Umělá inteligence přidělá CSO další vrásky

Je řada profesí, které se obávají, že jim umělá inteligence vezme práci. Jsou profese, které se na umělou inteligenci těší. Patrně žádný CSO se nezařadí ani do jedné z těchto skupin. Umělá inteligence se v brzké době stane součástí systémů napříč všemi odvětvími. Velké změny se týkají průmyslové výroby, dopravy, bankovnictví, IT, služeb.

MIROSLAV NEČAS

Společně s dalšími přelomovými technologiemi, zejména IoT a sítěmi 5. generace, umělá inteligence významně ovlivní podnikání i chování domácností. Ani zločin již nebude stejný. Ostatně, lidé, kteří se živí nekalým způsobem bývají ti první, kteří se na změny dokáží adaptovat. Vzpomeňme na léta ekonomické transformace.

Nové způsoby útoků na AI

Umělá inteligence přináší vedle nesporných výhod i zcela nové druhy zranitelností. Algoritmy založené na strojovém učení jsou do jisté míry černou schránkou. Ve srovnání se softwary, které známe nyní, je daleko složitější identifikovat a eliminovat jejich zranitelnosti. Ke slovu přicházejí nové vektory útoků. Například otevření biometrického zámku přiložením specifického symbolu, či zmatení systému autonomního vozidla pomocí samolepky na dopravní značce. Čím méně budeme rozumět principům fungování zařízení, která používáme, tím budeme zranitelnější.

Nekontrolované gigaflopy v síti

Dnešní chytré senzory obsahují procesory s výkonem v řádu GFLOPS. Třeba minipočítač Raspberry Pi 4 svým výkonem 13,5 GFLOPS překonává nejvýkonnější superpočítače z 90. let. Senzorů a chytrých zařízení bude v sítích přibývat a jejich výkon bude dále narůstat. V současné době si jen těžko lze představit, jakým způsobem budeme tato zařízení v sítích evidovat, natož centrálně spravovat a aktualizovat, abychom dokázali eliminovat rizika spojená se zneužitím tohoto výpočetního výkonu.

Mlhavý perimetr

Chytrá mobilní zařízení, connected cars, bezdrátové senzory, vysokokapacitní 5G sítě… To vše povede k narušení perimetru tak, jak ho známe nyní. Bude stále složitější oddělit chráněné oblasti od okolního světa.

Autor Miroslav Nečas, Business Development Manager TOVEK

To bude znamenat vyšší nároky na odolnost používaných zařízení i na schopnost sledovat provoz a rozpoznávat chybové stavy. V tom naopak může umělá inteligence pomoci.

Pro zajištění bezpečnosti je nezbytná spolupráce napříč organizací

Nové způsoby útoků, chytrá zařízení a rozmělnění perimetru kladou vysoké nároky na širší spolupráci v oblasti bezpečnosti. Je potřeba posilovat výměnu informací mezi CSO a informatiky, ekonomy, techniky a dalšími specialisty. To nelze bez názorné prezentace informací v souvislostech. Společný obraz situace pomáhá nalézt společnou řeč lidem z různých profesí a různého zaměření. Vizuální prezentace rizik jim umožní uvědomit si klíčové skutečnosti a vztahy a kvalifikovaně o nich diskutovat. Ve společnosti TOVEK se zabýváme využitím analytických nástrojů v oblasti bezpečnosti již více než 26 let. Postupně jsme pokročili od analýzy textů a strukturovaných dat k analýzám komunikace včetně hlasu či obrazu. Po celou jsou naše nástroje využívány na vrcholové úrovni, kde je potřeba dávat do kontextu informace z různých zdrojů do ucelených pohledů.

Celostní přístup k bezpečnosti

Naše dlouholeté zkušenosti ukazují, že je nutné přistupovat k bezpečnosti komplexně. Dnes to platí ještě více než kdy dříve. Není možné oddělit bezpečnost kybernetickou od bezpečnosti fyzické. Je potřeba zvažovat bezpečnostní rizika spojená s vlastními zaměstnanci, dodavatelským řetězcem a zákazníky v kontextu celkové ekonomické situace na trhu. Pominout samozřejmě nelze ani aktivity konkurence či různých zájmových skupin. Právě k tomu slouží systém ARMS. Umožňuje zpracovávat data z fyzické i digitální infrastruktury a srozumitelně je prezentovat různým odborníkům v kontextu klíčových cílů či procesů organizace. Vizuální prezentace dat podporuje účinnou spolupráci napříč organizací a umožňuje řídit bezpečnost komplexně.