**DOTAZNÍK PRO POJIŠTĚNÍ**

KYBERNETICKÝCH RIZIK

1. PROFIL SPOLEČNOSTI
2. OCHRANA DAT ULOŽENÝCH NEBO DRŽENÝCH V ORGANIZACI
3. OSOBNÍ ÚDAJE ULOŽENÉ NEBO DRŽENÉ V ORGANIZACI
4. MOŽNOST OBNOVY DAT
5. OUTSOURCING
6. ZÁVISLOST PODNIKÁNÍ NA INFORMAČNÍCH SYSTÉMECH
7. BEZPEČNOST INFORMACÍ
8. INFORMACE O ŠKODÁCH
9. PROHLÁŠENÍ

# 1. PROFIL SPOLEČNOSTI

|  |  |
| --- | --- |
| Obchodní firma a právní forma společnosti |  |
| Webová stránka |  |
| Adresa |  |
| Předmět podnikání |  |

Přiložte prosím k dotazníku

* kopii standardních smluvních/obchodních podmínek při uzavírání kontraktu
* firemní brožuru (pokud existuje)

**Rozdělení obratu společnosti podle území**

|  |  |  |
| --- | --- | --- |
|  | Předcházející rok | Stávající rok (odhad) |
| Celkový obrat společnosti |  |  |
| **Rozdělení podle obratu v %** |
| Česká republika |  |  |
| EU |  |  |
| USA/Kanada |  |  |
| Ostatní země |  |  |

# 2. OCHRANA DAT ULOŽENÝCH NEBO DRŽENÝCH V ORGANIZACI

Existuje písemná směrnice (či jiný obdobný dokument), podle které postupujete ve vztahu k Vámi zpracovávaným osobním údajům a jiným datům?

 [ ]  Ano [ ]  Ne

Pokud „NE“, uveďte prosím, jakým způsobem zajišťujete ochranu osobních údajů a jiných dat:

|  |
| --- |
|  |

Jsou všichni zaměstnanci společnosti seznámeni s uvedenou směrnicí či jinými postupy na ochranu osobních údajů a jiných dat a řádně školení v oblasti ochrany osobních údajů?

 [ ]  Ano [ ]  Ne

Potvrzují zaměstnanci svým podpisem účast na školení a seznámení se s uvedenou směrnicí?

 [ ]  Ano [ ]  Ne

Pokud „NE“, jaké jsou důvody?

|  |
| --- |
|  |

Kdy byla uvedená směrnice naposledy aktualizována a kým?

|  |
| --- |
|  |

Je uvedená směrnice a/nebo postupy společnosti v oblasti ochrany osobních údajů a jiných dat v souladu s příslušnými právními předpisy právních řádů všech zemí, ve kterých podnikáte?

[ ]  Ano [ ]  Ne

Pokud „NE“, uveďte prosím, se kterými právními řády není v souladu a proč?

|  |
| --- |
|  |

Máte dceřinou společnost v USA nebo v jiné zemi řídící se kterýmkoliv z právních řádů USA?

 [ ]  Ano [ ]  Ne

Pokud ano, je výměna informací mezi Vámi a takovou společností v souladu s programem SAFE HARBOR?

 [ ]  Ano [ ]  Ne

Pokud „NE“, uveďte prosím důvody:

|  |
| --- |
|  |

Máte ve společnosti stanovenou osobu (zaměstnance či externího spolupracovníka) odpovědnou za dodržování předpisů o ochraně osobních údajů a jiných dat, osobu odpovědnou za soulad podnikání s právními předpisy (compliance managera) nebo firemního právníka?

 [ ]  Ano [ ]  Ne

Pokud „NE“, kdo je ve společnosti odpovědný za ochranu osobních údajů a jiných dat a soulad s právními předpisy?

|  |
| --- |
|  |

#

#

# 3. OSOBNÍ ÚDAJE ULOŽENÉ NEBO DRŽENÉ V ORGANIZACI

Typ a počet záznamů

|  |  |
| --- | --- |
| Počet záznamů s osobními informacemi vedené společností | **Celkem:** |
| **Dle oblastí** |
| ČR: | EU: |
| USA/Kanada: | Zbytek světa: |
| **Kategorie shromažďovaných a zpracovávaných osobních údajů** | **Počet záznamů** |
| Obchodní a marketingové informace | ANO [ ]  | NE [ ]  |  |
| Informace o platebních kartách nebo finančních transakcích | ANO [ ]  | NE [ ]  |  |
| Zdravotní údaje | ANO [ ]  | NE [ ]  |  |
| Jiné: |

Zpracováváte data pro [ ]  Vlastní účely? [ ]  Jménem třetích stran?

Standardy ochrany osobních údajů

|  |  |  |
| --- | --- | --- |
| Zásady ochrany osobních údajů jsou formalizovány a odsouhlaseny vedením společnosti a předpisy pro jejich zabezpečení jsou definovány a komunikovány dotčeným zaměstnancům | ANO [ ]  | NE ⬜ |
| Školení jsou poskytována nejméně jednou ročně osobám oprávněným k přístupu nebo zpracovávání osobních údajů  | ANO [ ]  | NE [ ]  |
| Společnost určila pověřenou osobu pro ochranu osobních údajů  | ANO [ ]  | NE [ ]  |
| Dohoda o zachování důvěrnosti informací nebo klauzule o mlčenlivosti v pracovní smlouvě je podepsána příslušnými zaměstnanci | ANO [ ]  | NE [ ]  |
| Právní aspekty politiky ochrany osobních údajů jsou ověřeny právníkem/právním oddělením | ANO [ ]  | NE [ ]  |
| Monitoring je prováděn s cílem zajistit soulad s právními předpisy o ochraně osobních údajů | ANO [ ]  | NE [ ]  |
| Postupy nakládání s osobními údaji byly v posledních dvou letech auditovány externím auditorem | ANO [ ]  | NE [ ]  |
| Reakční plán při porušení ochrany údajů je zaveden a role jsou jasně komunikovány členům týmu  | ANO [ ]  | NE [ ]  |

Kontrola ochrany osobních údajů

|  |  |  |
| --- | --- | --- |
| Přístup k osobním údajům je omezen pouze na ty uživatele, kteří jej potřebují k plnění svých pracovních úkolů a přístupová oprávnění jsou pravidelně revidována | ANO [ ]  | NE [ ]  |
| Osobní data jsou šifrována při uložení do informačních systémů a zálohy těchto dat jsou též šifrovány  | ANO [ ]  | NE [ ]  |
| Osobní data jsou zašifrována při přenosu po síti | ANO [ ]  | NE [ ]  |
| Mobilní zařízení a pevné disky notebooků jsou šifrovány | ANO [ ]  | NE [ ]  |
| Politika bezpečnosti informací zakazuje kopírování nešifrovaných osobních údajů na výměnná paměťová zařízení nebo přenos těchto dat pomocí e-mailu  | ANO [ ]  | NE [ ]  |

Pokud osobní záznamy obsahují informace o platebních kartách (dále jen PCI), zodpovězte prosím následující:

Úroveň PCI DSS: [ ]  Úroveň 1 [ ]  Úroveň 2 [ ]  Úroveň 3 [ ]  Úroveň 4

Zpracovavatel plateb (Vy nebo třetí strany) je v souladu s PCI DSS: [ ]  Ano [ ]  Ne

Pokud ne:

PCI jsou uloženy zašifrované nebo je uložena pouze část čísel platebních karet [ ]  Ano [ ]  Ne

Doba držení PCI nepřekračuje dobu trvání platby

a zákonných/regulačních požadavků [ ]  Ano [ ]  Ne

Zpracování údajů platebních karet je externalizováno [ ]  Ano [ ]  Ne

Pokud “ANO”:

Vyžadujete od zpracovatele plateb, aby vás v případě porušení bezpečnosti odškodnil? [ ]  Ano [ ]  Ne

Prosím uveďte identifikační údaje zpracovatele plateb, dobu držení PCI a jakékoli další bezpečnostní opatření:

# 4. MOŽNOST OBNOVY DAT

Máte funkční firewall na zabránění neoprávněnému přístupu do Vašeho počítačového sytému z vnějšku, tj. například z externích sítí či počítačů třetích osob?

[ ]  Ano [ ]  Ne

Pokud „ANO“, vztahuje se ochrana na všechny počítačové systémy, mobilní zařízení a webové stránky?

 [ ]  Ano [ ]  Ne

Využíváte pouze firewall nebo i jiné systémy proti neoprávněnému přístupu do Vašeho počítačového systému?

|  |
| --- |
|  |

Používáte antivirovou ochranu a postupy na všech počítačích, emailových systémech a serverech za účelem komplexní ochrany (viry, spyware, malware apod.)?

 [ ]  Ano [ ]  Ne

Pokud „ANO“, jak často měníte, resp. obnovujete ochranu a postupy (update)

⬜Denně ⬜Týdně ⬜Měsíčně ⬜ Jinak

(prosím upřesněte)

|  |
| --- |
|  |

Máte zavedeny postupy na identifikaci a zjištění slabých míst v ochraně Vašich systémů?

 [ ]  Ano [ ]  Ne

Monitorujete své sítě a systémy za účelem odhalení úniku dat?

 [ ]  Ano [ ]  Ne

Máte zavedeny systémy, resp. postupy fyzické kontroly za účelem zjištění nebo zabránění neoprávněného přístupu do systémů společnosti, serverovny, datových center?

 [ ]  Ano [ ]  Ne

Vykonáváte nebo zabezpečujete platební styk nebo zpracování plateb včetně služeb tzv. eCommerce?

 [ ]  Ano [ ]  Ne

Pokud „ANO“, uveďte prosím počet klientů, kterým zpracováváte platby, a přibližný počet transakcí spadajících na jednoho klienta?

|  |
| --- |
|  |

Máte zavedeny postupy pro šifrování (kryptování) dat v průběhu jejich přenosu nebo archivace za účelem ochrany osobních údajů a jiných citlivých dat, včetně dat na přenosných médiích (například noteboocích, záložních DVD, přenosných harddiscích, USB zařízeních apod.)?

 [ ]  Ano [ ]  Ne

Pokud „ANO“, uveďte prosím, ve kterých případech používáte kódování, šifrování?

|  |
| --- |
|  |

Máte zavedeny postupy pro obnovu a zálohování:

* Kritických systémů? [ ]  Ano [ ]  Ne
* Dat a osobních údajů? [ ]  Ano [ ]  Ne

Pokud „ANO“, jsou zálohy a systémy šifrovány? [ ]  Ano [ ]  Ne

Prověřujete si důvěryhodnost všech zaměstnanců a nezávislých konzultantů? [ ]  Ano [ ]  Ne

Vyžadujete pro vzdálený přístup do Vašich systémů potvrzení o identifikaci a autenticitě?

 [ ]  Ano [ ]  Ne

#

#

# 5. OUTSOURCING

Zajišťujete správu své sítě a počítačových a bezpečnostních systémů prostřednictvím třetí osoby?

 [ ]  Ano [ ]  Ne

Pokud „ANO“, kdo zajišťuje zabezpečení?

|  |
| --- |
|  |

Vykonáváte pravidelný audit a kontrolu činností takové třetí osoby a jejich soulad s Vašimi směrnicemi a pravidly?

 [ ]  Ano [ ]  Ne

|  |  |  |
| --- | --- | --- |
| Smlouva o outsourcingu obsahuje požadavky na zabezpečení, jež by měly být dodržovány poskytovatelem služby | ANO [ ]  | NE [ ]  |
| S poskytovatelem služby je dohodnuta správa úrovní služeb (SLA – Service Level Agreement), aby bylo umožněno řízení incidentů a změn. V případě nedodržení jsou aplikovány sankce vyjmenované v SLA  | ANO [ ]  | NE [ ]  |
| Monitorovací a řídící výbor(y) jsou organizovány ve spolupráci s poskytovatelem služeb pro řízení a zlepšování služeb  | ANO [ ]  | NE [ ]  |
| Nevzdali jste se svých práv na náhradu škody vůči poskytovali služeb ve smlouvě o outsourcingu | ANO [ ]  | NE [ ]  |

|  |  |
| --- | --- |
| **Jaké jsou funkce ousourcovaného informačního systému?** | **Poskytovatel služby (oursourcer)** |
| Správa klientských stanic | ANO [ ]  | NE [ ]  |  |
| Správa serveru | ANO [ ]  | NE [ ]  |  |
| Správa sítě | ANO [ ]  | NE [ ]  |  |
| Správa bezpečnosti sítě | ANO [ ]  | NE [ ]  |  |
| Správa aplikací | ANO [ ]  | NE [ ]  |  |
| Správa osobních dat | ANO [ ]  | NE [ ]  |  |
| Správa jiných citlivých informací | ANO [ ]  | NE [ ]  |  |
| Využití cloudu | ANO [ ]  | NE [ ]  |  |
| Pokud ano, specifikujte charakter cloudových služeb: |  |
| SaS (Software as a service) | ANO [ ]  | NE [ ]  |  |
| PaS (Platform as a service) | ANO [ ]  | NE [ ]  |  |
| IaS (Infrastructure as a service) | ANO [ ]  | NE [ ]  |  |
| Jiné: |  |
| Smlouva o outsourcingu zahrnuje ustanovení o povinnosti poskytovatele služby sjednat pojištění profesní odpovědnosti za škody? | ANO [ ]  | NE [ ]  |  |

Požadujete od osob, které Vám poskytují výše uvedené služby, náhradu škody, kterou Vám způsobily?

 [ ]  Ano [ ]  Ne

Požadujete, aby všichni poskytovatelé výše uvedených služeb měli zavedeny své vlastní směrnice a pravidla pro ochranu osobních údajů a jiných dat?

 [ ]  Ano [ ]  Ne

Požadujete, aby jejich směrnice a pravidla byly v souladu s Vašimi směrnicemi a pravidly?

 [ ]  Ano [ ]  Ne

# 6. ZÁVISLOST PODNIKÁNÍ NA INFORMAČNÍCH SYSTÉMECH

Prosím zhodnoťte, při jakém výpadku by došlo k významnému ovlivnění vašeho podnikání.

|  |  |
| --- | --- |
| **Aplikace /činnost** | **Max. délka výpadku, než bude****negativně ovlivněno podnikání** |
| Ihned | > 12 hod. | > 24 hod. | > 48 hod. | > 5 dní |
|  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
|  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Počet uživatelů informačních systémů** | **<100** [ ]  | **101 – 1000** [ ]  | **>1000** [ ]  |
| **Počet notebooků** | **<100** [ ]  | **101 – 1000** [ ]  | **>1000** [ ]  |
| **Počet serverů** | **<100** [ ]  | **101 – 1000** [ ]  | **>1000** [ ]  |

Nabízíte své služby online pomocí webových stránek či e-commerce? [ ]  Ano [ ]  Ne

Pokud ano, jaké procento na celkových výnosech generují online služby?

(odhad)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (% nebo mKč)

# 7. BEZPEČNOST INFORMACÍ

Řízení rizik

|  |  |  |
| --- | --- | --- |
| Politika bezpečnosti informací je formálně schválena managementem společnosti a/nebo pravidla bezpečnosti jsou jasně definována a komunikována všem zaměstnancům a odsouhlasena jejich zástupci | ANO [ ]  | NE [ ]  |
| Školení o bezpečnosti informací je vyžadováno pro všechny zaměstnance alespoň jednou ročně | ANO [ ]  | NE [ ]  |
| Identifikujete kritická rizika informačních systémů a podnikáte vhodné kroky k jejich zmírnění  | ANO [ ]  | NE [ ]  |
| Provádíte pravidelnou kontrolu informačních systémů a implementujete vyplývající doporučení  | ANO [ ]  | NE [ ]  |
|  Informační zdroje jsou inventarizovány a klasifikovány podle jejich kritičnosti a citlivosti | ANO [ ]  | NE [ ]  |
|  Požadavky na bezpečnost, které se týkají informačních zdrojů jsou definovány podle stupně utajení/citlivosti  | ANO [ ]  | NE [ ]  |

Ochrana informačních systémů

|  |  |  |
| --- | --- | --- |
| Přístup do kritických informačních systémů vyžaduje dvojí ověření | ANO [ ]  | NE [ ]  |
| Uživatelé musí pravidelně aktualizovat svá hesla | ANO [ ]  | NE [ ]  |
| Autorizace pro přístup závisí na roli uživatele a je zaveden postup pro její správu | ANO [ ]  | NE [ ]  |
| Existují referenční nastavení/přírůčky pro ukázkové nastavení pro pracovní stanice, notebooky, servery a mobilní zařízení (přístroje)  | ANO [ ]  | NE [ ]  |
| Je zavedena centralizovaná správa a monitoring konfigurace počítačových systémů | ANO [ ]  | NE [ ]  |
| Notebooky jsou chráněny osobním firewallem | ANO [ ]  | NE [ ]  |
| Antivirový program je nainstalován na všech systémech a jeho aktualizace jsou monitorovány  | ANO [ ]  | NE [ ]  |
| Pravidelně jsou nasazovány bezpečnostní softwarové aktualizace  | ANO [ ]  | NE [ ]  |
| Existuje plán obnovy činnosti po havárii a je pravidelně aktualizován | ANO [ ]  | NE [ ]  |
| Zálohování dat se provádí denně, zálohy jsou pravidelně testovány a jejich kopie pravidelně umisťovány na vzdáleném místě  | ANO [ ]  | NE [ ]  |

Bezpečnost sítě a provozu

|  |  |  |
| --- | --- | --- |
| Filtrování síťového provozu mezi interní sítí a internetem je monitorováno a pravidelně aktualizováno  | ANO [ ]  | NE [ ]  |
| Je zaveden systém prevence a detekce narušení, který je pravidelně aktualizován a monitorován | ANO [ ]  | NE [ ]  |
| Interní uživatelé přistupují k internetovým stránkám přes síťové zařízení (proxy) vybavené antivirem a filtrem internetového obsahu  | ANO [ ]  | NE [ ]  |
| Síť je segmentována za účelem oddělení kritických oblastí od nekritických | ANO [ ]  | NE [ ]  |
| Penetrační testy jsou prováděny pravidelně a v případě potřeby je implementován plán nápravy  | ANO [ ]  | NE [ ]  |
| Hodnocení chyb zabezpečení je prováděno pravidelně a v případě potřeby je implementován plán nápravy | ANO [ ]  | NE [ ]  |
| Jsou implementovány postupy pro správu incidentů a řízení změn | ANO [ ]  | NE [ ]  |
| Bezpečnostní události jako například detekce viru, pokusy o přístup, atd. jsou zaznamenávány a pravidelně monitorovány | ANO [ ]  | NE [ ]  |

Fyzické zabezpečení serverovny

|  |  |  |
| --- | --- | --- |
| Kritické systémy jsou umístěny v alespoň jedné vyhrazené místnosti s omezeným přístupem a provozní alarmy jsou svedeny do monitorovacího místa  | ANO [ ]  | NE [ ]  |
|  Datové centrum hostující kritické systémy má odolnou infrastrukturu včetně redundatní dodávky energie, klimatizace a síťového připojení  | ANO [ ]  | NE [ ]  |
| Kritické systémy jsou v klastru typu Aktiv/Pasiv nebo Aktiv/Aktiv architektury  | ANO [ ]  | NE [ ]  |
| Kritické systémy jsou duplikovány ve dvou oddělených lokalitách | ANO [ ]  | NE [ ]  |
| Detekce požáru a automatický systém hašení v kritických oblastech | ANO [ ]  | NE [ ]  |
| Dodávka proudu je chráněna UPS a bateriemi a je v pravidelné údržbě  | ANO [ ]  | NE [ ]  |
| Napájení je zálohováno elektrickým generátorem jež je pravidelně udržován a testován | ANO [ ]  | NE [ ]  |

# 8. INFORMACE O ŠKODÁCH

Bylo ve společnosti někdy prováděno jakékoliv šetření či s ní vedeno jakékoliv řízení regulatorním orgánem/úřadem v oblasti ochrany osobních údajů?

 [ ]  Ano [ ]  Ne

Pokud „ANO“, uveďte prosím detaily:

|  |
| --- |
|  |

Byla společnost někdy požádána subjektem údajů o přístup k jeho/jejím osobním údajům zpracovávaným společností?

[ ]  Ano [ ]  Ne

Pokud „ANO“, uveďte prosím detaily:

|  |
| --- |
|  |

Bylo proti společnosti někdy vydáno nepříznivé rozhodnutí příslušného regulatorního orgánu v důsledku porušení předpisů o ochraně osobních údajů či jiných dat?

[ ]  Ano [ ]  Ne

Pokud „ ANO“, uveďte prosím detaily:

|  |
| --- |
|  |

Jste si vědomi existence jakýchkoli okolností, v souvislosti se kterými může dojít ke vzniku pojistné události ze sjednávaného pojištění?

 [ ]  Ano [ ]  Ne

Pokud „ANO“ prosím uveďte detaily:

|  |
| --- |
|  |

# 9. PROHLÁŠENÍ

Prohlašujeme, že informace uvedené v tomto dotazníku jsou správné a pravdivé a že jsme nezamlčeli žádné skutečnosti, které mohou být významné pro sjednání pojištění. Souhlasíme, aby na základě informací uvedených v tomto dotazníku byla uzavřena pojistná smlouva. Zavazujeme se informovat pojistitele o jakýchkoli důležitých změnách relevantních skutečností (včetně změn informací poskytnutých v tomto dotazníku), které nastanou před uzavřením pojistné smlouvy.

-----------------------------------------

 podpis

Jméno:

Funkce:

(podepisuje společník/ředitel nebo osoba s podobným postavením)

Společnost:

Datum: