HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 30. SEPTEMBRA –

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Sladký spánok bezpečnostného povedomia

EURÓPSKY MESIAC KYBERNETICKEJ BEZPEČNOSTI

OKTÓBER JE MESIAC KYBERNETICKEJ BEZPEČNOSTI UŽ DESIATY ROK.

MOTIVUJE PROFESIONÁLOV A OSLOVUJE ŠIROKÚ VEREJNOSŤ. PRINÁŠA AKTUÁLNE INFORMÁCIE O DIGITÁLNEJ BEZPEČNOSTI A ZDIEĽA OSVEDČENÉ POSTUPY V ČLENSKÝCH ŠTÁTOCH ÚNIE AJ VO SVETE. LEBO BEZPEČNOSŤ NEMÁ HRANICE.

TÉMOU AKTUÁLNEHO ROČNÍKA SÚ RANSOMVÉR A PHISHING – DVA HLAVNÉ TRENDY V PROSTREDÍ KYBERNETICKÝCH HROZIEB.

Ako uvádzajú v prieskume slovenské firmy, za ostatné obdobie sa „zlepšili“ aspoň v tom, ako vzdelávajú zamestnancov v téme kybernetickej bezpečnosti. FOTO: SHUTTERSTOCK

TÉMA

Na Slovensku chýba 10-tisíc odborníkov kybernetickej bezpečnosti. S veľkou pravdepodobnosťou niekto chýba aj u vás. Ako nájsť, vzdelávať a podporovať profesionálov a vyplniť prázdny priestor?

Na fakultách, ktoré majú akreditované študijné programy, odbory a predmety týkajúce sa ochrany informácií, ročne promuje približne 150 absolventov.

„Aj keby všetci z nich naozaj začali pracovať v odbore, ktorý vyštudovali, dieru na pracovnom trhu zaplnia až o generáciu neskôr,“ vypočítava Ivan Makatura, generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti.

Šanca tu je vždy

Čiastočne sa dá problém nedostatku odborníkov riešiť rekvalifikáciou profesionálov z iných odborov alebo špecializáciou z tých príbuzných. Takto postupujú bezpečnostní integrátori a veľké a stredné firmy.

„Špecialistov, ktorých hľadáme, je dlhodobo nedostatok, a keďže sme nároční na seba, tak rovnako sme aj na kandidátov,“ súhlasí Zuzana Urbaníková, finančná riaditeľka Aliter Technologies. Neustále napredovanie a vzdelávanie je nevyhnutnosťou a iba tak sa dá budovať kvalitný tím.

V Aliteri majú zároveň zavedený interný program, ktorý sa venuje mladým talentom. „Práve študentom a absolventom dávame priestor hľadať a navrhovať riešenia a učiť sa. Nie je možné povedať, z ktorej vysokej školy sú najlepší absolventi. V prvom rade ide o osobnosť, a tak hľadáme nastavenie, drajv a záujem rozvíjať sa.“

A tí menší?

Približne len tretina malých podnikov a polovica stredných sa zaoberá kybernetickou bezpečnosťou. Úroveň vyspelosti v tejto oblasti zisťovali v prieskume Slovak Business Agency a Národný bezpečnostný úrad.

Polovica opýtaných nezamestnáva špecialistov na kybernetickú bezpečnosť a externé služby si zabezpečujú len minimálne. Dve tretiny firiem uviedli, že príslušné náklady u nich neprevyšujú jedno percento z celkového rozpočtu. Hlavnou motiváciou prijať opatrenia na zvýšenie bezpečnosti sú najmä hrozby kybernetických útokov.

Malí a strední podnikatelia by najviac privítali na zlepšenie kybernetickej bezpečnosti opatrenia vo forme grantov, poukazov na nákup technológií a na školenia a vzdelávacie kurzy. Druhým podporným opatrením by boli informačné služby štátu.

A plán obnovy?

Kybernetická bezpečnosť je v pláne obnovy jedným z hlavných pilierov komponentu Digitálne Slovensko, na ktorý je alokovaných vyše šesťsto miliónov eur. „Reformné a investičné opatrenia v tejto oblasti sú však cielené predovšetkým na štátnu správu a samosprávu,“ upozorňuje Patrik Kováč zo Sekcie plánu obnovy Úradu vlády SR.

Pre súkromný sektor sú tu zatiaľ iba nepriame možnosti podpory kyberbezpečnosti. V rámci komponentov K9 a K17 sú plánované výzvy zamerané na inovatívne projekty, či už ide o procesy, alebo technológie, avšak obsahové zameranie ešte nie je definované. Takže malé aj stredné podniky sa budú môcť prihlásiť s najrôznejšími nápadmi až po spustení výziev.

Nerozmýšľanie bolí

Profesionálov sa často pýtajú, akú zručnosť v kybernetickej bezpečnosti by naučili hneď a navždy všetkých používateľov. Neklikať bez rozmyslu na všetko, čo im príde pod ruku, neveriť všetkému, čo „písali na internetoch“, a počúvať rady dôveryhodných bezpečákov. Počínajúc deťmi a končiac generálnymi riaditeľmi.

Väčšina sofistikovaných útokov sa totiž začala neopatrným kliknutím. Aj tie, kde sa platili vydieračom milióny. Phishing je nočnou morou profesionálov a ešte dlho bude.

Ak nerátame informatikov a bezpečákov, nedostatočné digitálne zručnosti majú azda všetci používatelia. „Až som niekedy prekvapený, ako môžu niektorí ľudia používať na prácu počítač. Sú, žiaľ, aj takí, ktorí doslova každým zapnutím počítača zvyšujú počet existujúcich bezpečnostných hrozieb,“ hodnotí skúsenosti Ivan Makatura.

> Záujem o vzdelávanie na vyšších stupňoch je nadštandardný. Potrebovali by sme však školiteľov vo firmách.
>
> **Tomáš Hettych,** viceprezident ISACA Slovensko

Znova a znova

Ak teda dáte otázku uznávaným profesionálom, kam smeruje ich úsilie v organizáciách, zhodnú sa, že do vzdelávania a tréningov. Napríklad v Slovenskej sporiteľni aktívne cvičia reakcie zamestnancov na podvodné e-maily a telefonáty.

„Výstupy následne používame na vyhodnotenie efektivity a zlepšenia bezpečnostných opatrení a školení,“ vysvetľuje Ján Adamovský.

Postupom času je progres badateľný. „Je to vidieť na rastúcej ochote zamestnancov byť súčasťou mechanizmu ochrany. Či už účasťou na vzdelávaní, alebo angažovanosťou pri oznamovaní podozrení o phishingových podvodoch,“ pridáva sa Peter Dufek, manažér kybernetickej bezpečnosti v sieti nemocníc a poliklinik Svet zdravia a Procare.

Na vrchole pomyselnej pyramídy

V prípade, ak by dostali programátori a informatici možnosť ďalšieho vzdelávania, úroveň kybernetickej bezpečnosti by významne narástla.

Pre budúcich IT audítorov a manažérov informačnej a kybernetickej bezpečnosti, ktorí majú ambíciu byť držiteľmi medzinárodnej certifikácie, obnovuje školenia po 13-ročnej pauze ISACA ako profesijná organizácia v oblasti riadenia, bezpečnosti a kontroly informačných technológií.

„Záujem o vzdelávanie na vyšších stupňoch je nadštandardný. Potrebovali by sme však školiteľov vo firmách,“ pripomína Tomáš Hettych, viceprezident ISACA Slovensko.

Tí, ktorým to nie je ľahostajné

Chýbajú nám aj učitelia na všetkých stupňoch škôl, a tak sa Slovensko opäť raz spolieha na aktivity „zdola“. Iba minulý rok vznikla učebnica informačnej bezpečnosti pre stredné školy, ktorej autormi sú odborníci z praxe.

Do roka si odborné školy, gymnáziá a knižnice rozobrali takmer sedemsto kusov tlačenej verzie a prihlásili sa aj základné a vysoké školy. V elektronickom vydaní dostali stovky škôl učebnicu bezodplatne.

Vtipné videá a online testy, ktoré využívajú učitelia, vyrába aj portál zmudri.sk. Skupina okolo Tímu pre riešenie bezpečnostných incidentov UPJŠ v Košiciach realizuje projekt Nauč sa základy informačnej bezpečnosti a vzdelávaj svoje okolie. Stredoškoláci vzdelávajú rodičov, základné školy a seniorov.

Budúcnosť vzdelávania je iná

Fenomenálny úspech zaznamenala prvá slovenská kyberbezpečnostná hra CyberGame typu CTF, kde sa za úspešné vyriešenie úloh zbierajú vlajky. Počas desiatich týždňov sa do súťaže registrovalo viac ako 1 200 účastníkov.

„Nároky na vzdelávanie a osvetu v kybernetickej bezpečnosti rastú a gamifikácia je účinný a efektívny model pre všetky vekové kategórie,“ hodnotí prvý ročník Rastislav Janota, riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT, ako odborný garant súťaže.

Bodovalo vyše 580 hráčov rôznych vekových kategórií a profesií, z toho takmer polovica študentov. Do konca roka sa hracia platforma ešte otvorí pre organizácie, ktoré chcú netradične vzdelávať zamestnancov.

V PRÍLOHE SA DOČÍTATE

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · ESET · Progress · MICRO FOCUS · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 30. SEPTEMBRA – 2. OKTÓBRA 2022

Bude to iskriť medzi generáciami?

ANKETA

Špecializovaná príloha Hospodárskych novín prináša odpovede lídrov a odborníkov už dva roky. Dnes je čas pozrieť sa, či nám rastú pokračovatelia.

OTÁZKA PRE PROFESIONÁLOV:

Čo najlepšie a čo najhoršie sa môže stať pre kybernetickú bezpečnosť?

Marián Illovský
auditor kybernetickej bezpečnosti Auditori.it

Je to zvláštny paradox, ale v oblasti kybernetickej bezpečnosti je často najlepšia a najhoršia vec, ktorá sa môže stať, to isté. Všetci registrujeme vtipné obrázky, že ako vyzerá rozpočet bezpečnosti pred incidentom a po incidente. A ono to naozaj aj praxi funguje – väčšinou až veľký problém prinúti najvyšších zodpovedných venovať sa bezpečnosti. A toto je tá najhoršia vec v kybernetickej bezpečnosti,

Tomáš Orieščik
Chief Technology Officer Aliter Technologies

Je nemysliteľné predpokladať stav, že kybernetická bezpečnosť nebude potrebná. Obrovským úspechom bude, keď ju firmy a ľudia začnú brať skutočne vážne, budú sa v nej vzdelávať a dennodenne ju aplikovať. Najhoršia situácia môže nastať, ak napriek úsiliu expertov a používateľov nastane moment „bezmocnosti“. Budú prelomené všetky zámky a nepodarí sa vyvinúť bezpečnejšie. Aktuálne majú veda a technologické spoločnosti slušný náskok a úspech zloprajníkov spočíva skôr v nedôslednosti ľudí ako v kvalite bezpečnosti.

Július Selecký
senior technický špecialista ESET

To najlepšie, čo by sa nám mohlo stať, je silno ovplyvnené osobnou skúsenosťou. Vzdelávanie na všetkých úrovniach v kybernetickej bezpečnosti od základných škôl až po špecializované odbory na vysokých školách, osveta v zamestnaní či vzdelávanie dôchodcov, aby sa nenechali oklamať. A aby firmy a štátne inštitúcie rozumeli tomu, že prostriedky kyberbezpečnosti sú investícia do budúcnosti, ktorá sa vyplatí. Hasiť problémy či odstraňovať škody po ransomvéri je násobne nákladnejšie ako ochrana zariadení.
To najhoršie, čo sa môže stať, je APT, teda pokročilá pretrvávajúca hrozba, ktorá číha v počítačoch vďaka využitiu zero day zraniteľnosti. Skupiny, ktoré takto útočia, si za svoje ciele vyberajú aj kritickú infraštruktúru, čo môže spôsobiť nielen stratu citlivých dát, ale aj napríklad výpadok elektrickej energie. Toto by malo fatálne následky na celkový chod štátu a služieb občanov.

Andrej Žucha
generálny riaditeľ ALISON Slovakia

Tie najlepšie riešenia na princípe Security by design sú už dávno vymyslené. Pred nami idú vyspelé a vzdelané krajiny, kde sa dá inšpirovať školstvom aj technologickými riešeniami. To najhoršie v kybernetickej bezpečnosti nebývajú ani chýbajúce financie, je to nedostatok komunikácie či faktov v argumentácii, kde naše rozpory a otáľanie zužitkujú agresori.

Roman Čupka
hlavný konzultant Progress | Flowmon a CEO Synapsa Networks

Najlepším scenárom je začať s osvetou, aké nástrahy sa v kybernetickom priestore ukrývajú a ako sa v ňom správať, a to už od prvého stupňa základných škôl. Základným lajtmotívom by malo byť heslo: Čo by som nerobil vo svete fyzickom, nerobím ani v tom digitálnom a naopak. Najhorším je túto tému nechať len na rodičov, ktorí nemajú vedomosti, čas ani pochopenie pre túto tému a ich morálny kompas je často naklonený nesprávnym smerom.

Stanislav Smolár
manažér oddelenia bezpečnosti Soitron

Najlepšie, čo sa môže stať, je, že kybernetická bezpečnosť sa stane ozajstnou, nielen deklarovanou prioritou štátu. Najhorší scenár je pre mňa osobne trvalý nedostatok ľudských zdrojov a nezáujem mladých talentov o tematiku, ktorý môže pre Slovensko znamenať stratu relevancie na európskom IT a startup trhu.

OTÁZKA PRE ŠTUDENTOV:

V mimoriadnom vydaní sa pýtame študentov, ako vnímajú kybernetickú bezpečnosť po absolvovaní Letnej školy kyberkriminality.

Emma Macháčová
Fakulta informatiky a informačných technológií, STU Bratislava

Kybernetická bezpečnosť je ako potápačská klietka a internet je ako more. Obe sú hlbšie, ako si človek bežne predstavuje, a nikdy neviete, kde na vás číha „žralok“.

Patrik Ondrejech
Právnická fakulta, Trnavská univerzita v Trnave

Kybernetická bezpečnosť je nevyhnutnou súčasťou života každého z nás, či už na osobnej alebo pracovnej úrovni. Táto letná škola mi jednoznačne ukázala, že to nie je len „nastavenie“ alebo jednoduchý krok pri začiatkoch tvorby systémov, ale kontinuálny proces, ktorý si vyžaduje neustálu starostlivosť odborníkov z technickej i právnej oblasti.

Henrieta Paločková
Prírodovedecká fakulta, Univerzita Pavla Jozefa Šafárika v Košiciach

Počas jednej z prednášok zaznela zaujímavá veta „Nič nie je 100-percentne bezpečné.“ Ukázalo mi to, aké potrebné je zaoberať sa kybernetickou bezpečnosťou v dnešnej dobe. Ide o rozsiahlu problematiku, pri ktorej len jeden pohľad nestačí. Ľudia z rôznych odborov prispievajú odlišným spôsobom, a preto pri riešení kybernetických incidentov je najdôležitejšia spolupráca a vzájomné pochopenie v tíme.

Denis Ivan
Fakulta informatiky a informačných technológií, STU Bratislava

Kybernetické hrozby sú na vrchole všetkých rizík, ktoré ohrozujú veľké množstvo populácie. Pod stálym útokom sú viac ako len naše siete a zariadenia. Ale je to najmä náš mobilný, flexibilný a vzájomne prepojený spôsob života. Na vlastné oči som sa presvedčil o tom, že som sa rozhodol pre výber svojej kariéry správne. Zaujímavé semináre, workshopy a náš super tím ma povzbudili naďalej sa vzdelávať v tejto oblasti.

Zuzana Hennelová
Prírodovedecká fakulta,Univerzita Pavla Jozefa Šafárika v Košiciach

Kyberkriminalita rastie spolu s vývojom technológií a je potrebné ju riešiť. Preto som sa zúčastnila na Letnej škole, kde som získala cenné skúsenosti a vedomosti. Naučila som sa lepšie pracovať s neznámymi ľuďmi, či už s informatikmi alebo s právnikmi, na spoločnom cieli a plne som si uvedomila, že na riešenie bezpečnostného incidentu je potrebné pozerať sa aj z právneho hľadiska.

Patrik Goldschmidt
Fakulta informačních technologií, Vysoké učení technické v Brně

Kybernetickú bezpečnosť som odjakživa považoval za jeden z kľúčových pilierov informačných technológií. Doteraz som ju však vnímal ako prevažne informatickú záležitosť. Táto letná škola mi však ukázaním právneho aspektu problematiky značne otvorila oči. Zistil som, že aj také výrazne rozdielne odbory, ako sú informatika a právo, musia spolupracovať, ak má byť boj proti kyberkriminalite úspešný.

Gabriela Filická
Právnická fakulta Univerzity Komenského v Bratislave

Po absolvovaní Letnej školy intenzívne vnímam, že kybernetická bezpečnosť ochraňuje hodnoty, ktorých hodnotu si (zjavne) ako spoločnosť dostatočne neuvedomujeme. Letná škola kyberkriminality mi ukázala, aké nevyhnutné je, aby sme tejto téme venovali adekvátnu pozornosť.

Sandra Morgošová
Právnická fakulta, Univerzita Komenského v Bratislave

Dosiahnuť v rámci našich možností čo najbezpečnejší kybernetický priestor je vzhľadom na vývoj trendov v posledných rokoch absolútne kľúčové. Drvivá väčšina ľudí využíva kybernetický priestor takmer na dennej báze. Najväčšie úskalie vidím v informovanosti a vzdelávaní ľudí v oblasti kybernetických útokov a hrozieb. Práve to by, podľa môjho názoru, mala byť absolútna priorita v najbližších rokoch.

Laura Buchelová
Fakulta elektrotechniky a informatiky, Technická univerzita v Košiciach

Kyberbezpečnosť vnímam ako oveľa obšírnejšiu oblasť ako doteraz. Zistila som, že nejde len o riešenie bezpečnostných incidentov ako takých, ale aj o ich prevenciu, vzdelávanie ľudí a seba samých. Taktiež ma prekvapilo, ako blízko musia spolupracovať skupiny ľudí z odlišných odborov, teda právo a informatika. Jeden bez druhého v kyberbezpečnosti veľa nezmôžu, teda je tu veľmi dôležitá interdisciplinárna spolupráca.

Lenka Strapková
Právnická fakulta, Univerzita Komenského v Bratislave

Pojem kyberbezpečnosť pre študenta práva nezahŕňa len technicky stručnú či zložitú definíciu. Dávno nepatrí na okraj právneho záujmu, ktorý jej vo vzdelávacom procese prislúcha. Za bezpečnostný incident je možné považovať už to, koľko málo vecných faktov sme pred absolvovaním letnej školy vedeli. Musíme dúfať, že kyberbezpečnosť počká, kým si my, študenti a školy, dobehneme resty.

Vladyslava Krivoshei
Právnická fakulta, Univerzita Pavla Jozefa Šafárika v Košiciach

Kyberbezpečnosť je veľmi aktuálnou témou, ktorej by sme mali venovať zvýšenú pozornosť, a adekvátne reagovať na hrozby v kyber prostredí. Nevyhnutnou v danom kontexte je dostatočná edukácia spoločnosti jasným a zrozumiteľným spôsobom. Napokon, dôležitou pri riešení bezpečnostných incidentov, ako aj pri zaistení bezpečnosti počítačových údajov, je spolupráca medzi ľuďmi z rôznych odborov, ako napríklad právo a informatika.

Lucia Kobzová
Bratislava international school of liberal arts

Letná škola mi ukázala, že kyberbezpečnosť je veľmi komplexná interdisciplinárna oblasť, ktorá sa nedá študovať iba z jednej perspektívy. Úspešne nastavené kyberbezpečnostné opatrenia totiž vyžadujú kooperáciu technických, právnych a politických expertov. Vzájomné porozumenie odlišných odborov, rovnako ako aj študovanie problematiky z viacerých uhľov pohľadu, sú preto absolútnou nevyhnutnosťou.

Jakub Mohler
Prírodovedecká fakulta Univerzita Pavla Jozefa Šafárikav Košiciach

Informácií je dnes viac ako kedykoľvek predtým, preto vznikajú nové hrozby, ktorým treba čeliť. Letná škola ma presvedčila, že kybernetická bezpečnosť je široká oblasť zahŕňajúca nielen informatiku, ale aj pre mňa neprebádanú oblasť práva. Toto zistenie mi ukázalo, že kybernetická bezpečnosť vyžaduje často alternatívny spôsob myslenia a sledovanie trendov v informatike aj v ďalších oblastiach.

Martin Pavelka
Fakulta informatiky a informačných technológií, STU Bratislava

Dnes sa ľudia veľmi spoliehajú na IT systémy. Čo sa stane, keď sa na ne jedného dňa nemôžu spoľahnúť? Čierna obrazovka v nemocnici znamená smrť pacienta, žiaľ rodiny a frustráciu lekárov. Aby sme odvrátili čierne scenáre, musíme riešiť bezpečnosť tak, aby bol virtuálny svet minimálne rovnako bezpečný ako ten skutočný. Je dobré, že aj na Slovensku máme šikovných ľudí, na ktorých sa iní spoliehajú, že ich budú chrániť Nesmieme zabúdať na to, že ide o bezpečnosť, ale súčasne aj zodpovednosť každého z nás.

Monika Rapavá
Prírodovedecká fakulta Univerzita Pavla Jozefa Šafárika v Košiciach

Naučila som sa spolupracovať v rôznorodom kolektíve a pripomenula si, že kybernetická bezpečnosť má viacero aspektov, ktoré je potrebné zladiť na vytvorenie fungujúceho celku. Kybernetickú bezpečnosť vnímam ako dynamickú oblasť, ktorá poskytuje nekonečné možnosti v rámci vzdelávania. Je mi ľúto, že sa o túto oblasť zaujíma stále málo ľudí, čo je taktiež mojou motiváciou zvyšovať povedomie.

Jakub Škoda
Fakulta matematiky, fyziky a informatiky, Univerzita Komenského v Bratislave

Akýkoľvek systém bude raz narušený. Reálna pripravenosť minimalizovať škody, je nevyhnutná. Nutné je neustále verne simulovať cielené útoky, a tak objaviť a zaplátať všetky nájdené bezpečnostné medzery. Bežne sa stáva, že máme zálohy dát, ale nevieme ich obnoviť alebo nájsť v nich to najdôležitejšie. Opatrenie, ktoré neotestujeme, vôbec nemusí fungovať.