

**Odbor informačních služeb
Oddělení informačních služeb - ústředí**

Vážený pan

.....

V Praze dne 4. 3. 2015

Zn.: Z-03333-CEN-15

Počet listů/příloh: 2/1

Vyřizuje: Mgr. Štěpánka Čejková

Tel.: 274 052 430

E-mail: stepanka.cejkova@czso.cz

**Věc: Odpověď na žádost o informace podle zákona č. 106/1999 Sb., o svobodném
přístupu k informacím, ve znění pozdějších předpisů**

Vážený pane,

na základě Vaší žádosti ze dne 22. února 2015 Vám v příloze zasílám vyplněný dotazník bezpečnosti ICT prostředí.

S pozdravem

Vlastní dotazník bezpečnosti ICT prostředí

Jméno subjektu / IČO: Český statistický úřad / 00025593

Korespondenční adresa subjektu: Na Padesátém 81, Praha 10



Část dotazníku určena pro kategorizaci společnosti (bude anonymizováno)



Část dotazníku pro statistickou analýzu

Otázka	Odpověď				Vysvětlení
Velikost podniku?	MALÁ	STŘEDNÍ	<input checked="" type="checkbox"/> VELKÁ		Rozdělení je očekáváno následující (počty osob jsou myšleny včetně externích spolupracovníků): <ul style="list-style-type: none"> • Malá: do 50 osob • Střední: do 250 osob • Velká: nad 250 osob
Kolik orientačně využíváte ve společnosti počítačů?	2000				
Týká se Vás zákon 181/2014 Sb. o kybernetické bezpečnosti?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		Zákon 181/2014 Sb. platí od 1. 1. 2015 a definuje, mimo jiné, požadavky na bezpečnostní politiku společnosti.
Je vaše společnost držitelem certifikace ISO/IEC 27000?	ANO	<input checked="" type="checkbox"/> NE	NEVÍM		Řada mezinárodně platných norem ISO/IEC 27000 je zaměřena na oblast bezpečnosti informací. Zákon 181/2014 Sb. z ní významně vychází.
Je u Vás zavedena bezpečnostní politika ICT?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		Bezpečnostní politikou jsou myšleny např. definovaná pravidla pro řízení aktiv, definice jejich vlastníků, požadavek na provozní deníky, klasifikace dokumentů apod.
Vedení společnosti formálně deklarovalo podporu k udržování a vytváření podmínek pro zajištění bezpečnosti informací.	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		Formální deklarací je myšlena existence, v rámci společnosti známého, závazku vedení společnosti k podpoře bezpečnosti informací.
Zaznamenala Vaše společnost v průběhu minulého roku bezpečnostní incident?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		Příklad incidentu: únik důvěrných informací na veřejnost, kybernetický útok na webové servery apod.
Máte zaveden proces řešení bezpečnostních incidentů?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		
Jsou zaměstnanci pravidelně školeni v oblasti bezpečnosti ICT?	ANO	<input checked="" type="checkbox"/> NE	NEVÍM		
Jsou otázky bezpečnosti ICT pravidelně projednávány na úrovni vedení společnosti?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		
Máte zpracovávánu aktuální analýzu rizik?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		
Klasifikujete aktiva z pohledu bezpečnosti (a v jaké míře) včetně stanovení jejich vlastníka?	Do 25 %	Do 50 %	<input checked="" type="checkbox"/> Do 75 %	100 %	
Kolik osob je přímo odpovědných za bezpečnost ICT prostředí ve společnosti?	5				Pokud není tato odpovědnost stanovena, prosím o uvedení počtu 0.
Využíváte pro ochranu datové sítě technologie IDS/IPS a SIEM?	NIC	IPS	SIEM	<input checked="" type="checkbox"/> OBĚ	IPS (Intruder prevention / detection system) SIEM (Security Incident & Event Monitoring)
Provozujete ve společnosti SCADA systémy?	ANO	<input checked="" type="checkbox"/> NE	NEVÍM		SCADA (Supervisory Control And Data Acquisition, tedy dispečerské řízení a sběr dat)
Jak často realizujete penetrační testování (bez rozlišení typu, počtu informačních systémů apod.)	NE	<input checked="" type="checkbox"/> ROČNĚ	MĚSÍČNĚ	ČASTĚJI	Penetrační testy ověřují bezpečnost prostředí simulací kybernetického útoku. Pokud penetrační testy nerealizujete, uveďte, prosím, „NE“.
Máte pocit, že je možné bezpečnost ICT outsourcovat?	<input checked="" type="checkbox"/> ANO	NE	NEVÍM		Outsourcingem je myšleno delegování plné správy klíčových bezpečnostních technologií (FW, IPS, SIEM apod.) jiné společnosti.