IMPLEMENTACE ZÁSAD KYBERNETICKÉ BEZPEČNOSTI DO FUNGOVÁNÍ FIRMY DODÁVAJÍCÍ SW A HW

Jindřich Zoubek, TECHSYS – HW a SW, a.s.

Příspěvek se zabývá organizačními opatřeními zajišťující bezpečnost dat, implementováním metodiky bezpečného vývoje SW, analýzou rizik všech produktů a technickými opatřeními (logování činnosti administrátorů a uživatelů, správou uživatelů navázánou na AD/LDAP a zabezpečením telemetrických komunikací (IEC 62351)

1. ÚVOD

Na úvod článku je dobré sdělit, co vedlo k výběru tématu, napsání článku a vlastní prezentaci zkušeností s implementací zásad kybernetické bezpečnosti do fungování firmy jakou je firma TECHSYS. Kromě toho, že jsme se chtěli podělit o naše zkušenosti z implementace a ukázat stručný návod, co to pro konkrétní firmu znamená, byla motivací celá řada dalších efektů majících na firmu vliv:

- přínos v podobě interních i externích organizačních opatření z pohledu kybernetické bezpečnosti,
- přínos v podobě dalšího know-how z moderní oblasti ICT,
- přínos v podobě zvýšení důvěryhodnosti pro partnery,
- přínos v podobě splnění jednoho z častých kvalifikačních kritérií pro výběrová řízení,
- organizační náročnost v podobě navýšení administrativy,
- ekonomická náročnost v podobě nákladů za pravidelné dozorové a recertifikační audity,
- atd.

Domníváme se a doufáme, že článek bude dobrým náhledem „pod pokličku“ toho co, přijetí opatření zásad kybernetické bezpečnosti nebo přímo certifikace ISMS, znamená pro firmu chystající se na implementaci a jaké jsou její praktické dopady.

2. PRÁVNÍ RÁMEC

Aktuálně je právní rámec dán několika zákony, vyhláškami a nařízeními z nich následující mají z našeho pohledu největší význam.

2.1. VYHLÁŠKA Č. 316 / 2014 – VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI

Celým jménem „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti“.

Tato vyhláška stanovuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah bezpečnostních opatření,
- rozsah zavedení bezpečnostních opatření,
- typy a kategorie kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,

- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku
- vzor oznámení kontaktních údajů a jeho formu.

Více k vyhlášce lze nalézt např. zde: https://www.govcert.cz/download/kii-vis/vkb_uz.pdf

2.2. NAŘÍZENÍ VLÁDY Č. 315 / 2014 – ODVĚTVOVÁ KRITÉRIA PRO URČENÍ PRVKU KRITICKÉ INFRASTRUKTURY

Příloha, která mění nařízení vlády č. 432 / 2010.

Pro odvětví:

- Enegetika,
- Vodní hospodářství,
- Potravinářství a zemědělství,
- Zdravotnictví,
- Doprava,
- Komunikační a informační systémy,
- Finanční trh a měna,
- Nouzové služby,
- Veřejná správa.

Zajímavostí z oblasti vodohospodářství, která možná leckoho překvapí, je např. to, že Povodí Labe není součástí kritické infrastruktury, přičemž Povolí Vltavy, ano. Překvapující to ale je jen zdánlivě, jelikož Povodí Labe nedisponuje na svém toku žádným vodním dílem o objemu zachycené vody nejméně 100 mil. m^3 (což je podmínkou daného nařízení vlády), na rozdíl od Povodí Vltavy, kde máme, nejen vodohospodářsky ale i energeticky významnou, celou Vltavskou kaskádu, kde tuto podmínku splní hned tři vodní díla (Lipno I., Orlík, Slapy).

Více k nařízení vlády lze nalézt např. zde: https://www.govcert.cz/download/kii-vis/urc_kriteria_KII.pdf

2.3. VYHLÁŠKA 437 / 2017 – O KRITÉRIÍCH PRO URČENÍ PROVOZOVATELE ZÁKLADNÍ SLUŽBY

Tato vyhláška zapracovává příslušný předpis Evropské unie a upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti.

Týká se subjektů nad rámec kritické infrastruktury státu.

Vždy je uveden druh služby, druh subjektu a speciální kritéria druhu subjektu a dopadová kritéria.

Příkladem druhu služby je „Prodej elektřiny“, druhem subjektu je „Obchodník s elektřinou podle energetického zákona“ a speciálním kritériem jsou „Systémy využívané k prodeji elektřiny, mající přímý vliv na dodávku elektřiny koncovým zákazníkům“.

Více k vyhlášce lze nalézt např. zde: http://www.psp.cz/sqw/sbirka.sqw?cz=437&r=2017

3. STÁTNÍ INSTITUCE

Ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany se od 1. srpna 2017 stal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dříve (před 1. 8. 2017) se problematikou kybernetické bezpečnosti zabýval přímo NBÚ (Národní bezpečnostní úřad).

obrázek 1 Logo NÚKIB

Z praktického hlediska z pohledu firmy má úřad dvě následující funkce:

- zveřejňuje aktuální hrozby a doporučení s ohledem na kybernetickou a informační bezpečnost,
- slouží k nahlašování a projednávání kritických bezpečnostních incidentů.

Jaké jsou obecně hlavní oblasti činnosti NÚKIB:

- provozovat Vládní CERT České republiky GovCERT.CZ (CERT = Computer Emergency Response Team),
- spolupráce s ostatními národními CERT týmy a CSIRT týmy (CISRT = Computer Security Incident Response Team, v ČR provozován sdružením CZ.NIC),
- spolupráce s mezinárodními CERT týmy a CSIRT týmy,
- příprava bezpečnostních standardů pro informační systémy KII a VIS,
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti,
- výzkum a vývoj v oblasti kybernetické bezpečnosti,
- ochrana utajovaných informací v oblasti informačních komunikačních systémů,
- kryptografická ochrana,
- Národní centrum PRS (NCPRS) - jedna ze služeb evropského satelitního systému Galileo (PRS = Public Regulated Service).

Více je o úřadu možno nalézt na: https://www.nukib.cz/

4. ZÁKLADNÍ POJMY

Nyní si definujme několik základních pojmů z problematiky určování kybernetické bezpečnosti:

1. Kritická infrastruktura (nebo též kritická informační infrastruktura = KII)
   a) Určujícím kritériem je nařízení vlády č. 315/2014 Sb. (https://www.govcert.cz/download/kii-vis/urc_kriteria_KII.pdf).
   b) V praxi se jedná o takové informační nebo komunikační systémy, příp. ICS/SCADA systémy, které naplní kritéria pro určení prvků KII dle schématu zde: zde: https://www.govcert.cz/download/kii-vis/container-nodeid-663/2schemakii-cz.pdf.
2. Významný informační systém (= VIS)
   a) Stanovuje jej vyhláška č. 317/2014 Sb. (https://www.govcert.cz/download/kii-vis/VVIS_UZ.pdf).
   b) Schéma pro určení VIS je možno nalézt zde: https://www.govcert.cz/download/kii-vis/container-nodeid-707/3schemavis-cz.pdf
3. Správce a Provozovatel KII

a) Správcem informačního nebo komunikačního systému KII je takový orgán nebo osoba, která určuje účel komunikačního systému nebo účel zpracování informací a podmínky provozování informačního nebo komunikačního systému.

b) Provozovatelem informačního nebo komunikačního systému KII je takový orgán nebo osoba, která zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém, správce je určil a o této skutečnosti informoval.

4. Dodavatel kritické infrastruktury

a) Je takový orgán nebo osoba, která musí splnit bezpečnostní požadavky provozovatele KII a prokázat kvalifikační předpoklady (zpravidla audit ISO 27001) a v případě požadavku provozovatele se podrobit jeho auditu.

5. Základní služba (ZS)

a) ZS je dle § 2 písm. i) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví.

b) Stanovuje vyhláška č. 437/2017 Sb.

c) Kritéria pro jednotlivá odvětví jsou určena druhem služby, druhem subjektu a speciálním kritériem druhu subjektu.

5. IMPLEMENTACE

5.1. POŽADAVKY NA ISŘ

Integrovaný systém řízeni (ISŘ) implementuje v TECHSYS požadavky všech přijatých norem, tedy.

- QMS – ČSN EN ISO 9001 : 2016
- EMS – ČSN EN ISO 14001 : 2016
- SM BOZP – ČSN OHSAS 18001 : 2008
- ISMS – ČSN EN ISO/IEC ISO 27001 : 2014

Získáním všechno těchto certifikací je možno obdržet tzv. Diamantový certifikát.


TECHSYS - HW a SW, a.s.

Březinova 640/3a, 186 00 Praha 8 – Karlín, Česká republika
a pracoviště: U Výstaviště 1485, 370 03 České Budějovice

obdržel

DIAMANTOVÝ CERTIFIKÁT

číslo CQS 142/2002 - 2018

pro integrovaný systém managementu v souladu s požadavky:

QMS - ČSN EN ISO 9001 : 2009
EMS - ČSN EN ISO 14001 : 2005
SM BOZP - ČSN OHSAS 18001 : 2008
ISMS – ČSN EN ISO/IEC 27001 : 2014

Tento certifikát platí pro:

Vývoj, výroba, projektování, prodej, instalace a servis řídicích systémů

Platnost certifikátu omezena do: 27. 02. 2020
Datum vydání: 24. 03. 2018

Ing. Jana Olšanská
Vedoucí certifikačního orgánu

IQNet

CQS

CQS je certifikačním orgánem, akreditovaným podle normy ČSN EN ISO/IEC 17021-1:2016 Českým institutem pro akreditaci, o.p.s. pod registračním číslem 3029 pro certifikaci systémů managementu.

obrázek 2 Diamantový certifikát

Z pohledu plnění podmínek kybernetické bezpečnosti je velmi praktické provázání procesů QMS s požadavky ISMS.

Požadavky ISMS prostupují všemi činnostmi firmy TECHSYS. Dle ISŘ máme následující hlavní procesy, kterých se to týká:

- Provoz
- Výroba a servis
- Vývoj
- Obchod

5.1.1. ISMS

Systém řízení bezpečnosti informací (Information Security Management System - ISMS) je dokumentovaný systém, řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že:

- jsou určena aktiva, která se mají chránit,
- jsou zvolena a řízena možná rizika bezpečnosti informací,
- jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována.

Při zavádění systému řízení bezpečnosti informací v organizaci se postupuje podle normy ISO/IEC 27001, která poskytuje doporučení, jak ze souboru doporučených nejlepších postupů, které uvádí norma ISO/IEC 27002 (původně ISO/IEC 17799), případná certifikace se pak provádí podle normy ISO/IEC 27001.

obrázek 3 Logo ISO 27001

Jaké jsou hlavní obecné přínosy zavedení a certifikace ISMS:

- Přechod od nesystémového a neuceleného řízení bezpečnosti k bezpečnosti řízené a komplexní.
- Efektivní řízení investic vkládaných do bezpečnosti.
- Inventura vlastních aktiv, jejich ocenění a klasifikace.
- Řízené odstranění nebo snížení rizik v oblasti informačních systémů.
- Zavedení systémového a systematického přístupu při používání IT/IS.
- Zvýšení povědomí a odpovědnosti zaměstnanců při práci s informacemi.
- Naplnění legislativních požadavků.
- Zvýšení důvěryhodnosti pro partnery.
- Trvalé monitorování a zlepšování systému řízení bezpečnosti informací (ISMS).
- Konkurenční výhoda, kultivace Image a firemní kultury.

Jaké jsou hlavní praktické přínosy zavedení a certifikace ISMS:

- **Jedna z alternativ, jak splnit požadavky na dodavatele kritické infrastruktury.**
- **Bezpečná varianta z pohledu požadavků výběrových řízení, často kvalifikační předpoklad.**

- **Předpoklad pro uzavírání a plnění bezpečnostních dodatků servisních smluv.**

Další praktickou výhodou je, že norma ISO 27001 zahrnuje všechny potřebné části z pohledu ISŘ v TECHSYS, tedy:

- Požadavky na integrovaný systém řízení.
- Technické požadavky na provoz.
- Požadavky na proces vývoj produktu.
- Požadavky na výrobu a servis.
- Požadavky na produkty.

5.2. POŽAFAVKY NA PROVOZ FIRMY

Požadavky na provoz firmy je možno rozdělit na následující kategorie i s uvedením konkrétních příkladů, konkrétních opatření.

5.2.1. Technické požadavky

- Fyzická bezpečnost (EZS, karty / klíče, evidence návštěv, pravidla pro pohyb zaměstnanců, atd.).
- Zajištění potřebného technického, HW a SW vybavení (UPS, Firewall, zálohovací systém, DFS, atd.).

5.2.2. Organizační požadavky

- Soustava procesních směrnic a bezpečnostních politik
- Vazba na běžné provozní procesy (jako správa budovy, ICT apod.)

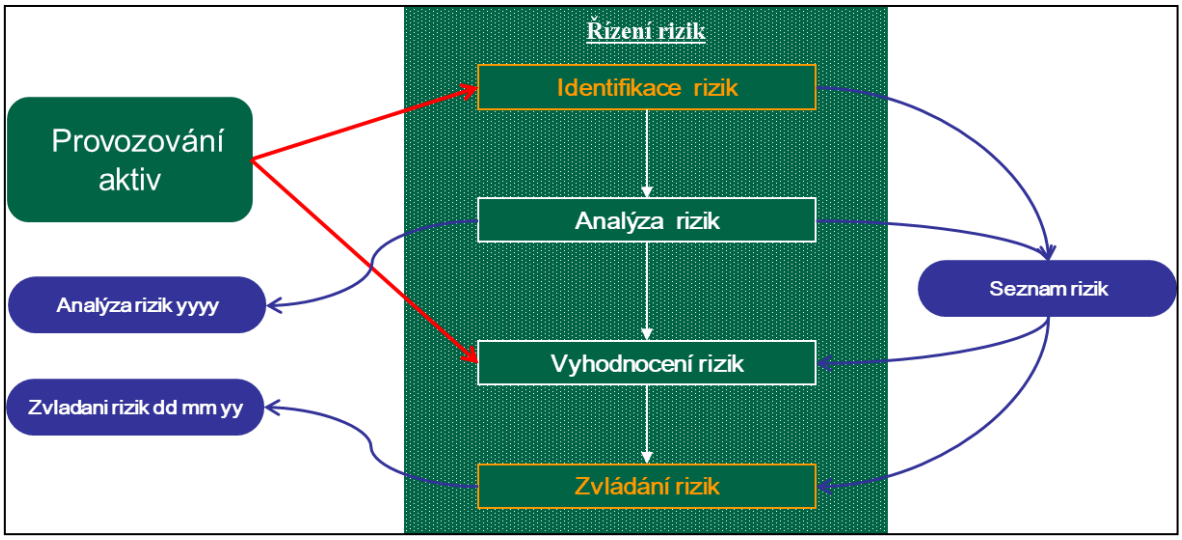
5.2.3. Prakticky prováděné činnosti

Prakticky prováděné činnosti jsou asi to nejzajímavější, pojďme se tedy zde podívat více do hloubky.

Které jsou tedy ty prakticky prováděné činnosti?

1. Systém kontrol
   a) Kontrola činností administrátora.
      - Kontrola prováděna v určené periodě.
      - Pokud je externí dodavatel, kontroluje se plnění bodů smlouvy.
   b) Penetrační test BSI (https://www.bsi.bund.de).
   c) Kontrola konfigurace aktivních prvků.
      - Kontrola prováděna v určené periodě.
      - Provádí se stažení aktuální konfigurace a porovná se se zálohou, čímž se dají zjistit případné změny.
   d) Kontrola konfigurace serverů, Kontrola UPS.
      - Např. pro UPS se v určené periodě prakticky otestuje funkčnost tím, že se provoz skutečně rozjede z UPS a ověří se požadované parametry.
   e) Kontrola zálohování.
   f) Kontrola konfigurace klientských stanic, Kontrola software.
      - Audit stanic.
   g) Kontrola havarijního plánu
      - Periodicky se provádí praktické zkoušení, že funguje. Např. se přiveze záložní diesel agregát a ověří se, že napájení firmy může být takto řešeno po dobu výpadku.

2. Vyhodnocování kontrol
    a) Provádí se periodicky (např. 1x za měsíc).
    b) V případě nalezení nedostatků se přijímají opatření.
3. Správa bezpečnostních incidentů
    a) Kritické incidenty se musejí hlásit na NÚKIB.
4. **Pravidelné audity systému a recertifikace.**
    a) Každý rok probíhají tzv. dozorové audity.
    b) 1x za 3 roky probíhá tzv. recertifikační audit.
5. Náročnost a náklady provozu.
    a) Všechny aktivity vedou k větší pracovní saturací odpovědných pracovníků (z pohledu pracnosti to znamená jednu osobu na plný úvazek).
    b) Audity a recertifikace jsou doprovázeny vlastními finančními náklady (typický odhad bývá 90MD/rok).
6. **Pravidelná analýza rizik a vyhodnocení. Probíhá dle následujícího schématu:**
    a) Identifikace rizik včetně příslušných aktiv a hrozeb.
    b) Analýza rizik a vyhodnocení rizik.
    c) Zvládání rizik – v tomto kroku se realizují navržená opatření ke snížení dopadu rizika.



obrázek 4 Struktura a vazby procesu Řízení rizik

5.3. POŽADAVKY NA VÝVOJ

Při návrhu systému se IT architekt musí řídit byznys požadavky, které mu byly při návrhu systému předloženy od zákazníka (tzv. funkční požadavky). Systém musí tyto požadavky naplnit, aby podporoval byznys cíle dané společnosti a v ideálním případě tvořil konkurenční výhodu. IT architekt však musí při návrhu systému myslet ještě na jednu skupinu požadavků, pokud chce vybudovat kvalitní a pro společnost konkurence-schopný software. Danou skupinou jsou nefunkční požadavky (NFR, resp. tzv. Service-level requirements, někdy také nazývány quality of service requirments). I tyto požadavky mají mnohdy kritický vliv na aplikaci, ale jejich samotným úkolem však není podpořit byznys cíle, ale vyvinout kvalitní stabilní aplikaci a její kvalitu měřit podle kritérií, kterých si u dané aplikace zákazník nejvíce cenní. Mezi základní požadavky patří výkon, škálovatelnost, spolehlivost, rozšiřitelnost, udržitelnost, spravovatelnost a bezpečnost. Při volbě požadavků, které jsou pro systém nejdůležitější, musejí architekt ve spolupráci se zákazníkem počítat s tím, že se jednotlivé požadavky vylučují navzájem. Chceme-li například navrhnout a realizovat systém, který si bude zakládat na vysokém výkonu, musíme obětovat požadavky, jako jsou udržitelnost a rozšiřitelnost. Musíme tedy počítat s tím, že rychlost naší aplikace bude vykoupena například tím, že v budoucnu budeme muset investovat více prostředků pro rozšíření dané aplikace o novou funkčnost.

5.3.1. Životní cyklus aplikace

Nyní bude praktické uvést životní cyklus aplikace. Nutno podotknout, že tyto principy jsou víceméně použitelné na obecný životní cyklus produkty a to jak SW, tak HW. Doplňme i části za bezpečnost, kterou popisuje **tzv. metodika bezpečného vývoje.**

1. Analýza a návrh – stanovení požadavků dle byznys požadavků, ale i **bezpečnostních požadavků a očekávaných hrozeb**. Funkční a nefunkční požadavky.
2. Implementace (realizace) – vývoj produktu na základě metodiky (např. interní).
3. Testování a ladění – z pohledu vývoje jde o zdrojový kód a funkč**nost, z pohledu bezpečnosti je to funkčnost a odolnost celé aplikace**.
4. Dokumentace – několikaúrovňová (programátorská, uživatelská), **z pohledu bezpečnosti jde především o zachování principu nahraditelnosti**.
5. Instalace – konfigurace okolního prostředí, nastavení správných parametrů **(včetně zabezpečení)**, **bezpečné a stabilní propojení s jinými aplikacemi**, distribuce nových verzí, vzájemné ovlivňování aplikací, atd.
6. Údržba resp. Provoz – **opravy chyb a bezpečnostních děr**, změny požadavků (jiná definice, legislativní změny), náklady na údržbu vs. cena nové aplikace.

5.3.2. Metodika bezpečného vývoje

Co tedy metodika bezpečného vývoje SW prakticky znamená? **Vymezuje základní aktivity a činnosti, které jsou nutné pro implementaci bezpečnosti do procesu Vývoj produktu.**

Jaké jsou hlavní zásady?

1. Specifikace požadavků na všechny kroky procesu, tedy na celý životní cyklus SW produktu – analýzu, realizaci, testování, dokumentaci a nasazení do produkce. (Provoz již není považován za vývojový krok).
2. Definice řízení přístupu – specifikace minimální sady rolí pro každou entitu (entitou je míněno: člověk, program, zařízení, …).
3. Zajištění **jednotného úložiště zdrojových kódů** (využití např. nástrojů jako GIT, CVS, atd.) – jedná se přímo o požadavek normy ISMS.
4. Ideálně zavedení tzv. Code Review – systematické zkoumání počítačového zdrojového kódu vedoucí ke zvýšení kvality SW (využití např. nástrojů jako GERRIT, …)

Dalším neopomenutelným hlediskem z pohledu procesu vývoj je personální bezpečnost. Co to znamená?

- Vývojářům nesmí být povoleno aktualizovat přímo ostrá data aplikace.
- Vývojářům nesmí být udělen přístup k personálním a jiným citlivým ostrým datům (výjimkou je např. souhlas zákazníka).
- Žádný vývojář nesmí být současně odpovědný za údržbu nebo opravy systémového programového vybavení (jinými slovy vývojář nesmí být tím, kdo danou aplikaci provozuje, udržuje nebo servisuje/spravuje).

Z pohledu vývoje a vlastní následného provozu aplikace je důležité také jasné oddělení vývoje, testu a provozu, konkrétně tedy:

- **Vývojové, integrační, testovací a provozní prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji.**
- **Provozní servery nesmí obsahovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.**
- **Testování a vývoj nových verzí Produktů se nesmí provádět v provozním prostředí.**

Implementace zásad bezpečnosti do procesu vývoj stanovuje rovněž rizika podle jejich stupně (Nízké, Střední, Vysoké). Stupeň rizika se stanovuje dle požadavků zákazníka. Stupeň vysoké se uplatňuje především u těch prvků, jež jsou vystaveny přímo na veřejném internetu. TECHSYS aktuálně tento stupeň nemusí řešit, jelikož naše produkty se uplatňují především v interních sítích a případná ochrana pro vysoký stupeň rizika probíhá na jiné úrovni v síti zákazníka (firewall, VPN, zabezpečený přístup, atd.)

Proces Vývoj produktu se v TECHSYS řídí dle následující tabulky s dané interní směrnice.

Implementace bezpečnosti do procesu Vývoj produktu		
Krok dle popisu procesu Vývoj produktu dle popisu produktu	**Nízké riziko**	**Střední riziko**
Převzetí a projednání požadavků na zahájení procesu a zpracování Zadání vývoje produktu (ZVP)	**Posouzení rizikovosti řešení**	
		Stanovení prováděných činností
Zpracování Návrhu řešení (NR)	Plán testování Definice bezpečnostních požadavků / mechanismů	Plán testování Definice bezpečnostních požadavků / mechanismů Identifikace rizik
Přezkoumání (NR)		
Vytvoření verze pro testy		Kontrola kódu Code review
Testování produktu dle požadavků NR	Ověření plnění bezpečnostních požadavků / mechanizmů	Penetrační testy a ověření plnění bezpečnostních požadavků / mechanizmů Ověření zapracování nálezů a chyb
Vytvoření verze pro validaci		
Validace produktu		Penetrační retesty

obrázek 5 Implementace bezpečnosti do procesu Vývoj produktu.

5.3.3. Role v bezpečném vývoji

Jaké role mají jednotlivé osoby vývojových týmů při bezpečném vývoji?

1. Manažeři nebo vedoucí
   a) Sledování trendů.
   b) Zavádění nebo aktualizace koncepce z pohledu bezpečnosti.
2. Project manažeři
   a) Systematický návrh aplikací s ohledem na bezpečnost.
3. Programátoři znalí bezpečného vývoje
   a) Identifikace zranitelností.
   b) Definice bezpečných postupů.
4. Programátoři noví v oblasti bezpečného vývoje
   a) Aktivní vzdělávání v oblasti bezpečného vývoje.
5. Software testeři
   a) Důraz na testování známých zranitelností.

5.3.4. Typické chyby při bezpečném vývoji

Dle portálu http://cwe.mitre.org patří mezi typické chyby při návrhu a vývoji aplikací následující chyby:

- SQL injection
- Buffer overflow
- Chybějící nebo špatná autorizace a oprávnění
- Používání zastaralých nebo nebezpečných šifrovacích algoritmů
- Špatné ošetření uživatelských vstupů

Tyto chyby se týkají všech druhů aplikací (Webové, nativní, server-side).

Pojďme se nyní u některých zastavit detailněji a zařaďme je mezi určité kategorie dle jejich charakteru a uveďme konkrétní příklady.

5.3.4.1. Nebezpečná interakce mezi komponentami

Mezi tyto typy patří

- SQL Injection and OS Command Injection
- Cross-site Scripting and Request Forgery
- Unrestricted Upload of File with Dangerous Type
- URL Open Redirect

Uveďme si příklad pro SQL Injection.

Co je to vlastně SQL Injection? Jedná se o jednu z nejběžnějších technik „hackování“ na WEBu, která může vést např. až ke zničení databáze. Jde umístění škodlivého SQL kódu do příkazů prostřednictvím neošetřeného vstupu na webové stránce.

Následující SQL dotaz má vypsat všechna data z tabulky pro uživatele s ID = 1234.

SELECT * FROM Users WHERE ID=1234

Co se ale stane v případě, že se útočníkovi podaří na konec příkazu „propašovat“ kód ***OR 1=1*** (např. pomocí jednoduchého skládání dotazu zřetězením)? Výsledný dotaz bude vypadat takto:

SELECT * FROM Users WHERE ID=1234 OR 1=1

… a vypíše všechna data z tabulky Users. Pokud šlo např. o tabulku obsahující uživatelská jména a hesla, pak získal útoční kompletní přístup k veškerým přístupovým údajům od vybrané entity.

Jak se bránit? Metod je několik. Jednou z nich je např. užívání SQL parametrů pro ochranu vstupních dat. Jednotlivé parametry mohou být testovány a hlavně je jejich význam omezen za zcela konkrétní rozsah a SQL dotaz tak skončí chybou.

obrázek 6 SQL Injection.

5.3.4.2. Riskantní správa zdrojů

Mezi tyto typy patří

- „Classic“ Buffer Overflow
- Path Traversal
- Download of Code Without Integrity Check

- Inclusion of Functionality from Untrusted Control Sphere
- Use of Potentially Dangerous Function
- Incorrect Calculation of Buffer Size
- Uncontrolled Format String
- Integer Overflow or Wraparound

Stručně si popišme pouze poslední jmenovaný a tím je „Integer overflow“ nebo-li přetečení čísla, které se u počítačů stává ve chvíli, kdy se snažíme do určitého datového typu umístit číslo, jež je větší než maximum, které je schopen daný datový typ reprezentovat. Např. do 16-ti bitového typu umístíme maximálně číslo 65535. Pouhým přičtením čísla 1 k tomuto maximum bude výsledek 0, jelikož došlo k přetečení. Takováto chybná práce s čísly nebo špatný návrh datových struktur může vést k dalším efektům: chybný výsledek matematické operace nebo alokace chybné velikosti paměti pro umístění dat určité délky a tím k přepsání paměti. Tato chyba vedla např. ke zničení rakety Ariane 5 v roce 1996. Programátor konvertoval 64-bitové floating-point číslo na 16-ti bitový znaménkový Integer, kde po dosažení maximální hodnoty 32767 došlo k přetečení, což mělo fatální následky. Více zde: https://en.wikipedia.org/wiki/Cluster_(spacecraft)

5.3.4.3. „Děravá“ obrana

Mezi tyto typy patří:

- Missing Authentication for Critical Function
- Missing Authorization
- Use of Hard-coded Credentials
- Missing Encryption of Sensitive Data
- Reliance on Untrusted Inputs in a Security Decision
- Execution with Unnecessary Privileges
- Incorrect Authorization
- Incorrect Permission Assignment for Critical Resource
- Use of a Broken or Risky Cryptographic Algorithm
- Improper Restriction of Excessive Authentication Attempts
- Use of a One-Way Hash without a Salt

Popišme si první příklad tedy „Missing Authentication for Critical Function“, tedy chybějící autentizace pro kritickou funkci. Zranitelnost umožňuje vzdálenému NE-ověřenému útočníkovi odeslat speciálně vytvořený požadavek dotčené aplikaci na konfigurační změny nebo na získání administrátorského přístupu, čím ovládne celý systém.

5.4. POŽADAVKY NA VÝROBU A SERVIS

Bezpečnostní požadavky se z pohledu servisní činnosti projevují především v zohlednění bezpečnostních příloh servisních smluv.

- Slouží k zajištění bezpečnostních opatření poskytovatele.
- Definují bezpečnostně provozní požadavky.
- Definují také bezpečnostní požadavky na vývoj SW (Hot Fixy, požadavky metodiky bezpečného vývoje).
- Definují požadavky na systémovou a provozní bezpečnostní dokumentaci.
- Řeší fyzickou ochranu a bezpečnost prostředí.
- Určují řízení přístupu a požadavky na monitorování.
- Popisují způsob výměny informací.
- Popisují zvládání bezpečnostních incidentů.

Výše uvedené body jsou platné i pro činnost oddělení výroby.

Dále uveďme další body týkající se čistě výroby:

1. Politika fyzického přístupu v rozsahu:
    a) Fyzický bezpečnostní perimetr
    b) Fyzické kontroly vstupu
    c) Zabezpečení kanceláří, místností a vybavení
    d) Ochrana před vnějšími hrozbami a hrozbami prostředí
    e) Práce v zabezpečených oblastech
    f) Oblasti pro nakládku a vykládku
2. Politika bezpečnosti informací pro dodavatelské vztahy v rozsahu:
    a) Iniciace
    b) Hodnocení
    c) Smlouva o úrovni služeb (SLA)
    d) Bezpečnostní požadavky na externího dodavatele
    e) Dohoda o kontrole shody a dotazování
    f) Řízení přístupů, autentizace a správa uživatelů

5.5. POŽADAVKY NA PRODUKTY

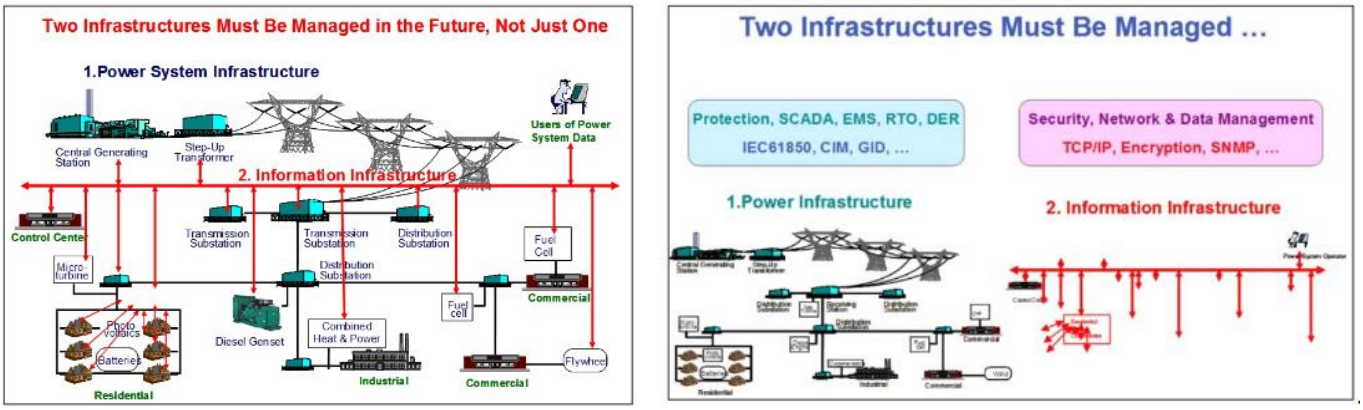
Požadavky na produkty vycházejí z obecných standardů kybernetické bezpečnosti, metodiky bezpečného vývoje a specifických bezpečnostních požadavků daného produktu, aplikace a koncového zákazníka.

Uveďme ty nejpodstatnější požadavky kladené na produkty:

1. **Vývoj a testování dle přijatých standardů.**
    a) **Dodržování metodiky bezpečného vývoje.**
    b) **Prokazatelné otestování na nezávislém testovacím prostředí.**
2. **Logování činnosti administrátorů a uživatelů.**
    a) **Auditní LOG.**
    b) **Spolupráce se SIEM** (Security Information and Event Management = management bezpečnostních informací a událostí). SIEM v reálném čase umožňuje analýzu bezpečnostních alertů, které generují síťová zařízení a aplikace. SIEM řešení zpravidla je postaveno na bázi aplikace, služeb a potřebného zařízení - tento základ konzumuje záznamy bezpečnostních dat (logy) a generuje reporty.
3. **Správa uživatelů navázána na AD/LDAP (Active Directory/ Lightweight Directory Access Protocol)**
    a) **Přidělování uživatelských rolí a oprávnění.**
    b) **Single Sign On (SSO).** SSO centralizuje autentizační proces uživatele do jednoho místa nazývaného také poskytovatel identity. Poskytovatel identity dělá autentizaci uživatele a tyto údaje pak poskytuje ostatním aplikacím (nazývaným též poskytovatelé služeb), které uživatel běžně používá**.**
4. **Konkrétní technické požadavky na provoz**
    a) **Zabezpečení síťových komunikací.**
    b) **Ochrana proti vnějším útokům.**
    c) **Šifrování.**
    d) **Zabezpečení telemetrických komunikací (IEC 62351).**

5.5.1. IEC 62351

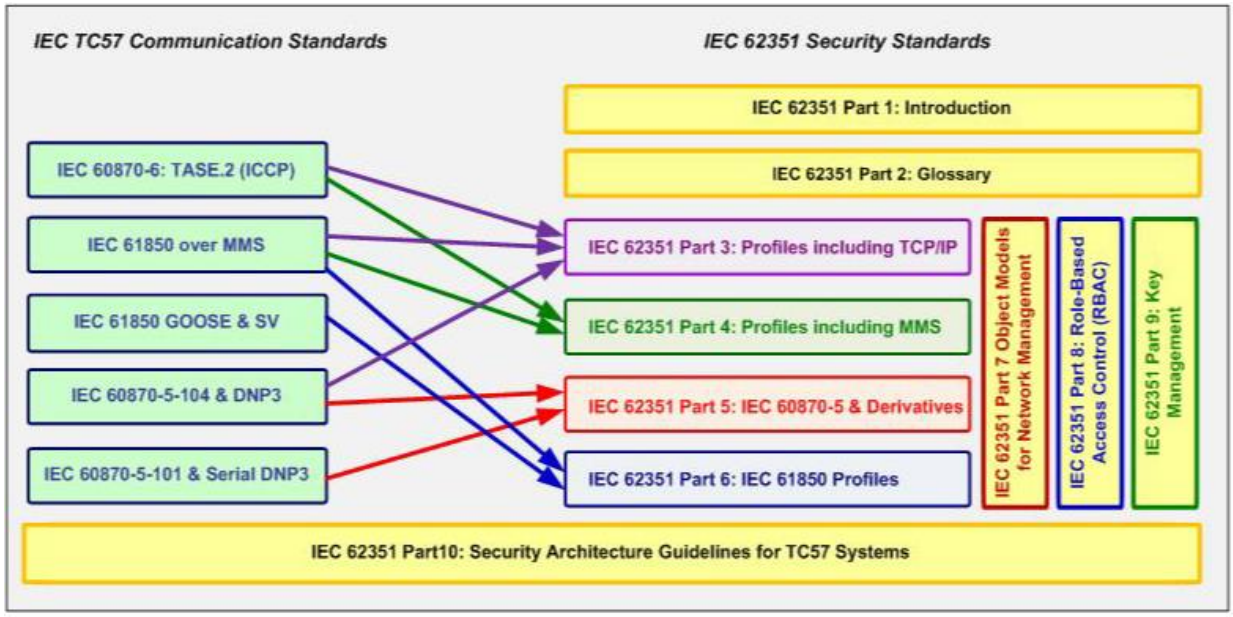
Již dávno si lidé uvědomili, že energetika není jen infrastrukturou silovou, ale rovněž informační, jelikož zde byly a jsou stále větší požadavky na dostupnost, přesnost a věrohodnost informací pro řízení elektrizační soustavy. Dekompozici celkové infrastruktury na obě zmíněné pěkně popisuje následující obrázek převzatý z dokumentu „IEC 62351 Security Standards for the Power Systém Information Infrastructure“. Je zde vysvětleno, že starý koncept „Security by Obscurity“ (tedy většinou proprietární řešení) je z dnešního pohledu již dávno přežitý a z řady důvodů se přešlo na standardní řešení.



obrázek 7 Energetická a ICT infrastruktura.

IEC 62351 je standard vyvinutý technickou komisí IEC 57 (IEC TC57) pro řešení bezpečnosti u protokolů rodin IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61968 + IEC61970 a IEC 61334 (DLMS). IEC komise 57 je zodpovědná za vývoj standardů pro výměnu informací u systémů používaných v energetice a u systémů příbuzných.

Neexistuje přímá vazba 1:1 mezi komunikačními standardy IEC TC57 a bezpečnostním standardem IEC62351. Vazby popisuje následující obrázek.

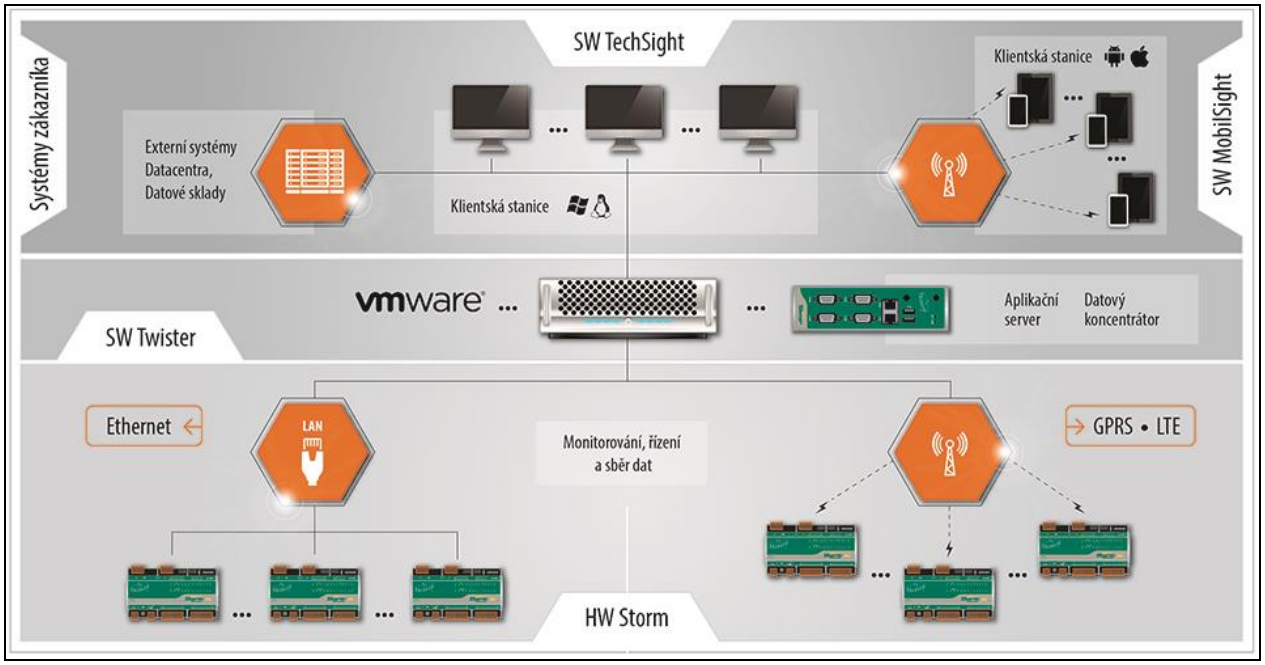


obrázek 8 Vazba mezi IEC 62351 a IEC TC57.

Např. z pohledu známého komunikačního protokolu IEC60870-5-104 jsou nevýznamnější části 3 a 5 ze standardu IEC 62351. Část 3 popisuje zabezpečení proti odposlechu pomocí TLS kryptování, část 5 doplňuje autentizaci.

5.5.2. Příklady produktů splňujících bezpečnostní požadavky

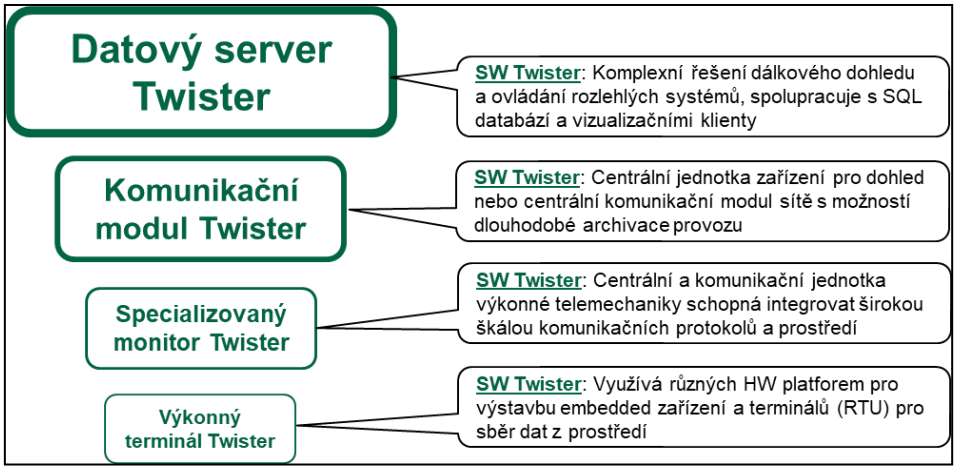
Kompletní produktová řada společnosti TECHSYS.



obrázek 9 Produktový koncept TECHSYS.

5.5.2.1. SW balík Twister – SW pro využití ve SCADA

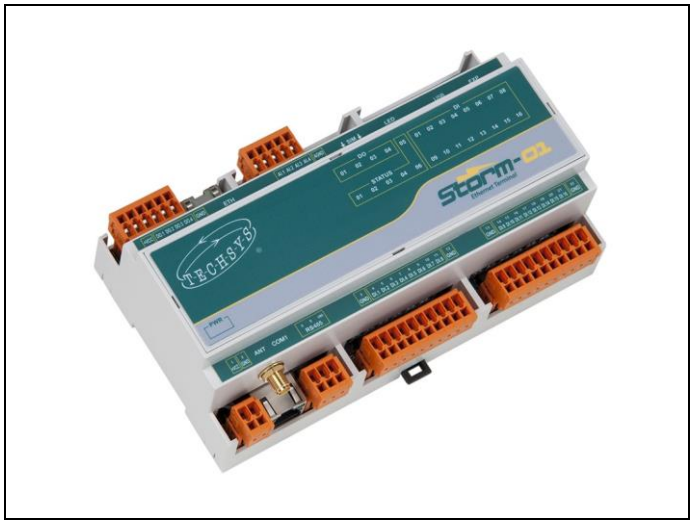
- Škálovatelný, modulární, multiplatformní.
- Vývoj a testování dle přijatých standardů.
- Logování činnosti administrátorů a uživatelů.
- Správa uživatelů navázána na AD/LDAP.
- Konkrétní technické požadavky na provoz.
- Bezpečnost komunikací dle IEC 62351.
- Univerzální použití ve SCADA.



obrázek 10 SW Twister.

5.5.2.2. Rodina RTU Storm – RTU pro monitorování a řízení, měřící převodníky

- Systém reálného času, modulární, řada rozšiřujících modulů.
- Vývoj a testování dle přijatých standardů.
- Logování činnosti administrátorů a uživatelů.
- Správa uživatelů navázána na AD/LDAP.
- Konkrétní technické požadavky na provoz.
- Bezpečnost komunikací dle IEC 62351.



obrázek 11 RTU Storm-01.

6. LITERATURA

[1] Interní materiály ISŘ firmy TECHSYS.

[2] Dokumentace procesu vývoj produktu TECHSYS.

[3] https://www.govcert.cz

[4] http://www.psp.cz

[5] https://cs.wikipedia.org

[6] http://cwe.mitre.org

[7] http://iectc57.ucaiug.org/wg15public

Ing. Jindřich Zoubek, MBA

V r. 2005 ukončil studium na ČVUT, elektrotechnické fakultě v Praze, obor Výpočetní technika, se zaměřením na systémové programování, operační systémy a sítě.

Od r. 2001 pracuje ve společnosti **TECHSYS – HW a SW, a.s.**, www.techsys.cz, kde prošel různými pozicemi v oddělení vývoje. Rovněž vedl nebo byl členem realizace těch nejvýznamnějších projektů.

Od r. 2015 je členem managementu a vrcholného vedení společnosti, se zodpovědností za obchodní a marketingovou činnost.

Kontakt: Tel.: +420 222 541 896, e-mail: zoubek@techsys.cz