V Praze dne 22. 2. 2015

Věc: **Prosba o poskytnutí podkladů pro zpracování bakalářské práce**

Dobrý den,
rád bych Vás poprosil o pár minut Vašeho času – prosím Vás velice o spolupráci ve formě poskytnutí dat v oblasti bezpečnosti ICT, která budou sloužit jako podklad pro dokončení mé bakalářské práce na téma: „Návrh bezpečnostní politiky informačních technologií v prostředí středně velké společnosti“.
Pokud jste veřejnoprávní instituce, žádám Vás o tyto informace na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
Data budou použita pouze jako zdroj pro tvorbu statistické analýzy a na základě ní provedeného zhodnocení. Identifikace subjektu bude využita pouze za účelem kategorizace společnosti. Pokud budete tak hodní a rozhodnete se poskytnout mi požadovaná data (i třeba pouze jejich část), odpovězte, prosím, nejpozději do 12. 3. 2015.

Veškerá Vámi poskytnutá **data budou pro uvedený účel po obdržení anonymizována** a připojena k závěrečné práci formou přílohy bez jakýchkoliv, společnost identifikujících, údajů. V případě Vašeho požadavku poskytnu závěrečnou práci včetně příloh k revizi před odesláním k tisku za účelem kontroly splnění této anonymizace. Poskytnutá data (včetně vazby společnosti a dotazníku) budou bezpečně skartována ihned po zpracování.
Vzhledem k tomu, že jsem zaměstnán ve společnosti zabývající se, mimo jiné, i bezpečností ICT (Unicorn Systems a.s.) a mohla by vzniknout pochybnost ohledně sdílení informací se zaměstnavatelem, zcela jednoznačně deklaruji, že tato **data nebudou v jakékoliv formě (ústní, elektronické, písemné, apod..) poskytnuta třetí straně** a budou výhradně určena pouze pro účely této bakalářské práce. Jsem si zároveň vědom veškerých zákonných a právních důsledků související s případným nedodržením této deklarace.

V rozsahu oslovených společností jsou zahrnuty jak soukromoprávní subjekty aktivní v různých oblastech podnikání, tak státní organizace včetně ministerstev, krajských, městských úřadů a dalších organizací.

Dotazník je dostupný i na URL adrese: http://login.oursurvey.biz/dotaznik-10455 pro elektronické vyplnění (tuto formu vyplnění preferuji).

V případě jakéhokoliv doplňujícího dotazu týkajícího se dotazníku mě neváhejte kontaktovat, avšak vzhledem k množství oslovených společností preferuji elektronickou formu komunikace.

Děkuji Vám velice za poskytnutou spolupráci, Vámi předané informace pro mě budou významným informačním vstupem.

J[redacted]K[redacted]

[redacted]

[redacted]

V Praze dne 22. 2. 2015

Vlastní dotazník bezpečnosti ICT prostředí

Jméno subjektu / IČO: .....

Korespondenční adresa subjektu: .....

Část dotazníku určena pro kategorizaci společnosti (bude anonymizováno)

Část dotazníku pro statistickou analýzu

Otázka	Odpověď				Vysvětlení
Velikost podniku?	MALÁ	STŘEDNÍ	VELKÁ		Rozdělení je očekáváno následující (počty osob jsou myšleny včetně externích spolupracovníků): • Malá: do 50 osob • Střední: do 250 osob • Velká: nad 250 osob
Kolik orientačně využíváte ve společnosti počítačů?					
Týká se Vás zákon 181/2014 Sb. o kybernetické bezpečnosti?	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	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?	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.	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?	ANO	NE	NEVÍM		Příklad incidentu: únik důvěrných informací na veřejnost, kybernetický útok na webové servery apod.
Máte zaveden proces řešení bezpečnostních incidentů?	ANO	NE	NEVÍM		
Jsou zaměstnanci pravidelně školeni v oblasti bezpečnosti ICT?	ANO	NE	NEVÍM		
Jsou otázky bezpečnosti ICT pravidelně projednávány na úrovni vedení společnosti?	ANO	NE	NEVÍM		
Máte zpracovánu aktuální analýzu rizik?	ANO	NE	NEVÍM		
Klasifikujete aktiva z pohledu bezpečnosti (a v jaké míře) včetně stanovení jejich vlastníka?	Do 25 %	Do 50 %	Do 75 %	100 %	
Kolik osob je přímo odpovědných za bezpečnost ICT prostředí ve společnosti?					Pokud není tato odpovědnost stanovena, prosím o uvedení počtu 0.
Využíváte pro ochranu datové sítě technologie IDS/IPS a SIEM?	NIC	IPS	SIEM	OBĚ	IPS (Intruder prevention / detection system) SIEM (Security Incident & Event Monitoring)
Provozujete ve společnosti SCADA systémy?	ANO	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	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?	ANO	NE	NEVÍM		Outsourcingem je myšleno delegování plné správy klíčových bezpečnostních technologií (FW, IPS, SIEM apod.) jiné společnosti.

J[redacted]K[redacted]

[redacted]