# Dajte im rozpočet a pozerajte sa!

ANKETA

Ak by ste mali veľmi veľký rozpočet a mohli urobiť iba jednu investíciu u vás vo firme alebo v úrade, čo by ste urobili v oblasti kybernetickej bezpečnosti?

**Tomáš Hettych**
**viceprezident**
**ISACA**

Nasadiť bezpečnostný a prevádzkový monitoring a pripojiť doň všetky relevantné informačné aktíva. Bez monitoringu je organizácia slepá a hluchá a spolieha sa len na klasické (väčšinou pasívne) bezpečnostné mechanizmy. Nasadenie centrálneho monitoringu je veľký a náročný projekt, ktorý organizáciu zabaví na niekoľko mesiacov, ale výsledok a výstupy sú väčšinou dosť dramatické a zaujímavé.

**Ján Grujbár**
**generálny riaditeľ**
**Aliter Technologies**

Sme technologická firma a tak by sa očakávalo, že investícia bude smerovať do najnovšej technológie. Avšak najcennejším aktívom každej organizácie sú ľudia. Ak im dáte adekvátny tréning a priestor, prinesú vám úžasné riešenia. Investícia v našom podaní by smerovala predovšetkým do rozšírenia vzdelávacích možností pre zamestnancov a vytvorení priestoru pre podporu inovatívnych projektov.

**Marián Trizuliak**
**architekt kybernetickej bezpečnosti**
**Západoslovenská distribučná**

Najať schopných útočníkov (whiteheťákov) – red, purple, blue team – a celú spoločnosť riadne otestovať, ako odolá rôznym formám útokov. A hlavne, ako by reagovala na veľmi kreatívne formy útokov a či vôbec dokáže vhodne reagovať alebo útok odhaliť. Kreativita útočníkov nepozná hraníc. V rozpočte by som pravdepodobne počítal aj s malou rezervou na lieky na upokojenie a vitamíny. Budeme ich potrebovať.

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

Výraz „investícia“ evokuje technické opatrenie. Avšak neexistuje technológia, ktorá by bola bezpečnostným všeliekom. Správnejšie je presadzovať koncept hĺbkovej ochrany, v ktorom sú informácie chránené niekoľkými bezpečnostnými vrstvami. Ak mám dať len jediné odporúčanie, potom nasadenie robustného procesu riadenia rizík. Na ten ani veľký rozpočet netreba. A z neho vyplynú čiastkové opatrenia.

**David Dvořák**
**audítor kybernetickej bezpečnosti**
**Auditori.it**

Inšpiroval by som riaditeľov a zodpovedných manažérov a nadchol ich pre tému. Urobil by som kyber bezpečnostnú hru s reálnymi úlohami, adrenalínovým dobrodružstvom a odmenami. Ak používateľ nepostrehne útok, celá organizácie je v ohrození. Cvičili by sme zručnosti zážitkami. Hovoriť v treťom tisícročí iba o školeniach je „old school“. Ak by zvýšilo, obsadil by som do hlavnej úlohy Daniela Craiga.

**Andrej Žucha**
**generálny riaditeľ**
**ALISON Slovakia**

Keďže má ísť o jedinú investíciu, tak by to bolo vybudovanie centra bezpečnostných operácií. To je ten moment mať „fungujúci orchester bez disonantných tónov“, ku ktorému sa snaží dopracovať každý, čo rieši bezpečnosť v organizácii. Ak by pod pojmom investícia, mala byť jedna technológia, tak by to bol bezpečnostný monitoring. Dôležité je vedieť, čo sa mi deje a podľa toho vedieť reagovať.

**Roman Čupka**
**hlavný konzultant**
**Flowmon a CEO Synapsa Networks**

Vybudoval by som profesionálne stredisko bezpečnostných operácií (SOC) vybavené viacerými vrstvami technológií a vyškolenými internými odborníkmi, ktoré by fungovalo s podporou externých tímov zameraných na overovanie pripravenosti organizácie na hrozby, reakcie na incidenty a forenzné vyšetrovanie.

**Ivan Kopáčik**
**bezpečnostný expert Gordias**

Vypočul by som si predstavy bezpečnostného manažéra o internom vzdelávaní v kyberbezpečnosti. Nechal ho systematicky vyhodnotiť zručnosti a vedomosti zamestnancov, vypracovať štruktúrovaný plán vzdelávacích aktivít podľa potrieb a cieľových skupín a potom ho s profesionálnymi lektormi realizovať. Tak, aby kurzy zohľadňovali špecifiká organizácie a potreby vedenia, IT špecialistov a používateľov.

**Stanislav Smolár**
**manažér oddelenia bezpečnosti**
**Soitron**

V Soitrone máme kybernetickú bezpečnosť už dnes na relatívne vysokej úrovni. Preto by som zvolil nástroj, ktorý dokáže posilniť detailné poznanie všetkých IT aktív, zanalyzovať ich bežné či anomálne správanie a priraďovať k týmto aktívam relevantné risk skóre. Nástroj by ma vždy upozorňoval na rizikové aktivity zariadení a potenciálne incidenty, a preto by som zintegroval detekciu incidentov s interným SOC.

**Július Selecký**
**senior technický špecialista**

Z hľadiska bezpečnosti by som odporučil investovať zákazníkom do EDR riešenia na ochranu koncových zariadení s prislúchajúcimi službami vyšetrovania incidentov. Stačí iba trochu vyšší rozpočet. Prevencia je vždy lepšia ako liečba, ale nie vždy je to možné. Najlepší spôsob, ako minimalizovať následky útokov, je ich včasné odhalenie. Nástroje, akými sú EDR riešenia, tento proces urýchľujú a zabraňujú tak šíreniu hrozieb.

**Tibor Paulen**
**manažér informačnej bezpečnosti**
**Stredoslovenská distribučná**

Investoval by som do systému budúcnosti, riadeného umelou inteligenciou, ktorý by zbieral a analyzoval dáta z našich systémov a učil sa tak predvídať a rozpoznať „stav mieru“ od „stavu vojny“. Postupne by sa naučil aktívne meniť parametre systémov a radiť ich správcom pri predchádzaní a reakcii na bezpečnostné incidenty. A mne by radil, do akých bezpečnostných technológií je potrebné investovať :-)

**Peter Dufek**
**manažér kybernetickej bezpečnosti**
**Procare a Svet zdravia**

Pokiaľ by som si mal vybrať, rozhodne by som odporúčal investovať do sofistikovaného nástroja Endpoint Detection and Response (EDR) na cielenú detekciu a reakciu na útoky na koncové zariadenia zamestnancov, pretože medzi súčasné najväčšie hrozby patria ransomvér, malvér, ako aj emailové útoky cielené na krádež hesiel alebo údajov smerované na koncového používateľa.

**Matej Síleš**
**manažér IT bezpečnosti**
**UPC BROADBAND SLOVAKIA**

Určite by som zvažoval investíciu do viacerých projektov, ale ak by som mal možnosť výberu výlučne jedného, tak by to bol projekt zameraný na mapovanie všetkých procesov v spoločnosti a aktív, ktoré sú s nimi viazané. To je totiž kľúčové pre správne riadenie rizík a ich následnú minimalizáciu. Lebo iba v prípade dobrej znalosti prostredia je možné efektívne smerovanie investícií do bezpečnosti.

**Zuzana Ďuračinská**
**projektová manažérka**
**LIFARS LLC**

Investovala by som do kvalitných ľudí so skúsenosťami. Dobrých ľudí by som nasadila tak do manažérskych, ako aj do technických úrovní. Až po dôslednom audite by som sa rozhodla, ako ďalej investovať a určite by som rozdelila investície do menších častí a na rôzne riešenia.

**Martin Fischer**
**manažér oddelenia bezpečnosti**
**Všeobecná zdravotná poisťovňa**

Nanešťastie, ani v prípade neobmedzeného rozpočtu sa oblasť kybernetickej bezpečnosti nedá pokryť jednou zázračnou škatuľkou. Investícia by však určite smerovala do technologického vybavenia, ktoré musí držať krok s dobou, aby sme vedeli efektívne čeliť najaktuálnejším hrozbám. Oblasť IT a predovšetkým kyber bezpečnosť sa vyvíjajú veľmi rýchlo, preto si nemôžeme dovoliť zaostávať.

**Marek Zeman**
**vedúci oddelenia bezpečnosti informačných systémov**
**Tatra banka**

Informačná bezpečnosť stojí na súhre veľkého počtu navzájom zapadajúcich koliesok. Každá firma si musí nájsť miesto v rozpočte na ochranu, monitoring systémov, mať nástroje na prevenciu, zastavenie útoku a dobrý incident manažment. Určite by som odporúčal, aby sa CISO venoval každému koliesku samostatne a zameral sa na najmodernejšie technológie. Neobmedzený rozpočet sa často nevidí.

**Ján Bodnár**
**konateľ**
**Unique People Košice**

Najcennejší, ale aj najviac zraniteľný článok sú samotní zamestnanci. Investoval by som preto do ich neustáleho vzdelávania tak, aby sa zžili s pravidlami kybernetickej bezpečnosti, boli schopní minimalizovať riziká napadnutia, rýchlo reagovali na prípadne hrozby a v krajnom prípade okamžite zasiahli. Pretože ani najlepší hardvér a softvér nás nedokáže ochrániť bez správne angažovaného zamestnanca.

**Pavel Nechala**
**partner**
**Advokátska kancelária WISE3**

Budovanie kultúry odolnosti voči kybernetickým hrozbám je zložitejší proces ako vzdelávanie o problematike. Cieľom je nielen odovzdať najnovšie poznatky, ale súčasne vysvetliť pracovníkom, ako konať a presvedčiť ich, že ich postoj je dôležitý. Ako je zrejmé, nebude na to postačovať jedna prednáška či smernica, ani jeden elearning, vyžaduje to kontinuálny proces budovania pozornosti.

**Richard Kiškováč**
**generálny riaditeľ**
**IstroSec**

Rozhodnutie o investícii by pravdepodobne smerovalo k nájdeniu odborne zdatného partnera, ktorý je schopný pokryť široké portfólio služieb kybernetickej bezpečnosti od prevencie až po riešenie bezpečnostných incidentov. Kľúčovým faktorom pri výbere by bol v prvom rade dostatočný počet kvalifikovaných expertov pre špecifické oblasti a ich reálne skúsenosti z praxe.

**Igor Práznovský**
**riaditeľ odboru bezpečnosti informačných systémov**
**Sociálna poisťovňa**

Nasadenie L7 firewallu a mikrosegmentácia siete so zapnutými threat profilmi aj pre vnútorné toky s cieľom implementovať princípy Zero Trust architektúry.

**Robert Mramúch**
**manažér kybernetickej bezpečnosti**
**MH Teplárenský holding**

S veľkou pravdepodobnosťou by som začal sieťovou infraštruktúrou. Kvalitný a (pre dané prostredie) správny návrh architektúry, zároveň i kvalitné nasadenie do prostredia, sú tie najlepšie predpoklady na budovanie bezpečnosti v každej organizácii.

**Petra Zorvanová**
**špecialistka informačnej bezpečnosti**
**Lidl Slovenská republika**

V skratke pár slovami: investovali by sme do awareness programu. Aby sme sa ešte viac venovali kolegyniam a kolegom. Pretože jedným z najslabších článkov je vo veľa prípadoch práve človek. A vzbudiť povedomie o informačnej bezpečnosti im pomôže nielen v pracovnom, ale aj súkromnom živote.

**Ján Golais**
**konateľ**
**JUDICIUM**

Kúpiť len jedinú vec by bola veľmi ťažká voľba. Kybernetický priestor je obrovský a taký bezpečný ako jeho najslabší prvok, preto je potrebné investovať do všetkých prvkov, ktorými sú technológie, personál. Súčasným trendom je zavedenie tzv. zero trust konceptu a určite sa oplatí investovať aj do viditeľnosti do siete.

**Juraj Koník**
**bezpečnostný manažér**
**Allianz-Slovenská poisťovňa**

Zabezpečiť kontinuálne a obsahovo rôznorodé vzdelávanie a nadobúdanie vedomosti všetkých našich zamestnancov za účasti nasadenia automatizovaných nástrojov pre zaznamenávanie bezpečnostných udalostí, ich flexibilnú a rýchlu analýzu prepojenia na biznis model spoločnosti až po celkovú eradikáciu.

**Jaroslav Oster**
**predseda správnej rady**
**Preventista.sk**

Investoval by som do vybudovania cyklického, systematického a cieleného zvyšovania bezpečnostného povedomia zamestnancov podľa reálnych potrieb. Realizácii by však muselo predchádzať zisťovanie aktuálneho stavu znalostí. Zvýšenú pozornosť by som venoval obsahu, aby reflektoval prostredie a zohľadňoval zavedené technické a organizačné opatrenia a skúsenosti z predchádzajúcich incidentov.

**Pavol Draxler**
**výkonný riaditeľ**
**Binary Confidence**

Objednal by som si Managed Security Service Provider (MSP) spoločnosť, ktorá sa bude starať o celú bezpečnosť v našej firme.

**Marián Klačo**
**vedúci oddelenia bezpečnosť informácií**
**Volkswagen Slovakia**

Vo všeobecnosti považujem za potrebné priebežne investovať do obnovy IT/OT technológií. Veľa organizácií totiž ešte stále používa zastarané a v praxi často už nepodporované technológie, ktoré býva problém vhodne zabezpečiť alebo patchovať. Rizikové sú najmä komponenty v priemyselných sieťach, často aj v kritickej infraštruktúre.