ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

MASARYKŮV ÚSTAV VYŠŠÍCH STUDIÍ

DIPLOMOVÁ PRÁCE

Metodika implementace TISAX®
pro dodavatele automobilového průmyslu

TISAX® Implementation Methodology
for Automotive Industry Suppliers

2024

Lenka Králová

Studijní program: Projektové řízení inovací

Vedoucí práce: Ing. Oldřich Bronec, CSc.

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Králová** Jméno: **Lenka** Osobní číslo: **516715**

Fakulta/ústav: **Masarykův ústav vyšších studií**

Zadávající katedra/ústav: **Institut manažerských studií**

Studijní program: **Projektové řízení inovací**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Metodika implementace TISAX pro dodavatele automobilového průmyslu

Název diplomové práce anglicky:

TISAX Implementation Methodology for Automotive Industry Suppliers

Pokyny pro vypracování:

Metodika implementace TISAX pro dodavatele do automobilového průmyslu za účelem posílení kybernetické bezpečnosti
V teoretické části práce popíše technologii TISAX a vysvětlí její účel a přínosy.
V praktické části navrhne metodiku této technologie pro konkrétního výrobce z oblasti automobilového průmyslu tak, aby tento systém a jeho užívání garantovali maximální kybernetickou bezpečnost dat

Seznam doporučené literatury:

Alexandre Dolgui, Dmitry Ivanov, and Boris Sokolov: Supply Network Dynamics and Control, Springer, Cham, Švýcarsko, 2022
Dokumentace Národního úřadu pro kybernetickou a informační bezpečnost
Florian Gleich: TISAX Participant Handbook, ENX Association, Boulogne-Billacourt, Francie, 2023
Dokumentace TISAX
Dokumentace vybrané firmy

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Oldřich Bronec, CSc. Masarykův ústav vyšších studií ČVUT v Praze

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **08.12.2023** Termín odevzdání diplomové práce: **25.04.2024**

Platnost zadání diplomové práce: _____

Ing. Oldřich Bronec, CSc. podpis vedoucí(ho) práce	Ing. Dagmar Skokanová, Ph.D. podpis vedoucí(ho) ústavu/katedry	prof. PhDr. Vladimíra Dvořáková, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomantka bere na vědomí, že je povinna vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání _____ Podpis studentky _____

KRÁLOVÁ, LENKA. *Metodika implementace TISAX® pro dodavatele automobilového průmyslu.* Praha: ČVUT 2024. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracovala samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citovala a uvádím je v přiloženém seznamu použité literatury.

Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: 17.04.2024 Podpis:

Poděkování

Ráda bych touto cestou vyjádřila poděkování Ing. Oldřichovi Broncovi, CSc. za odborné vedení mojí diplomové práce, jeho ochotu a vstřícnost při konzultacích.

Dále bych chtěla velmi poděkovat Ing. Martinovi Drastichovi, Ph.D., MBA za jeho expertní přístup a cenné rady během tvorby této diplomové práce.

Na závěr bych chtěla upřímně poděkovat mojí rodině za její neustálou podporu, lásku a trpělivost během mého studia a psaní této diplomové práce. Bez její podpory by dosažení toho milníku nebylo možné.

Abstrakt

Cílem této diplomové práce je navrhnout metodiku implementace TISAX® pro dodavatele z oblasti automobilového průmyslu tak, aby tento systém a jeho udržování garantovaly maximální kybernetickou bezpečnost informací a dat. Teoretická část práce zdůrazňuje potřebu ochrany informací a dat v dodavatelském řetězci, poukazuje na důležitost kybernetické bezpečnosti, uvádí přehled aktuálně platné i připravované legislativy, včetně kybernetického zákona a směrnice Evropské unie „NIS 2“, která musí být transponována do národního práva do října 2024. Především pak představuje systém TISAX® jako možný nástroj pro zabezpečení informací, ochranu prototypů a ochranu údajů a způsob jeho hodnocení a získání známky TISAX® k prokázání informační bezpečnosti. Praktická část práce představuje vybranou organizaci, která je dodavatelem výrobce automobilů OEM, jehož požadavkem je prokázání úrovně správy zabezpečení informací implementovaným systémem TISAX®. Výsledkem práce je návrh metodiky implementace systému TISAX® vycházející z provedeného hloubkového porovnání norem zabývajících se systémy managementu bezpečnosti informací, jejich požadavky a opatřeními, hodnotícího katalogu ISA, ve kterém jsou na základě kontrolních otázek definovány požadavky systému TISAX® dle stanovených cílů hodnocení, a Příručky pro účastníky systému TISAX®.

Klíčová slova

kybernetická bezpečnost, systém managementu bezpečnosti informací, TISAX®, informační bezpečnost, ochrana prototypu, ochrana údajů, automobilový průmysl, dodavatelský řetězec, OEM, ISMS

Abstract

The aim of this thesis is to propose a TISAX® implementation methodology for suppliers from the automotive industry so that this system and its maintenance can guarantee maximum cyber security of information and data. The theoretical part of the thesis emphasizes the need for information and data protection in the supply chain, points out the importance of cyber security, provides an overview of the currently valid and upcoming legislation, including the cyber law and the European Union directive NIS 2, which must be transposed into national law by October 2024. Above all, it represents the TISAX® system as a possible tool for information security, prototype protection and data protection, as well as a way of evaluating and obtaining the TISAX® label to demonstrate information security. The practical part of the thesis describes a selected organization that is a supplier of an OEM car manufacturer, whose requirement is to demonstrate the level of information security management system with the implemented system TISAX®. The result of the thesis is a proposal of the TISAX® implementation methodology based on a comparison of the standards dealing with information security management systems, their requirements and controls, and the ISA document, in which the requirements of the TISAX® system are defined based on control questions according to the established evaluation objectives, and the TISAX® Participant Handbook.

Keywords

cyber security, information security management system, TISAX®, information security, prototype protection, data security, automotive industry, supply chain, OEM, ISMS

Obsah

Úvod

V posledních letech se téma kybernetické bezpečnosti dostalo do popředí pozornosti zejména díky několika bezpečnostním incidentům, které přiměly veřejnost k zamyšlení o potřebě zabezpečení informací a dat. Každá organizace musí chránit svůj majetek, hmotný i nehmotný, a tudíž i zabezpečovat svoje citlivá data a informace. Jejich poškození, zneužití nebo ztráta můžou mít nedozírný vliv na organizaci i celou společnost a většinou jsou nenahraditelné.

Informace neexistují jen v podobě slov, čísel nebo obrázků, ale také v nehmotných formách, jako např. znalosti, nápady nebo know-how. Všechny informace mají svoji hodnotu, která je mnohdy nemalá. Nakládání s informacemi probíhá také v mnoha formách, nejen písemných, ale i ústních nebo elektronických. S tím souvisí nejen potřeba jejich shromažďování, ukládání, zpracování, ale také jejich likvidace nebo předávání či přeposílání, ať už fyzicky nebo prostřednictvím softwaru a hardwaru. Narušení kybernetické bezpečnosti může napáchat vysoké škody, ať už finanční, materiální, ale i duchovní. Nejde jen o náklady na obnovení poškozených či ztracených informací, ale také např. o vyzrazení obchodních záměrů nebo poškození dobrého jména organizace.

Automobilový průmysl je jedním z nejsilnějších průmyslových odvětví na světě. Od začátku výroby automobilů v roce 1913 a zavedení pásové linky Henrym Fordem došlo vlivem rozmachu automatizace, digitalizace a robotizace k jeho rapidnímu rozvoji. Významnou roli zde hrají inovace a vývoj nových informačních a komunikačních technologií. Jedním z nejdůležitějších kroků při výrobě automobilů je kooperace finálního výrobce s dodavateli. V případě narušení dodavatelského řetězce např. kvůli problémům s dodávkami, může být výrobní proces vážně ohrožen. Pro komunikaci mezi finálním výrobcem a jeho dodavateli je využívána převážně elektronická komunikace. Ta zahrnuje také přenos citlivých informací např. designových specifikací, plánů výroby, prototypových dat, což zvyšuje zranitelnost dodavatelského řetězce vůči různým hrozbám, jako jsou útoky na zabezpečení, falšování nebo vydírání. Všechny tyto činnosti čelí riziku narušení integrity, důvěrnosti a dostupnosti dat, informací, procesů, systémů a služeb.

Aby byla posílena kybernetická bezpečnost, měla by organizace na základě zohlednění svých specifických potřeb definovat svoje politiky informační bezpečnosti, identifikovat možná rizika, která představují hrozby a zranitelnosti jejích informačních systémů a infrastruktury, zabezpečovat školení svých zaměstnanců v oblasti informační bezpečnosti k zamezení nebo minimalizaci bezpečnostních incidentů způsobených lidskou chybou, zavádět systém správy a ochrany dat, včetně zálohování a plánů jejich obnovy v případě bezpečnostních incidentů, stanovovat opatření k minimalizaci rizik a zlepšování informační bezpečnosti, ať už organizačních (např. zavedení systému managementu

bezpečnosti informací) nebo technologických (např. firewallů, antivirových softwarů nebo šifrování dat).

Pro účely zajištění informační bezpečnosti v dodavatelském řetězci automobilového průmyslu byl vytvořen systém TISAX®. Ten je akceptován většinou výrobců automobilů a na základě požadavků některých z nich je implementace systému TISAX® a následně získání známky TISAX® na základě hodnocení nezávislým poskytovatelem auditu (např. certifikačním orgánem) povinným požadavkem pro všechny jejich dodavatele.

Cílem mojí diplomové práce je navrhnout metodiku implementace TISAX® pro dodavatele z oblasti automobilového průmyslu tak, aby tento systém a jeho udržování garantovaly maximální kybernetickou bezpečnost informací a dat.

Má práce je rozdělena do dvou částí. První teoretická část je věnována popisu struktury dodavatelského řetězce, způsobům výměny informací v dodavatelském řetězci a jeho bezpečnosti. Dále jsou popsány základní pojmy kybernetické bezpečnosti. Podrobněji je popsáno řízení bezpečnosti informací, které je založeno na definování firemní politiky a postupů, hodnocení a řízení rizik, relevantních systémů řízení bezpečnosti informací a kybernetické bezpečnosti, včetně legislativních požadavků v této oblasti nejen v rámci České republiky v podobě kybernetického zákona, ale i v rámci Evropské unie v podobě nové směrnice NIS 2. Další část teoretické části představuje systém TISAX®, který je určen dodavatelům v automobilovém průmyslu, kteří splněním jeho požadavků můžou prokázat zabezpečení informací a jeho hodnocení je uznáváno napříč společnostmi v automobilovém průmyslu. Poslední kapitola teoretické části popisuje metodologii této práce založené na hloubkovém porovnání norem z oblasti systémů managementu bezpečnosti informací a požadavků systému TISAX®.

Druhá praktická část práce zahrnuje implementaci systému TISAX®. Nejdříve charakterizuje vybranou organizaci, která je dodavatelem komponent, dílů a prototypů pro českého výrobce automobilů a která je vystavena jeho požadavku na prokázání zabezpečení důvěrných informací. Další podstatnou část práce tvoří návrh metodiky implementace TISAX® tak, aby organizace po její realizaci splňovala požadavky dané systémem TISAX® na zabezpečení důvěrných informací a maximálně posílila kybernetickou bezpečnost informací a dat.

Důvodem pro zpracování tohoto tématu je jeho aktuálnost v dnešní digitální době, závislost české ekonomiky na fungujícím automobilovém průmyslu bez narušení dodávek a subdodávek, rozmáhající se požadavky výrobců automobilů na prokázání zajištění bezpečnosti informací prostřednictvím systému TISAX® a neexistence závazné metodiky pro jeho implementaci.

TEORETICKÁ ČÁST

1 Informační a kybernetická bezpečnost

Zatímco informační bezpečnost a její zavedení se zaměřuje především na ochranu důvěrnosti, dostupnosti a integrity informací, kybernetická bezpečnost řeší spíše kybernetické incidenty. Průnikem obou jsou informace v digitální podobě, které mohou být zranitelné prostřednictvím informačních a komunikačních technologií (ICT – Information and Communication Technologies). Kybernetickou bezpečnost může podpořit zavedený systém řízení bezpečnosti informací v souladu s požadavky mezinárodní normy ISO/IEC 27001 a ještě více pak v kombinaci s dalšími normami pro různé typy dodavatelů.[1]

1.1 Dodavatelský řetězec a komunikace mezi dodavatelem a odběratelem

Dodavatelský řetězec je v souladu s celosvětovou odbornou terminologií označován anglickým pojmem supply chain. Představuje všechny struktury a procesy hodnototvorného procesu, tj. dodavatelů a subdodavatelů, zprostředkovatelů a poskytovatelů souvisejících služeb, vývojových a výrobních článků a zákazníků.[2]

Za klíč ke konkurenceschopnosti je považováno řízení dodavatelského řetězce neboli „Supply Chain Management“ (SCM). Vzájemná kooperace podnikatelských subjektů v rámci dodavatelského řetězce se dá dělit do tří etap: automatizace obchodních procesů (objednávky, zakázky) ve vztahu k ostatním subjektům podniku, optimalizace procesů v rámci subjektů a sdílení informací mezi subjekty (výrobní plány, plány odbytu) a celková optimalizace systému v rámci dodavatelského řetězce.[3] Z interního pohledu vytváří SCM prostor pro zvýšení produktivity práce, systematické plánování velikosti výrobních dávek nebo využívání průběžné doby výroby. Plánováním a řízením je možné např. zkrátit dodací lhůty o 10-60 %, zlepšit stupně plnění smluv o 50-90 %, zkrátit plánovací cykly až o 95 %, snížit stav zásob až o 75 % nebo zvýšit využití kapacit o 10-50 %.[4]

---

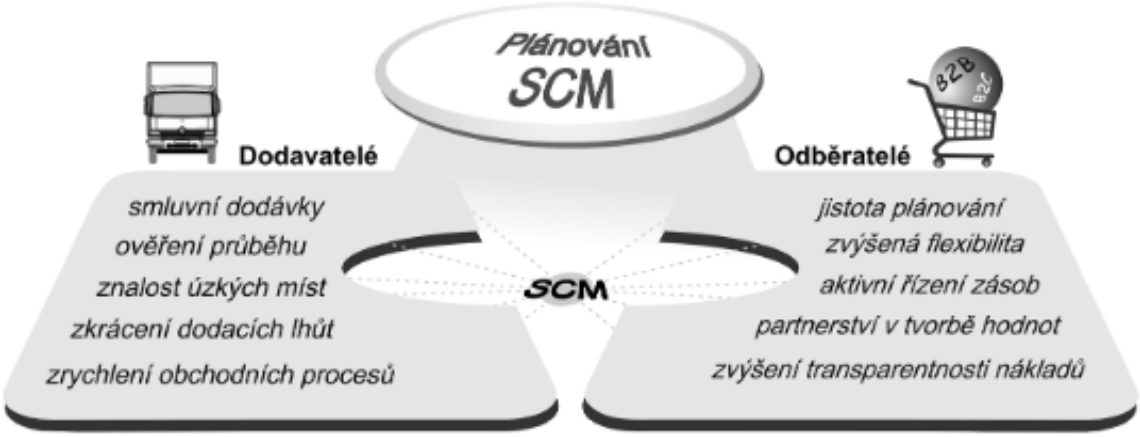
1 DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

2 TOMEK, Gustav a VÁVROVÁ, Věra. *Integrované řízení výroby: od operativního řízení výroby k dodavatelskému řetězci*. Expert (Grada). Praha: Grada, 2014. ISBN 978-80-247-4486-5.

3 FIALA, Petr. *Modelování a analýza produkčních systémů*. Praha: Professional Publishing, c2002. ISBN 80-86419-19-3.

4 TOMEK, Gustav a VÁVROVÁ, Věra. *Integrované řízení výroby: od operativního řízení výroby k dodavatelskému řetězci*. Expert (Grada). Praha: Grada, 2014. ISBN 978-80-247-4486-5.

OBRÁZEK 1: POTENCIÁL EFEKTIVNOSTI SCM



Zdroj: TOMEK, Gustav a VÁVROVÁ, Věra. Integrované řízení výroby: od operativního řízení výroby k dodavatelskému řetězci.[5]

1.1.1 Dodavatelský řetězec v automobilovém průmyslu

V automobilovém průmyslu jsou výrobci automobilů označování také jako výrobci originálního vybavení OEM (Original Equipment Manufacturer). Ti získávají různé komponenty a díly od různých dodavatelů a komponují je do svých výrobků. Výrobci OEM se soustředí především na svoje klíčové operace a ostatní, byť okrajové, ale důležité inženýrské činnosti outsourcuje. Jde především o návrh, výrobu a montáž. Z toho vyplývá, že OEM může využít externí technické znalosti bez investic do technologií, zapojit včas dodavatele do procesu vývoje produktu a prohlubovat vztahy s dodavateli, případně uzavírat partnerství. Prémiový výrobce OEM vyrábí většinou vozy vyšší střední třídy a vozy luxusní. Oproti svým konkurentům se odlišuje především kvalitnějšími technologiemi, kvalitou vozidel a také zákaznickým servisem. Objemový výrobce OEM se zaměřuje především na výrobu v nižším cenovém segmentu, vozy jsou vyráběny velkosériově a jsou malé nebo střední třídy. Návrhoví a výrobní dodavatelé (DMS – design and manufacturing suppliers) plní cíle výrobců OEM, které souvisí s náklady, kvalitou, časovým plánem a ekologickým designem.[6]

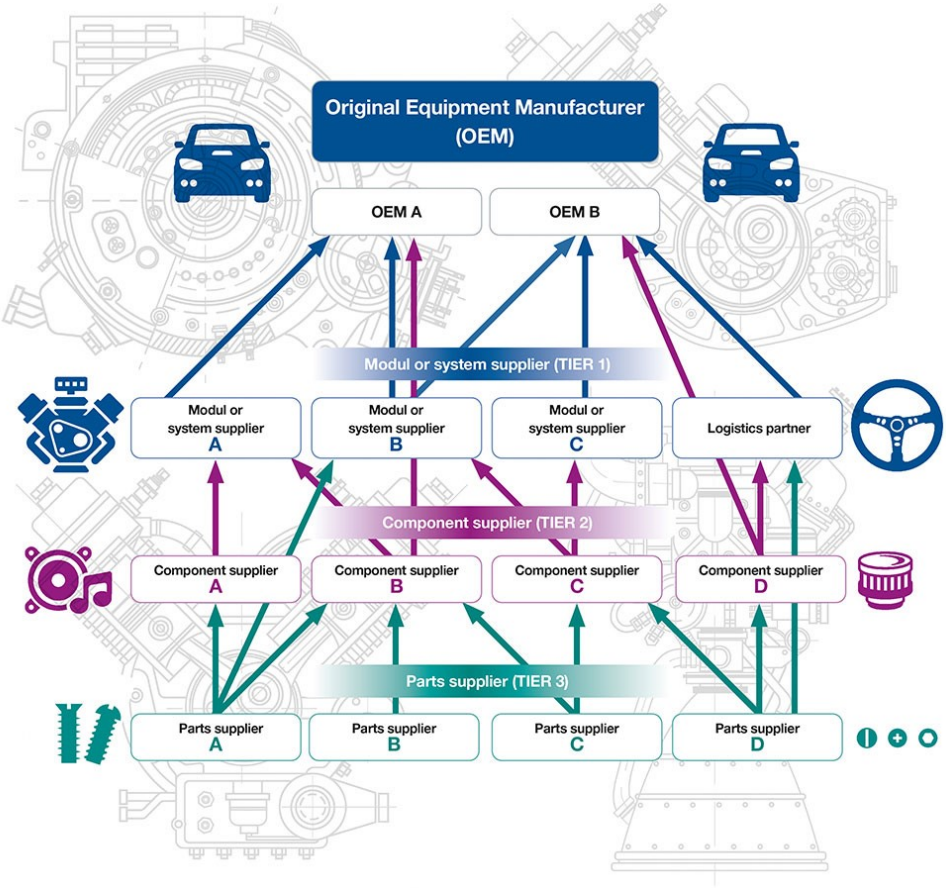
[5] TOMEK, Gustav a VÁVROVÁ, Věra. *Integrované řízení výroby: od operativního řízení výroby k dodavatelskému řetězci*. Expert (Grada). Praha: Grada, 2014. ISBN 978-80-247-4486-5.

[6] DIEHLMANN, Jens a HÄCKER, Joachim. *Die Automobilhersteller im Jahre 2020*. Online. Ed.: 2. Oldenbourg Verlag München, 2012. Dostupné z: https://search-ebscohost-com.ezproxy.techlib.cz/login.aspx?direct=true&db=e000xww&AN=758942&lang=cs&site=ehost-live&ebv=EB&ppid=pp_C1. [cit. 2024-02-27].

Hlavní hnací silou pro outsorcing jsou zákazníci, kteří tlačí výrobce OEM do snižování nákladů a vytváření inovací. Potřeba inovací pak vyplývá jednak ze specifických požadavků zákazníků, tak přísných směrnic na ochranu životního prostředí a bezpečnostní podmínky.[7]

Každé vozidlo obsahuje v průměru 30 000 dílů, přičemž každý díl se může skládat až ze 30 komponentů a může být vyroben v 15 různých zemích. Proto se dodavatelé první úrovně (Tier 1) geograficky soustředí co nejblíže výrobcům OEM kvůli snadnějšímu dodání. Např. dodavatelé první úrovně v USA mají v případě montáží metodami JIT (Just-in-Time) a JIS (Just-in-Sequence) zpravidla pouze 2 hodiny na výrobu a/nebo částečnou montáž dílů od objednávky výrobce OEM.[8]

OBRÁZEK 2: DODAVATELSKÝ ŘETĚZEC V AUTOMOBILOVÉM PRŮMYSLU



Zdroj: MOLNÁR, Jan. Dodavatelské řetězce v automobilovém průmyslu.[9]

[7] ILI, Serhan; ALBERS, Albert a MILLER, Sebastian. *Open innovation in the automotive industry*. Online. R&D Management, 2010, 40(3), 246-255. Wiley Online Library (distributor). Dostupné z: https://doi.org/10.1111/j.1467-9310.2010.00595.x. [cit. 2024-02-27].

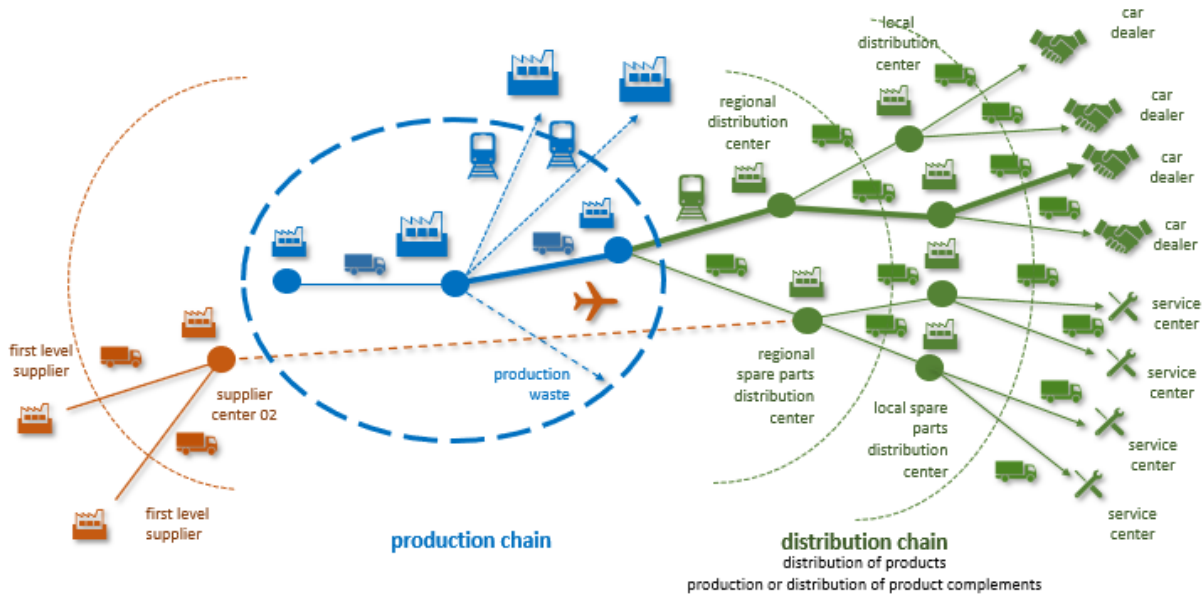
[8] YEUNG, Godfrey. *CODIFIABILITY AND GEOGRAPHICAL PROXIMITY OF SUPPLY NETWORKS IN AUTOMOTIVE INDUSTRY*. Online. Erdkunde. 2023, 77(2), 91-111. ISSN 00140015. Dostupné z: https://doi.org/10.3112/erdkunde.2023.02.01. [cit. 2024-02-28].

[9] MOLNÁR, Jan. *Dodavatelské řetězce v automobilovém průmyslu*. Online. 23.08.2023. Dostupné z: https://www.editel.cz/dodavatelske-retezce-v-automobilovem-prumyslu/. [cit. 2024-02-28].

Metoda JIT zohledňuje časové hledisko při dodávkách materiálů a polotovarů v požadovaném množství a čase. Byla vyvíjena v Japonsku, především firmou Toyota. Je vhodná zejména pro velké objemy produkce. Používá se ve spojení s metodou kanban (japonsky karta), která je používána pro řízení poptávky po materiálu od předcházející operace pro operaci následující, přičemž jsou zpracovávány pouze na kartě uvedené požadavky. Vytváří systém řízení poptávkou (tahem). Celkově jde o proces neustálého zlepšování systému, do kterého jsou zapojeni všichni zaměstnanci, a řízení kvality. Umožňuje udržování nízké hladiny zásob, což způsobuje úsporu místa a redukci situací, kdy jsou poruchy řešeny množstvím zásob, čímž minimalizuje plýtvání. Operace jsou koordinovány, vyrovnává se produkce vyrovnaným tokem materiálů a produktů systémem od dodavatelů až po konečný výstup. Pro metodu JIT je charakteristický malý počet dodavatelů, malé série, preventivní údržba a opravy zařízení. Ovlivňuje nejen vnitřní produkční systém firmy, ale také vztahy s dodavateli, od kterých jsou požadovány dodávky přesně v požadovaném čase a množství.[10]

Výrobce OEM stojí na konci hodnotového řetězce, který je v automobilovém průmyslu lineární a jednosměrný. Konečné výrobky pak distribuuje zákazníkům prostřednictvím distributorské sítě, která se skládá jak z vlastních prodejní sítě, tak franšízových prodejců.

OBRÁZEK 3: DISTRIBUČNÍ ŘETĚZEC V AUTOMOBILOVÉM PRŮMYSLU



Zdroj: BRONEC, Oldřich. Management in the engineering and automotive industry.[11]

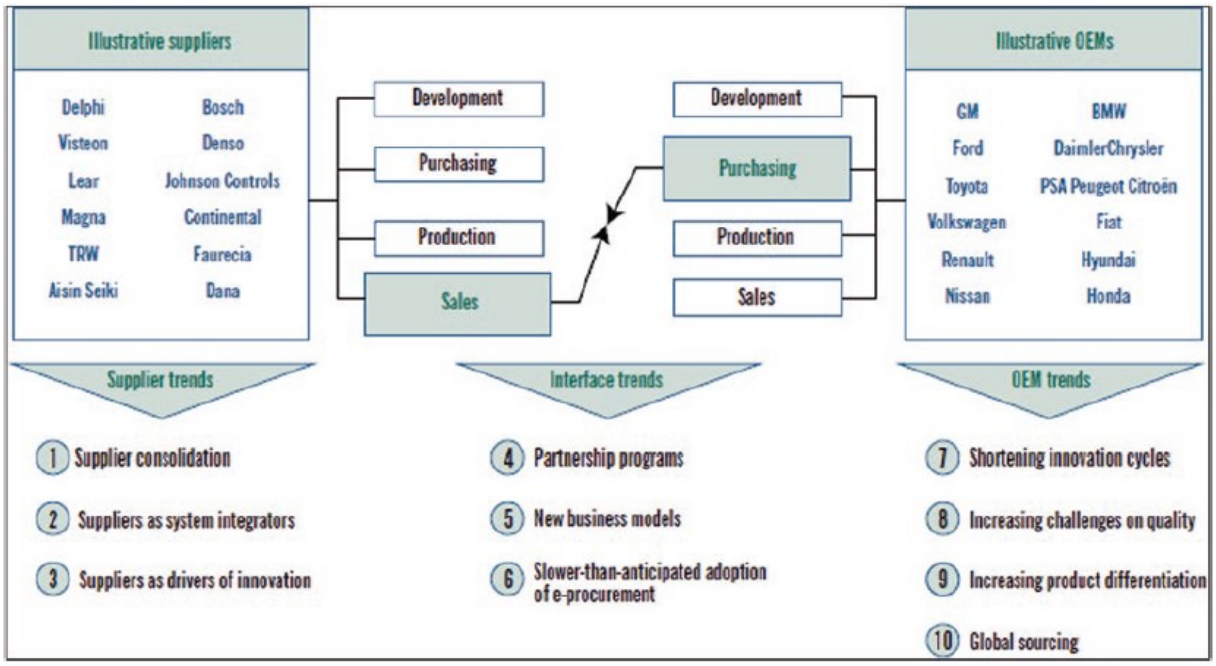
[10] FIALA, Petr. *Modelování a analýza produkčních systémů*. Praha: Professional Pub., 2002. ISBN 80-86419-19-3.

[11] BRONEC, Oldřich. *Management in the engineering and automotive industry*. PPTX. MÚVS, [March 19, 2024].

Vzhledem ke stále rostoucímu významu technologických a softwarových komponent se na hodnotovém řetězci podílí čím dál více IT společností. Zvyšuje se tím trend outsourcingu a off-shoringu.

V posledních desetiletích čelil automobilový průmysl vlně fúzí a akvizic, které vedly k postupné stabilizaci obchodních vztahů. Tím ovšem dochází ke snížení rozmanitosti dodavatelů a nutí výrobce OEM k udržování pevných vztahů s hlavními partnery, především v oblastech mechatroniky a elektrotechniky. Vzhledem k tomu, že dodavatelé hrají stále větší roli v oblasti inovací, vyhledávají výrobci OEM aktivně nové zdroje, aby zabránili přílišné závislosti a udrželi si konkurenceschopnost na trhu.[12]

OBRÁZEK 4: KLÍČOVÉ TRENDY MEZI DODAVATELI A VÝROBCI OEM



Zdroj: LEMPP, Martin a SIEGFRIED, Patrick. Automotive Disruption and the Urban Mobility Revolution: Rethinking the Business Model 2030.[13]

1.1.2 Způsoby výměny informací

Automatické zpracování objednávek a zakázek je možné pomocí techniky elektronické výměny dat **EDI** (Electronic Data Interchange). Tím se sníží transakční náklady a odstraní možnosti vzniku chyb. Automatizovaný přenos dat vede ke zvyšování efektivnosti jednotlivých členů řetězce. Dochází k efektu biče (bullwhip-effect), *„kdy při lokální informaci a lokálně omezeném rozhodování malé výkyvy*

[12] LEMPP, Martin a SIEGFRIED, Patrick. *Automotive Disruption and the Urban Mobility Revolution: Rethinking the Business Model 2030*. Online. c2022. ISBN 978-3-030-90035-9. Dostupné z: https://doi.org/10.1007/978-3-030-90036-6. [cit. 2024-02-28].

[13] Tamtéž.

v poptávce koncového zákazníka vedou ke stále větším výkyvům v objemech objednávek ve vyšších vrstvách řetězce"[14]. Způsobují ho zbytečné bezpečnostní zásoby napříč celým řetězcem, čímž dochází ke vzniku zbytečných nákladů. To je možné minimalizovat nebo úplně eliminovat pomocí řízení dodavatelských řetězců.[15]

Od roku 2000 funguje mezipodniková dodavatelská burza **Covisint**, kterou společně vytvořily automobilky DaimlerChrysler, Ford Motor Company a General Motors ke zlepšení spolupráce, viditelnosti a integrace automobilového průmyslu. Covisint slouží k bezpečné výměně informací na B2B trhu. V současné době je k dispozici pro více než 85 000 organizací a 500 000 uživatelů na celém světě. Na portálu Covisint je možné spravovat zabezpečení organizací a jejich uživatelů, přistupovat na portály výrobců OEM a dodavatelů Tier 1 a získávat zabezpečené informace z těchto portálů.[16]

Pro spojení s obchodními partnery po celém světě a propojení celého dodavatelského řetězce, nejen pro automobilový průmysl, slouží dynamická firemní síť **SupplyOn**, do které je zapojeno více než 140 000 organizací po celém světě. Mezi vlastníky patří Bosch, Continental, Schaeffler a ZF.[17] SupplyOn nabízí transparentní mapování procesů, jako je plánování kapacit, interaktivní upřesňování množství a termínu dodávek, objednávky a jejich potvrzování, doprava a příjem zboží a sledování stavu objednávky a doručení pro všechny zainteresované strany. Mezi benefity patří až 40% úspora času díky automatizovanému nákupu materiálu nebo využití umělé inteligence pro včasné odhalení zmírnění překážek dodávek.[18]

Pro zvýšení konkurenceschopnosti vytvořila v roce 2023 skupina Volkswagen Group platformu **ONE.KBP** (Konzern Business Plattform). Tato dynamická platforma zajišťuje optimální spolupráci mezi skupinou Volkswagen Group a jejími dodavateli.[19]

SKODETTE je portál pro komunikaci pro ŠKODA AUTO a její obchodní partnery. Elektronický přenos dat může probíhat prostřednictvím klasického EDI nebo webové aplikace pro dodavatele, kteří nemají vlastní EDI systém. Je využíván např. pro elektronické odvolávky, faktury dodací listy, štítky a další.

---

[14] FIALA, Petr. *Modelování a analýza produkčních systémů*. Praha: Professional Pub., 2002. ISBN 80-86419-19-3.

[15] Tamtéž.

[16] COVISINT. *About Automotive Exchange*. Online. ©2023. Dostupné z: https://portal.covisint.com/web/103853/2. [cit. 2024-02-28].

[17] SUPPLYON. *About Us*. Online. [b.d.]. Dostupné z: https://www.supplyon.com/en/about_us/. [cit. 2024-02-28].

[18] SUPPLYON. *Supply Chain Collaboration*. Online. [b.d.]. Dostupné z: https://www.supplyon.com/en/solutions/supply-chain-collaboration/. [cit. 2024-02-28].

[19] WOLKSWAGEN GROUP. *Welcome to the ONE.Group Business Platform*. Online. [b.d.]. Dostupné z: https://www.vwgroupsupply.com/one-kbp-pub/en/kbp_public/homepage/homepage.html. [cit. 2024-02-28].

K šifrování využívá ŠKODA AUTO kryptografické protokoly TLS (Transport Layer Security), které zajišťují bezpečnost a ochranu před zneužitím dat třetí stranou. Na základě legislativních požadavků nebo vzájemné domluvy z obchodními partnery používá funkcionalitu pro šifrování dat OFTP.[20] OFTP2 je nejvíce rozšířený protokol používaný při výměně kritických automobilových dat přes veřejný internet, který zajišťuje rychlý a bezpečný přenos důvěrných a citlivých informací a je implementován ve většině výrobců OEM a většině velký dodavatelů stupně Tier 1.[21]

1.1.3 Bezpečnost dodavatelského řetězce

Z pohledu kybernetického zákona jsou pro oblast dodavatelského řetězce definovány pojmy správce, provozovatel a významný dodavatel. Správce informačního nebo komunikačního systému stanovuje účel zpracování informací a podmínky provozování informačního a komunikačního systému, případně jeho účel. Funkčnost informačního systému nebo komunikačního systému kritické informační infrastruktury zajišťuje provozovatel, který je zároveň dodavatelem pro správce. Dodavatelem pro správce a provozovatele s plněním předmětu smlouvy s významným dopadem na bezpečnost je významný dodavatel. Správci a provozovatelé mají povinnost např. stanovit bezpečnostní požadavky pro své dodavatele a hodnotit je z hlediska bezpečnosti. Smlouvy s významnými dodavateli musí obsahovat např. ustanovení o bezpečnosti informací z hlediska důvěrnosti, dostupnosti a integrity, ustanovení o kontrole a auditu dodavatele (zákaznických auditech), podmínky pro formát předávání dat a informací na základě vyžádání správce nebo pravidla pro likvidaci dat.[22]

K ochraně dodavatelského řetězce a zabránění kybernetických hrozeb je možné přispět stanovením řízením rizik třetích stran, identifikací a stanovením priorit zranitelnosti dodavatelského řetězce, zapojením dodavatelů do klíčových bezpečnostních kroků řetězce (tj. všech subjektů, kteří vyrábí, upravují nebo distribuují komponenty v dodavatelském řetězci), v případě možnosti také využití testovací laboratoře pro odhalování skrytých chyb hardwaru a softwaru a posouzení blockchainu dalších technologií pro ověření dodavatelského řetězce, protože pro ochranu dodavatelského řetězce je zásadní mechanismus ověření každé změny v dodavatelském řetězci s nezpochybnitelným zdrojem a časovým razítkem.[23]

---

[20] ODETTE. *OFTP2*. Odette File Transfer Protocol v2. Online. ©2024. Dostupné z: https://www.odette.org/oftp2. [cit. 2024-02-28].

[21] ŠKODA AUTO. *SKODETTE – EDI*. Online. ©2019. Dostupné z: https://edi.skoda-auto.cz/index-2.html. [cit. 2024-02-28].

[22] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[23] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Bezpečnost dodavatelského řetězce řeší také normy řady 27k. Přímo bezpečností dodavatelského řetězce se zabývá mezinárodní norma ISO/IEC 27036 Informační technologie – Bezpečnostní techniky – Informační bezpečnost pro dodavatelské vztahy. Norma popisuje základní pojmy informační bezpečnosti v souvislosti s dodavatelskými vztahy, tj. vztahy, na které může mít vliv bezpečnost informací, např. informační technologie, poradenské služby, zdravotnické služby, outsourcing aplikací nebo cloud computtingové služby. Dále specifikuje základní bezpečnostní požadavky jako vodítko k pochopení rizik bezpečnosti informací a nakládání s informacemi k vzájemné spokojenosti. V další části navádí k řízení rizik bezpečnosti informací, které se týkají dodavatelského řetězce. Na závěr uvádí doporučení ohledně bezpečnosti informací pro dodavatele a zákazníky cloudových služeb, tzn. zabývá se riziky typickými pro používání cloudových služeb majících negativní dopad na bezpečnost informací organizace, které cloudové služby využívají.[24]

1.2 Kybernetická bezpečnost

Pro pojem kybernetická bezpečnost není jednotná obecně uznávaná definice. Z různých pohledů je možné uvést několik ustálených definic:

- Kybernetickou bezpečnost je možné definovat jako „soubor opatření přijatých k ochraně počítače nebo počítačového systému (jako na internetu) před neoprávněným přístupem nebo útokem“. [25]
- Kybernetickou bezpečnost je možno také definovat jako „souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“.[26]
- Podle Oxford Dictionary je možné kybernetickou bezpečnost definovat jako *„zabezpečení týkající se počítačových systémů nebo internetu, zejména která jsou určena k ochraně proti virům nebo podvodům“*.[27]
- Ve Výkladovém slovníku kybernetické bezpečnosti je kybernetická bezpečnost definována jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“*.[28]

---

[24] Tamtéž.

[25] MERRIAM-WEBSTER. *Dictionary*. Online. In: Merriam-Webster, Encyclopaedia Britannica. 05.04.2024. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity. [cit. 2024-04-16].

[26] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[27] OXFORD UNIVERSITY PRESS. *Oxford English Dictionary*. Online. ©2023. Dostupné z: https://www.oed.com/search/dictionary/?scope=Entries&q=cybersecurity&tl=true. [cit. 2024-04-16].

[28] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Online. Národní centrum kybernetické bezpečnosti (distributor). 2015. Dostupné z: https://www.govcert.cz/cs/informacni-servis/slovnik/. [cit. 2024-02-28].

- Dle normy ISO/IEC 27000:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník se kybernetická bezpečnost týká řízení rizik bezpečnosti informací vyskytujících se v digitální podobě v počítačích, úložištích a sítích.[29]
- Podle normy ISO/IEC 27032:2023 Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost je kybernetická bezpečnost součástí informační bezpečnosti. V této mezinárodní normě jsou definovány základní bezpečnostní postupy pro bezpečnost informací, sítí, internetu a ochrany kritické informační infrastruktury.[30]

Kybernetickou bezpečnost je třeba regulovat, protože používání informačních a komunikačních technologií v každodenním životě způsobuje závislost lidí na těchto technologiích, rostou rizika a možné dopady v souvislosti s jejich využíváním a postupuje rychlý technologický vývoj. Narůstá počet kybernetických útoků, přičemž kybernetický prostor přesahuje hranice států, a je proto nutné nastavit globální pravidla. Kybernetická bezpečnost zemí je důležitým kritériem konkurenceschopnosti pro investory. Požadavky na regulaci a koordinaci kybernetické bezpečnosti a předcházení kybernetickým bezpečnostním incidentům tak přichází jak ze strany jednotlivých států, tak ze strany OSN, NATO a Evropské unie.[31]

1.2.1 Základní pojmy kybernetické bezpečnosti

Informace je určitá veličina, která snižuje nebo částečně odstraňuje dosavadní neurčitost, neznalost o jevu nebo události. Zároveň je zbožím, které má svoji hodnotu, a tedy i cenu, které jsou dány její důležitostí pro příjemce.[32]

Data jsou zaznamenaná fakta, čísla, události, grafy, mapy, transakce atd. získaná čtením, pozorováním, výpočtem, měřením, vážením kreslením atd., vyjádřená pomocí čísel, textu, zvuku, obrazu apod. Data jsou tedy produktem lidské činnosti, která mají svou hodnotu na základě vynaložených nákladů na jejich pořízení, následné uchovávání a udržování a také ceny jejich informačního obsahu.[33]

---

[29] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[30] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[31] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[32] POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[33] POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Aktivum (Asset) představuje hmotný i nehmotný majetek, který má určitou hodnotu, v oblasti informační bezpečnosti pak především data a informace, jejichž zneužití nebo ztráta by způsobily nějakou škodu osobě nebo organizaci.[34] Základními aktivy, která jsou označována takové jako informační aktiva, jsou např. obchodní tajemství, kritické obchodní procesy, know-how nebo patenty. Podpůrnými aktivy, která zpracovávají informační aktiva, jsou např. IT systémy, IT služby, služby nebo zaměstnanci.[35] V praxi jsou aktiva rozdělována na primární a podpůrná. Primární aktiva jsou především informační aktiva (klíčový nástroj pro rozhodování), služby IT (informační a komunikační služby) a znalosti (know-how). Je možné stanovit jejich hodnotu z hlediska důvěrnosti, integrity a dostupnosti a určují výši škod v případě bezpečnostního incidentu. Mezi podpůrná aktiva patří objekty (např. budovy, trezory, ale i klimatizace nebo UPS), technologie (výpočetní a komunikační prostředky, programy), IT procesy (postupy a předpisy), data (např. paměťové nosiče a záložní média), osoby (např. administrátoři IT, manažeři ISMS) a dodavatelé (v souvislosti s ISMS organizace).[36]

Bezpečnost (Security) je možno chápat jako vlastnost (např. informačního systému nebo technologie), která má určitý stupeň ochrany proti škodám a hrozbám.[37]

Hrozba (Threat) je skutečnost, událost, síla nebo osoby, které můžou svým působením ohrozit bezpečnost poškozením, zničením, ztrátou důvěry nebo hodnoty aktiv (např. přírodní katastrofa, hacker, zaměstnanec apod.) a narušit tak jejich důvěrnost, integritu a dostupnost.

Riziko (Risk) vyjadřuje pravděpodobnost zničení nebo poškození konkrétního aktiva působením konkrétní hrozby a tím narušení důvěrnosti, integrity nebo dostupnosti.[38]

Útok nebo také **bezpečnostní incident** je úmyslné využití zranitelného místa ke způsobení škody na aktivech nebo neúmyslná akce, která vede ke škodě na aktivech.[39]

Zranitelnost (Vulnerability) představuje slabinu bezpečnostního systému vystavené hrozbě zneužití za účelem poškození nebo zničení hodnoty aktiv (např. datacentrum v záplavové oblasti).[40]

---

[34] POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[35] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[36] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[37] POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[38] Tamtéž.

[39] Tamtéž.

[40] Tamtéž.

1.2.2 Organizační bezpečnostní opatření

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen Vyhláška č. 82/2018) definuje požadavky na organizační opatření. Mezi ně patří mimo jiné ty následující:[41]

Systém řízení bezpečnosti informací (ISMS) jako jeden ze základních požadavků vyhlášky o kybernetické bezpečnosti slouží k řízení informační bezpečnosti a vychází z normy ISO/IEC 27001.[42] Právní základ pro bezpečnost informací poskytují dohody o mlčenlivosti, přičemž každá země musí dodržovat zákonná ustanovení týkající se ochrany údajů.[43]

Řízení aktiv znamená identifikaci, evidenci a hodnocení aktiv. Na základě klasifikace aktiv je určena nezbytná míra potřebných bezpečnostních opatření a možné způsoby zacházení s aktivy, je stanoven způsob jejich likvidace. V praxi to znamená např. základní formy ochrany, sdílení s třetími stranami a způsob likvidace aktiv nebo možnosti mazání a likvidace technických nosičů informací, provozních údajů, informací a jejich kopií.[44]

Řízení rizik znamená stanovení metodiky pro hodnocení rizik a stanovení kritérií pro jejich přijatelnost. Na základě provedených analýz rizik jsou zpracovávány zprávy o hodnocení rizik, na jejichž podkladě je sestaveno prohlášení o aplikovatelnosti, které obsahuje seznam zavedených a nezavedených opatření podle Vyhlášky č. 82/2018, způsob jejich zavedení, případně důvod, proč některá opatření nebyla zavedena.[45]

Řízení dodavatelů představuje pravidla pro řízení dodavatelů a uzavírání dodavatelských smluv. Týká se tzv. významných dodavatelů, tj. provozovatelů informačního nebo komunikačního systému, příp. jiných subjektů, kteří s nimi vstupují do právního vztahu, který je významný z hlediska bezpečnosti regulovaného systému.[46]

---

41 DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

42 Tamtéž.

43 ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

44 DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

45 Tamtéž.

46 Tamtéž.

Bezpečnost lidských zdrojů zahrnuje především průběžné vzdělávání a udržování bezpečnostního povědomí na potřebné úrovni, neboť velkou část kybernetických bezpečnostních incidentů zapříčiňuje nedostatečné bezpečnostní povědomí uživatelů. Týká se nejen interních uživatelů, ale i jiných zainteresovaných stran, např. významných dodavatelů.[47]

Řízení změn je jedním z klíčových procesů z hlediska provozu a bezpečnosti. Souvisí s ním také přezkoumání možných dopadů na všechny změny. Dle tohoto přezkoumání musí být identifikovány tzv. významné změny s vlivem na kybernetickou bezpečnost a vysokým rizikem.[48]

Řízení přístupu představuje oblast správy identit a přístupových oprávnění uživatelů, administrátorů, aplikací a dalších zařízení.[49]

Kontrola a audit kybernetické bezpečnosti zahrnují mimo jiné dodržování bezpečnostních politik, bezpečnostních opatření a smluvních závazků. V případě identifikace neshod musí být stanovena nápravná opatření, aby byla zajištěna shoda.[50]

1.2.3 Technická bezpečnostní opatření, resp. technologická opatření

Dalším požadavkem Vyhlášky č. 82/208 je stanovení technických bezpečnostních opatření. Mezi ně patří mimo jiné ty následující:[51]

Fyzická bezpečnost znamená stanovení bezpečnostních zón, kde musí být použity zejména mechanické prostředky pro zábranu, elektrické zabezpečovací signalizace, zabezpečovací prostředky proti vzniku a šíření požárů nebo prostředky kontrolující vstup.[52]

Bezpečnost komunikačních sítí se zaměřuje na řízení komunikace v rámci komunikační sítě a dále také na použití kryptografie, aby byla zajištěna důvěrnost a integrita pro vzdálený přístup a správu nebo bezdrátový přístup do komunikační sítě.[53]

Správa a ověřování identit klade důraz na využívání vícefaktorové autentizace, případně požadavky na skladbu hesel.[54]

---

47 DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
48 Tamtéž.
49 Tamtéž.
50 Tamtéž.
51 Tamtéž.
52 Tamtéž.
53 Tamtéž.
54 Tamtéž.

Řízení přístupových oprávnění vymezuje požadavky pro přístup k jednotlivým aktivům, pro čtení a zápis dat a změnu oprávnění. K tomu je využíváno stanovení rolí a uživatelských skupin.[55]

Detekce kybernetických bezpečnostních událostí požaduje implementaci nástrojů pro detekování bezpečnostních událostí (kybernetických bezpečnostních incidentů nebo kybernetických útoků) nebo jejich vzdorování.[56]

Aplikační bezpečnost požaduje provádění penetračních testů, jejichž účelem je nalezení zranitelných míst z pohledu bezpečnosti, které je nutno odstranit. Zároveň Vyhláška č. 82/2018 požaduje trvale ochránit aplikace, informace a transakce před neoprávněnými činnostmi.[57]

Kryptografické prostředky musí být odolné kryptografické algoritmy a šifrovací klíče a certifikáty v potřebné kvalitě s nezbytnou ochranou a správou.[58]

1.3 Principy kybernetické bezpečnosti

Základními principy pro uplatňování kybernetické bezpečnosti jsou triáda CIA, prvky kybernetické bezpečnosti a životní cyklus kybernetické bezpečnosti.[59]

1.3.1 Triáda CIA

Kybernetická bezpečnost zajišťuje bezpečnost jak prvků ICT, tak i těmito prvky přenášených, zpracovávaných a uchovávaných dat a informací. Přitom je kladen největší důraz na důvěrnost, integritu a dostupnost:

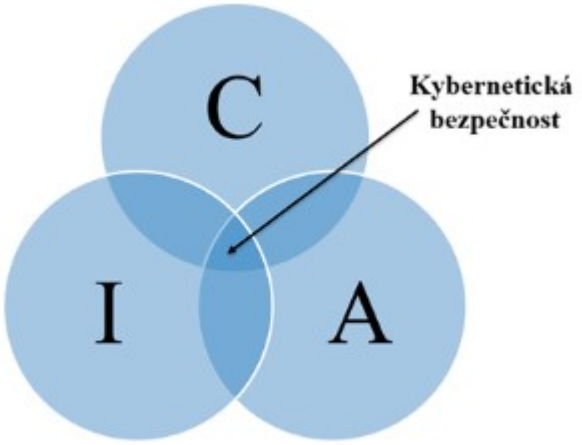
- **Důvěrnost** (Confidentiality) znamená, že k ICT, datům a informacím mají přístup pouze k tomu oprávněné osoby. V případě kybernetického útoku jde např. o krádež dat, přístupových údajů a klíčů nebo hardware.
- **Integrita** (Integrity) znamená, že zásah do informací, dat, počítačových systémů, jejich nastavení je možný pouze k tomu oprávněnou osobou. V případě kybernetického útoku jde např. o chyby v databázích nebo nastavení oprávnění.

[55] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
[56] Tamtéž.
[57] Tamtéž.
[58] Tamtéž.
[59] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

- **Dostupnost** (Availability) znamená přístup k informaci, datům, nebo počítačovému systému v okamžiku potřeby. V případě kybernetického útoku jde např. o DoS a DDoS útoky, fyzické útoky na servery nebo výpadky proudu.

Triádu CIA je možné znázornit i graficky.[60]

OBRÁZEK 5: TRIÁDA CIA A KYBERNETICKÁ BEZPEČNOST



Zdroj: KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity.[61]

1.3.2 Prvky kybernetické bezpečnosti

Mezi prvky vytvářející nebo vedoucí ke kybernetické bezpečnosti patří lidé, technologie a procesy.

Lidé (people) jsou klíčovými prvky kybernetické bezpečnosti, jsou nejslabším článkem a také nejčastějším cílem útočníků. Z tohoto důvodu je možné na ně nahlížet jako na:

- tvůrce kybernetické bezpečnosti, kteří prosazují a implementují její jednotlivé prvky,
- příjemce pravidel, kteří implementují již existující pravidla kybernetické bezpečnosti,
- subjekty s nutnou potřebou ochrany před kybernetickými útoky,
- subjekty s nutnou potřebou informovanosti a proškolením o pravidlech a principech,
- riziko nebo hrozbu, které mohou vzniknout v rámci vytváření a udržovaní kybernetické bezpečnosti.

Proto je pro ně nezbytné pochopení alespoň základních principů a pravidel kybernetické bezpečnosti, porozumění alespoň základních funkcí počítačových systémů (stolních počítačů, notebooků, chytrých telefonů, chytrých televizí apod.), analyzování používaných aplikací a používání pouze těch jim vyhovujících a v neposlední řadě vzdělávání v oblasti kybernetické bezpečnosti.[62]

---

[60] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
[61] Tamtéž.
[62] Tamtéž.

V případě kybernetického útoku jde např. o útok sociálním inženýrstvím, phishing, malware nebo krádeže.[63]

Technologie (technologies) představují prostředek, prostřednictvím něhož se uživatel připojí k internetu, sociálním sítím a dalším aplikacím. Pro běžného uživatele jsou to především koncové technologie jako počítač, tablet, mobilní telefon apod. Z hlediska organizace jde také o kompletní infrastrukturu sítě (např. LAN, Wi-Fi), služby (např. servery, aplikace) a další prvky sloužící k zajištění zabezpečení (firewall, IDS/IPS, prvky pro autentizaci, autorizaci, monitoring, analýzy).

Při implementaci kybernetické bezpečnosti je proto třeba všechna stávající aktiva analyzovat a jejich seznam doplňovat a modifikovat. Zároveň je třeba všechny technologie udržovat aktualizované a zabezpečené a v takovém stavu, aby byly schopny reagovat na změny v oblasti vývoje ICT.

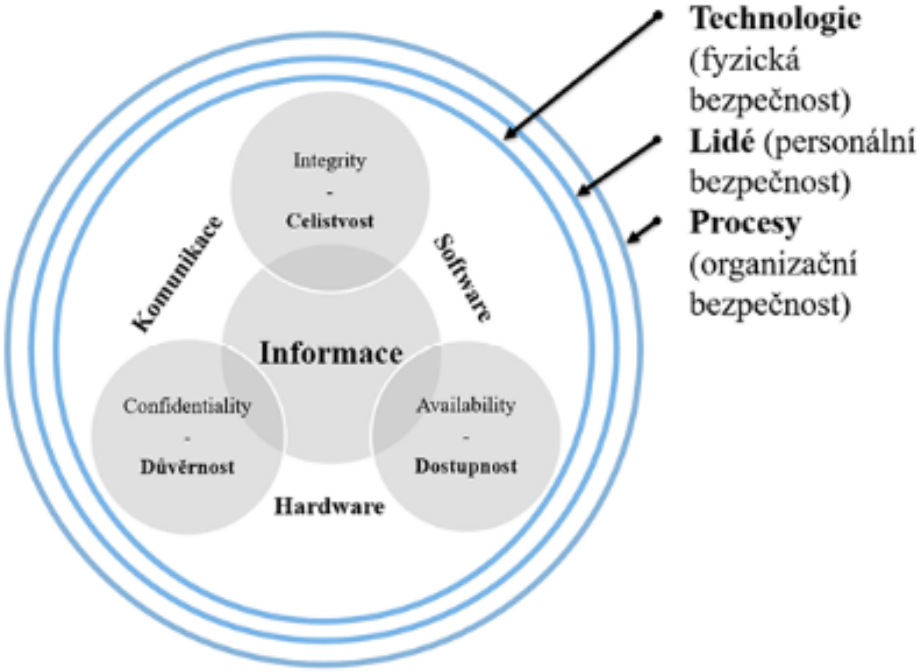
V případě kybernetického útoku jde o útok na hardware, databáze, síť a síťovou infrastrukturu, software (operační systém nebo jiné aplikace), informace a data uložená v počítačových systémech.[64]

Procesy (processes) jsou činnosti potřebné k používání technologií a s nimi spojených služeb lidmi. Mezi ně se řadí např. řízení rizik (jejich analýza a kategorizace), implementace ICT a aplikací, údržba systémů, testování zabezpečení, identifikace a zavedení nápravných opatření, audity kybernetické bezpečnosti, školení atd. Vhodná je simulace typických kybernetických útoků (např. phishing) a penetrační testování, které odhalí chyby v již nastavených procesech.

V případě kybernetického útoku jde např. o neoprávněné testování zabezpečení v organizaci[65]

[63] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
[64] Tamtéž.
[65] Tamtéž.

OBRÁZEK 6: TRIÁDA CIA DOPLNĚNÁ O TECHNOLOGIE, LIDI A PROCESY



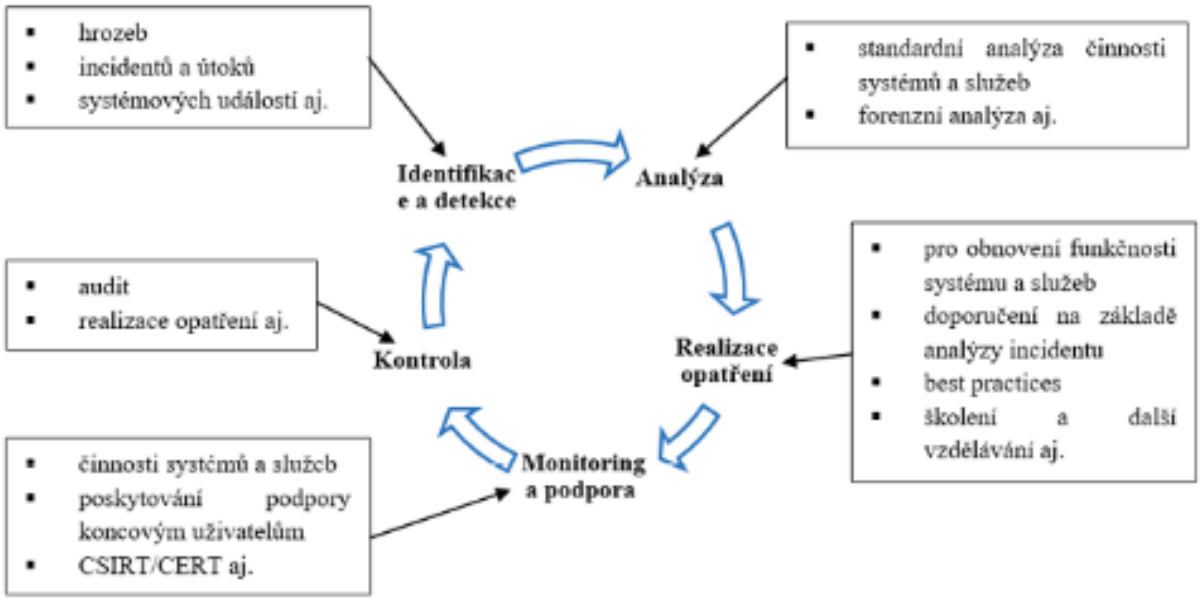
Zdroj: KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity.[66]

1.3.3 Životní cyklus kybernetické bezpečnosti

Již zmíněnou triádu CIA i dílčí prvky kybernetické bezpečnosti je třeba uplatňovat při realizaci kybernetické bezpečnosti po dobu celého jejího životního cyklu. Obecně by bylo možné životní cyklus kybernetické bezpečnosti popsat jako stále se opakující cyklus Prevence → Detekce → Reakce. Jde o nikdy nekončící analýzu rizik, která je doplněna o další podpůrné procesy.[67]

[66] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
[67] Tamtéž.

OBRÁZEK 7: ŽIVOTNÍ CYKLUS KYBERNETICKÉ BEZPEČNOSTI



Zdroj: KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity.[68]

1.4 Řízení bezpečnosti informací

Systém řízení bezpečnosti informací je součástí organizačních bezpečnostních opatření, která spolu s technickými bezpečnostními opatřeními zajišťují bezpečnost informací v informačních systémech a zároveň dostupnost a spolehlivost služeb a sítí elektronických komunikací v kybernetickém prostoru.[69]

1.4.1 Politiky a postupy

Prvním krokem při vytváření systému řízení bezpečnosti je stanovení bezpečnostních cílů vycházejících z celkových cílů organizace, legislativních, smluvních a interních požadavků. K nim je třeba určit bezpečnostní rizika a pro jejich eliminaci vhodná bezpečnostní opatření. Tato opatření pak tvoří základ bezpečnostní politiky organizace.[70]

[68] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

[69] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. In: Sbírka zákonů. 2014, částka 75. Dostupné z: https://www.e-sbirka.cz/sb/2014/181/2022-08-06?f=181&zalozka=text. [cit. 2024-04-16].

[70] POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

1.4.2 Hodnocení a řízení rizik

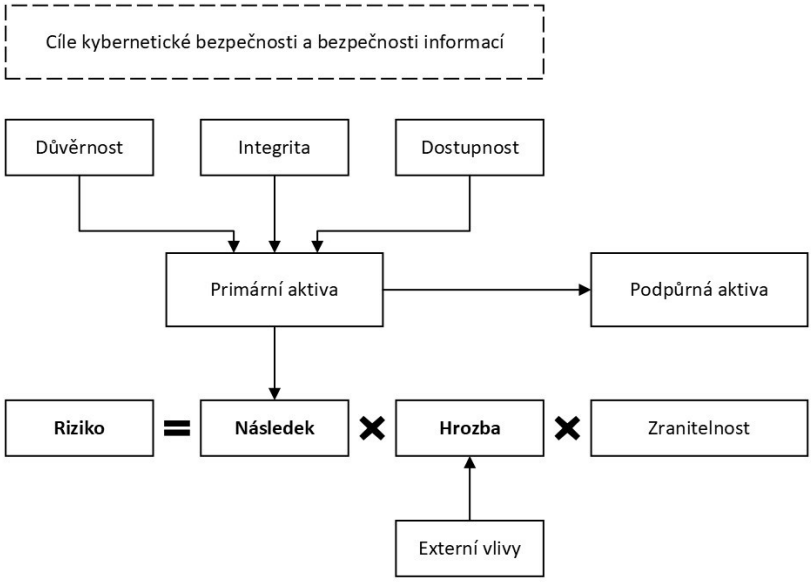
Vzhledem k závislosti organizací na informačních a komunikačních technologiích (ICT) je řízení rizik, a to zejména těch kybernetických a informačních, jedním z klíčových faktorů úspěchu organizace. V praxi se vyskytují dva rozdílné přístupy k řízení rizik – empirické a analytické. Analytický přístup, který je zatím významně preferován, je založený na „dobré praxi" (good practice), např. dle ISO/IEC 27005, NIST 800-30 rev 1, NIST 800-37, ISO/IEC 27015. Bezpečnostní opatření jsou implementována s cílem snížit rizika na úroveň, která je akceptovatelná. Empirický přístup se zakládá na potřebě zvládání kybernetických bezpečnostních incidentů, sdílení zkušeností s jejich řešením a následné optimalizaci již stanovených bezpečnostních opatření. Podstatné zdroje tvoří např. normy ISO/IEC 27035, ISO/IEC 27032 nebo doporučení pro organizaci SCIRT/CERT. Volba jedno z těchto přístupů je založena na zhodnocení jejich silných a slabých stránek a tvoří základ pro sestavení systému řízení bezpečnosti informací a následně pak systém řízení rizik. V běžné praxi se vyskytuje i kombinace obou přístupů pro různé oblasti.[71]

Analytický model představuje způsob hodnocení rizik opírající se o následek neboli dopad (I), hrozbu (T) a zranitelnost (V). Vlastní riziko je pak možno vyjádřit funkcí R = f(I,T,V), kde následek reflektuje míru škody, kterou dané riziko může přinést, hrozba reflektuje míru pravděpodobnosti, s jakou se dané riziko může projevit, nebo jak často k němu dochází a zranitelnost indikuje míru efektivity stávajících bezpečnostních opatření v tom, jak rychle a účinně dokáží detekovat projevy daného rizika.[72]

[71] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[72] Tamtéž.

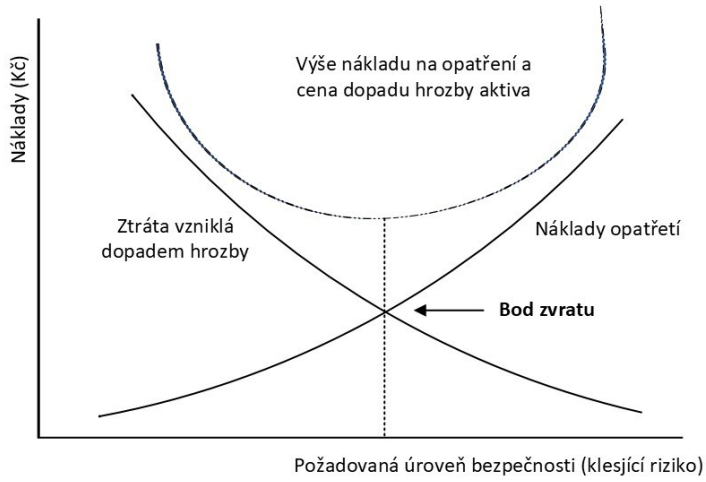
OBRÁZEK 8: PRINCIPY ANALYTICKÝCH MODELŮ ŘÍZENÍ RIZIK



Zdroj: Vlastní zpracování dle DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací.[73]

Pro vyčíslení ekonomického aspektu se využívá oceňování aktiv, které vyčíslí ztrátu v případě zničení nebo narušení užitné hodnoty aktiv. Následně můžou být stanoveny maximální náklady na opatření jich ochrany.[74]

OBRÁZEK 9: NÁKLADOVÝ MODEL PRO REALIZACI BEZPEČNOSTNÍCH OPATŘENÍ



Zdroj: Vlastní zpracování dle DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací.[75]

[73] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
[74] Tamtéž.
[75] Tamtéž.

V moderních metodách řízení rizik patří mezi základní prvek vytvoření tzv. registru rizik. Ten obsahuje informace o všech bezpečnostních rizicích, která je možné dále specifikovat, tj. určit např. jejich významnost, osobu odpovědnou za jejich zvládání a postup zvládání rizika sledovat v čase.[76]

Empirické modely řízení zahrnují také realizaci základních preventivních opatření bezpečnosti informací, ale zároveň využívají již existující zkušenosti v souvislosti s efektivní ochranou kybernetického prostoru, který je znám pod názvem „baseline security". Sem patří opatření např. identifikace a autentizace uživatelů, management přístupových oprávnění nebo dohled na činnostmi uživatelů v rámci informačního systému. V poslední době jsou tyto modely stále častěji požadovány regulačními orgány, neboť státy nebo jiné dozorové orgány potřebují mít informace o významných bezpečnostních incidentech, ke kterým speciálně zřízená centra formulují konkrétní technická doporučení.[77]

1.4.3 Systémy řízení bezpečnosti informací a kybernetické bezpečnosti

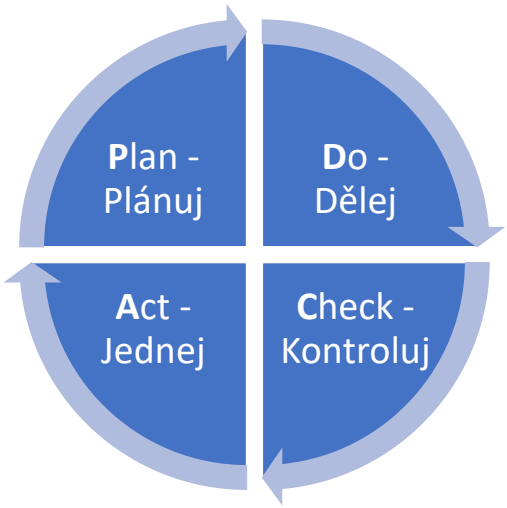
Když se odborné kruhy začaly zabývat problematikou bezpečnosti informací, vytvářely se postupy a procesy v různých skupinách zaměřených na tuto oblast. Tyto postupy postupem času získávaly status „osvědčených postupů" (best practice). Nejprve byly uznávány neformálně, avšak s časem se staly standardy, které našly akceptaci v široké odborné veřejnosti. Tyto standardy se následně staly základem mezinárodních standardů, jež byly mezinárodními organizacemi převedeny do normativní podoby.[78]

Základem pro mezinárodní standardy, včetně systémů řízení bezpečnosti informací, je tzv. **PDCA model** (Plan – Plánuj, Do – Dělej, Check – Kontroluj, Act – Jednej), který je známý také jako Demingův cyklus, pojmenovaný po W. Edwardu Demingovi, který byl jedním z průkopníků systému řízení kvality. Princip modelu PDCA spočívá ve schematickém vyjádření životního cyklu systému řízení a kontinuálním zlepšování procesů. Prvním krokem je „Plánuj", ve kterém jsou především definovány cíle systému řízení, způsob jejich měření na základě ukazatelů a jejich dosažení a měření účinnosti systému řízení. Druhým krokem je „Dělej", v rámci kterého je realizována strategie systému řízení a požadované ukazatele. Ve třetím kroku „Kontroluj" jsou stanoveny výchozí hodnoty sledovaných ukazatelů, ze kterých pak vychází měření účinnosti. V posledním, čtvrtém, kroku „Jednej" jsou implementována nápravná a preventivní opatření, která vedou k trvalému zlepšování systému řízení, a návrh nových

[76] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
[77] Tamtéž.
[78] Tamtéž.

postupů nebo změn. Jednou z významných částí modelu PDCA je dokumentace všech jeho etap. Procesy je třeba identifikovat, popsat, zdokumentovat a následně řídit a optimalizovat jejich průběh.[79]

OBRÁZEK 10: KONTINUÁLNÍ CYKLUS ZLEPŠOVÁNÍ (MODEL PDCA)



Zdroj: vlastní zpracování

ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky je norma vydaná Mezinárodní organizací pro normalizaci (ISO) ve spolupráci s Mezinárodní elektrotechnickou komisí (IEC), která stanovuje požadavky na zavedení, udržování a neustálé zlepšování systému managementu informační bezpečnosti s ohledem na kontext organizace. Zahrnuje také požadavky na hodnocení a řízení rizik informační bezpečnosti v souladu s potřebami organizace.[80] Systém řízení bezpečnosti informací, který je založen na principech PDCA, zahrnuje sedm základních prvků řízení kybernetické bezpečnosti a bezpečnosti informací:[81]

- **Kontext organizace** – Pro stanovení kontextu organizace je třeba porozumět organizaci a jejímu kontextu na základě zvážení externích i interních aspektů (např. zaměření organizace, organizačního uspořádání, technické infrastruktury apod.), porozumět potřebám a očekávání zainteresovaných stran (např. zákazníků, odběratelů, ale i zaměstnanců a státních či regulatorních

[79] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[80] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 17001. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Online. Česká agentura pro standardizaci, 2023. Dostupné z: https://sponzorpristup.agentura-cas.cz/zobrazit.aspx. [cit. 2024-04-16].

[81] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

orgánů), stanovit rozsah systému řízení bezpečnosti informací (které části organizace budou součástí ISMS a které ne) a vytvořit systém řízení bezpečnosti informací dle potřeb organizace.[82]

- **Vůdčí role** – Příkladem pro následování celou organizací je přístup vrcholového vedení ke kybernetické bezpečnosti a bezpečnosti informací a jejich účelnému prosazování v rámci organizace, k čemuž stavuje svůj závazek. Na základě specifických potřeb organizace musí být stanovena Politika kybernetické bezpečnosti a bezpečnosti informací (Politika ISMS). Důležitým bodem je také stanovení rolí, odpovědnosti a pravomocí organizace v souvislosti s prosazováním kybernetické bezpečnosti a bezpečnosti informací.

- **Plánování** – Součástí plánování musí být jak opatření zaměřená na rizika a příležitosti, tak i prohlubování cílů kybernetické bezpečnosti a bezpečnosti informací. Řízení rizik je základním kamenem ISMS a má zásadní vliv na účelnosti a účinnosti celého řízení bezpečnosti a ochrany informací. Blíže je popsáno v kapitole 1.4.3 Hodnocení a řízení rizik.

- **Podpora** – Mezi činnosti podpory kybernetické bezpečnosti a bezpečnosti informací patří zdroje pro realizaci jejich činností, kompetence pro jejich účinnost, povědomí všech osob zapojení do jejich činností, včetně povědomí o přínosech a také možných důsledcích v případě způsobených nedostatků, dále vnitřní i vnější komunikace organizace a řízení dokumentovaných informací v rámci celého jejich životního cyklu (udržování, vč. odebírání, zneplatnění, skartace neplatných verzí dokumentů).

- **Provozování** – Část provozování se zaměřuje na efektivní implementaci všech potřebných opatření bezpečnosti informací stanovených při plánování ISMS. Klíčové je zajistit, že připravené plány budou realizovány ve shodě se zadáním, stanovenými termíny a očekávanými výsledky. Důraz je kladen na to, aby všechna bezpečnostní opatření byla řádně zdokumentována, např. prostřednictvím Příručky bezpečnosti informací. Ta patří do druhé úrovně dokumentace a je určena k podpoře prosazování ISMS. Do první, nejvyšší, úrovně pak patří např. Politika ISMS, zpráva o hodnocení rizik, prohlášení o aplikovatelnosti a další dokumenty, které vyžaduje systém řízení a z hlediska požadavků ISMS jsou povinné. V nejnižší úrovni dokumentace jsou tzv. pracovní postupy vysvětlující úkony nezbytné pro naplnění dílčích procesů.[83]

- **Hodnocení výkonnosti** – Klíčovým cílem tohoto aspektu řízení ISMS je poskytnout zpětnou vazbu o reálném stavu ISMS a jeho výkonnosti. Zároveň by měla být prověřena všechna implementovaná bezpečnostní opatření a jejich vliv na ISMS. V praxi to znamená provedení monitoringu, měření,

[82] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[83] Tamtéž.

analýzy a hodnocení ISMS včetně klíčových ukazatelů a účinnosti opatření, provedení interních auditů celého rozsahu ISMS a připravení zprávy o stavu ISMS pro přehodnocení ISMS vrcholovým vedením organizace.

- **Zlepšování** – Poslední fází řízení ISMS je sběr námětů na zlepšení ISMS a náprava neshod. Náprava neshod čili nesouladu se stanovenými požadavky, probíhá formou realizace nápravných opatření. U neshod je nutné stanovit kořenovou příčinu a nápravná opatření realizovat tak, aby se předešlo možnosti jejich opakování. Zejména na základě přehodnocení vedením by měly být zaváděny náměty na zlepšení ISMS, které byly identifikovány v reálné praxi a na základě zkušenosti aktivních účastníků ISMS.[84]

ISO/SAE 21434:2021 Silniční vozidla – Inženýrství kybernetické bezpečnosti je norma vydaná Mezinárodní organizací pro normalizaci (ISO) ve spolupráci se SAE International, globálním sdružením více než 128 000 inženýrů a technických expertů z oblasti leteckého, automobilového průmyslu a průmyslu užitkových vozidel, která *„specifikuje technické požadavky na řízení rizik kybernetické bezpečnosti týkající se koncepce, vývoje produktu, výroby, provozu, údržby a vyřazování z provozu elektrických a elektronických (E/E) systémů v silničních vozidlech, včetně jejich součástí a rozhraní“*.[85] Shodou s touto normou může výrobce automobilů prokázat splnění požadavků Nařízení OSN č. 155 Jednotná ustanovení pro schvalování vozidel z hlediska kybernetické bezpečnosti a systému řízení kybernetické bezpečnosti.[86]

ISO 24089:2023 Silniční vozidla – Inženýrství softwaru je norma vydaná Mezinárodní organizací pro normalizaci (ISO), která *„specifikuje požadavky a doporučení pro inženýrství aktualizace softwaru pro silniční vozidla na organizační i projektové úrovni“*. Norma je určena pro organizace, které se zabývají vývojem aktualizací softwaru pro silniční vozidla. Můžou to být jak výrobci vozidel, tak dodavatelé a jejich dceřiné společnosti nebo obchodní partneři.[87] Shodou s touto normou může výrobce automobilů prokázat splnění požadavků Nařízení OSN č. 156 Jednotná ustanovení pro schvalování vozidel z hlediska kybernetické bezpečnosti a systému řízení kybernetické bezpečnosti.[88]

---

[84] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[85] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/SAE 21434:2021. *Silniční vozidla – Inženýrství kybernetické bezpečnosti*. Online. ISO, 2021. Dostupné z: https://www.iso.org/standard/70918.html. [cit. 2024-04-16].

[86] TÜV NORD CZECH. *ISO 21434:2021*. Online. [b.d.]. Dostupné z: https://www.tuv-nord.com/cz/cs/nase-sluzby/certifikace-systemu/automobilovy-prumysl/iso-21434/. [cit. 2024-04-16].

[87] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO 24089:2023. *Silniční vozidla – Inženýrství softwaru*. Online. ISO, 2023. Dostupné z: https://www.iso.org/standard/77796.html. [cit. 2024-04-16].

[88] MARTY, Kilian. *Software Update for Road Vehicles - Ep.1 - Overview of UN R156 and ISO 24089*. Online. CERTX. 03.11.2022. Dostupné z: https://certx.com/automotive/software-update-for-road-vehicles-ep-1-overview-of-un-r156-and-iso-24089/. [cit. 2024-04-16].

TISAX® je norma zavedená Německým sdružením automobilového průmyslu VDA (Verband der Automobilindustrie) v roce 2017, jejímž cílem je zvýšení zabezpečení informací v organizacích, které působí v automobilovém průmyslu. Základní požadavky vychází z výše uvedené normy ISO/IEC 27001 Systémy řízení bezpečnosti informací, a navíc jsou zde specifikovány požadavky z oblasti automobilového průmyslu. [89] Podrobněji se této normě věnuje samostatná kapitola 1.5 TISAX® této práce.

1.4.4 Legislativní rámec

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) vstoupil v účinnost 1. ledna 2015. Následně proběhlo několik novelizací, přičemž poslední platná novela proběhla zákonem č. 111/119 Sb. Cílem kybernetického zákona je stanovení práv a povinností v oblasti kybernetické bezpečnosti, posílení právního rámce a zvýšení efektivity při řešení kybernetických bezpečnostních incidentů. Zahrnuje také ochranu infrastruktury významné pro fungování státu, jejíž narušení by ohrozilo nebo poškodilo zájmy České republiky. V tomto směru se jedná o kritickou informační a komunikační infrastrukturu, významné informační systémy, významné sítě elektronických komunikací a tzv. základní služby. Ústředním správním orgánem České republiky pro kybernetickou a informační bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Součástí NÚKIB je tzv. Vládní CERT (Computer Emergency Response Team). Jde o pracoviště, které má za úkol chránit služby a sítě elektronických komunikací a informačních systémů před kybernetickými bezpečnostními událostmi a řeší bezpečnostní incidenty.[90]

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (**směrnice NIS**) je první směrnice ke zvýšení kybernetické bezpečnosti napříč členskými státy Evropské unie. Do české legislativy je promítnuta v ZKB a souvisejících vyhláškách.[91] Dne 27. prosince 2022 byla vydána **Směrnice Evropského parlamentu a Rady (EU) 2022/2555** o opatřeních k zajištění vysoké společné

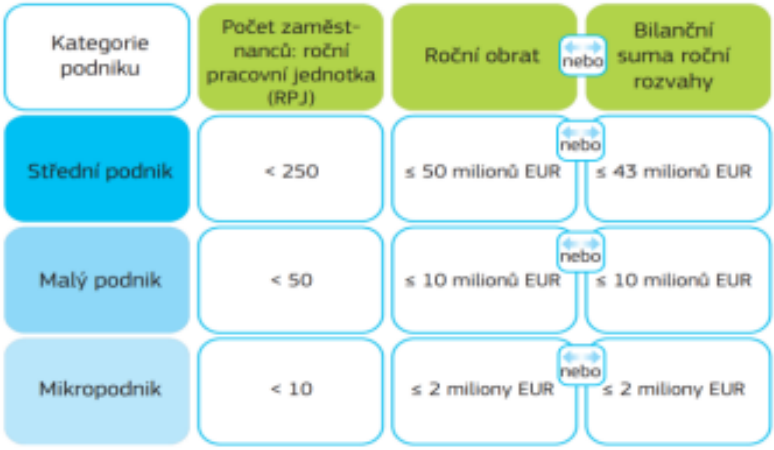
[89] ČESKÁ SPOLEČNOST PRO JAKOST (ČSJ). *Posouzení zabezpečení výměny důvěrných informací: Trusted Information Security Assessment Exchange – TISAX®*. Online. ©2023. Dostupné z: https://www.csq.cz/infocentrum/odborne-clanky/detail/posouzeni-zabezpeceni-vymeny-duvernych-informaci-trusted-information-security-assessment-exchange-TISAX®. [cit. 2024-04-16].

[90] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[91] Tamtéž.

úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148, známá pod označením **směrnice NIS 2**. Směrnice se vztahuje mimo jiné na veřejné i soukromé subjekty, které jsou považovány za střední a velké podniky a poskytují služby nebo vykonávají činnosti v rámci Evropské unie. Velikost podniku se stanovuje v souladu s doporučením komise 2003/361/ES, přičemž musí být naplněn zaměstnanecký nebo finanční ukazatel dle výhodnosti pro daný podnik. Směrnice NIS 2 musí být transponována do národního práva do 21 měsíců, tzn. do 18. října 2024. Pro Českou republiku to znamená nutnou novelizaci ZKB. V současné době je návrh nového zákona o kybernetické bezpečnosti v připomínkovém řízení.[92]

OBRÁZEK 11: POČÍTÁNÍ VELIKOSTI SUBJEKTU DLE ZAMĚSTNANECKÝCH NEBO FINANČNÍCH UKAZATELŮ



Zdroj: NÚKIB. Počítání velikosti subjektu.[93]

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES je obecné nařízení o ochraně osobních údajů (**GDPR**).[94]

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat je založena na mezinárodní normě ISO/IEC 27001. V případě, že si organizace nechá certifikovat systém řízení bezpečnosti informací akreditovaným orgánem, předpokládá se, že splňuje požadavky této

[92] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Nová směrnice EU o kybernetické bezpečnosti "NIS2" a návrh nového zákona o kybernetické bezpečnosti*. Online. [b.d.]. Dostupné z: https://osveta.nukib.gov.cz/course/view.php?id=145. [cit. 2024-04-16].

[93] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Počítání velikosti subjektu*. Online. PDF. 07.11.2023, v. 1.0. Dostupné z: https://osveta.nukib.gov.cz/pluginfile.php/58363/course/section/1391/factsheet_na_koho_regulace_dopadne_final.pdf. [cit. 2024-04-16].

[94] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

vyhlášky. Základními požadavky vyhlášky jsou organizační opatření, technická opatření, stanovení bezpečnostní politiky a dokumentace bezpečnosti, hlášení kontaktních údajů a kybernetických bezpečnostních incidentů.[95]

1.5 TISAX®

TISAX® je zkratka z anglického názvu „Trusted Information Security Assessment Exchange“ neboli Výměna důvěryhodných hodnocení bezpečnosti informací. Jde o *„hodnotící a výměnný mechanismus pro informační bezpečnost podniků a umožňuje uznání výsledků hodnocení mezi účastníky“*. [96]

1.5.1 Historie a význam

Vyráběné automobily jsou čím dál více vybaveny různými měřícími a kontrolními zařízeními, které jsou síťově propojeny. Nejen pro výrobní procesy, ale i vývoj a výměnu dat a informací, je klíčovým faktorem bezpečnost informací. K ochraně dat a zajištění jejich integrity a dostupnosti je možné přispět řízením a snižováním rizik v rámci implementace systému řízení bezpečnosti informací (ISMS). Zohlednění zvláštních požadavků, které se týkají zapojení třetích stran a zacházení s prototypy, dalo základ pro vznik programu TISAX®.[97]

V roce 2003 ustanovila německá asociace automobilového průmyslu VDA (Verband der Automobilindustrie e.V.) skupinu složenou z odborníků z automobilového průmyslu a vytvořila hodnotící katalog VDA ISA (Information Security Assessment). Tento katalog je založen na normě ISO/IEC 27001 a VDA doporučuje, aby společnosti, které působí v rámci hodnotového řetězce automobilového průmyslu, zavedly zabezpečení informací na základě VDA ISA.[98]

ENX Association je asociace založená v roce 2000, sídlící v Boulogne-Billancourt (Francie) a Frankfurtu (Německo). Je složená z výrobců automobilů, dodavatelů a čtyř národních automobilových asociací. Ve vedení asociace působí zástupci firem Renault, BMW a GALIA. Asociace ENX je iniciátorem a řídícím orgánem společných standardů (vč. TISAX®) a plní roli neutrálního orgánu pro jejich správu. Jejím cílem

---

[95] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[96] ENX ASSOCIATION. *About TISAX®*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/TISAX®/. [cit. 2024-03-28].

[97] TÜV NORD CZECH. *TÜV NORD CERT – Hodnocení systémů řízení bezpečnosti informací podle TISAX®*. Online. PDF. 2019. Dostupné z: https://www.tuv-nord.com/fileadmin/Content/TUV_NORD_COM/TUEV_NORD_CZECH/PDF/Produkt_listy/Produktovy_list_TISAX®-web.pdf. [cit. 2024-03-28].

[98] VERBAND DER AUTOMOBILINDUSTRIE (VDA). *Recommendation Information Security*. Online. 04.08.2020. Dostupné z: https://www.vda.de/en/news/publications/publication/recommendation-information-security#publication-title. [cit. 2024-03-28].

je zajištění srovnatelné úrovně ochrany všech zúčastněných stran a podpora konkurenceschopnosti.[99] ENX dohlíží na schválené poskytovatele auditů a sleduje výsledky provedených hodnocení i kvalitu implementace TISAX®. To zajišťuje účastníkům programu TISAX® možnost výběru jakéhokoliv schváleného poskytovatele auditu se standardizovanými výsledky hodnocení akceptovaných ostatními účastníky.[100]

Metodikou implementace TISAX®, která je předpokladem pro posílení kybernetické bezpečnosti a základem pro úspěšné absolvování hodnocení TISAX® akreditovaným poskytovatelem auditu s udělením známky TISAX®, se zabývá praktická část této práce.

1.5.2 Přínosy

TISAX® reflektuje požadavky automobilového průmyslu na zacházení s citlivými informacemi v rámci jeho dodavatelského řetězce. Přináší tak větší důvěru mezi obchodními partnery a je akceptován většinou členů Německého svazu automobilových výrobců (VDA), mezi které patří renomované firmy jako Audi, Volkswagen nebo BMW. Zavedení hodnocení podle TISAX® navíc vyžaduje mnoho výrobců automobilů jako nutnou podmínku pro účast výběrových řízeních a tím navázání další obchodní spolupráce. Zavedením systému řízení rizik jsou snížena možná rizika. Výsledky hodnocení, které má standardizované a přísné hodnocení, je možné porovnávat mezi všemi účastníky zahrnutými do programu TISAX®, přičemž každá společnost sama rozhoduje o zpřístupnění svých výsledků hodnocení. Zároveň je TISAX® svými požadavky silně orientován na potřeby zákazníků.

Účastníci programu TISAX® můžou zaujmout na základě svého rozhodnutí dvě role. V prvním případě se můžou stát pasivním účastníkem (např. OEM, výrobce automobilů), a tudíž vyžadovat provedení hodnocení jiné společnosti a zpřístupnění výsledků tohoto hodnocení. V druhém případě se můžou stát aktivním účastníkem v situaci, kdy provedení jeho hodnocení vyžaduje jiná organizace, příp. se k provedení hodnocení přihlásí na vlastní žádost. Výsledky hodnocení pak zpřístupní vybraným společnostem, např. OEM. Souběh obou rolí není vyloučen.[101]

[99] ENX ASSOCIATION. *About ENX Association*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/enxassociation/. [cit. 2024-03-28].

[100] ENX ASSOCIATION. *About TISAX®*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/TISAX®/. [cit. 2024-03-28].

[101] TÜV NORD CZECH. *TÜV NORD CERT – Hodnocení systémů řízení bezpečnosti informací podle TISAX®*. Online. PDF. 2019. Dostupné z: https://www.tuv-nord.com/fileadmin/Content/TUV_NORD_COM/TUEV_NORD_CZECH/PDF/Produkt_listy/Produktovy_list_TISAX®-web.pdf. [cit. 2024-03-28].

Na základě registrace účastníka vzniká registrovaným společnostem přístup na portál TISAX®. Tato registrace je mimo jiné také podmínkou pro to, aby hodnocení mohla provést akreditovaná auditorská společnost (XAP).[102]

1.5.3 Proces hodnocení TISAX®

Celý proces hodnocení TISAX® se skládá ze tří hlavních kroků, které je třeba absolvovat. V rámci registrace je třeba shromáždit informace o společnosti, která chce proces absolvovat. Poté následuje krok hodnocení zabezpečení, které vychází z katalogu ISA a při kterém je po vybrání poskytovatele auditu provedeno samotné hodnocení zabezpečení informací a následně je předán poskytovatelem auditu výsledek hodnocení. Posledním krokem je výměna, kdy je výsledek hodnocení sdílen s partnerem. Tento výsledek má platnost 3 roky a v případě zájmu účastníka (příp. požadavku jeho partnera) musí být celý třístupňový proces absolvován znovu.

Důležitým krokem v procesu TISAX® je informování hodnocené společnosti poskytovatelem auditu o právu hodnocené společnosti na podání stížnosti. Již samotné neposkytnutí této informace v rámci úvodní schůzky je důvodem ke stížnosti. Stížnost může být podána buď na ENX Association nebo na poskytovatele auditu.[103]

1.5.3.1 Registrace

Během procesu registrace je nutné podepsat dvě smlouvy. První je uzavírána mezi společností žádající o registraci a ENX Associaton ve formě Všeobecných podmínek a pravidel účasti v programu TISAX® (dále jen VPP). VPP jsou bez výjimek pro všechny stejné, aby byla pro všechny zajištěna stejná pravidla. Definují podrobně postup při nakládání s vyměněnými a získanými informacemi během procesu TISAX® a jejich podstatou je zachování důvěrnosti výsledků hodnocení TISAX®.[104]

Dalším krokem je stanovení rozsahu hodnocení zabezpečení informací, tj. definování těch částí společnosti, které nakládají s důvěrnými informacemi partnera a které musí být v rámci hodnocení poskytovatelem auditu posouzeny. Pro popis rozsahu je třeba vybrat buď standardní rozsah nebo vlastní rozsah. Pro většinu účastníků je nejvhodnější standardní rozsah, který je již předdefinován. Dále je třeba rozhodnout o lokalitách, které patří do rozsahu hodnocení. Pro společnost s jednou lokalitou

[102] TÜV NORD CZECH. *TÜV NORD CERT – Hodnocení systémů řízení bezpečnosti informací podle TISAX®*. Online. PDF. 2019. Dostupné z: https://www.tuv-nord.com/fileadmin/Content/TUV_NORD_COM/TUEV_NORD_CZECH/PDF/Produkt_listy/Produktovy_list_TISAX®-web.pdf. [cit. 2024-03-28].

[103] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

[104] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

je zvolen jeden rozsah, pro společnosti s více lokalitami je nutné rozhodnout, zda bude mít v registraci jeden rozsah (a získá tak jednu zprávu o hodnocení s jedním výsledkem a dobou platnosti s využitím posouzení centrálních procesů pouze jednou a tím snížením nákladů na hodnocení) nebo definuje více rozsahů (např. pokud mají lokality různé cíle hodnocení nebo je jejich hodnocení vyžadováno v jiných časových intervalech). Pro sdílení výsledků hodnocení se účastník TISAX® buď v rámci registrace, nebo kdykoliv později, rozhoduje o zveřejnění a sdílení výsledku hodnocení a požadované úrovně sdílení.

Při registraci je nutné definovat také cíl hodnocení na základě typu údajů, se kterými je ve spojení s partnerem nakládáno. Musí být vybrán jeden nebo více cílů hodnocení z aktuálně dvanácti stanovených cílů, a to buď na základě vlastního úsudku hodnocené společnosti nebo na základě požadavku konkrétního cíle od partnera. Cíl hodnocení je vlastně měřítkem zabezpečení informací (nař. cíl „info high“ je určen pro nakládání s informacemi s vysokou potřebou ochrany, cíl „very high availability“ je určen pro nakládání s informacemi s velmi vysokou potřebou ochrany v rámci jejich dostupnosti neboli velmi vysoká dostupnost informací).[105]

TABULKA 1: CÍLE HODNOCENÍ DLE KATALOGŮ KRITÉRIÍ ISA

č.	**Cíl hodnocení (Assessment objective)**	**Katalogy kritérií ISA**
1.	Info high	Information Security (Zabezpečení informací)
2.	Info very high	Information Security (Zabezpečení informací)
3.	Confidential	Information Security (Zabezpečení informací)
4.	Strictly confidential	Information Security (Zabezpečení informací)
5.	High availability	Information Security (Zabezpečení informací)
6.	Very high availability	Information Security (Zabezpečení informací)
7.	Proto parts	Prototype Protection (Ochrana prototypů)
8.	Proto vehicles	Prototype Protection (Ochrana prototypů)
9.	Test vehicles	Prototype Protection (Ochrana prototypů)
10.	Proto events	Prototype Protection (Ochrana prototypů)

[105] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

č.	Cíl hodnocení (Assessment objective)	Katalogy kritérií ISA
11.	Data	Information Security (Zabezpečení informací) Data Protection (Ochrana údajů)
12.	Special data	Information Security (Zabezpečení informací) Data Protection (Ochrana údajů)

Zdroj: ENX. Příručka pro účastníky systému TISAX®[106]

Zároveň je možné stanovit potřebu ochrany (normální, vysokou a velmi vysokou) a tím úroveň hodnocení (AL 1, AL 2, AL 3). V případě úrovně hodnocení 1 (AL 1) je auditorem kontrolována pouze existence dokončeného sebehodnocení, ale ne už jeho obsah. V systému TISAX® se výsledky hodnocení na úrovni 1 nepoužívají, protože mají nízkou úroveň důvěryhodnosti. Kontrolu věrohodnosti sebehodnocení všech lokalit dle stanoveného rozsahu hodnocení (ověření existence) a s kontrolou relevantních důkazů poskytovatelem auditu zahrnuje hodnocení na úrovni 2 (AL 2). Kontrola probíhá formou rozhovoru buď na dálku příp. na vlastní žádost hodnoceného na místě. Nejstriktnější je hodnocení na úrovni hodnocení 3 (AL 3), které také vychází ze sebehodnocení a předložené dokumentace, ale musí proběhnout na místě formou prověření dokumentů a důkazů, provedení plánovaných pohovorů s vlastníky procesů, pozorování lokálních podmínek, sledování realizace procesů a vedení neplánovaných pohovorů s vykonavateli procesu. V případě nemožnosti provedení hodnocení na místě ve všech lokalitách může být toto hodnocení provedeno vzdáleně pomocí video podpory, ale se záznamem drobné neshody ve zprávě o hodnocení TISAX® a stanovenými následnými opatřeními.

Registrace probíhá online po vytvoření účtu na portálu ENX. Po zadání kontaktních údajů, souhlasu s VPP, registrací rozsahu hodnocení (stanovení rozsahu, typu a cílů hodnocení, kontaktní osoby pro daný rozsah a lokality a příp. úrovně zveřejnění a sdílení) je vygenerováno jedinečné identifikační číslo účastníka (ID účastníka) a identifikátor rozsahu (ID rozsahu), které jsou nutné pro objednání hodnocení zabezpečení informací, které provede vybraný schválený poskytovatel auditu TISAX®.[107]

Každá společnost, která se zaregistruje do systému TISAX®, se stává účastníkem TISAX®, a to nezávisle na jeho roli, tj. ať už je aktivním účastníkem (nechává se hodnotit systémem TISAX® a sdílí výsledek

[106] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].
[107] Tamtéž.

hodnocení s ostatními účastníky) nebo je účastníkem pasivním (žádá o hodnocení systémem TISAX® jiného účastníka a obdrží jeho výsledky hodnocení).[108]

1.5.3.2 Hodnocení

Základem pro úspěšné hodnocení TISAX® je dobře zpracovaný systém managementu bezpečnosti informací (ISMS). Pro ověření, zda ISMS splňuje požadovanou úroveň, je nutné provést sebehodnocení pomocí katalogu ISA, který je k dispozici na stránkách ENX Association.[109] Katalog ISA ve formátu aplikace EXCEL obsahuje aktuálně tři katalogy kritérií: Zabezpečení informací (Information Security), Ochrana prototypů (Prototype Protection) a Ochrana údajů (Data Protection). Katalog kritérií je volen dle stanoveného cíle hodnocení, přičemž můžou platit požadavky pouze z jednoho katalogu nebo z více než jednoho katalogu kritérií (viz Tabulka 1 - Cíle hodnocení dle katalogů kritérií ISA). V každém záznamu v obou kategoriích „Další požadavky vysokých nároků na ochranu“ a „Další požadavky velmi vysokých nároků na ochranu“ je požadavek identifikován pomocí označení „C“ (důvěrnost – confidentiality), „I“ (integrita – integrity) nebo „A“ (dostupnost – availability) nebo kombinací těchto písmen.

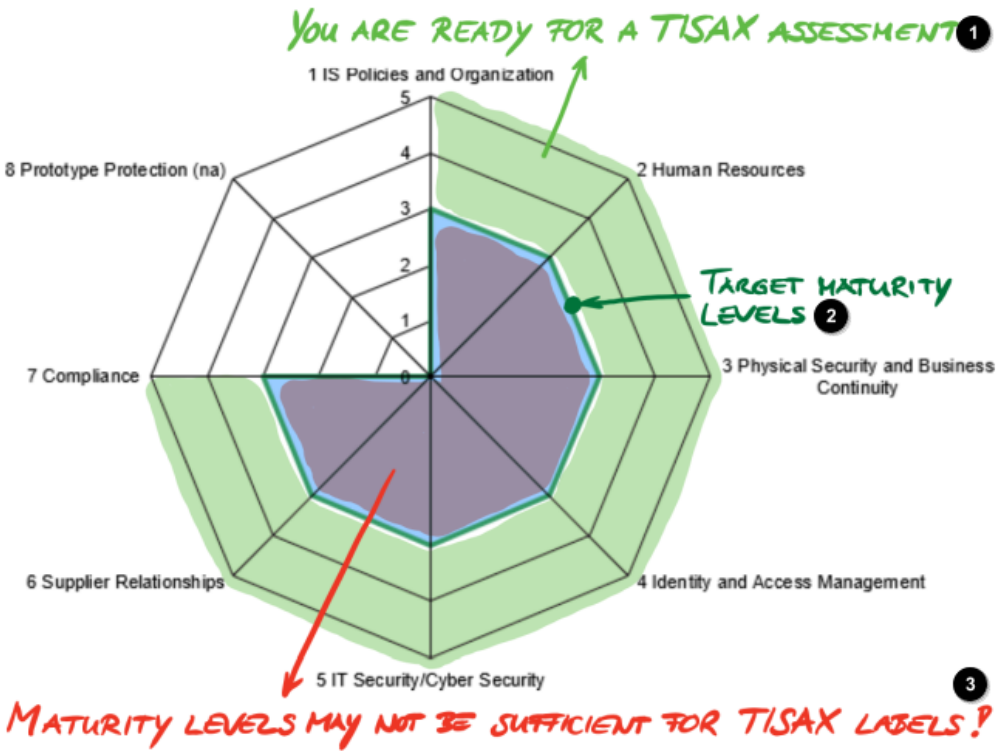
Pro hodnocení kvality všech aspektů systému managementu bezpečnosti informací využívá katalog ISA označení „úroveň vyspělosti“ (maturity levels), která může být neúplná (0), provedená (1), řízená (2), zavedená (3), předvídatelná (4) nebo optimalizační (5). Sebehodnocení je prováděno prostřednictvím zodpovězení kontrolních otázek v jednotlivých katalozích kritérií vztažených ke stanovenému cíli hodnocení. Aby bylo možno získat známku TISAX® (certifikát), měla by být každá otázka zodpovězena stejnou nebo vyšší úrovní vyspělosti, než je cílová úroveň vyspělosti. Celkové výsledné skóre pak představuje celkovou úroveň vyspělosti sytému managementu bezpečnosti informací a mělo by být co nejblíže maximálnímu výslednému skóre, čímž se zvyšuje pravděpodobnost na získání známky TISAX®. Výsledky sebehodnocení jsou graficky znázorněny na listu aplikace Excel „Výsledky“. Pokud leží úroveň vyspělosti na čáře znázorňující cílovou úroveň vyspělosti v jednotlivých kapitolách (viz 2 na obr. č. 10) nebo nad ní (viz 1 na obr. č. 10), pak je hodnocená společnost připravena na hodnocení TISAX®. Pokud leží úroveň vyspělosti pod čárou cílové úrovně vyspělosti (viz 3 na obr. č. 10), nemusí to stačit na získání známky TISAX®.[110]

[108] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

[109] ENX ASSOCIATION. *Downloads*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-28].

[110] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

OBRÁZEK 12: SPLNĚNÍ CÍLOVÉ ÚROVNĚ VYSPĚLOSTI V PAVUČINOVÉM DIAGRAMU



Zdroj: ENX. Příručka pro účastníky systému TISAX®.[111]

V případě potřeby vylepšení systému managementu bezpečnosti informací může společnost požádat o externí poradenství, které může provést i schválený poskytovatel auditu. V takovém případě ale již nesmí provádět hodnocení TISAX® v této společnosti z důvodu zachování nestrannosti a nezávislosti.

Schválené nestranné poskytovatele auditu je možné kontaktovat ve věci získání nabídky na hodnocení hned po registraci rozsahu hodnocení TISAX®. K co nejpřesnější kalkulaci je třeba předložit „Výpis rozsahu TISAX®“ (TISAX® scope excerpt). Hodnocení lze provést pouze pro registrované účastníky systému TISAX®. Při výběru poskytovatele auditu můžou hrát roli různé faktory jako dostupnost auditorů, náklady spojené s cestováním v případě schůzky na místě, jazyk hodnocení (včetně jazykové vybavenosti dalších účastníků pohovoru) nebo rozsah nabídky. Všichni poskytovatelé auditu jsou ale vázáni stejnou smlouvou a provádí hodnocení na základě stejných kritérií.[112]

Proces hodnocení TISAX® zahrnuje přípravu systému managementu bezpečnosti informací, poté poskytoval auditu prověřuje soulad systému managementu bezpečnosti informací se stanoveným souborem požadavků. V případě zjištěných nedostatků musí být tyto nedostatky ve stanovených

[111] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].
[112] Tamtéž.

lhůtách odstraněny. Jejich odstranění je znovu kontrolováno poskytovatelem auditu. Celý postup se opakuje do té doby, než jsou odstraněny všechny nedostatky.

Proces hodnocení TISAX® probíhá ve třech fázích – zahajovací schůzka, fáze 1 a fáze 2. V rámci zahajovací schůzky (kick-off meeting) jsou plánovány podrobnosti procesu hodnocení. Ta probíhá zpravidla vzdálenou formou v podobě konferenčního nebo video hovoru a předmětem jsou např. podrobnější informace o hodnocení společnosti, vysvětlení procesu hodnocení TISAX®, prověření správnosti rozsahu hodnocení, vyloučení střetu zájmu, plánování další fáze procesu hodnocení nebo kontaktní údaje v případě stížnosti. Další fáze hodnocení začíná obvykle jeden až tři měsíce po ukončení zahajovací schůzky a předání sebehodnocení, nicméně žádná konkrétní lhůta není stanovena.

V samotném procesu hodnocení TISAX® můžou nastat tři typy hodnocení – úvodní hodnocení, hodnocení plánu nápravných opatření a následné hodnocení. Úvodní hodnocení (initial assessment) je povinné, další dva typy můžou nastat, pokud nejsou odstraněny všechny nedostatky společnosti, dokud není ukončen proces hodnocení TISAX® nebo dokud neuplyne maximální lhůta, která činí devět měsíců od ukončení úvodního hodnocení (jinak je třeba provést úvodní hodnocení znovu).

Každé hodnocení začíná formální zahajovací schůzkou, která se zaměřuje na organizační záležitosti, kontrolu předpokladů hodnocení a dohodnutí termínů pro předložení sebehodnocení a další příslušné dokumentace, a může probíhat během jednoho nebo více, ne nutně osobních, setkání. Během samotného hodnocení, které probíhá dle připraveného plánu, prověřuje poskytovatel auditu všechny požadavky dle relevantní úrovně hodnocení. Zpravidla probíhá formou konferenčních hovorů a různých rozhovorů na místě. Na závěr hodnocení probíhá formální, ne nutně osobní, závěrečná schůzka, při které poskytovatel auditu oznamuje svá zjištění a výsledek hodnocení. Během této schůzky také vypracuje předběžnou zprávu o hodnocení TISAX®, na základě které, pokud k ní nemá hodnocená společnost výhrady, vystaví závěrečnou zprávu o hodnocení TISAX®.[113]

Zjištění, která definují nesoulad s požadavky, můžou být klasifikována jako „závažná neshoda“, „drobná neshoda“, „pozorování“ nebo „prostor pro zlepšení“. Závažná neshoda (major non-conformity) představuje významné riziko, které ohrožuje zabezpečení informací, nebo existují-li na základě hodnocení pochybnosti o celkové účinnosti systému bezpečnosti informací. Taková neshoda musí být bez prodlení řešena prostřednictvím vhodně stanovených a realizovaných nápravných opatření. Drobná neshoda (minor non-conformity) nepředstavuje významné riziko, které by ohrožovalo zabezpečení informací ani neiniciuje pochybnosti o celkové účinnosti systému bezpečnosti

[113] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

informací a nápravná opatření musí být zavedena bez zbytečného prodlení. Pozorování (observation) znamená neshodu s požadavky a stanovenými zásadami hodnocené společnosti, které může v budoucnu představovat významné riziko, které by ohrožovalo zabezpečení informací. Při takovém zjištění je třeba případná rizika přezkoumávat a vyhodnocovat. Prostor pro zlepšení (room for improvement) je typ neshody, která nepatří do výše uvedených kategorií, ale představuje určitý prostor pro zlepšení. Záleží potom na hodnocené společnosti, zda a jak ji bude řešit.

Cílem hodnocení je zjištění ze strany poskytovatele auditu, zda systém managementu bezpečnosti informací hodnocené společnosti vyhovuje stanoveným požadavkům. Výsledkem hodnocení tedy může být, že je v souladu s požadavky, tzn. „vyhovuje“, nebo „závažná neshoda“.

V případě celkového výsledku hodnocení „závažná neshoda“ musí hodnocená společnost stanovit způsob řešení zjištění z hodnocení formou plánu nápravných opatření (corrective action plan). Plán opatření by měl obsahovat vždy konkrétní zjištění, k němu určenou kořenovou příčinu, definované jedno nebo více nápravných opatření, které povedou k odstranění neshody, dále termín realizace nápravného opatření s dostatečným časovým prostorem, kompenzační opatření, tj. opatření pro kritická rizika do doby realizace nápravných opatření a lhůtu realizace nápravného opatření. V případě, že realizace nápravného opatření trvá déle než tři měsíce, musí být lhůta realizace zdůvodněna. V případě, že trvá déle než šest měsíců, musí být navíc předloženy důkazy o tom, že realizaci nápravného opatření není možné provést dříve. Maximální lhůta realizace smí být maximálně devět měsíců.

Po vypracování plánu nápravných opatření požádá hodnocená společnost poskytovatele auditu o hodnocení plánu nápravných opatření. To muže proběhnout buď jako samostatná akce nebo již při zavěřeném setkání. Při hodnocení plánu nápravných opatření je posuzována vhodnost nápravného opatření, dostatečnost zmírnění kritických rizik prostřednictvím kompenzačních opatření, přiměřenost stanovených lhůt realizace a soulad s požadavky na maximální lhůty realizace. Toto hodnocení probíhá většinou formou telefonní nebo videokonference, příp. e-mailem, a výstupem je zpracovaná „zpráva o hodnocení plánu nápravných opatření“ s celkovým výsledkem hodnocení „drobná neshoda“.[114]

V případě dosažení celkové výsledku hodnocení „drobná neshoda“ (po zpracování zprávy o hodnocení plánu nápravných opatření) může být udělena dočasná známka TISAX®. Ta je zpravidla akceptována partnery jako prokázání účinnosti systému managementu bezpečnosti informací, protože je

[114] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

rovnocenná trvalé známce TISAX®, s jediným rozdílem v jejich platnosti. Dočasná známka má platnost nejdéle shodně s nejdelší dobou realizace nápravných opatření, tj. maximálně devět měsíců.

Pokud jsou realizována všechna nápravná opatření, měla by hodnocená společnost požádat poskytovatele auditu o „následné hodnocení“. O to může požádat také hned po vypracování plánu nápravných opatření bez provedení hodnocení plánu nápravných opatření, pokud nepotřebuje dočasnou známku TISAX® a pokud si je jista, že nápravná opatření provede i bez schválení poskytovatelem auditu. Během následného hodnocení jsou vyhodnoceno, zda byly všechny dosud zjištěné neshody odstraněny. Následná hodnocení se mohou opakovat do té doby, než budou odstraněny všechny do té doby zjištěné neshody nebo nové neshody zjištěné během následných hodnocení, nejpozději však do devíti měsíců od ukončení původního hodnocení. Můžou probíhat jak fyzicky, tak prostřednictvím telefonní nebo videokonference.

Po ukončení procesu hodnocení (odstranění neshod realizací nápravných opatření nebo na základě celkového výsledku hodnocení „vyhovuje“) je udělena známka TISAX®, která má zpravidla platnost 3 roky. Pokud si chce hodnocená společnost udržet známku TISAX® dlouhodobě, musí pak znovu projít procesem TISAX® (zaregistrovat si oblast působnosti, oslovit poskytovatele auditu atd.). Známka TISAX® je udělena v souladu se stanoveným cílem hodnocení. Spolu s ním jsou automaticky uděleny také všechny známky TISAX®, které jsou hierarchicky níže, např. spolu se známkou TISAX® „Info very high“ jsou uděleny také známky „Strictly confidential“ a „Very high availability“, které jsou její podmnožinou.[115]

1.5.3.3 Výměna

Informace související s hodnocením hodnocené společnosti jsou vyměňovány prostřednictvím portálu ENX. Po nahrání zprávy o hodnocení TISAX® poskytovatelem auditu (zpravidla 5–10 pracovních dnů po jejím vystavení) jsou informace dostupné pouze pro hodnocenou společnost. Ta rozhoduje o úrovni sdílení informací.[116]

Úrovně sdílení se dělí na pět částí dle oddílů zprávy o hodnocení TISAX® s označením A–E (A. Informace týkající se hodnocení, B. Souhrnné výsledky, C. Souhrn výsledků hodnocení, D. Úrovně vyspělosti VDA ISA, E. Podrobné výsledky hodnocení). Výsledek hodnocení je možné sdílet se všemi účastníky TISAX®, pokud je celkový výsledek hodnocení „vyhovuje“, s těmito omezeními úrovní: „Nezveřejňovat“, „A. Informace týkající se hodnocení“, „A + Známky“, „A + Známky + Souhrnné výsledky“. Výsledky

[115] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].
[116] Tamtéž.

hodnocení je možné také sdílet pouze s konkrétními účastníky TISAX® s vyšší úrovní sdílení, a to i pokud je celkový výsledek hodnocení neshoda (závažná nebo drobná). Sdílení je pak omezeno na: „A. Informace týkající se hodnocení“, „A + Známky“, „A + Známky + B + C. Souhrnné výsledky“, „A + Známky + B + C + D. Podrobné výsledky hodnocení“ a „A + Známky + B + C + D + E. Úrovně vyspělosti podle ISA“. Udělené oprávnění ke sdílení informaci nelze zrušit, aby k němu měli trvale přístup i pasivní účastníci, a platí po celou dobu platnosti hodnocení TISAX®.

Výsledek hodnocení je možné zveřejňovat pouze prostřednictvím výměnné platformy, přičemž partner musí být minimálně registrován jako účastník TISAX® (nemusí mít registrovaný rozsah hodnocení ani absolvovat proces hodnocení). V případě potřeby doložení známky TISAX® zaměstnanci partnera, který nemá přístup do portálu, je možné stáhnout z portálu ENX speciální dokument PDF jako kopii informací sdílených se společností partnera.[117]

[117] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

2 Metodologie

Předmětem této diplomové práce je navržení metodiky implementace TISAX® ve vybrané organizaci, která je dodavatelem dílů pro výrobce automobilů. Vzhledem k citlivosti údajů a podstatě TISAX®, tj. bezpečnosti vyměňovaných informacích, je vybraná organizace anonymizována.

Prvním krokem je literární rešerše v teoretické části práce, která zahrnuje popsání procesu fungování dodavatelského řetězce v automobilovém průmyslu, způsobu výměny informací mezi jeho jednotlivými členy a důraz na zachování bezpečnosti dodavatelského řetězce. V další kapitole jsou vysvětleny pojmy kybernetické bezpečnosti a význam organizačních a technických, respektive technologických bezpečnostních opatření. Dále jsou detailněji popsány principy kybernetické bezpečnosti jako triáda CIA, prvky kybernetické bezpečnosti a cyklus kybernetické bezpečnosti. Následně jsou rozepsány podstatné vstupy pro řízení bezpečnosti informací, včetně existujících standardů a legislativních požadavků v této oblasti. Poslední kapitola teoretické části představuje systém TISAX®, hodnotící a výměnný mechanismus pro informační bezpečnost organizací, jehož požadavky vychází z výše uvedených pojmů a postupů, uvádí jeho historii a význam, přínosy pro členy dodavatelského řetězce a podrobně popisuje proces hodnocení, který je finální fází po jeho implementaci.

Praktická část diplomové se týká metodiky implementace systému TISAX®. Nejdříve je provedena charakteristika vybrané organizace, která je dodavatelem do automobilového průmyslu, a tedy typickým druhem organizace, od které je implementace systému TISAX® vyžadována. Podstatnou část praktické části tvoří návrh metodiky pro samotnou implementaci systému TISAX®.

Celkově je k dispozici relativně málo dostupných zdrojů týkajících se systému TISAX®. Proto navržená metodika vychází z normativních dokumentů systémů managementu bezpečnosti informací a dvou závazných dokumentů TISAX®, kterými je hodnotící katalog kritérií ISA a Příručka pro účastníky systému TISAX®.

K návrhu metodiky je využit kvalitativní výzkum formou hloubkového porovnání následujících dokumentů:

- Norma ČSN EN ISO/IEC 27001:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky, která se zabývá požadavky na stanovení, implementování, udržování a neustále zlepšování systému managementu informační bezpečnosti.

- Norma ČSN EN ISO/IEC 27002:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti, která se zabývá obecnými opatřeními informační bezpečnosti včetně pokynu k implementaci.

- Norma ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny, která se zaměřuje na kritické aspekty nutné pro úspěšný návrh a implementaci systému řízení bezpečnosti informací.

- Katalog ISA VDA, verze 6.0.1, který obsahuje kontrolní otázky pro sebehodnocení TISAX® pro zjištění stavu informační bezpečnosti v rámci organizace a požadavky, které organizace musí splnit, které by měla splnit, příp. další požadavky vysokých nároků na ochranu a další požadavky velmi vysokých nároků na ochranu pro splnění požadavků TISAX®.

- Příručka pro účastníky systému TISAX® popisující proces hodnocení TISAX®, který následuje po jeho implementaci v organizaci.

Součástí plánu implementace TISAX® je také návrh metodiky pro analýzu rizik, návrh metodiky hodnocení dodavatelů, návrh organizačního schématu a návrh stanovených cílů dle metody SMART.

PRAKTICKÁ ČÁST

3 Implementace TISAX®

Požadavkem automobilek je stále častěji certifikace TISAX® a organizace, které chtějí být součástí dodavatelského řetězce tak musí plnit požadavky na systém řízení bezpečnosti informací a implementovat systém TISAX®. Implementace TISAX® může být prokázána hodnocením nezávislého a nestranného poskytovatele auditu (certifikačního orgánu). Cílem je, aby byly ochráněny veškeré informace, které výrobce automobilů dodavatelům sděluje, včetně ochrany prototypů. V následujících kapitolách je popsána navržená metodika implementace systému TISAX® u vybrané organizace tak, aby splňoval všechny požadavky na systém řízení bezpečnosti informací a byl připraven pro hodnocení poskytovatelem auditu a získání známky TISAX®.

3.1 Charakteristika vybrané organizace

Veškeré informace o vybrané organizaci budou anonymizovány vzhledem k podstatě systému TISAX® o zabezpečení informací.

Vybraná organizace XY působí v průmyslovém městě Mladá Boleslav, což je její strategicky výhodná geografická poloha. Další závody má v Liberci, Chrastavě a Břehyni. Její základy vznikly v roce 2005 s 10 zaměstnanci a v současnosti má více než 250 zaměstnanců, včetně rozsáhlého týmu specialistů. Hlavním předmětem jejího podnikání je galvanizérství a smaltérství a nabízí velký rozsah služeb, především pro automobilový a energetický průmysl, železniční techniku a zpracovatelské stroje. Svoje klienty podporuje zejména v oblasti vývoje produktů a poskytování služeb v oblasti návrhu, inženýringu, testování a homologování a vyvíjí kontinuální úsilí v oblasti inovací.

Podnikání organizace je podporováno implementovaným integrovaným systémem managementu v souladu s mezinárodními standardy. Organizace je držitelem akreditovaných certifikátů pro systém managementu kvality podle ISO 9001:2015, systém environmentálního managementu dle ISO 14001:2015 a také systém managementu kvality pro automobilový průmysl dle IATF 16949:2016, který vychází z normy ISO 9001 a je doplněn o specifické požadavky automobilového průmyslu. Aby mohla být organizace součástí dodavatelského řetězce pro automobilový průmysl, musí doložit existenci implementovaného systému TISAX®, tj. systému managementu bezpečnosti informací pro automobilový průmysl.

Ve spojení s automobilovým průmyslem se organizace primárně zabývá povrchovou úpravou dílů včetně odmaštění, což představuje kód 25610 Povrchová úprava a zušlechťování kovů v rámci klasifikace ekonomických činností CZ-NACE, a dále výrobou měřících, zkušebních a navigačních

přístrojů s kódem 26510 a výrobou motorových vozidel (kromě motocyklů), přívěsů a návěsů s kódem 29. Tímto bude splňovat kritéria regulované služby dle návrhu Vyhlášky o regulovaných službách, která zapracovává příslušný platný předpis Evropské unie.[118] Organizace provozuje čtyři linky: dvě automatické ponorové linky a jednu postřikovou linku na odmašťování a pasivaci hliníkových a ocelových dílů a ponorovou linku na nanášení ochranné vrstvy zink-fosfátu na kovové díly. Disponuje výrobní plochou 2500 m^2 a skladovými plochami o výměře 3000 m^2. Mezi její další významné služby patří engineering v souvislosti s bezpečností a životností vozidel včetně jejich komponent a dále testování vozidel v oblasti pasivní i aktivní bezpečnosti. Pro elektronickou výměnu dat využívá WEB EDI, EDI a ASN.

Organizace je přímým dodavatelem OEM a je od ní vyžadována implementace a certifikace TISAX®. Jejími partnery jsou např. Škoda Auto, Mercedes-Benz, Continental, Porsche, Benteler, Jaguar, Audi, Grupo Antolin, Magna, STADLER, ČVUT, Centrum dopravního výzkumu, Ministerstvo dopravy, TÜV NORD Czech.

Na základě požadavků obchodních partnerů by měla organizace dosáhnout těchto cílů hodnocení: nakládání s informacemi s velmi vysokou potřebou ochrany (Info very high) na úrovni „důvěrnost“ (Confidentiality), ochranu prototypových dílů a součástí (Proto parts) a ochranu prototypů vozidel (Proto vehicles). K prokázání dosažení těchto cílů se organizace rozhodla zavést systém TISAX® a v dalším kroku pak požádat poskytovatele auditu o provedení hodnocení za účelem získání známky TISAX®.

3.2 Proces implementace TISAX®

Systém TISAX® vychází ve své podstatě ze systému managementu bezpečnosti informací, jak již bylo popsáno v kapitolách výše. Navržený plán implementace TISAX® tedy vychází z požadavků české verze normy ČSN EN ISO/IEC 27001:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky, z české verze normy ČSN EN ISO/IEC 27002:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti, z české verze normy ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny , dále ze specifických požadavků systému TISAX® dle katalogu ISA verze 6.0.1, který reflektuje specifické požadavky automobilového průmyslu, a Příručky účastníků systému TISAX®.

[118] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

Aktuálně platná verze katalogu ISA 6.0.1 je rozdělena na tři katalogy kritérií (Informační bezpečnost, Ochrana prototypů a Ochrana dat, jak je podrobněji uvedeno v kapitole 1.5.3.2 Hodnocení). Katalog Informační bezpečnost obsahuje požadavky, které organizace musí splnit („must“), požadavky, které by organizace měla splnit („should“), další požadavky vysokých nároků na ochranu a další požadavky velmi vysokých nároků na ochranu. Katalog Ochrana prototypů obsahuje požadavky, které organizace musí splnit („must“), požadavky, které by organizace měla splnit („should“) a další požadavky na vozidla klasifikovaná jako vozidla vyžadující ochranu. Katalog Ochrana údajů obsahuje požadavky, které organizace musí splnit („must“).[119]

Vybraná organizace musí s ohledem na stanovené cíle hodnocení splňovat požadavky v katalogu Zabezpečení informací, včetně dalších požadavků vysokých nároků na ochranu a dalších požadavků velmi vysokých nároků na ochranu s označením C (Confidentiality/Důvěrnost) a dále požadavky v katalogu Ochrana prototypů v rozsahu kapitol 8.1, 8.2 a 8.3.[120] Navržená metodika tak nebude zohledňovat požadavky, které nejsou pro vybranou organizaci relevantní.

Následující navržený proces implementace má sloužit jako vodítko pro zavedení systému TISAX® dle stanovených cílů vybrané organizace. Popisuje proces od analýzy současného stavu bezpečnostních opatření a analýzy rizik, přes stanovení rozsahu a cílů systému managementu bezpečnosti informací, až po implementaci bezpečnostních opatření. Cílem navrženého procesu je vytvoření finálního plánu pro implementaci TISAX® v rozsahu stanovených cílů vybrané organizace.

3.2.1 Analýza současného stavu bezpečnosti informací a bezpečnostních opatření

Klíčovým krokem pro implementaci TISAX® je analýza současného stavu bezpečnosti informací a bezpečnostních opatření, aby bylo možno identifikovat případné nedostatky a rizika. Musí být prověřeno:

- Aktuální politiky týkající se bezpečnosti informací, postupy a dokumentace.
  Výsledkem by měl být souhrn všech stávajících organizačních opatření.
- Definice požadavků bezpečnosti informací na základě cílů, vizí a priorit organizace pro bezpečnost informací a na základě souhrnu omezení, která se vážou k bezpečnosti informací organizace (legislativní, smluvní, oborová).
- Identifikace aktiv (včetně jejich vlastníků a přípustného používání) a jejich rozdělení na primární, podpůrná, kritická a informační, způsob nakládání s nimi (vznik, uložení, identifikace, manipulace,

[119] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].
[120] Tamtéž.

přeprava, skladování, vrácení, vymazání, likvidace) a jejich klasifikace pro stanovení potřeby ochrany (zejména důvěrnosti, integrity, dostupnosti) na základě stanoveného schéma pro klasifikaci aktiv.

Výsledkem je podrobný seznam všech identifikovaných aktiv (případně kategorií aktiv), včetně všech zmíněných relevantních informací a stanovených odpovědných osob především za informační a podpůrná aktiva. K informačním aktivům (např. obchodní tajemství, know-how) by měla být přiřazena odpovídající podpůrná aktiva (např. IT systémy, IT služby). Seznam aktiv by měl být následně pravidelně kontrolován a udržován během celého jejich životního cyklu (od vytvoření/uvedení do provozu/použití až po zničení/vymazání).

- Souhrn technických opatření, kterými může být jak hardware, tak software (např. antivirové programy, firewally, šifrování, systém pro zálohování dat, správa přístupů k datům a systémům).
  Výsledkem je podrobný seznam všech stávajících technických opatření.
- Souhrn fyzických opatření (např. definování bezpečnostních zón, zabezpečení prostor jako jsou serverovny a datová centra apod.).
  Výsledkem je podrobný seznam všech stávajících fyzických opatření.
- Souhrn opatření v oblasti lidských zdrojů.
  Na základě průzkumu mezi zaměstnanci je k dispozici přehled o aktuálním povědomí zaměstnanců o bezpečnosti informací, z čehož se bude později v dalších krocích odvíjet plán na školení a vzdělávání zaměstnanců a zavedení relevantních bezpečnostních opatření.
- Vyhodnocení bezpečnosti informací na základě porovnání současného stavu bezpečnosti informací se stanovenými cíli organizace.
  Na vyhodnocení by se měly podílet osoby s velmi dobrou znalostí současného prostředí napříč celou organizací (např. vedoucími, vlastníky procesů, ale i uživateli procesů). Výsledkem vyhodnocení by mělo být získání předběžné informace ohledně aktuálního stavu bezpečnosti informací organizace.[121]

3.2.2 Analýza rizik

Dalším důležitým krokem v implementaci TISAS je analýza rizik, která zahrnuje:

- Hodnocení rizik na základě již získaného aktuálního stavu bezpečnosti informací a identifikace aktiv. Zohledněny by měly být hrozby a jejich zdroje, již zavedená a také plánovaná opatření, zranitelnosti, které by mohly být zneužity hrozbami a vést k poškození aktiv nebo organizace,

[121] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

identifikace dopadů na aktiva v případě ztráty důvěrnosti, integrity a dostupnosti, hodnocení potenciálních dopadů na činnost organizace v případě incidentů bezpečnosti informací, ohodnocení možnosti vzniku incidentů, odhad úrovně rizik a srovnání této úrovně s kritérii hodnocení a akceptace rizik. Na vyhodnocení by se měly podílet osoby s velmi dobrou znalostí cílů organizace a pochopením bezpečnosti napříč celou organizací. Hodnocení rizik se po implementaci TISAX® provádí v pravidelných intervalech nebo v případě vzniku bezpečnostního incidentu jako reakce na něj.[122]

- Stanovení cílů opatření a bezpečnostních opatření na základě Přílohy A normy ČSN EN ISO/IEC 27001:2023 nebo jiných specifikovaných cílů opatření a jednotlivých bezpečnostních opatření pro zmírnění rizik, které vyžaduje plán rizik. Např. pro oblast klasifikaci informací musí být stanoveno opatření, že informace musí být klasifikovány podle potřeb organizace v oblasti informační bezpečnosti na základě důvěrnosti, integrity, dostupnosti a požadavků příslušných zainteresovaných stran.

  Výsledkem by měl být seznam vybraných bezpečnostních opatření a cílů opatření (vzhledem k citlivosti údajů je třeba zohlednit při zpracování seznamu okruh příjemců, tj. interních i externích, kterým bude seznam k dispozici) a také plán zvládání rizik s definováním vztahů jednak s vybranými variantami zvládání rizik, tak s cíli opatření a jednotlivými bezpečnostními opatřeními.[123]
- Získání souhlasu s implementací a provozováním TISAX® ze strany vedení organizace na základě popisu metodiky hodnocení rizik, výsledků hodnocení rizik a vybraných cílů opatření a plánu zvládání rizik.[124]

  Výsledkem by měl být písemný souhlas vedení organizace s implementací, přijetím zbytkových rizik a souhlasem s provozováním TISAX®.

Návrh metodiky analýzy rizik:

Hodnocení rizika úrovně zabezpečení je doporučeno metodou „WHAT-IF“, tzn. postup dle možných dopadů hrozeb na aktiva organizace a případné následky na činnost organizace. Předpokladem je provedené hodnocení rizik aktiv.

---

[122] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2023. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

[123] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27001:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Online. ČAS, ©2023. Dostupné z: https://sponzorpristup.agentura-cas.cz/zobrazit.aspx. [cit. 2024-03-30].

[124] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2023. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

Postup:

- Stanovení pravděpodobnosti výskytu rizika (PV) a přidělení váhy.

TABULKA 2: KLASIFIKACE PRAVDĚPODOBNOSTI VÝSKYTU RIZIK

Pravděpodobnost výskytu rizika (PV)	**Váha**
Velmi vzácný výskyt (> 10 let)	1
Výjimečně možný výskyt (1x za 5 let)	3
Možný výskyt (1x ročně)	5
Častý výskyt (1x půl roku)	7
Pravidelný výskyt (průměrně 1x měsíčně)	9

Zdroj: vlastní zpracování

- Stanovení následku rizika (N). Ke každému riziku je přiřazené číslo, které vyjadřuje „úroveň“ rizika podle její hodnoty. Kritérium závažnost rizika (K) je vypočítána jako $K = 2^n$ (n = 1, 3, 5).

TABULKA 3: KLASIFIKACE ÚROVNĚ RIZIK DLE KRITÉRIA ZÁVAŽNOSTI

Úroveň	**Kritérium závažnosti rizika (K)**	**Charakteristika**	**Popis závažnosti rizika**
1	$2^1 = 2$	Nevýznamný	Nízká míra narušení procesů a postupů v organizaci bez vlivu na chod organizace. Je možná okamžitá náprava.
2	$2^3 = 8$	Střední	Střední míra narušení procesů a postupů v organizaci, neoprávněné nakládání s aktivy v rámci organizace, nevědomé porušení legislativních předpisů a norem.
3	$2^5 = 32$	Katastrofální	Vysoká míra narušení procesů a postupů s vysokým vlivem na chod organizace, únik citlivých údajů a osobních údajů, vědomé porušení legislativních předpisů a norem.

Zdroj: vlastní zpracování

- Výpočet indexu rizika (IR). Celkové riziko je určeno součinem pravděpodobnosti a závažnosti rizika.

  IR = PV x N

TABULKA 4: VÝPOČET INDEXU RIZIKA

Pravděpodobnost výskytu rizika (PV)	**Následek (N)**		
	2 Nevýznamný	8 Střední	32 Katastrofální
1 Velmi vzácný výskyt	2	8	32
3 Výjimečně možný výskyt	6	24	96
5 Možný výskyt	10	40	160
7 Častý výskyt	14	56	224
9 Pravidelný výskyt	18	72	288

Zdroj: vlastní zpracování

- Celkové riziko je zatříděno do rizikové skupiny, případně je doporučeno zavedení opatření.

TABULKA 5: ZATŘÍDĚNÍ RIZIK DO RIZIKOVÝCH SKUPIN

Riziková skupina	**Popis**
1 (IR ≤ 14)	Běžné riziko, nejsou potřeba žádná zvláštní opatření
2 (IR 15-56)	Zvýšená úroveň rizika, je potřeba ho kontrolovat, je doporučeno zvážit zavedení bezpečnostního opatření
3 (IR > 56)	Velmi vysoká úroveň rizika, je potřeba implementovat bezpečnostní opatření a kontrolovat jeho dodržování

Zdroj: vlastní zpracování

3.2.3 Hodnocení dodavatelů

Pro efektivní řízení dodavatelského řetězce a zajištění konkurenceschopnosti a stability organizace je třeba provádět hodnocení dodavatelů. Hodnocení dodavatelů přispívá k zajištění kvality, protože dodané výrobky nebo služby splňují stanovené standardy a požadavky na kvalitu. Prostřednictvím řízení rizik se může organizace lépe připravit na potenciální rizika jako jsou zpoždění nebo snížená kvalita dodávek. Hodnocení dodavatelů pomáhá identifikovat oblasti pro zlepšení, čímž podporuje proces kontinuálního zlepšování a inovací v dodavatelském řetězci. Nespornou výhodou je také

optimalizace nákladů na základě identifikování dodavatelů s konkurenceschopnými cenami při požadované úrovni kvality.[125]

Pojem dodavatel zahrnuje systém TISAX® klasické dodavatele a subdodavatele, poskytovatele služeb, freelancery, partnerské společnosti i kooperační partnery (např. akademické instituce, ústavy).[126]

Aby mohla organizace ve svých vztazích s dodavateli udržovat určitou požadovanou **úroveň informační bezpečnosti**, měla by zpracovat:

- Politiku pro vztahy s dodavateli. To se vztahuje i na využívání poskytovatelů cloudových služeb. Za tímto účelem musí identifikovat a zavést procesy a postupy pro hodnocení a řešení bezpečnostních rizik v souvislosti s využíváním produktů a služeb poskytovaných dodavateli a s ohledem na informační bezpečnost.
- Seznam dodavatelů, kteří můžou mít vliv na důvěrnost, integritu a dostupnost informací organizace (např. služby ICT, finanční služby, logistika) se specifikací příslušné potřeby ochrany a z toho vyplývajících požadavků na zabezpečení.[127]

  Požadavky na specifikaci potřeb ochrany můžou v případě potřeby vysoké ochrany nebo potřeby velmi vysoké ochrany zahrnovat např. povinnost být účastníkem TISAX® nebo zajištění souladu s požadavky jiným vhodným způsobem (např. certifikací dle aktuální verze normy ISO/IEC 27001).[128]
- Způsob hodnocení dodavatelů a jejich výběr podle citlivosti informací, produktů nebo služeb (stanovení kritérií jako zavedený systém ISMS, kvalita, dodržování dodacích termínů atd.).
- Způsob hodnocení definovaných produktů nebo služeb dodavatelů a jejich výběr podle jejich odpovídajících opatření informační bezpečnosti na základě přezkoumání (schválení).
- Postupy pro ukončení vztahu s dodavatelem s ohledem na zrušení přidělených přístupových práv, nakládání s informacemi nebo duševní vlastnicí, které vzniklo během zakázky, vrácení aktiv a likvidaci informací.[129]

[125] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[126] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[127] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[128] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[129] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

Odpovídající úroveň informační bezpečnosti je zajišťována prostřednictvím **smluvních ujednání** s dodavateli, ve kterých jsou jasně stanovené povinnosti obou stran pro plnění požadavků na informační bezpečnost. Mezi požadavky na informační bezpečnost patří zejména:

- identifikace informací, které je možné poskytnout nebo zpřístupnit a jakou formou,
- přehled zákonných, statutárních, regulatorních a smluvních požadavků, včetně ochrany dat a určení způsobu jejich splnění,
- postupy pro povolené nakládání s informacemi a ostatními souvisejícími aktivy,
- seznam dohod s externími stranami (např. smluv nebo dohod o sdílení informací) pro ucelený přehled o tom, kam jsou informace organizace dále předávány, a který by organizace měla vytvořit, udržovat a pravidelně přezkoumávat, ověřovat a v případě změny aktualizovat.

Pro udržování dohodnuté úrovně informační bezpečnosti a poskytováním služeb v souladu s dohodami s dodavateli má organizace zavést **proces monitorování, přezkoumávání a management změn** dodavatelských služeb za účelem:

- monitorování úrovně výkonu služeb a ověřování dodržování dohod,
- sledování změn dodavatelů (např. vylepšení stávající nabízených služeb, používání nových technologií, změny subdodavatelů),
- přezkoumání servisních zpráv a dokumentů od dodavatelů apod.,
- provádění auditů dodavatelů,
- přezkoumání auditních záznamů a důkazů o zabezpečení informací dle potřeby ochrany informací dodavatelů (např. certifikáty, atesty, interní audity).[130]

Nezbytnou součástí dodavatelských vztahů jsou platné **dohody o mlčenlivosti**, které jsou uzavírány, pokud jsou informace vyměňovány mimo organizaci a obsahují požadavky na mlčenlivost, které musí být splněny. Obvykle obsahují tyto dohody informace o typu dotčených informací, kterých se smlouva týká, předmět smlouvy, doby platnosti smlouvy, smluvní strany a jejích povinnosti.

Postupy pro stanovení požadavků na mlčenlivost a uzavírání dohody o mlčenlivost musí být stanoveny a pravidelně přezkoumávány. Zároveň musí být stanoveny postupy pro proces sledování doby platnosti dohod o mlčenlivosti, včetně procesu prodlužování platnosti v řádném termínu.[131]

Metodiku hodnocení dodavatelů si stanovuje organizace dle svých specifických potřeb. Je možné využít např. Fullerovu metodu, bodové hodnocení, prosté hodnocení dle pořadí, váhové hodnocení dle

[130] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[131] Tamtéž.

pořadí, prosté hodnocení podle hodnot, váhové hodnocení podle hodnot. Pravděpodobně již zavedená kritéria pro hodnocení dodavatelů stávajícím systémem managementu kvality je vhodné rozšířit o kritéria týkající se informační bezpečnosti.

Návrh metodiky hodnocení dodavatelů:

- Stanovení kritérií hodnocení a bodové škály jednotlivých kritérií.

TABULKA 6: BODOVÁ ŠKÁLA KRITÉRIÍ HODNOCENÍ DODAVATELŮ

Kritérium hodnocení	**Počet bodů**
Certifikát ISO/IEC 27001 v platné verzi nebo TISAX®	10
Žádný bezpečnostní incident	10
Dohoda o mlčenlivosti	10
Bezpečná elektronická komunikace	10

Zdroj: vlastní zpracování

- Ohodnocení všech kritérií konkrétního dodavatele počtem bodů z bodové škály.
- Zařazení dodavatele do kategorie dle celkově získaného počtu bodů.

TABULKA 7: KATEGORIZACE DODAVATELŮ

Počet dosažených bodů	**Kategorie**	**Popis**
40	A	Dodavatel je považován za vhodného ke spolupráci. Žádná další bezpečnostní opatření nejsou třeba.
30	B	Dodavatel je považován za vhodného ke spolupráci. Další bezpečnostní opatření jsou vhodná.
20	C	Dodavatel je považován za vhodného ke spolupráci za podmínky stanovení dalších bezpečnostních opatření.
10	D	Dodavatel je považován za nevhodného ke spolupráci.

Zdroj: vlastní zpracování

Pro stanovení celkové metodiky lze také využít základní metodiku řízení dodavatelů NÚKIB, která vychází z požadavků zákona o kybernetické bezpečnosti (ZKB) a vyhlášky o kybernetické bezpečnosti (VKB).[132]

[132] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Řízení dodavatelů*. Online. PDF. 06.09.2023, v. 1.0. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Metodika-rizeni-dodavatelu.pdf. [cit. 2024-03-30].

Návrh kritérií hodnocení produktů a služeb dodavatelů:

- schválení pouze pro konkrétní případ nebo použití
- shoda s požadavky na bezpečnost informací
- práva na používání SW a licencování
- reference na SW
- speciální určení (např. na údržbu).

3.2.4 Stanovení cílů

Cíle organizace jsou kontrolní body, kterých chce organizace dosáhnout. Ke správně stanoveným a dosažitelným cílům je vhodné využít metodu SMART. Akronym SMART vychází z následujících anglických pojmů:

- Specific (specifický) – cíl by měl být stanoven jasně, konkrétně a srozumitelně.
- Measurable (měřitelný) – cíl by mělo být možné změřit (např. stanovením a sledováním ukazatelů).
- Accepted (akceptovaný) – cíl by měl být stanoven v souladu s vlastním ztotožněním (ne proti své vůli).
- Realistic (realistický) – cíl by měl být dosažitelný.
- Timed (termínovaný) – cíl by měl být časově ohraničen (do kdy má být splněn).[133]

Cíle informační bezpečnosti patří mezi dokumentované informace a musí být v souladu s politikou informační bezpečnosti, musí být měřitelné, monitorované, komunikované, aktualizované dle potřeby a zohledňovat zavedené požadavky informační bezpečnosti a výsledky z analýzy rizik.[134]

Návrh cílů dle metody SMART:

- Snížit počet bezpečnostních incidentů na 2 za kalendářní rok.
- Získat známku TISAX® se stupněm hodnocení 2 v následujícím roce.

[133] ŠAFROVÁ DRÁŠILOVÁ, Alena. *Základy úspěšného podnikání: průvodce začínajícího podnikatele*. Praha: Grada, 2019. ISBN 978-80-271-2182-3.

[134] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27001:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Online. ČAS, ©2023. Dostupné z: https://sponzorpristup.agentura-cas.cz/zobrazit.aspx. [cit. 2024-03-30].

Cíle hodnocení TISAX® jsou navrženy buď na základě vlastního úsudku podle aspektů současných 12 platných cílů hodnocení nebo na základě konkrétního požadavku obchodního partnera nebo dle požadované úrovně hodnocení (AL 1, AL 2, AL 3, viz podrobněji kapitola 1.5.3.2 Hodnocení).[135]

Cíle hodnocení vybrané organizace byly stanoveny na základě požadavku obchodního partnera a jsou uvedeny v kapitole 3.1 Charakteristika vybrané organizace.

3.2.5 Stanovení organizační struktury pro bezpečnost informací

Organizační struktura pro bezpečnost informací by měla být stanovena na základě stanovených rolí a jím přiřazených odpovědností a pravomocí podle potřeb organizace. Zejména je třeba stanovit a přidělit odpovědnosti za ochranu informací, specifické procesy dotýkající se informační bezpečnosti, řízení rizik a všechny pracovníky využívající informací a dalších souvisejících aktiv. Osoby, kterým byla přidělena odpovědnost za informační bezpečnosti, můžou delegovat úkoly v oblasti bezpečnosti na ostatní, čímž ovšem nejsou zbaveni své odpovědnosti za správnost provedení postoupených úkolů. Tyto osoby musí splnit kompetentní požadavky na znalost a dovednosti, které daná role vyžaduje. Za celkovou informační bezpečnost v rámci organizace bývá zpravidla jmenován manažer pro informační bezpečnost. Kontaktní osoby musí být k dispozici v rámci celé organizace i příslušným obchodním partnerům.[136]

Doporučené role jsou:

- Vrcholové vedení organizace – s odpovědností za vize, strategická rozhodnutí a řízení organizace.
- Bezpečnostní tým – s odpovědností za nakládání s informačními aktivy a s vedoucí úlohou pro bezpečnost informací v organizaci a spojení mezi vrcholovým vedením organizace a týmem pro plánování bezpečnosti informací.
- Tým plánování bezpečnosti informací – s odpovědností za TISAX® při jeho implementaci a s úlohou koordinátora konfliktů napříč všemi odděleními organizace a vysokou úrovní znalostí o bezpečnosti.
- Specialisté a externí konzultanti – osoby s povinností širokých znalostí a zkušeností v oblasti IT. Externí specialisté mohou vnést vnější pohled na organizaci a poskytovat cenné rady, ale bez hlubokých znalostí o organizaci a jejím provozu.
- Vlastníci informačních aktiv – jmenované osoby pro každý proces organizace odpovědné za delegování úkolů a zacházení s informacemi v rámci přidělených procesů organizace.

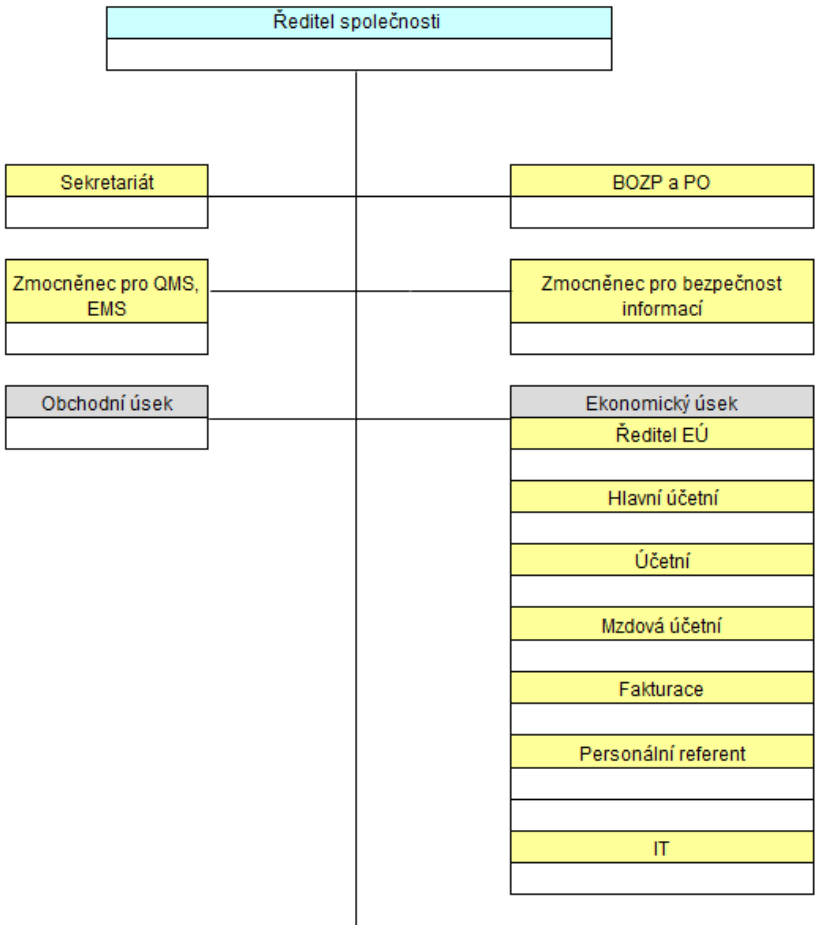
[135] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

[136] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

- Zainteresovaná strana – osoby nebo orgány jako např. zákazníci, dodavatelé, veřejné organizace (např. státní finanční správa, kontrolní správa).
- Manažer IT – osoba odpovědná za všechny zdroje IT (např. vedoucí IT oddělení).
- Fyzická bezpečnost – osoba odpovědná za fyzickou bezpečnost (např. správce zařízení, správce budov).
- Lidské zdroje – osoba odpovědná za všechny zaměstnance.
- Řízení rizik – osoba odpovědná za oblast řízení rizik, jejich vyhodnocování, zvládání a monitorování.
- Zaměstnanec / uživatel – každý zaměstnanec, který je odpovědný za udržování bezpečnosti informací v rámci svých pracovních činností.[137]

Návrh organizační struktury vedení organizace:

OBRÁZEK 13: ORGANIZAČNÍ SCHÉMA VEDENÍ ORGANIZACE



Zdroj: vlastní zpracování

[137] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2018. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

Další požadavky vysokých nároků na ochranu:

Za účelem snížení rizika podvodů a chyb, předejití střetu zájmů, případně obcházení opatření informační bezpečnosti by měly být odděleny **protichůdné povinnosti a protichůdné oblasti odpovědnosti**, aby jedna osoba nevykonávala sama potenciálně protichůdné povinnosti a nedocházelo ke střetu zájmů. Činnosti, které by mohly vyžadovat oddělení, jsou např. žádání o změnu a provádění změn, vyžadování a schvalování přístupových práv, používání a správa aplikací, provádění auditu a zavádění opatření informační bezpečnosti. Pokud by bylo obtížné role oddělit (např. v malých organizacích), je vhodné zvážit další opatření jako např. kontrolu činnosti nebo dohled vedení. Pokud má naopak organizace více rolí, je vhodné zvážit použití automatizovaného SW pro správu rolí a případnou detekci konfliktů, včetně odebrání nebo změny přidělení role.[138]

3.2.6 Vymezení rozsahu platnosti

Po stanovení externích a interních aspektů organizace relevantních pro její záměry a ovlivňujících její schopnost dosáhnout plánovaných výsledků ISMS musí organizace definovat zainteresované strany důležité pro ISMS a jejich požadavky (např. zákonné a regulatorní požadavky a smluvní závazky). Na základě toho musí organizace definovat hranice ISMS a stanovit jeho rozsah. Rozsah ISMS může pokrývat celou organizaci nebo pouze její části (útvary) a měl by zahrnovat všechny kritické oblasti organizace.[139] V rámci udržování ISMS jsou stanoveny monitorovací a kontrolní prostředky (např. přezkoumání managementu) a jeho účinnost je pravidelně přezkoumávána vedením.

Pro systém TISAX® je pak důležité stanovit přesně rozsah hodnocení TISAX®, do kterého spadají všechny části organizace, které nakládají s důvěrnými informacemi partnera. Ten může být odlišný od rozsahu ISMS, může být menší, ale musí odpovídat rozsahu ISMS. Je možné si vybrat ze dvou typů předem definovaných popisů rozsahu:

- standardní rozsah
- vlastní rozsah
  - vlastní rozšířený rozsah
  - úplný vlastní rozsah.

Naprostá většina účastníků TISAX® volí standardní předdefinovaný popis rozsahu, který není možné měnit. Aktuální platné znění popisu rozsahu verze 2.0 zní: *„Rozsah hodnocení TISAX® definuje rozsah*

[138] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[139] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2018. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

hodnocení. Hodnocení zahrnuje všechny procesy, postupy a zdroje spadající do okruhu odpovědnosti hodnocené organizace, které jsou relevantní k zabezpečení objektů ochrany a jejich cílů ochrany definovaných v uvedených cílech hodnocení na vyjmenovaných místech. Hodnocení se provádí alespoň v nejvyšší úrovni hodnocení uvedené v některém z uvedených cílů hodnocení. Hodnocení podléhají všechna kritéria hodnocení jmenovaná v uvedených cílech hodnocení."[140]

Dalším důležitým krokem při stanovení rozsahu je určení lokalit, které patří do rozsahu hodnocení. V případě malé organizace (jedné lokality) je stanoven jeden rozsah hodnocení. V případě velké organizace je možné stanovit více než jeden rozsah hodnocení. Výhodou jednoho rozsahu je jedna zpráva o hodnocení s jedním výsledkem hodnocení a jedním datem vypršení platnosti a snížení nákladů na hodnocení díky jednomu posouzení centrálních procesů, postupů a zdrojů poskytovatelem auditu. Nevýhodou jednoho rozsahu jsou stejné cíle hodnocení všech lokalit, dostupnost výsledku hodnocení až po posouzení všech lokalit poskytovatelem auditu a závislost všech lokalit na úspěšném hodnocení.

Stanovený rozsah může organizace změnit nejpozději do doby registrace na portálu ENX. V pozdějších fázích může rozsah hodnocení změnit pouze poskytovatel auditu, a to pouze do okamžiku uzavření hodnocení a nahrání výsledku hodnocení organizace na portál ENX.[141]

3.2.7 Stanovení politiky

Politika informační bezpečnosti musí být stanovena a schválena vedením organizace. Musí odpovídat cílům a potřebám organizace, včetně legislativních a smluvních požadavků, obsahovat krátkodobé i dlouhodobé cíle organizace v oblasti informační bezpečnosti a strategie k jejich dosažení, význam informační bezpečnosti v rámci organizace, závazek k dodržování relevantních požadavků týkajících se informační bezpečnosti a závazek ke kontinuálnímu zlepšování systému řízení informační bezpečnosti.

Politika musí být k dispozici jako dokumentovaná informace, sdělována v rámci organizace, v dostatečné míře dostupná i pro zainteresované strany a vzatá na vědomí. Musí být pravidelně a v případě významných změn přezkoumávána. Může být vypracována jedna politika nebo může být vypracována celková politika a několik podřízených politik, které jsou upraveny např. dle odlišných oblastí provozování organizace a můžou být na sobě nezávislé nebo můžou mít hierarchický vztah. [142]

---

[140] ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

[141] Tamtéž.

[142] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

Dále můžou být stanoveny např. následující specifické politiky na nižší úrovni:

- Politika klasifikace informací.
- Politika řízení přístupu.
- Politika zálohování.
- Politika výměny informací mezi organizacemi.
- Politika týkající se uživatelských účtů a přihlašovacích údajů (např. politika hesel).
- Politika práce na dálku.
- Politika ochrany dat a soukromí.
- Politika použití kryptografických opatření.
- Politika zálohování.
- Politika týkající se mobilních výpočetních zařízení a sdělovací techniky.

V případě změny jedné politiky je vhodné přezkoumat a případně aktualizovat i další související politiky. Politika, případně politiky by měly být vhodnou formou zpřístupněny zaměstnancům (např. na intranetu). O jakýchkoliv změnách, které se zainteresovaných stran týkají, by měli být informováni zaměstnanci i externí obchodní partneři.

Politika klasifikace informací je jedním ze základních preventivních organizačních opatření, ve které jsou informace klasifikovány podle potřeb organizace na základě důvěrnosti, integrity, dostupnosti a na základě požadavků příslušných zainteresovaných stran. Klasifikaci informací je možné založit na úrovni dopadu, jaký by znamenal pro organizaci v případě jejich poškození. Příkladem můžou být čtyři úrovně dopadu v případě zveřejnění informací: nezpůsobuje žádnou újmu, způsobuje malou újmu (např. poškození pověsti), má významný dopad na provoz nebo cíle v krátkodobém horizontu, má vážný dopad na cíle v dlouhodobém horizontu nebo ohrožuje chod organizace.[143]

3.2.8 Stanovení opatření

V návaznosti na stanovený kontext organizace musí organizace stanovit rizika a příležitosti a následně plánovat příslušná opatření orientovaná na rizika a příležitosti, způsob jejich implementace do systému managementu informační bezpečnosti a způsob hodnocení efektivnosti těchto opatření.[144]

[143] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[144] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27001:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Online. ČAS, ©2023. Dostupné z: https://sponzorpristup.agentura-cas.cz/zobrazit.aspx. [cit. 2024-03-30].

Proces posouzení rizika informační bezpečnosti musí organizace uchovávat v podobě dokumentovaných informací a musí ho definovat a aplikovat tak, aby:

- určil a dodržoval kritéria rizika informační bezpečnosti, a to kritéria akceptace rizik a kritéria pro samotné posouzení rizika,
- zajistil konzistentnost, platnost a porovnatelnost výsledků při opakovaném posouzení rizik informační bezpečnosti,
- identifikoval rizika informační bezpečnosti prostřednictvím procesu posouzení rizik informační bezpečnosti, aby odhalil rizika, která jsou spojena se ztrátou důvěrnosti, integrity a dostupnosti informací, a aby identifikovat vlastníky rizik,
- analyzoval rizika informační bezpečnosti posouzením potenciálních následků reálné pravděpodobnosti rizik a určením úrovně rizik,
- hodnotil rizika informační bezpečnosti porovnáváním výsledků analýzy rizik s kritérii rizik a stanovením priority analyzovaných rizik.[145]

Opatření představují kroky, které upravují nebo zachovávají riziko. Opatření musí být definována, zavedena, monitorována, přezkoumávána a případně zlepšována tak, aby organizace dosáhla splnění svých specifických cílů bezpečnosti. Při jejich stanovování musí být zohledněny také všechny příslušné národní a mezinárodní právní předpisy a nařízení. Měly by být vyvážené vynaložené prostředky na zavedení opatření a potenciální dopad bezpečnostních incidentů na činnosti organizace v případě nestanovení opatření.[146]

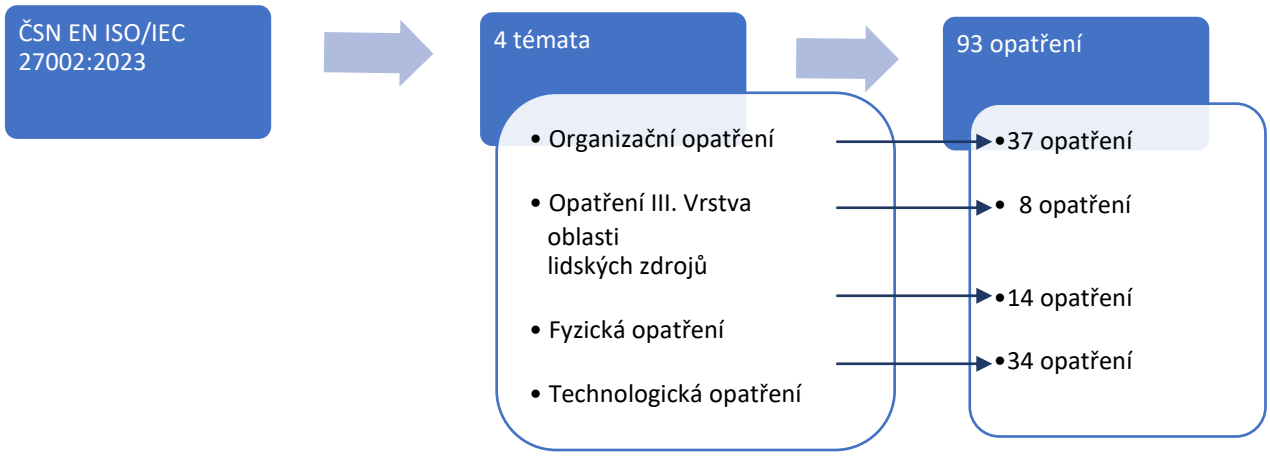
Pro účely implementace TISAX® je možno vycházet z normy ČSN ISO/IEC 27002:2022 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti. Norma dělí opatření na organizační opatření, opatření v oblasti lidských zdrojů, opatření fyzické bezpečnosti a technologická opatření.[147]

[145] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27001:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Online. ČAS, ©2023. Dostupné z: https://sponzorpristup.agentura-cas.cz/zobrazit.aspx. [cit. 2024-03-30].

[146] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[147] Tamtéž.

OBRÁZEK 14: STRUKTURA OPATŘENÍ DLE ISO/IEC 27002:2023



Zdroj: vlastní zpracování

Mezi organizační opatření patří např.:

- Politiky pro informační bezpečnost (viz podrobněji bod 2.2.7 Stanovení politiky).
- Role a odpovědnosti v oblasti informační bezpečnosti.
- Odpovědnosti vedení.
- Kontakt s autoritami.
- Kontakt se zvláštními zájmovými skupinami.
- Zpravodajství o hrozbách.
- Informační bezpečnost v řízení projektů.
- Klasifikace informací.
- Řízení přístupu.
- Přístupová práva.
- Informační bezpečnost ve vztazích s dodavateli.

Mezi opatření v oblasti lidských zdrojů patří např.:

- Povědomí, vzdělávání a školení o informační bezpečnosti.
- Dohody o důvěrnosti nebo mlčenlivosti.
- Práce na dálku.[148]

[148] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

Mezi opatření fyzické bezpečnosti patří např.:

- Fyzický vstup.
- Zabezpečení kanceláří, místností a vybavení.
- Monitorování fyzické bezpečnosti.
- Prázdný stůl a prázdná obrazovka.
- Paměťová média.
- Bezpečnost kabelových rozvodů.
- Údržba zařízení.

Mezi technologická opatření patří např.:

- Koncová zařízení uživatele.
- Privilegovaná přístupová práva.
- Omezení přístupu k informacím.
- Bezpečná autentizace.
- Ochrana před škodlivým softwarem.
- Vymazání informací.
- Prevence úniku dat.
- Zálohování informací používání kryptografie.[149]

Jedním z atributů opatření dle ČSN ISO/IEC 27002:2023 je jeho typ:

- **preventivní opatření** – zavedené preventivní opatření zabraňuje vzniku bezpečnostního incidentu, je stanoveno na základě analýzy rizik,
- **detekční opatření** – opatření, které je zavedeno okamžitě při vzniku bezpečnostního incidentu,
- **nápravné opatření** – nápravné opatření, které je stanoveno po vzniku bezpečnostního incidentu[150], podrobněji je popsáno v kapitole 2.2.12 Interní hodnocení a testování.

3.2.9 Zpracování směrnic a pracovních postupů

Na základě stanovené organizační struktury pro bezpečnost informací, vymezeného rozsahu platnosti TISAX®, stanovené politiky, hodnocení rizik a stanovení opatření by měly být vypracovány směrnice a postupy bezpečnosti informací, které se týkají buď celé organizace nebo jejích konkrétních částí. Na jejich vypracování by se měli podílet zástupci různých částí organizace, kterých se rozsah TISAX® týká

[149] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[150] Tamtéž.

a mají k tomu pravomoci. Můžou to být např. manažeři bezpečnosti informací, manažeři pro fyzickou bezpečnost, manažeři pro technologickou bezpečnost.[151]

Směrnice a postupy můžou být vypracovány jako zcela nové nebo můžou být upřesněny či rozšířeny stávající směrnice a postupy. Mělo by z nich být zcela jasné, jakou oblast z rozsahu platnosti pokrývají.[152]

Směrnice a postupy jsou typem dokumentované informace. Pro jejich vytváření a aktualizaci musí organizace stanovit způsob identifikace a popis (např. název, datum, autor, číslo revize), formát (např. jazykové provedení) a média (např. elektronicky, v papírové podobě) a přezkoumání a schválení vhodnosti a přiměřenosti. Dokumentované informace musí být řízeny, tzn. musí být zajištěna jejich dostupnost kdekoliv a kdykoli v případě potřeby a jejich přiměřená ochrana (např. před nevhodným použitím nebo ztrátou integrity). Je třeba stanovit jejich způsob:

- distribuce, přístupu, vyhledávání a používání,
- ukládání,
- řízení změn (např. verzování),
- uchovávání,
- likvidace.

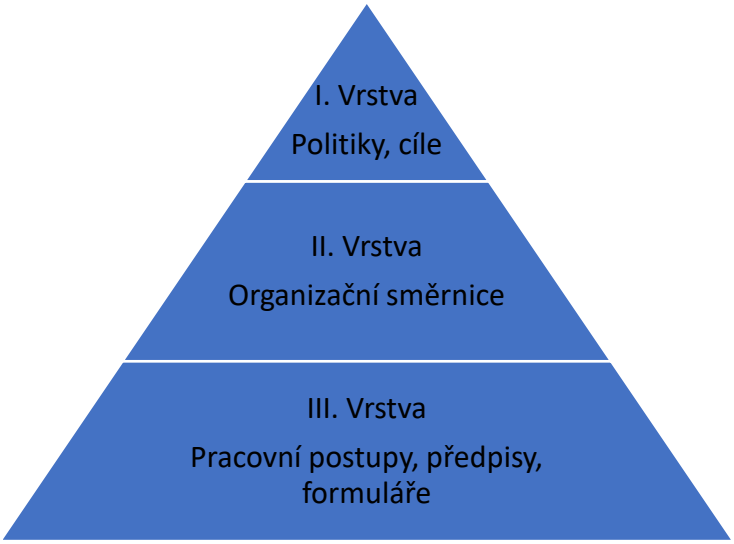
Je doporučeno vést směrnice a postupy v elektronické podobě a umístit je na centrální úložiště, např. intranet, aby byly dostupné všem zaměstnancům v jakémkoliv okamžiku a v nejnovější verzi. Je třeba, aby se zaměstnanci zavázali k dodržování směrnic a postupů. V případě potřeby přístupu externími organizacemi, např. obchodními partnery, je třeba zvážit potřebu smluvních ujednání. Také zaměstnanci zpracovávající osobní údaje jsou povinni zachovávat mlčenlivost (a to i po skončení pracovního poměru) a dodržovat platné zákony ochranu osobních údajů a tento závazek musí být zdokumentován.

[151] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[152] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2018. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

Návrh struktury dokumentace:

OBRÁZEK 15: NÁVRH STRUKTURY INTERNÍ DOKUMENTACE



Zdroj: vlastní zpracování

3.2.10 Školení

Organizace musí zajistit, aby zaměstnanci organizace i příslušné zainteresované strany získali povědomí, vzdělávání a školení o informační bezpečnosti a systému TISAX® a byli si vědomi svých odpovědností v oblasti informační bezpečnosti.

Na základě politiky informační bezpečnosti, příp. dalších specifických politik, a příslušných postupů v oblasti informační bezpečnosti by měla organizace sestavit program zvyšování povědomí, vzdělávání a školení o informační bezpečnosti. Zvyšování povědomí, vzdělávání a školení by měla organizace provádět pravidelně a týká se i nových pracovníků a pracovníků na nových pozicích.

Program na zvyšování povědomí o informační bezpečnosti zahrnuje seznámení pracovníků s jejich odpovědností za informační bezpečnost a prostředky jejího plnění. Je schvalován odpovědnými vedoucími pracovníky. Týká se interních i externích pracovníků (např. konzultantů, pracovníků dodavatele), je realizován pravidelně a vychází z incidentů informační bezpečnosti, se kterými má již organizace zkušenosti. Jsou k němu využívány vhodné fyzické nebo virtuální kanály, jako např. kampaně, brožury, plakáty, webové stránky, e-maily a další.[153]

[153] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

Plán vzdělávání a školení je určen pro technické specialisty se specifickými dovednostmi a odbornými znalostmi, aby mohli konfigurovat a udržovat požadované úrovně bezpečnosti zařízení, systémů, aplikací a služeb. Může mít např. formu samostudia nebo přednášek od odborných pracovníků nebo konzultantů a probíhat fyzicky nebo online.

Předmětem školení zaměstnanců by měla být např. politika bezpečnosti informací, hlášení incidentů bezpečnosti informací, politiky týkající se přístupových údajů a uživatelských účtů, postupy pro zachování mlčenlivosti apod.

Pro výběr potenciálních zaměstnanců a zajištění způsobilosti a vhodnosti pro příslušnou roli by měly být stanoveny požadavky na zaměstnance a jejich odbornou způsobilost a měla by být zavedena opatření z oblasti lidských zdrojů, která se týkají prověřování, podmínek pracovního poměru, povědomí, vzdělávání a školení o informační bezpečnosti, odpovědností po ukončení nebo změně pracovního poměru, dohod o důvěrnosti nebo mlčenlivosti, příp. práce na dálku.

Prověřování způsobilosti potenciálních zaměstnanců by mělo zahrnovat např. ověření předchozích referencí, ověření identity, kontrolu diplomů a certifikátů k potvrzení kvalifikace, příp. podrobnější ověření, např. bezúhonnost nebo bezdlužnost v případě požadavků na kritickou roli.

Součástí pracovních smluv by měly být dohody o důvěrnosti nebo mlčenlivosti, zákonné povinnosti (např. právní předpisy o ochraně dat), odpovědnost za klasifikaci informací a nakládání s informacemi od zainteresovaných stran, povinnost dodržování zásad bezpečnosti informací, včetně postupu řešení při porušení této povinnosti a také odpovědnosti a povinnosti platné i po ukončení nebo změně pracovního poměru, např. důvěrnost informací, duševní vlastností nebo jiné získané znalosti.[154]

3.2.11 Zavedení bezpečnostních opatření

Kromě opatření zavedených v rámci bodů implementace 3.2.1 – 3.2.10 je třeba implementovat také další preventivní bezpečnostní opatření z oblasti informační bezpečnosti, ochrany prototypu a ochrany dat podle stanoveného cíle hodnocení.

[154] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

3.2.11.1 Kritéria informační bezpečnosti

Aby byla efektivně řešena rizika informační bezpečnosti související s projekty, musí být informační bezpečnost integrována do **řízení projektů**. Měly by být stanoveny postupy a kritéria pro klasifikaci projektů. Hodnocení rizik by mělo být prováděno jak na začátku projektu, tak v případě jeho změn. Na základě identifikovaných rizik by měla být stanovena opatření.

Další požadavky vysokých nároků na ochranu (pro „C“, „I“, „A“):

- Stanovená opatření na základě identifikovaných rizik by měla být pravidelně revidována a přehodnocována v případě změn kritérií hodnocení.[155]

Důležitost informací z hlediska informační bezpečnosti musí být určena v rámci **evidence informací a dalších souvisejících aktiv**. Musí být zpracován a udržován seznam informací a dalších souvisejících aktiv, včetně jejich vlastníků, aby byla zachována jejich informační bezpečnost.

Musí být stanoveny a splněny požadavky na **přípustné používání podpůrných aktiv** (např. na přepravu, skladování, opravu, požadavky pro případ ztráty, vrácení nebo likvidaci), včetně mobilních IT zařízení a mobilních datových úložišť, u kterých musí být zohledněno např. šifrování, ochrana přístupu pomocí PIN nebo hesla, označení.[156]

Další požadavky vysokých nároků na ochranu (pouze pro „C“):

- Ochrana podpůrných aktiv.
- Likvidace podpůrných aktiv v souladu s jednou z příslušných norem (např. ISO 21964, min. 4. stupeň zabezpečení).
- Obecné šifrování mobilních datových úložišť nebo na nich uložených informačních aktiv (platí pro „C“, „I“).[157]

V souvislosti s klasifikací informací by měly být stanoveny postupy pro **označování informací**, týkající se nejen informací, ale i dalších souvisejících aktiv. Označování může být prováděno pomocí fyzického označení, uvedením záhlaví a zápatí, metadaty, použitím vodoznaků nebo razítek. Používání metadat napomáhá účinnému a správnému vyhledávání informací. S postupy označování informací by měli být

[155] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[156] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[157] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

seznámeni jak zaměstnanci, tak další zainteresované strany. Zaměstnancům by měla organizace zajistit nezbytné školení, týkající se postupů označování, aby bylo označování prováděno správně.[158]

Aby byla zajištěna bezpečnost předávaných informací jak v rámci organizace, tak s externími zainteresovanými stranami, měla by být vytvořena a všem relevantním zainteresovaným stranám zpřístupněna politika **předávání informací**, která zahrnuje pravidla, postupy a dohody pro předávání těchto informací v souladu s jejich klasifikací. V případě předávání informací mezi organizací a třetími strany musí být uzavírány a udržovány dohody o předávání informací za účelem jejich ochrany. Mezi základní způsoby předávání informací patří:

- **Elektronické předávání informací.**

  Pro elektronické předávání informací musí pravidla, postupy a dohody zahrnovat např. odhalování škodlivého SW elektronickou komunikací a způsoby ochrany proti němu, ochranu elektronických informací ve formě příloh, zabránění odesílání dokumentů a zpráv na nesprávnou adresu nebo číslo, vyžadování souhlasu se zasíláním rychlých zpráv, využíváním sociálních sítí, sdílením souborů nebo využíváním cloudových úložišť, omezení přístupu k elektronické komunikaci (např. zabránění automatického přeposílání elektronické komunikace na externí e-maily), zdůraznění zákazu zaměstnancům a dalším zainteresovaným stranám týkajícího se posílání krátkých textových zpráv (SMS) s citlivými informacemi, aby nebyly zpřístupněny na veřejných místech nebo zařízeních, kde nejsou dostatečně ochráněné. Pro elektronickou výměnu dat by mělo být použito šifrování dle příslušné klasifikace.[159]

  <u>Další požadavky vysokých nároků na ochranu (pouze pro „C“):</u>

  - Přenášet informace v zašifrované podobě, příp. jinými podobně účinnými opatřeními.

  <u>Další požadavky velmi vysokých nároků na ochranu (pouze pro „C“):</u>

  - Přenášet informace v obsahově zašifrované podobě, příp. jinými podobně účinnými opatřeními.[160]

[158] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[159] Tamtéž.

[160] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

- **Předávání informací na fyzických paměťových médiích (včetně papírových).**

  Pro předávání informací na fyzických paměťových médiích musí pravidla, postupy a dohody zahrnovat např. odpovědnost za předávání, odesílání a přijímání, správné adresování a přepravu, balení, které ochrání obsah před fyzickým poškozením při přepravě a které odpovídá specifikaci výrobců (např. chrání proti teplu, vlhkosti nebo elektromagnetickým polím), správu spolehlivých poskytovatelů přepravních nebo kurýrních služeb (včetně vedení seznamu organizací, kurýrů, postupu ověřování jejich totožnosti a vedení záznamů o přepravě a použité ochraně obsahu).[161]

- **Verbální předávání informací.**

  V souvislosti s důrazem na ochranu informací je třeba pro verbální předávání informací prostřednictvím pravidel, postupů a dohod upozornit zaměstnance a další zainteresované strany, aby se zdrželi vedení důvěrných verbálních rozhovorů na veřejnosti nebo prostřednictvím nezabezpečených komunikačních kanálů, aby nedošlo k jejich odposlechu, aby nezanechávali zprávy na záznamnících nebo hlasové zprávy, aby nedošlo k přehrání neoprávněnými osobami, aby byla ve jednacích místnostech zavedená vhodná opatření (např. zvukotěsné dveře nebo alespoň zavřené dveře) a aby uváděli na začátku citlivých rozhovorů úroveň klasifikace nadcházejících informací a dovolený způsob zacházení s nimi.[162]

Při **využívání externích IT služeb** musí organizace stanovit svoje požadavky v oblasti bezpečnosti informací a následně posoudit, zda je poskytovatel externích IT služeb splňuje. Posouzení probíhá zpravidla na základě informací od poskytovatelů externích IT služeb ohledně schopností v oblasti bezpečnosti informací a na základě posouzení rizik. Musí být vzaty v úvahu také právní, regulační a smluvní požadavky, včetně uzavření dohody o zachování mlčenlivosti. Využívání externích IT služeb by mělo být formou dokumentované informace, schváleno a následně by mělo být pravidelně ověřováno, zda jsou využívány pouze schválené externí IT služby. Měly by být stanoveny požadavky na pořízení, uvedení do provozu a schválení externích IT služeb.[163]

Řízení přístupu je typem preventivního opatření, které má zajistit oprávněný přístup a zamezit neoprávněnému přístupu k informacím, příp. dalším souvisejícím aktivům. Měla by být stanovena a zavedena pravidla pro fyzický a logický přístup k nim tak, aby respektovala požadavky vyplývající z činnosti organizace a požadavků na informační bezpečnost. Měla by zohledňovat např. identifikaci

[161] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[162] Tamtéž.

[163] Tamtéž.

entit, které vyžadují přístup k informacím a dalším souvisejícím aktivům a v jakém rozsahu, konkretizování fyzického přístupu a k tomu vhodných opatření, sdělování a autorizování informací (např. zásada nezbytně nutného rozsahu, kdy má entita povolený přístup pouze k informacím potřebných k plnění svých úkolů, nebo potřeba použití, kdy má entita povolený přístup k infrastruktuře informačních technologií pouze v případě jednoznačné potřeby), jejich klasifikaci a úroveň informační bezpečnosti. Dále musí zahrnovat správu **přístupových práv** (žádosti o přístup, oddělení funkcí pro žádosti o přístup, autorizaci přístupu, správy přístupu) nebo právní předpisy a nařízení a smluvní závazky, které se týkají omezení přístupu k datům nebo službám. Pro stanovení pravidel řízení přístupu je vhodné vycházet z předpokladu nejmenšího oprávnění, tj. „Vše je obecně zakázáno, pokud to není výslovně povoleno." Není doporučován předpoklad slabšího pravidla: „Vše je obecně povoleno, pokud to není výslovně zakázáno." Pro zavedení řízení přístupu je možné využít několik způsobů, např. „MAC (povinné řízení přístupu), DAC (volitelné řízení přístupu), RBAC (řízení přístupu založené na rolích) a ABAC (řízení přístup založené na atributech)".[164] Přístupová práva můžou být poskytnuta na omezenou dobu a odebírána, pokud již přístup není potřeba. Musí být pravidelně kontrolována, a to i ve vztahu k IT systémům zákazníků.

Ke kontrole přístupu je možné využít různé **identifikační prostředky** jako např. klíče, vizuální ID, kryptografické tokeny, pro které musí být stanoveny postupy pro zacházení s nimi v průběhu celého životního cyklu (od vytvoření, předání, oboru platnosti, vrácení, zničení nebo v případě ztráty).[165]

Další požadavky vysokých nároků na ochranu (pro „C", „I" i „A"):

- Omezit platnost identifikačních prostředků na přiměřenou dobu.
- Stanovit možnosti blokace nebo znehodnocení, pokud dojde ke ztrátě.[166]

V rámci **managementu identit** jsou identity (tzv. uživatelské účty) přiřazovány pouze jedné zodpovědné osobě. Sdílené identity (tzv. kolektivní účty) jsou přiřazovány pouze v nezbytných, regulovaných případech. Musí být včas deaktivovány, pokud nejsou potřebné (nejsou používány, osoby spojené s identitou nepracují v organizaci nebo změnily roli).

[164] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[165] Tamtéž.

[166] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

Autentizační informace je typem preventivního opatření, které na základě procesu přidělování a managementu autentizačních informací zajistí správnou autentizaci entity a zabrání selhání autentizačních procesů. Postupy pro autentizaci uživatelů jsou definovány na základě analýzy rizik.[167]

- Proces přidělování a managementu by měl zajistit neodhadnutelnost dočasných tajných autentizačních informací při automatickém generování osobních hesel nebo osobních identifikačních čísel (PIN) během procesů registrace a povinnost jejich změny po prvním použití, zavedení postupů pro ověření totožnosti uživatele, pokud mu mají být poskytnuty nové, náhradní nebo dočasné autentizační informace, předání autentizačních informací uživatelům bezpečným způsobem (např. přes ověřený a chráněný kanál a ne přes e-mail), potvrzení přijetí autentizačních informací od uživatelů, vedení záznamů o přidělování a managementu autentizačních informací schváleným způsobem (např. nástrojem pro úschovu hesel), aby byla zajištěna jejich důvěrnost. Je vhodné zvážit poskytnutí jednotného přihlášení (SSO) nebo např. trezoru hesel pro snížení množství autentizačních informací, které by si uživatelé museli zapisovat a chránit. Opačným efektem však může být vyšší pravděpodobnost prozrazení těchto autentizačních informací.

- Mezi odpovědnosti uživatele neboli osoby s přístupem k autentizačním informacím patří povinnost uchovávání tajných autentizačních informací (např. hesel) v tajnosti a nesdílení osobních tajných autentizačních informací s dalšími osobami, používání silných hesel podle doporučení osvědčených postupů, aby je nemohl někdo jiný lehce uhodnout (např. jméno, telefonní číslo nebo datum narození) a aby neobsahovala slova ze slovníku, ale obsahovala lehce zapamatovatelné fráze, které obsahují alfanumerické znaky a speciální znaky, a dála aby měla minimální délku a nebyla používána stejná hesla pro různé služby a systémy. Dodržování těchto pravidel by mělo být zahrnuto v pracovním řádu.

- V případě používání hesel jako autentizační informace by měl systém řízení hesel umožnit zvolení vlastních hesel a jejich změnu, vyžadovat silná hesla a jejich změnu v případě potřeby (např. po bezpečnostním incidentu nebo ukončení či změně zaměstnání), zabraňovat použití stejných hesel opakovaně, neumožnit zobrazování hesel na obrazovce při jejich zadávání, zajistit způsob ukládání a přenášení hesel v chráněné podobě.

- Mezi další typy autentizačních informací patří kryptografické klíče, což jsou data uložená na hardwarových tokenech (např. čipových kartách), které vytváří autentizační kódy a biometrická

[167] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

data (např. sken oční duhovky nebo otisky prstů). Při zavádění kryptografických postupů (např. šifrovacích, podpisových algoritmů) by měly být zohledněny předpisy a národní omezení týkající se kryptografických opatření. Je vhodné zavést management klíčů, prostřednictvím kterého jsou generovány, distribuovány, ukládány, archivovány, deaktivovány, měněny či aktualizovány a mazány klíče pro kryptografické systémy. Zváženy by měly být kryptografické postupy, sada klíčů a nouzový proces pro obnovu klíčového materiálu.[168]

Další požadavky vysokých nároků na ochranu (pro „C“, „I“, „A“):

- Rozšíření autentizačních postupů a kontrol přístupů o doplňková opatření jako např. nepřetržité monitorování přístupu, automatické odhlášení při nečinnosti.

Další požadavky vysokých nároků na ochranu (pro „C“, „I“):

- Stanovit a splnit klíčové požadavky na suverenitu (zejména v případě externího zpracování).

Další požadavky velmi vysokých nároků na ochranu (pro „C“, „I“):

- Autentizace uživatelů pomocí silné autentizace před přístupem k informacím s velmi vysokými nároky na ochranu (např. dvoufaktorová autentizace).[169]

Plánování a příprava managementu incidentů informační bezpečnosti zajistí, že bezpečnostní incidenty informační bezpečnosti budou mít rychlou a efektivní odezvu, včetně komunikace o událostech informační bezpečnosti. K tomu by měla organizace definovat role a odpovědnosti, stanovit postupy managementu incidentů a definovat postupy podávání zpráv. Organizace musí:

- Definovat pojem bezpečnostního incidentu a pozorování v souvislosti s personálem (např. nevhodné chování), fyzickou bezpečností (např. krádež, neoprávněný přístup), IT službami (např. IT útoky) a v souvislosti s dodavateli a dalšími obchodními partnery (jakékoliv incidenty s možným negativním dopadem na bezpečnost organizace).
- Stanovit kontaktní místo pro hlášení incidentů.
- Stanovit způsob hlášení bezpečnostních incidentů.
- Stanovit postup managementu incidentů zahrnující správu incidentů (dokumentování, odhalování, třídění, kategorizování, klasifikaci, upřednostňování, vyhodnocování dle kritérií informační

[168] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[169] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

bezpečnosti, komunikaci se zainteresovanými stranami) a včasnou odezvu na ně, včetně zohlednění externích požadavků na podávání zpráv o incidentech, např. regulatorním orgánům.

- Definovat a přiřadit odpovědnosti za zpracovávání bezpečnostních incidentů dle jejich kategorie, včetně podávání oficiálních zpráv.
- Analyzovat příčiny bezpečnostních incidentů a získané zkušenosti integrovat do procesů neustálého zlepšování.
- Stanovit proces školení, certifikace nebo odborného rozvoje zaměstnanců, kteří jsou povinni hlásit příslušné bezpečnostní incidenty.
- Definovat přijímaná opatření v případě vzniku bezpečnostní události (např. okamžité podání zprávy kontaktnímu místu, včetně záznamu podrobností).
- Určit způsob záznamu zpráv o incidentech (např. na formulářích).
- Definovat proces zpětné vazby o výsledcích vyřešení bezpečnostních incidentů.
- Plánovat udržení informační bezpečnosti na odpovídající úrovni během narušení (např. v případě přírodní katastrofy, fyzického útoku, pandemie, kybernetického útoku) zavedením opatření informační bezpečnosti a zavést pravidelně přezkoumávaný a aktualizovaný systém krizového řízení (např. mít dostatečné zdroje, přidělené odpovědnosti a pravomoci pro krizové řízení).

Organizace by měla v rámci řešení krizových situací:

- Stanovit metody k odhalování krizových situací.
- Identifikovat hrozící krizové situace.
- Zavést postupy pro vyvolání a/nebo eskalaci krizového řízení.
- Definovat strategické cíle a jejich prioritu při krizových situacích, např. etické priority (ochranu života a zdraví), priority obchodních procesů zajišťující chod organizace.[170]

<u>Další požadavky vysokých nároků na ochranu (pro „C“, „I“, „A“):</u>

- Stanovit maximální dobu odezvy podle kategorizace, klasifikace stanovení závažnosti, včetně podmínek eskalace v případě jejího nedodržení a průběhu eskalace až k nejvyššímu vedení organizace.
- Obeznámit zainteresované strany se zákonnými, regulačními a smluvními požadavky a kontaktními údaji.

[170] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

- Stanovit komunikační strategii, včetně určení, komu komunikovat (např. akcionářům, obchodním partnerům, zákazníkům, veřejnosti), kdy komunikovat, co komunikovat, jak komunikovat (např. jakými komunikačními kanály).
- Stanovit postupy pro odezvu na bezpečnostní incidenty dodavatelů, včetně dopadu na organizaci, vyvolání interních reakcí nebo reportingu.[171]

V případě umožňování **práce na dálku** je třeba definovat požadavky na ochranu informací, se kterými je nakládáno mimo prostory organizace, a to jak v tištěné nebo elektronické podobě prostřednictvím ICT. Může se jednat jak o práci z domova nebo jiného pracoviště, práci ve virtuálním pracovním prostředí nebo o vzdálenou údržbu. Bezpečnostní opatření by měla zohlednit:

- bezpečnostní principy fyzického prostředí, jako např. uzamykatelné skříňky, bezpečnou přepravu mezi jednotlivými místy,
- neoprávněný přístup k informacím ze strany jiných osob (např. v rodině nebo na veřejných místech),
- zavedení firewallů a jiných ochran před škodlivým softwarem,
- používání vzdáleného přístupu,
- používání bezpečných a silných autentizací.[172]

Další požadavky vysokých nároků na ochranu (pouze pro „C“):

- Zavedení ochranných opatření proti odposlechu a sledování.[173]

Fyzická bezpečnost

Z hlediska fyzické bezpečnosti musí být definovány **bezpečnostní zóny** pro ochranu oblastí s výskytem informací a dalších souvisejících aktiv. Stanoveny musí být ochranné vnitřní podmínky, např. pevné konstrukce stěn či podlah, dále celkové podmínky budov, např. bezpečnostní dveře, mříže, zámky, alarmy, pravidla pro uzavírání oken a dveří v případě nepřítomnosti a měl by být zajištěn vhodný

[171] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[172] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[173] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

poplachový systém a protipožární opatření (např. protipožární dveře). Je stanoven kodex chování v bezpečnostních zónách a je znám všem zainteresovaným stranám.[174]

Fyzický přístup do bezpečnostních zón by měl být umožněn pouze na základě autorizace. Měly by být stanoveny postupy pro:

- přidělování a odebírání přístupových práv,
- způsoby autentizace (např. biometrické nebo dvoufaktorové, přístupovými kartami, tajnými kódy),
- zabezpečení nouzových východů před neoprávněným přístupem,
- používání mobilních IT zařízení a zařízení pro ukládání dat a jejich přenášení,
- správu návštěvníků (včetně např. provádění záznamů o příchodech a odchodech návštěvníků a jejich dohledu),
- ukládání a zpracovávání informačních aktiv (např. sklady, dílny, garáže, testovací dráhy, centra zpracování dat).[175]

Další požadavky vysokých nároků na ochranu:

- Zavedení ochranných opatření proti odposlechu a sledování.[176]

Technologická bezpečnost

Pro zachování informační bezpečnosti při změnách v organizaci, obchodních procesech nebo IT systémech musí být zavedeny postupy pro **management změn**. Postupy by měly zahrnovat:

- schvalovací proces změn,
- plánování, vyhodnocování změn z hlediska jejich potenciálního dopadu na bezpečnost informací,
- testování v případě změn, které ovlivňují bezpečnost informací,
- zvažování nouzových situací v případě závad.[177]

[174] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

[175] Tamtéž.

[176] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[177] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

Další požadavky vysokých nároků na ochranu:

- Ověřování shody s požadavky na bezpečnost informací při změnách a po jejich zavedení.[178]

Musí být zajištěno **oddělení prostředí vývoje a testování od provozního prostředí** pro zachování dostupnosti, důvěrnosti a integrity produktivních dat. Na základě hodnocení rizik musí být IT systémy rozděleny na vývojové, testovací a provozní a implementována jejich segmentace. Měla by být stanovena a implementována pravidla pro vývojová a testovací prostředí, která zohledňují:

- oddělení vývojových testovacích a provozních systémů,
- nepoužívání vývojových a systémových nástrojů na operačních systémech (s výjimkou těch nutných pro provoz),
- používání různých uživatelských profilů pro vývoj, testování a operační systémy.[179]

Pomocí definovaných technických a organizačních opatření je třeba zajistit **ochranu IT před malwarem**. Stanovené postupy by měly zahrnovat:

- zakázání nepotřebných síťových služeb a jejich zpřístupnění pouze omezeně za pomoci vhodných ochranných opatření,
- pravidelnou instalaci a automatickou aktualizaci softwaru na ochranu před malwarem,
- automatickou kontrolu přijatých souborů a software před spuštěním na přítomnost malwaru,
- pravidelnou kontrolu dat všech systémů na přítomnost malwaru,
- automatickou kontrolu dat přenášených centrálními bránami pomocí ochranného softwaru (např. e-mail, internet, sítě třetích stran),
- zvážení šifrovaných spojení,
- definování a implementaci opatření proti deaktivaci nebo změně ochranného softwaru uživateli,
- opatření pro informovanost zaměstnanců o vzniklém případu,
- implementaci alternativních opatření na ochranu před malwarem pro IT systémy, které jsou provozované bez použití softwaru.[180]

Události (činnosti, výjimky, poruchy apod.) musí být **zaznamenávány formou logů** (protokolů), aby mohly být identifikovány události informační bezpečnosti a vytvářely důkazy pro případy vyšetřování incidentů informační bezpečnosti. Je třeba stanovit:

- požadavky na zaznamenávání událostí formou logů,

[178] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].
[179] Tamtéž.
[180] Tamtéž.

- logování systémových administrátorů a uživatelů,
- posuzování IT systémů z hlediska nutnosti logování,
- vyžadování informací o možnosti monitorování logování při využití externích IT systémů a jejich zohledňování v hodnocení,
- pravidelnou kontrolu logů s ohledem na porušení pravidel a nesoulad s právními a organizačními předpisy.

Měl by být stanoven postup eskalace relevantních událostí odpovědnému orgánu, zaznamenávání a monitorování všech akcí v síti, které jsou relevantní pro bezpečnost informací. Logy událostí by měly být chráněny proti změnám.

Další požadavky vysokých nároků na ochranu (pro „C“, „I“, „A“):

- Stanovení a implementování požadavků na bezpečnost informací při zpracovávání logů událostí (např. smluvní požadavky).
- Protokolování přístupů během připojování a odpojování externích sítí (např. vzdálené údržbě).

Další požadavky velmi vysokých nároků na ochranu (pro „C“, „I“):

- Protokolování všech přístupů k údajům, které jsou klasifikovány jako informace s velmi vysokými potřebami ochrany (je-li to možné s ohledem na právní a organizační ustanovení).[181]

Aby bylo zabráněno využívání technických zranitelností musí být zaveden **management technických zranitelností**. Odhalování technických zranitelností je klíčovou rolí v informační bezpečnosti. V rámci managementu technických zranitelností musí být:

- Sbírány a analyzovány informace o technických zranitelnostech u IT systémů, které jsou používány (např. informace od výrobce, provedené systémové audity, databáze CVS), a následně vyhodnocovány (např. prostřednictvím systému CVSS[182]).
- Identifikovány a vyhodnoceny IT systémy a software, které mohou být potenciálně ovlivněné.

Měly by být stanoveny postupy pro řízení oprav (např. testování, instalace), opatření ke snížení rizik, vhodné způsoby ověřování úspěšnosti instalace oprav ke zjištění správnosti aplikace.

[181] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[182] Common Vulnerability Scoring System

Provozní systémy zahrnující IT systémy a služby musí být podrobeny **auditním testům** nebo jiné ověřovací činnosti (systémovým nebo servisním auditům), které mají odhalit stavy, které by mohly ohrozit dostupnost, důvěrnost nebo integritu těchto IT systémů a služeb. Proto musí být:

- stanoveny požadavky na audit IT systémů nebo služeb,
- upřesněn rozsah auditu v dostatečném předstihu,
- zajištěna koordinace auditů s provozovatelem a uživateli IT systémů nebo služeb,
- archivovány výsledky auditů sledovatelným způsobem,
- hlášeny výsledky auditů příslušnému vedení,
- odvozena měření z výsledků auditů.

Systémové nebo servisní audity by měly být plánovány s přihlédnutím ke všem potenciálním bezpečnostním rizikům (např. poruchám), prováděny kvalifikovaným personálem nebo vhodnými nástroji (např. skenery zranitelnosti) a řízeny z internetu a vnitřní sítě. Po ukončení auditu by měla být zpracována zpráva.

K ochraně informací v sítích musí být stanoveny a plněny požadavky na **bezpečnost sítí a jejich segmentaci**. Měly by být definovány postupy pro řízení a kontrolu sítí a segmentaci sítí, která zohledňuje:

- omezení připojení IT systému k síti,
- používání bezpečnostních technologií (např. firewallové systémy, bezpečnostní software pro zamezení nechtěné výměny dat),
- hodnocení výkonu, důvěryhodnosti, dostupnosti a bezpečnostních aspektů,
- implementaci opatření pro minimalizaci dopadu v případě kompromitovaných IT systémů, odhalování potenciálních útoků,
- oddělování sítí podle provozního účelu (např. testovací a vývojové sítě, kancelářské sítě, výrobní sítě),
- zvážení rizika spojeného s poskytováním síťových služeb přes internet,
- specifikace technologických možností pro oddělení sítí při využívání externích IT služeb,
- vytvoření adekvátního oddělení mezi vlastními sítěmi a sítěmi zákazníků,
- implementaci opatření pro odhalování a prevenci ztráty nebo úniku dat.[183]

[183] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

Další požadavky vysokých nároků na ochranu (pro „C“, „I“, „A“):

- Stanovení a implementace rozšířených požadavků na správu a kontrolu sítí se zohledněním autentizace IT systémů v síti, omezení přístupu k rozhraním pro správu IT systému, definování specifických rizik (např. bezdrátového a vzdáleného přístupu).[184]

Za účelem zajištění dostupnosti informací a dalších souvisejících aktiv během narušení musí být zavedeno **plánování kontinuity pro IT služby**. Musí být identifikovány kritické IT služby a zvážen jejich obchodní dopad. Musí být stanoveny, plněny a příslušným zainteresovaným stranám známy požadavky a odpovědnosti za kontinuitu a obnovu IT služeb. Měly by být:

- identifikovány kritické IT systémy, včetně klasifikace odpovídající potřeby ochrany a implementace adekvátních a vhodných bezpečnostních opatření,
- stanoveny požadavky na plánování kontinuity zahrnující scénáře, které ovlivňují kritické IT systémy, především útoky typu Denial of Service, ransomwarové útoky, selhání systému, přírodní katastrofy,
- zohledněny alternativní komunikační strategie (pokud nejsou dostupné primární komunikační prostředky), alternativní strategie úložišť (pokud nejsou dostupná primární úložiště), alternativní napájení a síť,
- pravidelná revize a aktualizace plánů kontinuity.

Další požadavky vysokých nároků na ochranu (pro „C“, „I“):

- Zálohy musí být ochráněny před neoprávněnou úpravou nebo smazáním škodlivého softwaru.
- Zálohy musí být ochráněny před neoprávněným přístupem škodlivého softwaru.

Další požadavky vysokých nároků na ochranu (pro „C“, „I“, „A“):

- Jsou určena alternativní úložiště a zálohovací místa.[185]

Aby byla možná obnova po ztrátě dat nebo systémů (např. po selhání hardwaru, softwaru, chybách operátorů nebo útocích) musí být stanovena koncepce **zálohování** příslušných IT systémů, která obsahuje vhodná ochranná opatření k zajištění důvěrnosti, integrity a dostupnosti. Musí být stanoveny také koncepty obnovy pro relevantní IT služby.

[184] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].
[185] Tamtéž.

IT bezpečnost / kybernetická bezpečnost – Akvizice systému, správa požadavků a vývoj

K dosažení bezpečného vývoje je třeba stanovit požadavky na **informační bezpečnost v rámci životního cyklu návrhu a vývoje** IT systémů. Musí být stanoveny požadavky na informační bezpečnost při pořízení nebo rozšíření IT systémů a IT komponent, změnách vyvinutých IT systémů, provádění testů schválení systému. V rámci specifikace požadavků by měla být zvážena:

- doporučení dodavatele a osvědčené postupy pro bezpečnou konfiguraci a implementaci,
- bezpečnost při selhání,
- přezkoumání specifikací,
- kontrola IT systému před produktivním použitím v souladu se specifikacemi,
- vyloučení používání produktivních dat pro testování (příp. musí být testovací systém opatřen ochrannými opatřením srovnatelnými s operačním systémem,
- požadavky na životní cyklus testovacích dat, jako např. mazání, maximální životnost,
- definování případových specifikací pro generování testovacích dat.

Další požadavky velmi vysokých nároků na ochranu (pro „C“, „I“, „A“):

- Testování bezpečnosti účelového nebo rozsáhle přizpůsobeného softwaru (např. penetračními testy) při uvádění do provozu, v případě významných změn nebo v pravidelných intervalech.[186]

Požadavky na informační **bezpečnost síťových služeb** musí být identifikovány, zavedeny a monitorovány a měly by být dohodnuty formou dohody o provádění činnosti. Měl by být stanoven a implementován postup pro zabezpečení a používání síťových služeb a adekvátní řešení redundance.

Musí být stanoven a zaveden postup pro **vrácení informačních aktiv** při ukončení externí IT služby a jejich bezpečné odstranění. Měl by obsahovat popis celého procesu i s ohledem na případné změny a měl by být smluvně ošetřen.

Informace ve sdílených externích IT službách musí být ochráněny efektivní segregací mezi jednotlivými klienty, aby k nim neměly přístup uživatelé jiných organizacích. Koncepce segregace by měla být písemně stanovena a zohledňovat případné změny. Je vhodné zapracovat oddělení dat, funkcí zákaznického softwaru, operačního systému, uložiště a sítě a posoudit rizika pro provoz externího softwaru ve sdíleném prostředí.

[186] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

Postup pro definování, implementaci a sdělování **relevantních právních, regulačních a smluvních ustanovení**, které se týkají informační bezpečnosti, musí být stanoven a pravidelně aktualizován, včetně přezkoumání integrity záznamů za účelem ověření dodržení shody s těmito ustanoveními.

Organizace musí identifikovat a plnit požadavky na **zachování soukromí a ochranu osobních údajů** při zavádění informační bezpečnosti. Je třeba:

- Definovat zákonné a smluvní požadavky na zabezpečení informací, které se týkají postupů a procesů, v rámci kterých dochází ke zpracování osobních údajů.
- Definovat a sdělovat pověřeným osobám předpisy, které se týkají dodržování zákonných a smluvních požadavků na ochranu osobních údajů.
- Zohlednit procesy a postupy pro ochranu osobních údajů v systému řízení bezpečnosti informací.[187]

3.2.11.2 Kritéria ochrany prototypů

Prototypová ochrana se zabývá fyzickými produkty, které jsou identifikovány jako vyžadující ochranu. Prototypem můžou být vozidla, komponenty nebo díly. Vlastník duševního vlastnictví spojený s prototypem je považován za jeho vlastníka. Odpovědnost za klasifikaci potřeby ochrany prototypu má oddělení uvádění do provozu. Pokud jsou prototypy klasifikovány jako vyžadující vysokou nebo velmi vysokou úroveň ochrany, jsou stanoveny minimální požadavky na zabezpečení prototypů.[188]

Pro splnění požadavků cílů hodnocení vybrané organizace je proto třeba zavést bezpečnostní opatření dle katalogu kritérií ISA z oblasti ochrany prototypů v rozsahu požadavků bodů 8.1, 8.2 a 8.3, včetně dalších požadavků na vozidla klasifikovaná jako vozidla vyžadující ochranu.

Fyzická a environmentální bezpečnost

Za účelem splnění minimálních požadavků na fyzickou a environmentální bezpečnost pro ochranu prototypu musí být stanoven **bezpečnostní koncept**, který zahrnuje nezbytná opatření pro ochranu prototypů aplikovaných a implementovaných pro vlastnosti a zařízení dodavatelů, vývojových partnerů a poskytovatelů služeb. Zohledňuje stabilitu vnějšího pláště, ochranu pohledu a zraku, ochranu proti neoprávněnému vstupu a kontrolu přístupu, monitorování narušení, zaznamenávání návštěv, separaci klientů. Měl by zohledňovat také obvodové zabezpečení.[189]

[187] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].
[188] Tamtéž.
[189] Tamtéž.

Pro zabránění neoprávněnému přístupu k nemovitostem s výrobou, zpracováním nebo skladováním vozidel, komponentů nebo dílů vyžadujících ochranu musí být stanoven **bezpečnostní perimetr**. Měly by být umístěny vhodné pevné umělé bariéry (např. ploty nebo zdi), technické bariéry (např. detekce pohybu), nebo přirozené bariéry (např. stromy a jiná vegetace).[190]

Vnější plášť chráněných budov, kde se vyrábí, zpracovávají nebo skladují vozidla, komponenty nebo díly vyžadující ochranu, musí být konstruován tak, aby nebylo možné ho odstranit nebo otevřít pomocí standardních nástrojů. Měl by být vyroben z masivní konstrukce (např. ze zdiva, betonu, železobetonu) a okna a dveře by měly být vyrobeny v souladu s bezpečnostní třídou RC 2[191] nebo vyšší.

Ochrana pohledu a zraku ve vymezených bezpečnostních oblastech musí být zajištěna z důvodu zabránění neoprávněného sledování nového vývoje, který vyžaduje vysokou nebo velmi vysokou ochranu. Měla by být zajištěna ochrana pohledu do bezpečnostních oblastí přes skleněné plochy a zabráněn pohled otevřenými dveřmi, bránami nebo okny. To platí i pro vozidla vyžadující ochranu před neoprávněným pohledem.

Všechny přístupové body do bezpečnostních oblastí musí být ochráněny proti neoprávněnému vstupu formou **kontroly vstupu**. Podmínkou je splnění alespoň jednoho z těchto požadavků: mechanické zámky (se záznamem o přiřazení klíče), elektronické přístupové systémy (se záznamem o přidělení oprávnění), osobní kontrola (se záznamem vstupu). To platí i pro vozidla vyžadující ochranu před neoprávněným přístupem.

Bezpečnostní prostory musí být **monitorovány** z hlediska narušení, aby bylo zjištěno případné vniknutí. Musí být zajištěna kontrola narušení buď systémem detekce (v souladu s EN 50131 Poplachové systémy nebo jinými certifikovanými bezpečnostními službami nebo řídícími jednotkami) nebo ostrahou prostřednictvím certifikované bezpečnostní služby v rozsahu 24/7. Dále musí být zpracovány poplachové plány a zajištěno zpracování alarmu bez prodlení.

Pro ochranu před neoprávněným přístupem musí být zaveden dokumentovaný **management návštěvnosti**. Ten musí zahrnovat povinnost registrace a zdokumentování povinnosti mlčenlivosti před přístupem všech návštěvníků. Bezpečnostní a návštěvní řád musí být zveřejněn a musí být dodržována zákonná ustanovení, která se týkají ochrany údajů, platných v jednotlivých zemích.[192]

---

[190] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[191] vyšší odolnost a základní průlomové zkoušky pro případ pokusu o vloupání

[192] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

Za účelem ochrany specifického know-how klienta musí být zajištěna **segregace klientů** na místě, aby bylo zabráněno neoprávněnému prohlížení a přístupu do bezpečnostních oblastí. Segregace je možná personálními nebo technickými opatřeními podle zákazníků a/nebo dle projektů. V případě, že není segregace účinná, musí být vyžádán výslovný souhlas zákazníka. To platí i pro vozidla vyžadující ochranu.[193]

Organizační požadavky

Při přenosu informací, které jsou klasifikované jako vyžadující ochranu, je nutné zajistit uzavření **dohod o mlčenlivosti** mezi dodavatelem a zákazníkem i se všemi zaměstnanci a členy projektu (ve formě osobního závazku) podle platného smluvního práva jednotlivých zemí.

V případě **zapojení subdodavatelů** do projektu musí být stanoveny a plněny minimální požadavky na ochranu prototypu, které zahrnují:

- schválení od původního zákazníka,
- existující smluvně platnou dohodu o mlčenlivosti mezi dodavatelem a subdodavatelem i se všemi zaměstnanci a projektovými členy subdodavatele (formou osobního závazku),
- prokázání shody s bezpečnostními požadavky původního zákazníka,
- doložení splnění minimálních požadavků na ochranu prototypu ze strany subdodavatele (např. formou certifikátu nebo atestu).

Zaměstnanci a členové projektu musí získat potřebné znalosti a dovednosti pro bezpečné zacházení s vozidly, komponenty a díly, které vyžadují ochranu, na **školeních nebo osvětových seminářích**, které musí být zajištěny vedením. Školení ohledně manipulace s prototypy musí být zajištěno před zahájením projektu a dále pravidelně (minimálně ročně) opakováno. Podmínkami jsou: zajištění znalostí o příslušných potřebách ochrany a z nich vyplývajících opatřeních v rámci společnosti, povinná účast, zdokumentování dokončených opatření. Koncept školení pro ochranu prototypů musí být nedílnou součástí obecné koncepce školení.

Bezpečnostní klasifikace projektu a požadavky ve vztahu k postupu projektu musí být známy všem členům projektu. Zváženy musí být plány krok za krokem, včetně opatření pro utajení a maskování a politiky rozvoje. Požadavky jsou stejné jako požadavky týkající se informační bezpečnosti projektu.[194]

[193] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[194] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

Musí být stanoven proces pro **udělování přístupu** do bezpečnostních oblastí, aby byla zajištěna ochrana před neoprávněným přístupem. Musí být specifikovány a zdokumentovány odpovědnosti za autorizace přístupu, zavedeny procesy přidělení nových autorizací, změn a zrušení přístupových práv a stanoven a dodržován kodex chování pro případ, že dojde ke ztrátě nebo odcizení prostředků kontroly vstupu.[195]

K zabránění neoprávněnému vytvoření nebo přenosu obrazového materiálu musí být stanoveny postupy pro **záznam obrazu a manipulaci s vytvořeným obrazovým materiálem**. Součástí postupů musí být:

- postup schvalování záznamů obrazu,
- určení specifikace pro klasifikaci a kategorizaci obrazového materiálu,
- postup pro uložení, vymazání/likvidaci obrazového materiálu,
- postup pro zabezpečený přenos nebo zasílání obrazového materiálu pouze oprávněným osobám.

K zabránění neoprávněnému vytvoření nebo přenosu obrazového materiálu musí být dále stanoven **postup pro přenášení a používání mobilních video a fotografických zařízení** v bezpečnostních oblastech. Postup musí obsahovat specifikace pro přenášení (např. požadavky na zapečetění) a specifikace pro použití (např. možnost telefonování, fotografování atd.).

Manipulace s vozidly, komponenty a díly

Pro vozidla, komponenty a díly klasifikované jako vyžadující ochranu musí být popsán a implementován proces ochrany před neoprávněným prohlížením, neoprávněným záznamem obrazu a přístupem během jejich **přepravy**. Součástí procesu musí být:

- postup získání specifických požadavků zákazníka na přepravu,
- sdělení a dodržování bezpečnostních požadavků definovaných zákazníkem,
- pověření takové logistické nebo přepravní služby, která byla výslovně schválena zákazníkem,
- popsaný a implementovaný proces hlášení jakýchkoliv událostí zákazníkovi, které souvisí se zabezpečením.

V případě **parkování/skladování** vozidel, komponentů a dílů klasifikovaných jako vyžadující ochranu musí být tyto chráněny proti neoprávněnému prohlížení, fotografování a přístupu. Specifické požadavky zákazníka musí být prokazatelně předloženy a musí být dodržovány.[196]

[195] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

[196] ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

3.2.11.3 Kritéria ochrany dat

Požadavky na ochranu dat nejsou pro vybranou organizaci relevantní.

3.2.12 Interní hodnocení a přezkoumání

Organizace by měla identifikovat, co je potřeba monitorovat a měřit a jakou metodu pro monitorování, měření, analýzy a hodnocení zvolit. Aby zvolené metody poskytovaly porovnatelné výsledky, musí organizace stanovit harmonogram pro monitorování, měření, analýzy a hodnocení, určit odpovědné osoby za provádění monitorování a měření a za jejich analýzu a hodnocení.[197]

Nezávislým přezkoumáním informační bezpečnosti by mělo vedení organizace pověřit jednotlivce, který není závislý na přezkoumávané oblasti, ale má odpovídající odbornou způsobilost. K tomu může využít formu interních auditů a/nebo audity externí organizace. Přezkoumávání by mělo probíhat v plánovaných intervalech nebo v případě významných změn, jako např. při změně legislativních požadavků (zákonů, předpisů), výskytu významných bezpečnostních incidentů, zahájení nebo změně činnosti organizace nebo rozsáhlejší změně opatření a postupů. Výsledky přezkoumání by měly být předkládány k přezkoumání vrcholovému vedení.[198]

Pro získání informací o plnění požadavků organizace na systém bezpečnosti informací a efektivnosti implementovaného systému bezpečnosti informací musí organizace pravidelně provádět **interní audity**. Za tímto účelem musí vytvořit a udržovat program interních auditů s rozsahem každého auditu, odpovědností za jeho provedení. Dále musí jmenovat auditory a zajistit jejich objektivitu a nestrannost a zajistit předkládání výsledků auditů vedení organizace.[199]

Výsledkem auditu může být zjištění **neshody** s požadavky na plnění systému informační bezpečnosti, která musí být vypořádána v rámci neustálého zlepšování systému řízení informační bezpečnosti. V případě zjištění neshody musí organizace přijímat opatření a zabývat se jejími následky, ale také určit její kořenovou příčinu a opatření k odstranění této kořenové příčiny, aby se neshoda v budoucnu neopakovala.[200]

---

[197] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2018. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

[198] Tamtéž.

[199] Tamtéž.

[200] Tamtéž.

Vhodnost, přiměřenost a efektivnost systému bezpečnosti informací musí organizace zajišťovat formou **přezkoumání vedením organizace**. To musí zohlednit výsledky předchozích přezkoumání vedením organizace, změny týkající se systému bezpečnosti informací, neshody a nápravná opatření z auditů, výsledky posouzení rizik, příležitosti pro neustálé zlepšování. Výstupy z pravidelného přezkoumání vedením organizace musí obsahovat rozhodnutí ohledně příležitostí k trvalému zlepšováním a jakýchkoliv potřebných změn v systému řízení informační bezpečnosti.[201]

3.3 Závěry a doporučení

Implementací TISAX® a následně provedením hodnocení TISAX® na základě stanovených cílů je možné dosáhnout úspory času a nákladů vzhledem k ušetření opakovaných hodnocení ze strany různých zákazníků. Nespornou výhodou je také získání konkurenční výhody při prokázání splnění požadavků na zabezpečení informací. V neposlední řadě je minimalizována pravděpodobnost vzniku bezpečnostních incidentů na základě analýzy rizik a přijímání preventivních opatření proti jejich vzniku, příp. nápravných opatření po jejich odhalení.

V současné době neexistuje závazná metodika pro implementaci systému TISAX®. Navržená metodika implementace systému TISAX® vychází ze znalosti pojmů a principů z oblasti systémů managementu, kybernetické bezpečnosti, bezpečnosti informací a dodavatelských vztahů. Použití této metodiky v praxi předpokládá znalosti a odbornou způsobilost pověřených osob za tuto oblast, nejlépe minimálně na úrovni interního auditora na základě akreditovaného kurzu.

Ověření navržené metodiky je možné při reálném použití metodiky implementace systému TISAX® a následném provedení sebehodnocení dle katalogu kritérií ISA samotnou organizací, ve které byl systém TISAX® podle navržené metodiky implementován, a při provedení hodnocení nezávislým a nestranným poskytovatelem auditu (certifikačním orgánem), jehož role třetí strany musí být oddělena od poradenských či konzultačních činností v rámci implementace. Vzhledem k posuzování citlivých informací v rámci sebehodnocení nebo hodnocení, nutnosti dodržení platných právních ustanovení týkajících se ochrany údajů a uzavření smluv o mlčenlivosti, zachování nestrannosti a nezávislosti a rozsahu této diplomové práce nebylo možno toto sebehodnocení/hodnocení provést v rámci zpracování této diplomové práce.

[201] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

Závěr

Cílem mojí práce bylo navrhnout metodiku implementace TISAX® pro dodavatele z oblasti automobilového průmyslu tak, aby tento systém a jeho udržování garantovaly maximální kybernetickou bezpečnost informací a dat.

Diplomová práce shrnula důležitost kybernetické bezpečnosti v dnešní digitální éře a význam implementace systému TISAX® pro dodavatele v automobilovém průmyslu. Zdůraznila potřebu ochrany informací a dat v dodavatelském řetězci, a to nejen kvůli případným finančním ztrátám, ale také možnému narušení dodavatelského řetězce a možným škodám na dobrém jménu organizace.

Vybrána byla organizace působící v automobilovém průmyslu, která má strategickou polohu v průmyslové oblasti v Mladé Boleslavi a je přímým dodavatelem výrobce automobilů OEM. Jejími partnery jsou např. Škoda Auto, Mercedes-Benz, Continental, Porsche, Benteler, Jaguar, Audi, Grupo Antolin, Magna, STADLER, ČVUT, Centrum dopravního výzkumu, Ministerstvo dopravy, TÜV NORD Czech. Organizace se zabývá povrchovou úpravou dílů, výrobou měřících, zkušebních a navigačních přístrojů, engineeringem v souvislosti s bezpečností a životností vozidel včetně jejich komponent a testováním vozidel z hlediska pasivní i aktivní bezpečnosti. Pro komunikaci s obchodními partnery využívá elektronický systém výměny dat. Na základě specifických požadavků výrobce automobilů OEM je od ní vyžadována implementace systému TISAX® a provedení hodnocení a získání známky TISAX® pro cíle hodnocení: nakládání s informacemi s velmi vysokou potřebou ochrany na úrovni „důvěrnost“, ochranu prototypových dílů a součástí a ochranu prototypů vozidel.

Nejdříve byly analyzovány požadavky systému TISAX® stanovené formou kontrolních otázek v hodnotícím katalogu ISA, který vydává německá asociace automobilového průmyslu VDA, složená z odborníků z automobilového průmyslu, a který spravuje asociace ENX Association, složená z výrobců automobilů, dodavatelů a národních automobilových asociací. Katalog obsahuje požadavky z oblasti informační bezpečnosti, ochrany prototypů a ochrany údajů, které jsou pro organizace relevantní dle jejich stanovených cílů hodnocení dle aktuálního seznamu definovaných cílů systému TISAX®. Požadavky jsou označené jako povinné (musí být splněny), doporučené (měly by být splněny) a další požadavky vysokých nároků na ochranu a velmi vysokých nároků na ochranu, které jsou pro organizace rovněž relevantní dle jejich stanovených cílů hodnocení.

Všechny požadavky systému TISAX® byly porovnány s normami z oblasti bezpečnosti informací, na které se hodnotící katalog ISA přímo odvolává. Jedná se o normy ČSN EN ISO/IEC 27001:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu

informační bezpečnosti – Požadavky, která se zabývá požadavky na stanovení, implementování, udržování a neustálé zlepšování systému managementu informační bezpečnosti, dále ČSN EN ISO/IEC 27002:2023 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti, která se zabývá obecnými opatřeními informační bezpečnosti včetně pokynů k implementaci a také ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny, která se zaměřuje na kritické aspekty nutné pro úspěšný návrh a implementaci systému řízení bezpečnosti informací.

Na základě provedeného hloubkového porovnání relevantních dokumentů byla navrhnuta metodika implementace systému TISAX®, která je založena na principu zavedení systému managementu bezpečnosti informací se zohledněním specifických požadavků systému TISAX® pro cíle hodnocení specifikované vybranou společností, tj. nakládání s informacemi s velmi vysokou potřebou ochrany na úrovni „důvěrnost“, ochranu prototypových dílů a součástí a ochranu prototypů vozidel. Po implementaci systému TISAX® může organizace provést sebehodnocení a požádat o provedení hodnocení úrovně splnění požadavků TISAX® třetí stranou u nezávislého a nestranného poskytovatele auditu (certifikačního orgánu).

Při zpracování metodiky byly také využity moje více než 25leté pracovní zkušenosti v certifikačním orgánu, který se zabývá mimo jiné i certifikací systému managementu bezpečnosti informací dle ČSN EN ISO/IEC 27001:2023 a certifikací TISAX®.

Seznam zkratek

ABAC	Attribute Based Access Control
AL	Assessment Level
B2B	Business-to-Business
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
ČSN	česká technická norma
CVS	Concurrent Versions System
CVSS	Common Vulnerability Scoring System
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DMS	Design and Manufacturing Suppliers
DoS	Denial of Service
EDI	Electronic Data Interchange
EU	European Union
GDPR	General Data Protection Regulation
HW	Hardware
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISA	Information Security Assessment
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
JIS	Just-in-Sequence
JIT	Just-in-Time
LAN	Local Area Network
MAC	Mandatory Access Control
NIS	Network Information Security
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OEM	Original Equipment Manufacturer
OFTP	Odette File Transfer Protocol

PDCA	Plan, Do, Check, Act
RBAC	Role-based Access Control
SCM	Supply Chain Management
SSO	Single Sign-On
SW	Software
TISAX	Trusted Information Security Assessment Exchange
TLS	Transport Layer Security
UPS	Uninterruptible Power Source
VDA	Verband der Automobilindustrie
VKP	Vyhláška o kybernetické bezpečnosti
VPP	Všeobecné podmínky a pravidla
ZKB	Zákon o kybernetické bezpečnosti

Seznam použité literatury

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení *kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

BRONEC, Oldřich. *Management in the engineering and automotive industry*. PPTX. MÚVS, [March 19, 2024].

COVISINT. *About Automotive Exchange*. Online. ©2023. Dostupné z: https://portal.covisint.com/web/103853/2. [cit. 2024-02-28].

ČESKÁ SPOLEČNOST PRO JAKOST (ČSJ). *Posouzení zabezpečení výměny důvěrných informací: Trusted Information Security Assessment Exchange – TISAX®*. Online. ©2023. Dostupné z: https://www.csq.cz/infocentrum/odborne-clanky/detail/posouzeni-zabezpeceni-vymeny-duvernych-informaci-trusted-information-security-assessment-exchange-TISAX®. [cit. 2024-04-16].

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. In: *Sbírka zákonů.* 2014, částka 75. Dostupné z: https://www.e-sbirka.cz/sb/2014/181/2022-08-06?f=181&zalozka=text. [cit. 2024-04-16].

DIEHLMANN, Jens a HÄCKER, Joachim. *Die Automobilhersteller im Jahre 2020*. Online. Ed.: 2. Oldenbourg Verlag München, 2012. Dostupné z: https://search-ebscohost-com.ezproxy.techlib.cz/login.aspx?direct=true&db=e000xww&AN=758942&lang=cs&site=ehost-live&ebv=EB&ppid=pp_C1. [cit. 2024-02-27].

ENX ASSOCIATION. *About ENX Association*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/enxassociation/. [cit. 2024-03-28].

ENX ASSOCIATION. *About TISAX®*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/TISAX®/. [cit. 2024-03-28].

ENX ASSOCIATION. *Downloads*. Online. [b.d.]. Dostupné z: https://portal.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-28].

ENX ASSOCIATION. *Information Security Assessment*. XLS tabulka. In: ENX. Dostupné z: https://www.enx.com/en-US/TISAX®/downloads/. [cit. 2024-03-30].

ENX ASSOCIATION. *Příručka pro účastníky systému TISAX®*. Online. 06.03.2024. Dostupné z: https://www.enx.com/handbook/tph-cz.html. [cit. 2024-03-28].

FIALA, Petr. Modelování *a analýza produkčních systémů*. Praha: Professional Publishing, c2002. ISBN 80-86419-19-3.

ILI, Serhan; ALBERS, Albert a MILLER, Sebastian. *Open innovation in the automotive industry*. Online. R&D Management, 2010, 40(3), 246-255. Wiley Online Library (distributor). Dostupné z: https://doi.org/10.1111/j.1467-9310.2010.00595.x. [cit. 2024-02-27].

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO 24089:2023. *Silniční vozidla – Inženýrství softwaru*. Online. ISO, 2023. Dostupné z: https://www.iso.org/standard/77796.html. [cit. 2024-04-16].

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/SAE 21434:2021. *Silniční vozidla – Inženýrství kybernetické bezpečnosti*. Online. ISO, 2021. Dostupné z: https://www.iso.org/standard/70918.html. [cit. 2024-04-16].

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Online. Národní centrum kybernetické bezpečnosti (distributor). 2015. Dostupné z: https://www.govcert.cz/cs/informacni-servis/slovnik/. [cit. 2024-02-28].

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

LEMPP, Martin a SIEGFRIED, Patrick. *Automotive Disruption and the Urban Mobility Revolution: Rethinking the Business Model 2030*. Online. 2022. ISBN 978-3-030-90035-9. Dostupné z: https://doi.org/10.1007/978-3-030-90036-6. [cit. 2024-02-28].

MARTY, Kilian. *Software Update for Road Vehicles - Ep.1 - Overview of UN R156 and ISO 24089*. Online. CERTX. 03.11.2022. Dostupné z: https://certx.com/automotive/software-update-for-road-vehicles-ep-1-overview-of-un-r156-and-iso-24089/. [cit. 2024-04-16].

MERRIAM-WEBSTER. *Dictionary*. Online. 05.04.2024. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity. [cit. 2024-04-16].

MOLNÁR, Jan. *Dodavatelské řetězce v automobilovém průmyslu*. Online. 23.08.2023. Dostupné z: https://www.editel.cz/dodavatelske-retezce-v-automobilovem-prumyslu/. [cit. 2024-02-28].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Nová směrnice EU o kybernetické bezpečnosti "NIS2" a návrh nového zákona o kybernetické bezpečnosti*. Online. [b.d.]. Dostupné z: https://osveta.nukib.gov.cz/course/view.php?id=145. [cit. 2024-04-16].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Počítání velikosti subjektu*. Online. PDF. 07.11.2023, v. 1.0. Dostupné z: https://osveta.nukib.gov.cz/pluginfile.php/58363/course/section/1391/factsheet_na_koho_regulace_dopadne_final.pdf. [cit. 2024-04-16].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Řízení dodavatelů*. Online. PDF. 06.09.2023, v. 1.0. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Metodika-rizeni-dodavatelu.pdf. [cit. 2024-03-30].

ODETTE. *OFTP2.* Odette File Transfer Protocol v2. Online. ©2024. Dostupné z: https://www.odette.org/oftp2. [cit. 2024-02-28].

OXFORD UNIVERSITY PRESS. *Oxford English Dictionary*. Online. ©2023. Dostupné z: https://www.oed.com/search/dictionary/?scope=Entries&q=cybersecurity&tl=true. [cit. 2024-04-16].

POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

SUPPLYON. *About Us*. Online. [b.d.]. Dostupné z: https://www.supplyon.com/en/about_us/. [cit. 2024-02-28].

SUPPLYON. *Supply Chain Collaboration*. Online. [b.d.]. Dostupné z: https://www.supplyon.com/en/solutions/supply-chain-collaboration/. [cit. 2024-02-28].

ŠAFROVÁ DRÁŠILOVÁ, Alena. *Základy úspěšného podnikání: průvodce začínajícího podnikatele*. Praha: Grada, 2019. ISBN 978-80-271-2182-3.

ŠKODA AUTO. *SKODETTE – EDI.* Online. ©2019. Dostupné z: https://edi.skoda-auto.cz/index-2.html. [cit. 2024-02-28].

TOMEK, Gustav a VÁVROVÁ, Věra. *Integrované řízení výroby: od operativního řízení výroby k dodavatelskému řetězci*. Expert (Grada). Praha: Grada, 2014. ISBN 978-80-247-4486-5.

TÜV NORD CZECH. *ISO 21434:2021*. Online. [b.d.]. Dostupné z: https://www.tuv-nord.com/cz/cs/nase-sluzby/certifikace-systemu/automobilovy-prumysl/iso-21434/. [cit. 2024-04-16].

TÜV NORD CZECH. *TÜV NORD CERT – Hodnocení systémů řízení bezpečnosti informací podle TISAX®*. Online. PDF. 2019. Dostupné z: https://www.tuv-nord.com/fileadmin/Content/TUV_NORD_COM/TUEV_NORD_CZECH/PDF/Produkt_listy/Produktovy_list_TISAX®-web.pdf. [cit. 2024-03-28].

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27001:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Online. ČAS, ©2023. Dostupné z: https://sponzorpristup.agentura-cas.cz/zobrazit.aspx. [cit. 2024-03-30].

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN EN ISO/IEC 27002:2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*. Česká agentura pro standardizaci, 2023.

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ (ÚNMZ). ČSN ISO/IEC 27003:2018. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny*. Česká agentura pro standardizaci, 2018.

VERBAND DER AUTOMOBILINDUSTRIE (VDA). *Recommendation Information Security*. Online. 04.08.2020. Dostupné z: https://www.vda.de/en/news/publications/publication/recommendation-information-security#publication-title. [cit. 2024-03-28].

WOLKSWAGEN GROUP. *Welcome to the ONE.Group Business Platform*. Online. [b.d.]. Dostupné z: https://www.vwgroupsupply.com/one-kbp-pub/en/kbp_public/homepage/homepage.html. [cit. 2024-02-28].

YEUNG, Godfrey. *CODIFIABILITY AND GEOGRAPHICAL PROXIMITY OF SUPPLY NETWORKS IN AUTOMOTIVE INDUSTRY*. Online. Erdkunde. 2023, 77(2), 91-111. ISSN 00140015. Dostupné z: https://doi.org/10.3112/erdkunde.2023.02.01. [cit. 2024-02-28].

Seznam obrázků

Seznam tabulek