Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní plán obnovy pro oblast vysokých škol pro roky 2022-2024
Registrační číslo: NPO_OSU_MSMT-16610/2022

ANALÝZA SOULADU SOUČASNÉHO STAVU SYSTÉMU DISTANČNÍHO VZDĚLÁVÁNÍ S POŽADAVKY KYBERNETICKÉ BEZPEČNOSTI

Dílčí cíl 2, výstup č. 1, činnost č.2

Obsah

1. Základní vymezení

Pro potřeby tohoto analytického dokumentu je bezpečnost chápána z pohledu technického, personálního a procesního. Spojením vyjmenovaných zájmových oblastí definujeme celkovou kybernetickou bezpečnost systému distančního vzdělávání v prostředí Ostravské univerzity.

Problematika bezpečnosti systému distančního vzdělávání z pohledu netechnického, netechnologického, tedy pohledu vnímání různých psychologických stavů účastníků vzdělávání, není předmětem analýzy tohoto dokumentu.

Ostravská univerzita využívá pro podporu distančního vzdělávání zejména systémy Moodle LMS (dále jen "Moodle") a Microsoft Teams (dále jen "Teams"). Tyto systémy jsou doplňovány dalšími podpůrnými např. elektronická pošta, videokonferenčními systémy ZOOM nebo dokumentovými systémy z nich zásadní roli hraje univerzitní intranetové dokumentové úložiště studijních materiálů - Portal.

Systém Moodle a Teams jsou prostřednictvím integračních rozhraní propojeny se studijním systémem IS/STAG, který je dle zákona č. 181/2014 Sb. zákona o kybernetické bezpečnosti, vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 360/2020 Sb., určen univerzitou jako významný informační systém. Implementace integračního rozhraní je jedním z klíčových výstupů tohoto specifického cíle projektu.

Systémy distančního vzdělávání Ostravské univerzity nejsou určeny jako významné informační systémy. Tedy není povinností vyhovět všem kritériím a povinnostem daných zákonem o kybernetické bezpečnosti, avšak jejich propojenost se systémem studijní agendy je zásadní, a proto množina kritérií pro hodnocení souladu bude vycházet ze zmíněného zákona a vyhlášky o kybernetické bezpečnosti. Pro potřeby tohoto analytického dokumentu je vymezen rozsahem podpůrného dokumentu Minimální bezpečnostní standard vydaný Národním úřadem pro kybernetickou a informační bezpečnost[1]

1.1. Kybernetická bezpečnost

Kybernetická bezpečnost je soubor technologií, uživatelů, procesů a postupů navržených k ochraně univerzitních systémů, sítí, zařízení, programů a dat před kybernetickým útokem, poškozením, odcizením nebo neoprávněným přístupem a ztrátou. Je žádoucí pro potřeby tohoto analytického dokumentu si stanovit základní části kybernetické bezpečnosti, které budou analyzovány.

Části kybernetické bezpečnosti (a) organizační a (b) technická jsou definované Minimálním bezpečnostním standardem.

1.1.1. Organizační bezpečnost

Organizační část kybernetické bezpečnosti zahrnuje opatření zaměřená na ochranu systémů před útoky ze strany uživatelů. Mezi tato opatření patří například vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti, používání silných hesel a správců hesel, používání dvoufázové autentizace k zabránění neoprávněného přístupu a pravidelné aktualizace softwaru a aplikací k odstranění zranitelností.

Organizační část kybernetické bezpečnosti se také zabývá koordinací výzkumných a inovačních aktivit v oblasti kybernetické a informační bezpečnosti.

[1] Minimální bezpečnostní standard, NÚKIB, verze 1.2, 2023.

Základní vymezení části organizační bezpečnosti (personální, procesní):

a) Klasifikace a ochrana informací.
b) Řízení dodavatelů.
c) Řízení lidských zdrojů.
d) Řízení změn.
e) Řízení kontinuity činností.
f) Audit souladu s požadavky na kybernetickou bezpečnost.

1.1.2. Technická bezpečnost

Technická bezpečnost systémů zahrnuje soubor opatření a postupů, které jsou navrženy k ochraně a zabezpečení infrastruktury systému distančního vzdělávání. Zahrnuje také ochranu informací a dat před neoprávněným přístupem a zneužitím.

Základní vymezení části technické bezpečnosti:

a) Fyzická bezpečnost
b) Řízení přístupů
   - registrace, autentizace a identifikace uživatelů
   - politika hesel pro privilegované účty
   - politika hesel pro uživatelské účty
c) Požadavky v oblasti ochrany před škodlivým kódem
d) Bezpečnostní události a incidenty
e) Požadavky v oblasti aplikační bezpečnosti
f) Kryptografické prostředky
   - ukládání hesel
g) Požadavky pro zajištění dostupnosti služeb a informací
   - zálohování
h) Požadavky v oblasti cloudových služeb
i) Výjimky běhu, chyby hlášení
j) Ochrana systému distančního vzdělávání typu webové aplikace
k) Rozvoj systému
l) Komunikace, integrační rozhraní.

2. Analýza souladu stavu řešení s požadavky kybernetické bezpečnosti

Analýza souladu popisuje aktuální stav celého ekosystému distančního vzdělávání na Ostravské univerzitě z pohledu pracoviště Centra informačních technologií.

Pro potřeby tohoto analytického dokumentu byl stanoven následující rozsah systému distančního vzdělávání optikou informačních systémů:

a) Moodle LMS.

b) IS/STAG.

c) Microsoft 365 Teams.

d) Intranet univerzity Portal (studijní materiály).

2.1. Soulad organizační bezpečnosti

2.1.1. Klasifikace a ochrana informací

Cílem klasifikace informací a dat je stanovení jejich hodnoty. Na základě takto stanovené hodnoty je naplněn smysl, tedy ochrany informací a dat, a to navržením a implementací odpovídající ochrany.

Doporučení: *Vytvořit metodiku pro identifikaci a hodnocení informací. Provést identifikaci a hodnocení informací dle důležitosti (hodnocení z pohledu důvěrnosti, integrity a dostupnosti) v souladu s metodikou. Zařadit informace do výsledných úrovní. Vytvořit a zavést pravidla pro ochranu informací dle jednotlivých úrovní. Určit odpovědné osoby za vykonání výše uvedených činností.*

V prostředí univerzity k termínu červen 2023 není schváleno žádné organizační opatření na úrovni vedení univerzity, které by komplexně pokrylo oblast klasifikace a ochrany informací. Avšak je zpracováno několik organizačních opatření, které z pohledu ochrany osobních a citlivých údajů osob, svým dílčím způsobem tuto část řeší, a to ve formě Opatření rektora:

a) 134/2021: Knihovní řád Univerzitní knihovny Ostravské univerzity, Příloha č. 3: Zpracování a ochrana osobních údajů Univerzitní knihovnou Ostravské univerzity.

b) 102/2020: Ochrana duševního vlastnictví na OU.

c) 45/2018: Zpracování a ochrana osobních údajů na OU.

d) Informace o zpracování a ochraně osobních údajů (GDPR) v rámci internetové prezentace.

V rámci analytiky byly identifikovány další vnitřní předpisy, které mohu upravovat práci s informacemi a daty a stanovují určitá pravidla zejména pro důvěrnost a dostupnost:

e) Opatření rektora č. 88/2020: Etická komise OU.

f) Směrnice rektora č. 151/2010 k provoznímu řádu informačních systémů a sítě Ostravské univerzity v Ostravě.

Informace a data vytvářená a zpracovávaná v systému distančního vzdělávání lze v základu rozdělit do:

a) osobních a citlivých údajů studentů (osobní kontaktní údaje, zdravotní specifické údaje, množina studijních údajů a další),

b) osobní údaje akademiků, tj. vlastníků a tvůrců obsahu samotného vzdělávání,

c) lokalizační a provozní údaje distančního systému, jak uživatelů, tak provozu podpůrných aktiv systému.

Závěr: V čase zpracovávání tohoto analytického dokumentu jsou realizovány aktivity snažící se kategorizovat a identifikovat informace a data, která jsou na univerzitě zpracovávána. Analytika probíhá napříč celou organizační strukturou univerzity s cílem stanovit základní Politiku klasifikace informací ve formě vnitřního závazného předpisu, tj. opatření rektora.

Informace a data systému distančního vzdělávání nejsou žádnou specifickou kategorií.

2.1.2. Řízení dodavatelů

Cílem řízení dodavatelů je stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací a dat a vyžaduje jejich plnění. Smyslem je předcházení problémů při využívání služeb a systémů třetích stran, které by mohly mít dopad do provozu a řízení distančního vzdělávání ve formě kybernetických bezpečnostních událostí a co hůře pak incidentů.

Doporučení: *Identifikovat všechny dodavatele celého systému distančního vzdělávání. Stanovit pravidla podporující bezpečnost informací a dat a kontrolovat jejich plnění. Vytvořit šablonu smluvních ujednání, která by měla být součástí každého písemného smluvního vztahu, pokud tento vztah je možný.*

Identifikace základních dodavatelů částí systému distančního vzdělávání:

a) Moodle Pty Ltd – tvůrce open source systému Moodle LMS (privacy).

b) Západočeská univerzita v Plzni (ZČU) – tvůrce proprietárního systému studijní agendy (STAG), pro potřeby této analytiky pak části API systému, který je využíván integračním rozhraním systému Moodle.

c) PragoData Consulting, s.r.o. – tvůrce proprietárního integračního rozhraní systémů STAG a Moodle.

d) Microsoft – provozovatel množiny on-line služeb, zejména MS Teams.

Předmětem analytického dokumentu není detailně identifikovat každého dodavatele až na úroveň dodavatelů podpůrných aktiv. Avšak později navržená opatření, tj. ustanovení smluvních vztahů, mohou být součástí i smluvních vztahů těchto dodavatelů. Výčet podpůrných aktiv, tak jak je definuje legislativa kybernetické bezpečnosti je součástí interní Analýzy rizik univerzity.

Moodle

Systém Moodle využívá univerzita jako open source. Se společností, která je tvůrce tohoto systému nemá univerzita uzavřenu žádnou smlouvu o využívání, licenční smlouvu nebo smlouvu o poskytování služeb, včetně smlouvy o servisních službách. Moodle je provozován výhradně vlastními zdroji univerzity. Detailní technický popis systému Moodle je součástí analytického dokumentu Analýza současného technického a procesního zabezpečení na univerzitě – dokument je předmětem výstupu č.1 tohoto specifického cíle.

Západočeská univerzita v Plzni (ZČU)
Systém studijní agendy (STAG) je proprietární systém, který univerzita využívá na základě řádné Smlouvy o spolupráci. Tato smlouva již obsahuje minimální množinu ustanovení, které se snaží o nastolení souladu se základními požadavky kybernetické bezpečnosti:

a) Klasifikace, typy a priority incidentů. Tato část je formulována pohledem technickým, tedy není rozlišováno mezi událostí a incidentem z pohledu kybernetické bezpečnosti. Rozlišení je realizováno uvnitř helpdeskového systému univerzity při vlastním řízení a správě systému. V případě výskytu události může být tato klasifikována jako bezpečnostní událost nebo incident. Poté je eskalována na dodavatele s určením typu a priority.

b) Ochrana a zpracování osobních údajů. Tato část formuluje požadavky na správu a řízení osobních údajů zpracovávaných v systému STAG.

c) Řízení bezpečnosti. Určuje dodavatele jako významného dodavatele ve smyslu příslušné legislativy a zavazuje jej tímto k plnění povinností plynoucí z dané legislativy.

PragoData Consulting, s.r.o.
Programový balíček integračního rozhraní Moodle a STAGu. Smlouva obsahuje konzultační služby v dohodnutém rozsahu. Tato smlouva neobsahuje žádná ustanovení, byť jen náznakem se blížící jakékoliv povinnosti plynoucí z legislativy.

Závěr: V čase zpracovávání tohoto analytického dokumentu jsou realizovány aktivity snažící se definovat a stanovit množinu povinných smluvních ustanovení, které by zajistily akceptovatelný soulad smluvních vztahů s dodavateli, jenž jsou univerzitou označeny za významné. Popřípadě se k nim bude chovat jako k významným.

2.1.3. Řízení lidských zdrojů

Cílem řízení lidských zdrojů, tedy část personální kybernetické bezpečnosti, je obvykle pro jednoduchost omezována pouze na zvyšování bezpečnostního povědomí, stanovování procesů školení (povinná nebo nepovinná) popřípadě zajištění seznámení dodavatelů s bezpečnostními politikami.

Avšak pro potřeby tohoto dokumentu je snahou pokrýt i kapacity administrátorů, specialistů helpdesku a zohlednění rozsahu činností všech zapojených zaměstnanců (pohled technický, tj. zajištění IT služby systému distančního vzdělávání). Proto v definici názvu výstupu je uveden výraz personální.

Doporučení: *Poučit uživatele, administrátory a osoby zastávající bezpečnostní role o jejich povinnostech, teoreticky i prakticky je školit, s platnými bezpečnostními politikami seznámit nejen tyto uživatele, ale i relevantní osoby dodavatele a kontrolovat jejich dodržování.*

A. Zvyšování bezpečnostního povědomí

Jedním ze základních úkolů každého subjektu, bez ohledu na povinnost, která mu je přisuzována legislativou, jeho vnitřními procesy nebo čímkoliv jiným, je vzdělávat své uživatele. Univerzita má zpracovány on-line kurzy:

a) Základy kybernetické bezpečnosti. Školení v rozsahu pěti (5) modulů obsahující testování a možnost získat osvědčení o absolvování. Kurz je určen všem zaměstnancům studentům univerzity. Pro zaměstnance univerzity je povinný.

b) Řízení kybernetických událostí a incidentů. Vysvětluje specialistům IT, jak správně identifikovat událost a incident. Kurz je určený primárně pro zaměstnance pracoviště Centra informačních technologií.
c) Využití elektronického osobních certifikátu. Popisuje výhody využívání elektronických podpisů a šifrování dat.
d) Pošta a Antispam. Školení primárně pro nové zaměstnance obsahujíc prvky věnující se kybernetické bezpečnosti.

Je zpracováno opatření rektora č.133/2021: Metodika pro distanční průběh státní závěrečné zkoušky, které se svým obsahem dotýká problematiky bezpečnosti vzdělávání. Nicméně není zpracováno v podobě žádného vzdělávacího materiálu.

B. Personální zajištění systému

Personální zajištění systému distančního vzdělávání analyzujeme v rozsahu:

a) Aplikační, myšleno úvazek administrátora samotného systému Moodle.
b) Serverová, myšleno úvazek administrátora operačního systém, databázového systému, hardware serveru ať již fyzického, anebo virtuálního stroje.
c) Síťová, myšleno úvazek administrátora síťové infrastruktury.
d) Garant IS, myšleno role plynoucí z existujícího systému řízení informačních systémů, včetně systému řízení bezpečnosti informací. Role je dána organizačním opatřením Mapa klíčových procesů univerzity – příloha č.1 OR č. 156/2021 organizačnímu řádu Centra informačních technologií.
e) Množina tvůrců a konzumentů obsahu.

Závěr: Část vzdělávání v oblasti řízení lidských zdrojů na univerzitě je systémově řešena. Jsou připraveny vzdělávací kurzy, jsou realizovány osvětové aktivity ve formě článků, návodů, upozornění a vysvětlování možných rizik. Povinnost vzdělávat a projít školením kybernetické bezpečnosti je zakotvena v návrhu opatření rektora a je před schválením a vydáním. Je vydána závazná metodika pro distanční průběh státní závěrečné zkoušky. Na univerzitě existuje s podporou rektora univerzity odborná skupina zabývající se problematikou proctoringu.

Aktivity specializované pro distanční vzdělávání nejsou na univerzitě řešeny samostatně. Neexistuje žádný samostatný vzdělávací modul v jakékoliv formě např. online kurz, metodika, doporučení, který by se zabýval problematikou bezpečnosti distančního vzdělávání. Tato forma/způsob vzdělávání je řešena vždy jako samozřejmá součást celého systému vzdělávání.

Část personální je na tom výrazně hůře. Univerzita disponuje pouze jedním specialistou (administrátorem) systému Moodle. Neexistuje plnohodnotný zástup za tohoto primárního správce. Ano, v organizačním schématu a popisu pracovních činností vybraných zaměstnanců CIT je i sekundární správce (zástup) ovšem ten není plnohodnotný a není schopen plně zastoupit primárního. S takovým to výstupem lze realizovat analýzu i u serverové a síťové vrstvy systému, kde je situace nepatrně lepší.

Principiálním problémem je dlouhodobá přetíženost jednotlivých administrátorů, která s nárůstem činností vyžadovaných kybernetickou bezpečností se stává zcela kritickou. Je významným rizikem s kritickým dopadem.

2.1.4. Řízení změn

Cílem je průběžná identifikace všech změn systému distančního vzdělávání. Obecně změn ve všech analyzovaných částech a to technických, personálních i procesních. Zhodnocení identifikovaných změn ve smyslu dopadu na systém distančního vzdělávání. Zajímá nás zejména dopad, který může negativně ovlivnit dostupnost, integritu a důvěrnost celého systému včetně informací a dat. V této kapitole z pohledu technického.

Doporučení: *Při provozu systému distančního vzdělávání řešit problematiku řízení změn a konfigurací. Zahrnující evidenci všech změn, systematické vyhodnocování, koordinování a implementaci schválených změn a konfigurací. Zejména aktivity:*

a) přijímání opatření pro snížení nepříznivých dopadů na spravovaný systém,

b) aktualizace relevantních bezpečnostních politik a bezpečnostní dokumentace,

c) testování změn a zajištění možnosti navrácení do původního stavu.

Univerzita nemá aplikován žádný ucelený a formální systém pro řízení změn. Realizuje pouze vybrané části.

V rámci přijatých organizačních, konkrétně opatření č. 156/2021 k Organizačnímu řádu CIT a současně Směrnicí rektora č. 151/2010 k provoznímu řádu informačních systémů a sítě Ostravské univerzity je definována povinnost evidence všech požadavků na IT v rámci helpdeskového systému. Je zde také v základu popsán proces změn v rozsahu:

a) kdo má právo podat návrh na změnu,

b) jakým prostředkem se má návrh na změnu podávat,

c) kdo analyzuje podaný návrh, a to z pohledu (technického, ekonomického, personálního),

d) dopady návrhu na jiné systémy, včetně konzultace a souhlasu dotčených systémů a jejich Garantů,

e) proces kolizí zejména personálních kapacit IT.

V každém z uvedených kroků je analyzován dopad na dostupnost, integritu a důvěrnost dat.

Závěr: Proces řízení změn je aktuálně formalizován, vydán v rámci řídící normy a dodržován pro všechny dílčí systémy distančního vzdělávání (Moodle, Teams, Portal a další). V době vzniku tohoto analytického dokumentu je v připomínkovém řízení aktualizace organizačního opatření „Politika provozní bezpečnosti ICT“, která lépe popisuje proces řízení změn.

Avšak stále není v prostředí univerzity dostatečně řešena problematika *„testování změn a zajištění možnosti navrácení do původního stavu“*. Ano, jsou realizovány aktivity na úrovni správce Moodlu a příslušných serverů, které umožní v případě zásadní havárie systém obnovit. Nicméně tato činnost vzhledem k provozu není v pravidelných cyklech testována, a proto není vyzkoušeno, zda obnova je reálná, nebo jen teoretická.

2.1.5. Řízení kontinuity činností

Smyslem řízení kontinuity činností je zajistit odpovídající dostupnost služeb systému distančního vzdělávání, a to na úrovni organizační (personální, procesní) a technické. Mít k dispozici množinu plánů (postupů), které zajistí minimalizaci výpadků dostupnosti služby systému distančního vzdělávání.

Doporučení: *Ideálním stavem vyplývajícím jednak z legislativy, ale také z doporučené praxe, je mít vypracován plán kontinuity (Business Continuity Plan – BCP) a plán obnovy systému (Disaster Recovery Plan – DRP). V případě, že nic takového neexistuje, mít alespoň souhrn aktivit a prostředků, které umožní základní obnovu systému po havárii.*

Ostravská univerzita nemá zpracovány žádné plány kontinuity, ani plány obnovy po havárii a na základě analytických pohovorů nejsou zpracovány ani žádné postupy obnovy ze zálohy. Všechna znalost je držena individuálně u správců.

Následující analytický výstup se drží přesně základních bodů popsaných v rámci dokumentu Minimální bezpečnostní standard NÚKIB v.1.2:

a) Práva a povinnosti administrátorů, kteří se podílejí na správě systému distančního vzdělávání mají své povinnosti popsány v popisu pracovních činností. V žádném popisu činností není explicitně uvedeno, že jsou povinní podílet se nebo přímo vytvářet a testovat jakékoliv plány obnovy svěřeného systému. Nejsou stanoveny havarijní postupy a komunikační postupy a další.

b) Nejsou systémově hodnocena možná rizika ovlivňující negativně dostupnost systému. Nejsou popsány žádné scénáře v rámci, kterých jsou zachyceny alespoň základní situace a postupy, jak se v těchto situacích chovat. Není popsáno, jak se tyto situace mohou promítnout do dostupnosti, integrity a důvěrnosti dat.

c) Analýza identifikovala částečné plnění v rámci určitých fragmentů servisních smluv s dodavateli vybraných podpůrných aktiv. Avšak smluvní ujednání nemusí vždy odrážet realitu o čemž svědčí mnoho konkrétních případů útoků mimo naši univerzitu.

Závěr: Problematika a zejména nutnost vytvoření alespoň základních plánů obnovy systému po havárii byla přednesena v rámci porady vedení pracoviště Centra informačních technologií. Velmi ojediněle některé týmy tuto problematiku otevřely a vzaly si ji „za svou“ a začaly se zamýšlet nad možnými scénáři. Avšak denní provoz a priority jiných projektů tuto aktivitu upozadily. Nešvarem, který oddaluje započetí prací na plánech je obvykle vyžadování šablony, která by určila strukturu takového plánu obnovy po havárii. Problém je, že taková šablona, byť sebelepší, nevytvoří obsah samotného plánu. Zbytečně nutí administrátora do vyplňování kapitol, kterým nerozumí a nevedou k cíli (administrátor nesnáší papírování).

V roce 2023 je definován a schválen vedením univerzity úkol analyzovat problematiku havarijního plánování a krizového řízení s výstupy popisující zvládání bezpečnostních událostí a incidentů. Současně proběhla opakovaná individuální setkání se správci systémů s žádostí o reálné zamyšlení se nad plány obnovy po havárii.

2.1.6. Audit souladu s požadavky na kybernetickou bezpečnost

Smyslem auditů je prověřit soulad mezi stanoveným cílem, předepsaným kritériem a aktuálním stavem systému distančního vzdělávání. Audit má být prováděn ve stanovených intervalech, tj. opakovaně a současně nezávisle, což je velmi důležité.

Doporučení: *Pro zhodnocení stavu kybernetické bezpečnosti je vhodné v pravidelných intervalech provádět nezávislý audit kybernetické bezpečnosti. Audit kybernetické bezpečnosti upozorní na nalezené rozdíly, případné nedostatky a potenciální oblasti ke zlepšení.*

Univerzita v pravidelných intervalech, které jsou dány z rozhodnutí vedení, realizuje audity vlastním/interním auditem, který je podřízen přímo rektorovi OU. Plán auditu stanovuje po dohodě

s rektorem OU auditor. Realizované audity nevyhodnocují soulad s legislativou určující kybernetickou bezpečnost, avšak spíše shodou okolností mohou řešit vybrané procesní části distančního vzdělávání. Výjimkou je pak personální část.

Realizován audit v období září až prosinec roku 2021:

a) zjišťující soulad stavu univerzity s požadavky zákona a vyhlášky o kybernetické bezpečnosti,

b) provedena analýza rizik.

Obě aktivity se dotýkaly systému distančního vzdělávání, byť nepřímo, protože řešily systém studijní agendy (STAG) jako významný informační systém a primární aktivum a soustavu podpůrných aktiv.

Závěr: Audity souladu s požadavky kybernetické bezpečnosti nejsou v rámci systému distančního vzdělávání řešeny systémově. Jsou prováděna pouze technická šetření při identifikaci zranitelnosti se snahou najít vhodné technické opatření a to implementovat. Identifikace a implementace je evidována v helpdeskového systému pracoviště CIT.

2.2. Soulad technické bezpečnosti

2.2.1. Fyzická bezpečnost

Cílem fyzické bezpečnosti je zajištění ochrany zejména důvěrnosti a integrity informací a dat.

Doporučení: *Definovat nový či rozšířit stávající soubor opatření předcházející poškození, krádeži či zneužití informací či majetku nebo přerušení poskytování služeb informačního nebo komunikačního systému, vymezit fyzický perimetr.*

Fyzická bezpečnost univerzity začíná řízeným přístupem na pracoviště Centra informačních technologií, tj. budovy, která obsahuje kanceláře příslušných administrátorů a zázemí infrastruktury (serverové, síťové, datové). Prostory budovy jsou chráněny soustavou opatření:

a) nejsou volně přístupné; přístup do prostor je umožněn pouze vybraným zaměstnancům pracoviště CIT, všem ostatním pouze se souhlasem a doprovodem oprávněného zaměstnance CIT,

b) prostory jsou chráněny kamerovým systémem se záznamem a přístupovým systémem, který je napojen na službu Centrálního pultu ochrany s režimem 24/7,

c) prostory jsou zabezpečeny také protipožárními čidly,

d) prostory kanceláří uvnitř budovy jsou zabezpečeny zámky, a kromě vybraných specifických míst nejsou přístupny bez klíče.

Infrastruktury univerzity, tj. vybraná podpůrná aktiva, systému distančního vzdělávání jsou umístěna a chráněna v technologických místnostech s řízeným přístupem a definovanými pravidly.

Závěr: Není proveden žádný audit fyzické bezpečnosti, který by popsal stav technologických místností mimo centrální pracoviště CIT, tj. fakultních místností. Není přijat žádný systém pravidelných kontrol dodržování definovaných pravidel.

2.2.2. Řízení přístupu

Cílem řízení přístupu je jednoznačně identifikovat každého uživatele využívajícího informace, data a služby systému distančního vzdělávání. Evidovat a řídit přidělování přístupových oprávnění a stanovovat pravidla pro autentizaci těchto uživatelů.

Doporučení: *Přidělit jedinečné identifikátory jednotlivým uživatelům a administrátorům přistupujících k informačnímu nebo komunikačnímu systému. Řídit a evidovat identifikátory, přístupová práva a oprávnění aplikací a technických účtů. Provádět řízení přístupu na základě skupin a rolí.*

Problematiku řízení přístupu můžeme rozdělit do dvou základních částí a těmi jsou (a) uživatelé a (b) zařízení. Pro potřeby tohoto analytického dokumentu, jehož cílem je mapovat soulad systému distančního vzdělávání s požadavky bezpečnosti, se budeme věnovat části (a) uživatelů.

Ostravská univerzita spravuje a řídí vznik, blokaci, zánik uživatelských kont a s tím spojených přidělených, řízených a odebraných přístupových oprávnění nejednotně. Není nasazen žádný ucelený systém řízení identit tzv. systém IdM.

A. Registrace, autentizace a identifikace uživatele

Identita uživatele vzniká v systému LDAP, uživateli je přiřazen jednotný identifikátor a nemá přidělenu žádnou základní množinu přístupových práv. Práva jsou nastavena v jednotlivých systémech. Tedy uživatel získá přístup do systému Moodle, STAG, systému Teams, intranetu Portal a studijním dokumentům, ale do těchto systémů jde pouze s „vybavením“ student, zaměstnanec, externista, včetně množiny dalších speciálních „stavů“. Není mu přiřazena žádná role ve smyslu organizačního řízení univerzity. Role je definována v daných systémech samostatně a odděleně.

Systém Moodle ani systém Teams nepracuje s žádnou rolí uživatele, pokud mu není přímo administrátorem systému přiřazena, a to na základě žádosti v helpdeskovém systému a příslušným schválením, pokud je vyžadováno. Žádá zaměstnanec (uživatel) nebo jeho přímý nadřízený, schvaluje pak obvykle Garant systému (kapitoly Řízení lidských zdrojů a Řízení změn).

Uživatel systému Moodle má role dle nastavení Kurzu. Tedy v jednom může být učitel a v mnoha dalších jen jako student. O přiděleném oprávnění rozhoduje autor kurzu.

Monitorování činnosti uživatele je realizováno v příslušném systému.

B. Politika hesel pro privilegované a uživatelské účty

Jsou stanoveny základní pravidla pro délku hesla, a to jaké znaky heslo musí obsahovat. Není rozlišováno mezi uživatelským a privilegovaným účtem uživatele. Aktuálně nastavená pravidla a systém vzniku uživatelských hesel, zejména pro studenty, je identifikován jako významné riziko zejména pro důvěrnost a integritu informací a dat systému distančního vzdělávání.

Závěr: V době tvorby tohoto analytického dokumentu je implementován jednotným systém pro správu uživatelů, systém IdM. Systém změní skladbu uživatelského konta, sjednotí více kont uživatele do jednoho a připraví zázemí pro správu a řízení rolí. Ukončení projektu je plánováno na polovinu roku 2024.

Součástí této implementace je také přijetí nového OR Zajištění provozní bezpečnosti ICT, které stanovuje závazné procesy pro vytvoření, blokaci a smazání uživatelských kont. Stanovuje přesné lhůty a délky blokací kont. Významně mění proces vzniku, změny a resetu uživatelských hesel.

2.2.3. Požadavky v oblasti ochrany před škodlivým kódem

Smyslem aktivit a přijímání opatření pro ochranu systému před škodlivým kódem je zvyšování jeho bezpečnosti.

Doporučení: *Segmentovat síť, instalovat příslušný software a pravidelně jej aktualizovat.*

Univerzita důsledně implementuje segmentaci sítě. Systém distančního vzdělávání v rozsahu identifikovaných informačních systémů viz. kapitola č. 2 je rozdělen do samostatných podsítí a záleží na konkrétních částech systému ve smyslu WWW rozhraní a dále části aplikační, serverová, databázová, virtualizační, včetně prostředí cvičného a testovacího (týká se Moodle LMS). Zásadní je i část pro zálohování.

Serverová i aplikační část je chráněna soustavou opatření, příklady opatření[2]:

a) monitoring prostředků serveru – využití diskového prostoru, běh služeb na portech 80 a 443, expirace certifikátů, zatížení serveru, počty procesů, kontrolní součty vybraných souborových adresářů a další,

b) monitoring prostředků databáze a běhu provozovaných instancí Moodle LMS,

c) pravidelná kontrola na viry a zranitelnosti,

d) sbírání logů a jejich následné vyhodnocování.

V prostředí distančního vzdělávání jsou aplikovány vydané aktualizace a postupně implantováno nové bezpečnostní rozhraní mezi systémy IS/STAG a Moodle LMS. Implementace je předmětem jednoho z výstupů projektu.

Závěr: Je nezbytné přijmout taková vnitřní opatření, která umožní včasnou implementaci všech relevantních aktualizací systému. Praxe ukazuje, že aktuálně navržené opatření v rámci Zajištění provozní bezpečnosti (k 06.2023 není nová norma stále vydána jako závazný vnitřní předpis) definující několika týdenní období v roce, kdy lze aplikovat aktualizace a mít možnost odstávek systému je nedostatečné, byť se zdá prozatím jediné „politicky“ průchodné. Je nezbytné definovat vnitřní standard pracoviště CIT pro sběr a vyhodnocování provozních a lokalizačních údajů částí systému.

2.2.4. Bezpečnostní události a incidenty

Cílem řízení bezpečnostních událostí a incidentů je efektivně a systémově řešit a řídit narušení bezpečnosti důvěrnosti, integrity a dostupnosti systému distančního vzdělávání.

Doporučení: *Stanovit pravidla pro vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů, evidovat a analyzovat kybernetické bezpečnostní události a incidenty za účelem eliminace dalšího výskytu, stanovit auditní požadavky.*

Univerzita realizuje vybrané postupy při řízení kybernetických bezpečnostních událostí a incidentů, které se dají rozdělit do částí procesní, technické a personální.

A. Procesní

Pracoviště CIT navrhlo proces řízení kybernetických bezpečnostních událostí a incidentů. Návrh je v době přípravy tohoto dokument ve stavu připomínkování uvnitř pracoviště CIT. Součástí návrhu jsou

[2] Z bezpečnostních důvodů nejsou uvedeny přesné názvy programů, kterou jsou využívány, byť jsou většinou postaveny na platformě open source. Technický detail je součásti vnitřní analýzy pracoviště CIT – Analýza sběru provozních a lokalizačních údajů.

stanovené postupy identifikace událostí a incidentů a povinnost evidence v rámci helpdeskového systému CIT.

V helpdeskovém systému jsou nastaveny automatizmy, které pomáhají Referátu kybernetické bezpečnosti evidovat všechny události, vyhodnocovat jejich mírů závažnosti, identifikovat incidenty a z nich plynoucí další postupy mitigace.

B. Technické

Neoddělitelnou součástí poskytování služeb CIT je helpdeskový systém. Jsou přijata vnitřní opatření na úrovni organizačního opatření rektora, která stanovuje helpdeskový systém jako jediné možné místo pro žádání o služby CIT (vyjma výjimečných a individuálních situací). Nicméně povinností každého specialisty CIT je zajistit auditovatelnost řešených požadavků. Každý požadavek na úpravu, nahlášený nedostatek, problém, cokoliv je vyhodnocen příslušným specialistou a může být označen za bezpečnostní událost.

Detailní analýza sběru a vyhodnocování provozních a lokalizačních údajů, zejména v prostředí systému Moodle, STAGu, Portalu a Teams není předmětem této analýzy. Jsou řešeny na úrovni správy a pokud je identifikována bezpečnostní událost je okamžitě řešena v rámci helpdeskového systému.

C. Personální

Pracoviště CIT má vytvořen specifický on-line kurz věnující se správné identifikaci bezpečnostních událostí a incidentů. Proběhly semináře s vybranými specialisty CIT a kontinuálně se diskutuje s jednotlivými vedoucími oddělení CIT s cílem zlepšit identifikaci všech „skutečností a stavů systému“, které mohou mít charakter bezpečnostní události.

Závěr: Jednotlivé části procesu řízení kybernetických bezpečnostních událostí a incidentů jsou řešeny pouze částečně. V některých momentech spíše neformálně než, aby se řídily jasným a schváleným postupem (metodikou). Je nezbytné minimálně uvnitř pracoviště CIT přijmout jasné a srozumitelné postupy, zejména pro část řešení událostí a incidentů.

Rozvoj metod sběru provozních a lokalizačních údajů jednoznačně ukazuje na zásadní nedostatek personálních kapacit pro kvalifikovanou analýzu vytvářených dat. Tento nedostatek se stává kybernetickou bezpečnostní událostí.

Dalším zásadním nedostatkem je absence schválených a pravidelně testovaných plánů obnovy ze zálohy a sytému po havárii. Přesto, že tyto postupy jsou realizovatelné, spoléhají se pouze na individuální aktuální kvalifikaci a odbornost specialistů.

2.2.5. Požadavky v oblasti aplikační bezpečnosti

Stanovení základních požadavků a principů pro oblast aplikační bezpečnosti a jejího testování.

Doporučení: *Provádět testování v odděleném prostředí, stanovit pravidla pro testovací data.*

V prostředí univerzity pro systém distančního vzdělávání probíhají nesystémové, myšleno ad-hoc testy částí systému. Pro prostředí Microsoft, jehož součástí je služba MS Teams probíhají testy zranitelností[3], resp. zjišťování zabezpečení celého prostředí např. prostřednictvím služby Microsoft 365 Defender, který vyhodnocuje míru bezpečnosti proti referenčním hodnotám stanovených samotným Microsoftem.

[3] Detailní výstupy testů jsou z bezpečnostních důvodů součástí interních materiálů CIT. Dostupné lokálně na pracovišti CIT, a to po dohodě a souhlasu Manažera kybernetické bezpečnosti.

V prostředí Moodle neprobíhají žádné systémové testy, ať již vnitřní analýzou administrátora za použití nástrojů vlastních nebo třetích stran. Neprobíhá žádné penetrační testování. Jsou pouze identifikovány a řešeny hlášené zranitelnosti na úrovni tvůrce Moodle (bezpečnostní aktualizace, implementace nových verzí).

V prostředí intranetu Portal probíhá interní testování v rámci Oddělení vývoje a to na úrovni (a) aplikačního zázemí Portalu, IBM WepSphere Portal na kterém intranet běží a současně (b) samotných aplikací a systémů, které jsou vyvíjeny uvnitř oddělení.

Závěr: V prostředí univerzity nejsou nastaveny žádné povinné postupy pro oblast aplikační bezpečnosti. Je nezbytné tyto postupy navrhnout a implementovat do rutinního provozu pracoviště CIT.

2.2.6. Kryptografické prostředky

Smyslem využívání kryptografických prostředků je ochrana dat a informací prostřednictvím tzv. šifrování, a to nejlépe během celého jejich životního cyklu, tedy jak při jejich uložení, tak při jejich přenosu, zpracování, a také zálohování.

Doporučení: *Zajistit šifrování přenosu dat. Šifrování uložených dat je pouze doporučeno, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.*

Využití kryptografických prostředků v systému distančního vzdělávání můžeme v prostředí univerzity rozdělit na části:

a) zpracování a ukládání dat na diskových prostředcích univerzity a současně prostředcích Microsoftu,

b) přístup k těmto datům prostřednictvím autentizace a autorizace oprávněného uživatele, tj. práce s hesly,

c) individuální ukládání dat uživatelů na vlastních soukromých prostředcích a prostředcích třetích stran.

Data systému distančního vzdělávání nejsou nikterak šifrována, a to ve smyslu šifrování diskového prostoru, kde jsou uložena. Je šifrována cesta k těmto datům (šifrovaná komunikace), tedy přenos dat od uživatele na diskový prostor.

Je tedy zaručen autorizovaný přístup k těmto datům a informacím. Systémy distančního vzdělávání nepracují s hesly při autentizaci a následné autorizaci s hesly uživatelů ve smyslu jejich ukládání. Z těchto systémů tedy není možné uživatelské heslo offline útokem získat.

Závěr: Systém distančního vzdělávání využívá standardní metody šifrování a zajišťuje šifrovanou komunikaci, integritu komunikace a ověřuje identitu vzájemně komunikujících díky SSL certifikátům komunikujících stran (serverů).

2.2.7. Požadavky pro zajištění dostupnosti služeb a informací

Smyslem požadavků na zajištění dostupnosti systému distančního vzdělávání je mít služby systému, včetně dat vždy, kdy je to pro výkon činnosti nutné.

Doporučení: *Stanovit základní parametry dostupnosti, navrhnout vhodnou architekturu řešení.*

A. Dostupnost služeb

Univerzita stanovuje prostřednictvím organizačního opatření rektora č. 156/2021 organizační řád Centra informačních technologií a přílohy č.1 Mapa klíčových procesů univerzity základní parametry dostupnosti systémů Moodle, Microsoft a Portal. Těmito parametry jsou:

a) očekávaná doba provozu: požadovaná doba provozu je vyjádřena počtem hodin za den / počtem dnů v týdnu. Současně jsou uvedeny hodiny Od – Do v pracovních dnech.

b) priorita: priorita IS je dána v rozsahu P1 až P3. Tato priorita odráží požadavek na celkovou dostupnost IS, ale současně důležitost IS při financování provozu a rozvoje tohoto IS. Současně priorita určuje váhu řešení při souběhu několika požadavků z různých IS. Požadavky u IS s prioritou P1 jsou řešeny přednostně, pak následují P2 a P3. V rámci všech priorit IS je zákaznická podpora dostupná vždy 8/5, tj. od 8:00 do 16:00 v pracovních dnech.

V případě části služby Teams očekávaná a předpokládaná doba provozu 24/7 není plně řízena specialisty CIT univerzity. Vzhledem k charakteru služby, tzv. cloud služby, tato běží na prostředcích mimo infrastrukturu univerzity. Jsou využívány prostředky společnosti Microsoft.

B. Architektura

Nelze architekturu systému distančního vzdělávání popsat jednotně, protože je jiná pro systém Moodle, systém Teams a systém intranetu Portal. V této kapitole dokumentu se omezíme na Moodle.

Moodle je provozován na virtuálních serverech. Je tvořen množinou samostatných instancí, které nabízí různé druhy kurzů s různým zaměřením. Počínaje základní instancí pro výuku univerzity a konče specializovanými fakultními instancemi pro výuku nebo projektovými instancemi. Pro základní instanci je provozován také cvičný / testovací server.

Detailní popis architektury je obsahem dokumentu Analýza současného stavu v rámci zveřejněných výstupů Specifického cíle C2 na univerzitních stránkách Národního plán obnovy pro oblast vysokých škol pro roky 2022–2024.

C. Zálohování

V kapitole zálohování dokumentu se omezíme na systém Moodle. Tento je zálohován v intervalu denně s uchováním zálohy na 30 dnů. Zálohování probíhá ve večerních hodinách.

Závěr: Univerzita nemá stanovena závazná pravidla pro proces zálohování.

2.2.8. Požadavky v oblasti cloudových služeb

Cílem je zajištění kybernetické bezpečnosti při využívání cloudových služeb.

Doporučení: *V případě, že je využíváno cloudových služeb pro provoz informačního nebo komunikačního systému, zajistit kybernetickou bezpečnost i z pohledu těchto služeb, a to bez ohledu na to, jaký typ cloudové služby je používán (IaaS, PaaS, SaaS). Na poskytovatele cloudových služeb je potřeba vztáhnout stejná pravidla jako pro ostatní dodavatele.*

Pro potřeby distančního vzdělávání univerzita využívá cloudových služeb společnosti Microsoft, konkrétně službu Teams. Teams je propojen s IS/STAG a je schopen na vyžádání příslušného akademika automaticky vytvořit požadovanou studijní skupinu, včetně přihlášených studentů. Obsah tohoto vzdělávacího „objektu“ je tvořen individuálně dle potřeb akademika a studentů.

Se společností Microsoft má univerzita uzavřenu řádnou smlouvu:

a) je deklarováno, že data naší univerzity jsou umístěna v rámci EU,

b) služby jsou poskytovány dle ISO/IEC 2001 a v souladu s GDPR,

c) komunikace je šifrována,

d) smlouva o poskytování služeb obsahuje podmínky SLA,

Závěr: Univerzita nedisponuje žádným analytickým dokumentem, který by detailně vyhodnotil na jednom místě soulad s požadavky tohoto standardu.

2.2.9. Další požadavky

Standard minimálního zabezpečení vyjmenovává několik dalších požadavků na zajištění bezpečnosti:

a) výjimky běhu, chyby a hlášení,

b) ochrana systému distančního vzdělávání typu webové aplikace,

c) rozvoj systému,

d) rozvoj informačních a komunikačních systémů.

V této kapitole se budeme věnovat jen několika požadavkům, a to výjimkám a chybám a ochraně webových aplikací.

A. Výjimky běhu, chyby hlášení

Řízení výjimek a zabránění neřízeného selhání běhu informačního nebo komunikačního systému.

Doporučení: *Stanovit proces řízení výjimek a jejich evidence.*

Univerzita v rámci provozovaného systému distančního vzdělávání zaznamenává v podobě logů provozní a lokalizační údaje vybraných částí systému. Tyto logy vyhodnocuje a kontroluje kvalitu dostupnosti informací, dat a služeb.

Snahou je systematicky logy zpracovávat a vyhodnocovat na jednom centrálním místě v rámci log managementu.

Závěr: Univerzita nemá stanoven žádný proces pro identifikaci, vyhodnocování a řízení výjimek v běhu služeb. K těmto činnostem je přistupováno individuálně, dle rozhodnutí příslušných specialistů CIT je nastavována míra detailu sběru provozních a lokalizačních údajů.

Je nezbytné příslušný proces řízení výjimek standardizovat, měřit, vyhodnocovat a zlepšovat.

B. Ochrana systému distančního vzdělávání typu webové aplikace

Smyslem je zvyšovat ochranu webových aplikací systému distančního vzdělávání proti nejčastějším útokům.

Doporučení: *Řídit se doporučeními OWASP a věnovat pozornost zranitelnostem.*

Není předmětem tohoto analytického dokumentu detailně rozebírat soulad jednotlivých vyjmenovaných zranitelností. Jak je patrné z předcházejících kapitol pro distanční vzdělávání není přijat žádný ucelený systém řízení bezpečnosti informací a není tedy prováděno žádné systémové testování (penetrační testování), popřípadě systémové monitorování zranitelností – identifikované např. nezávislým společenstvím OWASP.

V případě využívaných systémů Moodle, Teams, Portal, IS/STAG jsou sledovány zranitelnosti identifikované tvůrci/výrobce daných systémů.

Závěr: Nastíněno v předešlém odstavci. Je nutné, aby univerzita přijala taková procesní, technická a personální opatření, která zajistí systémové vyhodnocování zranitelností a následně návrh a implementaci vhodných opatření.

3. Zhodnocení

Analytický dokument nepracuje s žádnými jasně definovanými a měřitelnými ukazateli v podobě číselných hodnot. Přesto, že základní materiál, vůči kterému se hledá soulad současného stavu distančního vzdělávání k požadavkům kybernetické bezpečnosti je slušnou základnou a ukazatele by se daly definovat. Pro potřeby této analýzy je to ovšem zbytečné. Současně bezpečnost distančního vzdělávání není věcí jen technickou, ale také procesní a personální.

Zda dělá univerzita pro bezpečnost distančního vzdělávání dost? Bohužel z každé kapitoly tohoto dokumentu je zřejmé, že ne. Je zapotřebí se na problematiku podívat vždy pohledem technickým, personálním a procesním.

Z pohledu technického, použiji-li jako autor nekorektní, ale výstižné pojmenování, úplně oči neštípou. Je realizováno mnoho na první pohled nepostřehnutelných opatření, monitorování a vyhodnocování provozních a lokalizačních údajů o chodu informačních systémů distančního vzdělávání, včetně podpůrné infrastruktury. S těmito údaje se pracuje.

Z pohledu procesního a personálního je situace výrazně jiná. Výrazně špatná. Kritická je část personální. Nedostatek personálních kapacit způsobuje:

a) dlouhodobé přetížení,

b) frustraci, demotivaci, vyhoření,

c) takřka zastavení odborného rozvoje příslušného specialisty CIT,

d) nulová systematická práce s vyhodnocováním stavu bezpečnosti svěřeného systému,

e) reálné riziko neplnění udržitelnosti povinné z projektů, není, kdo by systémově pracoval s pořízeným HW nebo SW.

Uvedené body nejsou obecným „literárním“ pojmenováním pro dosažení nějakého efektu (dramatického závěru dokumentu), ale zcela reálnými a konkrétním riziky, která se na pracovišti Centra informačních systémů již projevily a projevují.

Zhodnocení pohledu procesního? Ostravská univerzita distanční vzdělávání neřeší systémově.