



## SMLOUVA O DÍLO

podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „NOZ“),  
(tato smlouva o dílo dále jen „smlouva“)

### I. SMLUVNÍ STRANY



KUJIP0193HGG

#### Objednatel: Kraj Vysočina

Sídlo: Žižkova 1882/57, Jihlava, PSČ 587 33  
Zastoupený hejtmánem panem MUDr. Jiřím Běhounkem  
Bankovní spojení: Sberbank CZ, a.s. číslo účtu: 4200473310/6800  
IČO: 70890749 DIČ: CZ70890749  
Tel: 564 602 111 Fax: 564 602 420  
E-mail: posta@kr-vysocina.cz ID datové schránky: ksab3eu  
Kontaktní osoba objednatele ve věcech technických dle této smlouvy je:  
Ing. Petr Pavlinec, e-mail: pavlinec.p@kr-vysocina.cz, tel.: 564602114  
(dále jen „objednatel“)

#### Zhotovitel: Expect-IT, s. r. o.

Sídlo: Staňkova 103/18, Brno, 602 00  
Zapsaný v OR vedeném u Krajského soudu v Brně, oddíl C, vložka 48755  
Zastoupený jednatelkou paní Mgr. Radanou Šrubařovou  
Bankovní spojení: Československá obchodní banka, a.s. číslo účtu: 195799130/0300  
IČO: 26966603 DIČ: CZ26966603  
Tel: +420 724 753 662 Fax: ---  
E-mail: info@expect-it.cz ID datové schránky: 85h5gkv  
Kontaktní osoba zhotovitele ve věcech technických dle této smlouvy je:  
RNDr. Michal Batko, PhD., email: mbatko@expect-it.cz, tel.: +420 724 753 662  
Zdeněk Havelka, email: havelka@expect-it.cz, tel.: +420 734 220 300  
RNDr. Libor Škarvada, email: skarvada@expect-it.cz, tel.: +420 734 739 550  
(dále jen „zhotovitel“)

### II. ÚVODNÍ USTANOVENÍ

1. Smluvní strany prohlašují, že tato smlouva je uzavřena na základě výsledků zadávacího řízení veřejné zakázky s názvem „Bezpečnostní dashboard – III. vyhlášení“ (dále jen „veřejná zakázka“). Jednotlivá ustanovení této smlouvy tak budou vykládána v souladu se zadávacími podmínkami veřejné zakázky.
2. Předmět díla dle této smlouvy je spolufinancován formou účelové dotace v rámci Integrovaného operačního programu pro projekt s názvem: „Služby Technologického centra Kraje Vysočina 2014, registrační číslo CZ.1.06/2.1.00/19.09272, prioritní osa: 6.2 Zavádění ICT v územní veřejné správě - Cíl Konvergence (dále též jen „projekt“). Konkrétně tato zakázka řeší část projektu nazvanou Bezpečnostní dashboard. Tato veřejná zakázka je spolufinancována ze zdrojů Evropské unie a Evropského fondu pro regionální rozvoj v rámci Integrovaného operačního programu. Zadávací řízení veřejné zakázky bylo realizováno v souladu s pravidly v předchozí větě uvedeného Integrovaného operačního programu.



3. Zhotovitel prohlašuje, že je způsobilý k řádnému a včasnému provedení díla dle této smlouvy a že disponuje takovými kapacitami a odbornými znalostmi, které jsou třeba k řádnému provedení díla. Pověří-li zhotovitel provedením díla jinou osobu, má zhotovitel při provádění díla jinou osobou odpovědnost, jako by dílo prováděl sám.
4. Zhotovitel dále prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Rovněž prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek zhotovitele a že takové řízení nebylo vůči němu zahájeno.
5. Smluvní strany prohlašují, že identifikační údaje uvedené v čl. I této smlouvy odpovídají aktuálnímu stavu, a že osobami jednajícími při uzavření této smlouvy jsou osoby oprávněné k jednání za smluvní strany. Jakékoliv změny údajů uvedených v čl. I této smlouvy, jež nastanou v době po uzavření této smlouvy, jsou smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé smluvní straně.
6. V případě, že se kterékoliv prohlášení některé ze smluvních stran podle tohoto článku ukáže být nepravdivým, odpovídá tato smluvní strana za škodu a nemajetkovou újmu, která nepravdivostí prohlášení nebo v souvislosti s ní druhé smluvní straně vznikla.

### III. PŘEDMĚT SMLOUVY

Zhotovitel se zavazuje provést na svůj náklad a nebezpečí ve sjednaném termínu dále specifikované dílo a objednatel se zavazuje dokončené dílo převzít a zaplatit za něj sjednanou cenu. Zhotovitel se zavazuje postupovat při plnění této smlouvy v souladu s podmínkami a pravidly Integrovaného operačního programu.

### IV. PŘEDMĚT DÍLA

1. Zhotovitel se zavazuje provést pro objednatele dílo specifikované v této smlouvě a jejích přílohách, dle podmínek stanovených touto smlouvou a jejími přílohami (dále jen „*dílo*“).
2. Součástí díla jsou veškeré práce, dodávky, služby, činnosti a výkony, kterých je třeba trvale nebo dočasně k zahájení, dokončení a předání díla a k uvedení díla do řádného provozu, není-li v této smlouvě výslovně uvedeno jinak.
3. Zhotovitel je povinen zajistit veškeré nezbytné doklady, prohlídky a přejímky, spojené s prováděním díla, vyžadované touto smlouvou a jejími přílohami, platnými právními předpisy nebo orgány státní správy.
4. Rozsah a kvalita díla jsou dále dány příslušnými ČSN a předpisy platnými v době provádění díla, případně dalšími podmínkami objednatele sjednanými v této smlouvě.
5. Zhotovitel prohlašuje, že před podpisem této smlouvy převzal a seznámil se s přílohami této smlouvy a místem plnění a že s ohledem na své znalosti a zkušenosti provede dílo dle smlouvy

a jejich příloh, aby mohlo být řádně užíváno k účelu, k němuž má být provedeno. Zhotovitel je povinen v rámci plnění dle této smlouvy provést veškeré práce, dodávky, služby, činnosti a výkony, kterých je třeba trvale nebo dočasně k zahájení, dokončení a předání díla a k uvedení díla do řádného provozu.

6. Zhotovitel je při provádění díla vázán pokyny objednatele, pokud objednatel zhotoviteli takové pokyny udělí.
7. Změny díla, včetně provedení veškerých víceprací, méněprací, změny technologií nebo materiálů, doplňky, rozšíření či zúžení díla, je možné činit pouze za podmínek stanovených zákonem č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**zákon o veřejných zakázkách**“) a musí být vždy sjednány předem ve formě písemného dodatku k této smlouvě.

#### V. MÍSTO A TERMÍNY PLNĚNÍ

1. Místem plnění je sídlo objednatele Žižkova 57, Jihlava (dále jen „**místo plnění**“).
2. Jednotlivé části díla budou dodávány dle následujícího harmonogramu:

Fáze	Obsah plnění	Lhůta plnění
Fáze 1 – vyhotovení implementační analýzy	Zhotovitel zahájí plnění	Ihned po nabytí účinnosti této smlouvy
	Zhotovitel předá objednateli řádně dokončenou „ <i>Implementační analýzu včetně návrhu řešení</i> “ – vyhotovení akceptačního protokolu	Do 10 týdnů od nabytí účinnosti této smlouvy
Fáze 2 – implementace	Předání a převzetí řádně dokončeného díla bez vad a nedodělků – vyhotovení protokolu o předání a převzetí díla	Nejpozději do <b>31. 8. 2015</b>

3. Jestliže nevhodné nebo neúplné podklady nebo pokyny brání v řádném provádění díla, zhotovitel tyto skutečnosti bezodkladně oznámí objednateli a v nezbytném rozsahu přeruší provádění díla do doby změny nebo doplnění podkladů nebo pokynů objednatelem nebo do doby doručení písemného sdělení objednatele, že trvá na provádění díla s použitím předaných podkladů nebo za dodržování jeho pokynů. Zhotovitel je povinen pokračovat v provádění díla v rozsahu, ve kterém mu v tom nebrání nevhodné nebo neúplné podklady nebo pokyny. O dobu, po kterou bylo nutné provádění díla přerušit z důvodů uvedených v tomto odstavci, se prodlužuje doba pro předání a převzetí dokončeného díla.

## VI. PŘEDÁNÍ A PŘEVZETÍ DÍLA

1. Dluh zhotovitele provést dílo podle této smlouvy je splněn jeho řádným a včasným dokončením, včetně provedení zkušebního provozu, je-li touto smlouvou, jejími přílohami nebo objednatelem požadován, a předáním objednateli, včetně předání veškerých dokladů nezbytných k užívání díla a dokladů stanovených platnými právními předpisy, normami, a rozhodnutími orgánů veřejné moci, tj. zejména:
  - dokumenty osvědčující průběh zkušebního provozu;
  - návody k obsluze, návody k použití k dodávané technologii a SW v českém jazyce.
2. V případě, že platné právní předpisy nebo platné technické normy předepisují provedení zkoušek, revizí, atestů a měření či zajištění prohlášení o shodě týkajících se díla, je zhotovitel povinen zajistit jejich úspěšné provedení před předáním díla objednateli.
3. Objednatel dílo převezme za předpokladu, že je dílo dokončené, a že odpovídá této smlouvě, je plně funkční, a je prosté vad a nedodělků s výjimkou ojedinělých drobných vad a nedodělků, jež nebrání řádnému užívání díla.
4. O předání a převzetí díla bude smluvními stranami sepsán protokol, který bude obsahovat zhodnocení prací, soupis zjištěných vad a nedodělků, dohodnuté doby k jejich odstranění nebo jiná opatření (byla-li dohodnuta) a soupis dokladů předávaných zhotovitelem objednateli při předání díla (dále též „**předávací protokol**“). Pokud zhotovitel vady a nedodělky, uvedené v předávacím protokolu v dohodnuté době neodstraní, je objednatel oprávněn zajistit odstranění vad a nedodělků třetí osobou. Zhotovitel je povinen uhradit objednateli škodu i nemajetkovou újmu, která objednateli vznikla, včetně škody v podobě vynaložení nákladů na odstranění takových vad a nedodělků.
5. V případě, že objednatel dílo nepřevzme, bude mezi smluvními stranami sepsán zápis s uvedením důvodu nepřevzetí díla a s uvedením stanovisek obou smluvních stran. V případě nepřevzetí díla dohodnou smluvní strany dobu k odstranění vad nebo nedodělků a náhradní termín předání a převzetí díla.
6. Zhotovitel se zavazuje řádně odstranit veškeré vady a nedodělky, jež vyplynou z přejímacího řízení, a to v termínu stanoveném v předávacím protokolu. V případě nepřevzetí díla objednatelem je zhotovitel povinen řádně odstranit veškeré vady a nedodělky v době sjednané v zápisu o nepřevzetí díla podle odst. 5 tohoto článku. Nebude-li termín odstranění vady nebo nedodělku v předávacím protokolu nebo v zápisu o nepřevzetí díla stanoven, je zhotovitel povinen vadu nebo nedodělek odstranit nejpozději do 14 kalendářních dnů ode dne oboustranného podpisu předávacího protokolu, resp. zápisu o nepřevzetí díla. O odstranění vad a nedodělků sepíší smluvní strany protokol.

## VII. CENA DÍLA

1. Smluvní strany se dohodly, že celková cena za dílo činí **1 239 668,00 Kč bez DPH** (slovy: jeden milion dvě stě třicet devět tisíc šest set šedesát osm korun českých). Tato cena je podrobně rozčleněna v položkovém rozpočtu, který je přílohou č. 2 této smlouvy (dále jen „**položkový rozpočet**“).

2. V případě rozporu ceny uvedené v předchozím odstavci a ceny vyplývající z položkového rozpočtu je rozhodující cena uvedená v předchozím odstavci. Cena je stanovena jako závazná, nejvýše přípustná a nepřekročitelná s výjimkou změny platných daňových právních předpisů týkajících se DPH. Do ceny jsou zahrnuty veškeré náklady či poplatky a další výdaje, které zhotoviteli při realizaci díla vzniknou nebo mohou vzniknout.
3. V ceně díla je zahrnuta cena za veškeré práce, dodávky, služby, činnosti a výkony, kterých je třeba pro včasné a kompletní provedení díla a k uvedení díla do řádného provozu a veškeré další náklady zhotovitele, nutné pro včasné a kompletní provedení díla dle této smlouvy, včetně nákladů na zkušební provoz, je-li touto smlouvou, jejími přílohami nebo objednatelům požadován. V ceně díla je taktéž zahrnuto vypracování veškeré dokumentace ve smyslu čl. VI odst. 1 této smlouvy.
4. Objednatel je povinen zaplatit zhotoviteli pouze cenu díla dle zhotovitelem skutečně provedených prací, dodávek a služeb.

### VIII. FAKTURACE A PLATEBNÍ PODMÍNKY

1. Cena díla bude zaplacená do 30 dnů po předání a převzetí díla nebo části díla uvedené v předávacím protokolu a po odstranění veškerých vad a nedodělků vytknutých v předávacím protokolu.
2. Zhotovitel je povinen na částku odpovídající ceně díla vystavit daňový doklad (dále jen „*faktura*“) v souladu s § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „*zákon o DPH*“). Bude-li na faktuře uvedena doba splatnosti, musí odpovídat době, v níž je objednatel povinen zaplatit cenu díla dle předchozího odstavce.
3. Vystavená faktura musí splňovat náležitosti daňového dokladu dle § 29 zákona o DPH, náležitosti stanovené § 13a obchodního zákoníku 435 NOZ a náležitosti stanovené touto smlouvou vč. dohodnutých příloh a nedílných součástí. Dále musí být na faktuře uveden celý název a registrační číslo projektu, projekt je spolufinancovaný z Integrovaného operačního programu.
4. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost vč. dohodnutých příloh nebo nedílných součástí, nebo bude-li chybně stanovena cena, DPH nebo jiná náležitost faktury, je objednatel oprávněn tuto fakturu vrátit zhotoviteli k provedení opravy s vyznačením důvodu vrácení. Zhotovitel provede opravu vystavením nové faktury.
5. Bankovní účet uvedený zhotovitelem na jím vystaveném daňovém dokladu za účelem úhrady ceny díla musí odpovídat bankovnímu účtu zveřejněnému dle ustanovení § 98 zákona o DPH příslušným správcem daně způsobem umožňujícím dálkový přístup. V opačném případě je objednatel zhotovitelem vystavený daňový doklad za podmínek dle předchozího odstavce zhotoviteli vrátit.
6. Objednatel je oprávněn provést úhradu ceny díla zhotoviteli tak, že zhotoviteli bude uhrazena cena díla bez daně z přidané hodnoty, přičemž částka připadající na úhradu daně z přidané hodnoty bude objednatelům za zhotovitele v souladu s ustanovením § 109a zákona o DPH uhrazena přímo na účet příslušného správce daně.

7. Objednatel je oprávněn využít své právo přímé úhrady daně z přidané hodnoty u každého jednotlivého daňového dokladu vystaveného zhotovitelem, přičemž na základě písemné žádosti doloží objednatel zhotoviteli provedení úhrady příslušné částky na účet správce daně. Smluvní strany sjednávají, že v případě využití oprávnění objednatele dle tohoto ustanovení nevzniká zhotoviteli nárok na úhradu částky připadající na daň z přidané hodnoty dle příslušného daňového dokladu.
8. Okamžikem zaplacení ceny díla se rozumí datum odepsání příslušné částky, odpovídající ceně díla, z účtu objednatele ve prospěch účtu zhotovitele.
9. Veškeré úhrady objednatele na základě této smlouvy budou prováděny bezhotovostním převodem na bankovní účet zhotovitele uvedený v čl. I. této smlouvy.

### IX. PŘECHOD VLASTNICKÉHO PRÁVA, NEBEZPEČÍ ŠKODY NA DÍLE

1. Vlastnické právo ke zhotovovanému dílu má bez jakýchkoliv výjimek od počátku objednatel, přičemž vlastnické právo na jakoukoliv část díla přechází na objednatele jejím zabudováním do díla, popřípadě instalací či montáží v místě plnění. Objednatel zůstává vlastníkem díla i v případě zániku závazku z této smlouvy jinak než splněním, např. odstoupením některé ze smluvních stran od této smlouvy.
2. Nebezpečí škody na díle nese zhotovitel. Nebezpečí škody na díle přechází na objednatele okamžikem oboustranného podpisu předávacího protokolu. Smluvní strany se dohodly, že § 1976 se nepoužije.

### X. LICENČNÍ UJEDNÁNÍ (VARIANTA 1 – POVINNÉ MINIMUM)

1. Ke všem částem díla, které mají povahu autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**autorský zákon**“), a k nimž zhotovitel má nebo mu vznikne majetkové autorské právo, poskytuje zhotovitel objednateli licenci ke všem způsobům užití známým ke dni uzavření této smlouvy, a to s účinností ode dne přechodu vlastnického práva k věci, v níž bylo konkrétní autorské dílo zahrnuto, nejpozději však ode dne dokončení díla.
2. Licenci dle předcházejícího odstavce této smlouvy zhotovitel uděluje objednateli jako bezúplatnou, nevýhradní, na dobu trvání majetkových práv autora, v neomezeném územním rozsahu. Zhotovitel uděluje objednateli oprávnění k zapracování, sloučení nebo připojení autorských děl a jejich částí, dodaných zhotovitelem dle této smlouvy, do systémů objednatele nebo do jakýchkoliv jiných systémů dle potřeb a vůle objednatele.
3. Zhotovitelem udělená licence se vztahuje ve shora uvedeném rozsahu i na jakékoli rozšíření, upgrady, updaty a další změny autorských děl, jsou-li dodány zhotovitelem dle této smlouvy.
4. Zhotovitel se zavazuje učinit všechna nezbytná opatření nutná pro zabezpečení nerušeného výkonu práv vyplývajících z této smlouvy pro objednatele.

5. Zhotovitel prohlašuje, že je oprávněn udělit licence uvedené v tomto článku. Pokud zhotovitel zjistí, že nebude moci dostát prohlášení dle předchozí věty, je povinen na takovou skutečnost objednatele neprodleně písemně upozornit. Zhotovitel odpovídá objednateli za jakoukoliv škodu, nemajetkovou újmu či náklady, včetně veškerých výdajů na odbornou právní pomoc, vyplývající z jakéhokoli porušení autorských a jiných práv duševního vlastnictví zhotovitele nebo třetích osob užíváním autorských děl dodaných zhotovitelem za účelem provedení díla.

## XI. ZÁRUČNÍ PODMÍNKY

1. Zhotovitel odpovídá za to, že dílo je provedeno řádně v souladu s touto smlouvou a jejími přílohami, ČSN a platnými právními předpisy.
2. Zhotovitel poskytuje záruku za jakost díla (dále jen „záruka“). Pokud nejsou délka záruky a počátek jejího běhu v konkrétních případech výslovně sjednány jinak, záruční doba na celé dílo činí 60 měsíců a počíná běžet ode dne oboustranného podpisu předávacího protokolu v případě, že dílo bylo předáno bez vad a nedodělků (dále jen „záruční doba“). V případě, že dílo bylo předáno s drobnými vadami a nedodělků, jež nebrání řádnému užívání díla, počíná záruční doba běžet ode dne odstranění takových vad a nedodělků.
3. Zhotovitel poskytuje záruku, že dílo a všechny jeho součásti budou po celou dobu trvání záruční doby splňovat sjednané technické parametry a budou v souladu s příslušnými normami a předpisy, touto smlouvou, jejími přílohami a platnými právními předpisy.
4. Záruka se vztahuje na všechny vady, jež se projeví jako rozpor s ustanovením odstavců 2 a 3 tohoto článku v záruční době (dále jen „záruční vady“), s výjimkou vad díla:
  - způsobených výlučně objednatelem nebo třetími osobami. Výluka dle předchozí věty se nevztahuje na vady, které se vyskytnou v důsledku zásahu do díla objednatelem nebo jím pověřenou třetí osobou v případě, kdy zhotovitel neplní svoji povinnost provádět činnosti uvedené v odstavci 5 a 6 tohoto článku a objednatel využije svého práva dle odst. 7 tohoto článku provést příslušné činnosti sám nebo prostřednictvím třetí osoby;
  - jež byly způsobeny po přechodu nebezpečí škody na díle vnějšími událostmi a nezpůsobil je zhotovitel nebo osoby, s jejichž pomocí zhotovitel plnil svůj závazek.
5. Zhotovitel je povinen bez zbytečného odkladu, nejpozději do 3 kalendářních dnů po oznámení vady objednatelem zhotoviteli, dostavit se po předchozí dohodě na místo stanovené objednatelem v oznámení vady, a není-li takové místo určeno, pak do sídla objednatele, za účelem projednání reklamace vad a v téže době objednateli písemně sdělit, zda jsou oznámené vady záručními vadami nebo zda jde o vady mimozáruční. Pokud tak zhotovitel neučiní, má se za to, že jde o záruční vady. Pokud zhotovitel sdělí, že reklamované vady jsou vadami mimozáručními, je objednatel oprávněn vady odstranit sám nebo prostřednictvím třetí osoby. Ukáže-li se, že reklamované vady, o nichž zhotovitel sdělil, že jsou vadami mimozáručními, a jež objednatel odstranil dle předchozí věty, byly záručními vadami, je zhotovitel povinen uhradit objednateli škodu i nemajetkovou újmu, která objednateli vznikla, včetně škody v podobě vynaložení nákladů na odstranění takových vad.
6. Zhotovitel je povinen záruční vady odstranit nejpozději do 10 kalendářních dnů od jejich oznámení

objednatelem zhotoviteli, nebude-li mezi smluvními stranami písemně dohodnut jiný termín pro odstranění vad.

7. Pokud zhotovitel neodstraní záruční vady ve sjednané době od jejich oznámení objednatelem zhotoviteli, je objednatel oprávněn podle vlastního uvážení vadu buď sám odstranit, nebo pověřit jejím odstraněním třetí osobu. Zhotovitel je povinen uhradit objednateli škodu, která objednateli vznikla v podobě vynaložení nákladů na odstranění takových vad.
8. Záruční doba se prodlužuje o dobu počínající dnem oznámení záručních vad objednatelem zhotoviteli a končící dnem řádného odstranění oznámených záručních vad.

## XII. OSTATNÍ PODMÍNKY PLNĚNÍ PŘEDMĚTU SMLOUVY

1. Zhotovitel je povinen při provádění díla postupovat v souladu s platnými právními předpisy ČR a EU.
2. Zhotovitel je povinen zajistit účast svých pověřených pracovníků při kontrole prováděných prací, kterou provádí dozor objednatele, a činit neprodleně opatření k odstranění zjištěných vad. Výkon tohoto dozoru nezbavuje zhotovitele odpovědnosti za řádné a včasné plnění dluhů z této smlouvy.
3. Zhotovitel se zavazuje informovat objednatele o stavu rozpracovaného díla na pravidelných poradách (tzv. kontrolních dnech), které bude objednatel organizovat podle potřeby. Zápisy z těchto porad bude pořizovat dozor objednatele. Zhotovitel se zavazuje zajistit vždy účast osoby oprávněné jednat za zhotovitele.
4. Dozor při realizaci díla nesmí provádět zhotovitel ani osoba s ním propojená.
5. Zhotovitel se dále zavazuje zajistit odborné technické vedení provádění díla, dodržovat bezpečnost práce při provádění díla, průběžně odklízet případný odpad, udržovat čistotu v místě plnění a v jeho okolí a po dokončení díla na svůj náklad odklidit veškerý odpad vzniklý z jeho činnosti.
6. Zhotovitel je oprávněn zajistit provedení částí díla subdodavateli.
7. Zhotovitel je povinen provádět dílo, nebo jeho část subdodavatelem, pokud jím ve své nabídce podané v zadávacím řízení veřejné zakázky prokazoval splnění kvalifikačních předpokladů. Pokud ze závažných objektivních důvodů nebude zhotovitel schopen zajistit, aby se takový subdodavatel podílel na realizaci díla, je zhotovitel oprávněn takového subdodavatele nahradit jiným subdodavatelem pouze na základě předchozího písemného souhlasu objednatele. Subdodavatel nahrazující původního subdodavatele musí prostřednictvím zhotovitele prokázat stejnou či vyšší kvalifikaci jako původní nahrazovaný subdodavatel. Objednatel nesmí změnu subdodavatele se stejnou či vyšší kvalifikací jako původní nahrazovaný subdodavatel odmítnout, nejsou-li k tomu dány závažné důvody.
8. Objednatel je oprávněn kontrolovat provádění díla zhotovitelem. Dozor objednatele je oprávněn zejména:
  - kontrolovat, zda práce jsou prováděny v souladu se smluvními podmínkami, přílohou č. 1



této smlouvy, příslušnými platnými právními předpisy, ČSN a rozhodnutími veřejnoprávních orgánů;

- upozorňovat zhotovitele na zjištěné nedostatky a kontrolovat termíny a způsob jejich odstranění;
- kontrolovat dodržování právních předpisů, směrnic, apod.

### XIII. UKONČENÍ SMLOUVY

1. Objednatel je oprávněn (kromě případů uvedených v § 2001 a násl. NOZ) od této smlouvy písemně odstoupit:
  - byl-li pravomocně zjištěn úpadek zhotovitele a rozhodnuto o způsobu řešení úpadku konkursem, nebo byl-li insolvenční návrh pravomocně zamítnut pro nedostatek majetku zhotovitele;
  - jestliže se zhotovitel ocitne v prodlení s předáním díla delším než 20 dní;
  - jestliže se zhotovitel ocitne v prodlení s odstraněním vad a nedodělků zjištěných při předání díla delším než 20 dní;
  - jestliže zhotovitel provádí dílo v rozporu s touto smlouvou nebo pokyny objednatele a nezjedná nápravu ani v dodatečné době stanovené objednatelem;
  - jestliže zhotovitel poruší svoji povinnost uvedenou v čl. XII. odst. 1 této smlouvy.
2. Pokud před dokončením díla dojde k odstoupení od smlouvy, předá zhotovitel nedokončené dílo objednateli písemným protokolem podepsaným oběma smluvními stranami, ve kterém bude popsán stupeň rozpracovanosti díla a současně předá objednateli veškeré dokumenty, zejména dokumenty dle čl. VI. odst. 2 této smlouvy a jiné listiny vztahující se k dílu, získané za dobu trvání účinnosti této smlouvy, jakož i případné listiny předané objednatelem zhotoviteli k provedení díla. Po vyhotovení a podepsání tohoto protokolu bude provedeno finanční vyrovnání smluvních stran. Objednatel uhradí zhotoviteli provedenou část díla podle podmínek této smlouvy.
3. Odstoupení od smlouvy se mimo jiné nedotýká ujednání o licencích, zárukách za jakost díla a o sankcích, které zavazují smluvní strany i po odstoupení od této smlouvy. Ode dne podpisu protokolu dle odst. 2 tohoto článku začne běžet záruční doba u provedených částí díla.
4. Ustanovení odst. 2 a 3 tohoto článku zavazují smluvní strany dle jejich výslovné vůle i po odstoupení od této smlouvy.

### XIV. ODPOVĚDNOST ZHOTOVITELE A SANKCE

1. Zhotovitel odpovídá za veškeré škody a nemajetkové újmy, které vzniknou objednateli v důsledku porušení této smlouvy zhotovitelem. Zhotovitel je povinen nahradit takto vzniklou škodu a nemajetkovou újmu v plném rozsahu, včetně případných sankcí udělených objednateli orgány veřejné moci, jejichž příčinou bylo porušení povinností zhotovitele dle této smlouvy.
2. Ocitne-li se zhotovitel v prodlení s plněním dle smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši 0,05 % z celkové ceny díla bez DPH podle čl. VII. odst. 1 této smlouvy za každý započatý den prodlení.

3. Ocitne-li se objednatel v prodlení s úhradou ceny díla podle čl. VII odst. 1, je povinen zaplatit zhotoviteli smluvní pokutu ve výši 0,05 % z dlužné částky za každý započatý den prodlení.
4. V případě prodlení zhotovitele s odstraněním vad nebo nedodělků vyplývajících z předávacího protokolu, vplynuvších ze zkušebního provozu díla, je-li touto smlouvou, přílohou č. 1 této smlouvy nebo objednatel požadován, nebo záručních vad zjištěných v záruční době, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 5 000,- Kč za každý započatý den prodlení do okamžiku jejich odstranění. Odstraní-li objednatel vady sám nebo prostřednictvím třetí osoby v souladu s touto smlouvou, je zhotovitel povinen uhradit smluvní pokutu pouze ve výši, v níž smluvní pokuta přesahuje škodu, která objednateli vznikla v podobě vynaložení nákladů na odstranění vad. Sankce dle tohoto ustanovení budou účtovány pouze do okamžiku, kdy celková cena takto účtovaných sankcí dosáhne celkové ceny díla stanovené v čl. VII odst. 1 této smlouvy.
5. Kterákoliv smluvní strana je oprávněna požadovat po druhé smluvní straně náhradu škody i nemajetkové újmy způsobené porušením povinnosti, na kterou se vztahuje smluvní pokuta, a to v rozsahu, v němž škoda či nemajetková újma sjednanou smluvní pokutu přesahuje, pokud není v této smlouvě stanoveno jinak.
6. V případě, že objednateli vznikne nárok na smluvní pokutu dle této smlouvy vůči zhotoviteli, je objednatel oprávněn započíst pohledávku z titulu smluvní pokuty oproti nároku zhotovitele na úhradu jím vystavené faktury.

## XV. ZÁVĚREČNÁ USTANOVENÍ

1. Smluvní strany se dohodly, že zhotovitel není oprávněn postoupit nebo zastavit pohledávku za objednatel z této smlouvy bez předchozího písemného souhlasu objednatele. Zhotovitel není oprávněn svou pohledávku za objednatel z této smlouvy nebo pohledávku na zaplacení smluvní pokuty vzniklé na základě této smlouvy použít k jednostrannému započtení na pohledávku objednatele za zhotovitelem.
2. Zhotovitel na sebe bere nebezpečí změny okolností ve smyslu § 1765 odst. 2 NOZ.
3. Smluvní strany se dohodly, že § 1912, § 1921, § 2112, § 2595, § 2605 odst. 2, § 2609, § 2611 a § 2618 NOZ se nepoužijí.
4. Vzhledem k veřejnoprávnímu charakteru objednatele zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním této smlouvy v rozsahu a za podmínek vyplývajících z příslušných platných právních předpisů, zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ustanovení § 147a zákona o veřejných zakázkách.
5. Zhotovitel je povinen spolupůsobit při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů a také při výkonu kontroly ze strany poskytovatele dotace, třetích osob pověřených poskytovatelem dotace, Ministerstva financí České republiky, Evropské komise, Evropského účetního dvora a Nejvyššího kontrolního úřadu české republiky. Pro účely finanční kontroly se zhotovitel považuje za osobu povinnou

- spolupůsobit při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů.
6. Zhotovitel je povinen strpět veškeré kontroly vyplývající z režimu financování z prostředků Evropské unie a státního rozpočtu České republiky a poskytnout při takové kontrole veškerou nezbytnou součinnost.
  7. Zhotovitel je povinen archivovat originální vyhotovení smlouvy včetně jejích dodatků, originály účetních dokladů a dalších dokladů vztahujících se k realizaci předmětu této smlouvy po dobu 10 let od zániku této smlouvy, minimálně však do roku 2024. Po tuto dobu je zhotovitel povinen umožnit osobám oprávněným k výkonu kontroly projektů provést kontrolu dokladů souvisejících s plněním této smlouvy.
  8. Zhotovitel je povinen všechny písemné zprávy, písemné výstupy a prezentace opatřit vizuální identitou projektů dle *Pravidel pro provádění informačních a propagačních opatření a manuálu vizuální identity IOP*. Zhotovitel prohlašuje, že ke dni nabytí účinnosti této smlouvy je s těmito pravidly seznámen. V případě, že v průběhu plnění této smlouvy dojde ke změně těchto pravidel, je objednatel povinen o této skutečnosti zhotovitele bezodkladně informovat.
  9. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami a může být měněna pouze písemnými dodatky k této smlouvě podepsanými objednatelem a zhotovitelem.
  10. Tato smlouva je vyhotovena ve čtyřech stejnopisech s platností originálu, z nichž každá ze smluvních stran obdrží po dvou vyhotoveních.
  11. Zhotovitel prohlašuje, že se před uzavřením této smlouvy nedopustil v souvislosti se zadávacím řízením veřejné zakázky sám nebo prostřednictvím jiné osoby žádného jednání, jež by odporovalo zákonu nebo dobrým mravům nebo by zákon obcházelo, zejména že nenabízel žádné výhody osobám podílejícím se na zadání veřejné zakázky, a že se zejména ve vztahu k ostatním uchazečům nedopustil žádného jednání narušujícího hospodářskou soutěž.
  12. Zhotovitel výslovně souhlasí se zveřejněním celého textu této smlouvy na veřejně přístupných webových stránkách Kraje Vysočina.
  13. Přílohy této smlouvy tvoří:
    - Příloha č. 1 – Technická specifikace
    - Příloha č. 2 – Položkový rozpočet

V Jihlavě dne

- 7 -04- 2015

Kraj Vysočina  
MUDr. Jiří Běhounek, hejtmán

**Kraj Vysočina**

Žižkova 57, 587 33 Jihlava

2

V Brně dne 25. března 2015

**EXPECT-IT, s.r.o.**  
Stankova 18, 602 00 Brno  
IČ: 269 86 603  
DIČ: CZ26986603  
www.expect-it.cz

**Expect-IT, s. r. o.**  
Mgr. Radana Šrubařová, jednatelka

## Příloha č. 1: Technická specifikace

### 8. Technická specifikace

#### 8.1 Vymezení stávajícího hardware a software

Projekt bude realizován v budově Krajského úřadu Kraje Vysočina, Žižkova 57, Jihlava v rámci krajem zřízeného a provozovaného Technologického centra (TCK) a bude využívat jeho stávající infrastruktury. Projekt nevyžaduje žádné stavební úpravy.

Technické řešení datového centra, do kterého budou ukládána veškerá data, je řešeno projektem Technologického centra kraje Vysočina (TCK).

##### 8.1.1 Hardwarové a systémové zajištění TCK

TCK poskytne potřebnou infrastrukturu a systémové služby pro datové i aplikační potřeby projektu:

##### 1. Datové úložiště

- disková virtualizace Falcon Istor,
- disková pole IBM DS5100 (v provedení SAS/FC, popřípadě SATA),
- pro řešení bezpečnostního dashboardu je v rámci provozního úložiště k dispozici celkově maximálně 300 IOPS a 5 TB diskové kapacity.

##### 2. MS SQL 2008 Std. Cluster

- storage cluster zajišťuje plně bezvýpadkový provoz,
- replikace a mirroring dat do záložního úložiště,
- zajištěno zálohování a obnova dat.

##### 8.1.2 Aplikační servery

Řešení bude provozováno v TCK v prostředí serverové virtualizace (VMware vSphere architektura) typicky na serverové platformě MS Windows 2008 R2, popřípadě Linux, FreeBSD.

Maximální výkon alokovaný z fyzických hostů všemi virtuálními stroji (maximálně 9 kusů, libovolný OS podporovaný VMWare) je 20 GHz CPU, maximální spotřeba paměti je 64 GB RAM.

K dispozici budou mechanismy vysoké dostupnosti (HA režim VMW), síťové ochrany včetně Web Application Firewallu (F5 BIG IP) a zálohování bude zajištěno nativními nástroji použité serverové virtualizace a nástrojem Symantec BackupExec.

Licence OS Microsoft Windows 2008 R2 Server jsou zajištěny zadavatelem, včetně koncového antivirového řešení (SEP 12).

#### 8.2 Předmět plnění zakázky Bezpečnostního dashboardu

Plnění zakázky Bezpečnostního dashboardu bude rozděleno do několika etap:

1. Dodávka implementační analýzy bezpečnostního dashboardu a analýzy rizik, jejichž akceptace bude předcházet samotnou implementaci řešení.
2. Navržení harmonogramu implementace navrhovaného řešení včetně definovaných požadavků na součinnost ze strany zadavatele.

3. Dodávka a implementace aplikačního řešení bezpečnostního dashboardu do infrastruktury Krajského úřadu Kraje Vysočina (dále jen "KrÚ").
4. Připojení zdrojů bezpečnostních událostí dle zadávací dokumentace.
5. Nastavení systému pro ověření dodávaných funkcionalit dle akceptačních požadavků, které budou definovány v rámci implementační analýzy.
6. Dodávka dokumentace.
7. Proškolení.
8. Testovací a zkušební provoz.
9. Akceptace dle požadavků, zátěžové testy, předání díla do užívání.
10. Technická podpora a údržba bezpečnostního dashboardu po dobu udržitelnosti projektu (5 let).

### 8.3 Popis požadovaného a nabízeného řešení

Bezpečnostní dashboard je rozdělen do několika (vzájemně propojených) funkčních bloků popsaných v rámci zadávací dokumentace samostatně:

- obecné požadavky na bezpečnostní dashboard,
- správa bezpečnostních incidentů (označovaných též jako BI),
- konfigurační management,
- změnový management,
- znalostní báze,
- správa aktiv.

Dále (jak v této subkapitole, tak v kapitole 9) se budeme podrobněji věnovat jednotlivým definovaným funkčním blokům.

#### 8.3.1 Bezpečnostní dashboard – obecné požadavky

Bezpečnostní dashboard zpracovává bezpečnostní události generované zdroji bezpečnostních událostí a dále je sdílí ostatním funkčním blokům.

Námi navrhované řešení je postaveno na našem vlastním softwarovém produktu GPC, který mimo jiné nabízí následující funkcionality:

1. Přehledné zobrazení bezpečnostních událostí
2. Kategorizace událostí
3. Kategorizace událostí na základě vlastních definic (*plněné nepovinné*)
4. Přiřazení různých stupňů důležitosti zdrojům bezpečnostních událostí (*plněné nepovinné*)
5. Grafické zobrazení bezpečnostních událostí (*plněné nepovinné*)
6. Definice korelačních pravidel mezi jednotlivými bezpečnostními událostmi
7. Vytváření reportů včetně plánovaných a následně odeslání předdefinovaným příjemcům
8. Jednotná informační struktura bezpečnostní události, jednoznačně specifikující zdroj, čas vzniku události, čas sběru události, popis události, emitenta, závažnost, název události a další parametry volitelné dle požadavků zadavatele
9. Mapování atributů vstupních událostí na parametry bezpečnostních událostí
10. Sběr událostí ze standardních typů zdrojů bezpečnostních událostí, přičemž celkový počet zdrojů bezpečnostních událostí těchto standardních typů, které budou předmětem analýzy a implementace, nepřesáhne počet 20.

Sběr událostí bude probíhat z následujících devíti **standardních typů** zdrojů bezpečnostních událostí: syslog, SNMP trap, WS – SOAP (webová služba), textový soubor (plain text, csv), DB view / tabulka, CEF = Common Event Format (*plněné nepovinné*), email, netflow (*plněné nepovinné*), OS Windows Event Log.

Co se týče sběru událostí z **nestandardních typů** zdrojů bezpečnostních událostí, nabízíme jako součást našeho řešení následující 3 zdroje povinné (IDM – Autocont, SIEM – Dragon, SIEM – NetIQ) a 9 zdrojů *plněných nepovinných* (Symantec endpoint protection, OS Linux / Unix Syslog, FlowMon, PRTG, The Dude – mikrotik, Veeam, BackupExec, WAF BIG-IP F5, Enterasys HiPath).

11. Vztažení bezpečnostní události k aktivu, konfigurační položce, evidované změně
12. Řízení přístupů uživatelů
13. Ověření uživatelů vůči MS Active Directory
14. Externí odkaz do zdroje událostí, pokud to tento podporuje (*plněné nepovinné*)
15. Konfigurace systému je možná bez našeho (dodavatelského) zásahu – GUI, editovatelný konfigurační soubor, customizační skript
16. Správa (vytvoření, úprava, odstranění) připojení k systému pomocí standardních rozhraní (zdrojového, cílového) je možná bez našeho (dodavatelského) zásahu – GUI, editovatelný konfigurační soubor, customizační skript
17. Úprava připojení systému mimo standardní rozhraní (zdrojové, cílové) je možná bez našeho (dodavatelského) zásahu – GUI, editovatelný konfigurační soubor, customizační skript (*plněné nepovinné*)
18. Kompletní datový model dodávaného řešení, včetně popisu jednotlivých položek a jejich vzájemných vazeb (*plněné nepovinné*)
19. Podpora sledování trendů, možnost akce na základě změn trendů (*plněné nepovinné*)
20. Implementace rolí dle nejlepších postupů a zkušeností s možností redefinice a rozšíření v rámci dodávky (*plněné nepovinné*)
21. Verzování dat, auditní stav v libovolném časovém okamžiku, možnost generování reportů, a to i zpětně (*plněné nepovinné*)
22. Zpracování minimálně 100 událostí za sekundu (100EPS)
23. Zpracování minimálně 500 událostí za sekundu (500EPS) (*plněné nepovinné*)
24. Zachování odezvy systému v reálném čase při práci s kompletními daty za 100 dní provozu (bez retence, při 100EPS)
25. Zachování odezvy systému v reálném čase při práci s kompletními daty za 200 dní provozu (bez retence, při 100EPS) (*plněné nepovinné*)
26. Definování retenčních politik
27. Předdefinovaná pravidla (signatury) pro detekci bezpečnostních incidentů (*plněné nepovinné*)
28. Definované standardizované rozhraní pro automatizované vyčítání informací z bezpečnostního dashboardu (*plněné nepovinné*)
29. Definované standardizované rozhraní pro automatizovanou správu uživatelů a jejich oprávnění (z IDM) (*plněné nepovinné*)
30. Definování přístupových oprávnění pro role minimálně v rozsahu administrátor (nastavení a konfigurace systému), operátor (obsluha bezpečnostního dashboardu) a servisní manažer (reporty)

### 8.3.2 Správa Bezpečnostních incidentů

31. Systém umožňuje spravovat bezpečnostní incidenty
32. Definování pravidel, na základě jakých bezpečnostních událostí či jejich kombinací vzniká bezpečnostní incident
33. Notifikace o jednotlivých úkonech týkajících se bezpečnostních incidentů (*plněné nepovinné*)
34. Přiřazování bezpečnostních incidentů k řešení jednotlivým operátorům a zobrazování stavu řešení bezpečnostních incidentů
35. Automatické založení předdefinovaného ticketu včetně dat obsahující bezpečnostní incident do externího systému procesního řízení (HelpDesk). Tuto skutečnost evidujeme, případně přebíráme

stav řešení z externího systému (*plněné nepovinné*)

36. Kategorizování bezpečnostních incidentů
37. Vytváření reportů včetně plánovaných a následné odeslání předdefinovaným příjemcům
38. Zobrazení událostí, na základě kterých vznikl bezpečnostní incident
39. Zobrazení vazeb dotčených konfiguračních položek, aktiv
40. Definování pravidel pro určení false positive bezpečnostního incidentu
41. Definování Workflow pro jednotlivé bezpečnostní incidenty
42. Definování pravidla pro automatické přiřazení Workflow na základě parametru bezpečnostního incidentu (*plněné nepovinné*)
43. Přehledné grafické zobrazení bezpečnostních incidentů (dashboard)

### 8.3.3 Konfigurační management

44. Umožňuje vést evidenci konfiguračních položek v libovolném počtu úrovní ve stromové struktuře
45. Umožňuje provázat bezpečnostní události s jednotlivými konfiguračními položkami
46. Umožňuje zobrazit stavy konfiguračních položek k danému datu a času
47. Umožňuje propojení s externím systémem řízení změn – HelpDesk (*plněné nepovinné*)
48. Umožňuje zobrazení řízených změn (evidovaných ve změnovém managementu) pro dotčenou konfigurační položku
49. Grafické zobrazení vazeb mezi jednotlivými konfiguračními položkami (*plněné nepovinné*)
50. Umožňuje automatizovaně načítat hodnoty vlastností jednotlivých konfiguračních položek (*plněné nepovinné*)
51. Umožňuje administrátorům jednoduchým způsobem popsat realizovanou změnu konfigurační položky přímo ze systému samotného, pokud to tento podporuje (*plněné nepovinné*)
52. Umožňuje stanovit jednotlivé typy konfiguračních položek a k nim definovat vlastnosti
53. Umožňuje definovat libovolné vlastnosti konfigurační položky a ukládat zadané hodnoty
54. Umožňuje vytváření reportů, včetně plánovaných, a následné odeslání předdefinovaným příjemcům (*plněné nepovinné*)
55. Umožňuje vést evidenci přístupu a bezpečnostních událostí k jednotlivým konfiguračním položkám
56. Umožňuje vytvořit manuální záznam ke konfigurační položce či vlastnosti
57. Podporuje automatizované editace z dohledovaného systému směrem ke konfiguračnímu managementu a opačně (*plněné nepovinné*)
58. Periodické sledování stavu konfiguračních položek a jejich hodnot a porovnávání oproti aktuálnímu stavu. V případě nesouladu reálného stavu se záznamem v konfiguračním managementu nastane inteligentní reakce typu automatická aktualizace, upozornění o změně s možností schválení, řízený schvalovací proces pomocí definovaného workflow (*plněné nepovinné*)

### 8.3.4 Změnový management

59. Umožňuje vazbu do externího systému procesního řízení (HelpDesk) s možností transformovat ticket v něm založený na změnu (*plněné nepovinné*)
60. Umožňuje zobrazit bezpečnostní události vázané na aktivum, konfigurační položku či její vlastnost ve vazbě na definovanou (ohlášenou) změnu
61. Vytvoření požadavku na změnu – popis změny, vazba na aktivum, konfigurační položku či její vlastnost, respektive hodnotu
62. Umožňuje definování workflow změny, životního cyklu a stavů změny
63. Umožňuje automatické založení předdefinovaného ticketu včetně dat obsahující změnový požadavek do externího systému procesního řízení (HelpDesk). Tuto skutečnost umožňuje evidovat a případně přebírat aktuální stav řešení z externího systému (*plněné nepovinné*, pokud HelpDesk

poskytuje API).

64. Umožňuje kategorizaci změn s možností předdefinovaných workflow

### 8.3.5 Znalostní báze

65. Umožňuje vytváření znalostní báze

66. Fulltext vyhledávání ve znalostní bázi

67. Znalostní báze pro objekt typu BU, bezpečnostní incident, pravidla, aktivum, konfigurační položka, vlastnost, hodnota (*plněné nepovinné*)

68. Možnost vkládat dokumenty (*plněné nepovinné*)

69. Fulltext vyhledávání obsahu dokumentů – pdf, doc, txt (*neplněné nepovinné* – možnost rozšířit přikoupením separátní licence)

### 8.3.6 Správa aktiv

70. Umožňuje evidenci aktiv

71. Umožňuje k danému aktivu vazbu na konfigurační položky a bezpečnostní události a incidenty

72. Umožňuje ohodnocení aktiv s vazbou na určení závažnosti bezpečnostní události, popřípadě incidentu

73. Umožňuje definovat oprávnění přístupu k danému aktivu – zobrazení vazeb, informací, událostí, bezpečnostních incidentů týkajících se aktiva (*plněné nepovinné*)

74. Umožňuje evidovat rizika aktiv v minimální rozsahu definovaném v zákoně o kybernetické bezpečnosti a příslušných vyhláškách (Zákon č. 181 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, dále jen „ZKB“)

75. Umožňuje evidovat hrozby aktiva včetně možnosti definování vlastních

76. Umožňuje k aktivu definovat libovolný uživatelský atribut a ukládat zadané hodnoty (*plněné nepovinné*)

77. Umožňuje vytvářet souhrnné reporty obsahující informace vázané k jednotlivým aktivům (ohodnocení, rizika, hrozby)

## 8.4 Popis zdrojů bezpečnostních událostí

### 1. SIEM – Dragon

- SIEM vytvořený firmou Enterasys (Extreme Networks), který v současné době sbírá informace o síťovém provozu (FlowMon) a také z několika připojených síťových systémů, např. Wifi kontrolér Enterasys HiPath
- verze: 7.7.0 Maintenance Release 5 (Build 301846 (7.0.0.301503))

### 2. SIEM – NetIQ

- SIEM – aktuálně sbírá informace z OS některých serverů, Audit MSSQL DB, logy z některých aplikací
- verze: NetIQ Security Manager 6.5.4

### 3. WAF BIG-IP F5

- aplikační firewall použitý pro monitorování provozu vůči webovým aplikacím provozovaných v rámci infrastruktury technologického centra Kraje Vysočina
- verze: BIG-IP 11.3.0 Build 2806.0 Final



4. FlowMon (Probe + Collector)
  - analyzuje síťový provoz
  - verze: FlowMon 6.05.00
5. Enterasys HiPath
  - WiFi kontrolér – udržuje o informace o jednotlivých uživateli WiFi, jejich roamingu, umožňuje administrovat jednotlivé AP i síť jako celek
  - verze: Enterasys® Wireless Version 8.31.XX
6. PRTG
  - provozní monitoring – v reálném čase kontroluje stav, dostupnost, aktuální hodnoty vlastností systému
  - verze: PRTG Network Monitor 14.3.11.2750
7. The Dude – mikrotik
  - monitoruje dostupnost služeb, síťových prvků, serverů
  - verze: Dude v3.6
8. IDM – Autocont (dále jen „IDM“)
  - správa identit a oprávnění k přístupů k jednotlivým systémům
  - verze: 2.1.4
9. Veeam Backup
  - zálohování virtuální infrastruktury TCK
  - verze: 7.0.0.871
10. BackupExec
  - zálohování fyzických serverů, databází, webových aplikací a jiných konkrétních aplikací
  - verze: 14.0 Rev 1798 (64-bit)
11. Symantec Endpoint Protection
  - antivirové řešení koncových bodů (pracovní stanice, servery)
  - verze: 12.1.4104.4130

## 8.5 Popis požadované funkcionality – ideový záměr

Námi nabízený produkt GPC (nastíněný blíže v následující kapitole) umožňuje optimalizaci v širokém spektru zákaznických požadavků a podmínek. V případě nasazení na Kraji Vysočina bude naše softwarové řešení GPC v maximální možné míře přizpůsobeno následujícímu popisu zadavatele a požadavkům, procesům a funkcionalitám z něj plynoucím.

Na zdroji bezpečnostních událostí, připojeném na bezpečnostní dashboard, vznikne událost, podle nastavení zdroje samotného dojde k odeslání či neodeslání této události definovaným komunikačním kanálem na stranu bezpečnostního dashboardu, popř. na straně bezpečnostního dashboardu je rozhodnuto, zda má být bezpečnostní událost přijata. Po přijetí události do bezpečnostního dashboardu je analyzován obsah samotné události, na základě mapovacích funkcí se

system pokusi událost přiřadit konfigurační položce (popř. změně hodnoty její vlastnosti) nebo celému aktivu. Na základě přiřazeného aktiva, zdroje události dojde k ohodnocení závažnosti dané bezpečnostní události. Na základě definovaných pravidel pro zdroj, typ události, aktiva, stupně závažnosti dojde k vyhodnocení samotné události případně ke korelaci s ostatními událostmi. Výsledkem může být pouhé zaevidování bezpečnostní události nebo mohou být splněny podmínky pro vytvoření bezpečnostního incidentu.

Bezpečnostní incident se dále řídí předdefinovaným životním cyklem. Je přiřazen operátorovi, dojde k notifikaci, k založení ticketu v externím systému HelpDesk, je mu přiřazena kategorie apod. Operátor bezpečnostního dashboardu si bude moci zobrazit podrobnosti bezpečnostního incidentu, události a pravidla, na základě kterých vzniknul, a pokud to zdrojový systém umožňuje, zobrazí se odkaz pro zobrazení události přímo ve zdrojovém systému. Na základě těchto informací o bezpečnostním incidentu operátor bezpečnostního dashboardu začne bezpečnostní incident řešit. Může prohledat znalostní bázi, zobrazit si související incidenty, předat k řešení jinému operátorovi, založit ticket v externím systému apod. Výsledkem by měly být informace kým, jakým způsobem a kdy byl bezpečnostní incident vyřešen, jaká protipatření byla realizována. Bezpečnostní incident je vyřešen a nadále archivován. V případě detekování bezpečnostních incidentů, které jsou obsluhou uznány jako legitimní, umožní systém definovat pravidla pro tzv. false positive. Obdobné bezpečnostní incidenty se již dále evidují jako false positive a nezatežují obsluhu jejich opětovným řešením.

Bude možné zobrazit vizualizované přehledové reporty s počtem bezpečnostních incidentů za definované období a to včetně popisu incidentu, kategorie, způsobu vyřešení atd. Tento report bude plnit funkci výstupu ze systému řízení bezpečnosti informací směrem k managementu organizace. Reporty bude možno předdefinovat a plánovaně generovat a popř. odesílat definovaným příjemcům / uživatelům. Systém bude umožňovat řízení přístupu k jednotlivým funkcím a zdrojům tak, aby například management mohl kontrolovat stav pomocí uživatelsky definovaných reportů, jednotliví správci aktiv mohli sledovat události týkající se jejich aktiv atp. Pro zajištění uživatelského komfortu je nezbytné, aby systém mohl ověřit identitu vůči adresářové službě MS Active Directory, která je v rámci organizace využívána.

Dalším funkčním celkem bezpečnostního dashboardu je Konfigurační management a Správa aktiv, tyto části umožňují níže uvedené funkčnosti. Bude definována databáze aktiv včetně jejich ohodnocení zejména z pohledu požadavků na úroveň dostupnosti, důvěrnosti a integrity. K takto definovanému aktivu bude dále možnost definovat konfigurační položky různých typů, vlastností, hodnot či stavů. Systém by tak měl být schopen automaticky identifikovat jednotlivé události a přiřadit je k aktivům či konfiguračním položkám, jejich vlastnostem a hodnotám. Měl by tak být schopen zjistit, že je dané aktivum nedostupné, že na něm byly provedeny konfigurační změny. Správce aktiva by měl mít možnost co nejjednodušeji popsat jakou konfigurační změnu a jaké položky provádí, ideálně přímo z místa, kde dochází k samotné konfiguraci (serveru). Přílišná administrativní obtížnost zapsání záznamu o změně konfigurace vede k neefektivnímu využití pracovní síly nebo k nezapsání samotných informací o provedené změně konfigurace. Dále by měl být systém schopen graficky zobrazit vazby mezi jednotlivými aktivy a konfiguračními položkami.

## 8.6 Implementace dodávaného řešení

V rámci implementace bude identifikován nejvhodnější způsob předávání informací z bezpečnostních zdrojů, případně bude uvedeno, jakým způsobem nastavit samotný zdroj bezpečnostních událostí.

Uchazeč Expect-IT, s. r. o. zadavateli rád předvede ukázky funkčního řešení vybrané části

architektury (konkrétně výběru z funkcionalit č. 1., 2., 6. – 9., 10. a), d), i), 15., 16., 31., 32., 34., 38., 41., 44.) v termínu maximálně 30 dnů od vyžádání.

## **8.7 Akceptace a předání dodávaného řešení**

V rámci akceptace a předání hotového díla bude prezentována jeho funkčnost dle předem domluvených akceptačních kritérií, která budou definována v implementační analýze. Dále budou zhotovitelem provedeny zátěžové testy dodávaného řešení.

Zhotovitel předá zadavateli dokumentaci k dílu v požadovaném rozsahu.

V rámci předání díla dojde k realizaci školení uživatelů v ovládání systému z pohledu minimálně tří standardizovaných rolí: administrátor, operátor, servisní manažer.

## **8.8 Požadavky na bezpečnost dodávaného řešení**

Jako nezbytná součástí řešení bude dodána procesní a technologická dokumentace v souladu s mezinárodní normou ISO / IEC 27001:2005, a to pro oblasti:

### **8.8.1 Analýza rizik navrhovaného řešení**

Zejména pro technické vybavení, komunikační prostředky, programové vybavení a objekty dodávaného řešení se zaměřením na následující hrozby:

- poškození nebo selhání hardwaru nebo softwaru,
- užívání software v rozporu s licenčními podmínkami,
- kybernetický útok z vnější komunikační sítě,
- škodlivý kód (například viry, spyware, trojské koně),
- přerušení dodávky komunikačních služeb nebo elektrické energie,
- zneužití nebo modifikace údajů,
- kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků,
- fyzická bezpečnost.

Na základě bezpečnostních potřeb a výsledků hodnocení rizik bude zpracováno prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření a popis vazeb mezi identifikovanými riziky a příslušnými bezpečnostními opatřeními.

### **8.8.2 Dokumentace provozních postupů**

Bude vypracován dokument „Provozní monitoring systému“ obsahující metriky provozuschopného stavu systému. Dokument bude obsahovat:

- které provozní parametry mají být sledovány – výčet procesů, kapacity výpočetních zdrojů;
- jaké limity parametrů nemají být dosaženy a překročeny;
- soupis provozních symptomů, které mají být detekovány, lokalizovány, eskalovány k řešení.

### **8.8.3 Popis oddělení prostředí pro vývoj, test, provoz dodávaného řešení**

Oddělením vývojového prostředí bude zajištěna jeho bezpečnost a ochrana používaných testovacích dat. V případě začlenění do stávající infrastruktury musí být definovány požadavky na konfiguraci jednotlivých síťových prvků pro zajištění požadované bezpečnosti a funkčnosti.

### **8.8.4 Postup ověření identity uživatelů**

V případě využití interních uživatelů, kteří používají autentizaci pomocí hesla, budeme definovat

pravidla pro jeho minimální délku a složitost, a to v souladu s platnými interními pravidly organizace.

#### **8.8.5 Řízení přístupových oprávnění**

Bude popsána úroveň privilegovaných i neprilegovaných přístupových oprávnění.

#### **8.8.6 Návrh a popis zálohování navrhovaného řešení**

Návrh zálohování navrhovaného řešení bude vypracován včetně popisu postupu pro obnovu částí nebo celého systému, vypracování plánů záloh a návrhu DR testů (co, jak často, do jaké úrovně apod.).

#### **8.8.7 Zaznamenávání událostí, včetně návrhu jejich vyhodnocování**

Klíčovým úkolem je zajištění ochrany získaných informací před neoprávněným čtením nebo změnou. Nejen z tohoto důvodu bude v rámci dodávaného řešení realizováno zaznamenávání přinejmenším následujících událostí:

- přihlášení a odhlášení uživatelů a administrátorů,
- činnosti provedené administrátory (privilegovanými účty),
- činnosti vedoucí ke změně přístupových oprávnění (standardních i privilegovaných),
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- zahájení a ukončení činností jednotlivých komponent systému,
- automatická varovná nebo chybová hlášení komponent systému,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

#### **8.8.8 Aplikační bezpečnost**

V rámci dodávaného řešení bude zajištěna:

- trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou,
- trvalá ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.

#### **8.8.9 Kryptografické prostředky**

V případě využití kryptografických prostředků pro činnost dodávaného řešení (např. šifrovaná komunikace mezi agentem a GPC masterem; https) zajistíme použití kryptografických algoritmů a kryptografických klíčů v úrovni odolnosti vyplývající z analýzy rizik.

Nepředpokládá se, že v rámci řešení budou zpracovávána data dle klasifikace NBÚ dle zákona č. 412/2005 Sb.

#### **8.8.10 Monitorování systémů**

Součástí monitorování systémů bude:

- popis zdrojů, metrik a způsobu pro monitorování provozních stavů systému a jeho komponent včetně případných prahových hodnot (normální provoz / omezená funkčnost / nedostupnost),
- záznamy selhání,
- jednoznačná chybová hlášení systému.

## 9. Popis nabízeného informačního systému

### 9.1 Výňatek z produktového listu GPC

**GPC Framework** je obecné softwarové řešení pro popis, standardizaci a automatizaci procesů.

GPC Framework podporuje užití principiálně libovolných datových struktur, nad těmito strukturami lze provádět libovolné operace, definovat libovolné procesy, sledovat a vyhodnocovat změny aj. Naše řešení umožňuje zaznamenávat vývoj všech konfiguračních položek v čase, včetně reflektování typu konfigurační položky poplatné životnímu cyklu. Veškeré změny jsou logovány a stav prostředí je možné zobrazit k libovolnému časovému okamžiku sledovaného období.

GPC Framework se skládá z několika Úrovní. Úroveň obsahuje nástroje a funkce pro podporu řešení určité skupiny úloh.

Výrazný přínos řešení pro daného zákazníka nastává v okamžiku, kdy je nad GPC Frameworkem implementována funkcionalita (obchodní logika, Business Logic) přesně odrážející použité procesy, pracovní postupy, firemní know-how a další požadavky tohoto zákazníka.

Naším cílem není přizpůsobovat zákazníka (či jeho požadavky) jednostranně zaměřenému produktu, ale naše řešení je přizpůsobováno konkrétním (mnohdy velice specifickým) požadavkům našich zákazníků. Nesnažíme se (potřeby) zákazníka nasoukat do uniformní neforemné krabičky nevhodných rozměrů, ale „šijeme pro něj jedinečné šaty na míru“. Toho všeho lze zpravidla dosáhnout pouhým nastavením a konfigurací GPC Frameworku, ve složitějších případech lze doprogramovat modul na míru.

Nad popsáním frameworkem může být provozována libovolná nastavba, tzv. **Business Logic**.

### 9.2 Motivace

Komplexní IT prostředí tvoří velmi složitý systém složený z jednotlivých konfiguračních položek (konfigurační položkou chápeme jakoukoliv komponentu HW i SW, která zajišťuje chod poskytovaných IT služeb), jež jsou poplatné použitým technologiím, době implementace, zaměřením organizace apod.

Je-li přidávána do tohoto systému další technologie, je-li technologie měněna (například i při změně firmware technologie) nebo při změně logiky fungování způsobené konfiguračním zásahem administrátorů, při změně designu a podobně je zpravidla nutné provést redefinici konfiguračních položek, znovuvytvoření konfigurační databáze a správné spárování proti původnímu stavu. Dále je třeba znovu definovat reakce na incidenty vzniklé nad konfigurační položkou, v krajním případě redefinovat či přeprogramovat „dohledové“ nástroje.

Je-li tato činnost prováděna manuálně, je to nejen časově náročné, ale zpravidla dochází též ke vzniku nekonzistencí způsobených chybou lidského faktoru, případně nepochopením dané technologie nebo designu. Dalšími problémy, které často vznikají, jsou komunikační potíže (například mezi odbornými pracovišti a odděleními).

Tyto problémy odpadají nebo jsou minimalizovány použitím vhodných softwarových řešení a dobře zdokumentovaných procesů.

## 9.3 Nabídka řešení

V současné době existuje v organizaci Kraj Vysočina velké množství různých proprietárních řešení na správu a vyhodnocování událostí nad konfiguračními položkami, které jsou ukládány do mnoha databází konfiguračních položek a událostí, jejichž synchronizaci je potřeba zajistit.

To lze provést pomocí převodu dat do unifikovaných meta struktur, které lze posléze pomocí datových pump a importních můstků distribuovat mezi jednotlivými systémy. Tento princip zajistí aktuálnost, flexibilitu ITIL procesů firmy a pomůže mimo jiné odhalit nekonzistence v datech, postupech a očekáváních. Příkladem mohou být detekované nekonzistence elektronických procesů Incident / Problem / Change Managementu vzhledem k realitě.

Cílem nasazení Bezpečnostního dashboardu tedy není nahrazení stávajících nástrojů či řešení (což často ani principiálně nelze), ale umožnění automatizovaného sběru dat v reálném čase přímo ze systémů (data jsou tudíž vždy aktuální a plně odpovídající realitě), provádění synchronizace sebraných dat vůči standardním nástrojům, upozorňování zodpovědných osob na rozdíly stavu skutečného a dříve evidovaného, a lze-li, tak i strojové provádění oprav a korekcí.

Celé řešení bude tvořeno z následujících šesti modulů:

### 9.3.1 Modul Bezpečnostní dashboard

Jedná se o centrální modul pro správu bezpečnostních událostí. Tento modul bude sloužit jako zdroj pro ostatní funkční bloky. Bezpečnostní události budou zobrazovány v závislosti na kategorii konfigurační položky. Bezpečnostní události bude možné porovnávat dle definovaných pravidel. Zaznamenané bezpečnostní události lze reportovat. Reporty bude možné automatizovat a rozesílat předdefinovaným příjemcům.

Bezpečnostní události budou mít jednotnou informační strukturu (viz zadávací dokumentace). Zajistíme automatizované vyčítání všech takto specifikovaných konfiguračních položek, a to ze všech relevantních infrastrukturních zdrojů.

Sběr událostí bude probíhat zejména ze standardních i nestandardních zdrojů bezpečnostních událostí, typicky dohledových nástrojů pro správu diskových polí, nástrojů pro správu infrastruktury, nástrojů pro management hardware, nástrojů pro správu hypervisorů, databází, OS a další (viz zadávací dokumentace).

Jakákoliv bezpečnostní událost bude přiřazena k dané konfigurační položce tak, aby bylo možné vyhodnotit závažnost bezpečnostní události a dopad na konfigurační položku, potažmo na IT službu.

Řešení předpokládá implementaci Access Managementu (řízení přístupů), a to na základě definovaných oprávnění a ověření v MS Active Directory organizace. Řešení umožňuje libovolné množství uživatelských rolí. Předpokládáme implementaci tří základních uživatelských rolí: administrátor, operátor a servisní manažer.

### 9.3.2 Modul Správa incidentů

Tento modul umožní sběr a přehledné grafické zobrazení bezpečnostních incidentů z definovaných zdrojů (viz zadávací dokumentace). V rámci tohoto modulu bude možné definovat, na základě jakých bezpečnostních událostí vzniká bezpečnostní incident a tyto následně kategorizovat, reportovat, případně odeslat automatickou notifikaci do externího nástroje HelpDesku na řešení bezpečnostního incidentu. Bezpečnostní incident bude možné přiřadit k řešení operátorům, případně přebírat stav řešení z externího systému. Automatické notifikace mohou zpřístupnit definovaným příjemcům konkrétně specifikované informace týkající se Bezpečnostního incidentu.

Pokud Bezpečnostní incident vznikl na základě konkrétní bezpečnostní události, bude možné ji

zobrazit, a to včetně provázání na dotčené konfigurační položky.

Nedílnou součástí efektivní správy bezpečnostních incidentů je definování pravidel false positive a odfiltrování falešných bezpečnostních událostí.

V rámci správy bezpečnostních incidentů budou nadefinována základní workflow pro řešení bezpečnostních incidentů s možností jejich úpravy, případně vytváření nových workflow, včetně možnosti automatizovaných workflow (automatické přiřazení workflow na základě parametru bezpečnostního incidentu).

### 9.3.3 Modul Konfigurační management

Tento modul umožní vést evidenci konfiguračních položek v libovolném počtu úrovní stromové struktury.

V průběhu implementace popíšeme relevantní konfigurační položky poplatné aktuálně používaným technologiím datového centra, prostředí, logice fungování a dalším určujícím faktorům. Konfigurační položky popíšeme včetně jejich vlastností, vzájemných vazeb a atributů vazeb.

Navrhne datový model tak, aby bylo možné podchytit výše popsané, a současně aby jej bylo možné při změně rozšířit nebo modifikovat. Garantujeme připravenost provést tyto změny na vyžádání. Podchytíme vývoj všech konfiguračních položek v čase, včetně reflektování typu konfigurační položky poplatné životnímu cyklu.

Upozorníme na abnormality a anomálie v chování konfiguračních položek (skokové změny sledovaných atributů, nepodchycené zmizení konfigurační položky, existující – avšak nepodchycená – vazba mezi položkami, jako je například existence databáze na nedatabázovém – a tedy nelicencovaném – serveru).

Každá konfigurační položka bude provázána s eventuální bezpečnostní událostí, bude zobrazovat svoje stavy k definovanému datu a času. Změny konfigurační položky bude možné propojit s externím nástrojem HelpDesku, a to spolu se zobrazením řízených změn pro danou konfigurační položku.

Součástí modulu je grafické znázornění vazeb mezi jednotlivými konfiguračními položkami.

Modul umožní správcům konfiguračních položek popis jejich změn přímo ze systému samotného (pokud to tento podporuje), včetně záznamů o přístupech a bezpečnostních událostech konfiguračních položek.

K dispozici bude možnost vytvářet reporty či provádět manuální záznamy nad konfigurační položkou. Pokud umožní dohledový systém vložit záznam, bude automaticky vložen i do záznamu konfigurační položky.

### 9.3.4 Modul Změnový management

Tento modul umožní vytvoření požadavku na změnu včetně vazby do externího systému nástroje HelpDesk, s možností transformace ticketu (který je v něm založený) na požadavek na změnu. Umožní zobrazit bezpečnostní události vázané na konfigurační položku v případě její změny.

Modul bude umožňovat založení předdefinovaného ticketu včetně dat obsahujících změnový požadavek do externího nástroje HelpDesk (pokud má tento nástroj pro tuto funkcionalitu podporované API rozhraní – web services, DB Access, SNMP, apod.). Dále umožní tento modul definování workflow změny, životního cyklu a aktuálního stavu změny, nevyjímaje možnosti předdefinovaných workflow v závislosti na kategorii požadavku na změnu.

### 9.3.5 Modul Znalostní báze

Tento modul umožní vytvoření rozsáhlé znalostní databáze založené na existující CMDB a jednotlivých konfiguračních položkách. Součástí modulu je znalostní báze pro objekty typu

bezpečnostní událost, bezpečnostní incident, aktivum, konfigurační položka včetně přiřazených informací typu vlastnost, hodnota, pravidlo.

Modul umožní vkládat externí dokumenty (doc, pdf, txt) a fulltextově vyhledávat v rámci znalostní báze. Fulltextové vyhledávání v obsahu dokumentů je možné realizovat po zakoupení separátní licence.

### 9.3.6 Modul Správa aktiv

Tento modul bude určený ke správě a evidenci jednotlivých informačních aktiv organizace. Celkový koncept správy aktiv bude v souladu se zákonem o kybernetické bezpečnosti a příslušnými vyhláškami (zákon č. 181/2014 Sb., o kybernetické bezpečnosti) a s mezinárodním bezpečnostním rámcem ISO / IEC 27001 – ISMS.

Každé aktivum bude možné evidovat, ohodnocovat a vyhodnocovat, včetně propojení vazeb na konfigurační položky, bezpečnostní události a bezpečnostní incidenty.

Modul umožní ohodnocení aktiv s vazbou na určení závažnosti bezpečnostní události, bezpečnostního incidentu a dále ve vazbě na krizové plány a scénáře. Součástí bude funkcionalita umožňující evidovat hrozby (např. dle ISO / IEC TR 13335), s možností definovat vlastní hrozby.

Ke každému aktivu bude možné vkládat libovolné uživatelské atributy a vytvářet souhrnné reporty obsahující informace vázané k jednotlivým aktivům (čímž máme na mysli především ohodnocení aktiva, rizika, hrozby, SLA apod.).

## 9.4 Požadavky na hardware a software

Naše řešení je dodáváno formou virtuální appliance pro VMware.

### 9.4.1 Požadavky na virtual appliance

1. CPU: Intel, minimálně 5 x 2GHz, 64-bit
2. RAM: 16 GB minimálně
3. Disk: minimálně 40 GB svazek pro OS, minimálně 100 GB svazek pro data aplikace, zálohované a s redundancí
4. OS: je součástí (používáme Linux, obvykle Debian, a MySQL)
5. Připojení k datové síti zadavatele

### 9.4.2 Požadavky na síť a síťovou komunikaci

1. IP adresa + netmask, hostname a související DNS A + PTR záznamy (které se pokud možno už nebudou měnit, viz SSL certifikát níže), IP default gateway, adresy DNS a NTP serverů a názvy DNS a MS domén používaných interně.
2. Pokud se uživatelé budou identifikovat a ověřovat proti stávajícímu zdroji zadavatele (MS AD, LDAP), pak bude třeba i pro jednotlivé interní domény sdělit též IP adresy LDAP serveru a povolit a nakonfigurovat LDAP (SSL zabezpečení) na straně serveru zadavatele.
3. Obvykle používáme pro komunikaci mezi agentem a serverem porty 12121 a 12122. Komunikace probíhá obousměrně, a to (dle objemu zpráv) jak TCP, tak UDP protokolem. Lze změnit dle požadavků zadavatele i na jiná nepoužívaná čísla portu.
4. Administrátoři a operátoři zadavatele se přihlašují na web rozhraní aplikace (TCP port 443 nebo port 8443). Pokud to bude zadavatel vyžadovat, bude nutné vystavit SSL certifikát web serveru, který bude důvěryhodný pro interní prohlížeče zadavatele.
5. Po dobu implementace budeme potřebovat a využívat vzdálený přístup via ssh (TCP port 22). Lze



- omezit na konkrétní zdrojovou IP adresu / adresy používané firmou Expect-IT, s. r. o. nebo poskytnout přístup pomocí VPN.
6. Pro monitoring aplikací na serverech zadavatele mimo lokálně instalovaného agenta potřebujeme povolit ICMP na všechna monitorovaná zařízení, přichodí syslog na náš server a odchozí LDAP a SNMP pro načítání ze systémů zadavatele.
  7. V případě zaslání alertů a notifikací budeme potřebovat odesílat poštu z platné interní emailové adresy na interní mailserver zadavatele. Pokud se počítá s mailem i pro předávání dat z aplikací zadavatele, budeme lokálně instalovat také mail server a bude tedy potřeba povolit komunikaci a konfigurovat směrování na něj minimálně z interního mailserveru zadavatele.
  8. V případě požadavku zadavatele na notifikace SMS pomocí SMS brány bude zapotřebí, abychom měli přístup k SMS bráně.
  9. Další bude upřesněno dle specifických požadavků zadavatele během realizace, v rámci propojení se SIEM a dalšími systémy zadavatele.

V Jihlavě dne

- 7 -04- 2015

**Kraj Vysočina**  
MUDr. Jiří Běhounek, hejtman

**Kraj Vysočina**  
Žižkova 57, 587 33 Jihlava

2

V Brně dne 25. března 2015

**EXPECT-IT, s.r.o.**  
Stankova 18, 602 00 Brno  
IČ: 269 66 603  
DIČ: CZ26966603  
www.expect-it.cz

**Expect-IT, s. r. o.**  
Mgr. Radana Šrubařová, jednatelka

## Příloha č. 2: Položkový rozpočet

Položka	Cena bez DPH	Cena včetně DPH
Implementační analýza	239 668,00 Kč	289 998,28 Kč
Dodávka bezpečnostního dashboardu	700 000,00 Kč	847 000,00 Kč
Připojení zdrojů bezpečnostních událostí, konfigurace systému dle akceptačních požadavků	250 000,00 Kč	302 500,00 Kč
Školení	50 000,00 Kč	60 500,00 Kč
<b>Celkem cena nabízeného řešení</b>	<b>1 239 668,00 Kč</b>	<b>1 499 998,28 Kč</b>

V Jihlavě dne

- 7 -04- 2015

**Kraj Vysočina**  
MUDr. Jiří Běhounek, hejtmán

**Kraj Vysočina**  
Žižkova 57, 587 33 Jihlava

2

V Brně dne 25. března 2015

**EXPECT-IT, s.r.o.**  
Stankova 18, 602 00 Brno  
IČ: 269 66 603  
DIČ: CZ26966603  
www.expect-it.cz

**Expect-IT, s. r. o.**  
Mgr. Radana Šrubařová, jednatelka



**EXPECT-IT, s.r.o.**  
Stankova 18, 602 00 Brno  
IČ: 269 66 603  
DIČ: CZ26966603  
www.expect-it.cz



**EXPECT-IT, s.r.o.**  
Stankova 18, 602 00 Brno  
IČ: 269 66 603  
DIČ: CZ26966603  
www.expect-it.cz