ Prevádzkovateľovi do 10 pracovných dní všetky informácie potrebné pre zhodnotenie bezpečnosti Plnenia, ako sú správy o skúškach / auditoch bezpečnosti, kontroly zraniteľnosti, či analýzy robustnosti kódu. Pokiaľ Dodávateľ poskytuje Prevádzkovateľovi Plnenia týkajúce sa kybernetickej bezpečnosti, je povinný poskytovať Prevádzkovateľovi všetky potrebné informácie, súčinnosť a spoluprácu.

Bezpečnostné politiky

Dodávateľ musí mať zavedenú firemnú politiku bezpečnosti informácií, ktoré svojím obsahom zodpovedá norme ISO/IEC 27001 alebo inému podobnému štandardu uznávanému v danom odvetví.

Ak je Dodávateľ certifikovaný, musí Prevádzkovateľovi predložiť svoju bezpečnostnú certifikáciu a priebežne ho informovať o obnovení alebo odstránení svojich certifikátov.

Ak bol Dodávateľ Prevádzkovateľom vybraný na základe určitej certifikácie (napr. ISO / IEC 27001), potom je Dodávateľ povinný takúto certifikáciu udržiavať po celú dobu plnenia svojich zmluvných záväzkov.

Audit

Prevádzkovateľ  je oprávnený vykonávať audity u Dodávateľa s cieľom overiť dodržiavanie bezpečnostných požiadaviek Prevádzkovateľa definovaných v Zmluve.

Tretie osoby

V prípade, že Dodávateľ pri poskytovaní Plnenia Prevádzkovateľovi využíva tretie osoby, je Dodávateľ povinný zabezpečiť, aby tieto tretie osoby spĺňali bezpečnostné opatrenia dohodnuté v Zmluve.

# ORGANIZÁCIA BEZPEČNOSTI

Štruktúra

Na žiadosť Prevádzkovateľa je Dodávateľ povinný poskytnúť informácie o organizácii svojej bezpečnosti, vrátane systému riadenia kybernetickej bezpečnosti pokiaľ sa táto povinnosť Dodávateľa týka.

Kontaktné miesto

Dodávateľ menuje kontaktnú osobu pre bezpečnostné otázky. Kontaktné osoby budú zabezpečené pre každé plnenie a ich zmeny je nutné okamžite oznámiť Prevádzkovateľovi.

Kontroly bezpečnosti

Raz ročne, na žiadosť jednej alebo oboch Zmluvných strán, usporiadajú Dodávateľ a Prevádzkovateľ stretnutie, ktorého cieľom bude vykonať kontrolu bezpečnostných otázok (napr. vývoj a plánované aktivity, ktoré môžu mať vplyv na bezpečnosť).

Každá Zmluvná strana môže požiadať o mimoriadne stretnutie v záležitostiach týkajúcich sa bezpečnosti, pričom druhá Zmluvná strana je povinná túto požiadavku akceptovať v prípadoch, keď situácia vyžaduje spoločnú analýzu alebo okamžité rozhodnutie (napríklad v prípade vážneho incidentu alebo veľkého nárastu hrozieb).

Bezpečnostné opatrenia pre dáta Prevádzkovateľa

Údaje Prevádzkovateľa sú všetky druhy aktív Prevádzkovateľa, napr. informácie ako zmluvy alebo plány alebo technické informácie (ako sieťové schémy).

Dodávateľ zavedie a dodržiava bezpečnostné opatrenia na Prevádzkovateľom sprístupnené údaje podľa stupňa klasifikácie dát Prevádzkovateľa. Dodávateľ je povinný zaviesť nasledujúce opatrenia vzťahujúce sa na dáta Prevádzkovateľa t. j. údaje zašifrované Prevádzkovateľom a/alebo označené ako Chránené:

* + takéto dáta musia byť zašifrované keď sú uložené a prenášané,
  + bude implementovaný silný autentizačný systém (napr. dvojfaktorová autentizácie).

V prípade nutnosti výmeny zašifrovaných informácií sa zmluvné strany vopred dohodnú na spôsobe ich výmeny.

# RIEŠENIE INCIDENTOV

Odhaľovanie

Dodávateľ bude mať zavedené opatrenia na detekciu bezpečnostných incidentov, ktoré majú vplyv na Prevádzkovateľa, a ku ktorým dôjde v prostredí Dodávateľa. Medzi bezpečnostné incidenty patria okrem iného strata, zmena, vyzradenie alebo neoprávnený prístup k dátam či informáciám Prevádzkovateľa a ďalej neoprávnené zverejnenie proprietárneho zdrojového kódu alebo iných práv duševného vlastníctva a taktiež kybernetické bezpečnostné incidenty podľa Zákona o kybernetickej bezpečnosti.

Oznamovanie

Dodávateľ akýkoľvek bezpečnostný incident vrátane všetkých skutočností majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti bezodkladne oznámi Prevádzkovateľovi.

V prípadoch, keď dôjde k zisteniu akéhokoľvek narušenia a / alebo zneužitia dát alebo informácií Prevádzkovateľa, je Dodávateľ povinný Prevádzkovateľa informovať v súlade s príslušnými právnymi predpismi, bezodkladne, najneskôr však do 24 hodín.

Podrobnosti o bezpečnostných incidentoch budú Dodávateľom uchované v súlade s príslušnými právnymi predpismi, najmenej do ďalšej bezpečnostnej kontroly vykonávanej Zmluvnými stranami.

Vyriešenie

Dodávateľ vynaloží všetko úsilie na to, aby bezpečnostné incidenty ihneď vyriešil a bude Prevádzkovateľa informovať o postupe a vyriešení incidentu vrátane prijatia nápravných a nových prevenčných opatrení pre účely zamedzenia výskytu toho istého incidentu.

Správa o bezpečnosti

Prevádzkovateľ môže od Dodávateľa požadovať predloženie správy o bezpečnosti týkajúce sa poskytovaných Plnení a to najviac jedenkrát ročne; tým nie je dotknuté právo Prevádzkovateľa požadovať potrebné informácie priebežne kedykoľvek, ak je to potrebné v súvislosti s plnením jeho zákonných povinností. Táto správa o bezpečnosti musí okrem iného obsahovať tieto informácie:

* počet bezpečnostných incidentov zistených za posledných 12 mesiacov, a to oddelene pre vnútorné a vonkajšie príčiny, ak je toto rozdelenie relevantné,
* podrobnosti o bezpečnostných incidentoch v danom období (čas ich odhalenia, povaha a dopad, vyriešenie, doba obnovy služieb, čas uzavretia, čas nutný na vyriešenie problému),
* všetky informácie, ktoré bude Prevádzkovateľ požadovať v súvislosti s plnením jeho zákonných povinností a požiadaviek, najmä v súvislosti s platnou legislatívou v oblasti kybernetickej bezpečnosti a ochrany súkromia.

# ŠIFROVANIE A AUTENTIZÁCIA

Zmena autentizačných údajov a šifrovacích kľúčov Prevádzkovateľom

Všetky autentizačné údaje a šifrovacie kľúče (napr. certifikáty, páry kľúčov, symetrické kľúče, heslá) Plnení v oblasti Softvéru, Hardvéru,  Plnení týkajúcich sa kybernetickej bezpečnosti bude Prevádzkovateľ môcť zmeniť a budú chránené pomocou najmodernejších (state-of- the- art) technológií. U autentizačných údajov a šifrovacích kľúčov, ktoré Prevádzkovateľ nemôže zmeniť, predloží Dodávateľ Prevádzkovateľovi zoznam takýchto údajov vrátane informácií o ich účele. V prípade XaaS / cloudových služieb sa táto požiadavka vzťahuje len na autentizačné údaje včítane administrátorských účtov využívané Prevádzkovateľom pre ochranu jeho dát.

Sila šifrovacích algoritmov a kľúčov

Dodávateľ implementuje len štandardizované šifrovacie algoritmy a dĺžky kľúčov odporúčané verejnoprávnymi bezpečnostnými autoritami (napr. BSI, Anssi a NIST) v čase uzavretia alebo predĺženia Zmluvy a pravidelne aktualizuje takéto štandardizované kryptografické algoritmy a dĺžky kľúčov pre nové Plnenia.

# BEZPEČNOSŤ NÁVRHU

Zvýšenie odolnosti

Dodávateľ pri systémoch uplatní najlepšie postupy pre zvyšovanie odolnosti (hardening). Tieto postupy zahŕňajú, okrem iného, obmedzenia protokolov pre prístup, odstránenie alebo deaktiváciu nepotrebného softvéru, sieťových portov a služieb, odstránenie nepotrebných súborov, užívateľských účtov, obmedzenie povolenia k súborom, správu záplat a protokolovanie.

Dodávateľ poskytne Plnenie (vrátane súčastí a služieb tretích osôb), ktoré bude štandardne (by default) bezpečne nakonfigurované v súlade s najmodernejšími (state-of-the-art) postupmi pre konfiguráciu bezpečnosti (ako sú uvedené napríklad na stránkach [https: //www.cisecurity. org /](https:// /www.cisecurity. org%20/) ).

Okrem toho je Dodávateľ povinný zabezpečiť, aby Plnenie neobsahovalo žiadne tzv. Zadné vrátka (Back Doors).

Testovanie softwaru vzhľadom na bezpečnostné chyby

Dodávateľ je povinný vykonať testy Plnenia s cieľom zabezpečiť, že Plnenie nebude k dátumu odovzdania obsahovať žiadne nebezpečné softvérové chyby uvedené v "CWE / SANS Top 25" ( <http://cwe.mitre.org> ) a/alebo v "OWASP TOP 10" ( [http://www.owasp.org](http://www.owasp.org/) ) (napr. odolnosť voči neočakávaným vstupom, ako je SQL Injection, predvídateľnosť správania v prípadoch preťaženia).

Transparentnosť dokumentácie

Dodávateľ poskytne Prevádzkovateľovi:

* dokumentáciu potrebnú na bezpečnú konfiguráciu Plnení a bude udržiavať túto dokumentáciu v aktuálnom stave,
* súpis softvéru v strojovo čitateľnom formáte (vrátane názvu dodávateľa, ak je to vhodné, názvu softvéru a/alebo otvoreného zdroja a jeho verzie) a bude udržiavať tento súpis aktuálny.

Dodatočné opatrenia

Na žiadosť Prevádzkovateľa sa môžu Zmluvné strany navzájom dohodnúť na dodatočných bezpečnostných opatreniach, ktoré musí Plnenie spĺňať.

Tieto dodatočné opatrenia môžu byť uvedené v dokumente nazvanom "Vyhlásenie o zhode v oblasti bezpečnosti" a môžu byť obsiahnuté v Zmluve alebo inom dokumente, ktorý je jej súčasťou.

# OPRAVY ZRANITELNOSTÍ SOFTvérU

Odhaľovanie

Dodávateľ zaistí prijatie takých opatrení, ktoré umožnia nepretržité monitorovanie externých zdrojov bezpečnostných informácií (ako sú kooperačné bezpečnostné testy, externý výskum v oblasti bezpečnosti, open source a objavy tretích osôb,...) a bude sledovať Zraniteľnosti, ktoré by mohli mať vplyv na Plnenie ( vrátane súčastí tretích osôb).

CVE Štandard

V prípade potreby bude každej zraniteľnosti zistené Dodávateľom priradený jedinečný identifikátor CVE spojený so skóre CVSS (verzia 3 alebo vyššia) pozostávajúci z CVSS base, dočasného skóre a identifikátora vektora.

Oznámenie

Dodávateľ bezodkladne poskytne Prevádzkovateľovi informácie o každej Zraniteľnosti a to vrátane Zero-Day, s dopadom na Plnenie a informácie o prípadných dôsledkoch (napr. prípadných CVE, skóre CVSS, dotknutých komponentov alebo služieb).

Dodávateľ oznámi bezpečnostné upozornenia v akomkoľvek analyzovateľnom formáte (napríklad CVRF, CSAF, XML, JSON) prostredníctvom e-mailu kontaktnej osoby.

Zmluva o úrovni služieb v súvislosti s opravou Zraniteľnosti

Pre každú Zraniteľnosť, ktorá má vplyv na Plnenie, je Dodávateľ povinný poskytnúť Prevádzkovateľovi Dočasnú opravu a Oficiálnu opravu.

Údržba bezpečnosti súčastí Tretích osôb

Dodávateľ zabezpečí, aby všetky súčasti Plnenia poskytnuté tretími osobami, ktoré boli použité v rámci Plnenia na základe Zmluvy mali zaistenú údržbu z hľadiska bezpečnosti počas celého životného cyklu Plnenia.

Bezpečnostné Nedostatky

Dodávateľ súhlasí s tým, že pre každú Zraniteľnosť ovplyvňujúcu Plnenie, ktorú Prevádzkovateľ v priebehu zmluvnej doby údržby a / alebo záručnej doby zistí, je Prevádzkovateľ oprávnený zadať Požiadavku na údržbu so žiadosťou o jej odstránenie.

Výnimky

Dodávateľ vynaloží komerčne primerané úsilie na to, aby Prevádzkovateľovi s odstraňovaním zraniteľnosti pomohol:

* + v situáciách vyžadujúcich rýchlejšiu reakciu (napríklad pri zverejnení Zraniteľnosti Plnenia používaného Prevádzkovateľom prostredníctvom médií),
  + v technickom prostredí nevyhnutnom pre prevádzku Plnenia (napr. v operačnom systéme v prípade softvérového Plnenia).

Údržba súvisiace s bezpečnosťou

Dodávateľ musí pre každé Plnenie definovať minimálnu dobu podpory, ktorá nesmie byť kratšia ako záručná doba.

Počas životného cyklu Plnenia Dodávateľ poskytne Prevádzkovateľovi:

* + aktuálnu verziu Plnenia a budúce verzie so všetkými bezpečnostnými opravami,
  + bezpečnostné opravy podľa toho, ako a kedy budú vydané,
  + informácie (napr. CVE, CVSS skóre) o opravených zraniteľnostiach.

# DÁTA prevádzkovateľa V XAAS / CLOUDOVÝCH SLUŽBÁCH, PLNENIA týkajúce sa kybernetickej bezpečnosti

Pod pojmom XAAS sa rozumie čokoľvek, čo je užívateľom poskytované ako služba, vrátane SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) či podobné.

Obmedzenie používania dát Prevádzkovateľa

Dodávateľ bude dáta Prevádzkovateľa prenášať, spracúvať, vytvárať a / alebo ukladať v XaaS / Cloudové službe iba za účelom poskytovania uvedenej Služby.

Oddelenie dát Prevádzkovateľa

Dodávateľ bude dbať na oddelenie dát Prevádzkovateľa od dát iných zákazníkov Dodávateľa.

Dôverné dáta Prevádzkovateľa

Všetky dáta, ktoré budú Prevádzkovateľom klasifikované ako Interné alebo Chránené, budú Dodávateľom pre prenos a uloženie zašifrované.

Šifrovací mechanizmus Dodávateľa

V prípade, že Prevádzkovateľ využíva na ochranu svojich dát šifrovací mechanizmus poskytnutý Dodávateľom, je Dodávateľ povinný zabezpečiť, aby:

* + také dáta boli v priebehu uloženia a prenosu zašifrované,
  + pre prístup k takýmto dátam bola využívaná silná autentizácia (napr. dvojfaktorová autentizácia).

Zaznamenávanie (logovanie) prístupu k dátam Prevádzkovateľa a ich použitie

Dodávateľ zabezpečí:

* + zaznamenávanie (logovanie) prístupu k dátam Prevádzkovateľa a ich použitie, a to vrátane prístupov svojich vlastných zamestnancov a akýchkoľvek poverených tretích osôb,
  + uchovanie takých záznamov (logov) na obdobie dohodnuté Zmluve a / alebo Objednávke vrátane súvisiacich dokumentov (napr. v Zmluve o zachovaní dôverností alebo Zmluve o spracovaní osobných údajov), alebo štandardne po dobu 6 mesiacov.

Výpisy z uchovaných záznamov (logov) budú na požiadanie poskytnuté Prevádzkovateľovi.

Vrátenie dát Prevádzkovateľovi

Po skončení zmluvy a / alebo Objednávky vráti Dodávateľ Prevádzkovateľovi všetky dáta Prevádzkovateľa, a to v dohodnutom formáte a po dobu, na ktorých sa s Prevádzkovateľom vopred dohodne.

V súlade s ustanoveniami vyššie bude pre vrátenie dát Prevádzkovateľovi  použité výhradne šifrované pripojenie, ak nedá Prevádzkovateľ písomný súhlas s výnimkou z tohto pravidla.

Na konci lehoty na vrátenie dát Dodávateľ zlikviduje všetky prostredia Prevádzkovateľa, a to spôsobom, ktorý zaručí, že k žiadnym dátam Prevádzkovateľa nebude naďalej umožnený prístup a dáta nebude možné načítať.

Dodávateľ poskytne Prevádzkovateľovi osvedčenie o takomto zničení.

Fyzická bezpečnosť

Dodávateľ je povinný zabezpečiť priestory so zodpovedajúcou úrovňou fyzickej bezpečnosti ako pre produkčnú cloudovú infraštruktúru, tak pre lokality pre vzdialené činnosti.

Opatrenia budú spĺňať aspoň nasledujúce požiadavky:

* + fyzický prístup vyžaduje oprávnenia a je monitorovaný,
  + každý musí byť pri pohybe v priestoroch viditeľne označený oficiálnou identifikáciou,
  + návštevy sa musia zapísať do knihy návštev a musia byť pri pohybe v priestoroch sprevádzané a / alebo sledované,
  + držanie kľúčov / prístupových kariet a možnosti prístupu do lokalít sú monitorované. Pracovníci, ktorí ukončia pracovný pomer u Dodávateľa, musia kľúče / karty vrátiť.

Riadenie prístupu k systému a správa hesiel

Dodávateľ zaistí riadenie prístupov do systémov pre poskytovanie Služieb, pričom prístup bude obmedzený len na oprávnených pracovníkov.

Dodávateľ bude pre súčasti infraštruktúry a systémov pre správu cloudu, ktoré budú slúžiť pre servisné prostredie Dodávateľa, dôsledne uplatňovať politiku hesiel. Dodávateľ zabezpečí ochranu hesiel prostredníctvom bezpečných mechanizmov.

Kontrola prístupových práv

Účty pre zamestnancov Dodávateľa v sieti a v operačných systémoch budú pravidelne kontrolované tak, aby sa zabezpečila primeranú úroveň prístupových oprávnení pre príslušných zamestnancov.

V prípade, že niektorý zamestnanec Dodávateľa zmluvný projekt opustí, prijme Dodávateľ rýchle opatrenia, aby ukončil sieťový, telefonický a fyzický prístup takýchto bývalých zamestnancov.

Opatrenia proti škodlivému kódu, malwaru

Dodávateľ bude využívať softvér na ochranu proti malvéru, ktorý bude slúžiť na kontrolu ukladaných súborov. Definícia malvéru bude aktualizovaná prinajmenšom raz denne.

# PREVÁDZKA XAAS / CLOUDOVÝCH SLUŽIEB, PLNENIA týkajúce sa kybernetickej bezpečnosti

Penetračné testy

Dodávateľ bude vykonávať hodnotenie bezpečnosti poskytovaných Plnení prostredníctvom penetračných testov, a   to najmenej raz ročne. Správa z   hodnotenia a plán zmierňovanie následkov takých testov budú poskytnuté Prevádzkovateľovi.

Bez ohľadu na vyššie uvedené platí, že Dodávateľ umožní Prevádzkovateľovi vykonávanie penetračných testov na svojej produkčnej platforme a XaaS / Cloudovej službe.

Produkčné dáta a prostredie

Dodávateľ nebude pre testovanie využívať produkčné dáta.

Dodávateľ oddelí vývojové, testovacie a produkčné prostredie (siete, dáta, aplikácie atď.).

Plán obnovy po havárii (Disaster recovery plan)

Dodávateľ vytvorí a bude udržiavať plán obnovy po havárii a zaistí, aby tento plán bol v pravidelných intervaloch testovaný.

Správa, vrátane výsledkov týchto testov, sa na požiadanie poskytne Prevádzkovateľovi.

Zálohy budú Dodávateľom pri likvidácii bezpečne zmazané.

Údržba súvisiaca s bezpečnosťou

V prípade akýchkoľvek bezpečnostných záplat (patchov), ktoré Dodávateľ chce nasadiť pri poskytovaní Plnenia, je Dodávateľ povinný danú bezpečnostnú záplatu nasadiť a otestovať v testovacom prostredí. Až po úspešnom dokončení testov v testovacom prostredí môže Dodávateľ záplatu nasadiť v produkčnom prostredí.

Služby Tretích osôb

Dodávateľ je oprávnený pri poskytovaní Plnenia využívať služby tretej osoby (napr. služby dátového centra), len po predchádzajúcom písomnom schválení Prevádzkovateľom.

Premiestnenie údajov

Dodávateľ je povinný vopred informovať Prevádzkovateľa, ak sa údaje Prevádzkovateľa premiestnia do iného dátového centra (vrátane záloh), než bolo pôvodne dohodnuté v Zmluve.

# PRÍSTUP K SYSTÉMOM A ZDROJOM prevádzkovateľa A ICH VYUŽITIE

Tento článok sa uplatňuje len v prípadoch, kedy Prevádzkovateľ poskytne Dodávateľovi na účely plnenia Zmluvy prístup a umožní mu použitie systémov Prevádzkovateľa.

Fyzický prístup

Ak Prevádzkovateľ poskytne prístup k vybaveniu a/alebo samotné vybavenie pre pripojenie, ktoré je/bude umiestnené v priestoroch Dodávateľa, Dodávateľ zabezpečí, aby:

* sa v technickom priestore, kde sa takéto zariadenie nachádza, uplatnilo riadenie fyzického prístupu,
* fyzický prístup k takému zariadenia bol obmedzený len na tie osoby, ktoré prístup k takémuto zariadenia potrebujú na účely plnenia Zmluvy a sú Dodávateľom riadne oprávnené a poučené o týchto Pravidlách.

Systémy Prevádzkovateľa

Dodávateľ pre ním riadené osoby zabezpečí:

* prístup k systémom Prevádzkovateľa a ich používanie výhradne za účelom poskytovania Plnenia,
* dodržiavanie spôsobov prístupu a pravidiel definovaných Prevádzkovateľom (vrátane pravidiel dobrej praxe) a vopred poskytnutých Dodávateľovi (napr. bude rešpektovať sieťové adresy pridelené Prevádzkovateľom, bude rešpektovať doby odozvy Prevádzkovateľa pre riadenie aktív Prevádzkovateľa,...),
  + v prípade využívania vzdialeného prístupu k systémom Prevádzkovateľa, dodržiavanie povinnosti Dodávateľa dodržiavať pravidlá, spôsoby a postupy špecifikované Prevádzkovateľom,
* aby každá osoba konajúca za Dodávateľa, ktorá potrebuje používať systémy Prevádzkovateľa, bola Dodávateľom riadne autorizovaná a aby jej identifikačné údaje boli poskytnuté Prevádzkovateľovi a zoznam konajúcich (oprávnených) osôb bol priebežne udržiavaný a aktualizovaný,
* aby k systémom Prevádzkovateľ boli pripojené iba riadne autorizované Zdroje Dodávateľa.

Zdroje Dodávateľa

Dodávateľ bude pristupovať k sieti Prevádzkovateľa len pomocou riešenia vzdialeného prístupu od Prevádzkovateľa.

Ak sa zdroje Dodávateľa používajú na prístup a/alebo prepojenie so systémami Prevádzkovateľa, Dodávateľ je povinný:

* dodržiavať osvedčené bezpečnostné postupy pri správe takýchto zdrojov (napr. udržiavať tieto zdroje v aktuálnom stave s najnovšími bezpečnostnými záplatami, ako sú záplaty antimalvérového softvéru a operačných systémov a nainštalovaného softvéru, konfigurovať obmedzené oprávnenia pre používateľov, konfigurovať obmedzené práva na vykonávanie na vymeniteľných médiách, zaviesť mechanizmy na blokovanie relácií na takýchto zdrojoch po krátkom čase nečinnosti, ...),
* zabezpečiť, aby Zdroje (vrátane autentifikačných tokenov, mobilných zariadení a súvisiacich telefónnych čísel) boli vyhradené Dodávateľovi a aby ich používali len jeho zamestnanci a všetky Tretie strany určené na poskytovanie Plnení),
* zaviesť kontrolu prístupu do siete na Zdrojoch Dodávateľa používaných na poskytovanie Služieb,
* implementovať silný autentifikačný systém (napr. dvojfaktorová autentifikácia) pre prístup k takýmto zdrojom; a zabezpečiť sledovateľnosť používania takýchto zdrojov všetkými používateľmi,
* uchovávať protokoly resp. logy po dobu dohodnutú v zmluve a/alebo Objednávke vrátane súvisiacich dokumentov (napr. zmluvy o mlčanlivosti alebo zmluvy o spracovaní údajov) alebo štandardne 6 mesiacov,
* na požiadanie poskytnúť Prevádzkovateľovi výpisy z uchovávaných protokolov resp. logov.

Systémy a aplikácie Prevádzkovateľa

Ak Prevádzkovateľ poskytne Dodávateľovi účty, je Dodávateľ povinný:

* bezodkladne Prevádzkovateľa informovať v prípade, keď daný užívateľský účet nie je naďalej vyžadovaný,
* zabezpečiť, aby účty poskytnuté pre serverovú komunikáciu boli používané výhradne na tento účel.

Riadenie Aktív Prevádzkovateľa

Ak Prevádzkovateľ poskytne Dodávateľovi Aktíva Prevádzkovateľa je Dodávateľ povinný takéto Aktíva Prevádzkovateľa evidovať a riadiť prístup k nim za uplatnenia náležitej klasifikácie takýchto Aktív. Obdobný prístup Dodávateľ uplatňuje aj v prípade spracúvania osobných údajov sprístupnených Prevádzkovateľom.

Ak Dodávateľ poskytuje Plnenia týkajúce kybernetickej bezpečnosti Prevádzkovateľa, je dodávateľ povinný:

* + dodržiavať pravidlá prepájania systémov Prevádzkovateľa a prenosu elektronických informácií,
  + riadiť bezpečnosť sietí a zmien infraštruktúry podľa pravidiel a pokynov Prevádzkovateľa,
  + uplatniť riadenie kapacity systémov a služieb podľa pravidiel a pokynov Prevádzkovateľa,
  + využívať riadené kryptografické opatrenia,

# ODBORNOSŤ PRACOVNÍKOV A BEZPEČNOSŤ

Školenie a vzdelávanie

Dodávateľ je povinný zabezpečiť, aby jeho zamestnanci a akékoľvek tretie osoby poverené poskytovaním Plnenia:

* disponovali zodpovedajúcimi schopnosťami v oblasti bezpečnosti (napr. aby boli schopní riešiť bezpečnostné incidenty),
* boli oboznámení s obsahom a implementáciou príslušných bezpečnostných pravidiel a všetky aktivity vykonávali podľa týchto pravidiel,
* dodržiavali mlčanlivosť o všetkých skutočnostiach a informáciách Prevádzkovateľa a podpísali prehlásenie o zachovávaní mlčanlivosti.

Špecifické bezpečnostné pravidlá Prevádzkovateľa

Ak Prevádzkovateľ určí osobitné bezpečnostné pravidlá Plnení týkajúcich sa kybernetickej bezpečnosti, je Dodávateľ povinný zabezpečiť, aby jeho zamestnanci a poverené tretie osoby boli pred začatím akýchkoľvek činností o takýchto pravidlách informované.

Subdodávky

Ak Dodávateľ plánuje využiť k Plneniu Zmluvy uzatvorenej s Prevádzkovateľom subdodávateľa, môže tak konať iba po predchádzajúcom súhlase Prevádzkovateľa, musí ich výslovne označiť ako subdodávateľa a zabezpečiť a zmluvne zaviazať, že bude z ich strany vždy vynakladaná minimálne rovnaká riadna starostlivosť akú je povinný vynakladať Dodávateľ. Takéto vynakladanie riadnej starostlivosti platí pre všetky subdodávateľské vzťahy vrátane akvizície, vývoja a údržby systémov a aplikácií. Prevádzkovateľ je oprávnený na základe individuálnych požiadaviek pravidelne kontrolovať aj dodržiavane týchto záväzkov zo strany Dodávateľa, ako aj jeho subdodávateľov.