Informace jsou jako pytel blech

PRO-ENERGY | 1.12.2017 | Rubrika: Elektro - energetika | Strana: 20 | Autor: Milena Geussová | Téma: Masarykova univerzita, vysoké školy

Některé věci byly dřív jen sci-fi. Dnes je to realita, říká Jan Šmolík, manažer bezpečnosti informací ČEPS, a vysvětluje, jak se s kybernetickými hrozbami vyrovnává provozovatel elektroenergetické přenosové soustavy.

* Od srpna funguje Národní úřad pro kybernetickou bezpečnost a letos byl také novelizován zákon o kybernetické bezpečnosti. Jaké změny to přineslo pro ČEPS?

Ani dvě novely zákona o kybernetické bezpečnosti, ani vznik nového úřadu neměly na nastavenou spolupráci s naší společností žádný vliv. Nepřibyly nám nové povinnosti. S úřadem trvale komunikujeme a spolupracujeme, jako například při určování prvků kritické informační infrastruktury nebo výkladu zákona. Jsem mile překvapen vstřícností jeho pracovníků a oceňuji jejich kvalifikaci pro tuto oblast. Velkou zkušenost získávám osobně také tím, že jsem se stal členem expertního týmu, který se podílí na novele vyhlášky o kybernetické bezpečnosti.

* Kdo odpovídá za celkovou bezpečnostní politiku v ČEPS?

Odpovědnost za bezpečnost je zakotvena v interní řídící dokumentaci, v Bezpečnostním řádu, kde jsou stanoveny jednotlivé role, odpovědnosti a pravomoci. Za společnost je odpovědný předseda představenstva, který deleguje odpovědnost na bezpečnostního ředitele. Za jednotlivé oblasti bezpečnosti jsou odpovědné další defi nované role.

* Některé informace je třeba chránit ve zvláštním režimu. Jak u vás fungují procesy spojené s utajovanými skutečnostmi?

Řídíme se zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti. Shodou okolností nám nově vzniklý úřad přidělil certifikát s pořadovým číslem jedna, který společnosti ČEPS umožňuje zpracovávat dokumenty obsahující utajované informace. Podle tohoto certifikátu s nimi můžeme nakládat do stupně Vyhrazené. Vyzrazení takového dokumentu by mohlo znevýhodnit zájmy ČR.

* Jak poznáte, že určité informace by neměly být veřejné?

Máme defi nované tři klasifikační stupně informací. Klasifikační stupeň určuje vlastník informace. Nejnižší stupeň je stanovený pro informace určené ke zveřejnění. Další dva stupně mají nastavená různá pravidla, jak s těmito informacemi pracovat v listinné a elektronické podobě a při přenosu mluveným slovem. Jejich zveřejnění by mohlo mít negativní dopad na společnost. Jedná se např. o porušení zákonných povinností, smluvních ujednání a z toho plynoucích sankcí, reputační dopad, případný dopad do poskytování našich služeb. Informace jsou jako pytel blech. Dají se lehce sdílet, neznají hranice a není žádoucí, aby se dostaly do nepovolaných rukou. Proto musíme mít taková opatření, abychom je opravdu chránili.

* Nejslabším článkem bývají lidé. Jakým způsobem riziko jejich selhání snižujete?

Lidský faktor hraje významnou roli a je třeba průběžně zvyšovat povědomí zaměstnanců v oblasti kybernetické a informační bezpečnosti. Každý nový pracovník projde vstupním školením, kde se seznámí se základními pravidly při práci s výpočetní technikou, jak a podle čeho pozná bezpečnostní události nebo incidenty a kam je má hlásit. Každý rok musí zaměstnanci absolvovat e-learningový kurz a na intranetu také zveřejňujeme články na aktuální bezpečnostní témata. Pro správce infrastruktury pořádáme kybernetická cvičení. Cílem je procvičit si řešení krizových situací,

komunikaci s uživateli a nadřízenými, spolupráci a koordinaci v týmu pod narůstajícím tlakem, postupy podle zákona o kybernetické bezpečnosti a ochraně osobních údajů. Cvičení probíhají například v **Kybernetickém polygonu na Masarykově univerzitě v Brně**.

* Jak zajistíte bezpečnost při práci externích firem v ČEPS?

Zákon o kybernetické bezpečnosti nám ukládá přenést bezpečnostní požadavky na dodavatele služeb pro prvky kritické informační infrastruktury formou smluvního ujednání. Jejich míra vychází z analýzy rizik a z rozsahu poskytovaných služeb. Novela zákona o kybernetické bezpečnosti nám umožňuje přenést přímo regulatorní požadavky na tyto dodavatele. Osobně to vnímám jako pozitivní krok.

* V čem se proměnila analýza rizik, spojených s přenosovou soustavou, oproti minulosti? Přicházejí rizika nová?

Na jedné konferenci mne zaujal následující výrok: „Bezpečnost jako taková není o bezpečnosti, ale o řízení rizik.“ Je to kontinuální proces, ve kterém je třeba zohlednit aktuální a nové příchozí hrozby a odpovídajícím způsobem reagovat. Svět je globalizován. Kybernetické útoky neznají hranic. Je třeba na to být připraven.

* ČEPS funguje v propojeném světě přenosu elektřiny, propojují se také kybernetické hrozby?

S tím, jak se mění svět, mění se také pohled na bezpečnost. Historicky byl koncept bezpečnosti postaven na fyzickém zabezpečení objektů. Pohybujeme se však ve světě daleko více závislém na informačních a řídicích systémech. Proto je zvýšená pozornost věnovaná kybernetické a informační bezpečnosti. Ta je postavená na pilířích „bezpečnost ICT“, „personální bezpečnost“ a „fyzická bezpečnost“ a je řízená prostřednictvím řízení rizik. Varovné byly například loňské výpadky přenosové soustavy na Ukrajině, které způsobil kybernetický útok. Ten byl připravován dlouhodobě a dodnes se spekuluje, kdo za ním stál a zda nešlo jen o jakousi přípravnou akci před širším využitím. K tomu, jak zanést do informačních systémů škodlivé kódy, lze využít nejrůznějších metod. Oblíbenou, ne příliš nákladnou a hlavně dostatečně účinnou formou je sociální inženýrství. Je znám případ, kdy pachatelé rozházeli na podnikovém parkovišti pověstné zavirované fl ešky. Lidská zvědavost a pokušení pracuje pro útočníky. Je jen otázkou času, kdy někdo ze zaměstnanců vloží fl ešku do pracovního počítače a dílo je dokonáno.

* Zaznamenali jste už nějaké pokusy o narušení kybernetické bezpečnosti? Už jste se s takovým incidentem setkali v ČEPS?

Zatím jsme nezaznamenali takovou událost nebo incident, který bychom dle zákona měli hlásit. Naše bezpečnostní infrastruktura detekuje robotické skenování našeho internetového perimetru, což je rozhraní mezi kybernetickým prostorem a naší společností. Průchody pro komunikaci s okolním světem musíme mít nastaveny tak, aby byly bezpečné.

* Nejsou dnes některé firmy či úřady příliš bezstarostné?

V energetice to určitě neplatí. Domnívám se, že profesní uvědomění je u lidí v energetice a zvláště v přenosové soustavě naprosto zakořeněné. Bezpečnost a spolehlivost je nedílnou součástí naší společnosti. Je to součást firemní kultury.

* Co když se něco stane v nějaké sousední zemi? Jsme před tím chráněni?

V roce 2015 se naše společnost účastnila procesního cvičení CMX NATO. Část scénáře byla postavena na kybernetickém útoku na polského a následně českého provozovatele přenosové soustavy s následným dopadem na udržení řádného fungování přenosových soustav v rámci dispečerského řízení v hraničních oblastech obou států. Cvičení bylo zaměřeno na ověření mezinárodní komunikace odpovědných státních úřadů, eskalaci na odpovědné orgány v rámci

jednotlivých států, komunikaci s médii, výměnu informací mezi provozovateli přenosových soustav, ověření nastavení bezpečnostních procesů a v neposlední řadě, kdo a na které úrovni a na základě jakých informací bude o čem rozhodovat. Cvičení je jeden z možných způsobů, jak se na obdobné situace připravovat a případně jim i předcházet.

* Myslíte, že hrozby jsou větší než dřív?

Ano, to rozhodně. Jak jsem se již zmínil, svět je globalizovaný a kybernetický prostor je všude kolem nás. To, co se dřív objevovalo jen ve sci-fi knihách a filmech, je dnes často realitou. Bohužel. Musíme s tím počítat a být připraveni.

* Jak získáváte odborníky v oboru kybernetické bezpečnosti, aby nedali přednost soukromému sektoru?

Nepracují jen u nás. Měli jsme šťastnou ruku ve výběru konzultantů, kteří s námi v této oblasti spolupracují. Jsou to dlouhodobí partneři. Nebylo by ani vhodné je často měnit, neslo by to i určité bezpečnostní riziko. Ale samozřejmě potřebujeme lidi pro oblast informačních technologií, řídicích systémů. Zjistili jsme, že některé z nich motivuje to, že se tu setkají s nejnovějšími technologiemi, mohou si je osahat, pracovat s nimi. To je pro ně motivem, aby neodešli do sféry, kde by tomu tak nemuselo být. Byť to třeba nemusí být platově zcela srovnatelné.

***

JAN ŠMOLÍK vystudoval České vysoké učení technické, Fakultu elektrotechnickou, obor řízení. Zkušenosti získával v průběhu let 1983 až 2009 na různých pozicích v ICT v Českých energetických závodech, později Hlavní správa ČEZ, a.s., a ENIT, a.s. Od roku 2010 zastává roli manažera bezpečnosti informací ve společnosti ČEPS, kde odpovídá za systém řízení bezpečnosti informací (ISO/IEC 27001) a soulad s požadavky zákona o kybernetické bezpečnosti. Je vedoucím odboru Kybernetická a informační bezpečnost, do jehož gesce náleží i governance bezpečnosti informací.