Kulatý stůl s názvem
Kyberbezpečnost: Post-covidová nová realita v České republice

DIGITAL SUSTAINABILITY FORUM

Dne 31. března 2021 se uskutečnil expertní kulatý stůl na téma Kyberbezpečnost: Post-covidová nová realita v České republice, který pořádal Aspen Institute Central Europe ve spolupráci s Microsoft Česká republika a s Ústavem práva a technologií Právnické fakulty Masarykovy univerzity. Akce se konala v rámci diskusní platformy s názvem Digital Sustainability Forum. Experti ze soukromé i státní sféry se setkali, aby diskutovali o dlouhodobých i aktuálních výzvách v rámci kyberbezpečnosti. Věnovali se i vlivům globální pandemie na kyberbezpečnost a definovali konkrétní doporučení pro následující období.

Důležitým prvkem kyberbezpečnosti je interdisciplinarita, která se prolíná napříč obory jako jsou technologie, právo, státní i soukromá sféra, zdravotnictví a další. Kombinace všech těchto oblastí je podstatná pro správné pochopení klíčových otázek kybernetické bezpečnosti. Důležitost kyberbezpečnosti významně roste se zvyšující se závislostí společnosti na digitalizaci.

Kulatý stůl byl otevřen otázkou: Jaká je důvěra lidí v technologie a jaké jsou naše schopnosti využívat je bezpečně? Faktem je, že každodenní využívání technologií přináší spoustu výhod, ale i rizik. Je důležité, abychom se naučili daná rizika rozpoznávat a pracovat s nimi. Například Microsoft Digital Crimes Unit (DCU) se zaměřuje na kyberbezpečnost, unikátním způsobem odhaluje a předchází kybernetickým útokům.

Téma kyberbezpečnosti bylo diskutováno v několika oblastech.

ROLE STÁTU PŘI ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

Právní rámec kybernetické bezpečnosti v České republice prošel v uplynulých letech řadou změn, zejména na úrovni prováděcích předpisů. Jedná se o poměrně komplexní a komplikovaný set pravidel. Vede tato právní úprava k reálnému zvýšení kybernetické bezpečnosti?

Role státu při zajišťování kyberbezpečnosti je nepostradatelná, avšak stát není jediným aktérem. Kyberbezpečnost je komplexním tématem, které má velký přesah do zahraničních aktivit státu, soukromé i akademické sféry. Klíčovým faktorem je zde důvěra a také koordinace mezi jednotlivými subjekty.

Regulace kyberbezpečnosti ze strany státu může hrát důležitou roli pouze za předpokladu, že je smysluplná a umí pracovat s riziky. Regulace není jediným řešením, nýbrž jedním z nástrojů.

Regulace kybernetické bezpečnosti byla v posledních letech doplněna řadou prováděcích předpisů. Jedním z hlavních přínosů tohoto legislativního vývoje by mohlo být zjednodušení procesu získávání peněz na zajištění kyberbezpečnosti ve státním sektoru.

Se zvyšujícími se kybernetickými riziky a procesem digitalizace by legislativa mohla být detailnější i přísnější, ale to by nebylo v souladu s principem minimálního zásahu, na kterém je tato legislativa postavena. Do budoucna si lze představit její další úpravy formou tzv. „postupného dotahování šroubů", tak aby regulované osoby měly čas se novým požadavkům přizpůsobit. Regulace by měla na dané subjekty dopadat postupně, aby byly schopny ji absorbovat, a zároveň nebýt odtržená od jejich každodenní reality.

V rámci státu jsou různé pohledy na kyberbezpečnost. Hrozby jsou komplexní a zahrnují jak hybridní hrozby, tak i hrozby narušení informačního prostoru pomocí šíření dezinformací apod. Hlavní úsilí by mělo být zaměřeno na nalezení rovnováhy mezi rozvojem a implementací technologií a bezpečností.

Pohled soukromé sféry je pro stát významný. Fundamentálním rozdílem mezi byznysem a veřejnou správou je, že ve státní správě zatím neumíme vyčíslit ztráty způsobené případnými bezpečnostními incidenty. Vyčíslení ztrát by mohlo fungovat jako motivace k vyšším investicím do kyberbezpečnosti.

Velmi důležité je také celkové pojetí kyberbezpečnosti v organizacích. Je hlavně třeba změnit mentální nastavení managementu a uvědomit si, že kyberbezpečnost není pouze věcí IT oddělení, ale měla by být jednou z priorit leadershipu všech institucí.

KYBERNETICKÁ BEZPEČNOST VE ZDRAVOTNICTVÍ

Zdravotnictví v poslední době čelilo několika kybernetickým útokům. Lze to interpretovat tak, že situace ve zdravotnictví je tak špatná, že zdravotnická zařízení nejsou schopna ustát dané útoky, nebo je to pouze současnou covidovou situací, kdy je zdravotnictví přetížené a je tedy "vhodným" cílem pro hackery?

Zdravotnictví je heterogenní sektor, který zahrnuje nejen nemocnice, ale i ambulantní praxe a centrální systémy. Zdravotnictví má pověst poměrně snadného cíle, z nějž lze získat hodnotná data. Nejde jen o osobní a zdravotní údaje, ale i údaje potřebné pro poskytování zdravotní služby, distribuce léčiv a další.

Kromě klasických informačních systémů jsou ve zdravotnictví také využívány zdravotnické přístroje se speciálním softwarem, u kterých aspekt kybernetické bezpečnosti buď není dostatečně akcentován nebo není řešen vůbec.

Informatizace zdravotnictví nezřídka výrazně předcházela snaze zajistit kybernetickou bezpečnost, a zdravotnické programy tak nejsou koncepčně připraveny na to, aby se dokázaly vypořádávat s kybernetickými hrozbami. V rámci priorit zdravotnických zařízení je často kybernetická bezpečnost informačních technologií na posledním místě.

Důležité je vnímání kyberbezpečnosti mezi aktéry ve zdravotnictví a snaha najít rovnováhu mezi tím, aby se s ohledem na kyberbezpečnost neznemožňoval výkon jejich práce, ale aby zároveň byla dodržována rozumná bezpečnostní opatření. Klíčové je také, aby si i pacienti uvědomovali, že jejich osobní a zdravotní údaje mají nějakou hodnotu a podle toho k nim přistupovali.

KYBERNETICKÁ BEZPEČNOST Z POHLEDU BUSINESSU

Spousta firem se musela vyrovnat s přechodem na home office. Jaký problém představuje větší míra dálkové komunikace z hlediska kyberbezpečnosti? Budou firmy investovat více peněz do bezpečnosti v kybernetickém prostoru?

Pandemie covidu zrychlila celý proces digitalizace. Silnější potřeba zajistit kyberbezpečnost v businessovém prostředí vyvstala hlavně s větším tlakem na to, aby organizace přecházely na virtuální řešení umožňující práci z domova.

Komerční sféra digitalizaci hodně akcelerovala a je si vědoma potřeby investic do kyberbezpečnosti. Digitalizace bude čím dál tím větším zdrojem příjmů, a proto je důležité prioritizovat strategické investice do digitálních technologií a jejich zabezpečení. Legislativa a regulace pak mohou businessu pomoci při definování celkového směřování s ohledem na kyberbezpečnost.

VZDĚLÁVÁNÍ SPOLEČNOSTI V KYBERBEZPEČNOSTI

Vzhledem k masivnímu přechodu společnosti do digitálního prostředí a nárůstu kybernetických útoků a jevů, jako je (cyber)phishing, je klíčovým tématem také vzdělávání společnosti.

Mělo by se podpořit vzdělávání široké veřejnosti, zvýšit tak její povědomí o kyberbezpečnosti a vyzdvihnout témata, jako je správné chování na internetu, aby byla kybernetická rizika minimalizována.

Důležitý je meziresortní přesah ve vzdělávání odborníků na všech úrovních. Dobrým příkladem by mohlo být propojení mezi SŠ, VOŠ a VŠ. To by mohlo přispět ke zvýšení počtu občanů se solidním základním kybernetickým vzděláním, na kterém by se dalo posléze stavět. Nesmí být také opomíjeno udržování prestiže a následné využitelnosti tohoto povolání na trhu práce.

ZÁVĚRY A DOPORUČENÍ

Kybernetická bezpečnost jako manažerská priorita: Účastníci se shodli, že je důležité, aby kybernetická bezpečnost byla strategickou prioritou vedení organizace a jako taková se promítala do všech oblastí činnosti organizace, jak ve státní správě, tak v soukromém sektoru. Účinnou kybernetickou bezpečnost nelze zajistit, pokud bude tato oblast delegována na juniorní pracovníky. K tomu mohou napomoci i právní nástroje zaměřené na odpovědnost statutárních orgánů za dodržování povinností organizace v oblasti kybernetické bezpečnosti.

Role regulace a její dopady na investice do kybernetické bezpečnosti: Účastníci diskuse se shodli, že význam regulace je klíčový ve státní správě. Důležitým dopadem regulace je lepší obhajitelnost investic do kybernetické bezpečnosti. V soukromém sektoru regulace tuto roli nehraje, protože soukromé firmy mohou lépe vyčíslit hodnoty kybernetické bezpečnosti a případných ztrát hrozících při úspěšném kybernetickém útoku. Pro organizace státní správy může být obtížné odhadnout náklady nebo jinou ztrátu, která by vznikla např. dočasnou nedostupností určité agendy.

Kybernetická bezpečnost ve zdravotnictví: Kybernetické útoky na česká zdravotnická zařízení v posledních letech nejsou náhodné a ukazují na určité systémové problémy kybernetické bezpečnosti v tomto sektoru. Zdravotnická zařízení mají pověst snadných cílů kybernetických útoků, které skýtají cenná data. Jednou z priorit je proto zlepšení pověsti o úrovni kybernetické bezpečnosti českých zdravotnických zařízení. Další prioritou je také zajistit pro zdravotnická zařízení účinné nástroje podpory pro odhalování a řešení kybernetických útoků, a posílit tak jejich schopnost reagovat na kybernetické incidenty. Významnou roli v této oblasti má také zvýšení kybernetické prevence, navázání další spolupráce s vojenskými složkami a získávání odborníků v oblasti kyberbezpečnosti.

Vzdělávání odborníků jako klíčová priorita: Panuje shoda, že klíčovou oblastí je další vzdělávání odborníků na všech úrovních. Je velmi důležité zvýšit prestiž povolání v kybernetice, které vede k růstu zájmu o vzdělávání v této oblasti. Je nutné také výrazně zvýšit počet absolventů vzdělaných v oblasti kybernetické bezpečnosti – těchto odborníků je na trhu velký nedostatek, který nadále roste. Zároveň je klíčové se zaměřit i na vytvoření koncepce a vzdělávání konkrétních profilů odborníků v této oblasti, které státní správa i komerční sféra potřebuje. Podstatné je i zvyšování povědomí běžných uživatelů, jak se bezpečně chovat na internetu, a tím i minimalizovat kybernetické útoky.