scaut

Rizika

Zaměstnáváte lidi, o kterých nic nevíte?

Pro zajištění souladu s předpisy a bezpečnosti při najímání zaměstnanců existuje mnoho důvodů. Děláte dost pro řízení rizik, kterým vaše firma čelí?

Jste chráněni před těmito riziky?

Nedodržování předpisů

S regulačními požadavky EU a členských států na zabezpečení kritické infrastruktury (NIS 2, CER a další) se zvyšuje povinnost mít prověřenou pracovní sílu.

Ochrana dodavatelského řetězce

Práce na dálku umožňuje lidem s nekalými úmysly lehce vytvořit falešnou identitu a připojit se k vašemu týmu. Dodavatelský řetězec je často využíván při kybernetické kriminalitě.

Krádeže identity

Nepoctiví zaměstnanci mohou zneužít osobní údaje kolegů nebo klientů k vlastnímu obohacení nebo jiným nezákonným činnostem.

Krádeže dat

Neoprávněný přístup k firemním datům může vést k jejich krádeži, což ohrožuje soukromí klientů a obchodní tajemství společnosti.

Finanční kriminalita

Finanční podvod může společnostem způsobit obrovské finanční ztráty, od odklonění plateb až po zpronevěru majetku.

Poškození reputace

Zaměstnání nesprávné osoby může způsobit značné ztráty finančního kapitálu, sociálního kapitálu a/nebo podílu na trhu.

Jen v Británii byl účet za zaměstnanecké podvody v roce 2023 ve výši 24 mld. liber

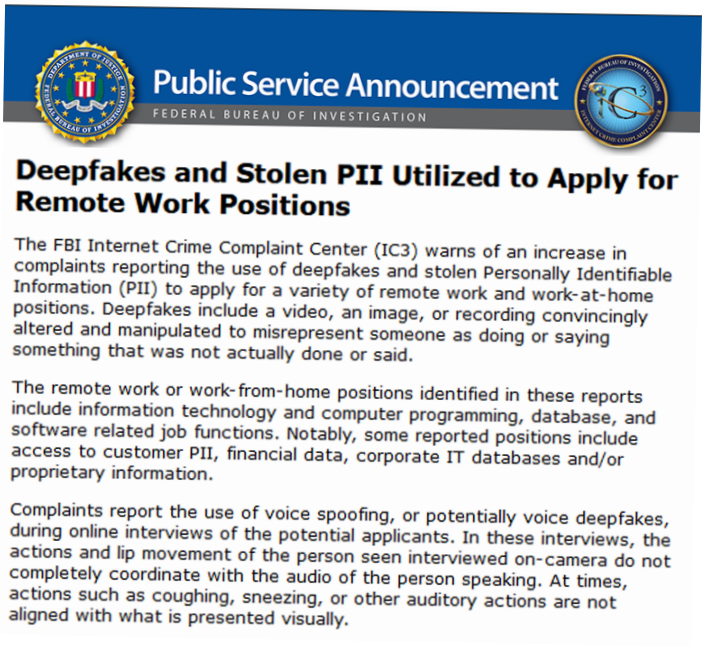
Asociace certifikovaných vyšetřovatelů podvodů (Association of Certified Fraud Examiners) odhaduje, že **organizace přicházejí o přibližně 5 % svých ročních příjmů** v důsledku podvodů, přičemž značná část z nich připadá je **páchána zaměstnanci.**

Organizace, které investují do kontroly lidí, jako je screening, zaznamenávají menší ztráty a rychleji odhalují podvody**. Kontaktujte Scaut ještě dnes.**

Číňané pronikají do českých firem. Startupy narážejí na falešné ajťáky“

České startupy a firmy podnikající v informačních technologiích najímají zaměstnance na práci z domova. Když si však několik z nich důsledně proklepli, zjistilo se, že zájemci o práci předložili falešné evropské doklady a ve skutečnosti jde o Číňany. Jednou z verzí je průmyslová nebo vojenská špionáž.

To byl i případ jednoho z českých technologických startupů, s nímž se MF DNES seznámila (vzhledem k citlivosti případu jméno firmy redakce neuvádí). Do výběrového řízení se jí přes sociálně-profesní síť LinkedIn přihlásil zájemce o práci developera. Podle dokladů, které firmě poskytl, mělo jít o občana Dánska, který žije v Estonsku. Úspěšně prošel několika koly přijímacího řízení, která prověřovala jeho programátorské schopnosti. Jenže údaje uvedené v jeho cestovním pasu byly firmě podezřelé. A tak se rozhodla programátora důkladně prověřit.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

“Když jsme šli po stopě toho linkedinového profilu, zjistili jsme, že je provázaný s dalšími. Všechny mají společné znaky, snaží se působit tak, že ti lidé jsou absolventy evropských univerzit a většinou pracují delší dobu na dálku, například ze Srbska nebo Estonska,“ popisuje Petr Moroz ze společnosti Scaut, která pro zmíněnou společnost kandidáty na pracovní pozici prověřovala.

Klubko stovek linkedinových profilů se pak sbíhá do dvoumilionového čínského města Dandong nedaleko hranice mezi Čínou a Severní Koreou. V tomto městě je mimo jiné základna čínské armády.

Že mohou za aktivitami “falešných ajťáků“ být přímo čínské tajné služby, je pouze jedna z teorií. Největší tuzemská tajná služba, kontrarozvědka BIS, však před čínskými aktivitami na území Česka dlouhodobě varuje.

Zjistěte více o ochraně své společnosti. Kontaktujte Scaut ještě dnes.

source: excerpt from scaut.com/blog