EURACTIV

BEZPEČNÁ DIGITÁLNA BUDÚCNOSŤ

s podporou: AmCham Slovakia

ŠPECIÁL | 2. OKTÓBER 2018
Výstup z konferencie Responsibility in Digital Age: Awareness in Cyber Security

EURACTIV

BEZPEČNÁ DIGITÁLNA BUDÚCNOSŤ

ŠPECIÁL | 2. OKTÓBER 2018
http://bit.ly/BezpecnaDigitalnaBuducnost

Významný rast digitálnej ekonomiky ide ruka v ruke s rastúcim významom počítačovej bezpečnosti a ochrany údajov. V dôsledku toho dochádza v posledných mesiacoch k niekoľkým regulačným zmenám na Slovensku aj v EÚ.

Súkromné spoločnosti okrem toho venujú väčšiu pozornosť zvyšovaniu povedomia o rizikách a hrozbách, ktoré prichádzajú s exponenciálnym rastom technológií. Investujú viac do informačných kampaní pre svojich obchodných partnerov a zamestnancov. Kybernetická bezpečnosť sa bude musieť tiež stať súčasťou formálneho vzdelávacieho programu, aby sa čo najskôr vyrovnal s požiadavkami generácie Z.

Obsah

NÁZOR

Ronald Blaško:
Kybernetické hrozby a útoky ohrozujú našu modernú ekonomiku

Ronald Blaško | výkonný riaditeľ, Americká obchodná komora v SR

Ronald Blaško, výkonný riaditeľ [AmCham Slovakia]

Ohrozujú naše strategické a konkurenčné výhody a ročne stoja spoločnosti a celú ekonomiku milióny eur. Malé aj veľké spoločnosti musia akceptovať skutočnosť, že útoky v digitálnom priestore predstavujú pre ich zisky obrovské a okamžité riziko.

Je preto nutné brať ochranu našich firiem a ekonomiky ako celku pred touto sústavne rastúcou hrozbou veľmi vážne. Diskusiu na tému kybernetickej bezpečnosti musíme viesť naprieč štátnymi organizáciami a súkromnými firmami. Počnúc rokovacími miestnosťami, kde sa stretávajú predstavenstvá spoločností, cez pracovníkov pre styk so zákazníkmi až po back office.

Jedným z dôvodov prečo zdôrazňujeme nutnosť kybernetickej bezpečnosti je, že potrebujeme šíriť osvetu, aby sme spoločne pomohli zlepšiť úroveň ochrany slovenskej ekonomiky. Našim zámerom je ponechať ekonomiku otvorenú pre podnikanie a zároveň zabezpečiť, aby boli firmy aj občania v online prostredí v bezpečí.

Významnou časťou agendy slovenskej vlády sú investície do digitalizácie.

Podobne ako prístup k pitnej vode a elektrine, aj prístup k digitálnym produktom a službám sa stal zásadnou zložkou infraštruktúry nevyhnutnou pre podnikanie. Hospodársky rast a úspech v dnešnej digitálnej ére bez nich jednoducho nie je možný.

Znamená to rýchlejší a výhodnejší spôsob komunikácie, výmeny nápadov a nových ideí, poskytovania produktov a služieb zákazníkom. A predstavuje aj prístup na globálne trhy.

Onedlho bude mať každý občan Slovenska príležitosť vyťažiť z digitálnej ekonomiky pozitíva, ako sú kvalitné tovary, či služby ako si aj celkovo zvyšovať kvalitu života.

A keďže dúfame v lepšie využitie internetu, musíme tiež zabezpečiť online prostredie, ktoré bude čo najlepšie chránené a bezpečné. Je to rovnako dôležité pre medzinárodnú reputáciu našej krajiny, ako bezpečného miesta pre podnikanie.

Naša závislosť na zariadenia pripojené na sieť a na nové technológie ako celok rastie úmerne s čoraz väčšími hrozbami v oblasti kybernetickej bezpečnosti.

Kým vy tvrdo pracujete a budujete produktívnu a konkurencieschopnú ekonomiku, kybernetické útoky ju môžu zastaviť, či dokonca – čo je ešte horšie – zraziť ju na kolená.

Ako poznamenal Leon Panetta, bývalý minister obrany USA: „Najbližší Pearl Harbor, ktorému budeme čeliť by poľahky mohol predstavovať kybernetický útok, ktorý ochromí naše energetické systémy a rozvodnú sieť."

Na jeden relatívne nedávny prípad z nášho susedstva si možno spomínate.

V noci 23. decembra 2015 sa Ukrajina stala prvou krajinou na svete, ktorá sa stala obeťou overeného rozsiahleho kybernetického útoku na svoju kritickú infraštruktúru. Viac než 225 000 Ukrajincov sa z ničoho nič ocitlo bez kúrenia a svetla po útoku na časť rozvodnej siete ich krajiny.

Všetci vieme, že moderné technológie poskytujú nové príležitosti aj osobám, ktoré sú motivované zločinnými alebo nepriateľskými zámermi. Jednoducho povedané, zákerné kybernetické útoky sa dajú uskutočniť z ktoréhokoľvek miesta na svete a v ľubovoľnom čase.

Z globálneho hľadiska sme každý rok svedkami čoraz vyššieho počtu firiem a občanov, ktorí sú obeťami kybernetických útokov, či už sa jedná o drobné útoky vo forme počítačových vírusov a škodlivého softvéru, podvodné operácie s kreditnými kartami, online podvody, phishing alebo prípady krádeže identity.

A hoci Slovensko ešte nezažilo taký rozsiahly kybernetický útok, akého svedkami sme boli na Ukrajine alebo v Estónsku, nie je a nebude voči takýmto hrozbám imúnne.

Jeden príklad za všetky: Marc Goodman vo svojej knihe „Future Crimes" píše, že: „Podľa správy FBI jedna krajina potajomky vyškolila armádu 180 tisíc kybernetických špiónov, ktorí podniknú neuveriteľných 90 tisíc útokov ročne len proti sieťam amerického ministerstva obrany."

Jeden z nedávnych prípadov tiež zahŕňal útok na Sony Pictures, v rámci ktorého boli odcudzené a následne online zverejnené citlivé informácie patriace tejto spoločnosti.

Prípadne vyhlásenie spoločnosti Facebook z 28.9.2018, v ktorom spoločnosť priznala, že hackeri jej ukradli prihlasovacie údaje umožňujúce prístup k 50 miliónom používateľských účtov, čo následne okamžite poslalo cenu jej akcií prudko nadol. A to je len niekoľko príkladov.

Ak chceme maximálne zužitkovať najnovšie technológie, aby sme zvýšili náš blahobyt a prosperitu, musíme tiež urobiť maximum pre pochopenie súvisiacich rizík a ich manažment.

Jeden z najväčších problémov v oblasti kybernetickej bezpečnosti je samotná definícia celkového prostredia. Je to spôsobené veľkou rozmanitosťou v typológii aktérov, ktorí páchajú útoky, škôd, ktoré sa snažia spôsobiť a cieľov, na ktoré sa zameriavajú.

Čo sa týka samotných útočníkov, na Slovensku verejnosť nemá vedomosť o špionáži podporovanej vládami iných krajín a len okrajovo si uvedomuje existenciu organizovaných zločineckých skupín. Je pravdepodobné, že na nás útočia extrémisti či dokonca aktivisti, bojujúci za svoje vlastné ciele. Celkom určite osamelí kybernetickí hackeri a nahnevaní alebo sklamaní „insideri", teda jednotlivci pracujúci vo vnútri danej organizácie.

Jestvuje mnoho druhov hrozieb a kybernetických útokov s cieľom uškodiť. Nielen ťažko objaviteľné tzv. „zero-day" útoky, ale tiež cielený spam, emaily posielané za účelom podvodu alebo krádeže a škodlivý software, ktorého cieľom je narušiť a poškodiť rôzne systémy. A všadeprítomná špionáž s cieľom získať hospodárske, alebo strategické výhody.

Cieľov je celá škála. V podstate ktokoľvek — počnúc jednotlivcami alebo malými a strednými podnikmi, ktorým chýbajú zdroje na to, aby riešili tento problém, až po nadnárodné korporácie podnikajúce v strategických odvetviach a kritickej infraštruktúre. A samozrejme, ani vlády nie sú mimo ohrozenia.

Tieto útoky si vyžadujú komplexnú a koordinovanú reakciu a naše vládne orgány v tomto smere zohrávajú významnú úlohu.

Zahŕňa to políciu na boj proti kybernetickému zločinu, vládne agentúry, ktorých úlohou je reagovať na pokročilé hrozby a chrániť prvky našej kritickej informačnej infraštruktúry.

Otázka bezpečnosti však nemôže byť ponechaná výlučne na vládu. Vládne orgány nemajú exkluzívne práva na odborné znalosti a skúsenosti v oblasti kybernetickej bezpečnosti, najmä, ak si uvedomíme, že technológie a hrozby sa sústavne menia a vyvíjajú.

Dovoľte mi len jeden príklad, ktorý dokazuje, že riešenie nie vždy spočíva v objeme investovaných financií a od-

borných znalostiach. Ako píše Alex Klimburg vo svojej najnovšej knihe „The Darkening Web“: „Prieskum spoločnosti McAfee z roku 2012 medzi IT bezpečnostnými odborníkmi pracujúcimi pre vládne orgány v USA zaradil Spojené štáty na jednu úroveň spolu s krajinami tretieho sledu s celkovou kvalitou národnej kybernetickej bezpečnosti na úrovni „dobrý“ až za Izrael a mnohé Európske štáty. A to napriek tomu, že Spojené štáty majú zďaleka najvyššie výdaje na vládne aktivity v oblasti kybernetickej bezpečnosti v porovnaní so zvyškom sveta a nepochybne disponujú najkvalitnejšími technickými a odbornými skúsenosťami a znalosťami.

Rozdiel z hľadiska vynaložených financií je enormný. USA míňajú pravdepodobne tri až desaťkrát viac, ako dokáže investovať všetkých dvadsaťosem členských štátov EÚ a Švajčiarsko, a to hovoríme len o vládnych výdajoch. Výdaje na kybernetickú bezpečnosť v súkromnom sektore sú podobne nevyvážené. Európske výdaje na kybernetickú bezpečnosť za rok 2015 sa odhadujú na zhruba 27 miliárd eur a americký trh dosahoval približne 75 miliárd dolárov (uvedené čísla zahŕňali aj predaje vládnym orgánom). Zdá sa však, že všetky tieto výdaje navyše USA nijak zvlášť nepomáhajú. Štúdia spoločnosti Grant Thornton hovorí, že v roku 2015 súkromný sektor v Severnej Amerike utrpel straty na výnosoch vo výške približne 61 miliárd dolárov v porovnaní so 62 miliardami dolárov v celej EÚ (nezabúdajme, že hovoríme o stratách na výnosoch, nie celkových škodách, ktoré sú odhadované na oveľa vyššej úrovni). Zdá sa teda, že EÚ celkovo vynakladá na tento problém oveľa menšie sumy a dosahuje na prvý pohľad podobný (t. j. podobne slabý) výsledok.”

Všetci vieme, že v súčasnosti mnohé spoločnosti - predovšetkým tie menšie - nemajú povedomie, alebo dostatočné zdroje, aby sa vysporiadali s kybernetickými útokmi na ich podnikanie, a to aj v prípade, ak by akceptovali skutočnosť, že kybernetická bezpečnosť predstavuje pre ich biznis enormnú a okamžitú hrozbu.

Je preto kľúčové, aby tieto spoločnosti prijali kroky na ochranu informácií, ktoré sú životne dôležité pre ich každodenné fungovanie a aby zmiernili riziká spájané s ich prípadnou stratou.

Musíme tiež nájsť spôsoby, ako podporovať sústavnú výmenu informácií a odborných znalostí a skúseností medzi vládou a súkromným sektorom s cieľom riešiť riziká v oblasti kybernetickej bezpečnosti.

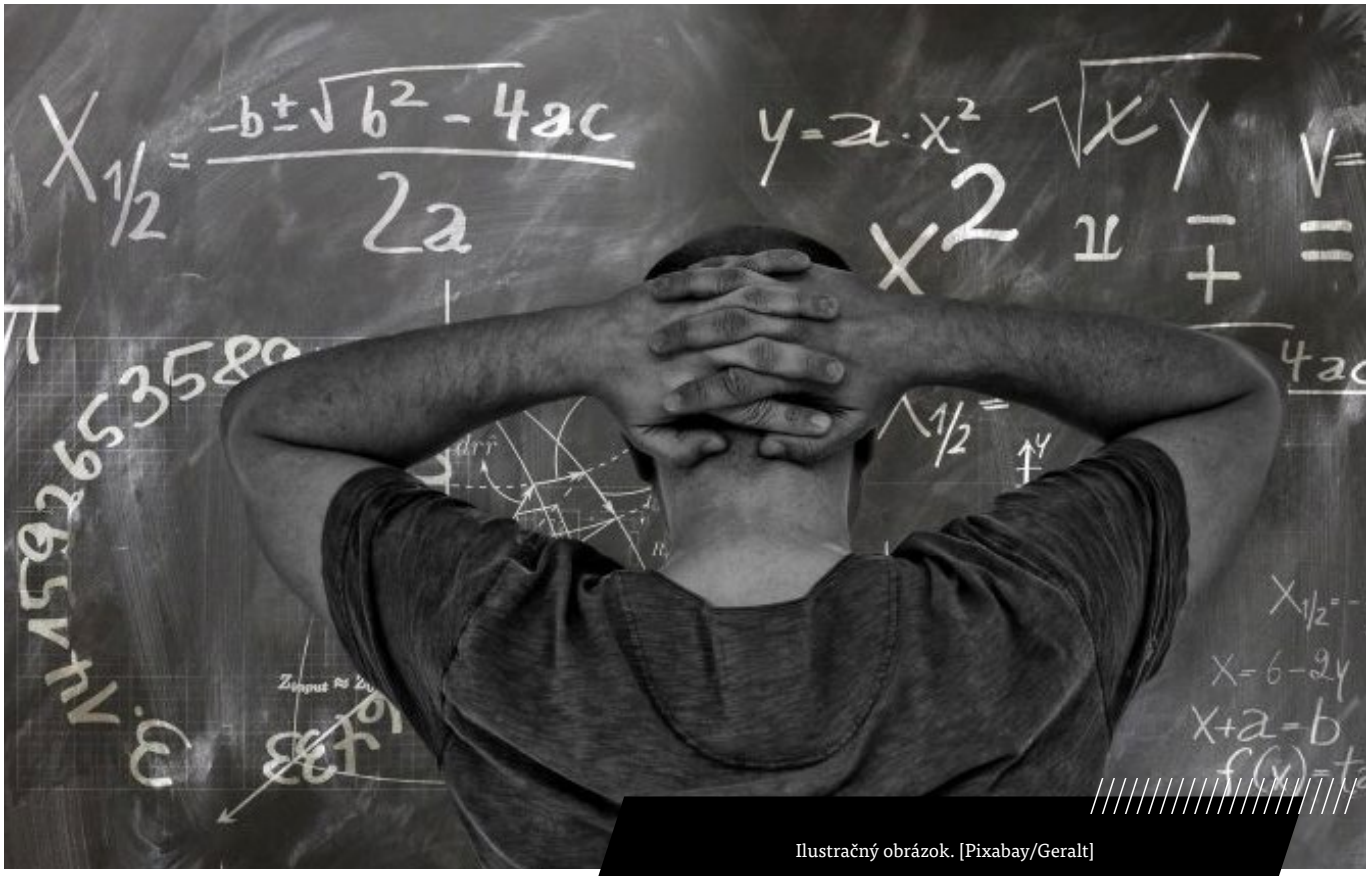
Bezpečný internet a rozvinutá digitálna ekonomika majú kľúčový význam pre našu hospodársku budúcnosť.

A každý z nás môže k tomuto cieľu pozitívne prispieť svojim zodpovedným správaním. V opačnom prípade, ako kedysi povedal bývalý americký prezident Dwight Eisenhower: „...si sami spôsobíme bankrot svojím márnym úsilím o absolútnu bezpečnosť.” ■

ČLÁNOK

Ak chcú firmy odborníkov na kybernetickú bezpečnosť, myslieť musia aj na ich školiteľov

Lucia Yar | EURACTIV Slovensko



Ilustračný obrázok. [Pixabay/Geralt]

Najúspešnejší študenti odchádzajú do zahraničia, najaktívnejších vyučujúcich lákajú súkromné firmy. Prestaňme sa hrať propagandistické koalície a odpovedzme si na otázku, či chceme mať informatikov alebo stačia preškolení sociálni pracovníci, nabádajú učitelia technických odborov.

Nedostatok kvalifikovanej pracovnej sily na Slovensku zasahuje aj do sektora kybernetickej bezpečnosti. Prierezový problém, ktorý má riešiť ministerstvo školstva, vnútra, financií, Úrad podpredsedu vlády pre investície a informatizáciu, či iné podriadené organizácie, ale tradične naráža na nespoluprácu medzi rezortami.

Stredné školy, univerzity, vzdelávacie inštitúcie a súkromný sektor hľadajú alternatívne riešenia. Rečníci panelu *Zvyšovanie povedomia ako najlep-*

ší nástroja zmierňovania následkov počas konferencie *Americkej obchodnej komory na Slovensku* sa ale zhodli na tom, že zmena zdola je viac ako problematická.

V KYBERBEZPEČNOSTI NEVIEME VYŠKOLIŤ MANAŽÉROV A PRÁVNIKOV

Kybernetická a informačná bezpečnosť je novou oblasťou, na ktorú sa nedajú aplikovať staré pravidlá, či existujúce princípy grantových schém. Štát preto potrebuje čo najskôr reagovať vhodnou legislatívou, či centrálnym odborným orgánom, ktorý by sa problematike kybernetickej bezpečnosti prierezovo venoval.

„Koordinácia medzi jednotlivými ministerstvami je takmer neexistujúca," hovorí **Andrea Cox, výkonná riaditeľka organizácie DigiQ**, ktorá organizuje výchovou k digitálnemu občianstvu a venuje sa problematike bezpečného používania internetu. Podľa nej chýba kybernetickej oblasti združujúca osoba alebo inštitúcia.

Príkladom môže byť podľa **Daniela Olejára, prorektora pre IT Univerzity Komenského v Bratislave** nemecký Spolkový úrad pre informačnú bezpečnosť, ktorý slovenská odborná verejnosť sleduje od začiatku deväťdesiatych rokov. Česi plánujú vybudovať Úrad pre kybernetickú bezpečnosť s približne 400 členmi v Brne pri úspešnej Masarykovej univerzite.

„Nám chýba spolupráca so štátnou správou, aby veci, ktoré máme pripravené, neostali len na úrovni: „Škola, ponúkni to!", ale aby sa koncepcie, ktoré napíšeme, aj zrealizovali," hodnotí Olejár.

V KRAJINE NEBUDE MAŤ KTO UČIŤ

Súkromné firmy sa na vysoké školy častokrát podľa Olejára pozerajú ako na zdroj hotových ľudí, ktorých môžu bez problémov využiť. Problémom však je, že z inštitúcií sťahujú aj tých, ktorí majú učiť. Motivácie sú logické: uplatnenie, kariérny rast, či financie – to slovenské školstvo podľa rečníkov nedokáže vyučujúcim ani potenciálnym učiteľom zabezpečiť.

„Prestaňme sa hrať na rôzne digitálne koalície a podobné propagandistické akcie a odpovedzme si na otázku, či chceme mať informatikov alebo stačia takí, ktorí budú preškolení sociálni pracovníci alebo hovorcovia? Ak chceme mať solídnych informatikov, tak je treba myslieť aj na ľudí, ktorí ich budú pripravovať," nabádal odborné publikum prorektor Olejár.

„Generácia otcov-zakladateľov odchádza do dôchodku a v krajine jednoducho nebude mať kto učiť," tvrdí. V diskusii firiem a vysokých škôl je podľa neho dôležité pozrieť sa na to, „za akých podmienok fungujeme a ako dlho takto ešte fungovať vieme".

„Ako odborná spoločnosť sa nerozprávame ani medzi sebou, ani s našimi cieľovými spotrebiteľmi a prijímame iba to, čo k nám prichádza prostredníctvom nariadení alebo podľa toho, aký je pohyb v Európe, dodáva Andrea Cox.

BEZ ZANIETENÝCH ĽUDÍ TO NA SLOVENSKU NEJDE

Úspešným príkladom inštitúcie, ktorá začala v systéme bojovať o výrazné miesto na trhu pre svojich absolventov, je aj Stredná odborná škola Ostrovského 1 z Košíc. Ako prvá na Slovensku proaktívne odpovedala na požiadavku trhu a v septembri otvorila pomaturitný študijný odbor Špecialista informačnej bezpečnosti. Vyšší odborný program trvá tri roky a končí sa absolventskou skúškou s titulom Diplomovaný špecialista.

„Absolvent má dokázať navrhnúť, testovať a následne aj implementovať bezpečnostné opatrenia akéhokoľvek informačného systému," hovorí jedna z tvorcov odboru, **Marcela Timková, vedúca Centra odborného vzdelávania SOŠ Ostrovského**.

Medzi kľúčové kompetencie, ktoré by študent mal počas štúdia nadobudnúť, patrí bezpečnosť počítačových sietí, bezpečnosť operačných systémov, zabezpečenie komunikácie, vrátane základov kryptografie a kryptovania dát, právne aspekty informatiky, či bezpečnostná politika a audit. To všetko s posilnenou výučbou anglického jazyka.

„Sme pripravení zareagovať na akúkoľvek požiadavku, či už vytvorením experimentálneho odboru, ako to bolo v prípade odboru Špecialista informačnej bezpečnosti, alebo naše vzdelávacie programy vieme určitými percentami prispôsobovať požiadavkám zamestnávateľov," **vysvetľuje riaditeľka školy, Elena Tibenská**.

Dodáva, že hoci inštitúcia, ktorú riadi, už teraz čelí nedostatku odborníkov, snažia sa v rámci možností a spoluprácou so súkromným sektorom motivovať aj súčasných vyučujúcich.

„Ak nemáte zanietených ľudí, tak sa o otváranie podobného programu ani nepokúšajte," radí Timková tým, ktorí by mali záujem na svojej škole ísť cestou SOŠ. ■

Pre viac informácií o ***EURACTIV*** *Špeciáloch...*

Kontaktujte nás:
Zuzana Gabrižová,
Šéfredaktorka
+421 254 432 633,
gabrizova@euractiv.sk
Pavel Nikodem,
Výkonný riaditeľ
+421 910 929 575,
nikodem@euractiv.sk
Kde nás nájdete:
Štefánikova 19
811 05 Bratislava
Vydavateľ:
I-Europa s.r.o.
www.euractiv.sk

Partneri:

SILVER SPONSORS

AON Empower Results®

eset

BRONZE SPONSORS

ALITER TECHNOLOGIES

AT&T

MEDIA PARTNERS

DENNÍK N

EURACTIV

PC REVUE

SITA