

Čo nám odhalil kyberútok na kataster?

ANKETA

Január vystavil účet Slovensku o stave kybernetickej bezpečnosti. Či už hovoríme o odbornej alebo širokej verejnosti, dostali sme lekciu. Tento mílnik je už osadený a profesionáli hodnotia jeho význam.



Jaroslav Ďurovka,
riaditeľ, Národné centrum
kybernetickej bezpečnosti

Odhaliť to, že kybernetickú bezpečnosť, osobitne v organizáciách s takými rozsiahlymi informačnými aktivitami, nie je možné podceňovať. Liekom síce môže byť kvalitný systém zálohovania, ale oveľa dôležitejšia je prevencia. A to prevencia komplexná, čo znamená primerane aplikovaná kombinácia bezpečnostných opatrení. Zároveň odhalil, že na Slovensku máme šikovných a ochotných odborníkov na riešenie kybernetických incidentov.



Tibor Szabo,
vedúci Odelenia auditu IT,
Všeobecná úverová banka

Veľmi ťažká otázka vzhľadom na málo informácií. Kyberútok možno ukázal na investičný dlh v tejto oblasti, potrebu neustáleho zlepšovania úrovne kyberbezpečnosti aj povedomia spoločnosti. Ale hlavne útok vypovedá o dobe, ktorú žijeme. Kybernetický útok ako jedna z hybridných hrozieb je súčasťou našich životov. Naučme sa dôkladnejšie brániť, uplatňujme dôkladnejšie všetko, čo vieme, lebo máme šikovných ľudí.



Ľubomír Kríž,
manažér kybernetickej
bezpečnosti,
Slovenská pošta

Incident odhalil, že ešte stále nemáme pod kožu vryté adekvátne reakcie na podobné udalosti vrátane požadovanej komunikácie. A to nielen v kyberútokom zasiahnutej organizácii, ale aj celej komunite kybernetickej bezpečnosti. Všetcí vieme, ako by to malo vyzerať, menej je tých, ktorí to vedú aj zabezpečiť. Viacerým hodnoteniam, popri nesporenej odbornosti, by pristala tiež malá dávka pokory.



Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Tak ako v hokeji, vo futbale, tak aj tu je zrazu „päť miliónov“ kyberbezpečnostných expertov, ktorí presne vedú, čo všetko sa malo urobiť. Po bitke je však každý generál. Nesúdime bez hlbšej znalosti všetkých súvislostí a dôverujeme tým, čo to vedú robiť, a držme si všetci palce, aby sa to vrátilo do normálneho stavu čo najskôr. Nikto nevie, kedy sa môže ocitnúť v podobnej situácii, aj keď urobil maximum, čo mohol.



Michal Srnec,
vedúci oddelenia informačnej
bezpečnosti,
Aliter Technologies

Všetko a nič. Myslím si, že pre profesionálov v kybernetickej bezpečnosti neodhalil nič nové. V podstate „len“ poukázal na stav mnohých spoločností a inštitúcií, na ktorý dlhodobo poukazujeme vo svojich bezpečnostných analýzach, správach či komentároch. Avšak to, aký mal tento incident vplyv na širokú verejnosť a jej precitnutie ohľadne stavu aktuálnej kybernetickej bezpečnosti, či už v privátnom, alebo vo verejnom sektore – to je už iný príbeh, tam ukázal všetko.



Tomáš Zařko,
CEO, etický hacker,
Citadelo

Je mi to ľúto. Z takéhoto ochromenia sa nedá tešiť. Útok ukázal dvojité zlyhanie štátnej inštitúcie. V bezpečnosti aj v komunikácii. Ako je na tom zvyšok štátu? Ak sa riešenie bezpečnosti nezlepší, ďalšie útoky sú len otázkou času. Tento moment musí byť katalyzátorom zásadnej zmeny v kybernetickej bezpečnosti aj v krízovej komunikácii.



Maroš Rajnoch,
architekt kybernetickej
bezpečnosti,
Soitron

Dnes už vieme povedať, že bezpečnosť informačného systému ÚGKK SR nebola v najlepšej kondícii. Sme svedkami toho, že vybrané inštitúcie nie sú pripravené na zvládnutie kybernetického útoku. Udalosť nám tiež odhalila, že štát s ťažkosťou komunikuje v kritických situáciách. Po vyšetrovaní budeme poznať, či išlo o technologický dlh, chýbajúce opatrenie, nevhodné postupy alebo niečo úplne iné.



Peter Matej,
manažér kybernetickej
bezpečnosti,
eMsec

Pre znalých problematiky kyberútok na kataster potvrdil to, čo vedeli: útoky na kritickú infraštruktúru nemajú dosah len na samotnú obeť. Obeťami sa stávajú aj sekundárne a terciárne subjekty závislé od služieb obeť. Že schopnosť zvládnuť incident si vyžaduje tím skúsených ľudí, vysoké nasadenie, dostupné zálohy a jasnú komunikáciu. Prekvapením pre mňa bol exponenciálny nárast množstva „odborníkov“.



Eduard Hertl,
obchodný riaditeľ,
skupina CYLLIUM

Vzhľadom na vplyv útoku na bežný život si musíme uvedomiť, že kybernetická bezpečnosť sa týka nás všetkých, a musíme k tejto téme pristupovať zodpovedne. Odporúčam spracovať a pravidelne testovať komplexné plány kontinuity činnosti pre efektívne zvládnutie krízových situácií.



Ivan Kopáčik,
bezpečnostný expert,
Gordias

Aktuálne kyberútoky dokazujú, že nemenej dôležitá ako technická pripravenosť je aj spoločenská rovina. Ukazuje sa, že pokrývajúca vecná a informačne adekvátna komunikácia zo strany štátu voči verejnosti. Spolupráca (nie improvizácia!) všetkých zainteresovaných strán má tiež priestor na zlepšenie. A v neposlednom rade je dôležité vyvodit poučenia do budúcnosti a prijať nápravné opatrenia.



Benjamin Würfl,
obchodný zástupca Eviden,
Eviden Slovakia

Útok na kataster jasne ukázal stav IT bezpečnosti, ktorý na Slovensku pretrvávajú. Zároveň poskytol priestor a šancu tieto nedostatky odstrániť tým, ktorí na ne vo svojich organizáciách upozorňovali, ale neboli vypočutí. Zvýšime našu pozornosť na zraniteľnosť, patchovanie alebo vzdelávanie IT?



Jaroslav Ušiak,
prodekan pre vedu a výskum,
Fakulta politických vied
a medzinárodných vzťahov UMB
Banská Bystrica

Tento útok na kataster odhalil, že kybernetická bezpečnosť Slovenska pripomína domček z kariet – na prvý pohľad stabilný, ale stačí malý vánok a všetko sa rozsype. Ukázal nám, že v digitálnom svete sa neoplatí spoliehať na náhodu, a dnes už aj kataster zistil, že pravidelné zálohovanie nie je možnosť, ale nutnosť. Ale za akú cenu...



Tomáš Hettych,
viceprezident,
ISACA

Ukázali sa slabiny v pripravenosti na krízové situácie. Incident nestačí riešiť len technologicky, ale občas je oveľa dôležitejšie o ňom správne komunikovať. Súčasťou krízových plánov by mal byť aj efektívny plán komunikácie.



Pavol Vrabec,
manažér kybernetickej
bezpečnosti,
Univerzitná nemocnica Martin

Úspešný útok na kataster demonštroval, že kyberbezpečnosť sa bez výnimky dotýka každého z nás a je potrebné o tom hovoriť, a to nielen vtedy, keď sa incidenty vyskytnú. Proti kyberútočníkom nie je jedno ducho nikto imúnny. Verím, že tento incident dal mnohým zainteresovaným osobám podnet na zamyslenie. Dúfam, že útok bude transparentne vysvetlený, aby sme sa z neho mohli poučiť v budúcnosti.



Diana Legdanová,
riaditeľka divízie
pre bezpečnosť,
Západoslovenská energetika

Obávam sa, že kyberútok odhalil realitu stavu kybernetického prostredia vo väčšine verejných inštitúcií na Slovensku. Veľmi chcem veriť, že to bolo skutočne varovanie pre mnohých zodpovedných aj v iných organizáciách, a začnú konať. Pre verejnosť je to praktická ukážka toho, čo znamená narušenie princípu CIA – dôvernosti, integrity a dostupnosti dát. A tam sa už končia všetky vtipné a amatérske odporúčania.



Július Selecký,
senior technický špecialista,
ESET

Laickej verejnosti ukázal, aký môže mať kybernetický útok vplyv na chod štátu a bežných občanov. Slovensko sa pýši kvalitnou legislatívou v oblasti kybernetickej bezpečnosti, ktorá je uznávaná aj v medzinárodnom kontexte. Avšak na to, aby táto legislatíva plnila svoj účel a prinášala reálne výsledky, je nevyhnutné, aby sme ju nielen deklarovali, ale aj dôsledne dodržiavali v praxi.



Róbert Mramúch,
manažér oddelenia
kybernetickej bezpečnosti,
MH Teplárenský holding

Fatálna výpoveď o zlom stave základných služieb štátu a o tom, ako kolektívne nevyžadujeme zodpovednú správu vecí verejných. Oblasť, ktoré majú byť výkladnou skriňou, sú dlhodobo zanedbávané a finančne aj odborne podvyživené. Ale máme šťastie – z EÚ prišla smernica NIS2, ktorá prikazuje nápravu a zaväzuje štátov konáť. Držím Slovensku palce, čaká nás ešte veľmi veľa práce.



Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Potvrdila sa realita, o ktorej sa sa vo svete cybersec hovorí už dávno – podceňovanie všetkých úrovní riadenia bezpečnosti. Ukázala sa dôležitosť kvality nastaveného reputačného manažmentu, vývoj prvých dní potvrdil, že zle nastavená krízová komunikácia dokáže vytvoriť podhubie pre vznik teórií a „overených právd“ všetkého druhu. Na strane druhej táto udalosť otvorila takú prepotrebnú diskusiu o stave KB štátnych a samo-správnych inštitúcií.



Ivan Makatura,
generálny riaditeľ,
Kompetenčné a certifikačné
centrum kybernetickej
bezpečnosti

Pre mňa z tohto incidentu neplynie poučenie, ale potvrdenie faktu, o ktorom dávno viem: že od predsedu vlády až po traktoristu Joža v krčme v Hornej Dolnej tu máme samých odborníkov na kybernetickú bezpečnosť. A na hokej. A na makroekonómiu. Žiaľ, k veciam, ktorým absolútne nerozumejú, sa vyjadrujú aj inak pričetní ľudia. Možno sa to stane aj v tejto ankete. Nepotrebuje kvalifikáciu. Len názor.



Richard Kiřkováč,
generálny riaditeľ,
Elkan

Odhaliť, že byrokraticko-akademická bezpečnosť sa iba málo stretáva s realitou v praxi a žije si svoj virtuálny svet. Ukázal aj to, že nasávanie právomocí sa deje bez akejkoľvek zodpovednosti za konečný výsledok a napriek komplexnosti neexistuje žiadna koordinácia, iba zmes vlastných záujmov a nekonečného alibizmu. Zistili sme, že tím nevyhrá ligu ani pod hrozbou sankcií, ani tak, že zakúpime zlaté kopačky hráčom, ktorí neexistujú.



Tomáš Valenta,
riaditeľ,
Check Point Software
Technologies na Slovensku

Nemyslím si, že kyberútok niečo odhalil. Mojm kolegovi, mne a ďalším bezpečákovi potvrdil to, čo vieme a o čom neustále hovoríme. Pre firmy, inštitúcie, ich riaditeľov a majiteľov, ale aj pre verejnosť je to ďalší varovný prst a impulz k posunu do reálnych riešení. Vlastne jednu vec to predsa len odhalilo – ako nie sme pripravení na tieto situácie z hľadiska komunikácie. Tá bola po útoku žalostná.



Jana Puřkáčová,
vedúca špecialistka IT
bezpečnosti,
Slovnaft

Žiadna kampaň na budovanie bezpečnostného povedomia by nemala taký dosah ako kyberincident v spojitosti s katastrofou. Bežní občania zaradili do slovníka slovičko ransomvér a na vlastnej koži zažili jeho dôsledky. Itečkári získali argumenty, prečo zálohovať, plátať starý softvér a testovať obnovu dát zo zálohy. Biznis zistil, aký význam má komunikácia a na čo je dobré riadenie kontinuity podnikania. Bezpečáci vedú zdôvodniť, prečo treba plány na obnovu po katastrofe a aký môže byť prínos procesu, ako reagovať na kybernetický incident. A top manažment sa presvedčil, že správna otázka naozaj nie je „či“, ale „kedy“ by sa organizácia mohla stať obeťou kybernetického útoku.



Maroš Trnka,
vedúci odboru IT,
Vodohospodárska výstavba

Ak vynecháme časť so šifrovaním a za predpokladu, že útočníci boli v katastri dlhšie, tak mohli (útočníci) napríklad manipulovať s údajmi o vlastníctve a meniť ich, čo by mohlo v extrémne viesť napríklad k podvodným predajom nehnuteľností či pozemkov nezistených vlastníkov, a to by bol celkom iný typ problému. Prečo niekto útočí na štát, kde je predpoklad na zaplatenie výkupného minimálny? Uvidíme.



Roman Varga,
manažér kyberbezpečnosti,
Dôvera, zdravotná poisťovňa

Odpoveď je rozprávka Cisárovo nové šaty. Kyberodborníci dlhodobo upozorňujú, že cisár je nahý! Žiaľ, ten náš „cisár“ sa dlhodobo obklopuje neschopnými radcami. Ak by to bral vážne, systematicky by sa budovala kyberobrana v tomto našom štáte a zmenšoval by sa technologický dlh. Na problémy v sektore zdravotníctva upozorňujeme už dlhodobo. Podobnú skúsenosť ako kataster s ransomvérovým útokom majú až dve percentá ambulancií.



Katarína Kročková,
odborníčka na ochranu osobných
údajov,
Kročka & Partners

Kyberbezpečnosť je stále podceňovaná, hoci sa neustále ukazuje ako kľúčová pri ochrane dát. Rovnako tak aj kataster narába s citlivými údajmi, ktoré mohli alebo môžu byť zneužitú. Ďalším „kameňom úrazu“ bola aj následná nedostatočná komunikácia smerom k verejnosti. Žiaľ, vznikali tak rôzne teórie a vynorilo sa množstvo „odborníkov“ na kybernetickú bezpečnosť, predovšetkým v oblasti zálohovania.