Název předmětu: Kybernetická bezpečnost

Téma: 2. Normy a zákony kybernetické bezpečnosti. Ochrana utajovaných informací a určení neutajovaných informací

Cíl: Cílem je seznámit studenty s platnými normami, zákony, vyhláškami a nařízeními v oblasti kybernetické bezpečnosti, s jejich základním obsahem. Seznámení se zákonem k ochraně utajovaných informací. Seznámení s obsahem významu neutajovaná informace.

Úkoly pro samostatnou práci: Zopakovat si platné normy, zákony, vyhlášky a nařízení v oblasti kybernetické bezpečnosti. Zopakovat si zákon k ochraně utajovaných informací. Zopakovat si obsah pojmu neutajovaná informace.

Studijní literatura:

1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
2. 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)
3. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
4. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
5. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
6. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
7. Normy řady ISO / IEC 27000
8. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
9. aktuální zákony, vyhlášky a normy z oblasti kybernetické bezpečnosti

Obsah:

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Dne 29. srpna 2014 vstoupil v platnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Zákon vstoupil v účinnost 1. ledna 2015. V roce 2017 proběhly dvě obsahově významné novely zákona o kybernetické bezpečnosti a to prostřednictvím zákona č. 104/2017 Sb. s účinností od 1. července a zákona č. 205/2017 Sb. s účinností od 1. srpna 2017. Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušné předpisy Evropské unie (jedná se o transpozici směrnice NIS) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

Hlavním cílem zákona je:

- stanovit základní úroveň bezpečnostních opatření,
- zlepšit detekci kybernetických bezpečnostních incidentů,
- zavést hlášení kybernetických bezpečnostních incidentů,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť.

Původní znění zákona nabylo účinnosti 1. ledna 2015, aktuální znění zákona je účinné od 7. března 2018.

Zákon je dostupný na stránkách NÚKIB pod tímto odkazem:

- Zákon o kybernetické bezpečnosti

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)

Dne 6. července 2016 byla uveřejněna směrnice Evropského parlamentu a Rady (EU) 2016/1148 (dále jen „směrnice NIS“). Tato směrnice má za cíl harmonizovat právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti s cílem zlepšení fungování vnitřního trhu.

Některé povinnosti, které směrnice NIS ukládá, jsou v České republice zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcími předpisy již řešeny.

Směrnice NIS mimo jiné rozšiřuje okruh subjektů, pro které budou stanoveny povinnosti v oblasti ochrany a prevence před kybernetickými bezpečnostními incidenty – jedná se o tzv. provozovatele základní služby a poskytovatele digitálních služeb (internetové vyhledávače, cloud computing a online tržiště). Požadavky směrnice zapracovává novela zákona o kybernetické bezpečnosti cestou zákona č. 205/2017 Sb. s účinností od 1. srpna 2017.

Směrnice NIS je dostupná na oficiálních stránkách EU pod tímto odkazem:

- Směrnice NIS

Vyhláška o kybernetické bezpečnosti

Tato vyhláška zapracovává Směrnici NIS a pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,

- typy, kategorie a hodnocení významnosti 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,
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

Dostupná verze vyhlášky:

- Nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Dne 19. prosince 2014 vstoupila v platnost vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. Vyhláška stanoví významné informační systémy a kritéria pro jejich určení.

Tato vyhláška nabyla účinnosti 1. ledna 2015.

Vyhláška je dostupná na stránkách NÚKIB pod tímto odkazem:

- Vyhláška o významných informačních systémech

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Nařízení vlády je platné od 30. prosince 2010. Nařízení vlády definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury. V příloze k nařízení vlády je definováno 9 odvětví, včetně jednotlivých odvětvových kritérií pro určení prvku kritické infrastruktury.

Toto nařízení vlády nabylo účinnosti 1. ledna 2011. V souvislosti se zahrnutím oblasti kybernetické bezpečnosti do odvětvových kritérií proběhla novela nařízením vlády č. 315/2014 Sb., s účinnosti od 1. ledna 2015.

Nařízení vlády je dostupné na stránkách NÚKIB pod tímto odkazem:

- Nařízení vlády o kritériích pro určení prvku kritické infrastruktury (vč. kritické informační infrastruktury)

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Dne 15. prosince 2017 byla ve Sbírce zákonů České republiky vydána nová vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s odbornou veřejností. Vyhláška zapracovává požadavky 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).

Vyhláška 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.

Vyhláška nabývá účinnosti dne 1. února 2018.

Vyhláška byla rozeslána stejnopisem částky Sbírky zákonu České republiky č. 157/2017 dne 15. prosince 2017. Tato částka Sbírky zákonů České republiky je dostupná zde:

- http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=437/2017&typeLaw=zakon&what=Cislo_zakona_smlouvy

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby je dále dostupná zde:

- http://www.psp.cz/sqw/sbirka.sqw?cz=437&r=2017

Prováděcí nařízení EK ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb

Dne 31. ledna 2018 zveřejnila Evropská komise prováděcí nařízení komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS). Toto prováděcí nařízení obsahuje bližší upřesnění bezpečnostních opatření, které musí poskytovatelé digitálních služeb (§ 3 písm. h) podle ZKB) zohledňovat při řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, a dále bližší upřesnění parametrů pro posuzování toho, zda je dopad incidentu významný. Toto prováděcí nařízení je účinné od 10. května 2018 a je přímo aplikovatelné. Pro poskytovatele digitálních služeb je tedy závazné.

Řada norem ISO/IEC 27000

ISO (International Organization for Standardization) rezervovala sérii ISO 27000 pro normy z oblasti bezpečnosti informací. Podobně, jako tomu je u norem pro řízení kvality série ISO 9000. Na základě standardu “ISO Guide 83” publikovaného v dubnu 2012, mají všechny standardy rodiny 27K definovanou jednotnou strukturu a pravidla pro začlenění specifických požadavků.

Do této doby byly publikovány následující normy:

- ISO 27000 - definuje pojmy a terminologický slovník pro všechny ostatní normy z této série.
- ISO 27001 (BS7799-2) - hlavní norma pro Systém řízení bezpečnosti informací (ISMS), dříve známá jako BS7799 část 2, podle které jsou systémy certifikovány. Poslední revize normy byla publikována v říjnu 2013.
- ISO 27002 (ISO/IEC 17799 & BS7799-1) - norma byla prvně publikována v červnu 2005 jako ISO/IEC 17799:2005. V červenci 2007 došlo k jejímu přejmenování na ISO/IEC 27002:2005, kdy obsah předchozí normy byl zachován. Poslední revize normy byla vydána v říjnu 2013.
- ISO 27003 - návod pro návrh a zavedení ISMS v souladu s ISO 27001.
- ISO 27004 - norma byla publikována v roce 2009 a následně revidována v roce 2016. Normu přeložila společnost Risk Analysis Consultants.
- ISO 27005 - norma byla publikována v červnu 2008 pod názvem "Information technology - Security techniques - Information security risk management" a následně v červnu 2011 revidována. Normu přeložila společnost Risk Analysis Consultants. Český překlad je k dispozici na stránkách ÚNMZ.
- ISO 27006 - norma byla poprvé publikována v březnu 2007 a naposledy revidována v roce 2015. Normu přeložila společnost Risk Analysis Consultants. Český překlad je k dispozici na stránkách ÚNMZ.
- ISO 27007 - revize normy byla publikována v roce 2017 pod názvem "Information technology - Security techniques - Guidelines for information security management systems auditing".
- ISO 27008 - norma byla publikována v listopadu 2011 pod názvem "Information technology - Security techniques - Guidelines for auditors on information security management systems controls". Obsahuje doporučení auditorům ISMS a doplňuje ISO 27007.
- ISO 27009 - norma byla publikována v roce 2016 pod názvem " Information technology - Security techniques - Sector-specific application of ISO/IEC 27001 - Requirements" Definuje požadavky pro používání ISO/IEC 27001 ve specifických odvětvích.
- ISO 27010 - norma byla publikována v dubnu 2012 a revidována v roce 2015. Poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci.
- ISO 27011 - norma byla publikována v roce 2008 a revidována v roce 2016. Obsahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- ISO 27013 - norma byla publikována v říjnu 2012. Norma poskytuje doporučení pro implementaci ISO/IEC 20000 a ISO/IEC 27001. Poslední revize normy byla vydána v prosinci 2015.
- ISO 27014 - norma byla publikována v první polovině roku 2013 pod názvem "ITU-T Recommendation X.1054 & ISO/IEC 27014:2013 Information technology - Security techniques - Governance of information security". Norma organizacím poskytuje doporučení při návrhu Information Security Governance.
- ISO 27015 - norma byla publikována v listopadu 2012 pod názvem "ISO/IEC TR 27015:2012 Information technology - Security techniques - Information security management guidelines for financial services".Obsahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí finančních institucí (banky, pojišťovny apod.).
- ISO 27016 - norma byla publikována v roce 2014 jako technická zpráva (Technical Report) pod názvem ISO/IEC TR 27016:2014 - IT Security - Security techniques -

Information security management – Organizational economics. Poskytuje doporučení pro nastavení bezpečnostního programu s ohledem na předpokládané finanční výsledky.

- ISO 27017 - norma byla publikována na koci roku 2015 pod názvem ISO/IEC 27017:2015 / ITU-T X.1631 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services a poskytuje doporučení pro zabezpečení cloud computingu
- ISO 27018 - norma byla publikována v srpnu 2014 pod názvem ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors. Poskytovatelům cloudových služeb dává vhodná bezpečnostní opatření pro zabezpečení soukromí zákazníků.
- ISO 27019 - revize normy byla publikována v roce 2017 pod názvem"ISO/IEC 27019:2017 - Information technology - Security techniques - Information security controls for the energy utility industry". Norma pomáhá organizacím v energetickém průmyslu interpretovat a aplikovat normu ISO/IEC 27002, aby byla zajištěna bezpečnost jejich systémů pro elektronické řízení procesů.
- ISO 27021 - norma byla publikována v říjnu 2017 pod názvem ISO/IEC 27021:2017 - Information technology - Security techniques - Competence requirements for information security management systems professionals. Norma stanovuje požadavky na odbornou způsobilost specialistů z oblasti ISMS.
- ISO 27023 - norma byla publikována v červenci 2015 pod názvem ISO/IEC TR 27023:2015 Information technology - Security techniques - Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002 a srovnává poslední vydání norem ISO/IEC 27001 a ISO/IEC 27002 s vydáními předchozími.
- ISO 27031 - norma byla publikována v březnu 2011 pod názvem "ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity". Obsahuje doporučení pro zajištění kontinuity činností organizace (business continuity).
- ISO 27032 - norma pod označením "Guidelines for cybersecurity" vyšla v červnu 2012, obsahuje bezpečnostní doporučení týkající se kyberprostoru.
- ISO 27033 - soubor norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí. Prozatím bylo vydáno šest částí normy.
- ISO 27034 - soubor norem poskytující doporučení pro bezpečnou tvorbu, implementaci a užívání aplikačního softwaru. Byly vydány čtyři části normy.
- ISO 27035 - revize normy byla publikována v roce 2016 pod názvem "Information security incident management". Norma se věnuje řízení incidentů bezpečnosti informací.
- ISO 27036 - soubor norem publikovaný v roce 2013 pod názvem "Information security for supplier relationships" poskytuje doporučení pro hodnocení a řízení informačních rizik spojených s pořizováním zboží a služeb od dodavatelů.
- ISO 27037 - norma byla publikována v říjnu 2012 pod názvem "ISO/IEC 27037:2012 - Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence". Norma obsahuje doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů.
- ISO 27038 - norma byla publikována v roce 2014 pod názvem "ISO/IEC 27038:2014 - Information technology - Security techniques - Specification for digital redaction". Norma obsahuje doporučení pro publikování digitálních dokumentů.
- ISO 27039 - norma byla publikována v roce 2015 pod názvem "ISO/IEC 27039:2015 - Information technology - Security techniques - Selection, deployment and operation of intrusion detection [and prevention] systems (IDPS)" a obsahuje doporučení pro výběr,

nasazení a provoz systémů pro detekci a prevenci bezpečnostních průniků (Intrusion Detection and Prevention Systems - IDPS).

- ISO 27040 - norma byla publikována v roce 2015 pod názvem "ISO/IEC 27040:2015 - Information technology - Security techniques - Storage security" a obsahuje doporučení pro bezpečné ukládání dat.
- ISO 27041 - norma byla publikována v roce 2015 pod názvem "ISO/IEC 27041:2015 - Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative methods" a obsahuje doporučení pro výběr forenzních metod pro zajištění a zkoumání digitálních důkazů.
- ISO 27042 - norma byla publikována v roce 2015 pod názvem "ISO/IEC 27042:2015 - Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence" a obsahuje doporučení pro analýzu a vyhodnocování digitálních důkazů.
- ISO 27043 - norma byla publikována v roce 2015 pod názvem "ISO/IEC 27043:2015 - Information technology - Security techniques - Incident investigation principles and processes" a shrnuje zásady a postupy při vyšetřování incidentů s využitím digitálních důkazů.
- ISO 27050 - soubor norem publikovaný v roce 2016 pod názvem "Electronic discovery" se zabývá problematikou zkoumání elektronických stop (Electronic discovery).
- ISO 27799 - doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

- Zákon č. 412/2005 Sb.

Pro účely tohoto zákona se rozumí:

a) utajovanou informací informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací (§ 139),

b) zájmem České republiky zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob,

c) porušením povinnosti při ochraně utajované informace porušení povinnosti uložené tímto zákonem nebo na základě tohoto zákona,

d) orgánem státu organizační složka státu podle zvláštního právního předpisu, kraj, hlavní město Praha, městská část hlavního města Prahy a obec při výkonu státní správy ve věcech, které stanoví zvláštní právní předpis; orgánem státu se rozumí i Bezpečnostní informační služba, Vojenské zpravodajství a Česká národní banka,

e) odpovědné osoby (výpis odpovědných osob od ministerstvech až po podnikající fyzické osoby),

f) původcem utajované informace orgán státu, právnická osoba nebo podnikající fyzická osoba, u nichž utajovaná informace vznikla, nebo Úřad průmyslového vlastnictví podle § 70 odst. 4,

g) cizí mocí cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán,

h) neoprávněnou osobou fyzická nebo právnická osoba, která nesplňuje podmínky přístupu k utajované informaci stanovené tímto zákonem,

i) poučením písemný záznam o seznámení fyzické osoby s jejími právy a povinnostmi v oblasti ochrany utajovaných informací a s následky jejich porušení,

j) bezpečnostním standardem utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací,

k) bezpečnostním provozním módem prostředí, ve kterém informační systém pracuje, charakterizované stupněm utajení zpracovávané utajované informace a úrovněmi oprávnění uživatelů.

Utajovaná informace se klasifikuje stupněm utajení:

a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,

b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,

c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,

d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

Druhy zajištění ochrany utajovaných informací

Ochrana utajovaných informací je zajišťována:

a) personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,

b) průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,

c) administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,

d) fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,

e) bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému a

f) kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.

Určená neutajovaná informace

Při zařazení informace do kategorie určená neutajovaná informace musí provést původce (vlastník informace, zpracovatel) posouzení, zda neautorizované použití, modifikace, zničení nebo ztráta zpracovávané informace mohou způsobit narušení služebního zájmu, oprávněných zájmů osob nebo jinou škodu. Zároveň musí posoudit, zda daná informace nepodléhá zvláštní ochraně podle *zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve smyslu nařízení vlády č. 522/2005 Sb. ve znění nařízení vlády č. 240/2008 Sb., kterým se stanoví seznam utajovaných informací*.