SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Bezpečnostní projekty realizované ve společnosti OTE, a.s. - případová studie

Vojtěch Szaló,
OTE, a. s.

Jan Poduška
AEC, spol. s r. o.

Kroky k informační bezpečnosti

- OTE identifikovalo potřebu zvýšení úrovně informační bezpečnosti – podpora vedení
- Výběr partnera
- Orientace v prostředí společnosti
- Realizace prvotních kroků
- Nastavení dlouhodobé spolupráce
- Reakce na požadavky Evropské komise
- Realizace navazujících kroků
- Možná úskalí spolupráce, vnímání zákazníka

Založení naší společnosti

- OTE byl založen z energetického zákona v roce 2001 a své poslání naplňuje od roku 2002.
- Jediným akcionářem společnosti je stát.
- Společnost svou činnost vykonává na základě licence přidělené ERÚ na základě energetického zákona

Poslání společnosti OTE

- OTE slouží jako platforma pro obchodování s elektřinou a plynem v liberalizovaném prostředí.
- Hlavní činnosti:
  - organizování krátkodobého trhu s elektřinou a plynem
  - vyhodnocování odchylek a zajišťování jejich zúčtování a vypořádání mezi subjekty

Další činnosti OTE

dále

- zpracování a zveřejňování měsíční a roční zprávy o trhu s elektřinou a plynem v ČR
- zpracování podkladů pro návrh Pravidel trhu s elektřinou a Pravidel trhu s plynem
- zpracování zprávy o budoucí očekávané spotřebě elektřiny a plynu a o způsobu zabezpečení rovnováhy mezi nabídkou a poptávkou elektřiny a plynu.

Rejstřík emisních povolenek

- správa veřejně přístupného rejstříku obchodování s povolenkami na emise skleníkových plynů podle zákona č. 695/2004 Sb. o podmínkách obchodování s povolenkami na emise skleníkových plynů.

Způsob zajištění činností

- Počet zaměstnanců 34 plus 3členné představenstvo
- „Obchodní“ i kancelářský systém jsou plně outsoursingované.
- Smluvní vztah s Logica

Jak vznikla spolupráce s dodavatelem

- Nutná potřeba zvýšení bezpečnosti IT
- Potřebný stálý dozor, avšak instalace manažera IT bezpečnosti z vlastních řad by bylo neúčelné.
- Společnost AEC pro nás představovala neznámou firmu, tím byla zajištěna nestrannost.

Orientace v prostředí společnosti

- Analýza současného stavu – oblasti definované řadou norem ISO/IEC 27 000
- Zdroje informací:
  - Revize interní dokumentace klienta
  - Interview s vybranými zaměstnanci
  - Anonymní dotazníky
  - Technické testy
  - Revize smluv klienta (třetí strany, NDA, zaměstnanci)
  - Revize fyzické bezpečnosti
- Výstup: identifikované zranitelnosti, vypracovaná sada doporučení

Prvotní kroky

- Na základě závěrů Analýzy současného stavu
- Penetrační testy – vhodný doplněk Analýzy současného stavu
- Bezpečnostní politika a návazná bezpečnostní dokumentace
- Testování uživatelů metodami sociálního inženýrství
- Školení uživatelů
- eLearningový portál

Dlouhodobá spolupráce

Služby externího bezpečnostního správce:

- Příprava a realizace školení informační bezpečnosti
- Příprava a realizace pravidelných technických testů
- Analýza logů a dalších auditních záznamů
- Pravidelná aktualizace dokumentace a ověření shody s praxí
- Analýza a zpracování bezpečnostních incidentů
- Kontrola dodržování bezpečnostních pravidel zaměstnanci
- Pravidelné přezkoumání rizik
- Roční zpráva pro management
- **Operativa:** Posouzení návrhu Wi-fi sítě, VPN, ověření nastavení uživatelských notebooků, …

Navazující kroky

- Komplexní audity stěžejních IS
  - Penetrační testy – interní, externí, web. aplikací
  - Audity používaných technologií – servery, síťové prvky
  - Modelování hrozeb
- Ad hoc poradenství
- Připravenost rychle reagovat na nenadálé události
- …

Reakce na nenadálé události

Impulsy:

- Významný bezpečnostní incident, zásadní změna legislativy, přírodní katastrofa, …

Limitující faktory:

- Omezený čas na reakci – výběrové řízení čas ještě prodlouží
- Důkazní materiál zapůjčený policií ČR – partner zná prostředí, souvislosti

Možná úskalí z pohledu zákazníka

- Zodpovědně přistoupit k Analýze současného stavu – nezakrývat skutečnost
- Interní IT vs. Outsourcované IT – outsourcované nemusí mít zájem nechat si „koukat pod prsty“
- Negativní vnímání zaměstnanců – bezpečnost vs. uživatelský komfort
- Sledování bezpečnostních trendů

Hlavní přínosy spolupráce pro nás

- Zajištění bezpečnostního manažera IT externě.
- Možnost vyžádání ad hoc vyjádření (instalace wifi, VPN, atd.)
- Zvýšení „uvědomělosti“ v oblasti IT bezpečnosti u zaměstnanců i u představenstva.
- Skutečně ze života: provázanost školení se zjištěními skutečnostmi na bázi sociálního inženýrství.

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Vojtěch Szaló, Jan Poduška
vszalo@ote-cr.cz
jan.poduska@aec.cz