



RENOMIA

RENOMIA

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

OBSAH

- > Kybernetická rizika - oblasti, formy
- > GDPR - nová směrnice, květen 2018
- > **Pojištění kybernetických rizik - CYBER**
- > Pojištění kybernetických rizik - cílová skupina
- > Pojištění kybernetických rizik - příklady škod

KYBERNETICKÁ RIZIKA

- > 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 HW
- > On-line rizika – e-mail, cloud computing, internet banking



RIZIKA OHROŽUJÍCÍ DATA

- > 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, vydírání (ransomware)

JAKÁ JSOU RIZIKA A JEJICH DŮSLEDKY

Únik dat a informací – odpovědnost vůči 3. stranám

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

Dopady na řízení IT – náklady související s kybernetickým incidentem

- > Obnovení dat / systému

PR & reputace – náklady související s kybernetickým incidentem

- > Ztráta důvěry
- > Poškození dobrého jména

Finanční dopady

- > Finanční škody třetích stran / odpovědnost
- > Pokuty od ÚOOÚ / regulatorní řízení



NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ - GDPR

- > Nařízení Evropského parlamentu a Rady EU – účinnost 25.5.2018
- > **Cíl** - sjednotit (a zpřísnit) pravidla ochrany osobních dat občanů EU
- > **GDPR** zavádí mimo jiné tato opatření:
 - Povinnost provádět posouzení dopadu na ochranu osobních údajů
 - Povinnost vést záznamy o zpracování osobních údajů
 - Povinnost ohlašovat případy narušení bezpečnosti
 - Povinnost jmenovat inspektora ochrany údajů – Data Protection Officer
- > Zásah do IT systémů, smluvní dokumentace a vnitřních postupů, **rozšíření odpovědnosti**
- > GDPR zavádí možnost udělení několikanásobně vyšších pokut – **až 20.000.000 EUR nebo 4 % z celkového ročního obrátu společnosti** (vyšší z obou možností)



POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

Odpovědnost za neoprávněné nakládání s údaji – škody 3. stran

- > Odpovědnost za neoprávněné nakládání s osobními údaji / důvěrnými informacemi
- > Odpovědnost za subdodavatele
- > Odpovědnost za selhání zabezpečení sítě (DoS / DDoS útoky)
- > Náklady na obranu (právní výlohy)



Povinnosti vůči dozorovým orgánům – škoda pojištěného

- > Sankce uložené dozorovým orgánem (GDPR nařízení 2018) – Úřad pro ochranu osobních údajů
- > Náklady na obranu (právní výlohy)

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

Náklady na odborné služby – škoda pojištěného

- > PR - náprava dobré pověsti společnosti / dobrého jména jednotlivce
- > Náklady na oznámení
- > Náklady na IT experty (forenzní audit), na obnovu dat

Vydírání prostřednictvím sítě (ransomware)

- > Náklady na IT experty + „výkupné“

Výpadek sítě / přerušení provozu

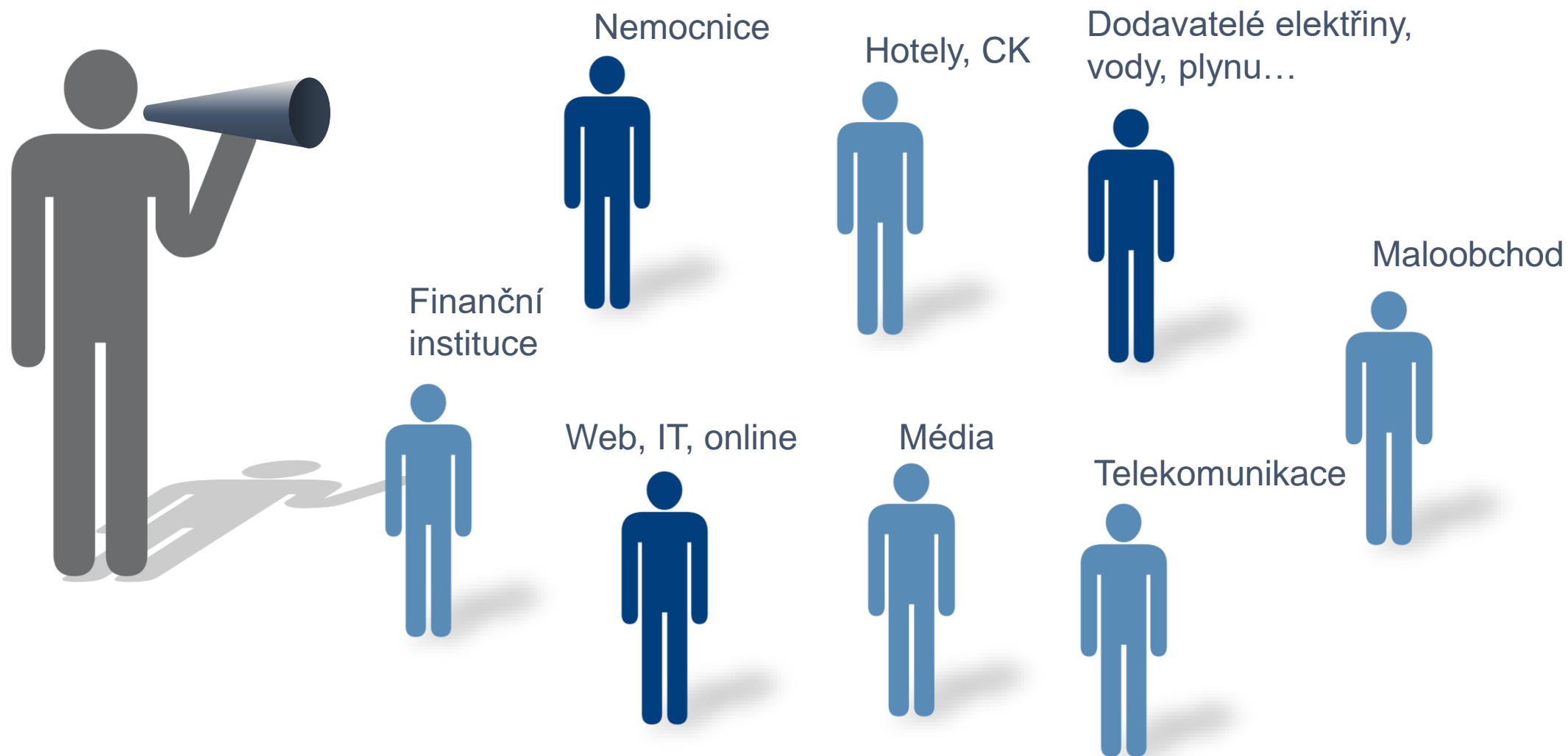
- > Ušlý zisk a náklady



POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

- > Územní rozsah - celý svět
- > Pojištěný
 - společnost + dceřiné společnosti, včetně vedení a zaměstnanců
 - subdodavatelé
- > Výluky (hlavní)
 - smluvní odpovědnost / smluvní záruky
 - úmyslná jednání / trestné činy (vyjma úmyslu zaměstnance)
 - předchozí nároky / známá pochybení
 - neoprávněně shromažďovaná data
- > Pojištění se nevztahuje na vlastní data pojištěného.

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK – CÍLOVÁ SKUPINA



POJIŠTĚNÍ KYBERNETICKÝCH RIZIK – PŘÍKLADY ŠKOD

Únik osobních údajů pacienta:

- > osobnostní újma pacienta, znemožnění výkonu povolání z důvodu zveřejnění zdravotního stavu
- > žaloba o finanční kompenzaci ze strany pacienta
- > pokuta udělená dozorovým orgánem za zveřejnění citlivých informací o pacientovi

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

POJIŠTĚNÍ KYBERNETICKÝCH RIZIK – PŘÍKLADY ŠKOD

Útok hackerů na PC síť obchodního řetězce:

- > následuje výpadek PC systému, zcizení údajů o účtech a platebních kartách
- > snížení zisku pojištěného v důsledku nemožnosti prodávat zboží
- > finanční újma držitelů platebních karet
- > náklady na IT experty, oznámení a PR

Přerušení provozu – letiště

- > vyřazení IT systému odbavení zavazadel z provozu – malware / zaměstnanec
- > snížení zisku pojištěného v důsledku zpoždění letadel a storen, finanční újma zákazníků
- > náklady na IT experty, náklady na PR, náklady na „extra“ manuální externí pracovníky (8 dnů)

T-Mobile, data odcizená bývalým zaměstnancem : pokuta od ÚOOÚ 3,5 mio Kč



RENOMIA

TĚŠÍME SE NA SPOLUPRÁCI

RENOMIA