**POJIŠTĚNÍ KYBERNETICKÝCH RIZIK**

**PODKLADY PRO VÝPOČET POJISTNÉHO**

Tento podklad slouží pro posouzení rizika pro pojištění kybernetických rizik pro podnikatele bez ohledu na to, jestli se jedná o právnické osoby nebo fyzické osoby podnikající. V případě, že není v dokumentu uvedeno nějaké riziko, případně není dostatečný prostor pro dostupné údaje ani v polích „POZNÁMKY“, uveďte je na samostatné příloze, popřípadě v průvodním e-mailu. Podklady zašlete na adresu [poptavky@maxima-as.cz](mailto:poptavky@maxima-as.cz). Dotazník je v případě sjednání pojištění nedílnou součástí pojistné smlouvy.

Pokud je více pojištěných, vycházejte z údajů za všechny společnosti. V případě označení otázky hvězdičkou (\*) zaškrtněte pouze jeden údaj odpovídající skutečnosti.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **POJISTNÍK1** | Jméno/název společnosti: |  | | | IČ: |  |
| 1 Pojistníkem je ten, kdo sjednává pojištění v prospěch svůj nebo v prospěch někoho jiného. Pojistník zároveň hradí pojistné. | | | | | | |
| Je pojistník zároveň pojištěným? \* | | | | **ANO**  **NE** | | |
| **POJIŠTĚNÝ2** | Jméno/název dceřiné společnosti: | 1. |  | IČ: | |  |
| 2. |  | IČ: | |  |
| 3. |  | IČ: | |  |
| 2 Vyplňte v případě, že se pojištěný liší od pojistníka.  **POJIŠŤOVACÍ ZPROSTŘEDKOVATEL** | | | | | | |
| |  |  |  |  | | --- | --- | --- | --- | | Jméno/název firmy: |  | Registrační číslo (ČNB): |  | | Zastoupená/ý: |  | Registrační číslo (ČNB): |  | | | | | | | |

**ODDÍL A** (SPOLEČNÝ PRO VŠECHNY ZÁJEMCE O POJIŠTĚNÍ BEZ OHLEDU NA VÝŠI OBRATU I ČINNOSTI)

**ČINNOST ZÁJEMCŮ O POJIŠTĚNÍ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obrat a ekonomické ukazatele** | | |  | **Popis činnosti** |
| Česká republika |  | Kč |  |
| Evropa3 |  | Kč |
| Celý svět s výjimkou USA a Kanady |  | Kč |
| USA a Kanada |  | Kč |
| CELKEM |  | Kč |
| Podíl on-line tržeb na obratu |  | % |
| Počet zaměstnanců (vč. ředitelů) |  | |

3 Jedná se o Evropu v geografickém smyslu, nikoli politickém (nezahrnuje tedy pouze státy Evropské unie, ale i další)

**Předmět činnosti**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Služby v oblasti zábavního průmyslu pro dos-pělé |  |  | Výrobní podniky |
|  | Činnosti nebo služby v oblasti kryptoměn |  |  | Zdravotnická zařízení |
|  | Provoz sociální sítí |  |  | Škola nebo vzdělávací instituce |
|  | Provoz e-shopu v rámci svého podnikání |  |  | IT společnosti – vývoj softwaru, tvorba webových stránek, cloudové služby atd. |
|  | Zemědělství |  |  | Data agregátoři/analytici |
|  | Obchodní činnost |  |  | Výrobce nebo vydavatel počítačových her |
|  | Výrobce/prodejce potravin |  |  | Výrobce/dodavatel energie *(budou následně individuálně vyžádány informace po posouzení rizika)* |
|  | Pořadatel kulturních a sportovních akcí |  |  | Telekomunikace *(budou následně individuálně vyžádány informace po posouzení rizika)* |
|  | Poskytovatel odborných služeb (účetní, archi-tekti apod.) |  |  | Televizní a rozhlasové vysílání *(budou následně individuálně vyžádány informace po posouzení rizika)* |

**ZABEZPEČENÍ SÍTĚ A DAT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Máte implementována opatření zajišťující splně-ní požadavků plynoucích z obecného nařízení o ochraně osobních údajů 2016/679 Evropské unie (GDPR) a příslušné právní úpravy, které se týkají ochrany osobních údajů, dané českým právním řádem? \* | **ANO**  **NE** |  | Pokud jste organizací, která přijímá, předává, ukládá nebo jinak zpracovává údaje  o jakémkoli typu platebních karet a transakcích s nimi, splňujete příslušné podmínky PCI DSS (Bezpe-nostní standardy ochrany dat  o kreditních a platebních kartách a transakcích s nimi)? \* | **ANO**  **NE**  **údaje nezpra-covává-me** |
|  |
|  |
|  |
|  |
|  |
| Máte počítače a síť chráněny firewalem a antivi-rovým programem určeným pro profesionální komerční využití (nejedná se tady o bezplatný program volně dostupný ke stažení na inter-netu)? \* | **ANO**  **NE** |  |
|  | Máte všechna přenosná média (vč. smartpho-nů i USB disků) chráněna heslem? \* | **ANO**  **NE** |
|  |
|  | Zálohujete (a v případě, že využíváte poskyto-vatele IT služeb – úložiště apod. – také tento poskytovatel) vaše data, která souvisí s podni-káním nejméně jednou za 7 dní? \* | **ANO**  **NE** |
|  |
| Utrpěli jste v minulých 24 měsících výpadek funkčnosti počítačů, systému nebo IT služeb, který trval déle než 4 hodiny? | **ANO**  **NE** |  |
|  |
|  | **Pro firmy s příjmy nad 100 000 000 Kč**  V případě, že používáte vzdálený přístup k Vaší síti a datům (přístup přes internet), je tento přístup zabezpečen dvoufaktorovým ověřením uživatele? \* | **ANO**  **NE** |
| **Pro firmy s příjmy nad 100 000 000 Kč**  Pokud zpracováváte osobní údaje nebo citlivé údaje, jsou ve Vašich počítačích, datech a síti zašifrovány? \* | **ANO**  **NE** |  |
|  |
|  |
|  |

**LIMIT PLNĚNÍ**

|  |  |
| --- | --- |
| **5 000 000 Kč** **10 000 000 Kč** **15 000 000 Kč** **20 000 000 Kč** **30 000 000 Kč** **40 000 000 Kč** **JINÝ 5** | |
| 5 Požadovaný jiný limit plnění (Kč): |  |

**ŠKODY/NÁROKY**

|  |
| --- |
| Pokud jste v předchozí části odpověděli, že jste v předchozích 24 měsících zaznamenali výpadek funkčnosti počítačů, systému nebo IT služeb delší než 4 hodiny, uveďte, kdy a jakým způsobem k výpadku došlo (např. zda se jednalo o výpadek systému z přetížení nebo napadením malwarem, poté se také ale zaměřte na to, jaká byla přijata opatření, aby se situace v budoucnu  už neopakovala). |
|  |

|  |  |
| --- | --- |
| Byly citlivé nebo osobní údaje, za které jste právně odpovědní, během uplynulých 36 měsíců ohroženy nebo ztraceny? Pokud ano, uveďte podrobnosti, kdy a jak k incidentu došlo, dále se pak zaměřte  na opatření, která byla přijata, aby v budoucnu k podobné situaci nemohlo dojít. \* | **ANO**  **NE** |
|  | |

**POZNÁMKY**

|  |
| --- |
|  |

**ODDÍL B** (VYPLŇUJÍ POUZE PODNIKATELÉ, JEJICHŽ OBRAT PŘESÁHL V PŘEDCHOZÍM UZAVŘENÉM ÚČETNÍM ROCE ČÁSTKU **400 000 000 Kč**)

**CELKOVÝ POČET ZÁZNAMŮ, ZA KTERÉ JSOU ZÁJEMCI O POJIŠTĚNÍ PRÁVNĚ ODPOVĚDNÍ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Payment Card Industry: |  |  | Jiné osobní údaje: |  |
| Řidičské průkazy, daňové nebo čísla sociálního zabezpečení: |  | Finanční údaje (jiné než kreditní a debetní karty: |  |

**BEZPEČNOST SÍTĚ – DOPLNĚNÍ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Jak často je aktualizována virová data-báze?\* | **automaticky**  **denně**  **týdně**  **jinak 6** |  | Jak často jsou instalovány záplaty kritických chyb? \* | **automaticky**  **denně**  **týdně**  **jinak 6** |
| Šifrujete všechna citlivá data? \* | **ANO**  **NE**  **ANO**  **NE**  **ANO**  **NE** | Máte v platnosti a dodržujete zásady auditu a správy počítačových a uživa-telských účtů? \* | **ANO**  **NE** |
| a) během přenosu |
| b) uložená na serveru |
| c) uložená na přenosných zařízeních | Jsou automaticky rušeny všechny přístupy a oprávnění zaměstnancům, kterým skončil pracovní poměr? \* | **ANO**  **NE** |
| Jak často je prováděn externí bezpeč-nostní audit? \* | **ročně**  **jinak 6** |
| Kdo má celkovou odpovědnost za za-bezpečení sítě? |  | Dodržujete zásadu změny hesel alespoň jednou za 3 měsíce? \* | **ANO**  **NE** |
| Jak často jsou revidovány zásady zabez-pečení informací? \* | **ročně**  **jinak 6** | Je přístup k citlivým údajům omezen pouze na oprávněné požadavky, zaměstnance? \* | **ANO**  **NE** |

6 V případě, že je uvedena odpověď „jinak“, upřesnění uveďte v poli „Poznámky“ s odkazem, které otázky se týká.

**PAYMENT CARD INDUSTRY COMPLIANCE**

Odpověděli-li jste v oddílu A, že přijímáte, předáváte, ukládáte nebo jinak zpracováváte údaje o platebních kartách, uveďte následující podrobnosti:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Jaké úrovně dle PCI DSS dosahujete? \* | | **1** |  | ***Jste-li obchodníkem úrovně 1, uveďte všechny informace specifikované dále v tomto bodě*** | |
| **2** |
| **3** | Kdy byl proveden poslední audit PCI?  (uveďte datum) |  |
| **4** |  |
| Zaznamenali jste jakékoli závažné nedo-držení předpisu? \* | **ANO**  **NE** | |  | Pokud ano, byla provedena opětovná certifikace? \* | **ANO**  **NE** |
| Jste v souladu se standardem EMV (zkratka z názvů společností Europay, MasterCard  a Visa) \* | **ANO**  **NE** | |  | Používáte program Microsoft XP Pos Ready nebo jiné nepodporované aplika-ce? \* | **ANO**  **NE** |
|  |
|  |

**KONTINUITA PROVOZU**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Máte písemný plán kontinuity provozu (BCP)? \* | **ANO**  **NE** |  | Zálohujete oproti menším firmám (viz ODDÍL A) kritické aplikace alespoň kaž-dých 5 dní? \* | **ANO**  **NE** |
|  |
| Posuzuje plán kontinuity provozu (BCP) riziko z kybernetického ohrožení? \* | **ANO**  **NE** |  |
|  | Jak často je testována integrita zálohova-ných dat? \* | **týdně** |
| Testujete Disaster Recovery Plan (DRP)/ plán kontinuity provozu minimálně ročně? \* | **ANO**  **NE** |  | **měsíčně** |
|  | **ročně** |
| Po jak dlouhé době bude Vaše podnikání ovlivněno poškozením/ztrátou sítě? \* | **6 hodin** |  | Jak dlouho trvá úplné obnovení kritických systémů? \* | **6 hodin** |
| **12 hodin** |  | **12 hodin** |
| **24 hodin** |  | **24 hodin** |
| **48 hodin** |  | **48 hodin** |
| Máte síť nakonfigurovánu tak, aby poskytovala vysokou dostupnost nebo failover řešení pro Vaše webové stránky a další kritické aplikace? (totéž platí i pro partnera v cloudu nebo outsourcingu) \* | | | | **ANO**  **NE** |

**POZNÁMKY**

|  |
| --- |
|  |

**ODDÍL C** (VYPLŇUJÍ POUZE PODNIKATELÉ, KTEŘÍ PROVOZUJÍ NĚKTEROU ZE SPECIFICKÝCH ČINNOSTÍ UVEDENÝCH V BA-REVNĚ OZNAČENÉM SEZNAMU ČINNOSTÍ UVEDENÉM V ODDÍLU A)

**VÝROBNÍ PODNIKY**

|  |  |  |  |
| --- | --- | --- | --- |
| Provozujete CNC stroje na základě DNC, tj. v DNC síti, s použitím DNC komunikace nebo software? \* | | | **ANO**  **NE** |
| ***Pokud jste v předchozí otázce uvedli „ANO“, zodpovězte prosím následující dotazy:*** | | | |
| Jak oddělujete výrobní prostředí (DNC) od všech sítí? |  | | |
| Uveďte podrobnosti o logických vazbách mezi vaším výrobním prostředím a dalšími aplikacemi (logis-tika/zásoby/nákup atd.) |  | | |
| Pracuje Vaše výrobní síť v rámci nepodporovaných operačních systémů (např. Windows XP)? \* | | | **ANO**  **NE** |
| Pokud pracujete na nepodporovaných platformách, jsou tyto aplikace zcela izolovány od jiných platforem (fyzicky odděleny – air gapped)? \* | | | **ANO**  **NE** |
| Jak rychle se používají opravy kritických chyb software (kritické záplaty – critical patches) ve vašem výrobním prostředí? | |  | |
| Jsou některé z vašich serverů, na který jsou spouštěny ovladače výrobních procesů (DNC síť), připojeny k internetu? \* | | | **ANO**  **NE** |
| Aplikujete white-listing, tj. že ve vašich počítačových systémech lze spouštět pouze povolené aplikace? \* | | | **ANO**  **NE** |

**ZDRAVOTNICKÁ ZAŘÍZENÍ**

|  |  |  |
| --- | --- | --- |
| Jaký je maximální počet zpracovávaných záznamů? |  | |
| Splňujete zákonné normy o ochraně dat ve zdravotnictví? \* | | **ANO**  **NE** |
| Poskytněte prosím smluvní ujednání o odškodnění s poskytovateli outsorcingu nebo poskytovateli clou-dových služeb. |  | |
| Poskytněte prosím zásady, které používáte pro apli-kaci záplat kritických chyb systémů a aplikací. |  | |
| Jsou veškeré údaje o zdravotní péči zašifrovány, ať už při uchovávání v databázi nebo při transportu? \* | | **ANO**  **NE** |

**VZDĚLÁVÁNÍ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Poskytněte prosím informace o vaší High Level Architecture (HLA), včetně topologie LAN a případně WAN. |  | | | |
| Kdo je v instituci zodpovědný za zabezpečení sítí a dat? |  | | | |
| Existuje jednotná politika řízení bezpečnosti sítí a dat, která je závazná v celé instituci? \* | | | **ANO**  **NE** | |
| Jaký je roční rozpočet na IT? | |  | | **Kč** |
| Jaký je celkový počet evidovaných žáků/studentů? |  | | | |

**IT SPOLEČNOSTI**

|  |  |  |  |
| --- | --- | --- | --- |
| Dodržujete stávající právní předpisy týkající se nakládání s osobními údaji? \* | | **ANO**  **NE** | |
| Uveďte prosím ujednání o ztrátě dat, které používáte ve smlouvách se zákazníky: |  | | |
| Jaké jsou Vaše smluvní povinnosti při zpracování osobních údajů o klientovi? |  | | |
| Jaký podíl zákazníků tvoří spotřebitelé (soukromé osoby) a jaké komerční subjekty (podnikatelé)? | Spotřebitelé: |  | **%** |
| Komerční subjekty: |  | **%** |
| Používáte pro ukládání dat vlastní servery? \* | | **ANO**  **NE** | |
| Pokud jste v předchozí otázce uvedli, že data ukládá-te na vlastních serverech, uveďte, kde jsou umístě-ny. |  | | |
| Jaký je počet a druh zpracovávaných záznamů,  za které jste právně odpovědní? 7 | Payment Card Industry: |  | |
| Řidičské průkazy, daňové nebo čísla sociálního zabezpečení: |  | |
| Jiné osobní údaje: |  | |
| Finanční údaje (jiné než kreditní a debetní karty): |  | |

7 Vyplňte v případě, že roční příjmy Vaší společnosti jsou méně než 400 000 000 Kč, resp. jste nevyplňovali oddíl B.

**DATA AGREGÁTOŘI/ANALYTICI**

|  |  |  |
| --- | --- | --- |
| Jaké je množství spravovaných nebo zpracovávaných záznamů? 8 |  | |
| Byla data ošetřena s ohledem na znemožnění identifikace jednotlivce z údajů (např. šifrováním nebo token-izací)? \* | | **ANO**  **NE** |
| Jste si vědomi svých zákonných povinností při zpracování osobních údajů? \* | | **ANO**  **NE** |
| Jak je smluvně ošetřeno odškodnění, které Správce osobních údajů poskytnou pojištěnému v případě po-rušení právních předpisů o ochraně soukromí ze stra-ny Správce osobních údajů? |  | |

8 Vyplňte v případě, že roční příjmy Vaší společnosti jsou méně než 400 000 000 Kč, resp. jste nevyplňovali oddíl B.

**VÝROBCI NEBO VYDAVATELÉ POČÍTAČOVÝCH HER**

|  |  |  |
| --- | --- | --- |
| Uveďte datum, od kdy působíte na trhu. |  | |
| Jaký je počet výrobků? |  | |
| Získali jste příslušné licence a oprávnění od všech osob nebo subjektů uvedených ve Vašich produktech? \* | | **ANO**  **NE** |
| Upřesněte proces schvalování, který je prováděn před zveřejněním produktů, a proces vnitřního schvalování produktů. |  | |

**ODDÍL D – DOPLŇUJÍCÍ ÚDAJE**

|  |
| --- |
|  |

**PROHLÁŠENÍ**

Prohlašuji, že údaje v tomto dotazníku jsou pravdivé a že žádné závažné skutečnosti nebyly při vyplňování nesprávně uvedeny nebo zamlčeny.

Souhlasím, že tento dotazník spolu s jakýmkoli dalšími poskytnutými informacemi tvoří podklad a je součástí každé pojistné smlouvy, která byla nebo bude na jeho základě uzavřena.

Zavazuji se informovat pojistitele o jakékoli změně v poskytnutých informacích, které mohou mít vliv na přijetí nebo posouzení rizika a uzavření pojistné smlouvy, a to před uzavřením i v době jejího trvání.

|  |  |  |  |
| --- | --- | --- | --- |
| V/e |  | dne |  |

|  |  |
| --- | --- |
| **PODPIS OSOBY ZASTUPUJÍCÍ ZÁJEMCE O POJIŠTĚNÍ:** |  |
| **JMÉNO/NÁZEV ZÁJEMCE O PO-JIŠTĚNÍ:** |  |
| **OSOBA JEDNAJÍCÍ ZA ZÁ-JEMCE O POJIŠTĚNÍ:** |  |
| **FUNKCE:** |  |