RENOMIA

KOMPLEXNÍ SLUŽBY
V OBLASTI POJIŠTĚNÍ A RISK MANAGEMENTU

Pojištění kybernetických rizik – Praha 22.3.2016

WBN
Worldwide Broker Network

Sloužíme Vám s radostí

OBSAH

RENOMIA

- Kybernetická rizika - oblasti, formy
- **Pojištění kybernetických rizik**
- Pojištění kybernetických rizik - cílová skupina
- Pojištění kybernetických rizik - příklady škod

KYBERNETICKÁ RIZIKA

RENOMIA

- Součást každodenního života – data, informace , citlivé údaje
- Výskyt : počítače, mobilní telefony, notebooky, tablety, webové stránky, e-mail….

Každá společnost, která shromažďuje, pracuje či jakýmkoliv způsobem nakládá s daty je v ohrožení.

Kybernetická rizika - formy:

- Kybernetická kriminalita (cílené útoky, terorismus)
- Ztráta / odcizení dat
- Ztráta /odcizení HW
- On-line rizika – e-mail, cloud computing

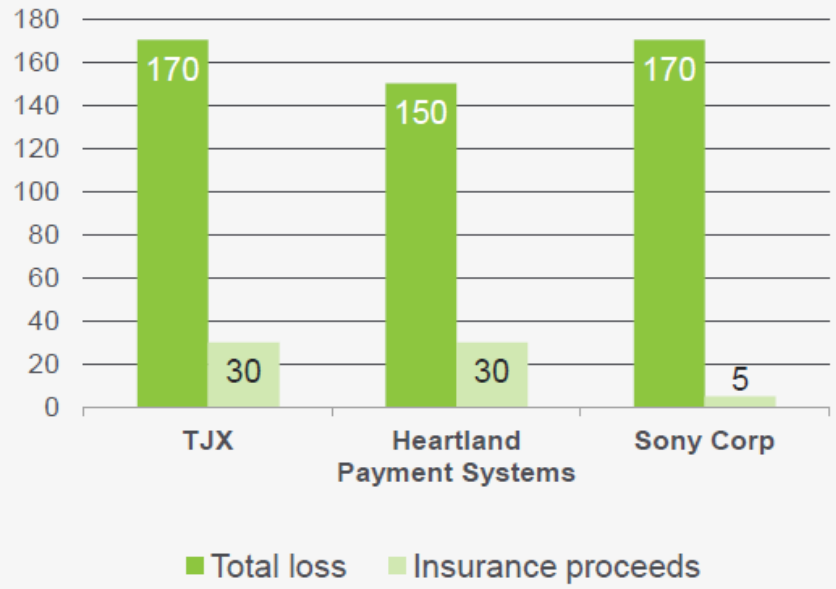
RIZIKA OHROŽUJÍCÍ DATA

RENOMIA

- 1. Zastaralý HW a SW,
  nedostatečná ochrana dat
- 2. Neloajální zaměstnanci
- 3. Ztráta/ zcizení hardware,
  zařízení obsahující citlivé informace, údaje, data
  např. mobilní telefony,notebooky, tablety, PC ...
- 4. Hackerský útok - kybernetická kriminalita

PŘÍKLADY TOP CYBER ŠKOD

RENOMIA



Large security incidents so far exhibit an insurance cover in the range of 0-30%.

- TJX: 45.6 million credit and debit card numbers were stolen
- HPS: 130 million credit and debit cards were compromised
- Sony: theft of 77 million peoples' details on the PlayStation Network (PSN)

Figures approximate in million USD
Source: SEC filings

Zdroj – prezentace
Munich RE, 2014

Příklady z praxe

RENOMIA

Sloužíme Vám s radostí

KYBERNETICKÁ RIZIKA

RENOMIA

Odpovědnost za bezpečnost IT sítě

- Zneužití dat (odcizení dat, neoprávněný přístup nebo zneužití)
- Přenos IT virů
- Odmítnutí přístupu k uloženým datům (DOS / DDoS attack)

Odpovědnost za osobní a korporátní údaje (data)

- Osobní údaje (interní)
- Osobní údaje (externí)
- Korporátní údaje (externí)
- Data shromažďovaná
- Data sdílená

JAKÁ JSOU RIZIKA A JEJICH DŮSLEDKY ?

RENOMIA

1. Únik dat a informací

- Jaká data, jaké informace ?
- Odkud data unikla ?

2. Dopady na řízení IT

- Obnovení dat
- Obnovení systému

3. PR & reputace

- Ztráta důvěry
- Poškození dobrého jména

4. Finanční dopady

- Finanční škody třetích stran
- Pokuty, penále

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

RENOMIA

Základní krytí

- Neoprávněné nakládání s údaji
- Povinnosti vůči dozorovým orgánům
- Náklady na odborné služby

Volitelná rozšiřující pojištění

- Zveřejnění digitálního obsahu
- Vydírání prostřednictvím sítě
- Výpadek sítě / přerušení provozu

- Územní rozsah – celý svět
- Pojištěný - společnost + dceřiné společnosti
  - včetně subdodavatelů

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

RENOMIA

Odpovědnost za neoprávněné nakládání s údaji

- Osobní údaje
- Důvěrné informace společnosti
- Subdodavatelé
- Zabezpečení sítě
    - Napadení, zavirování dat třetí osoby
    - Odepření přístupu k datům
    - Neoprávněné získání přístupového kódu
    - Zničení, poškození, smazání dat
    - Odcizení hardware
    - Zpřístupnění dat zaměstnancem

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

RENOMIA

Povinnosti vůči dozorovým orgánům

- Sankce uložené dozorovým orgánem
- Náklady na právní poradenství a zastupování před dozorovým orgánem

Náklady na odborné služby

- PR - náprava dobré pověsti společnosti
náprava dobrého jména jednotlivce
- Náklady na oznámení
- Náklady na IT experty
- Náklady na obnovu dat

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

RENOMIA

Zveřejnění digitálního obsahu

- Pomluva, zásah do dobré pověsti
- Zásah do práva na soukromí
- Porušení autorského práva, plagiátorství
- Nekalosoutěžní jednání

Vydírání prostřednictvím sítě

Výpadek sítě / přerušení provozu

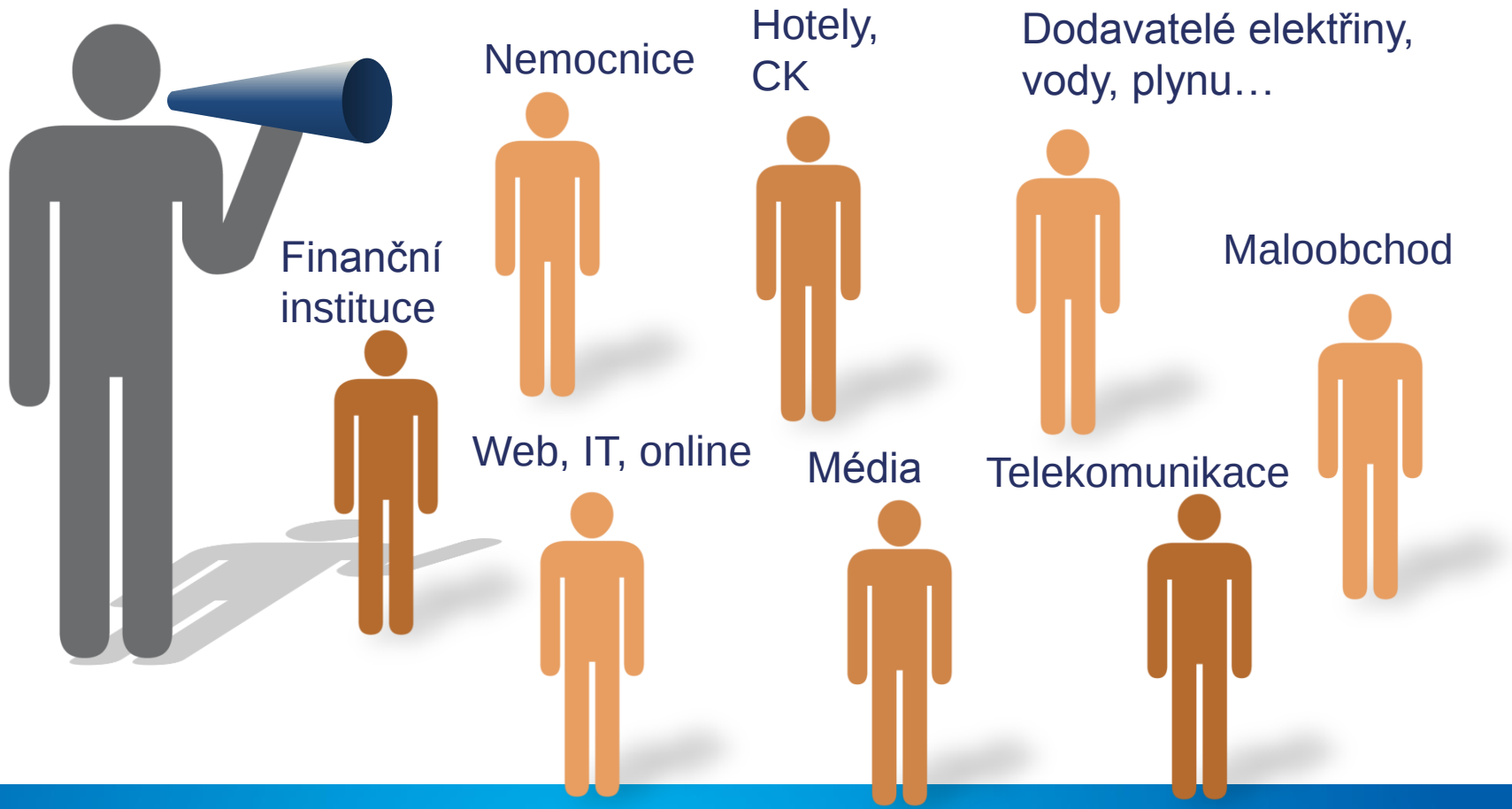
ARGUMENTY – (PROTI) PRO CYBER POJIŠTĚNÍ

RENOMIA

- Jsme chránění – máme pojištění:
    - Profesní odpovědnost, obecná odpovědnost
    - Pojištění zpronevěry, majetku- přerušení provozu
- Nepotřebujeme pojištění – máme spolehlivé a dostatečné IT zabezpečení
- Jsme příliš malá společnost, útok na naše data nám nehrozí
- Nejsme cílová skupina, pro nás se toto pojištění nehodí
- Naše data nejsou zajímavá pro hackery
- Náklady spojené se ztrátou dat nejsou velké
- Pojištění kybernetických rizik je příliš drahé
- Naše data jsou ukládána a chráněna u třetích subjektů
- Nikdy jsme se nestali terčem kybernetického útoku, nepotřebujeme toto pojištění

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK – CÍLOVÁ SKUPINA

RENOMIA



Sloužíme Vám s radostí

CÍLE KYBERNETICKÝCH ÚTOKŮ

RENOMIA

V roce 2011 bylo celosvětově zaznamenáno více jak 855 případů narušení bezpečnosti, během kterých bylo zasaženo 174 milionů dat.

Nejčastější cíle kybernetických útoků:

- *71% ze všech případů, kdy došlo k narušení bezpečnosti a ztrátě dat se týkalo malých a středních společnosti s 1 – 100 zaměstnanci*
- *96% všech útoků bylo velmi jednoduchých k provedení*
- *v 97% všech případů se dalo předejít ztrátě dat dodržováním základních bezpečnostních pravidel a aktualizací bezpečnostních systémů*
- *každou minutu je zasaženo malwarem 232 počítačů*

(Malware je počítačový program určený ke vniknutí nebo poškození počítačového systému)

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK – PŘÍKLADY ŠKOD

RENOMIA

Hackerský útok a následné zveřejnění tisíců osobních údajů pacientů ze zdravotních karet:

- náklady na IT experty za účelem zjištění příčiny útoku a přesného počtu zveřejněných údajů,
- náklady na oznámení (informační dopis všem pacientům a zřízení call centra),
- náklady na PR (zlepšení reputace a dobré pověsti nemocnice),
- pokuta udělená dozorovým orgánem za zveřejnění citlivých informací.

Útok hackerů na PC síť internetového obchodu:

- následuje - výpadek PC systému,
- snížení zisku pojištěného v důsledku nemožnosti prodávat zboží,
- náklady na IT experty za účelem zjištění příčiny výpadku systémů,
- náklady na PR.

.

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK – PŘÍKLADY ŠKOD

RENOMIA

Hackerský útok a následné zveřejnění 117 000 osobních údajů studentů:

- náklady na IT experty za účelem zjištění příčiny útoku a přesného počtu zveřejněných údajů,
- náklady na oznámení (informační dopis všem studentům a zřízení call centra) + náklady na PR,
- pokuta udělená dozorovým orgánem za zveřejnění citlivých informací.

Útok hackerů na PC síť obchodního řetězce:

- následuje - zcizení údajů o účtech a platebních kartách,
- finanční újma držitelů platebních karet ,
- náklady na IT experty, oznámení a PR .

RENOMIA

TĚŠÍME SE NA SPOLUPRÁCI

RENOMIA

Sloužíme Vám s radostí