2.11.2024.

Moćan saveznik u urbanoj sigurnosti - njegovo veličanstvo videonadzor!

Časopis Zaštita je godinama provodio istraživanja bazirana na podacima MUP- a o tome koji su gradovi iznad 20 000 stanovnika u Hrvatskoj najsigurniji. Rezultatima nisu svi bili zadovoljni, pogotovo čelnici gradova koji bi se našli na dnu liste. Rekli da da ankete zorno pokazuju da se građani osjećaju sigirno u tim gradovima, da je statistika varljiva jer veći postotak kaznenih djela ustvari znači da policija bolje obavlja posao jer je više počinitelja kaznenih djela otkriveno no u nekim drugim sredinama. Stoga je pitanje je li sigurnost gradova stvar subjektivne percepcije njegovih stanovnika ili se ipak u obzir uzimaju rizici poput vandalizma, narušavanja javnog reda i mira, kaznenih djela protiv ljudi i imovine, prometnih nesreća, požara, terorizma...

Već samo postojanje kamera smanjuje broj kriminalnih djela

U pokušaju da se preveniraju određena kaznena djela te da se stvaraju što sigurniji gradovi, posljednjih je godina moćan saveznik gradskim upravama - videonadzor. No, što ustvari njime štitimo i zašto? Krenimo redom, videonadzor je idealno rješenje za nadzor prometa jer može utjecati na smanjenje gužvi u gradu, sprječavanje nesreća, ali i kažnjavanje prekršaja. Tu je i dodatna korist od kontrole i organizacije javnog prijevoza i parkiranja. Videonadzor se pokazao učinkovitim i u zaštiti javne imovine i procesuiranju vandalizma i remećenja javnog reda i mira, ali i u nadzoru i zaštiti osjetljivih lokacija kao što su škole, vrtići ili pak mjesta masovnog okupljanja. Na temelju toga lako bismo mogli zaključiti da videonadzor služi za podizanje opće sigurnosti i smanjenje učestalosti kaznenih djela jer dokazano je da već samo postojanje kamera smanjuje broj kriminalnih djela. I ne bismo bili u krivu.

Prema UN-u, dvije od svake tri osobe živjet će u gradovima do 2050. godine, a rješenje tog globalnog buma gradskog stanovništva svjetski stručnjaci vide u famoznom pojmu 'Pametni grad'. Europska komisija pametne gradove definira kao "mjesto gdje tradicionalne mreže i usluge postaju učinkovitije korištenjem digitalnih rješenja za dobrobit svojih stanovnika i poslovanja." Nije ni čudno onda da se umjetna inteligencija za videonadzor koji se integrira s drugim rješenjima predstavlja kao budućnost. Posjedovanje moderne objedinjene platforme koja obuhvaća sustave poput videonadzora, kontrole pristupa, ANPR-a, upada i analitike put je u budućnost pametnog grada i rješenje za svladavanje kaosa prenapućenosti urbanih središta.

Procjenjuje se da Kina ima više od polovice pametnih gradova svijeta. U Shenzhenu, hvaljenom kao 'prvi potpuno pametni grad na svijetu', senzori i kamere drže gotovo cijeli grad pod stalnim nadzorom. Podaci se prikupljaju, centraliziraju i integriraju za informiranje o urbanom upravljanju, planiranju i pojedinačnim odlukama. Belgijski grad Genk, na primjer, koristi Nokijin Scene Analytics za mjerenje razine buke na ulici i izvještavanje zabrinutih stanovnika. Ista je tehnologija isprobana u australskom Melbourneu kako bi se vlastima pomoglo u borbi protiv ilegalnog odlaganja otpada.

Umjetna inteligencija u videonadzoru također omogućuje dubinski pregled snimaka u pametnim gradovima kako bi se pronašli određeni ljudi ili registarske pločice. Nadalje, u slučaju izvanrednog stanja u javnom zdravstvu, kao što je pandemija COVID-19, podaci se mogu prikupiti putem videonadzora koji pokreće AI o tome nose li ljudi maske za lice ili poštuju pravila socijalnog distanciranja.

Predviđa se da će globalno tržište videonadzora biti vrijedno 38,2 milijarde dolara do 2027., a videonadzor ostaje temeljni dio slagalice u osiguravanju ljudi, mjesta i imovine, no predstavlja i puno više od toga. Veliki postotak sustava videonadzora se već koristi za rješavanje

operativnih izazova ili pružanje dodatne poslovne inteligencije. Usvajanje umjetne inteligencije i analitike temeljene na AI već je 'stara' vijest, no ChatGPT je potaknuo eksploziju generativne AI.

Sve veća kombinacija sigurnosnih kamera i umjetne inteligencije ključna je za transformaciju videotehnologije iz čistih funkcija nadzora u širu poslovnu upotrebu. Prediktivna analitika vođena podacima i umjetnom inteligencijom pruža dragocjene uvide u kritične poslovne procese i pomaže u prepoznavanju rizika prije nego što se pojave. Prediktivna analitika temeljena na umjetnoj inteligenciji sastoji se od tri procesa: prikupljanje videoinformacija, istraživačka analiza podataka i modeliranje scenarija. Sektori, uključujući pametne gradove, maloprodaju, proizvodnju, logistiku i zdravstvenu skrb, stavljaju ovu tehnologiju u pogon kako bi postigli učinkovitost kroz smanjenje troškova, optimizaciju procesa i poboljšanja kvalitete usluga. Također koriste videonadzor kako bi poboljšali sigurnost i spriječili nesreće.

Kombinacijom AI i rubnog računalstva u samoj kameri ('na rubu'), podaci se obrađuju kada i gdje su generirani. Ovo pomaže korisnicima da steknu trenutni uvid u svoje video podatke i uštede vrijeme i novac, budući da velike količine podataka ne moraju biti prebačene na odvojena mjesta za pohranu i obradu. Jedini rubni uređaj brine se za sve – od snimanja video zapisa i pohrane do analize i povezivanja s oblakom. Najveća prednost rubnih AI kamera je da se videoanaliza odvija na licu mjesta, pružajući brže uvide kako bi se olakšalo donošenje odluka u stvarnom vremenu u kritičnim scenarijima.

Ključni termin Video Surveillance as a Service

Sustav videonadzora temeljen na oblaku ili VSaaS (Video Surveillance as a Service) sve je značajniji jer može se jednostavno ugraditi u postojeći sustav i integrirati s drugim sigurnosnim sustavima kao što su kontrola pristupa, detekcija požara i upravljanje zgradom. No, kako to obično biva, gdje je sreća u je i nesreća jer ssa svim dobrim stvarima koje je tehnologija donijela, stigli su i rizici. Prijetnje kibernetičkoj sigurnosti su eksplodirale. S obzirom na to da videonadzor postaje sve više povezan putem Interneta stvari (IoT) i platformi u oblaku, osiguravanje sigurnosti podataka postalo je ključno. Sustavi videonadzora, naime, oslanjaju se na pohranu u oblaku i IoT tehnologije za snimanje, obradu i pohranjivanje golemih količina podataka. Međutim, ovaj je pomak donio nove izazove kibernetičke sigurnosti jer nadzorne snimke mogu biti osjetljive na hakiranje, povrede podataka i druge kibernetičke prijetnje. Lideri u industriji stoga provode rigorozne sigurnosne mjere kako bi riješili te rizike i svojim klijentima pružili snažnu zaštitu za podatke videonadzora.

Kao odgovor na rastuće kibernetičke prijetnje, u 2024. je uvedena i Direktiva o mrežnoj i informacijskoj sigurnosti (NIS2) u cijeloj EU. NIS2 je direktiva koju su usvojili Europski parlament i Vijeće Europske unije u prosincu 2020. Države članice EU-a uskladile su se s NIS2 u listopadu 2024. kako bi ispunile posebne mjere usmjerene na poboljšanje kibernetičke sigurnosti sustava diljem EU.

Usklađenost s regulativom ključna je za tvrtke u sektoru videonadzora, posebice jer zakoni o zaštiti podataka postaju sve stroži. Usklađenost ne samo da umanjuje pravne rizike, već i gradi povjerenje kod kupaca koji žele jamstvo da se s njihovim podacima postupa odgovorno. Certifikati poput SOC 2, sukladnosti tipa 2 i ISO 27001 pokazuju predanost tvrtke cyber sigurnosti i privatnosti podataka.

No, kako se videonadzor nastavlja širiti u IoT okruženjima, kibernetička sigurnost ostat će glavni prioritet. Integracija IoT uređaja povećava količinu generiranih podataka, što zauzvrat zahtijeva robusnije mjere zaštite. Tvrtke će morati nastaviti ulagati u napredne sigurnosne tehnologije, kao što je otkrivanje prijetnji pokretano umjetnom inteligencijom i end-to-end enkripcija, kako bi osigurale da podaci ostanu sigurni u sve povezanijem svijetu.

Krešimir Pučić

(Članak je objavljen uz financijsku potporu Agencije za elektroničke medije u okviru Programa poticanja novinarske izvrsnosti)