scaut.com

2026 Report

Neviditelná pracovní síla

Jak falešné identity, “interview farmy“ a podvody poháněné umělou inteligencí pronikají do kritické infrastruktury

scaut

Neviditelná pracovní síla

Jak falešné identity, “interview farmy“ a podvody poháněné umělou inteligencí pronikají do kritické infrastruktury

Hodnocení hrozby pro vedení podniků kritické infrastruktury

Leden 2026

Obsah

scaut

Úvodní slovo

Sofistikované, nepřátelskými státy podporované operace popsané v tomto dokumentu se vyvinuly z okrajové hrozby do globální krize, která postihuje dodavatelský řetězec většiny kritických dodavatelů států NATO, společnosti z žebříčku Fortune 500, zdravotnické organizace i technologické firmy po celém světě. To, co začalo izolovanými incidenty, přerostlo v průmyslově organizovanou infiltrační kampaň, v níž útočníci využívají pokročilou umělou inteligenci, technologii deepfake a taktiky organizovaného zločinu k tomu, aby podvodní pracovníci pronikali do nic netušících organizací pod rouškou běžného náborového procesu. Nikoliv pod rouškou tmy a zadními vrátky - pozváni a uvítáni hlavním vchodem...

Klíčová zjištění:

- Zločinecké organizace vygenerovaly více než 17 milionů USD prostřednictvím jediné "laptop farmy", která zprostředkovala 309 falešných zaměstnání v amerických firmách.
- Technologie deepfake lze dnes vytvořit za méně než 70 minut, bez odborných znalostí, na běžném notebooku a s volně dostupnými nástroji.
- Téměř každý CISO ve firmách Fortune 500 se s touto hrozbou již setkal (podle technického ředitele Mandiant).
- Hrozba se rozšířila mimo Severní Ameriku – organizované operace jsou nyní aktivní v Evropě (Německo, Portugalsko, Polsko, Rumunsko, UK), v Rusku a Asii.
- 27% zjištěných podvodných IT pohovorů míří na neamerické firmy.
- Interview farmy v Asii umožňují "živé napodobování identit" – týmy zde vedou stovky paralelních pracovních pohovorů pod falešnými identitami.
- V roce 2025 uvedlo 85 dotazovaných zdravotnických organizací zkušenost s tímto typem podvodů. Cílem byl přístup k citlivým údajům o pacientech

220%

nárůst infiltrací severokorejských IT pracovníků během 12 měsíců

1 z 4

kandidátských profilů bude do roku 2028 falešný (predikce Gartner, červenec 2025)

Tato hrozba přesahuje rámec prostého pracovního podvodu. Jakmile se operativci dostanou dovnitř, zapojují se do krádeží duševního vlastnictví, šíření ransomwaru, průmyslové špionáže a úniků dat. Někteří přecházejí k vydírání – vyhrožují zveřejněním odcizených informací, pokud nedostanou zaplaceno.

Tradiční bezpečnostní perimetr byl prolomen – útočník už je uvnitř, pracuje po boku legitimních zaměstnanců, s plným přístupem do sítě a platnými přihlašovacími údaji.

Tento dokument přináší komplexní analýzu vyvíjející se hrozby, zkoumá její infrastrukturu, vektory útoku, skutečné dopady a obranné strategie. A především upozorňuje na zásadní mezeru, kterou si mnoho organizací stále neuvědomuje: oddělení HR a náboru nenesou odpovědnost za kybernetické riziko, čímž vzniká nebezpečná "díra" v obranném systému organizace.

Hrozba neúmyslného zaměstnání severokorejských IT pracovníků je větší, než si většina lidí uvědomuje. Je skrytá, globální a aktivní právě teď.

— Kevin Mandia, bývalý CEO Mandiant

Osobní zamyšlení nad vznikající hrozbou

V roce 2022, kdy se svět potýkal s bezprecedentními dopady pandemie COVID-19, můj tým ve Scaut.com – tehdy mladém projektu zaměřeném na pokročilé prověřování pracovníků – narazil na první náznaky sofistikované podvodné operace spojené se severokorejskými hackery. To, co zpočátku vypadalo jako ojedinělé nesrovnalosti v ověřování kandidátů, se brzy proměnilo ve zřetelný vzorec falešných identit a koordinovaných infiltračních taktik. Netušili jsme, že o tři roky později tato hrozba nabude průmyslového měřítka a zasáhne společnosti z žebříčku Fortune 500, poskytovatele zdravotních služeb i kritickou infrastrukturu po celém světě.

Ještě znepokojivější je, že povědomí o této problematice zůstává stále nízké i dnes. Jen menšina náborářů a HR profesionálů si uvědomuje její rozsah a závažnost, což umožňuje,

aby se tyto schémata dál nerušeně šířila. Tato skutečnost nás přiměla využít všechny dostupné prostředky – nejen jako podnikatelský závazek, ale i jako odpovědnost vůči širší komunitě – a systematicky tyto poznatky sdílet. Cílem této zprávy je popsat úplný rozsah tohoto problému a vybavit organizace nástroji, které jim umožní zabránit jeho dalšímu šíření.

Jako CEO a zakladatel společnosti Scaut.com, poskytovatele automatizovaného prověřování zaměstnanců se sídlem v Praze, jsem měl možnost z první ruky sledovat, jak se kybernetické hrozby stále více prolínají s lidskými procesy v oblasti náboru.

Scaut jsme založili v roce 2020, abychom reagovali na rostoucí potřebu přesného, a v souladu s předpisy prováděného, ověřování v době, kdy pracovní trh rychle směřoval k vzdálené a globalizované formě práce. Naše SaaS platforma spojuje špičkové technologie s analytickým dohledem odborníků, aby firmám umožnila komplexní prověrky – od ověření identity a trestní bezúhonnosti po kontrolu sankčních seznamů, či průběžný monitoring – a zajišťovala tak důvěru i dodržování předpisů napříč dodavatelským řetězcem.

Objev podvodů napojených na Severní Koreu už dva roky po založení společnosti byl sice náhodný, ale alarmující.

Zatímco svět se soustředil na dopady COVID19 krize, naše systémy zachytily nesrovnalosti v údajích uchazečů, které vedly ke státem řízeným aktérům využívajícím falešné identity, “interview farmy“ a umělou inteligenci k oklamání zaměstnavatelů. Zprávy z té doby, později potvrzené dalšími analýzami, ukazovaly, že cílem těchto operativců byla infiltrace do západních firem, k získání platů i duševního vlastnictví, čímž financovali režimní aktivity a obcházeli sankce.

Do roku 2026 – jak uvádějí naše vlastní zprávy i odborné studie – tato infiltrace dramaticky zesílila.

Zdokumentované případy ukazují, že jednotlivé operace generují milionové částky prostřednictvím mechanismů, jako jsou tzv. “laptop farmy“.

Nejznepokojivější však zůstává nedostatečná reakce.

Průzkumy a odborné pohledy ukazují, že i přes varování institucí, jako jsou FBI nebo ENISA, značná část evropských náborářů zůstává nepřipravena.

Tato slepá skvrna – často vznikající oddělením HR a bezpečnostních funkcí – vystavuje organizace hrozbě vnitřních útoků, úniku dat i reputačním škodám.

Ve Scautu nás tento nesoulad motivoval k akci: stali jsme se první evropskou

screeningovou firmou, která veřejně upozornila na tyto infiltrace, a vyvinuli jsme specializované nástroje pro odhalování anomálií – od nesouladů v IP adresách přes skriptované odpovědi u pohovorů až po padělané reference a doklady.

Naše poslání se rozšířilo z pouhé osvěty na praktická řešení.

Platforma Scaut nabízí modulární strukturu služeb – od jednoduchých plateb za jednotlivé prověrky až po podnikové předplatné s pokročilými funkcemi a vlastními pracovními postupy.

Základem je soulad s předpisy a bezpečnost dat: máme certifikaci ISO 27001, používáme end-to-end šifrování a zajišťujeme plnou kompatibilitu s GDPR, aby se minimalizovalo riziko úniku citlivých informací.

Tento dokument je proto naším příspěvkem ke kolektivní obraně – komplexním hodnocením hrozby doplněným o praktická opatření, která mohou organizace skutečně zavést, bez vysokých vstupních nákladů a stovek hodin externích konzultantů.

Problém: globální krize podvodů v náboru

Rozsah infiltrace

To, co bylo dříve považováno za izolovanou kuriozitu, se proměnilo v průmyslově organizovanou operaci.Státem podporovaní aktéři, především z Korejské lidově demokratické republiky (KLDR), vybudovali propracovaný ekosystém pracovních podvodů, který spojuje krádež identity, moderní technologie a metody organizovaného zločinu.

Mezi lety 2021 a polovinou roku 2025 zaznamenala společnost Okta, specializující se na ověřování identity, více než 130 potvrzených falešných identit, které provedly přes 6 500 úvodních pracovních pohovorů pro více než 5 000 firem po celém světě.

A to představuje pouze detekované případy – skutečný rozsah bude s největší pravděpodobností mnohonásobně větší.

Nedávné zprávy ukazují alarmující trendy:

- Vyšetřovatelé CrowdStrike zaznamenávají přibližně jeden případ severokorejského IT pracovníka denně
- Infiltrace se meziročně zvýšily o 220 % (k polovině roku 2025)
- Tisíce operativců se již úspěšně infiltrovaly do firem z žebříčku Fortune 500
- Jediná operace tzv. “laptop farmy“ v Arizoně vygenerovala 17,1 milionu USD z 309 falešných náborů

Zločinecká infrastruktura

Nejde o jednotlivce. KLDR vybudovala komplexní zločinecký aparát, který funguje spíše jako státem řízená mafie než jako klasická zpravodajská služba.

Celý systém zahrnuje specializované role a logistickou síť.

Krádež a tvorba identit

Operativci začínají získáváním nebo vytvářením falešných identit. Někteří kradou skutečné identity prostřednictvím úniků dat nebo sociálního inženýrství, jiní vytvářejí zcela syntetické identity pomocí nástrojů využívajících čím dál častěji umělou inteligenci.

Služby jako VerifTools (do listopadu 2025, kdy byla odstavena Nizozemskou policií a FBI, generující realisticky vypadající falešné doklady – pasy, občanské průkazy, výpisy z bank či diplomy – za částky kolem 8,99 USD. Tyto digitální padělky (šablony) jsou upravené tak, aby prošly kontrolou běžných online ověřovacích procesů.

“Interview farmy”

V Indii, Pákistánu, Číně a dalších asijských zemích vznikají specializovaná pracoviště, kde desítky operátorů vedou současně pracovní pohovory pro různé uchazeče. Za poplatek 200–500 USD dostane kandidát kompletní “podporu“ — jeden člověk naslouchá otázkám a přes ChatGPT v reálném čase diktuje odpovědi, druhý řeší technické testy a třetí spravuje sdílení obrazovky či dokumenty. Samotný uchazeč se stává pouhou tváří na kameře, zatímco celý tým řídí jeho výkon ze zákulisí.

Stačí zadat na Facebooku výraz “Interview Support Proxy“ a objeví se desítky skupin nabízejících tyto služby...

Zprostředkovatelé v USA a Evropě

Tato operace vyžaduje komplice v cílových zemích. Tito “facilitátoři“ — někteří vědomě, mnozí nevědomky — zajišťují klíčové služby: přijímají a uchovávají služební notebooky, instalují software pro vzdálený přístup, zakládají bankovní účty, vytvářejí adresy firem, nakupují AI nástroje a i provádějí rozhovory namísto severokorejských pracovníků.

Jedna Američanka, Christina Chapman, byla odsouzena k 8,5 roku vězení za provoz “laptop farmy“, kde spravovala 90 notebooků a umožnila 309 podvodných náborů, které vynesly pachatelům přes 17,1 milionu USD.

Maskování plateb

Platy se převádějí složitou strukturou praní peněz. Platformy jako Ruul.io, Payoneer, TransferWise nebo kryptoměnové burzy slouží jako prostředníci — často nevědomky. Tyto legitimní společnosti se tak stávají nechtěnými součástmi mechanismu obcházení sankcí, protože peníze nakonec končí na účtech spojených s vládou KLDR.

Operativci pravidelně mění bankovní účty, jakmile jsou původní uzavřeny kvůli podezření, což vytváří neustálou hru na kočku a myš s finančními institucemi.

Organizační struktura a motivace KLDR:

Výzkum společnosti DTEX Systems ukazuje, že severokorejské operace fungují spíše jako zločinecký syndikát řízený potřebou přežití než jako klasická špionážní služba.

Režim provozuje sofistikovanou hierarchii, která rozmazává hranice mezi kyberzločinem, špionáží a vojenskými operacemi. Operativci jsou motivováni především základními potřebami – zajistit jídlo, vzdělání pro rodiny a uniknout chudobě v ekonomice nedostatku. Tato kombinace zoufalství a elitního technického výcviku vytváří mimořádně nebezpečné a motivované aktéry.

Klíčové organizační prvky:

1. ***Výzkumné centrum 227:*** pokročilé vývojové středisko pro umělou inteligenci, které vytváří technologie deepfake, autonomní systémy a nástroje pro rychlé operace. Toto centrum urychluje tvorbu falešných identit a umožňuje operativcům vést přesvědčivé video pohovory s využitím AI generovaných osob.
2. ***RGB (Hlavní průzkumné byro):*** hlavní zpravodajská a speciální operační agentura zodpovědná za sběr informací, kyberoperace a sabotáže. Jednotky RGB často sdílí zdroje s podvodnými pracovními operacemi, čímž vytvářejí plynulé propojení mezi pracovním podvodem a klasickou špionáží.
3. ***Talent pipeline:*** KLDR identifikuje technicky nadané děti už od 10 let a zařazuje je do elitních výcvikových programů. Absolventi získávají vzdělání v matematice, informatice a cizích jazycích a poté jsou nasazeni do zahraničních operací. Výsledkem jsou mimořádně schopní infiltrátoři s reálnými odbornými znalostmi.
4. ***Strategie více zaměstnání:*** Mnoho operativců současně drží několik plných úvazků, které spravují pomocí AI nástrojů. Ty jim umožňují automatizovat komunikaci, rutinní úkoly a udržovat iluzi, že pracují pouze pro jednoho zaměstnavatele. Tak maximalizují výnosy a zároveň si zachovávají krytí..

Porozumění této organizační struktuře je klíčové pro efektivní obranu. Tito lidé nejsou amatérští podvodníci ani příležitostní hackeři – jsou produktem desítky let trvajícího státního programu, který má za cíl pronikat do západních technologických firem a kritické infrastruktury.

Režim ročně generuje odhadem 1 miliardu dolarů prostřednictvím krádeží kryptoměn a pracovních podvodů. Tyto prostředky přímo financují vývoj zbraní a destabilizační kampaně.

Každé falešné zaměstnání tak přispívá k šíření jaderných zbraní a podkopávání globální bezpečnosti.

scaut

Technologie umožňující tyto hrozby

Deepfakes: od science fiction ke komoditě

V dubnu 2025 provedli výzkumníci z Unit 42 (Palo Alto Networks) experiment:

Dokázal by člověk bez technických znalostí vytvořit přesvědčivý deepfake pro pracovní pohovor?

Výsledek byl šokující. Pomocí běžného vyhledávače, pět let starého notebooku s grafickou kartou GTX 3070 a volně dostupných nástrojů vytvořili plně funkční deepfake během pouhých 70 minut.

To představuje zásadní zlom.

To, co dříve vyžadovalo specializované znalosti, drahé vybavení a mnoho hodin práce, je dnes běžně dostupné komukoli. Technologie se demokratizovala – a KLDR tuto dostupnost plně využila.

Jak tato technologie funguje:

- Operativci používají aplikace pro výměnu obličejů, které nahrazují jejich vzhled syntetickou tváří generovanou nástroji jako ThisPersonDoesNotExist.com
- Díky zpracování videa v reálném čase lze během hovoru okamžitě manipulovat s obrazem obličeje
- Nástroje pro modulaci hlasu a překlad v reálném čase maskují přízvuk i jazykové nedostatky
- AI asistenti poskytují okamžité odpovědi na technické otázky a vytvářejí dojem hluboké odbornosti
- Pomocí více monitorů mohou operativci současně číst otázky, vyhledávat odpovědi a řídit vizuální podobu své “syntetické“ osoby

Společnost CrowdStrike zdokumentovala, že severokorejští operativci aktivně vyhledávají a odebírají prémiové služby pro tvorbu deepfake během svých operací.

Investice je minimální – často méně než 50 USD měsíčně – ale návratnost obrovská: jeden falešný pracovní poměr může vynést více než 100 000 USD ročně

Tvorba identit pomocí umělé inteligence

Generativní AI proměnila každý krok životního cyklu podvodů.

Výzkumníci společnosti Okta zdokumentovali rozsáhlé využívání AI nástrojů napříč celým procesem — od žádosti o zaměstnání až po samotný výkon práce:

Během podávání žádosti o práci:

- AI generuje přesvědčivé životopisy a motivační dopisy, přizpůsobené konkrétním popisům pozic
- Na LinkedInu vznikají syntetické profily s AI generovanými fotografiemi a smyšlenou kariérní historií.
- Pozadí pro falešné průkazy identity je často generováno pomocí Midjourney nebo DALL-E

Během pohovorů:

- Služby překladu v reálném čase umožňují plynulou komunikaci i neanglicky mluvícím kandidátům
- "Mock interview" platformy poskytují trénink a zpětnou vazbu, jak obstát v testech
- AI vyhodnocuje kvalitu deepfake videa a navrhuje vylepšení světla či kamery
- Chatboti poskytují okamžité odpovědi na technické otázky

Po nástupu do zaměstnání:

- AI pomáhá udržovat více paralelních pracovních poměrů, například tím, že asistuje při psaní zpráv na Slacku nebo e-mailů
- Generátory kódu umožňují pracovníkům dodávat výsledky bez hlubších znalostí
- Jazykové modely zajišťují gramaticky správnou a profesionálně znějící komunikaci

Případové studie: hrozby v praxi

Případová studie 1: Česká cloudová společnost (2023)

V roce 2023 zveřejnila česká cloudová firma nabídku práce na pozici vývojáře softwaru na LinkedInu. Mezi uchazeči byl Denys Emil L., který tvrdil, že je dánský občan žijící v Evropě. Jeho profil působil důvěryhodně: asijský vzhled, profesionální vystupování, dokumenty v pořádku. Úspěšně prošel prvním kolem HR pohovoru a zaslal průkazy totožnosti i potvrzení o předchozím zaměstnání.

Společnost Scaut, pověřená screeningem kandidáta, však odhalila nesrovnalosti. Jeden z

analytiků zjistil, že Denysovy dokumenty byly vygenerovány pomocí online nástrojů – na první pohled nerozeznatelné od skutečných. Záhy se ukázalo, že si přivlastnil identitu nic netušícího dánského občana, jehož živnostenské oprávnění se pokoušel zneužít.

Vyšetřování odhalilo, že Denys Emil byl ve skutečnosti čínský občan, který vytvořil více falešných identit a současně se ucházel o práci ve firmách po celé Evropě

Tento případ vyvolal zásadní otázky: Šlo o průmyslovou špionáž? Nebo o pokus získat přístup k infrastruktuře cloudové společnosti?

Pozdější analýzy potvrdily napojení na organizovanou skupinu se spojitostí s KLDR. Rozsah a systematičnost útoků naznačovaly státní koordinaci, nikoli individuální podvod.

Případová studie 2: Bezpečnostní firma KnowBe4 (2024)

Možná nejvíce ironickým případem je událost ve společnosti KnowBe4 – firmě specializující se právě na školení v oblasti kybernetické bezpečnosti.

Navzdory své expertize nechtěně zaměstnala severokorejského IT pracovníka.

Dotyčný kandidát prošel všemi koly náboru, úspěšně absolvoval pohovory a dokonce i standardní prověrku. Po přijetí mu firma zaslala služební notebook.

Jakmile zařízení dorazilo, operativní pracovník okamžitě začal instalovat škodlivý software a pokusil se infikovat firemní systém.

Bezpečnostní tým KnowBe4 si podezřelé aktivity rychle všiml a pracovní poměr okamžitě ukončil.

Firma následně incident transparentně zveřejnila v obsáhlém blogovém příspěvku, čímž poskytla cenný případ pro celou bezpečnostní komunitu.

Závěr je varovný: Pokud se společnost, která se živí výukou kybernetické bezpečnosti, může stát obětí této infiltrace, pak je ohrožena každá organizace — bez ohledu na její úroveň zabezpečení či povědomí.

Případová studie 3: “Laptop farma“ Christiny Chapman (2024–2025)

Christina Chapman, padesátiletá obyvatelka Arizony, provozovala ze svého domu to, co žalobci označili jako “laptop farmu“ – systém, v němž spravovala desítky firemních notebooků jménem severokorejských IT pracovníků. Na tato zařízení instalovala software pro vzdálený přístup, který umožňoval operativcům pracovat z ciziny, jako by fyzicky seděli v kancelářích amerických firem.

Operace byla mimořádně úspěšná:

309 podvodných náborů do amerických společností vygenerovalo 17,1 milionu dolarů.

Přibližně 70 Američanů mělo odcizenou identitu, která byla využita k vytvoření falešných pracovních profilů.

Mezi oběťmi byly i významné korporace — například Nike ve své výpovědi potvrdila, že nevědomky zaměstnala severokorejského operativce právě prostřednictvím Chapmanovy operace.

Christina Chapman se přiznala k vině a byla odsouzena k 8,5 roku vězení.

Vyšetřovatelé však věří, že její síť nebyla ojedinělá.

Podle zpráv CrowdStrike se po zásazích amerických orgánů podobné “laptop farmy“ objevily v Evropě, především v Rumunsku a Polsku, kde se snaží napodobit stejný model a využít méně přísné místní regulace.

Případová studie 4: Evropské “interview farmy“ (2024–2025)

Zkušený český IT náborář, který vedl stovky pohovorů, začal v posledních dvou letech pozorovat znepokojivý vzorec. Kandidáti s perfektními životopisy, profesionálními profily na LinkedInu a výbornou písemnou komunikací se při video pohovorech chovali podezřele podobně:

- Kamera často nefungovala nebo byla vypnutá.
- V pozadí bylo slyšet více hlasů, jako by se hovor odehrával v call centru.
- Technické otázky byly zodpovězeny plynule, ale osobní dotazy vyvolávaly váhání.
- Při zmínce o okolním hluku nebo žádosti o otočení kamery se spojení okamžitě přerušilo.
- IP adresa často odhalila připojení z Asie, i když kandidát tvrdil, že žije v Evropě.

Vyšetřování ukázalo, že tito kandidáti byli připojeni z asijských interview farem – provozů, kde týmy operátorů pomáhají desítkám uchazečů současně.

Rozsah a organizovanost naznačovaly průmyslový charakter, nikoliv individuální pokusy.

Ve většině případů, kdy byl kandidát konfrontován s otázkami o svém místě pobytu nebo požádán, aby ukázal okolí kamery, hovor okamžitě ukončil.

V devíti z deseti případů se již na další komunikaci nikdy neozval.

Případová studie 5: Německá energetická infrastruktura (2024)

Velký německý provozovatel energetické infrastruktury, klasifikovaný jako součást kritické infrastruktury podle národních předpisů KRITIS i směrnice EU CER, odhalil na konci roku 2024 sofistikovaný infiltrační pokus při běžném bezpečnostním auditu.

Společnost přijala na pozici systémového inženýra kandidáta s německými doklady a dlouholetou praxí v oblasti správy systémů SCADA.

Po třech měsících jeho práce si bezpečnostní tým všiml neobvyklých datových toků — konkrétně pokusů o exfiltraci konfigurací řídicích systémů, map elektrické sítě a provozních protokolů.

Další analýza odhalila, že zaměstnanec používal software pro vzdálený přístup, který umožňoval ovládání jeho pracovního počítače z Asie během nočních hodin.

Incident představoval závažné selhání bezpečnosti s potenciálním dopadem na národní infrastrukturu.

Operativní pracovník měl přístup k systémům, které řídí distribuci elektřiny pro statisíce domácností i průmyslových provozů.

Německé úřady incident klasifikovaly jako státem sponzorovanou špionážní operaci, i když jméno společnosti nebylo zveřejněno kvůli ochraně pověsti.

Tento případ urychlil diskusi o povinném bezpečnostním prověřování personálu v rámci kritické infrastruktury napříč celou EU.

Případová studie 6: Únik dat ve zdravotnictví ve Velké Británii (2025)

Na začátku roku 2025 zjistil dodavatel Národní zdravotní služby (NHS) ve Spojeném království, že jeden z jeho databázových administrátorů, zaměstnaný teprve šest měsíců, exfiltroval více než 4,2 milionu záznamů pacientů.

Operativní pracovník se prokázal britským občanstvím a doložil bezchybné dokumenty, díky čemuž mu byl udělen rozšířený přístup k citlivým zdravotnickým databázím obsahujícím osobní, anamnestické i léčebné informace.

Incident se týkal společnosti Synnovis, poskytovatele patologických služeb pro hlavní londýnské nemocnice.

Únik přímo předcházel ransomwarovému útoku, který paralyzoval provoz několika nemocnic NHS a ukázal, jak se personální bezpečnostní selhání může přenést do rozsáhlé provozní krize.

Odhalení přišlo ve chvíli, kdy automatizovaný systém zaznamenal neobvyklé hromadné exporty dat o víkendech, kdy měl být zaměstnanec offline.

Forenzní analýza ukázala, že operativní pracovník systematicky kopíroval celé databázové tabulky na šifrovaná externí úložiště po dobu několika měsíců.

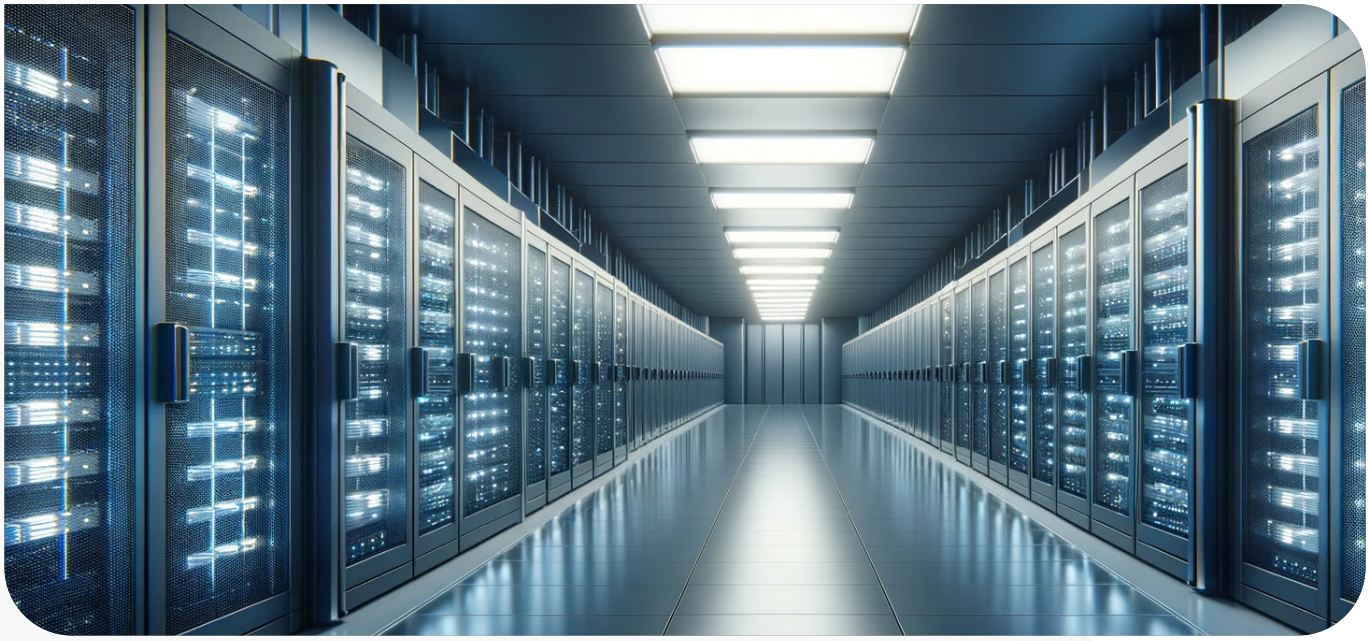
Exfiltrovaná data zahrnovala nejen běžné zdravotní záznamy, ale i psychiatrické posudky, záznamy o léčbě závislostí a výsledky genetických testů – přesně ten typ informací, které jsou cenné pro vydírání, pojistné podvody nebo krádež identity.

Finanční dopad incidentu přesáhl 22 milionů liber, zahrnujících okamžitou reakci, informování pacientů, služby ochrany identity a pokuty podle britského GDPR.

Závažnější však byl dopad reputační a systémový: případ vyvolal komplexní revizi prověřovacích postupů pro externí pracovníky napříč NHS.

Úřad pro ochranu osobních údajů (ICO) označil nedostatečné ověření zaměstnance za klíčový faktor incidentu a konstatoval, že dodavatel neověřil pracovní historii ani vzdělání.

Případ se stal precedentem v debatě o povinném prověřování personálu ve zdravotnickém sektoru Spojeného království.



Případová studie 7: Polská finanční instituce a přesměrování plateb (2024)

Varšavská finanční společnost zjistila v polovině roku 2024, že její seniorní vývojář softwaru prováděl sofistikované přesměrování plateb.

Zaměstnanec, který byl ve firmě téměř osm měsíců, vloženým škodlivým kódem v systému pro zpracování plateb odváděl drobné částky z mezinárodních převodů na kryptoměnové účty. Schéma bylo mimořádně nenápadné – kód zaokrouhloval částky dolů o zlomky centů a rozdíl přesměrovával na externí účty.

Během osmi měsíců tak bylo odčerpáno přibližně 840 000 eur, než byla manipulace odhalena při rutinním auditu. Zaměstnanec předložil polské doklady totožnosti a uváděl předchozí praxi ve finančních institucích v Estonsku a Litvě.

Ověření zpětně odhalilo, že všechny tyto dokumenty byly vygenerovány pomocí AI.

Na tomto případu byla znepokojující především trpělivost a technická sofistikovanost útočníka. Nešlo o rychlý útok, ale o dlouhodobé a promyšlené zneužívání systému, které zůstalo měsíce nepovšimnuto.

Polský finanční dohled na základě incidentu doporučil zvýšení personálních bezpečnostních standardů, zejména pro pracovníky s přístupem k platebním systémům a klíčovým datovým infrastrukturám.

Případ rovněž upozornil na zranitelnost finančních institucí ve východní Evropě, které bývají častěji cílem podobných útoků kvůli své poloze a propojení s evropským finančním systémem.

Případová studie 8: Důvěra jako cíl (Rakousko, 2025)

Na začátku roku 2025 se rakouská společnost zaměřená na čištění odpadních vod ocitla pod tichým, ale intenzivním vyšetřováním.

Nešlo o kyberútok, únik dat ani vydírání – ale o člověka.

Podezřelý ruský agent se měl dostat do firmy nikoli hackerským útokem, ale navázáním osobních vztahů.

Účastnil se odborných seminářů, zapojoval se do technických diskusí, seznamoval se s inženýry, získával důvěru — a postupně se stal součástí vnitřního kruhu důvě.

Po léta zůstával bez povšimnutí.

Tento případ se stal varováním pro evropskou průmyslovou a bezpečnostní komunitu: infiltrace už dnes nevypadá jako špionáž minulosti.

Neprobíhá potají – je pozvána dovnitř.

Zásadní poučení zní: nestačí "znát své zaměstnance" — je nutné vědět i koho znají oni.

Každý externí kontakt – konzultant, návštěvník, účastník konference – může být potenciálním bodem přístupu do sítě důvěry, která tvoří základ moderních organizací.

Jakmile se do této sítě dostane outsider, síla vašich kybernetických opatření ztrácí význam.

Nejcennější aktivum každé firmy není technologie, ale důvěra.

A nejslabším článkem nebývá heslo — ale člověk, kterému jste důvěřovali bez ověření.

Dopady a důsledky pro korporace

Finanční dopady na společnost

Přímý finanční dopad této hrozby se projevuje v několika dimenzích:

Krádeže mezd a generování příjmů:

Každé podvodné zaměstnání generuje ročně mezi 50 000–150 000 USD, přičemž tyto prostředky nakonec směřují do režimu DPRK (Severní Koreje).

Operace Chapman sama o sobě vygenerovala 17,1 milionu USD. Při tisících takových operativců zaměstnaných po celém světě celkový roční příjem pravděpodobně přesahuje 100 milionů USD, které přímo financují vývoj zbraní a obcházení sankcí.

Provozní neefektivita:

Mnoho podvodných pracovníků zastává více pracovních pozic současně, což rozděluje

jejich pozornost a snižuje kvalitu práce. Firmy platí plný úvazek za poloviční výkon, čelí zpožděním projektů, problémům s kvalitou a technickému dluhu. Náklady na nápravu — přepisování špatného kódu, opravy bezpečnostních zranitelností, obnova po selhání projektu — často přesahují původní mzdové výdaje.

Únik dat a krádež duševního vlastnictví:

Podle IBM Cost of Data Breach Report 2024 činí průměrné globální náklady na únik dat 4,88 milionu USD. V oblasti zdravotnictví se průměrná částka pohybuje kolem 11 milionů USD. Když operativci exfiltrují zdrojové kódy, data zákazníků nebo strategické informace, mohou být finanční dopady katastrofální. Hodnota ukradeného duševního vlastnictví v technologickém, finančním a zdravotnickém sektoru je nevyčíslitelná.

Ransomware a vydírání:

Od konce roku 2024 stále více operativců přechází po ukončení pracovního poměru k vydírání. Společnost Secureworks zaznamenala případy, kdy nedávno propuštění IT pracovníci vyhrožovali zveřejněním důvěrných dat nebo jejich prodejem konkurenci, pokud jim nebude zaplaceno. To představuje posun od pasivní krádeže dat k aktivní monetizaci, což výrazně zvyšuje závažnost hrozby.

Právní a regulatorní rizika

Organizace, které nevědomky zaměstnávají operativce DPRK, čelí závažným právním důsledkům:

Porušení sankcí:

Platby severokorejským občanům porušují sankce USA, EU a OSN. I neúmyslné porušení může vést k vysokým pokutám. Americké společnosti čelí možným sankcím ze strany Office of Foreign Assets Control (OFAC), které se mohou pohybovat od statisíců až po miliony dolarů.

Porušení ochrany osobních údajů:

Podle GDPR, NIS2, CER a obdobných předpisů mají organizace přísnou povinnost chránit osobní a citlivá data. Pokud podvodný pracovník exfiltruje informace zákazníků, firma čelí riziku pokuty až do 4 % z celosvětového ročního obratu podle GDPR. Zdravotnické organizace v USA podléhají postihům dle HIPAA a finanční instituce riziku sankcí ze strany svých regulátorů.

Žaloby akcionářů a zákazníků:

Po únicích dat nebo bezpečnostních incidentech čelí firmy hromadným žalobám zákazníků a žalobám akcionářů za nedostatečná bezpečnostní opatření. Reputační škody mohou převýšit přímé finanční ztráty — zákazníci ztrácí důvěru a investoři zpochybňují řízení společnostie.

Evropský rozměr: rostoucí cíl

Geografické rozšíření mimo Severní Ameriku

S tím, jak orgány činné v trestním řízení v USA zesilují represe — včetně obžalob, zátahů na “laptop farmy“ a kampaní na zvyšování povědomí — operace DPRK se záměrně rozšiřují geograficky.

Podle Google Threat Intelligence Group bylo potvrzeno, že se tyto aktivity rozšířily do více evropských zemí.

Aktuálně je 27 % zjištěných podvodných pracovních pohovorů zaměřeno na ne-americké společnosti.

CrowdStrike hlásí, že evropské incidenty vyšetřuje na denní bázi.

Podle hodnocení UK Treasury Probability Yardstick je “s téměř jistotou“ pravděpodobné, že falešní IT pracovníci cíleně napadli britské firmy.

Proč je Evropa zranitelná

Rozptýlený a nejednotný regulační rámec:

Evropa je lákavým cílem nejen díky své ekonomické síle, ale i kvůli rozdílným úrovním regulačních požadavků mezi členskými státy. Zatímco některé země (např. Německo nebo Nizozemsko) mají striktní bezpečnostní rámce pro pracovníky s přístupem k

citlivým datům, jiné jurisdikce — zejména východní a jižní Evropa — uplatňují mírnější nebo zpožděné implementace směrnic.

Tento roztříštěný přístup vytváří prostor pro operativce, kteří využívají mezery mezi legislativami. Náborová agentura sídlící v jedné zemi může poskytovat pracovníky jiné firmě v jiném státě EU, kde se na ověřování identity vztahují jiné nebo slabší předpisy.

Útočníci tak využívají volného pohybu pracovních sil – principu, který byl navržen pro podporu inovací a mobility, ale nyní se obrací proti evropským firmám.

Dálková práce jako katalyzátor:

Pandemie a následný přechod na vzdálené pracovní modely výrazně zrychlily tempo náboru v mezinárodním měřítku.

Zaměstnavatelé se zaměřili na rychlost a dostupnost namísto důkladného ověřování.

To vytvořilo prostředí, v němž je falešná identita prakticky neodhalitelná – zejména pokud pracovník nikdy fyzicky nenavštíví kancelář.

Přes 60 % evropských technologických firem podle European Tech Survey 2025 přiznalo, že nemají standardizovaný proces pro ověřování identity při nástupu vzdálených zaměstnanců nebo externích dodavatelů.

Z tohoto důvodu jsou právě start-upy a menší poskytovatelé IT služeb nejčastějšími oběťmi.

Zaměření na dodavatelské řetězce:

Evropské společnosti jsou vysoce propojené prostřednictvím komplexních dodavatelských řetězců.

Jeden kompromitovaný subdodavatel může otevřít dveře k celé síti partnerů.

Útočníci se proto zaměřují na malé či střední firmy, které poskytují služby větším korporacím – zejména v oblastech cloudových řešení, vývoje softwaru a údržby IT systémů.

Jakmile se podvodník dostane do jednoho článku řetězce, může eskalovat přístupové oprávnění nebo získat přístup k citlivým klientským datům prostřednictvím legitimních kanálů.

Evropská unie začíná na tuto hrozbu reagovat prostřednictvím nové legislativy, včetně směrnic NIS2 a CER, ale implementace napříč členskými státy je stále nerovnoměrná a pomalá.

Dokud nebude zavedena společná metodika prověřování personálu a dodavatelů, zůstane Evropa pro tyto hrozby snadno zranitelná.

Lidský firewall: proč je prověřování zaměstnanců první linií obrany

Osobní pohled Petra Moroze, zakladatele Scaut.com

Když jsme v roce 2020 objevili našeho prvního podezřelého severokorejského operativce, pamatuji si ten okamžik naprosto jasně. Nebyl to žádný sofistikovaný algoritmus umělé inteligence, kdo ho odhalil. Nebyl to automatizovaný systém detekce podvodů ani platforma. Byla to Anna, jedna z našich vedoucích analytiček, která se během kontroly náhle zarazila a řekla: “Něco na tomhle kandidátovi nesedí.“

Dokumenty vypadaly dokonale — vlastně až příliš dokonale. Estonský pas se všemi správnými bezpečnostními prvky, dokonce s QR kódem vedoucím na vládní potvrzení pravosti. Vysokoškolský diplom z renomované technické univerzity. Na první pohled všechno souhlasilo. Ale Anna si všimla něčeho jiného: fotografie na profilu LinkedIn byla zjevně obrázek z fotobanky. Později jsme objevili několik dalších profilů s drobnými nesrovnalostmi v údajích. Profesní reference odpovídaly až podezřele rychle – jako by nás očekávaly, ale když jsme se doptávali na konkrétní detaily projektů, nedokázaly si nic vybavit. Vzorce e-mailové komunikace zároveň naznačovaly, že dotyčný pracuje z jiného časového pásma, přestože tvrdil, že žije v Evropě.

Tohle nebyly datové body, které by spustily výstrahu algoritmu.

Byly to signály, které vyžadovaly lidskou interpretaci – schopnost propojit zdánlivě nesouvisející informace, rozpoznat vzorce, které do sebe úplně nezapadají, a klást otázky, které stroj klást neumí.

Tomu říkám lidský firewall: kritická vrstva inteligentní lidské analýzy, která stojí mezi surovými daty a informovaným rozhodováním při náboru.

Mýtus automatizované bezpečnosti

V oblasti kybernetické bezpečnosti jsme vybudovali pozoruhodné technologické obranné systémy. Firewally, které monitorují miliardy datových paketů za sekundu.

Systémy detekce průniků poháněné strojovým učením. Architektury nulové důvěry (zero trust), které ověřují každý jednotlivý požadavek na přístup. A přesto tu máme paradox: **ti nejsofistikovanější útočníci nepronikají skrze váš firewall — vcházejí předními dveřmi s nabídkou práce a firemním notebookem v ruce.**

Tradiční bezpečnost se zaměřuje na perimetr: jak udržet neoprávněné aktéry mimo síť Ale co se stane, když je hrozbou osoba, která je oprávněná? Když má platné přihlašovací údaje, schválený přístup k systému a podepsanou pracovní smlouvu?

Váš systém pro detekci průniků se nespustí, protože k žádnému průniku nedošlo — ten člověk tam má být. Vaše nástroje pro prevenci úniku dat nevyhlásí poplach, protože zaměstnanec má přístupová oprávnění ke všem informacím, které právě exfiltruje.

A právě tady se lidský firewall stává nepostradatelným. Prověřování historie kandidátů není jen formální “povinnost HR“, ale první a často nejdůležitější obrannou linií proti interním hrozbám, které obejdou všechny ostatní bezpečnostní mechanismy, do nichž jste investovali.

Je to rozdíl mezi tím, když odhalíte podvodného zaměstnance už během náboru, a tím, když ho odhalíte až po šesti měsících, kdy už stihl odcizit vaše duševní vlastnictví, nainstalovat zadní vrátka do systémů nebo prodat přístup k vaší síti ransomwareovým skupinám.

Tři dimenze moderního prověřování zaměstnanců

Moderní bezpečnostní prostředí vyžaduje, aby se proces prověřování rozšířil za hranice tradičního ověřování minulosti. Nestačí pouze potvrdit, že někdo existuje — je nutné ověřit, kým skutečně je, co může udělat, a jak se v čase mění:

1. ***Prověřování před nástupem do zaměstnání: kritická brána***

   Tady se bitva vyhrává – nebo prohrává. Jakmile někdo získá firemní notebook a přístupové údaje k síti, jeho odstranění se stává násobně obtížnějším a dražším Prověřování před nástupem do zaměstnání je příležitostí odhalit hrozbu dřív, než získá přístup. A tady dělá většina organizací zásadní chybu: považují ho za ověření dokumentů, nikoli za zpravodajskou činnost zaměřenou na hrozby.

   Vzpomínám si na náš první případ z roku 2020. Dokumenty toho kandidáta nebyly technicky falešné – byly skutečné, pečlivě vytvořené s využitím kradených identit a nástrojů pro syntetickou identitu.

   Automatizovaný systém by ho schválil okamžitě. Číslo pasu bylo platné. Bankovní účet existoval. Univerzita potvrdila studijní záznamy. Živnost patřila stejné osobě. Ale náš analytik si všiml nesrovnalostí v příběhu, který tyto dokumenty dohromady vyprávěly.

   Efektivní prověřování před nástupem znamená propojovat datové body z různých zdrojů a hledat vnitřní logiku příběhu. Odpovídá pracovní historie kandidáta jeho vzdělávací časové ose? Uváděné reference poskytují konkrétní detaily, nebo jen obecnou chválu? Odpovídá digitální stopa deklarovanému místu pobytu a zaměstnání? Jsou v jeho historii mezery, které se zdráhá vysvětlit?

   Na tyto otázky dokáže odpovědět pouze lidský úsudek, podpořený zkušeností a schopností rozpoznávat vzorce získané analýzou tisíců legitimních profilů.

   Ve Scautu jsme tento přístup pojmenovali “screening s profesní skepsí“. Naši analytici a nástroje dokumenty pouze neověřují – aktivně hledají důvody, proč příběhu nevěřit. Nejde o nespravedlivé zpochybňování poctivých uchazečů, ale o uznání skutečnosti, že sofistikovaní útočníci dokážou vytvářet přesvědčivé materiály.

   Cílem není dokonalost, ale zvýšení rizika odhalení a složitosti pro podvodníky natolik, aby se celá operace stala neekonomickou.

2. ***Průběžný monitoring zaměstnanců: vyvíjející se hrozba***

   Pravda, kterou nechceme slyšet: to, že někdo prošel vstupní prověrkou, neznamená, že zůstane důvěryhodný po celou dobu zaměstnání.

   Finanční potíže, osobní krize, ideologické změny nebo vnější nátlak mohou proměnit legitimního zaměstnance ve vnitřní hrozbu.

Navíc sofistikovaní operativci si často budují čisté kredity a historii roky dopředu, aby mohli udeřit ve vhodný okamžik.

Průběžný monitoring tuto realitu reflektuje. V organizacích spadajících pod regulované rámce kritické infrastruktury není volitelné – je povinné.

Ale i tam, kde zákon takovou povinnost neukládá, je třeba se ptát: Kolik stojí odhalit kompromitovaného zaměstnance po šesti měsících, oproti tomu, kdybychom ho zachytili včas?

Efektivní průběžné sledování kombinuje automatické výstrahy s periodickým lidským dohledem. Nové zápisy na sankčních seznamech, trestní obvinění, ukazatele finančních potíží, změny chování na sociálních sítích — to vše může signalizovat zvýšené riziko. Ale technologie sama o sobě nestačí.

Když se zaměstnanec náhle objeví na finančním seznamu sledovaných osob, je to kvůli krádeži identity, skutečným finančním problémům, nebo účasti na nezákonné činnosti?

Lidský analytik určuje kontext a posuzuje reálné riziko, nikoli jen signalizaci systému.

Průběžný monitoring vnímám jako imunitní systém bezpečnosti organizace. Prověřování před nástupem je jako kožní bariéra – první linie, která zachytí většinu hrozeb. Ale některé hrozby se detekci vyhnou nebo se rozvinou až později.

Průběžný monitoring cirkuluje napříč organizací, odhaluje anomálie a reaguje dřív, než se z nich stanou katastrofální incidenty.

3. *Rozšířená pracovní síla a bezpečnost dodavatelského řetězce: zapomenutá hranice*

Právě zde organizace nejčastěji selhávají — a právě sem útočníci soustřeďují své úsilí Proč by se někdo měsíce snažil proniknout přímo do korporace z žebříčku Fortune 500, když se může nechat najmout u jejího dodavatele nebo poskytovatele služeb a získat přístup skrze dodavatelský řetězec, kde je kontrola mnohem slabší?

Zvažte rozsah útoku: Vaše firma zaměstnává 500 lidí. Provádíte důkladné prověrky, školení o bezpečnosti, průběžný monitoring.

Ale spolupracujete s 50 dodavateli, partnery a poskytovateli služeb, kteří dohromady zaměstnávají dalších 5 000 lidí — z nichž mnozí mají přístup k vašim systémům, datům nebo prostorám. Kolik z těchto 5 000 osob bylo prověřeno stejným standardem jako vaši vlastní zaměstnanci?

Případ “laptop farmy“ Christiny Chapmanové tuto zranitelnost dokonale ilustruje.

Místo přímého pronikání do cílových firem se severokorejští operativci napojili na

personální agentury a outsourcingové společnosti. Tyto prostředníky se hodnotilo hlavně podle ceny a rychlosti dodávky, nikoli podle kvality prověřování.

Výsledek: 309 úspěšných umístění generujících 17,1 milionu USD, než byly odhaleny.

Bezpečnost dodavatelského řetězce se netýká jen ověřování bezpečnostních standardů vašich partnerů — týká se i ověření lidí, které tito partneři zaměstnávají.

To dnes výslovně vyžadují jak směrnice CER, tak i český zákon o kybernetické bezpečnosti (ZKI): provozovatelé kritické infrastruktury musí prověřovat nejen své vlastní pracovníky, ale i zaměstnance subjektů, které se podílejí na poskytování základních služeb. Je to uznání reality, že hranice organizací jsou propustné a že hrozby nerespektují organizační struktury ani firemní schémata.

Ve Scautu jsme zaznamenali, že se dodavatelský řetězec stává čím dál častějil hlavním vektorem útoku.

Když prověřujeme pracovníky dodavatelů a externích partnerů, nacházíme podvodné kandidáty třikrát až čtyřikrát častěji než mezi přímými zaměstnanci.

Proč? Protože útočníci velmi správně vyhodnocují, že externí pracovníci podléhají menší kontrole, zatímco často získávají stejnou úroveň přístupu jako interní zaměstnanci.

Váš lidský firewall se proto musí rozšířit za hranice vaší organizace – a chránit celou rozšířenou pracovní sílu, která tvoří skutečnou tvář vaší firmy.

Umění a věda rozlišování signálů

Co dělá z analytika prověřování skutečně efektivního odborníka? Není to jen přístup k databázím nebo ověřovacím nástrojům — ale schopnost oddělit šum od signálu a rozpoznat, co má skutečný význam. V dnešním prostředí se topíme v datech, ale hladovíme po vhledu.

Typická prověrka může zahrnovat:

1. Doklady totožnosti z různých zemí, z nichž každá má jiné bezpečnostní prvky a postupy ověření.
2. Pracovní historii napříč státy a jazyky.
3. Dokumenty od vzdělávacích institucí s rozdílnými procesy potvrzování.
4. Rejstříky trestů, které mohou být neúplné nebo zastaralé.
5. Digitální stopu na sociálních sítích, profesních platformách a ve veřejných registrech.
6. Finanční záznamy a historie, které mohou být pravé, odcizené nebo syntetické.
7. Reference, které mohou být autentické, naučené nebo zcela smyšlené.

Efektivní analytik se nespokojí s tím, že ověří, zda každý z těchto prvků vypadá platně. Zkoumá, zda všechny dohromady vytvářejí soudržný příběh. Hledá to, čemu říkám “narativní tření“ – jemné nesrovnalosti, které naznačují konstruovanou identitu, nikoli autentický životní příběh.

Například kandidát tvrdí, že má pět let zkušeností s prací na dálku, ale jeho profil na LinkedInu vznikl teprve před šesti měsíci. To je narativní tření.

Jiný kandidát uvede referenci, která nadšeně chválí jeho technické schopnosti, ale nedokáže si vzpomenout, jaké konkrétní technologie při projektech používal. To je narativní tření.

Nebo univerzita potvrdí absolvování, ale časově se to překrývá s vízovými omezeními, která by fyzickou účast na studiu znemožnila. To je také narativní tření.

Žádný z těchto signálů sám o sobě neprokazuje podvod. Každý může mít logické vysvětlení. Ale dohromady vytvářejí vzorec, který si zaslouží hlubší prověření. A právě zde lidský firewall exceluje: v rozpoznávání vzorců, které automatizované systémy přehlížejí, protože vyžadují kontextové porozumění a mezioborové znalosti.

Partnerství analytika a náboráře: jak porozumět signálům

Lidský firewall neslouží jen k zastavení hrozeb — jeho úkolem je umožnit informovaná rozhodnutí. Screeningoví analytici nejsou strážci, kteří svévolně odmítají kandidáty; jsou to zpravodajští analytici, kteří poskytují náborářům a manažerům přesné a ověřené informace pro rozhodování založené na faktech.

Toto partnerství je klíčové. Náboráři rozumí obchodním potřebám, požadavkům role a kvalifikaci kandidátů. Analytici zase chápou metodiky ověřování, ukazatele podvodů a vzorce hrozeb. Společně dokážou rozlišit mezi varovnými signály, které skutečně naznačují hrozbu, a neškodnými odchylkami, jež vyžadují pouze objasnění.

Uveďme reálný příklad, s nímž jsme se setkali: Kandidát na seniorní inženýrskou pozici měl osmiměsíční mezeru v zaměstnání. Automatizovaný screening ji označil jako problém. Povrchní posouzení by vedlo k odmítnutí. Náš analytik však kontaktoval náboráře, který se spojil s kandidátem pro vysvětlení. Ukázalo se, že šlo o rodičovskou dovolenou po narození dvojčat, během níž kandidát dokončil pokročilou profesní certifikaci. Poskytl dokumentaci o obou skutečnostech. Mezera tedy nebyla varovným signálem — byla životní událostí, která zvýšila jeho kvalifikaci.

Porovnejme to s jiným případem: Kandidát měl drobné nesrovnalosti v datech zaměstnání – několik týdnů rozdílu mezi životopisem a profilem na LinkedInu. Na první pohled snadno vysvětlitelné jako nevinná chyba v evidenci. Když však náš analytik pátral hlouběji, zjistil, že kandidát zcela vymyslel jedno z uvedených zaměstnání – u firmy, která mezitím zanikla, což ztěžovalo ověření. Ty malé časové rozdíly tak byly ve skutečnosti důkazem špatně vystavěné falešné identity.

Rozdíl mezi těmito případy? Lidský úsudek aplikovaný v kontextu. Právě to odlišuje efektivní prověřování od formálního zaškrtávání políček. Cílem není odmítat každého kandidáta s anomálií, ale pochopit, které odchylky jsou významné a poskytnout náborářům informace, na základě kterých mohou činit uvážená rozhodnutí.

Cena chyby

V této kapitole jsem obhajoval důkladné prověřování zaměstnanců, ale buďme upřímní — je třeba si přiznat, o co tu skutečně jde. Co se stane, když lidský firewall selže? Jaká je skutečná cena za přijetí podvodného zaměstnance?

Přímé finanční dopady

Ty lze vyčíslit. “Laptop farma“ Christiny Chapmanové vygenerovala 17,1 milionu USD na falešných výplatách. Únik dat ve Spojeném království (NHS Synnovis) stál 22 milionů liber. Polská finanční instituce přišla o 840 000 eur. To jsou doložené případy s jasným finančním dopadem.

Nepřímé ztráty

Často přesahují ty přímé. Krádež duševního vlastnictví nemá cenovku — dokud neuvidíte konkurenta, který půl roku po přijetí vašeho “dodavatele“ spouští produkt s vaším designem. Přístup k síti prodaný ransomwareovým skupinám se neobjeví v účetních výkazech — dokud není celý váš provoz zašifrován a nevyjednáváte o výkupném. Zadní vrátka nainstalovaná skrytými operativci nic nestojí — dokud nejsou využita při útoku, který vyřadí kritickou infrastrukturu.

Regulační postihy

A pak jsou tu regulační rizika. Podle českého zákona o kritické inrastruktuře (ZKI) může nedostatečné prověřování pracovníků KI vést k pokutám až 50 milionů Kč nebo 1,5 % z ročního obratu. Podle GDPR může porušení ochrany osobních údajů stát až 4 % globálního obratu. A v rámci různých sankčních režimů může neúmyslné zaměstnání občanů KLDR znamenat obrovské pokuty a trestní odpovědnost.

Závěr: co si můžete dovolit

Otázka tedy nezní, zda si můžete dovolit důkladné prověřování. Otázka zní, zda si můžete dovolit ho nemít. Komplexní prověrka před nástupem stojí přibližně 200–500 EUR na kandidáta. Průběžné sledování může přidat dalších 50–100 EUR ročně na zaměstnance. Ověřování dodavatelského řetězce se může zdát složité a nákladné — ale ve srovnání s cenou jediného úspěšného proniknutí je návratnost drtivě jednoznačná.

Budování vašeho lidského firewallu

Jak tedy mohou organizace vybudovat efektivní lidský firewall?

Na základě pěti let zkušeností s bojem proti této hrozbě jsem zjistil, že funguje několik zásadních principů:

Investujte do odbornosti, ne jen do technologií

Technologie jsou nezbytné — databáze, ověřovací nástroje, systémy detekce podvodů s podporou umělé inteligence. Ale technologie bez lidské odbornosti představuje pouze drahý druh automatizace. Váš poskytovatel prověřování by měl kombinovat pokročilé nástroje s týmem zkušených analytiků, kteří rozumějí vzorcům hrozeb, dokážou rozpoznat narativní tření a vědí, kdy je třeba eskalovat podezření.

Ve společnosti Scaut výrazně investujeme do školení a vzdělávání analytiků, protože právě lidská vrstva je místem, kde vzniká skutečná hodnota.

Přizpůsobte hloubku prověřování úrovni rizika

Ne každá pozice vyžaduje stejnou míru prověření. Juniorní marketingový koordinátor bez přístupu k systémům potřebuje pouze základní ověření. Seniorní databázový administrátor s přístupem k zákaznickým datům však vyžaduje komplexní screening, zahrnující přímé ověření vzdělání, důkladné prověření zaměstnání a případně i kontrolu finančního pozadí. Pozice v rámci kritické infrastruktury podle zákona ZKI podléhají povinným minimálním standardům. Prověřování založené na úrovni rizika umožňuje efektivní alokaci zdrojů a zároveň zajišťuje odpovídající úroveň ochrany.

Nezapomínejte na externisty a dodavatele

Bezpečnost vaší organizace je tak silná, jak silný je její nejslabší článek — a ten se často nachází právě v dodavatelském řetězci. Stanovte jasné požadavky na prověřování dodavatelů, partnerů a poskytovatelů služeb. Udělejte z ověřování minulosti smluvní povinnost a pravidelně kontrolujte a vymáhejte její dodržování. Dodatečné náklady na rozšíření prověřování do dodavatelského řetězce jsou zanedbatelné ve srovnání s mírou snížení rizika, kterou přinášejí - navíc je můžete smluvně přenést na dodavatele a bez dokladu o screeningu neakceptovat jím dodané pracovníky..

Zaveďte průběžný monitoring tam, kde na tom záleží

Není nutné průběžně sledovat všechny zaměstnance. Ale měli byste monitorovat osoby s privilegovaným přístupem, finanční pravomocí nebo přístupem k citlivým datům. Moderní platformy umožňují tento proces efektivně a s minimálním narušením soukromí. Cílem není dohled, ale včasné varování na základě rizikových faktorů, které vyžadují pozornost.

Podporujte partnerství mezi analytiky a náboráři

Proces prověřování by neměl být černou skříňkou, do které kandidáti vstupují a z níž vychází verdikt. Podporujte dialog mezi analytiky a náborovými týmy. Pokud se objeví pochybnosti, diskutujte je. Pokud je potřeba něco objasnit, umožněte to. Cílem je informované rozhodování, nikoli binární výsledky typu “schválen/odmítnut“.

Držte krok s vývojem hrozeb

Útočníci se neustále přizpůsobují. Podvodné techniky, které fungovaly v roce 2020, se do roku 2026 výrazně vyvinuly. Dokumenty generované umělou inteligencí jsou sofistikovanější, deepfaky dostupnější a interview farmy profesionálnější než kdy dříve. Aktivně sledujte vývoj hrozeb a průběžně aktualizujte metodiky. Statické, neměnné postupy se stávají zastaralými dřív, než si to organizace uvědomí.

Závěrečné zamyšlení: Lidský prvek v digitální hrozbě

Když se ohlížím zpět na ten první případ — na kandidáta, kterého Anna označila, protože “něco na něm nesedělo“ — uvědomuji si, kolik se od té doby změnilo a kolik zůstává stejné. Rozsah hrozby explodoval. Technologie se staly sofistikovanějšími. Regulační požadavky se zpřísnily. Ale základní princip se nezměnil: lidé se brání proti lidem.

Severokorejští operativci, čínští zpravodajci, organizované zločinecké skupiny — to všechno jsou lidé, kteří činí strategická rozhodnutí o tom, jak proniknout do vaší organizace. Studují vaše náborové procesy, hledají slabá místa a vytvářejí přístupy navržené tak, aby je využili. A jedinou skutečně účinnou obranou jsou opět lidé – ti, kteří používají úsudek, zkušenost a intuici k rozpoznání hrozeb, které čistě algoritmické přístupy nikdy nezachytí. Proto nazývám proces prověřování “lidským firewallem“.

Firewally v počítačových sítích pracují podle předem definovaných pravidel: blokují určitý provoz, jiný povolují, vše porovnávají s databází známých hrozeb. Ale lidé čelí hrozbám, které neodpovídají žádným známým vzorcům — novým metodám, sofistikovanému sociálnímu inženýrství, pečlivě vytvořeným falešným identitám, které na první pohled působí zcela legitimně.

Lidský firewall se přizpůsobuje, učí se, rozpoznává vzorce a aplikuje kontextový úsudek. Je to klíčová první linie obrany, která rozhoduje o tom, zda sofistikovaný útočník získá důvěryhodný přístup do vaší organizace, nebo bude zastaven u brány. Je to rozdíl mezi tím, když odhalíte severokorejského operativce během náboru, a tím, když ho odhalíte až po dvou letech, kdy už je hluboko ve vaší infrastruktuře, pracuje na několika projektech a aktivně exfiltruje data.

Organizace investují miliony do kybernetické bezpečnosti — firewally, systémy detekce průniků, ochranu koncových bodů, bezpečnostní operační centra. To všechno jsou nezbytné investice.

Ale pokud neinvestujete obdobně i do lidského firewallu — do robustního prověřování, které spojuje technologii s lidskou expertizou — pak necháváte otevřené hlavní dveře, zatímco pečlivě zajišťujete všechna okna. Útočníci to vědí.

Otázka zní: víte to i vy?

Evropská regulační reakce: směrnice CER a národní implementace

Evropská unie reagovala na rostoucí hrozby vůči kritické infrastruktuře zavedením komplexních regulačních rámců, které výslovně řeší i oblast personální bezpečnosti.

Směrnice Critical Entities Resilience (CER) – (EU) 2022/2557, kterou byly členské státy povinny implementovat do října 2024, stanovuje závazné požadavky na ochranu základních služeb napříč sektory energetiky, dopravy, bankovnictví, finančních trhů, zdravotnictví, zásobování pitnou vodou, nakládání s odpadními vodami, digitální infrastruktury, veřejné správy a vesmírných technologií.

Klíčové požadavky směrnice CER:

Článek 13 směrnice CER výslovně ukládá členským státům povinnost zajistit, aby subjekty kritické infrastruktury přijaly "přiměřená a přiměřeně účinná technická, bezpečnostní a organizační opatření" zajišťující jejich odolnost. To zahrnuje zejména:

1. Bezpečnost prostor a infrastruktury, včetně opatření pro řízení přístupu,
2. Bezpečnost personálu, tedy screeningové a ověřovací postupy,
3. Bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se dodavatelů a poskytovatelů služeb,
4. Postupy hodnocení rizik a schopnost reakce na incidenty,
5. Zajištění kontinuity provozu a řízení krizových situací.

Směrnice výslovně uznává, že personální bezpečnost je klíčovým pilířem odolnosti infrastruktury.

Organizace nemohou zabezpečit své budovy a sítě, pokud zároveň umožňují neprověřeným osobám — včetně podvodných zaměstnanců nebo dodavatelů — přímý přístup k citlivým systémům.

Hrozba falešných IT pracovníků a infiltrovaných dodavatelských řetězců tak přímo podkopává základní cíle směrnice CER: zajistit, aby evropská kritická infrastruktura zůstala funkční, bezpečná a odolná i tváří v tvář moderním hybridním hrozbám.

Česká implementace: Zákon o kritické infrastruktuře (ZKI)

Česká republika implementovala směrnici CER prostřednictvím zákona č. 266/2025 Sb., o kritické infrastruktuře (Zákon o kritické infrastruktuře – ZKI), který vstoupil v platnost 19. srpna 2025. ZKI zavádí komplexní požadavky na personální bezpečnost, které přímo reagují na hrozbu infiltrování provozovatelů kritické infrastruktury podvodnými pracovníky.

Požadavky ZKI na personální bezpečnost:

1. ***Rozsah prověřování:*** Organizace jsou povinny ověřovat spolehlivost (ověření spolehlivosti) všech pracovníků (interních zaměstnanců, dohodářů, externistů, ale i ekvivalentů u svých externích dodavatelů), kteří mají přímý nebo vzdálený přístup k prostorám či systémům kritické infrastruktury. Tento požadavek se tak v minimu týká nejen IT pracovníků, údržbářů, bezpečnostního personálu, ale také poskytovatelů služeb třetích stran, kteří mají přístup k IT systémům např. vzdáleně.
2. ***Minimální standardy prověřování:*** V minimálním rozsahu musí organizace ověřit identitu a trestní bezúhonnost u všech pracovníků. U cizích státních příslušníků, kteří v posledních 3 letech pobývali mimo Českou republiku déle než 3 měsíce, musí prověřování zahrnovat také odpovídající zahraniční výpisy z rejstříku trestů. Rozsah a hloubku prověrky nad rámec minima si dále určuje každá organizace na základě hodnocení rizik dané pozice.
3. ***Kritičtí dodavatelé:*** Ne všichni externí pracovníci podléhají povinnosti prověřování — pouze ti, kteří pocházejí z entit nezbytných pro zajištění základní služby kritické infrastruktury, nebo přistupují do jejích prostor či systémů. Organizace musí pak kritické dodavatele identifikovat a registrovat prostřednictvím procesů hodnocení rizik.
4. ***Povinnost mít dokumentovanou politiku / směrnice:*** Organizace musí vytvořit a zdokumentovat politiku ověřování spolehlivosti, která definuje prověřovací postupy, kritéria, četnost kontrol a požadavky na vedení auditních záznamů.
5. ***Termín implementace:*** Subjekty označené jako provozovatelé kritické infrastruktury musí dokončit prověřování stávajících zaměstnanců a zavést prověřovací procesy pro nové kandidáty i dodavatele nejpozději do 1. března 2026.
6. ***Přísné sankce:*** Porušení povinností stanovených ZKI podléhá významným sankcím — pokutám až 50 milionů Kč (přibližně 2 miliony EUR) nebo 1,5 % ročního obratu, podle toho, která hodnota je vyšší. To představuje zásadní finanční riziko pro organizace, které nezavedou odpovídající personální bezpečnostní opatření..

Soulad s popsanou hrozbou:

Požadavky ZKI přímo reagují na hrozbu podvodných IT pracovníků, která je v této publikaci detailně zdokumentována. Zavedením povinnosti ověření identity a kontroly trestní bezúhonnosti vytváří zákon základní obrannou linii proti operativcům využívajícím falešné nebo syntetické identity.

Požadavek na ověření ekvivalentních zahraničních záznamů u osob, které v nedávné době pobývaly v zahraničí, pomáhá odhalit operativce snažící se využít mezer v mezinárodním ověřování.

Tento prvek reaguje na skutečnost, že mnoho podvodníků střídá rezidence nebo využívá státy s omezeným sdílením informací, aby se vyhnuli detekci. Důraz na bezpečnost dodavatelského řetězce — tedy povinnost ověřovat i kritické externí dodavatele — uzavírá jednu z nejčastěji zneužívaných zranitelností.

Jak bylo popsáno v případové studii č. 8, infiltrace často neprobíhá přímým zaměstnáním, ale prostřednictvím dodavatelských a servisních organizací, které mají přístup k systémům cílové společnosti.

Tím, že ZKI rozšiřuje ověřovací požadavky i na nezbytné třetí strany, snižuje vektor útoku, který mohou protivníci využít. Nejdůležitější je však to, že ZKI zavádí jasnou odpovědnost. Organizace již nemohou tvrdit, že personální bezpečnost je odpovědností někoho jiného.

Díky výslovným právním povinnostem, významným sankcím za neplnění a pevnému termínu implementace musí nyní provozovatelé kritické infrastruktury v České republice chápat ověřování zaměstnanců jako nedílnou součást bezpečnosti, nikoli jako administrativní formalitu.

Tento regulační tlak, v kombinaci s reálně zdokumentovanými případy hrozeb, konečně nutí organizace uznat, že vnitřní hrozba začíná už ve fázi náboru.

Strategie detekce a prevence

Varovné signály během náboru

Organizace mohou odhalit podvodné kandidáty tím, že rozpoznají opakující se vzorce chování a nesrovnalosti.

Níže jsou uvedeny typické red flags, které se objevují během výběrového procesu::

Anomálie při video pohovorech:

- Kamera je trvale nefunkční nebo vypnutá, zatímco mikrofon funguje.
- Problémy s kvalitou obrazu – zamrzající snímky, nesoulad mezi pohybem rtů a zvukem, nepřirozené pohyby obličeje.
- Zvukové pozadí naznačuje prostředí call centra nebo sdílený pracovní prostor.
- Neochota upravit úhel kamery nebo ukázat okolí.
- Oční pohyby nepůsobí přirozeně – kandidát může číst odpovědi z obrazovky.

Anomálie ve vzorcích odpovědí:

- Technické otázky jsou zodpovězeny plynule, ale osobní otázky způsobují váhání nebo zmatek.
- Odpovědi působí naučeně či příliš uhlazeně, bez přirozené spontánnosti.
- Kandidát nedokáže mluvit o konkrétních detailech z minulých projektů.
- Náhlé přerušení hovoru po nečekaných otázkách ohledně lokality nebo identity.
- Obecné fráze při dotazech na motivaci, týmovou spolupráci nebo firemní kulturu.

Problémy v dokumentaci:

- Nesrovnalosti mezi profilem na LinkedInu, životopisem a uvedenými zkušenostmi.
- Obecně znějící jména (např. Mike Smith, Thomas Williams) kombinovaná s neevropským vzhledem.
- Uvedené adresy bydliště se nacházejí v odlehlých nebo neobydlených oblastech.
- Profil na LinkedInu postrádá interakce, připojení nebo aktivitu.
- Požadavek na změnu poštovní adresy ihned po nástupu (často s výmluvou na rodinnou nouzi)

Finanční a logistické varovné signály:

- Preferování platby v kryptoměnách.
- Používání platebních prostředníků jako Ruul.io, Payoneer nebo TransferWise.
- Časté změny bankovních údajů.
- Používání VoIP telefonních čísel místo běžných mobilních operátorů.

Technické metody detekce

Organizace by měly zavést technická kontrolní opatření, která pomohou identifikovat podvodné pracovníky a falešné identity.

Níže uvedené postupy představují osvědčené metody detekce:

Ověřování identity:

- Používejte technologie pro ověřování dokladů k detekci synteticky generovaných identifikačních dokumentů.
- Implementujte biometrické ověřování během nástupu a v pravidelných intervalech.
- U rolí s přístupem k systémům vyžadujte vyšší úroveň ověření totožnosti – např. u náboru na dálku ověření s pomocí digitální identity.
- Ověřujte vzdělání a zaměstnání přímo u konkrétních institucí, nikoli prostřednictvím samotného kandidáta.

Monitorování sítě a zařízení:

- Sledujte IP adresy a geolokaci připojení, abyste odhalili používání VPN nebo proxy serverů.
- Monitorujte instalaci neautorizovaného softwaru pro vzdálený přístup.
- Sledujte připojení pocházející z neočekávaných geografických oblastí.
- Analyzujte vzorce přihlášení a vyhledávejte anomálie — například přihlášení v neobvyklých hodinách nebo tzv. “nemožné cestování“ (připojení z míst, mezi nimiž nelze fyzicky cestovat v daném čase)

Detekce deepfake technologií:

- Požádejte kandidáty, aby během videohovoru mávli rukou před obličejem — deepfaky zde často selhávají.
- Požádejte kandidáta, aby otočil kameru k oknu a popsal, co vidí venku.
- Sledujte nesrovnalosti v osvětlení, nepřirozené pohyby obličeje nebo nesynchronizovaný zvuk.
- Pokud vznikne podezření, nahrávejte pohovor pro pozdější forenzní analýzu.

Behaviorální analýza:

- Pokládejte nečekané osobní otázky, které nejsou součástí technického scénáře.
- Vyžadujte konkrétní příklady práce s detailním popisem úkolů a prostředí.
- Upřednostňujte živá testovací cvičení (např. kódování) před zadáváním úkolů "na doma".
- Porovnávejte výkon při pohovoru s výkonem po nástupu – může odhalit, že za zaměstnance pracuje jiná osoba.

Doporučené postupy dle FBI

Pokyny FBI z července 2025 obsahují konkrétní doporučení, jak zabránit náboru podvodných IT pracovníků a identifikovat falešné identity:

- Pečlivě kontrolujte identifikační dokumenty – všímejte si překlepů, nesrovnalostí a ověřujte údaje napříč sociálními sítěmi, portfoliovými weby a platebními platformami.
- Ověřujte předchozí zaměstnání a vzdělání přímo u firem a institucí, nikoli prostřednictvím kontaktů, které poskytne kandidát.
- Upřednostňujte osobní setkání vždy, když je to možné; při vzdálených pohovorech vyžadujte video s nezakrytým pozadím.
- Pořizujte snímky z pohovoru a využívejte je při budoucích setkáních pro porovnání – umožní to odhalit případnou záměnu osob.
- Analyzujte platební účty všech zaměstnanců, sledujte shodné bankovní údaje.
- Zasílejte pracovní vybavení pouze na adresy uvedené v identifikačních dokladech; každou žádost o změnu adresy ověřujte dodatečně.
- Nepřidělujte přístup do systémů, dokud není zcela dokončen screening.
- Školte externí poskytovatele IT služeb o těchto typech hrozeb.

Strategická doporučení

Pro jednotlivé organizace

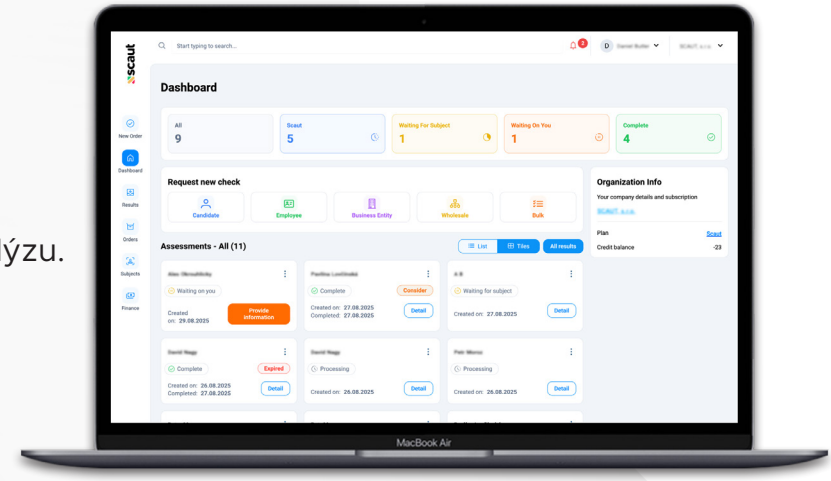
Stanovte jasnou odpovědnost a kompetence

Přiřaďte odpovědnost za prevenci pracovních podvodů konkrétnímu týmu – ideálně mezioborové skupině zahrnující HR, IT bezpečnost, právní oddělení a compliance
Zaveďte formální politiky, které vyžadují bezpečnostní prověření pro všechny pozice s přístupem k citlivým systémům nebo datům.

1. ***Zaveďte vícestupňové ověřování identity***
   Implementujte komplexní prověřovací proces, který zahrnuje: ověřování dokumentů, přímé potvrzení pracovních a vzdělávacích záznamů, ověřování s digitální identitou, a průběžný monitoring rizik.

2. ***Vyžadujte osobní ověření u klíčových pozic***
   U rolí s přístupem k provozním systémům, zákaznickým datům nebo kritické infrastruktuře vyžadujte alespoň jedno osobní setkání. Pokud to není možné kvůli geografické vzdálenosti, využijte důvěryhodné lokální partnery k ověření identity kandidáta.

3. ***Zlepšete postupy při pohovorech***
   Školte náboráře a manažery, aby uměli rozpoznat varovné signály. Vyžadujte video pohovor u všech vzdálených kandidátů. Pokládejte nečekané osobní otázky, které nesouvisejí přímo s technickými dovednostmi. Požádejte o kontext prostředí (např. otočit kameru k oknu, popsat okolí). Nahrávejte a archivujte pohovory pro případnou forenzní analýzu.



4. ***Zavedťe robustní technické kontroly***
   Monitorujte přístup do sítě kvůli: neautorizovanému použití VPN, neobvyklým geografickým připojením, nebo používání podezřelého softwaru pro vzdálený přístup. Implementujte řízení zařízení (device management), které zabrání instalaci neautorizovaných aplikací. Sledujte vzorce přihlašování a analyzujte anomálie.

5. ***Prověřujte dodavatele a externí partnery***
   Pokud využíváte personální agentury nebo outsourcujete např. vývojové týmy, provádějte due diligence jejich screeingových procesů. Zahrňte požadavky na prevenci podvodů do smluvních podmínek. Pravidelně provádějte audity ověřování identity a dalších faktorů u dodavatelů. Nespoléhejte na čestná prohlášení!

6. ***Zavedťe monitorování po nástupu***
   Během prvních týdnů po nástupu proveďte bezpečnostní přezkum. Periodicky znovu ověřujte identitu zaměstnance. Sledujte známky vícenásobného zaměstnání (nekonzistentní dostupnost, pokles kvality práce, neobvyklé pracovní hodiny).

scaut

Scaut.com: váš partner pro bezpečný nábor

Jako unikátní SaaS platforma pro screening a monitoring pracovníků ve střední Evropě nabízí Scaut nástroje pro ověřování kandidátů a sledování zaměstnanců v souladu s GDPR. S možností nepřeberného množství customizací, vlastních workflows, řízení dle vlastních pravidel, a napojení vlastních databází.

Naše platforma spojuje automatizaci s odborností analytiků, aby zajistila přesné a spolehlivé ověření, navržené přímo pro detekci a prevenci sofistikovaných infiltračních hrozeb, popsaných v této publikaci.

Řešení

Scaut je online platforma pro screening zaměstnanců a externích pracovníků / dodavatelů.

Umožňuje firmám i jejich dodavatelským řetězcům budovat důvěryhodnou pracovní sílu a plnit požadavky legislativ v oblasti kybernetické bezpečnosti a kritické infrastruktury, včetně NIS2, směrnice CER, českého zákona ZKI, ISO 27001, DORA, SOC 2 a dalších.

Platformu lze nastavit během několika hodin, nikoliv týdnů – a můžete se na ní zcela spolehnout.

Naše řešení přinášejí:

1. ***Úsporu nákladů a bezpečnost:*** Postaráme se o složitost i compliance. Provádějte veškeré screeningy pracovníků a firem na jednom místě – bez rizika úniku dat. Garantujeme procesy v souladu s GDPR a jsme certifikováni dle ISO 27001.
2. ***Ověřenou pracovní sílu:*** Prověřování před nástupem, monitorování zaměstnanců, KYC kontroly, bezpečnostní prověrky nebo ověřování identity – dokážeme ověřit vše. Naše nástroje odhalují dokumenty generované umělou inteligencí, falešné identity i vzorce “interview farem“.
3. ***Auditní jistotu:*** Zůstaňte v souladu s předpisy a dokažte, že děláte vše pro ochranu svého odvětví. Naše interní reporty a řízení přístupových rolí vás udrží v souladu s požadavky ZKI, NIS2, CER a dalších regulačních rámců.
4. ***Komplexní řešení:*** Platforma Scaut spojuje sílu SaaS konektivity a automatizace s odborností našich lidských analytiků. Zahrnuje vše — od forenzní analýzy dokumentů až po behaviorální analýzu.

Platforma

1. ***Moderní uživatelské rozhraní:*** Intuitivní design zjednodušuje správu procesů pro HR týmy a bezpečnostní manažery. Uživatelské prostředí umožňuje efektivní práci,

rychlou orientaci a snadnou kontrolu všech kroků prověřování.

2. ***Automatizované kontroly:*** Naše ověřovací procesy šetří čas a poskytují okamžité informace, kde jsou dostupné — včetně automatického screeningu sankčních seznamů a ověřování identifikačních dokumentů v reálném čase.
3. ***Integrace s HRIS a ATS systémů***: Díky otevřenému API lze platformu Scaut snadno propojit s náborovými a personálními systémy (HRIS, ATS), což zajišťuje plynulý tok dat a přehledný náborový proces.
4. ***Průběžný monitoring:*** Zajišťuje nepřetržitou bezpečnost zaměstnanců, partnerů i dodavatelů – klíčové pro včasnou detekci hrozeb po nástupu do zaměstnání a pro splnění regulatorních požadavků.
5. ***Škálovatelný systém:*** Platforma je vhodná pro firmy všech velikostí – od startupů po velké podniky. Nabízíme modely od platby za jednotlivé prověrky až po komplexní předplatné s rozšířenými funkcemi.
6. ***Špičkové technologie:*** Neustále integrujeme forenzní a analytické nástroje, včetně detekce deepfake videí, geolokační analýzy IP adres a ověřování pravosti dokumentů. Díky tomu poskytujeme nejpřesnější a nejspolehlivější prověřování na trhu

Bezpečnost dodavatelského řetězce

Můžete si dovolit nevědět nic o lidech ve svých dodavatelských řetězcích? Dochází k neobvyklé aktivitě mezi vašimi vzdálenými IT pracovníky? Co vlastně víte o zaměstnancích třetích stran, se kterými spolupracujete? Zajištění bezpečnosti se netýká jen vašich interních zaměstnanců. Je nezbytné prověřovat také dodavatele, obchodní partnery a všechny společnosti, které tvoří váš dodavatelský ekosystém.

Jste před těmito riziky chráněni?

1. ***Bezpečnostní hrozby:*** Bez důkladných prověrek se do vašeho dodavatelského řetězce mohou infiltrovat osoby s kriminální minulostí nebo vazbami na škodlivé entity. Důsledkem může být krádež, sabotáž či neoprávněný přístup k citlivým informacím.
2. ***Provozní narušení:*** V oblastech, kde záleží na kontinuitě – například při práci s rychle se kazícím zbožím nebo v just-in-time výrobě – mohou i drobné výpadky způsobit řetězový kolaps celé dodavatelské sítě.
3. ***Porušení předpisů:*** Zaměstnávání osob bez platného pracovního oprávnění nebo s historií regulačních porušení může vystavit firmu vysokým právním rizikům.
4. ***Vnitřní hrozby:*** Zaměstnanci se zlými úmysly mohou zneužít přístupová oprávnění k úniku důvěrných dat, manipulaci s procesy nebo ke spolupráci s konkurencí či nepřátelskými státními aktéry.

5. ***Poškození reputace:*** Ať už jde o únik dat, stažení produktu nebo regulační sankci, následky zaměstnání neprověřených osob mohou být dlouhodobé a ničivé pro pověst firmy.

Organizace, které investují do řízení rizik spojených s lidmi – například prostřednictvím prověřování a monitorování pracovní síly – prokazatelně zaznamenávají nižší ztráty a rychlejší odhalování podvodů. Vyžadujte proto komplexní prověřovací proces pro všechny osoby v rámci svého dodavatelského řetězce, včetně background checků a průběžného monitorování. Promluvte si se Scautem ještě dnes.

Spojte se s námi - proč Scaut

Řídíme vaše náborová rizika na globální úrovni. Naším cílem je pomáhat organizacím všech velikostí najímat důvěryhodné kandidáty i dodavatele a zároveň splňovat legislativní a bezpečnostní požadavky – to vše v rámci jednoduché, škálovatelné digitální platformy. Se Scautem získáte:

1. Rychlé výsledky prověření ve velkém měřítku
2. Špičkové technologie včetně detekce umělé inteligence
3. Soulad s předpisy NIS2, CER, SOC2, českým ZKI a ISO 27001
4. Bezpečné ověřování pracovní síly v dodavatelském řetězci
5. Měřitelnou due diligence při náboru
6. Komplexní ověřování klíčových ukazatelů na jednom místě
7. Přizpůsobené screeningové řešení podle potřeb organizace
8. Vyšší kvalitu a efektivitu týmů
9. Žádná zbytečná administrativa a papírování
10. Globální pokrytí screeningových potřeb
11. Okamžité ověření tam, kde je dostupné

Prověřování zaměstnanců je klíčové pro úspěch vaší organizace. Najímejte spolehlivé lidi, snižujte ztráty a zvyšujte produktivitu..

Navštivte https://www.scaut.com nebo kontaktujte náš tým a probereme, jak může Scaut přispět k bezpečnosti vašeho náboru.

scaut

Zdroje a citace

Tato publikace vychází ze syntézy informací z důvěryhodných a ověřených zdrojů, včetně vládních institucí, bezpečnostních agentur, výzkumných organizací, firem z oblasti kybernetické bezpečnosti a z přímých provozních zkušeností společnosti Scaut Všechny uvedené statistiky, případové studie a zpravodajské poznatky o hrozbách byly převzaty nebo odvozeny z následujících dokumentovaných zdrojů:

Vládní a bezpečnostní zdroje

1. ***U.S. Department of Justice:*** "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote IT Worker Fraud." Available at: https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote
2. ***DOJ - Chapman Case:*** "Arizona Woman Sentenced for $17M Information Technology Worker Fraud Scheme." Available at: https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue
3. ***DOJ US Attorney's Office:*** "Arizona Woman Sentenced in $17M IT Worker Fraud Scheme That Illegally Generated Revenue for North Korea." Available at: https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north

Firmy z oblasti kybernetické bezpečnosti a zpravodajství o hrozbách

1. ***Microsoft Security:*** "Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations." Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/
2. ***CrowdStrike (Fortune):*** "North Korean operatives have infiltrated hundreds of Fortune 500 companies." Available at: https://cyberscoop.com/north-korea-workers-infiltrate-fortune-500/
3. ***Okta Threat Intelligence:*** "North Korea's IT Workers expand beyond US big tech." Okta Newsroom. Available at: https://www.okta.com/newsroom/articles/north-korea-s-it-workers-expand-beyond-us-big-tech/
4. ***DTEX Systems:*** "Exposing DPRK: Nation-State Threat Actors." Available at: https://www.dtexsystems.com/exposing-dprk/
5. ***Palo Alto Networks Unit 42:*** "Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation." Available at: https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/

scaut

Průmyslový výzkum a analýzy

1. ***Gartner Research:*** "Gartner Survey Shows Just 26% of Job Applicants Trust AI Will Fairly Evaluate Them." Press release, July 31, 2025. Available at: https://www.gartner.com/en/newsroom/press-releases/2025-07-31-gartner-survey-shows-just-26-percent-of-job-applicants-trust-ai-will-fairly-evaluate-them
2. ***HR Dive:*** "By 2028, 1 in 4 candidate profiles will be fake, Gartner predicts." Available at: https://www.hrdive.com/news/fake-job-candidates-ai/757126/
3. ***Fortune:*** "North Korean IT worker infiltrations exploded 220% over the past 12 months." August 4, 2025. Available at: https://fortune.com/2025/08/04/north-korean-it-worker-infiltrations-exploded/
4. ***Crowell & Moring:*** "From Deepfakes to Sanctions Violations: The Rise of North Korean Remote IT Worker Schemes." Available at: https://www.crowell.com/en/insights/client-alerts/from-deepfakes-to-sanctions-violations-the-rise-of-north-korean-remote-it-worker-schemes
5. ***Fordham University:*** "America's Best Remote Workers Might Be North Korean." Fordham Now. Available at: https://now.fordham.edu/university-news/americas-best-remote-workers-might-be-north-korean/
6. ***Becker's Hospital Review:*** "North Korean IT workers targeting healthcare jobs—85 interviews detected in 2025." Available at: https://www.beckershospitalreview.com/healthcare-information-technology/north-korean-it-workers-targeting-healthcare-jobs-report/

Zpravodajství a investigativní žurnalistika

1. ***CNN Interactive:*** "How North Korean IT workers leverage AI and vulnerable Americans to infiltrate US companies." August 5, 2025. Available at: https://www.cnn.com/interactive/2025/08/05/world/north-korea-it-worker-scheme-vis-intl-hnk/index.html
2. ***Wired:*** "Leak Reveals the Workaday Lives of North Korean IT Scammers." Available at: https://www.wired.com/story/leaked-data-reveals-the-workaday-lives-of-north-korean-it-scammers/
3. ***CyberScoop - Okta Report:*** "North Korea IT worker scheme swells beyond US companies." Available at: https://cyberscoop.com/north-korea-it-worker-global-scheme-okta/
4. ***The Record:*** "North Korea IT worker scheme expanding to more industries beyond tech." Available at: https://therecord.media/north-korea-it-worker-scheme-expands-outisde-us-tech

Poznámka k metodologii: Tato bílá kniha kombinuje informace z více ověřených a autoritativních zdrojů, aby poskytla komplexní hodnocení současných hrozeb. Všude tam, kde jsou v textu uvedeny konkrétní statistiky nebo tvrzení, vycházejí z výše uvedených zdrojů. Všechny případové studie jsou založeny buď na veřejně zdokumentovaných incidentech, nebo na přímých provozních zkušenostech společnosti Scaut.com z oblasti prověřování pracovníků. Odkazy a URL adresy byly ověřeny jako aktivní k 11. listopadu 2025.

Pro nejaktuálnější zpravodajství o hrozbách a nové poznatky o infiltračních kampaních severokorejských IT pracovníků doporučujeme sledovat: FBI Internet Crime Complaint Center (IC3) – aktuální varování a doporučení pro organizace, CISA Cybersecurity Alerts – bezpečnostní upozornění a pokyny k mitigaci rizik, ENISA Threat Landscape Reports – evropské analýzy kybernetických hrozeb a trendů.

Společnost Scaut.com zároveň pravidelně aktualizuje blog zaměřený na evropský kontext personální bezpečnosti a hrozbovou analytiku: https://scaut.com/blog

scaut

Závěr: Naléhavost okamžité akce

Neviditelná pracovní síla už je tady. Sofistikovaní operativci, podporovaní státy, již pronikli do tisíců organizací po celém světě, vydělávají stovky milionů dolarů na nelegálních příjmech, zatímco současně kradou duševní vlastnictví, instalují malware a připravují půdu pro budoucí kybernetické útoky.

Toto není hypotetická hrozba ani vzdálené varování.Děje se to právě teď, ve velkém rozsahu — a s znepokojivě vysokou úspěšností. Technologie, které tyto operace umožňují — deepfaky, AI generování identit, šifrovaná komunikace — se vyvíjejí rychleji než obranná opatření. To, co ještě před dvěma lety vyžadovalo odborníky a drahé vybavení, lze dnes provést během jediné hodiny pomocí běžných nástrojů.

Nejznepokojivější je zneužití důvěry. Organizace si vybudovaly celé kultury vzdálené práce na předpokladu, že lidé jsou tím, za koho se vydávají. Videohovory, digitální dokumenty a online pohovory nahradily osobní ověření. Tato efektivita však vytvořila nové zranitelnosti – otevřené dveře pro ty, kteří je dokážou využít.

Evropa čelí v tomto směru zvláštnímu riziku. Roztříštěné regulační prostředí, byrokratická složitost a chybějící centralizované povědomí o hrozbách vytvářejí prostor pro protivníky Zatímco Spojené státy těží z koordinovaných varování FBI a společné reakce bezpečnostních složek, mnoho evropských organizací si ani neuvědomuje, že hrozba existuje.

Řešení vyžaduje akci na více úrovních:

Cena nečinnosti mnohonásobně převyšuje náklady na prevenci. Jediná úspěšná infiltrace může vést k milionovým ztrátám na duševním vlastnictví, k regulačním pokutám a nevratnému poškození reputace. Průměrná ztráta při úniku dat typu “ChapmanCost“ činí 4,88 milionu dolarů. V případě krádeže IP nebo útoku ransomwarem mohou být důsledky katastrofální. Co je však nejdůležitější — tato hrozba přímo souvisí s národní bezpečností. Příjmy z těchto operací financují vývoj zbraní, obcházení sankcí a destabilizační kampaně. Každé podvodné zaměstnání poskytuje protivníkům strategické informace o západní korporátní infrastruktuře. Někteří z těchto operativců dnes působí přímo na ruské frontě na Ukrajině — vycvičení kybernetičtí bojovníci, kteří dříve infiltrací pronikli do firem z žebříčku Fortune 500.

Neviditelná pracovní síla představuje jasné a bezprostřední nebezpečí.

Prvním krokem obrany je rozpoznání hrozby.
Následovat musí okamžitá akce.

scaut

O této zprávě

Tato publikace byla vytvořena s cílem zvýšit povědomí o zásadní a rychle se vyvíjející kybernetické hrozbě, které čelí organizace po celém světě. Výzkum v ní obsažený syntetizuje informace z více autoritativních zdrojů, mimo jiné z:

- Federal Bureau of Investigation (FBI) public service announcements and Internet Crime Complaint Center advisories
- Google Threat Intelligence Group (Mandiant) analysis and reporting
- Unit 42 threat research from Palo Alto Networks
- CrowdStrike Counter Adversary Operations investigations
- Okta Threat Intelligence assessments
- DTEX Systems Insider Intelligence and Investigations analysis
- European Union Agency for Cybersecurity (ENISA) reporting
- Případové studie odborníků na kybernetickou bezpečnost a firem provádějících prověřování pracovníků
- Soudní dokumenty a záznamy orgánů činných v trestním řízení, včetně případu tzv. Chapman laptop farm prosecutions

Tento dokument je určen pro:

- CISOs a vedoucí pracovníky v oblasti kybernetické bezpečnosti
- Ředitele HR a náborové týmy
- Výkonné vedení a členy představenstev odpovědné za řízení podnikových rizik
- Odborníky na background screening a ověřování identity
- Právní a compliance oddělení, která řeší regulatorní požadavky
- Vládní a politické činitele podílející se na tvorbě strategií kybernetické obrany

Pro dotazy, doplňující informace nebo diskusi o tom, jak může prověřování pracovníků pomoci snížit tato rizika, se obraťte na své bezpečnostní a compliance týmy, nebo konzultujte se specializovanými poskytovateli ověřovacích služeb.

Scaut s.r.o., listopad 2025

scaut

Nový Zákon o kritické infrastuktuře (ZKI)

Je vaše organizace připravena splnit požadavky personální bezpečnosti?

Splňte povinnosti dle
ZKI, **nZoKB**, **DORA**, **ISO 27001** a dalších!

Ověření spolehlivosti dle ZKI

Zákon o kritické infrastruktuře (ZKI) 266/2025 Sb. vstoupil v účinnost 19.8.2025, a mimo jiné vyžaduje ověřování spolehlivosti interních i externích pracovníků.

U koho je třeba ověřit spolehlivost?

Interních a externích pracovníků s přímým nebo vzdáleným přístupem do prostor, či systémů KI.

Všech externích pracovníků?

Pracovníků subjektů nezbytných pro zajištění základní služby KI. Kritické dodavatele je třeba řádně identifikovat a evidovat.

Co je ověření spolehlivosti?

Minimálně se jedná o ověření totožnosti a trestní bezúhonnosti. U cizinců i zahraniční ekvivalenty, pokud pobývali v cizině déle než 3 měsíce v posledních 3 letech. Další rozsah stanoví subjekt na základě posouzení rizik.

Lhůta pro splnění povinností

Splnění požadavků u stávajících pracovníků a zahájení screeningu kandidátů a dodavatelů je třeba bezodkladně po zařazení do KI – tedy nejpozději 1.3.2026.

Za porušení povinností podle ZKI hrozí sankce až 50 milionů Kč nebo 1,5 % obratu v pokutách!

Ověřte svou připravenost

1. Identifikovali jste kritické pracovníky a dodavatele?
   ☐ Ano ☐ Ne ☐ Pracujeme na tom
2. Provádíte již screening zaměstnanců a externích pracovníků?
   ☐ Ano ☐ Ne ☐ Částečně
3. Máte zavedenou dokumentovanou politiku ověřování spolehlivosti?
   ☐ Ano ☐ Ne ☐ Ještě ne
4. Jsou záznamy o screeningu a auditní záznamy bezpečně uloženy?
   ☐ Ano ☐ Ne ☐ Nevím
5. Budete nejpozději do 1. března 2026 splňovat provozní požadavky ZKI?
   ☐ Ano ☐ Ne ☐ Nevím

Pokud jste odpověděli “Ne” nebo “Ještě ne”, je čas jednat.

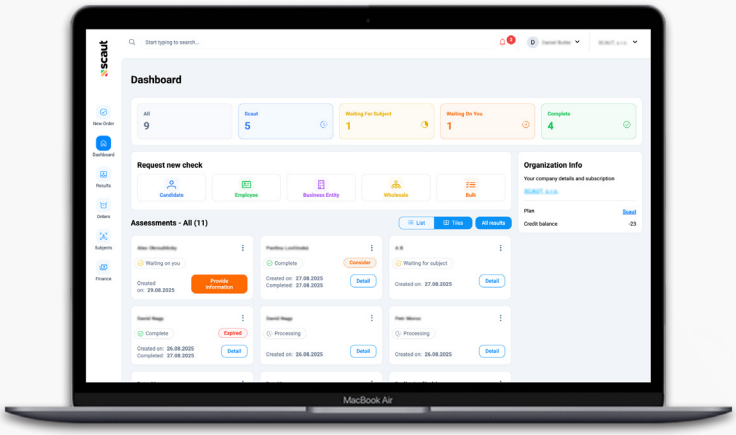
Ověření spolehlivosti bezpečně a v souladu s předpisy.
Kontaktujte Scaut ještě dnes!

scaut.com

scaut

Prověřování zaměstnanců a dodavatelů od podzimu 2025: splňte zákon a získejte náskok.

Od podzimu 2025 musí organizace kritické infrastruktury a jejich dodavatelé systematicky prověřovat pracovníky. Scaut to řeší automatizovaně – sbírá a vyhodnocuje data online, výsledky doručí během minut. Splníte zákonné požadavky a získáte konkurenční výhodu.



Benefity využití Scaut:

- **Automatizované ověření**
  Výsledky automatizovaných kontrol jsou doručeny během pár minut.
- **Auditní stopa**
  Veškeré kontroly a přístupy jsou logovány, dokládají auditní stopu, umožňují export dat a doložení souhlasu pracovníka.
- **Přehled na jednom místě**
  o zaměstnancích, kontraktorech a pracovnících vašich dodavatelů. Včetně sdílení reportů.

Hledáte podporu při plnění legislativních povinností?

I když se to může zdát jako velký krok, jsme tu pro vás – ať už potřebujete poradit s rozsahem kontrol nebo si promluvit o tom, jak implementovat screening do vaší organizace.

Sady balíčků pro ověření až 10 000 osob

(vhodné pro potřeby kritické infrastruktury)

	Počet kontrol	Kreditů za kontrolu
M	1,000	8
L	5,000	7
XL	10,000	6

Co kontrola zahrnuje:

- Ověření totožnosti
- Ověření trestní bezúhonnosti

Poznámka:

1. Každá další kontrola nad rámec sady bude zpoplatněna částkou 14 kreditů za kontrolu.
2. Platby v platformě jsou v kreditech. 1 kredit = €1
3. Sady balíčků a Speciální balíčky jsou dostupné pouze uživatelům s předplatným Business a výše.

Začněte ověřovat pracovníky ještě dnes.
Kontaktujte Scaut a získejte náskok před konkurencí.

scaut.com

Integrita je základ.