HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 29. NOVEMBRA – 1. DECEMBRA 2024

Komu dôverovať a kedy radšej utekať

ANKETA

Či už ide o odborníkov v teréne, stratégov, manažérov, audítorov, autority alebo lídrov veľkých tímov, hovoria o tom, čo si na kolegoch cenia. Aké osobné vlastnosti a dispozície sú dôležité v kybernetickej bezpečnosti?

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies

Analytické myslenie. Odolnosť proti stresu. Etika a integrita. Schopnosť rozhodovať pod tlakom. Schopnosť riadiť riziká. Technická znalosť a orientácia v oblasti. Vytrvalosť a odhodlanie robiť svet bezpečnejším miestom na život.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Kybernetická bezpečnosť nie je nikdy uzavretý stav a ani proces. Vysoký stupeň paranoje je síce vyčerpávajúci, ale pre bezpečákov užitočný.

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

Ak chcete byť (a zostať) uznaným profesionálom v ochrane hodnôt, tak na to sú bezpodmienečne nutné tri dispozície: kvalifikácia, dôveryhodnosť a poctivosť. Nie špekulantstvo, nie podvádzanie, nie „šmejdovské" metódy, nie konjunkturálna pseudoexpertíza a v žiadnom prípade nie práca pre zločincov. A čuduj sa svete, aj takí sa v tejto branži vyskytujú. Našťastie, netvoria jadro komunity bezpečákov.

Tomáš Hettych,
viceprezident,
ISACA

Profesionáli v kyberbezpečnosti musia mať hard skills: vzdelanie a skúsenosti v oblasti IT a KB, systematický prístup, manažérske zručnosti a riadenie času. Potrebujú však aj soft skills, ako sú nekonečný optimizmus, efektívna komunikácia a vyjednávanie, vytrvalosť pri presviedčaní nadriadených a vieru v lepší stav súladu po audite. Dobrého profesionála pozná viacero ľudí a má dobré referencie, meno si buduje roky.

Ján Adamovský,
riaditeľ bezpečnosti,
Slovenská sporiteľňa

Odvaha. Odvaha postaviť sa výzvam čelom, a nie opačnou stranou tela. Odvaha pomenovať problematické oblasti pravým menom. Odvaha ísť do rizika a zabojovať, keď som presvedčený, že ide o správnu vec. Odvaha ísť aj neprebádanými chodníčkami. Zároveň aj ten najväčší profesionál potrebuje aj kúsok šťastia. Nezabúdajme však, že práve odvážnym šťastie praje.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť,
Západoslovenská energetika

Určite zvedavosť a vytrvalosť, ktoré nás vnútorne nútia porozumieť veciam najhlbšie, ako sa dá. Motivujú nás hľadať a skúmať nové súvislosti a nakoniec nás dovedú k najlepším riešeniam.

Richard Kiškováč,
generálny riaditeľ,
Elkan

V praxi som sa stretol s mnohými profesionálmi, niektorí boli vo svojej misii úspešní viac, iní menej. Spoločnou vlastnosťou tých úspešných však bola veľmi dobrá schopnosť komunikácie. Aj keď sú odborné znalosti nutnosťou, komunikačné schopnosti považujem za nevyhnutné na úspešné pôsobenie profesionála v kybernetickej bezpečnosti.

Marek Madžo,
technický riaditeľ void SOC,
Soitron

Ako je dobrým zvykom, dobrý bezpečák býva často na spektre. To znamená – silné analytické myslenie, precíznosť až perfekcionizmus, schopnosť rýchleho učenia sa a v neposlednom rade taktiež odolnosť proti stresu. Nezabúdajme na schopnosť motivovať druhých k nepopulárnym a veľakrát nechceným riešeniam.

Benjamin Würfl,
obchodný manažér,
Eviden Slovakia

Základom je výborný prehľad v technológiách. Tie sa však vyvíjajú tak dynamicky, že nevyhnutnou vlastnosťou je aj zvedavosť a chuť stále sa učiť niečo nové. Dobrý bezpečák by mal byť dôkladný a trpezlivý, no zároveň by sa nemal ľahko uspokojiť – v tejto oblasti sa k úspechu človek často prepracuje len tak, že neustále skúma nové možnosti, objavuje nové spôsoby a s vášňou sa púšťa na nové chodníčky.

Štefan Pilár,
advokát,
SIGNUM legal

Prácu v kyberbezpečnosti, obdobne ako v oblasti práva, možno prirovnať k plávaniu proti prúdu. Ak zastanete, odbornosť a napokon aj celá oblasť vám ujdú. Preto je dôležitá neustála práca na sebe, sústavné vzdelávanie a kontakt s praxou. A schopnosť pozrieť sa na vec optikou klienta, aby sa mu dostalo to, čo skutočne potrebuje. Často som totiž videl výsledky auditu kyberbezpečnsoti, kde mnoho „pomocí" končí v koši a klient je tam, kde predtým.

Pavol Vrabec,
manažér kybernetickej bezpečnosti,
Univerzitná nemocnica Martin

Z môjho pohľadu sú kľúčové vlastnosti ako precíznosť a dôslednosť, kde polovičaté riešenia môžu mať a často aj mávajú vážne následky. Rovnako dôležitá je vytrvalosť a s tým súvisiaca psychická odolnosť, pretože práca v tejto oblasti je behom na dlhú trať a stav absolútnej bezpečnosti je nereálny, teda aspoň zatiaľ.

Tibor Szabo,
vedúci oddelenia auditu IT,
Všeobecná úverová banka

Ak si všimnem, že sa v mojom okolí vyskytol človek, ktorý je konzervatívny v zásadách, inovatívny v prístupoch a riešeniach a efektívny v manažmente zdrojov, vždy si spomeniem na slová „sekuriťákov" na prelome tisícročí – hľadať nové možnosti, nepodceňovať hrozby, ako proti nim bojovať, a nemíňať viac peňazí, ako je hodnota chráneného aktíva, tak zisťujem, že tieto princípy stále platia a máme kandidáta.

Veronika Paulinyová,
audítorka kybernetickej bezpečnosti,
Skupina CYLLIUM

Profesionál v kybernetickej bezpečnosti je človek schopný myslieť niekoľko krokov vpred a strategicky plánovať, tak ako šachista predvída kroky protivníka a plánuje obranu kráľa.

Roman Čupka,
hlavný konzultant,
Progress a CSO Istrosec

Tak ako v každej profesii je to najmä chuť sa vzdelávať a zdieľať skúsenosti. Navyše – húževnatosť spojená s prekonávaním prekážok umožňuje aj v kybernetickej bezpečnosti dosahovať ciele, na ktoré by si človek ani nepomyslel. Dôležité je identifikovať oblasti, kde sa človek cíti komfortne, a v tých sa ďalej posúvať trpezlivo dopredu. A hlavne si nezamieňať ego so zdravým sebavedomím.

Ivan Kopáčik,
bezpečnostný expert,
Gordias

Profesionáli v kybernetickej bezpečnosti problematiku riešia nie pre seba, ale pre kolektívy, organizácie či podniky. Okrem odbornej kompetencie je preto dôležitá aj istá miera empatie. V závislosti od svojej pozície by mali byť schopní vcítiť sa do potrieb a uvažovania tak vedenia, ako aj radových používateľov. Empatia môže výrazne uľahčiť presadzovanie vhodných bezpečnostných opatrení.

Róbert Mramúch,
manažér kybernetickej bezpečnosti,
MH Teplárenský holding

Ternom je mať za parťáka „osvieteného" IT riaditeľa, ktorý nepozerá iba po najbližší horizont, ale berie bezpečnosť ako prostriedok k udržateľnosti implementovanej stratégie prevádzkových technológií a IT. Prínos manažéra kyberbezpečnosti je hodnotný, ak s pochopením načúva potrebám biznisu, je dostatočne technicky a odborne podkutý do rozpravy so špecialistami IT alebo prevádzkových technológií a zároveň dokáže vyhodnotiť často protichodné požiadavky inak ako zákazom.

Július Selecký,
senior technický špecialista,
ESET

Kyberbezpečnosť si vyžaduje zvláštny talent predvídať katastrofy skôr, ako sa stanú. Schopnosť myslieť ako hacker, ale zároveň ním nebyť. Kľúčová je prirodzená paranoja so štipkou kreativity. Bonusom môže byť trpezlivosť, hlavne keď vám niekto tvrdí, že jeho „admin/admin" účet je úplne ok. To si niekedy vyžaduje úroveň zenového majstra.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti,
Aliter Technologies

V kybernetickej bezpečnosti je kľúčová schopnosť chápať komplexné systémy a problémy na elementárnej úrovni – redukcionizmus. Medzi ďalšie vlastnosti by som zaradil prirodzenú zvedavosť a snahu byť o krok vpred. Neustále napredovanie je doslova nevyhnutné, aby sme mohli udržiavať krok s útočníkmi. Rovnako však oceňujeme kolegov s prehľadom v legislatíve či s výbornými komunikačnými zručnosťami, ktoré sú dôležité na netechnických pozíciách.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií,
Volkswagen Slovakia

Opatrenia kybernetickej bezpečnosti a z nich vyplývajúce pravidlá a zásady sa nedajú často zaviesť okamžite, chvíľu trvá, kým sa „zažijú". Každý človek presadzujúci tieto opatrenia by mal byť trpezlivý. Mal by mať v sebe zápal pre vec, ten vnútorný oheň, nadšenie a sebamotiváciu posunúť veci v danej oblasti k lepšiemu, aj v časoch, keď nie je vždy slnečno.

Tibor Paulen,
manažér informačnej bezpečnosti,
Stredoslovenská distribučná

Ideálneho človeka pracujúceho v oblasti kybernetickej bezpečnosti si predstavujem ako racionálneho, trpezlivého, vytrvalého, odolného proti stresu, s minimálnym egom a maximálnou empatiou a komunikačnými schopnosťami. Nadšenie pre nové veci a ochota učiť sa sú samozrejmosťou.

Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Ťažká otázka. Rozhliadnuc sa vo svojom okolí medzi „kyberbezpečákmi", s potešením konštatujem, že je medzi nimi hneď niekoľko ľudí, u ktorých sa stretlo niekoľko pozitívnych vlastností. Profesionalitu považujem za štandardnú výbavu. Ale ak sa k nim pridá ešte skromnosť, spoľahlivosť a férovosť, našli ste niečo ako zlatý grál. Poznať takýchto ľudí je pre mňa cťou. Menovať nebudem, veď viete – GDPR.

Martin Oczvirk,
riaditeľ odboru informačnej bezpečnosti a certifikácie,
Úrad na ochranu osobných údajov

Prvá najdôležitejšia vlastnosť je pre mňa vysoký stupeň etiky a dôveryhodnosti, keďže práca kybernetickej bezpečnosti zahŕňa prácu s citlivými informáciami. Druhá vlastnosť je schopnosť kriticky myslieť. Vedieť identifikovať a posúdiť riziká. Potom je to schopnosť rozhodovať sa v rôznych situáciách. A v neposlednom rade vedieť efektívne spolupracovať s kolegami, jasne komunikovať technické informácie nielen s odborníkmi, ale aj s neodbornou verejnosťou.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov,
Tatra banka

Každé odvetvie pociťuje v súčasnosti tlak na výkon. Profesionál v kybernetickej bezpečnosti pozná aj znásobený tlak počas incidentov. Najväčšia výhoda je, ak je profesionál pokojný, rozvážny, rozmýšľa s nadhľadom a v kontexte organizácie a vzhľadom na rýchle a kvalitné riešenie incidentu. Veľké ego v kybernetickej bezpečnosti nemá miesto.

Timea Tomčová,
manažérka informačnej bezpečnosti,
Poisťovňa Union

Človek pracujúci v oblasti kybernetickej bezpečnosti by mal disponovať kombináciou technických, analytických, komunikačných a osobnostných vlastností. Z osobnostných vlastností považujem za najdôležitejšie spoľahlivosť, odolnosť a etiku.