Pravidla kybernetické bezpečnosti pro dodavatele České televize

Obezřetnost při práci v kyberprostoru

• Při výkonu činnosti na počítači, mobilním zařízení, na internetu nebo při přístupu k informačním a komunikačním systémům České televize (ČT) se dodavatel chová vždy obezřetně, protože existuje velké množství hrozeb (např. viry, škodlivý kód, útočníci), jejichž cílem je odcizit přístupové údaje nebo napadnout zařízení, například pomocí podvodných emailů, SMS, telefonických hovorů nebo nakažených webových stránek, a z takto napadeného zařízení se dostat do počítačové sítě České televize za účelem způsobení škody (krádeže nebo narušení dat, výpadku služeb, vymáhání výkupného, apod.).

Bezpečnost lidských zdrojů

- Dodavatel je povinen dodržovat příslušná ustanovení interních řídicích dokumentů České televize.
- Dodavatel je povinen seznámit se s pravidly kybernetické bezpečnosti ČT a dodržovat je.
- Dodavatel zajistí, aby se:
    - Pro uložení a sdílení dat a informací Objednatele využívaly pouze k tomu schválené prostředky.
    - Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele.
    - Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem.
    - Nenavštěvovaly internetové stránky s eticky nevhodným obsahem.
    - Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů.
    - Nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy.

Účty a hesla

• Dodavatel nikdy nikomu nesděluje hesla, ani se nesnaží získat hesla zaměstnanců ČT, externistů a dodavatelů ČT.

• Heslo je dodavatelem vždy tvořeno unikátně, tj. nepoužívá jedno stejné heslo pro více účtů, aby prozrazení jednoho hesla neohrozilo ostatní účty.

• Je zakázáno používat stejná hesla pro soukromé účely a pro účely spolupráce s Českou televizí.

• Hesla tvoří dodavatel s minimální délkou 12 znaků a splněním 3 z těchto 4 podmínek:

  - Malé písmeno
  - Velké písmeno
  - Číslo
  - Znak (#, @, &, !, atd.)
- Hesla si dodavatel v pravidelných intervalech mění, i tam, kde to není vynucené.
- Je zakázáno zaznamenávat hesla na papír, do souborů nebo na přenosná zařízení a média nebo je ukládat do internetových prohlížečů. Pro ukládání hesel je možné využít schválený správce hesel.
- V případě, že má dodavatel podezření, že jeho heslo mohlo být vyzrazeno, je povinen jej neprodleně změnit a nahlásit událost na IT Helpdesk (+420 261 131 777, Helpdesk@ceskatelevize.cz).
- Dodavatel chrání autentizační prostředky a údaje. Nikdy neposkytuje chráněné autentizační prostředky (jméno, heslo, pin, OTP) cizí osobě.

E-mail

- Dodavatel dbá zvýšené opatrnosti, zejména u neočekávaných příchozích e-mailů nebo neznámých odesílatelů. Nikdy neotvírá přílohu emailu ani nekliká na odkaz v emailu, dokud nerozpozná, zda se nejedná o podvodný email.
- Dodavatel se nepodílí s prostředky Objednatele na šíření spamu ani škodlivého softwaru.
- Dodavatel nerozesílá nic, co by obtěžovalo příjemce nebo vrhlo špatné světlo na ČT.

Internet

• Dodavatel nepřistupuje při výkonu činnosti pro Českou televizi na webové stránky, které nepotřebuje ke své činnosti, zvláště ne na stránky s nevhodným obsahem (pornografie, drogy, násilí apod.) nebo na stránky, které nelegálně sdílejí filmy, seriály a podobné soubory (torrent, warez atp.), nebo na stránky pro sdílení souborů (např. uloz.to atp.).

• Je zakázáno používat veřejná či soukromá úložiště v internetu (např. disk Google, Dropbox, OneDrive, domácí storage NAS, …) pro data ČT.

• Pokud dodavatel potřebuje obecně nevhodné materiály pro svou práci, musí být prokazatelná vazba na výkon sjednané činnosti a povolena výjimka.

Vypůjčené věci – technická zařízení (např. počítač, notebook, mobilní telefon, tablet)

• Dodavatel nezasahuje do hardwarové nebo softwarové konfigurace počítače a telefonu, s výjimkou uživatelských nastavení nebo schválených připojitelných zařízení typu USB.

• Dodavatel nesmí měnit schválené bezpečnostní nastavení pracovního vybavení, zejména vypínat nebo obcházet bezpečnostní mechanizmy (např. firewall, antivirový program, mazat aplikaci ČT MDM, apod.).

• Na počítač může dodavatel instalovat software z Centra software (který spravuje Úsek IT) a na mobilní telefon nebo tablet může instalovat aplikace pouze z Apple Store, Google Obchod Play nebo Samsung Galaxy Store či jiného zdroje schváleného Úsekem IT.

• Dodavatel nestahuje a nepoužívá neschválený software na počítači, ani když je zadarmo.

• Při používání výměnných médií (CD, DVD, flashdisk, USB disk, apod.) dodavatel dbá zvýšené opatrnosti a médium zkontroluje antivirovým programem. V případě nálezu podezřelého souboru se ihned obrátí na IT Helpdesk.

• Aktualizace systému, programů a restarty zařízení dodavatel zbytečně neodkládá a provede je v nejbližším možném termínu.

• Dodavatel bere na vědomí, že aktualizace systému a programů nebo restart zařízení mohou být z bezpečnostních důvodů vzdáleně vynuceny, a proto vždy průběžně ukládá svou práci na počítači, aby nepřišel o neuložená data.

Data (obrazové a zvukové materiály, papírové i elektronické dokumenty a jiné informace)

• Dodavatel vždy chrání data České televize, a proto dodržuje pravidlo prázdného stolu (nenechává dokumenty, média nebo mobilní zařízení bez dozoru a neuzamčená) a vždy uzamyká počítač, pokud ho opouští zapnutý (spořič obrazovky s heslem – pomocí kláves WIN+L, odhlášení uživatele).

• K ukládání či vyměňování souborů s Českou televizí smí dodavatel používat pouze úložiště schválená Českou televizí.

• Data ve vlastnictví České televize, popřípadě dodavatelů a externistů, ke kterým má dodavatel přístup, smí používat pouze pro výkon činnosti pro Českou televizi.

• Data, ke kterým nemá Česká televize autorská práva nebo licenci, nesmí mít dodavatel uložena na pracovních zařízeních typu počítač nebo notebook ani pro soukromé použití.

- Dodavatel zajistí, že všechny osobní údaje zpracovávané v rámci plnění smlouvy budou chráněny v souladu s platnými právními předpisy o ochraně osobních údajů, včetně GDPR.

Malware (škodlivé programy) a nežádoucí aktivity

• Pro ochranu před malwarem (např. počítačové viry, ransomware, spyware, těžba kryptoměn) musí mít počítač nainstalovaný schválený antivirový program a dodavatel jej nesmí vypnout.

• Jakékoli podezření na malware, kliknutí na phishingový emaily, nežádoucí aktivity nebo chybová hlášení antivirového programu (např. nelze ho aktualizovat, ochrana je vypnutá, nelze odstranit malware) hlásí dodavatel na IT Helpdesk (+420 261 131 777, Helpdesk@ceskatelevize.cz).

Vzdálený přístup k informačním systémům ČT (IS ČT)

• Vzdálený přístup k IS ČT dodavatel využívá pouze na schváleném ICT zařízení (vypůjčený notebook, apod.).

• Dodavatel udržuje přístupové údaje ke vzdálenému přístupu v tajnosti a pravidelně je aktualizuje.

• Pro VPN připojení dodavatel využívá řešení Checkpoint VPN. Pro připojení je vyžadována 2FA.

• Dodavatel nesmí pro připojení do sítě ČT využívat veřejné WIFI sítě.

Použití vlastního technického zařízení pro vzdálený přístup k informačním a komunikačním systémům ČT (např. počítač, notebook, mobilní telefon)

• Vzdálený přístup k IS ČT z vlastního zařízení je možný pouze po jeho schválení Českou televizí.

• Dodavatel používá pouze schválený způsob vzdáleného připojení a nesnaží se obcházet jeho bezpečnostní nastavení a mechanismy.

• Pro vzdálený přístup používá dodavatel pouze zařízení, na kterém:

- má instalovaný výrobcem podporovaný operační systém, na který jsou dostupné aktualizace,
- pravidelně aktualizuje aplikace, ovladače a operační systém bezodkladně po vydání aktualizací výrobcem,
- má instalovaný aktuální a funkční antivirový program (anti-malware ochranu),
- nemá nelegální software nebo data,
- nepoužívá pro běžnou práci (i pro vzdálené připojení do ČT) účet se zvýšeným administrátorským oprávněním, tento používá výhradně k instalaci softwaru nebo úpravě konfigurace operačního systému.

Bezpečnostní incident

• Bezpečnostní incident je situace, která může znamenat ohrožení bezpečnosti systémů nebo dat České televize, proto podezření na bezpečnostní incident nebo neobvyklé chování počítače nebo telefonu hlásí dodavatel na IT Helpdesk (+420 261 131 777, Helpdesk@ceskatelevize.cz).

• Dodavatel bere na vědomí, že IT ČT může zablokovat jeho přístup k informačním a komunikačním systémům ČT v případě výskytu bezpečnostní události nebo incidentu.

• Dodavatel poskytuje veškerou nutnou součinnost pro úspěšné zvládnutí případného kybernetického bezpečnostního incidentu.

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:

- Bez zbytečného odkladu hlásit všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na ČT, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.
- Bez zbytečného odkladu a po dohodě s ČT realizovat opatření, v dohodnutých termínech, ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu, který může mít bezpečnostní dopad

Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků, jehož příčina je na straně dodavatele, nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany ČT. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.

Ztráta nebo krádež vypůjčené věci (technické zařízení, např. počítač, notebook, mobilní telefon, tablet)

• Vypůjčená zařízení nesmí být ponechána bez dozoru a na nechráněných místech (např. v automobilu, automatické úschovné schránce či šatní skříňce na sportovišti). To platí i pro telefony, tablety nebo výměnná média typu CD/DVD, paměťové karty, USB flashdisky, přenosné disky, apod.

• Dodavatel se přiměřeně stará o vypůjčená technická zařízení i v interních prostorách České televize.

• Ztrátu či odcizení ICT zařízení dodavatel neprodleně ohlásí na IT Helpdesk a odpovědným osobám v ČT.

Bezpečnostní nástroje

• Dodavatel realizuje přístup z mobilního zařízení do prostředí ČT pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).

• Dodavatel připojuje do prostředí ČT pouze ta zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno.

• Dodavatel bez zbytečného odkladu deaktivuje všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.

• Na aktiva ČT dodavatel neinstaluje a nepoužívá následující nástroje, pokud nejsou součástí předmětu plnění:

o Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

o Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

o Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, aplikací a jejich verzí, apod.

- Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
- Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí ČT.

• Dodavatel připojuje do prostředí ČT pouze zařízení ICT, která splňují následující požadavky:

- Musí být aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče, balíku MS Office, Javy a případně dalšího softwarového vybavení, pokud je používáno).
- Musí mít nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
- Používaná paměťová média (flash disky, diskety, CD a DVD nosiče, apod.) musí být před použitím zkontrolována na zařízení s aktualizovanou antivirovou ochranou.
- Musí být připojována pouze do vyhrazené bezpečnostní zóny a způsobem definovaným v provozní nebo projektové dokumentaci. Pokud v provozní nebo projektové dokumentaci definováno není, předpokládá se, že připojení takových zařízení není dovoleno.