Smlouva o dílo

Česká republika - Úřad pro ochranu osobních údajů
se sídlem Pplk. Sochora 27, 170 00 Praha 7
IČ: 70837627zastoupený: RNDr. Igorem Němcem, předsedou úřadu

(dále jen “Objednatel”)

a
AEC, spol. s r.o.
se sídlem Purkyňova 101, 612 00 Brno
IČ: 26236176, DIČ: CZ26236176
zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 38808
jednající Vítem Urbancem, jednatelem

(dále jen “Zhotovitel”)

uzavřeli tuto **Smlouvu o dílo** v souladu s ustanovením §2586 a násl. zákona č. 89/2012 Sb. občanský zákoník, v platném znění (dále jen “Smlouvu”).

Smluvní strany, vědomy si svých závazků v této smlouvě obsažených a s úmyslem být touto smlouvou vázány, dohodly se na následujícím znění Smlouvy:

1. Předmět Smlouvy

1.1 Zhotovitel se touto Smlouvou zavazuje provést pro Objednatele dílo, spočívající v poskytování definovaných činností externího bezpečnostního správce (dále jen „Dílo“) v rozsahu a za podmínek stanovených touto smlouvou.

Cílem těchto činností je zajistit bezpečnost dvou navzájem nezávislých informačních systémů, které Objednatel provozuje – Informačního systému Úřadu pro ochranu osobních údajů a Informačního systému ORG, který je provozován Objednatelem v rámci systému základních registrů ČR.

Podrobná specifikace Díla je obsažena v Příloze č. 1 Smlouvy.

2. Místo a termín provedení díla

2.1. Místem plnění Díla je sídlo Objednatele - Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7.

2.2. Zhotovitel se zavazuje provádět jednotlivé činnosti v rozsahu a v termínech dle dohody s Objednatelem.

3. Předání a převzetí díla

3.1. Předání a převzetí Díla probíhá prostřednictvím akceptační procedury, která zahrnuje porovnání skutečných vlastností Díla se specifikací Díla uvedenou Příloze č. 1 této Smlouvy.

4. Cena - Odměna a platební podmínky

4.1. Cena za předmět plnění byla stanovena dohodou smluvních stran jako roční částka 212 500,- Kč bez DPH (slovy dvě stě dvanáct tisíc pět set korun českých) splatná formou čtvrtletních plateb ve výši 53 125,- Kč bez DPH (slovy: padesát tři tisíc sto dvacet pět korun českých). Cena zahrnuje veškeré náklady Zhotovitele spojené s realizací Díla.

4.2. Objednatel se zavazuje cenu – odměnu za provedení Díla dle předchozího článku zaplatit na základě faktury vystavené Zhotovitelem k poslednímu dni příslušného kalendářního čtvrtletí. K dohodnuté ceně je Zhotovitel oprávněn připočítat částku DPH ve výši dle obecně závazných právních předpisů, účinných ke dni zdanitelného plnění.

4.3. Daňové doklady Zhotovitele musí obsahovat náležitosti daňového dokladu dle zákona č. 235/2004 Sb., o DPH, v platném znění. Pokud nebude daňový doklad (faktura) obsahovat všechny náležitosti stanovené příslušnými právními předpisy, je Objednatel oprávněn fakturu ve lhůtě její splatnosti vrátit s odůvodněním Zhotoviteli, a ten je povinen bezodkladně vystavit řádný daňový doklad (fakturu).

4.4. Doba splatnosti daňového dokladu (faktury) je stanovena na 14 kalendářních dnů ode dne doručení daňového dokladu Objednateli. V případě, že Objednatel oprávněně vrátí Zhotoviteli daňový doklad (fakturu) z důvodu, že neobsahuje všechny náležitosti stanovené příslušnými právními předpisy, běží lhůta splatnosti daňového dokladu až ode dne doručení opraveného daňového dokladu (faktury) vystavené Zhotovitelem.

Faktury se platí bankovním převodem na účet druhé smluvní strany uvedený ve faktuře.

4.5. V případě prodlení se zaplacením peněžité částky je smluvní strana, která je se zaplacením v prodlení, povinna zaplatit druhé smluvní straně smluvní pokutu za každý i započatý den prodlení ve výši 0,05 % z dlužné částky.

6. Oprávněné osoby

6.1. Každá ze smluvních stran jmenuje oprávněnou osobu či oprávněné osoby. Oprávněné osoby budou zastupovat smluvní stranu ve smluvních a obchodních záležitostech souvisejících s plněním této Smlouvy.

6.2. Jména oprávněných osob jsou uvedena v **Příloze č. 2** této Smlouvy. Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny na takovou změnu druhou smluvní stranu písemně upozornit.

7. Ochrana informací

7.1. Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Tato povinnost platí bez ohledu na ukončení účinnosti této Smlouvy. Strany mají právo požadovat navzájem doložení dostatečnosti utajení důvěrných informací. Strany jsou povinny zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty. Za porušení ochrany utajených informací se nepovažuje povinné zveřejnění smlouvy Objednatelem podle zvláštního zákona.

7.2. Právo užívat, poskytovat a zpřístupnit důvěrné informace mají obě strany pouze v rozsahu a za podmínek nezbytných pro řádné plnění práva a povinností vyplývajících z této Smlouvy.

7.3. Za důvěrné informace se bez ohledu na formu jejich zachycení považují veškeré informace, které nebyly některou ze stran označeny jako veřejné a které se týkají této Smlouvy a jejího plnění (zejména informace o právech a povinnostech stran jakož i informace o cenách), které se týkají některé ze stran (zejména obchodní tajemství, informace o jejich činnosti, struktuře, hospodářských výsledcích, know-how) anebo informace pro nakládání, s nimiž je stanoven právními předpisy zvláštní režim utajení (zejména hospodářské tajemství, státní tajemství, bankovní tajemství, služební tajemství). Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně některou ze stran označeny.

7.4. Za důvěrné informace se v žádném případě nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany, dále informace získané na základě postupu nezávislého na této Smlouvě nebo druhé straně, pokud je strana, která informace získala, schopna tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany.

7.5. Žádné ustanovení této Smlouvy přitom nebrání nebo neomezuje Zhotovitele ve zveřejnění nebo obchodním využití jakékoliv technické znalosti, dovednosti nebo zkušenosti obecné povahy, kterou získal při plnění této Smlouvy.

7.6. Zhotovitel je oprávněn užít informaci o existenci smluvního vztahu mezi účastníky této smlouvy pro účely svého marketingu a reklamy. Ustanovení této smlouvy o ochraně důvěrných informací tím není dotčeno.

7.7. Žádná ze smluvních stran není bez předchozího písemného souhlasu druhé smluvní strany oprávněna po dobu platnosti této Smlouvy a jeden rok po ukončení platnosti této Smlouvy zaměstnat zaměstnance druhé smluvní strany přímo nebo nepřímo, a to ani v subjektech, v nichž má rozhodující účast nebo možnost jiného způsobu ovlivňování rozhodování. „Zaměstnancem druhé smluvní strany“ se rozumí osoba, která jako konzultant nebo zaměstnanec jedné smluvní strany měla v jakoukoliv dobu vztah k plnění předmětu této Smlouvy. „Zaměstnáním“ zaměstnance druhé smluvní strany se rozumí uzavření pracovního nebo podobného poměru s daným zaměstnancem, či uzavření smluvního vztahu o poskytování služeb nebo provádění díla daným zaměstnancem přímo s daným zaměstnancem nebo s jakoukoliv jinou osobou. V případě porušení této povinnosti strana, která závazek vyplývající z tohoto odstavce Smlouvy porušila, zaplatí druhé smluvní straně 500.000,- Kč (slovy pět set tisíc korun českých) za každý případ porušení a to ve lhůtě pěti (5) dnů, kdy bude k zaplacení smluvní pokuty vyzvána. Součinnost a vzájemná komunikace

7.8. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

7.9. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob, statutárních orgánů smluvních stran, popř. jimi pověřených pracovníků.

8. Ukončení platnosti smlouvy č. 200600737

8.1. Obě smluvní strany souhlasí s ukončením platnosti Smlouvy č. 200600737 ze dne 28. 6. 2006 (o výkonu funkce externího bezpečnostního správce) ke dni 31. 3. 2014.

9. Platnost a účinnost Smlouvy

9.1. Tato Smlouva se uzavírá na dobu neurčitou a nabývá platnosti a účinnosti dnem 1. 4. 2014.

9.2. Každá ze smluvních stran této smlouvy je oprávněna smlouvu vypovědět vždy k 30. listopadu příslušného roku. Výpovědní doba činí 1 měsíc. Výpověď lze učinit pouze písemně, doručením druhé smluvní straně.

9.3. Každá ze smluvních stran této smlouvy je oprávněna od této smlouvy nebo její příslušné části odstoupit v případě jejího podstatného porušení druhou smluvní stranou.

9.4. Za podstatné porušení smlouvy Zhotovitelem se považuje zejména, jestliže Zhotovitel neprovádí dílo dohodnutým způsobem, nezjedná nápravu ani do patnácti (15) dnů od doručení písemného oznámení Objednatele o takovém pochybení nebo prodlení a tento postup nebo dosavadní výsledek provádění díla vedou nepochybně k opakovanému vadnému plnění.

9.5. Za podstatné porušení této smlouvy Objednatelem se považuje zejména, jestliže je Objednatel v prodlení s úhradou některé z faktur trvajícím déle než 15 dnů po lhůtě splatnosti, případně při jeho neposkytnutí potřebné součinnosti a spolupráce či neúměrně dlouhá odezva v poskytování potřebných informací ze strany Objednatele, která znemožňuje práci dokončit v dohodnutém termínu.

9.6. V případě odstoupení od smlouvy dle článku 9.3. uhradí Objednatel Zhotoviteli skutečně vynaložené náklady spojené se zhotovením díla ke dni zániku smlouvy a Zhotovitel předá objednateli všechny výsledky řešení dosažené ke dni zániku smlouvy.

10. Závěrečná ustanovení

10.1. Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných oprávněnými zástupci obou smluvních stran.

10.2. Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1 Specifikace Díla

Příloha č. 2 Oprávněné osoby

10.3. Tato Smlouva je uzavřena ve dvou (2) vyhotoveních, z nichž každá strana obdrží po jedno (1) vyhotovení.

10.4. Zhotovitel souhlasí s tím, aby subjekty oprávněné dle ZFK provedly finanční kontrolu závazkového vztahu vyplývajícího z této smlouvy s tím, že Zhotovitel se podrobí této kontrole a bude působit jako osoba povinná ve smyslu § 2 písm. e) ZFK;

Strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Zhotovitel	**Objednatel**
V Praze dne 18.3.2014	V Praze dne 20.3.2014
.....	.....

AEC, spol. s r.o.	**Úřad pro ochranu osobních údajů**
Vít Urbanec	RNDr. Igor Němec
Jednatel	Předseda

Příloha č. 1 - Specifikace Díla

Činnost	Popis	Frekvence (ročně)	MD/ činnost	MD celkem
Bezpečnostní fórum	Schůzky Bezpečnostního fóra úřadu a související agenda.	4	XXX	XXX
Aktualizace bezpečnostní dokumentace	Přezkoumání a aktualizace vybrané dokumentace úřadu, připomínky k vytvářené dokumentaci úřadu z pohledu bezpečnosti, návrhy na úpravy v dokumentaci apod.	1	XXX	XXX
Školení zaměstnanců ÚOOÚ	Příprava a realizace periodického prezenčního školení bezpečnosti pro běžné uživatele/zaměstnance úřadu. Školení je zpravidla prováděno v prostorách Úřadu.	1	XXX	XXX
Školení zaměstnanců OZI	Příprava a realizace periodického prezenčního školení bezpečnosti pro zaměstnance OZI.	1	XXX	XXX
Technická prověrka sítě (penetrační testy, skeny apod.)	Provedení penetračních testů vnitřní sítě, síťového perimetru nebo vybraných systémů úřadu dle dohodnutého rozsahu.	1	XXX	XXX
Kontrola dodržování bezpečnostních pravidel v rámci ÚOOÚ	Provedení kontroly v dohodnutém rozsahu, kontrola může být zaměřená na běžné uživatele (např. metodami sociálního inženýrství, kontrola na uživatele a jeho PC místě, audit uživatelských návyků apod.), na vybrané procesy v rámci úřadu apod.	1	XXX	XXX
Kontrolní činnost OZI/IS ORG	Provedení kontroly/auditu v rámci OZI/IS ORG v dohodnutém rozsahu, kontrola vychází z Bezpečnostní politiky IS ORG a souvisejících požadavků na IS ORG.	1	XXX	XXX
Analýza a vyhodnocení incidentů v rámci OZI/IS ORG	Sběr (na základě záznamů OZI, pohovorů apod.), analýza a vyhodnocení bezpečnostních incidentů v rámci IS ORG nebo souvisejících s IS ORG, určení dopadů a trendů incidentů, návrh protiopatření.	1	XXX	XXX
Roční zpráva	Vypracování souhrnné zprávy o činnosti externího bezpečnostního správce a informačně bezpečnostní situaci úřadu.	1	XXX	XXX
Individuální konzultace	Individuální konzultace dle aktuálních potřeb úřadu.	průběžně	XXX	XXX
Celkem za 1 rok				XXX

Veškeré služby/činnosti externího bezpečnostního správce jsou na straně AEC řízeny a koordinovány určenou kontaktní osobou (případně jejím určeným zástupcem). Hlavní kontaktní osobou na straně úřadu je náměstek Sekce informatiky a základních identifikátorů, případně pro jednotlivé činnosti další členové Bezpečnostního fóra úřadu.

Cílem všech činností je zajistit jednotlivým odborným úsekům úřadu komplexní podporu v oblasti informační a ICT bezpečnosti a zajistit tak potřebnou úroveň informační bezpečnosti úřadu, která je vzhledem k oboru působení úřadu nezbytným parametrem jeho fungování.

Bezpečnostní fórum

Bezpečností fórum (dále jen BF) představuje poradní, konzultační a koordinační orgán předsedy úřadu v oblasti informační a ICT bezpečnosti úřadu. BF typicky jedná ve složení externí bezpečnostní správce, Bezpečnostní ředitel úřadu, náměstek Sekce informatiky a základních identifikátorů (v roli interního bezpečnostního správce/managera), ředitelka Odboru základních registrů a ředitel Odboru informatiky. V rámci BF, které se schází na návrh kteréhokoliv ze členů, jsou projednávány veškeré záležitosti související jak s jednotlivými činnostmi externího bezpečnostního správce, tak i např. s bezpečnostními incidenty, změnami v rámci informačního systému, změnami v rámci organizace úřadu atd. Role externího bezpečnostního správce v rámci BF je zejména konzultační a podpůrná. BF se vždy účastní určená kontaktní osoba AEC (případně její zástupce), která zodpovídá mj. za vedení zápisu z jednání

Aktualizace bezpečnostní dokumentace

V rámci této činnosti provádí externí bezpečnostní správce na základě momentální potřeby úřadu přezkoumání a aktualizaci vybrané bezpečnostní (nebo související) interní dokumentace úřadu, připomínkuje vytvářenou dokumentaci úřadu z pohledu bezpečnosti, připravuje návrhy na úpravy v dokumentaci, případně provádí v určeném rozsahu přípravu zcela nové dokumentace apod.

Dokumentace, která je předmětem této činnosti a rozsah prací externího bezpečnostního správce (AEC) určuje BF v rámci svého jednání.

Externí bezpečnostní správce v rámci této činnosti dbá zejména na to, aby dokumentace úřadu byla v souladu s platnými bezpečnostními standardy, požadavky legislativy ČR, současnou nejlepší praxí (best practice) a současně byla efektivní a účinná.

Školení zaměstnanců ÚOOÚ

V rámci této činnosti externí bezpečnostní správce připravuje a prezenční formou realizuje periodické školení informační bezpečnosti pro běžné uživatele/zaměstnance úřadu. Školení je prováděno 1 x ročně zpravidla v prostorách úřadu.

Obsah školení je sestavován na základě aktuální bezpečnostní situace, zejména např. výskytu aktuálních bezpečnostních hrozeb, minulých bezpečnostních incidentů a na základě dalších aktuálních trendů v oblasti bezpečnosti. Školení je typicky rozděleno do následujících částí:

- Vysvětlení důležitosti zajišťování bezpečnosti informací a ICT, základní pojmy z oblasti bezpečnosti.
- Seznámení s aktuálními bezpečnostními hrozbami, útoky apod.
- Přehled nejdůležitějších bezpečnostních pravidel a uživatelských bezpečnostních návyků, které by měli uživatelé znát a dodržovat.
- Přehled zásad pro používání vybraných bezpečnostních nástrojů a technologií z pohledu běžného uživatele.
- Shrnutí nejdůležitějších bezpečnostních zásad (tzv. desatero bezpečnosti).

Obsah školení je vždy připravován v předstihu a je připomínkován interním bezpečnostním správcem. Výstupem je kromě samotné realizace školení vždy prezentace ve formátu ppt, která je poskytnuta úřadu pro další využití.

Školení je prováděno zkušeným lektorem, který má s realizací bezpečnostních školení dlouholetou praxi. Samotné školení je prováděno v rozsahu 1 až 2 hodiny. V případě potřeby může být školení rozděleno do více samostatných běhů.

Školení pracovníků OZI

V rámci této činnosti externí bezpečnostní správce připravuje a prezenční formou realizuje periodické školení pracovníků Odboru základních identifikátorů (dále jen OZI). Školení je prováděno 1 x ročně zpravidla v prostorách úřadu.

Obsah školení je sestavován na základě aktuální bezpečnostní situace, zejména např. výskytu aktuálních bezpečnostních hrozeb, minulých bezpečnostních incidentů v rámci OZI a na základě dalších aktuálních trendů v oblasti bezpečnosti. Obsah školení přizpůsobován momentálním potřebám pracovníků OZI.

Obsah školení je vždy připravován v předstihu a je připomínkován ředitelkou OZI. Výstupem je kromě samotné realizace školení vždy prezentace ve formátu ppt, která je poskytnuta úřadu pro další využití.

Školení je prováděno zkušeným lektorem, který má s realizací bezpečnostních školení dlouholetou praxi. Samotné školení je prováděno v rozsahu 2 až 4 hodiny.

Technická prověrka sítě

Tato činnost zahrnuje provedení penetračních testů a/nebo technických auditů vybraných částí infrastruktury informačního systému nebo aplikací či jiných ICT technologií úřadu. Může se jednat např. o interní penetrační test vnitřní sítě úřadu, externí penetrační test síťového perimetru, audit nastavení firewallu úřadu, prověrku určité aplikace apod.

Technická prověrka sítě se provádí 1 x ročně. Rozsah prověrky je zpravidla určován v rámci jednání BF na základě aktuálních potřeb úřadu. Jednotlivé testy jsou následně prováděny v úzké koordinaci s Odborem informatiky, mj. s ohledem na případný dopad na fungování informačního systému úřadu.

Výstupem činnosti je vždy detailní zpráva, která je připomínkována Odborem informatiky, případně dalšími stranami. Obsahem detailní zprávy jsou konkrétní zjištění související s jednotlivými zkoumanými oblastmi. Detailní zpráva obsahuje následující informace:

- Cíl a rozsah testu.
- Popis předmětu testu.
- Stanovení stupnice a metodiky hodnocení – kategorizace zjištěných zranitelností a jejich přehledné značení v rámci dokumentu.
- Detailní postup provedených testů včetně nástrojů a technik použitých v jednotlivých fázích.
- Popis nalezených zranitelnosti, každá v členění uvedeném níže.
- Doporučení pro odstranění identifikovaných slabin a zranitelných míst.
- Závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti testovaných aplikací.

Všechny identifikované zranitelnosti jsou popsány v následující struktuře:

- **hodnocení/kategorizace** zranitelnosti - veškeré nalezené problémy a zranitelnosti jsou rozděleny do pěti kategorií podle závažnosti:

C - kriticky závažná chyba (KRITICKÁ) – CRITICAL

Jako kritické chyby jsou označeny nedostatky, které byly při testech zneužity a vedly (mohou vést) k přímé kompromitaci testovaného systému.

H - závažné chyby (VYSOKÁ) – HIGH

Jako závažné klasifikujeme chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. U těchto chyb existuje velmi vysoká pravděpodobnost zneužití. Jejich okamžitá náprava je nutná.

 - středně závažné chyby (STŘEDNÍ) – MEDIUM

Do této kategorie spadají chyby, jejichž využití k potenciálnímu útoku na IS je technologicky náročnější na realizaci, nebo které umožňují průnik do systému pouze v případě splnění několika určitých navzájem souvisejících podmínek. Jejich závažnost nelze podceňovat s ohledem na potenciálně hrozící zneužití.

 - méně závažné chyby (NÍZKÁ) – LOW

Tato kategorie zahrnuje méně závažné chyby, které napomáhají napadení systému. Např. poskytují potenciálnímu útočníkovi informace, jež lze uplatnit v rámci útoku na IS – organizace o svém IS prozrazuje více, než je nezbytně nutné. Ve většině případů se jedná pouze o konfigurační opomenutí apod.

 - (INFORMATIVNÍ) – INFO

Informativní kategorie označuje vše, co lze zjistit o systémech a sítích, aniž by bylo možné jakýmkoliv způsobem zabránit úniku těchto informací. Tyto údaje nejsou většinou příliš důležité pro vedení vlastního útoku, ale mnohdy mohou napomoci útočníkovi při dokreslení či doplnění celkového obrazu o cíli potenciálního napadení.

- **Klasifikace dle schopnosti útočníka -** skill, neboli schopnosti útočníka, je klasifikace, která popisuje nároky kladené na schopnosti a znalosti útočníka pro realizaci daného útoku.

Pro identifikaci a případné zneužití zranitelnosti postačují základní znalosti a schopnosti uživatele – útočníka. Ke zneužití může dojít také neúmyslnou chybou nebo náhodným jednáním.

Středně obtížná náročnost s využitím automatizovaných nástrojů. Technicky zdatní útočníci, kteří s větší mírou využívají manuální metody útoku, případně převzaté skripty.

Velmi znalí a zkušení útočníci, kteří k útokům používají úzce specializované a sofistikované nástroje. Jedná se o přesně cílené útoky.

- **zjištění** – popis zranitelného místa/nálezu včetně popisu kde a jakým způsobem byla zranitelnost identifikována;
- **riziko** – popis rizik plynoucích z možného zneužití zranitelného místa včetně možných scénářů zneužití (kdo a za jakých podmínek je možné zranitelnost zneužít a jaké jsou možné dopady tohoto zneužití), posouzení dopadu rizika na produkční prostředí;
- **doporučení** – doporučení vedoucí k odstranění nalezených nedostatků, případně návrhy na zvýšení bezpečnosti stávajících bezpečnostních mechanismů a opatření. Tato doporučení se mohou týkat procesních změn, konfigurace zařízení (hardening systémů), návrhu nových bezpečnostních mechanismů pro zvýšení stávající úrovně bezpečnosti, doporučení pro uživatelská PC pro zvýšení bezpečnosti atd.
- **přílohy** (výstupy z použitých nástrojů, důkazy apod.).

Kontrola dodržování bezpečnostních pravidel v rámci ÚOOÚ

Předmětem této činnosti/služby je provedení kontroly v dohodnutém rozsahu. Kontrola může být zaměřená např. na prověření úrovně bezpečnostního povědomí uživatelů IS (např. metodami sociálního inženýrství), prověření dodržování stanovených bezpečnostních pravidel úřadu (kontrola na pracovišti uživatele formou interview a kontrola jeho PC), kontrola a analýza vybraných logů (např. logů antivirové ochrany, logů z web proxy apod.), kontrola fungování vybraných procesů v rámci úřadu z hlediska bezpečnosti apod.

Kontrola se provádí 1 x ročně. Rozsah a způsob konkrétní kontroly je dojednán v rámci jednání BF, kde externí bezpečnostní správce (resp. kontaktní osoba AEC) navrhuje na základě námětů a požadavků dalších členů BF možný postup. Samotná kontrola je koordinována a prováděna ve spolupráci s Odborem informatiky.

Výstupem činnosti je zpráva v obdobné struktuře jako zpráva z technické prověrky sítě, tzn., popisuje rozsah, postup a konkrétní zjištění kontroly. Zpráva podléhá připomínkovému řízení.

Kontrolní činnost OZI/IS ORG

Předmětem této činnosti/služby je provedení kontroly/auditu v rámci OZI. Audit je prováděn 1 x ročně. Rozsah a zaměření auditu je dojednáno v rámci jednání BF. Audit vychází zejména z požadavků Bezpečnostní politiky IS ORG a souvisejících požadavků na IS ORG. Dále jsou v rámci auditu zohledňovány požadavky aktuálních bezpečnostních standardů, požadavky vyplývající z legislativy ČR i tzv. nejlepší praxe. Provádění auditu je koordinováno s Odborem základních identifikátorů.

Výstupem činnosti je zpráva v obdobné struktuře jako zpráva z technické prověrky sítě, tzn., popisuje rozsah, postup a konkrétní zjištění auditu. Zpráva podléhá připomínkovému řízení.

Analýza a vyhodnocení incidentů v rámci OZI/IS ORG

Předmětem této činnosti/služby je sběr, analýza a vyhodnocení bezpečnostních incidentů, případně dalších bezpečnostních událostí v rámci IS ORG resp. OZI. Sběr je prováděn na základě existujících záznamů OZI, pohovorů se zaměstnanci apod. Na základě zjištěných skutečností je následně provedena analýza a vyhodnocení bezpečnostních incidentů s ohledem na určení míry rizika a dále i na určení dopadů a trendů incidentů. Na základě této analýzy je zpracován návrh protiopatření.

Analýza je prováděna 1 x ročně v součinnosti s Odborem základních identifikátorů. Výstupem činnosti je zpráva, která popisuje jednotlivá konkrétní zjištění analýzy a obsahuje návrh doporučených protiopatření současně s návrhem způsobu jejich implementace. Zpráva podléhá připomínkovému řízení.

Roční zpráva

Účelem roční zprávy je informovat vedení úřadu o realizovaných činnostech externího bezpečnostního správce a o aktuálním celkovém stavu informační bezpečnosti úřadu. Dále je v rámci zprávy navrženo, jakým způsobem v budování informační a ICT bezpečnosti ICT pokračovat v dalším období.

Zprávu zpracovává externí bezpečnostní správce 1 x ročně – vždy na závěr kalendářního roku (tj. po provedení jednotlivých činností). Podkladem pro vypracování zprávy jsou nejen výstupy z činností, ale také další aktuální informace z oblasti bezpečnosti (nové a potenciální hrozby, nové technologie apod.). Zpráva tedy neshrnuje jen aktuální stav bezpečnosti úřadu, ale také navrhuje další postup při jejím budování a posilování.

Zpráva je projednána v rámci BF, jehož ostatní členové mohou vznášet připomínky a náměty, které externí bezpečnostní správce po diskusi zapracovává do zprávy. Definitivní podoba zprávy je poté předána (případně prezentována) vedení úřadu prostřednictvím interního bezpečnostního správce.

Individuální konzultace

Předmětem této činnosti/služby jsou individuální konzultace v oblasti bezpečnosti informací a ICT dle aktuálních potřeb úřadu.

Požadavky na individuální konzultace jsou předkládány v rámci jednání BF a jsou schvalovány interním bezpečnostním správcem (náměstkem Sekce informatiky a základních identifikátorů). Koordinátor za AEC následně zajistí realizaci konzultačních prací, případně jiných prací, v dohodnutém rozsahu.

Příloha č. 2 - Oprávněné osoby

Pro obchodní jednání:

za Zhotovitele:

za Objednatele:

I

Pro provádění Díla:

za Zhotovitele:

za Objednatele: