

## INTERVJU

**Yoann Klein,**  
Huawei

## TEME

Glasovna **kontrola**  
bez **korištenja glasa**

## TRŽIŠTA

**Modernizacija vatrodojave**  
u pametnim zgradama

**Sigurniji dom  
ZA KUĆNE  
LJUBIMCE**





## Touchless Access Control Solutions. Protect your people. And their people.



We're seeing our world a little differently now. The decisions you make affect more people than ever before. And HID Global is leading the industry with touchless security solutions that protect your workforce—and their families—holistically. From no-contact secure entries and over-the-air credentialing to occupancy control and social distance monitoring, our comprehensive solutions allow you to reassure your employees and ensure a safe, secure, successful return to work.



TOUCHLESS ENTRY



MOBILE ACCESS



VISITOR MANAGEMENT



REAL-TIME LOCATION  
SERVICES

For a limited time, HID Global is offering new customers

**50% OFF** mobile IDs for one full-year subscription.

Learn more at [hidglobal.com/touchless](http://hidglobal.com/touchless)



# Dahua termalno rješenje za mjerjenje temperature ljudskog tijela

## Učinkovito, jasno i beskontaktno

Dahua termalno rješenje nalazi se na prvoj liniji fronta i pomaže u sprečavanju i kontroli epidemije u zračnim lukama, željezničkim stanicama, bolnicama, školama i drugim mjestima širom svijeta.



CE FC CCC UL ROHS ISO 9001:2000



**DAHUA TECHNOLOGY Hrvatska**

Avenija. V. Holjevca 40, 10000 Zagreb

Email: info.dhslo@dahuatech.com

Tel: +385 1 5790 052

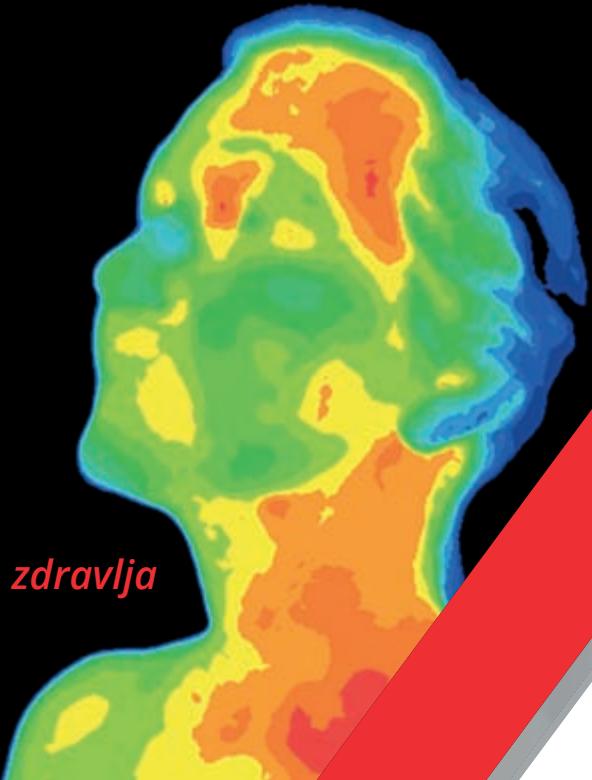
[www.dahuasecurity.com](http://www.dahuasecurity.com)



## SISTEMI ZA MJERENJE TEMPERATURE

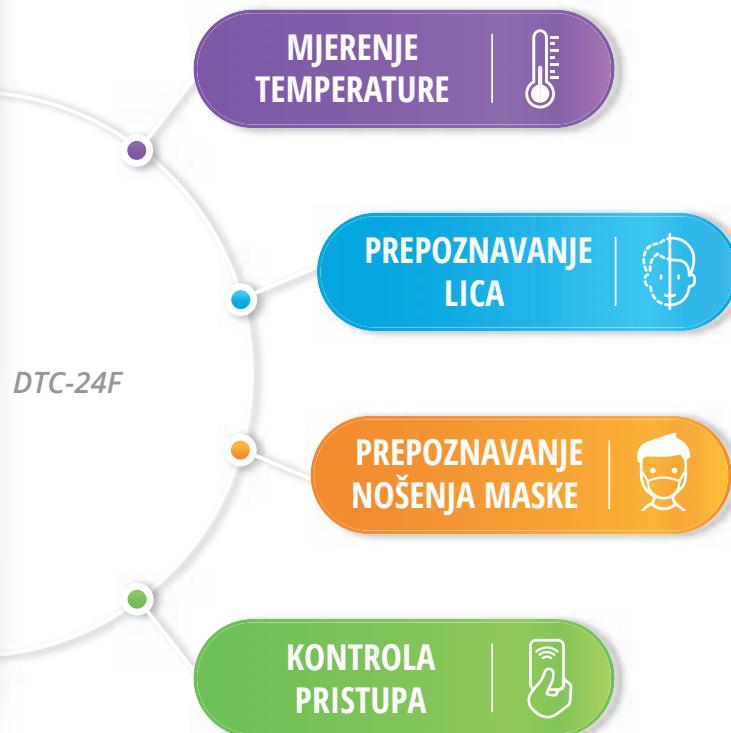
**Napredna tehnologija za sigurnost i zaštitu zdravlja**

Alarm automatika predstavlja rješenja vlastitog brenda kojeg razvija od 2003. godine



### Smart & Flexible Solution

Idealno za mesta srednje frekvencije prolaza kao što su banke, javne ustanove, tvornice i poslovni prostori, domovi za starije prostore, restorani, hoteli, dječji vrtići, fitness i sportski centri.



### Smart Intelligence Solution



- Zračne i trajektne luke, autobusni i željeznički kolodvori, veliki trgovački centri
- Beskontaktna obrada **do 30 ljudi** istovremeno
- Pametna videoanalitika (AI VCA)
- Kontrola pristupa

### Advanced Solution



- Bolnice, škole, stadioni, kongresni centri, sportske i kinodvorane, sveučilišta, kampusi, učenički i studentski domovi
- Beskontaktna obrada **do 10 ljudi** istovremeno
- Kontrola pristupa

### Fast & Simple Solution



- Kozmetički i frizerski saloni, uslužni obrti i manja poduzeća
- Ekonomično
- Precizno mjerjenje temperature pomoći toplinskog senzora unutar 0.5 sekundi

### Fast & Simple Solution



- Bolnice, škole, društveni centri, tvornice, hoteli, supermarketi, tržnice i sajmovi, kolodvori
- Brzo i efikasno mjerjenje temperature
- Sterilizacija i dezinfekcija ruku



Alarm automatika d.o.o.  
Džemala Bijedića 156, 71000 Sarajevo

T: 033 218 872  
E: sarajevo@alarmautomatika.com

[www.alarmautomatika.com](http://www.alarmautomatika.com)



Saznaj više!



## 46 Sigurniji dom za kućne ljubimce

Zašto su kamere za nadzor kućnih ljubimaca postale važne njihovim vlasnicima, kakve opcije nude i da li zaista mogu pomoći ukoliko ih odlučite instalirati u svom domu, pročitajte u ovom broju

### INTERVJU

**18 BYoann Klein,**  
viši savjetnik za cyber sigurnost,  
Huawei

### TRŽIŠTA

**24 S rastom pametnih zgrada**  
Modernizacija vatrodojave

### PROIZVODI I SISTEMI

**30 Pet-friendly kamere**  
Sigurniji dom za kućne ljubimce

**34 Videonadzorne kamere za noćno snimanje**  
Kako odabrati onu najbolju?

### PROIZVODI I SISTEMI

**42 HID Global: Izazovi pandemije**  
Beskontaktna sigurnost  
i povratak na radna mesta

**40 Cambium Networks predstavio cnVision**  
Profesionalno bežično  
rješenje za videonadzor

**42 Kontrola događaja u vremenu nove normalnosti**  
Hikvisionovo rješenje  
za spajanje ljudi

**43 Ingram Micro: Slučaj iz prakse**  
Rješenje za zaštitu  
objekata, ljudi i okoline

**44 FrogBlue: Vrijeme je za "virtuelne" kablove**  
Jednostavne, bežične  
i sigurne pametne zgrade

### PROIZVODI I SISTEMI

**45 Svestrani senzori**  
Bežični predajnici  
za OPTEX senzore

**46 Incedo Business platforma**  
Kontrola pristupa  
koja vam je potrebna

### TEME

**48 Nova vrsta hakerskih napada**  
Glasovna kontrola  
bez korištenja glasa

**50 Izazovi cyber sigurnosti**  
Važnost konvergencije fizičke i  
cyber sigurnosti

**52 Kućne nadzorne kamere i privatnost**  
Umjetnost, nauka i sigurnost  
u privatnosti domova



**SAFEPOINT**

## SAFEPOINT

Rješenje za kontrolu  
tjelesne temperature,  
nošenje zaštitne maske  
i dezinfekciju ruku



## TAGIT

Zaštitne naljepnice  
idealne za ručno  
apliciranje u  
trgovinama,  
ergonomične i  
cjenvovno povoljnije

**TAGIT**  
EAS TECHNOLOGIES



**PURIFOOG**  
by UR FOG

## URFOG I PURIFOOG

**URFOG** - Efikasan, brz  
i pametan sistem maglene  
protivprovalne zaštite

**PURIFOOG** - Sistem dvostrukе  
namjene koji čisti,  
higijenizira i štiti



## RECONEYEZ

Potpuno bežični  
video alarmni sistem  
za vanjske aplikacije

**RECONEYEZ**

## SMART IoT SISTEMI

Senzori, kontrola svjetala i uređaja,  
videonadzorni i interkom sistemi



Za više informacija: +387 33 869 873    +387 66 223 169

[www.spscgroup.com](http://www.spscgroup.com)

[info@spscgroup.com](mailto:info@spscgroup.com)

**SPSC**  
GROUP

# a&S ADRIA

Mi promoviramo sigurnost

[www.asadria.com](http://www.asadria.com)  
ISSN 1986-5031

## REDAKCIJA/EDITORIAL

Adis Hodžić [Direktor/Director](#)  
adis.hodzic@asadria.com

Mahir Hodžić [Glavni urednik/Editor in Chief](#)  
mahir.hodzic@asadria.com

Damir Muharemović [Urednik/Editor](#)  
redakcija@asadria.com

Sanel Palislamović [Grafički urednik/Art&Design Editor](#)  
sanel.palislamovic@asadria.com

Nelmedin Kolubara [DTP grafička obrada/ DTP&Art Design](#) dino.kolubara@asadria.com

Nermin Kabahija [Saradnik/Associate](#)  
redakcija@asadria.com

Mara Dragić [Novinarke/Journalist](#)

Senad Matić Karić [Saradnik/Associate](#)

Vesna Matić Karić [Saradnik/Associate](#)

Mirza Bahić [Saradnik/Associate](#)

Global Security d.o.o.

Safeta Zajke 115c, 71000 Sarajevo,  
Bosna i Hercegovina

Tel: +387 (0)33/788-985

Fax: +387 (0)33/788-986

Web: [www.asadria.com](http://www.asadria.com)

Marketing: [marketing@asadria.com](mailto:marketing@asadria.com)

**PDV broj: 201142740001**  
**Identifikacijski broj: 4201142740001**

Messe Frankfurt New Era Business Media Ltd. je najveći ponuđač medijskih usluga u globalnoj sigurnosnoj industriji. Našu medijsku platformu sačinjava 14 publikacija, sajmova i konferencije, web-stranice i mobilne aplikacije. Portfolio a&s magazina čine: a&s Adria, a&s International, a&s Asia, a&s Japan, a&s China, a&s Intelligent System, a&s Italy, a&s Polska, a&s Rubezh Russia, a&s India, a&s Vietnam, a&s Taiwan i a&s SMAhome. Magazin a&s Adria pokriva države jugoistočne Europe: Bosnu i Hercegovinu, Crnu Goru, Hrvatsku, Kosovo, Makedoniju, Sloveniju i Srbiju.

Messe Frankfurt New Era Business Media Ltd. is a largest media service provider in the global security industry. Our media platform consists of 14 magazines, trade shows, web sites, and mobile apps. The portfolio of a&s Magazine includes: a&s Adria, a&s International, a&s Asia, a&s Japan, a&s China, a&s Intelligent System, a&s Italy, a&s Polska, a&s Rubezh Russia, a&s India, a&s Vietnam, a&s Taiwan and a&s SMAhome. Magazine a&s Adria covers Southeastern Europe countries: Bosnia and Herzegovina, Croatia, Montenegro, Kosovo, Macedonia, Slovenia and Serbia.

Copyright© 2011 Global security d.o.o. Sva prava zadržana. Zabranjeno je svako republiciranje, kopiranje, redistribuiranje i reproduciranje magazina u bilo kojoj formi, uključujući i elektronsku, bez prethodne pismene saglasnosti izdavača.

Oglašivači su sami odgovorni za sadržaj reklamnog materijala. Izdavač ne snosi nikakvu odgovornost povodom mogućih zakonskih, patentnih, sadržajnih ili brendovnih sporova oglašivača.

Magazin a&s Adria izlazi u prvoj trećini mjeseca.

## Jedna neobična "vertikala"

**Videonadzorni sistemi s dvostrukom komunikacijom nalaze uspješnu primjenu u jednoj sasvim neobičnoj "vertikali". Naime, sve više zabrinutih vlasnika širom svijeta poseže za tehnološkim rješenjima kako bi mogli nadgledati, ali i komunicirati sa svojim kućnim ljubimcima kada su odsutni od kuće. Ovi sistemi im omogućavaju ne samo da ih stalno nadziru već i da imaju dvosmjerni audiosignal zahvaljujući kojem je moguća i komunikacija. Vlasnici tako mogu svoje ljubimce umiriti ukoliko su uplašeni ili uzremeni, ali i jednostavno detektovati bilo koji drugi problem.**

*Ovaj trend počinje graditi jedno sasvim novo tržiste, u kojem psihološko-socijalni aspekt prednjači ispred sigurnosnog. Jer, iako sigurnosne kamere omogućavaju da pratite i snimate svog kućnog ljubimca dok niste kod kuće, one ne čine ništa na uspostavljanju odnosa s njim, što, pretpostavljamo, žele svi vlasnici. Ove kamere mogu još nešto. One omogućavaju da im se obraćate, da se gledate preko kamere, a neke čak imaju i opciju da s vremenom na vrijeme izbace poslasticu za vašeg četveronožnog "člana porodice". Kamere mogu rješiti i problem anksioznosti ili dosade kod psa, koja se često javlja ukoliko je predugo ostavljen sam, a to nerijetko dovodi i do pojave uništavanja namještaja, odjeće, obuće itd. Da ne govorimo o rastu nivoa stresa koje neki ljubimci doživljavaju kada su ostavljeni sami.*

*I s tehnološkog aspekta su ove kamere zanimljive. Većina donosi visoku rezoluciju i široke uglove gledanja, opremljene su pametnim sistemom za dvosmjernu audio i video komunikaciju, imaju čak i lasere za igru, pa i pametne hranilice, a na sve to dodajmo još da mogu poslužiti i za nadzor i pohranu videomaterijala. Dakle, šta jedan vlasnik kućnog ljubimca još može poželjeti?*

**Mahir Hodžić, glavni urednik**

## KAKO SE PRETPLATITI

Uplate na devizni račun:

Raiffeisen bank 502012000-0003070;

SWIFT: RZBABA2S

**Cijena: 60 eura/evra.**

Uplate na KM račun:

Raiffeisen bank 1610000056880035

**Cijena: 80 KM**

Uz obaveznu naznaku PRETPLATA NA MAGAZIN A&S ADRIA

Kontakt: [preplata@asadria.com](mailto:preplata@asadria.com)

Pretplata: 12 mjeseci (11 brojeva, dvobroj juli/august)

Poštarnina uključena u cijenu.

**ASADRIA.COM**

**ADRIASECURITYSUMMIT.COM**

**VSECURITYSUMMIT.COM**

**CONNECT2BNET.COM**



## Ingram Micro, kao globalni distributer, svojim jedinstvenim položajem u tehnološkom ekosistemu omogućava direktni pristup najnovijim tehnologijama i poslovnim rješenjima

Partnerima nudimo pristup najnovijim tehnologijama, Cloud uslugama, komunikacijskim i kolaboracijskim alatima te infrastrukturnim i sigurnosnim rješenjima. Uspješno razvijajte svoje posovanje bez obzira na kojem tržištu poslujete. Također, nudimo logističku podršku i tehnološku ekspertizu kako bi ste iskoristili sve što vam tehnološki ekosistem pruža u vidu unapređenja posovanja i povećanja profitabilnosti.

Axis je lider na svjetskom tržištu IP CCTV-a koji nudi mrežna video rješenja za profesionalne instalacije kreirajući proizvode i rješenja koja su zasnovana na inovativnim i otvorenim tehničkim platformama.



### Za pametniji i sigurniji svijet

#### HRVATSKA

Ingram Micro d.o.o. Zagreb Štefanovečka cesta 10, 10000 Zagreb | Tel: +385 1 3000 465 | Email: marko.peica@ingrammicro.com | <https://hr.ingrammicro.eu>

#### SLOVENIJA

Ingram Micro Ljubljana d.o.o. Verovškova ulica 55, 1000 Ljubljana | Tel: +386 1 600 25 80 | Email: tadej.peternelj@ingrammicro.com | <https://si.ingrammicro.eu>

#### SRBIJA, BOSNA I HERCEGOVINA, MAKEDONIJA, ALBANIJA, CRNA GORA

Ingram Micro doo Beograd Tošin Bunar 272V, 11070 Novi Beograd | Tel: +381 64 822 75 611 | Email: predrag.acimov@ingrammicro.com | <https://rs.ingrammicro.eu>

## ALARM AUTOMATIKA OSAM GODINA U KONTINUITETU NOSILAC AAA CERTIFIKATA

Alarm automatika je i 2020. nosilac AAA Certifikata bonitetne izvrsnosti, što znači da je ostvarila odlične poslovne rezultate, zadovoljila stroge finansijsko-analitičke kriterije prema metodologiji jedinstvenoj za cijelu Evropu i da spada u 5% najboljih firmi u Hrvatskoj. Od svih aktivnih poslovnih subjekata u Primorsko-goranskoj županiji samo 9 posto je ispunilo uvjete za dobivanje ovog certifikata. Alarm automatići je osam godina u kontinuitetu dodijeljeno pravo na certifikat kompanije Bisnode, vodećeg ponuđača poslovnih informacija u Evropi. Taj certifikat u poslovnom



svijetu predstavlja dokaz o natprosječnom kvalitetu poslovanja firme. Više desetaka statistički značajnih varijabli, formula provjerenih na temelju finansijskih podataka, blokada, navika plaćanja i tužbi dokazuju sigurnost, konkurentnost, trajnost, stabilnost, kvalitet i pouzdanost poslovnih subjekata. ◀

## VELIKI RAST BROJA NAPADA RANSOMVEROM U SRBIJI

Pandemija izazvana virusom SARS-CoV-2 potaknula je rad na daljinu, što je postao sigurnosni izazov firmama i zaposlenicima, ali i prilika za cyber kriminalce. Globalno istraživanje Kasperskyja ukazalo je na zabrinjavajuću činjenicu da je tek nešto više od polovine zaposlenih za rad od kuće opremljeno korporacijskim uređajima (55%), a nešto manje (53%) VPN zaštitom veze kako bi se sigurno povezivali na korporativnu mrežu. Isto istraživanje pokazalo je i da se



više od četvrtine (27%) zaposlenih koji rade od kuće već susrelo s e-mail porukama na temu COVID-19 infekcije koji su sadržavali maličiozne fajlove. "Tehnikom socijalnog inžinjeringu, tematika COVID-a poslužila je prvenstveno pokretanju phising kampanja i učestalijim napadima trojancima usmerenim na krađu bankarskih podataka korisnika. Uslijedio je niz DDoS i ransomver napada na bolnice, WHO ili kompanije koje su se bavile razvojem vakcine protiv COVID-a. Konačno, cyber kriminalci su napore usmjerili i na one koji rade od kuće, pa je broj napada na protokole za rad na daljinu globalno porastao za 242%, što je ogroman skok", rekao je Miroslav Koren, generalni direktor Kasperskyja za Istočnu Evropu. Prema istraživanju te kompanije, u Srbiji je tokom 2020. došlo do primjetnog pada u broju napada na računare (-30,64%), kao i do pada u ukupnom broju detekcija malvera za mobilne uređaje (-32,62%). No, zabilježen je znatan rast u trećem kvartalu u odnosu na isti period prošle godine, čak 67,10%. Jedna od najzanimljivijih činjenica je da je broj korisnika u Srbiji pogodenih ransomverom ove godine porastao za čak 143,16%, s najvećim zabilježenim porastom u prva tri mjeseca ove godine (257,65%). "Jedan od najefektivnijih modela zarade sajber kriminalaca jeste upravo targetiranje kompanija sa nižim stepenom zaštite, prvenstveno putem softvera za iznudu ili ransomwarea. Otud i ne čudi rast ove vrste pretnji i u Srbiji", kaže Dragan Davidović, menadžer prodaje kompanije Kaspersky. ◀

## VIDEONADZOR U OPĆINI NOVIGRAD PODRAVSKI

U Novigradu Podravskom, općini na sjeveru Hrvatske, puštene su u rad nove nadzorne kamere. Zbog učestalog nepropisnog odlaganja otpada nadzirat će se površine Zelenih otoka u Vlaislavu, Borovljanima i Delovima te površina uz cestu Plavšinac – Vlaislav, gdje se ubrzano stvara “divlje” odlagalište, i takozvanih laguna za deponiranje uvehlog cvijeća i vijenaca na groblju Sv. Klara. Zbog kontrole i sprečavanja eventualnog vandalizma nadzire se i dječje igralište u sklopu parka Pod lipama. "Prije postavljanja kamera za videonadzor ishodili smo svu potrebnu propisanu dokumentaciju, suglasnosti i dozvole", poručili su iz Općine. ◀





# SECURITY SUMMIT

VIRTUAL EVENT  
CONFERENCE & EXHIBITION

## See You in May



FOCUS  
ON THE  
FUTURE

04  
DAY

06  
DAY

05  
MONTH

'21  
YEAR

<http://vsecuritysummit.com>

## ALLIED UNIVERSAL SECURITY KUPUJE G4S ZA 5,1 MILIJARDU DOLARA

Upravni odbori kompanija Allied Universal i G4S objavili su da su postigli dogovor o uslovima preporučene finansijske ponude koju će dati Atlas UK Bidco, novoosnovana kompanija kojom posredno upravlja Allied Universal. Ponuda podrazumijeva akviziciju postojećeg i budućeg dioničkog kapitala G4S-a. Ugovor čija se vrijednost procjenjuje na 5,1 milijardu dolara dovest će do objedinjavanja dvije velike sigurnosne kompanije, a sklopljen je nakon što je G4S mjesecima odbijao ponude kanadskog Gardaworlda. Uprava G4S-a jednoglasno je preporučila dioničarima da prihvate ponudu, a oni su se neopozivo obavezali da će to učiniti s vlastitim dionicama G4S-a, što je oko 0,21 posto ukupnog dioničkog kapitala. Spajanje će dovesti do stvaranja velike globalne sigurnosne kompanije, s prihodom od približno 18 milijardi dolara i radnom snagom od preko 750.000 ljudi, jakom međunarodnom platformom i širokom bazom klijenata u javnom i privatnom sektoru.



"G4S je transformiran u fokusiranog globalnog lidera u oblasti sigurnosnih usluga, s vodećim tržišnim rješenjima i bazom bogatih kupaca koju opslužuje posvećeni i nadareni tim s više od 530.000 zaposlenih. Spajanje G4S-a i Allied Universal-a kreirat će globalnog lidera u sektoru sigurnosti s više od 750.000 zaposlenih, vodećim mogućnostima u industriji i neprikosnovenom pokrivenošću tržišta. Ova jedinstvena i snažna kombinacija ponudit će kupcima izuzetnu uslugu, a zaposlenima uzbudljivu budućnost", kaže Ashley Almanza, izvršna direktorka G4S-a. "Drago nam je što je našu ponudu od 245 penija po dionici preporučio Upravni odbor G4S-a. Naše se kompanije dobro poznaju, dijelimo sličnu kulturu i vrijednosti i sretan sam zbog svega što ovaj spoj može pružiti. G4S ima izvrsnu ponudu usluga, zavidan globalni portfolio kupaca i vodi ga iskusan menadžerski tim. Zajedno ćemo imati više od 100 godina industrijskog iskustva i širu globalnu mrežu u pogledu ljudi, kupaca i mogućnosti", kaže Steve Jones, predsjednik i izvršni direktor Allied Universal-a. ◀

## PREPOZNAVANJE LICA POSTAJE UNOSNO TRŽIŠTE

Tržište prepoznavanja lica porast će sa 3,8 milijardi dolara u 2020. na 8,5 milijardi do 2025., po složenoj godišnjoj stopi rasta od 17,2%, procjene su Marketsandmarketsa. Istraživači predviđaju da su razlog veća ulaganja vladinih agencija i odbrambenog sektora, ali i rast nadzorne industrije. Još



od 60-ih godina prepoznavanje lica je doživjelo velike promjene. Blizu 60% prihoda od te tehnologije odnosi se na organe reda, vojsku i odbranu, domovinsku sigurnost te državne agencije. Softverski alati pružaju bržu i lakšu identifikaciju i verifikaciju na osnovu karakteristika lica, što olakšava brojne procese, kao što su imigracija, praćenje prisustva i kontrola pristupa. Softverski alati se dijele na 2D i 3D prepoznavanje lica te analitiku lica. Utvrđeno je da rast stope kriminalnih i terorističkih aktivnosti potiče potražnju za naprednim tehnologijama. Trenutno softver za 3D prepoznavanje lica postaje privlačniji krajnjim korisnicima jer može precizno detektirati i prepoznati različite izraze lica i položaje. Kompanije kao što su NEC, Ayonix, Idemia i Stereovision Imaging nude softverske alate za to, koji će, prema procjenama, ostvariti najvišu stopu rasta u narednih pet godina. Američko i kanadsko tržište najviše se razvijaju u ovom segmentu, prvenstveno zbog većeg prihvatanja tehnologije prepoznavanja lica u kompanijama, ali i rasta inicijativa vezanih za pametne gradove, e-pasoše i e-vize. Najveći proizvođači navedeni u istraživanju su: NEC, Aware, Ayonix, Cognitec, NVISO, Animetrics, Neurotechnology, Daon, Stereovision Imaging, Techno Brain, Innovetrics, Id3 Technologies, Thales, Idemia, Nuance Communication, Bio ID, Fulcrum Biometrics, Trueface.AI, Amazon, Facephi, Herta Security, Kairos AR, Sightcorp i Microsoft. ◀



**Sustavi elektrokemijske zaštite i satelitskog praćenja gotovine i vrijednosti na šalterima, u bankomatima i ostalim uplatno/ isplatnim uređajima**



### Antiskimming sustavi za bankomate

 Cennox

### Pametni depozitni sefovi



BODE PANZER

### Elektrokemijski sustavi zaštite gotovine u transportu

**GEHRER AG**  
SECURITY SOLUTIONS



**SAIMA**  
GLOBAL ACCESS CONTROL

### Upravljanje ključevima – Keywatcher



**MORSE WATCHMANS**

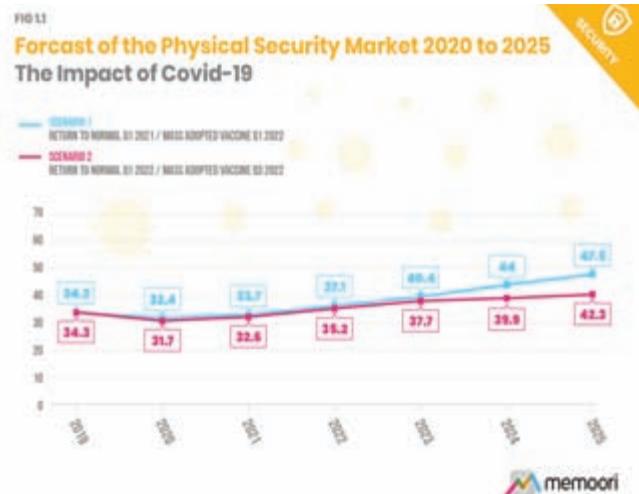
### Elektronske sefovskе brave



**INSYS locks**  
Security Systems

## ZAUSTAVLJEN 11-GODIŠNJI RAST INDUSTRIJE SIGURNOSTI

Memoorijev 12. godišnji izvještaj o globalnoj sigurnosnoj industriji procjenjuje da ukupna vrijednost sigurnosnih uređaja po proizvodnim cijenama u 2020. godini iznosi 31,7 miljardi dolara, što je pad od preko 7% u odnosu na 2019. Prodaja je opala u sva četiri kvartala kao rezultat pandemije koronavirusa. Time je okončano jedanaest uzastopnih godina rasta u industriji. Sjjetska banka je u junu objavila prognozu koja predviđa smanjenje ukupnog svjetskog BDP-a od 5,2% za 2020. U ovom trenutku broj zaraženih u trećem i četvrtom kvartalu raste, a pojedine zemlje opet uvode zabranu kretanja. Stoga istraživači Memoori smatraju da je najprihvativiji scenarij onaj u kojem će globalnim tržištima trebati oko godinu dana da se vrate u određenu normalu, a masovno globalno vakcinisanje provede otprilike 18 mjeseci. Takav scenarij ima vjerovatnoću od 65%, navodi Memoori. Analitičari su i dalje uvjereni u otpornost industrije i njen srednjoročni i dugoročni rast. Tržišni pokretači poput prijetnje od terorizma i kriminala vjerovatno se neće umanjiti, dok će urbanizacija i pametna infrastruktura dodatno poticati potrebu za naprednjim sigurnosnim sistemima. Covid-19 prisilit će dobavljače da radikalno preispitaju svoje po-



slovanje, posebno otpornost na vanjske faktore. Paralelno s tim, potrebno je raditi na uspostavljanju koordiniranijeg i otpornijeg opskrbnog lanca. Videonadzor je, smatraju, previše ovisan o kineskim proizvođačima originalne opreme i komponentama. Kada su mnoge od tamošnjih fabrika bile zatvorene u prva dva mjeseca 2020. godine, to je prouzrokovalo privremene probleme u opskrbnom lancu. Nakon što svijet prevaziđe ovu pandemiju, dobavljači će, zaključuje Memoori, morati temeljito razmotriti zahtjeve kupaca, posebno onih preduzeća čije je poslovanje bilo ozbiljno narušeno. Takvim kupcima će biti teže odvojiti novac za ulaganje u sigurnost i zato moraju biti uvjereni u povrat uloženog. ACaaS i VSaaS mogu pružiti rješenje za ovaj problem, što potvrđuju i dokazi o znatnom ubrzavanju rasta usluga u oblaku. ◀

## HUAWEIJU USLOVNO ZELENO SVJETLO ČIM NJEMAČKA VLADA USVOJI ZAKON O MREŽNOJ SIGURNOSTI

Njemačka vlada je odlučila da dozvoli upotrebu Huaweijeve 5G tehnologije u zamjenu za nadzor i obećanje kineske kompanije o sigurnosti svoje opreme, iako Sjedinjene Američke Države zahtijevaju njenu zabranu. Ovom odlukom Njemačka je pokazala naklonost Kini kao njenom najvećem trgovinskom partneru. Njemačka kancelarka Angela Merkel zalaže se za pronaštaženje tehničkog rješenja koje bi zahtijevalo da svi provajderi prođu stroge tehnološke standarde i budu transparentni za službe mrežne sigurnosti. Ministar unutrašnjih poslova Horst Zehofer objasnio je da vlada teži stvaranju pravne osnove koja će održati tržište otvorenim za konkurentne tehnologije. Prema prijedlogu zakona, prodavači mrežne opreme morali bi pružiti garantije da je njihova oprema sigurna za upotrebu, čineći ih finansijski odgovornim u slučaju kršenja pravila. Zakon bi zahtijevao i da prodavci i operatori osiguraju njemačkim sigurnosnim agencijama dalekosežna tehnička i pravna sredstva za nadzor integriteta mreže. Huaweiju tehnologiju već su prihvatile i usvojile određene njemačke kompanije. Proizvođači automobila koriste kinesku tehnologiju u segmentu povezanosti automobila i automatskog upravljanja, a Deutsche Telekom AG, njemački telekomunikacijski gigant, koristi je za svoje 4G i 5G bežične



širokopojasne mreže. Huawei je vodeći svjetski proizvođač televizorske opreme s prodajom od 123 milijarde dolara u 2019. godini. Privatna je kompanija u potpunom vlasništvu svojih zaposlenih, upošljava 194.000 radnika i posluje u više od 170 zemalja i regiona. ◀



PRVI IZBOR ZA SIGURNOSNE STRUČNJAKE



***Veliki izbor sigurnosne opreme  
za sve namjene na jednom mjestu***

**HIKVISION**  
Authorised Distributor

**TCS<sup>®</sup>**

**Visonic<sup>®</sup>**

**DSC**

**BENTEL<sup>®</sup> SECURITY**

**Teletek<sup>®</sup> electronics**

**golmar**

Kobel Promet d.o.o.  
Remetinečka cesta 13, 10000 Zagreb  
T – 01 3640 343 / 01 3638 992  
F – 01 3664 134  
E – kobel@kobel.hr

Kobel d.o.o. Sarajevo  
SafetaZajke 115c, 71000 Sarajevo  
T – 033 466 800  
F – 033 466 808  
E – dzemal@kobel.eu



## IMENOVAN NOVI GENERALNI DIREKTOR HANWHA TECHWINA ZA EVROPU

**■** Jeff Lee novi je generalni direktor kompanije Hanwha Techwin Europe. Radio je za Hanwha Grupu više od 21 godinu, a u augustu 2019. imenovan je za direktora prodaje za Evropu. Na toj poziciji usko je sarađivao s prethodnim generalnim direktorom Bobom (H.Y.) Hwangom, koji je kompaniju vodio u posljednjih pet godina. Hwang se vraća u Južnu Koreju, gdje će preuzeti drugu, seniorsku poziciju u Upravi. "Izgradnja partnerstava i stjecanje povjerenja integratora i distri-

butera uvijek je bilo od ključne važnosti za nas u Hanwha Techwin Europeu. U vezi s tim, čvrsto vjerujem da se trajni uspjeh naše kompanije može osigurati poslovanjem s integritetom te, uz kvalitetne proizvode i rješenja, izvrsnošću u svemu što radimo. Naš sveobuhvatan assortiman Wisenet proizvoda i rješenja pruža nam fantastičnu bazu na osnovu koje zajedno možemo postići veliki uspjeh tokom 2021", izjavio je Lee u poruci poslovnim partnerima Hanwehe. ▲



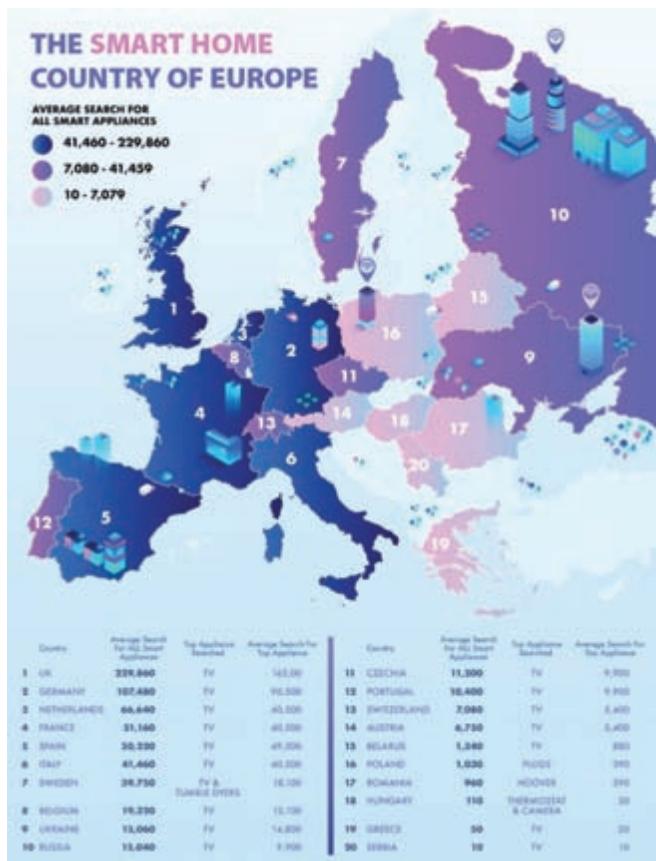
## USPJEH KING ICT-a I U POSLOVNO IZAZOVNOJ GODINI



**■** KING ICT je, zahvaljujući uspješnoj saradnji s partnerima i klijentima, uspio u 2020. dodatno proširiti raspon poslovanja. U kriznom periodu hrvatska kompanija je zadržala svih 470 zaposlenih, isti nivo plata, imala nešto manje konsolidirane prihode, ali zadovoljavajuću profitabilnost, te realizirala projekte finansirane iz EU fondova. KING ICT je napravio dosad najveći iskorak na zapadnoevropsko tržište potpisavši ugovor s NATO-ovom Agencijom za komunikacije i informacije u području kibernetičke sigurnosti. Ugovor uključuje isporuku i implementaciju SIEM rješenja za upravljanje sigurnosnim zapisima i događajima s kompletom, najsavremenijom IT infrastrukturom. Kada je riječ o regiji, u Dubrovniku je implementiran sistem za uspostavljanje zone zagušenja saobraćaja, koji se sastoji od prometno-analitičkih kamera s mogućnošću prepoznavanja kategorije vozila i registarske oznake. Za HŽ Infrastrukturu završena je implementacija rješenja SAP Enterprise Asset Management – integrisanog softverskog sistema koji upravlja prugama u dužini 2.617 km. U bankarskom sektoru implementiran je firewall s naprednim sigurnosnim zaštitama te sistem za siguran VPN pristup u privatnu mrežu. KING ICT je implementirao i modernu IT infrastrukturu podatkovnih centara temeljena na HCI infrastrukturni u KBC Sestre milosrdnice, Klinici za tumore i Klinici za traumatologiju, čime je smanjen rizik od gubitka osjetljivih podataka i povećana sigurnost od vanjskih napada i prijetnji. U Bosni i Hercegovini je uspostavljen moderan sistem video nadzora na međunarodnim graničnim prijelazima, rekonstruiran i opremljen podatkovni centar za Ministarstvo sigurnosti, odnosno 21 agenciju za provođenje zakona, dok je za Telemach Slovenije proveden projekt implementacije rješenja za zadovoljenje zahtjeva IFRS16 standarda kojim se određuju nove smjernice praćenja najmova i leasinga. ▲

## HOMEDIT.COM: UK NA VRHU, SRBIJA NA ZAČELJU SMART EVROPSKIH ZEMALJA

**■** Portal Homedit.com proveo je studiju o tome koje evropske države najviše prihvataju pametne tehnologije. Istraživanje je provedeno na 20 najmnogoljudnijih zemalja. Analizirana je količina pretraga njihovih stanovnika za pametnim uređajima putem Google pretraživača. Na prvom mjestu je Ujedinjeno Kraljevstvo sa čak 229.860 mjesечnih pretraga, pri čemu Britanci najviše traže pametne televizore. Iza njega je Njemačka s više nego dvostruko manjim brojem, 107.480, te Holandija sa 66.640 pretraga. Na dnu su Mađarska s tek 110 prosječnih mjesечnih pretraga za pametnim uređajima, Grčka sa 50 te Srbija sa samo 20. Kada je riječ o uređajima, najtraženiji su pametni televizori (483.000), pametni termostati (29.500) te pametne utičnice (19.250). Najmanje su traženi pametni laptopi. ▲



# INTEGRISANA RJEŠENJA ZAŠTITE



DUGOROČNO OSIGURAN SERVIS ZA SVE INSTALIRANE SISTEME  
SPECIJALISTIČKI KURSEVI I OBUKA IZ OBLASTI KONTRADIVERZIONE ZAŠTITE

#### ZASTUPNIŠTVO I PARTNERSTVO:

SMITH HEIMANN SYSTEMS, CEIA, LABOR STRAUSS, BENTEL, MOTOROLA,  
VIVOTEK, MILESTONE SYSTEMS, NICE, GUNNEBO, CNB TECHNOLOGY,  
JANTAR, ARECONT VISION, APRIMATIC, ALLEN, CENTRAL WEIGHING,  
AVIGILON, RIVA, CROSS, SPECIJALNA OPREMA ZA POLICIJU



ISO 9001:2000

Džemala Bijedića 35, 71000 Sarajevo  
Tel: +387 33 677 155 / 677 157  
e-mail: [info@mpoint.ba](mailto:info@mpoint.ba)  
[www.mpoint.ba](http://www.mpoint.ba)



**Middle point**  
ELECTRONICS D.O.O.

# VJERUJEMO U STANDARDE CYBER SIGURNOSTI I OBJEKTIVNU PROCJENU

HUAWEI NIJE IMAO VEĆIH CYBER SIGURNOSNIH INCIDENATA U PROCESU SARADNJE S VIŠE OD 500 PRUŽALACA TELEKOMUNIKACIJSKIH USLUGA, UKLJUČUJUĆI VEĆINU OD 50 NAJVEĆIH TELEKOM-OPERATERA. TAKVA JE SITUACIJA BILA U PROTEKLIMA SKORO 20 GODINA U 170 ZEMALJA, U KOJIMA JE POVEZANO VIŠE OD 3 MILIJARDE LJUDI. NIJEDAN DRUGI PROIZVOĐAČ NE MOŽE REĆI DA JE POSTIGAO OVAJ NIVO USPJEŠNOSTI U CYBER SIGURNOSTI

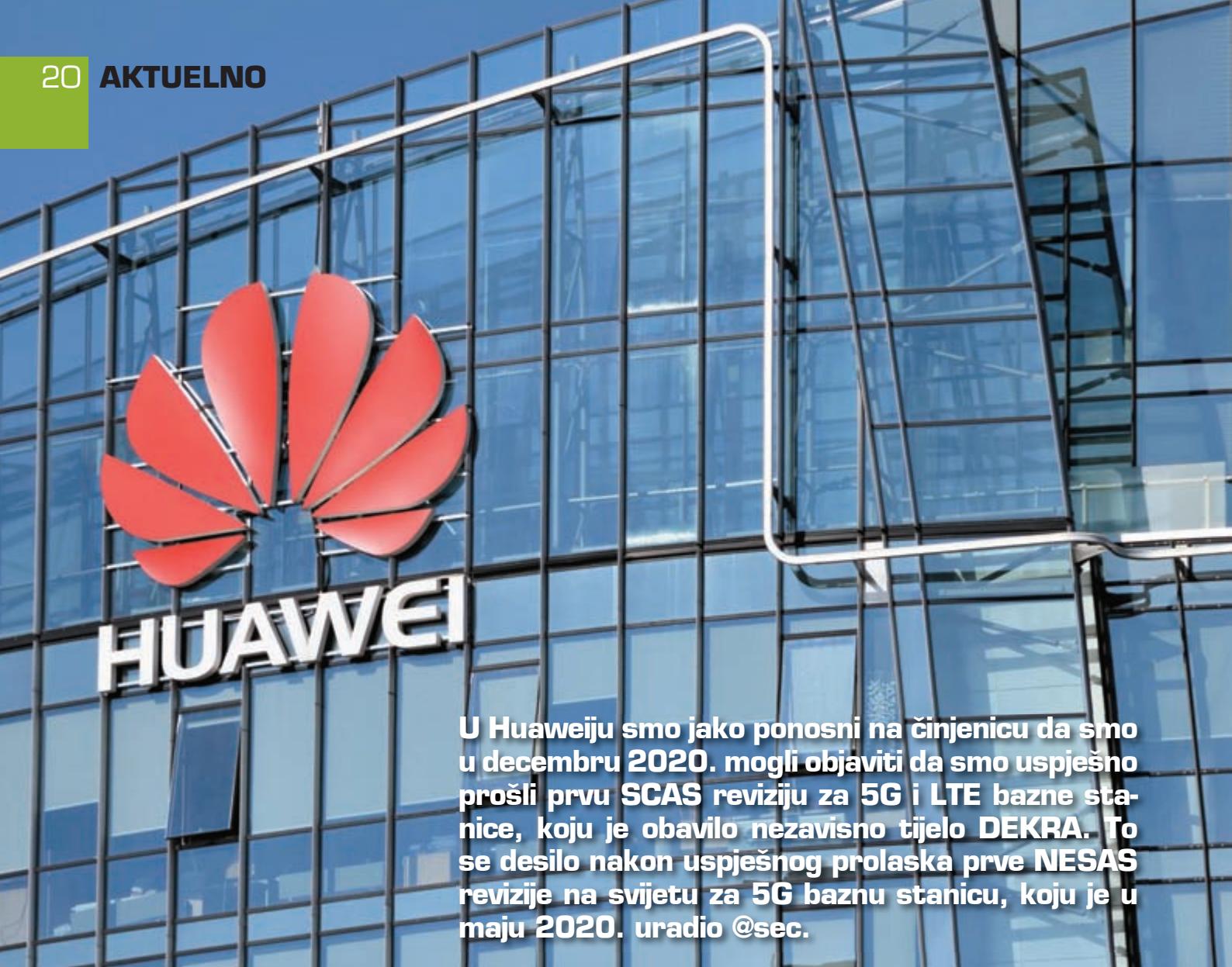
■ Razgovarao: Damir Muharemović  
redakcija@asadria.com

**a&s Adria:** Gospodine Klein, možete li se predstaviti našim čitaocima, s naglaskom na vašu poziciju u Huaweiju?

**Klein:** Magistarski studij iz telekomunikacija i računarstva završio sam na IMT Lille Douaiju, građevinskoj školi u sjevernom Parizu. Prije Huaweija skoro 15 godina sam radio u velikim evropskim cyber kompanijama kao što su Airbus i Thales. Sve vrijeme sam preuzimao ulogu tehničkog autoriteta i vodio cyber inžinjerske timove koji rade u raznim kritičnim okruženjima poput odbrane, javne sigurnosti, aeronautike, svemira i transporta. Sada sam viši savjetnik za kibernetičku sigurnost u Huaweijevom Centru za cyber sigurnost i transparentnost u Briselu. Član sam našeg Globalnog ureda za cyber sigurnost i privatnost (GSPO). Ovaj ured odgovoran je za razvoj strategije i politika kibernetičke sigurnosti i zaštite privatnosti te za upravljanje i nadzor nad organizacijom i operacijama cyber sigurnosti i zaštite privatnosti u određenim odjelima. Također osiguravamo da se takva strategija primjenjuje u svim odjelima, regijama i procesima, te da potičemo komunikaciju sa zainteresovanim stranama kao što su vlade, kupci, potrošači, dobavljači, partneri i zaposlenici.



**YOANN KLEIN,  
VIŠI SAVJETNIK ZA CYBER  
SIGURNOST, HUAWEI**



**U Huaweiju smo jako ponosni na činjenicu da smo u decembru 2020. mogli objaviti da smo uspješno prošli prvu SCAS reviziju za 5G i LTE bazne stанице, koju je obavilo nezavisno tijelo DEKRA. To se desilo nakon uspješnog prolaska prve NESAS revizije na svijetu za 5G baznu stanicu, koju je u maju 2020. uradio @sec.**

**a&s Adria:** Vaš Centar za cyber sigurnost i transparentnost bavi se sigurnošću 5G mreže i IoT-a. Koje vrste poslova to podrazumijeva?

**Klein:** Centar je svoja vrata otvorio u martu 2019. On pruža platformu za unapređenje komunikacije i zajedničkih inovacija sa svim interesnim stranama, javnim i privatnim. Također, našim kupcima pruža tehničku platformu za verifikaciju i evaluaciju. Otvorenost, saradnja i transparentnost su tri riječi koje pokreću ovu inicijativu. Otvorenost u prikazivanju naših cyber sigurnosnih praksi, od strategija i lanca opskrbe do istraživanja i razvoja, kroz prezentacije, videozapise, demonstracije Huaweijevih proizvoda i rješenja u područjima kao što su 5G, IoT, cloud itd. Saradnja, jer organizujemo namjenske stručne radionice i konferencije s ključnim zainteresovanim stranama (organizacijama, regulatorima, državnim vlastima itd.) o sigurnosnim praksama kako bismo istra-

žili i promovisali razvoj standarda, mehanizama provjere i tehnoloških inovacija u cyber sigurnosti. I na kraju, transparentnost, jer pružamo platformu za testiranje i provjeru nivoa sigurnosti naših proizvoda kupcima i nezavisnim laboratorijima. To uključuje testna okruženja metodama tzv. crne i bijele kutije (s pristupom izvornom kodu). U Briselu možemo istovremeno izvoditi pet takvih projekata.

**a&s Adria:** Radna grupa SA3, u okviru organizacije Projekat partnerstva 3. generacije (3GPP), održala je 2018. sedam sastanaka. Pri tome su 74 kompanije poslale svoje tehničke stručnjake da prisustvuju sastancima s ciljem formulisavanja 5G sigurnosnih standarda. 3GPP SA3 grupa je analizirala 5G prijetnje i rizike u 17 oblasti. Koje su to oblasti, kao i najveće prijetnje i rizici povezani s njima?

**Klein:** U okviru 3GPP grupe za tehničke specifikacije usluga i sistema (TSG SA)

kao glavni ciljevi radne grupe 3GPP TSG SA WG3 (SA3) navedeni su definisanje zahtjeva i arhitekture, kao i protokola za sigurnost i privatnost u 3GPP sistemima. Kako bi se što kvalitetnije ispunili ovi ciljevi, definisano je i ispitano više oblasti: sigurnosna arhitektura (1), autentifikacija (2), sigurnosni kontekst i upravljanje ključevima (3), sigurnost radijske pristupne mreže (RAN) (4), sigurnost u NG-UE (5), autorizacija (6), privatnost prijavljivanja (7), sigurnost dijeljenja mreže (8), zaštita odašiljača (9), sigurnost mrežne domene (10), sigurnosna vidljivost i konfigurabilnost (11), osiguravanje akreditiva (12), međusobno povezivanje i migracija (13), mali podaci (14), zaštita emitovanja / višestrukog slanja (15), sigurnost upravljanja (16) i kriptografski algoritmi (17). Među ovih 17 domena vrlo je teško definisati jednu oblast koja je rizičnija od drugih. One se prilikom procjene cyber rizika ne mogu i ne trebaju tretirati kao nezavisne. Potencijalna prijetnja ili ma-

njak sigurnosti u jednoj može direktno ili indirektno utjecati na druge. Ipak, ako moram odabrat jednu, navest će onu koju već godinama promovišem u raznim industrijskim, a to je važnost balansiranja zaštite i detekcije. Zbog svega toga mislim da oblast "vidljivosti i konfigurabilnosti" ima najveću važnost kada su u pitanju funkcije detekcije integralnih sistema.

**a&s Adria:** Je li 5G siguran? Kako stručnici iz industrije i organizacija za standardizaciju mogu osigurati da se rizicima povezanim s 5G tehnologijom može efikasno upravljati u smislu sigurnosnih protokola i standarda i mehanizama provjere sigurnosti?

**Klein:** Kako rekoh, mnoge visokostručne zainteresovane strane, kao što su regulatori, proizvođači, operateri, akademsko osoblje, bile su uključene u definisanje 5G standarda i nastavljaju rad na dolazećim 3GPP standardima. Oni su doprinijeli postizanju visokog nivoa sigurnosti za definisanje 5G specifikacija. Ovakav saradnički pristup bio je inspiracija i prilikom kreiranja sistema provjere sigurnosti mrežne opreme (NESAS). Riječ je o okviru za kontrolu sigurnosti koji je dobro poznat u mobilnoj industriji. Globalno se koristi kao sigurnosna osnovica i uključuje zajedničke zahtjeve za sigurnosne procjene mrežne opreme i procjenu dobavljača telekomunikacijske opreme. NESAS pruža potrebne alate za osiguranje efikasnog testiranja i provjera. To je zajednički projekt organizacija 3GPP SA3 i GSMA, a uključuje i procjene na osnovu standarda za 5G sigurnost koje su dio sigurnosne provjere specifikacija (SCAS). Evaluaciju proizvoda vrše kompetentne laboratoriјe koje su akreditovane u skladu s ISO 17025. Zbog toga smo u Huaweiju jako ponosni na činjenicu da smo u decembru 2020. mogli objaviti da smo uspješno prošli prvu SCAS reviziju za 5G i LTE bazne stanice (reviziju koju je obavilo nezavisno tijelo DEKRA). To se desilo nakon uspješnog prolaska prve NESAS revizije na svijetu za 5G baznu stanicu koju je u maju 2020. uradio @sec.

**a&s Adria:** Većina prijetnji i izazova 5G sigurnosti istovjetna je onima s kojima se suočavala 4G tehnologija. No, treba užeti u obzir sigurnosne izazove koje nove usluge, arhitekture i tehnologije nose na 5G mrežama. Tu, naprimjer, spadaju autentifikacija pristupa za nezavisne pružače usluga dijeljenja, dijeljenje mreže, ar-

## Mehanizmi sigurnosne provjere

**a&s Adria:** Pristup "mnogo očiju i ruku" doprinosi većoj sigurnosti vaše opreme?

**Klein:** Naravno. U Huaweiju smo usvojili mehanizam sigurnosne provjere u stilu "mnogo očiju i ruku". Osim sigurnosnih testova linija proizvoda, uspostavili smo i Nezavisni laboratoriј za cyber sigurnost (ICSL), koji je nezavisan od sistema za istraživanje i razvoj. On je odgovoran za konačnu provjeru proizvoda. Rezultati testa direktno se šalju Globalnom uredu za cyber sigurnost i privatnost (GSPO), koji ima pravo veta na slanje proizvoda na tržište. Program testiranja i verifikacije koju provode nezavisna tijela realizuje se uz saradnju klijenata i industrijskih regulatora. Zato smo radi još veće transparentnosti otvorili testne centre u Velikoj Britaniji, Njemačkoj, Briselu i Kanadi kako bismo omogućili nezavisno testiranje Huaweijeve opreme, sve do nivoa izvornog koda. Mi vjerujemo u standarde cyber sigurnosti i objektivnu procjenu zasnovanu na činjenicama i dokazima.

hitektura zasnovana na uslugama (SBA), sigurna upotreba računarskih resursa, posebno u uvjetima šire primjene arhitekture oblaka u 5G svijetu i utjecaj novih tehnologija kao što je razvoj kvantnog računarstva. Možete li na jednostavan način opisati ove nove izazove?

**Klein:** S jedne strane, tačno je da 5G mreža nasleđuje sigurnosnu arhitekturu 4G mreže. Kao i prethodna generacija, 5G pristupne i jezgrene mreže imaju jasne granice, međusobno se povezuju putem standardnih protokola, podržavaju interoperabilnost različitih proizvođača i posjeduju mehanizme zaštite utemeljene na standardima. S druge strane, nesporno je i da će nove usluge i vidovi primjene donijeti nove izazove. Zato su dodatne mjere sigurnosti definisane i precizirane u 3GPP standardu. Ukratko, kao ključna poboljšanja u vezi s novim izazovima želim istaći četiri: (1) veća sigurnost bežičnog interfejsa koja nudi zaštitu integriteta korisničkih podataka. To ide u kombinaciji s postojećim šifriranjem korisničkih podataka u 2G, 3G i 4G mrežama, (2) naprednija zaštita privatnosti korisnika prenošenjem korisničkih ID-jeva (IMSI) u šifriranom tekstu u odnosu na 2G, 3G i 4G mreže, kod kojih se ove informacije prenose bežičnim putem u običnom tekstu, (3) veća sigurnost roaminga između operatera, pri čemu se napadače sprečava da iskorištavaju slabosti SS7 i neovlašteno manipulišu osjetljivim podacima (kao što su npr. ključ, korisnički ID i SMS), koji se razmjenjuju između osnovnih mreža različitih operatera, te (4) poboljšani kriptografski algoritmi s podrškom za 256-bitne algoritme, koji su dovoljno otporni na buduće napade kvantnim kompjuterima.

**a&s Adria:** Zašto je Huaweijev 5G sigu-

ran? Koje je tehničke prakse vaša kompanija primijenila kako bi garantovala da je njena oprema sigurna od hakerskih napada?

**Klein:** Prije svega želim naglasiti da navodi u medijima usmjereni protiv Huaweija nisu povezani s našim tehničkim pristupom ili načinom na koji rješavamo pitanje cyber sigurnosti prilikom dizajniranja i razvoja naših proizvoda. Huawei nije imao većih incidenta u pogledu cyber sigurnosti dok je sarađivao s više od 500 pružalaca telekomunikacijskih usluga, uključujući većinu od 50 najvećih telekom operatora. Takva je situacija bila u proteklih skoro 20 godina u 170 zemalja, u kojima je povezano više od 3 milijarde ljudi. Nijedan drugi proizvođač ne može reći da je postigao ovaj nivo uspješnosti u cyber sigurnosti. Možemo čista srca reći da je Huawei danas kompanija koja je pod najvećom prizmom na svijetu. Zbog toga se gotovo opsensivno bavimo strogim pravilima koja smo donijeli za svoje zaposlenike, dobavljače i razvojne procese. To je zato što, za razliku od drugih, shvatamo da bi nam došao kraj ako bi se desio i jedan sigurnosni incident koji bi uključio Huawei.

Konkretno, u Huaweiju su istraživanje i razvoj fokusirani na sigurnost tokom razvoja proizvoda, uz pridržavanje principa sigurnosti ugrađene u dizajn i sigurnosti u procesu. Aktivnosti na planu cyber sigurnosti ugrađene u ovaj proces izvode se uz strogo praćenje usklađenosti tokom cijelog životnog ciklusa proizvoda. To znači da se sigurnosni zahtjevi mogu implementirati u svakoj fazi. Istraživanje i razvoj u Huaweiju osigurava postupak integriranog razvoja proizvoda (IPD). To se radi s ciljem usmjeravanja razvoja cijelovitog (E2E) proizvoda u skladu s

industrijskim sigurnosnim praksama i standardima kao što su OWASP-ov model provjere sigurnosti softvera (OpenSAMM), sistem jačanja sigurnosti kroz provjeru zrelosti tehnologije (BSIMM), Microsoftov životni ciklus razvoja sigurnosti (SDL) i Okvir za cyber sigurnost američkog Nacionalnog instituta za standarde i tehnologiju (NIST CSF), kao i zahtjevi korisnika i država u pogledu cyber sigurnosti.

**a&s Adria:** Kako osigurati 5G opremu od cyber napada, uključujući Huaweijevu podršku za cyber zaštitu i preporuke o načinu instalacije i upravljanja 5G mreža-ma na siguran način?

**Klein:** Huawei se zalaže za zaštitu povjerenljivosti, integriteta, dostupnosti, sljedivosti i privatnosti korisnika 5G opreme na bazi 3GPP sigurnosnih standarda. Osim toga, kompanija zagovara i saradnju s operaterima u kreiranju visokog stepena cyber otpornosti na mrežama iz perspektive upravljanja i održavanja (O&M). Na primjer, da bi se ubrzao oporavak usluge u slučaju da se desi sigurnosni incident, tehnički dizajn mora ponuditi kontinuirano praćenje i reagovanje na incidente tako da se njihov opseg utjecaja i prateći gubitak usluge mogu svesti na minimum. Huawei, kao proizvođač, koristi IPDRR metodologiju, koja se bazira na identificiranju, zaštiti, otkrivanju, odgovoru i oporavku, a u skladu s NIST CSF okvirom za cyber sigurnost. Metodologija se koristi za identifikaciju i kontrolu ključnih rizika u mrežnim uslugama i jačanje cyber otpornosti operatera. Korištenjem IPDRR metodologije Huawei može pomoći operaterima koji pružaju kritičnu informacijsku infrastrukturu da kvalitetnije ispune regulatorne zahtjeve u pogledu cyber sigurnosti. Osim mrežne sigurnosne arhitekture, potreban je i sveobuhvatan i siguran skup pravila koje operateri moraju slijediti kako bi upravljali O&M nivoom upravljanja i održavanja. On je presudan u kontroli rizika na cijeloj mreži. Zato se za svaki zadatak u ovom segmentu moraju primjenjivati stroga sigurnosna pravila,

## Povjerenje se temelji na činjenicama

**a&s Adria:** Šta je Huawei učinio na polju transparentnosti nivoa cyber sigurnosti svoje opreme i rješenja?

**Klein:** Povjerenje je osjećaj. Ali kada je u pitanju cyber sigurnost, i povjerenje i ne-povjerenje trebaju se temeljiti na činjenicama, a ne na osjećajima, nagađanjima i neutemeljenim glasinama. Vjerujemo da činjenice moraju biti provjerljive, a provjera mora biti zasnovana na standardima. Zbog toga je Huawei otvorio Centar za transparentnost cyber sigurnosti u Briselu. Ovo je dobar i konkretni primjer kako podizamo nivo transparentnosti. Našim kupcima i nezavisnim laboratorijama dajemo pristup našem izvornom kodu i omogućavamo im da ocjenjuju naša rješenja koristeći vlastite alate, osoblje i procese. Transparentnost je neophodna jer je u osnovi pouzdanosti. Historija ICT industrije pokazala je da nejasnost u pogledu sigurnosti nikada nije bila pravi izbor. U Huaweiju vjerujemo da postojimo da bismo služili našim kupcima i oni imaju pravo da zahtijevaju i zaslžuju visok nivo transparentnosti.

s nultom tolerancijom na greške tokom obrade tokova podataka.

**a&s Adria:** Kako kontinuirano poboljšavati nivo sigurnosti 5G mreže iz perspektive različitih zainteresovanih strana kako bi se rješili budući izazovi?

**Klein:** 5G postaje stvarnost, koja će trajati još dugo. Na osnovu iskustva u 4G sigurnosti mogu kazati da se kontrola rizika 5G mreže može postići zajedničkim naporima svih industrija. Moramo kontinuirano unapređivati sigurnosna rješenja tehnološkim inovacijama i graditi sigurne sisteme i mreže kroz standarde i saradnju ekosistema. Kao proizvođači i dobavljači, trebali bismo nastaviti doprinositi radu industrijskog sigurnosnog standarda, uskladiti proizvodnju sa standardima i integrirati sigurnosne tehnologije. Nakon toga, operateri su odgovorni za sigurno poslovanje i otpornost vlastitih mreža na cyber napade. 5G mreže su privatne. Granice između različitih mreža su jasne. Operateri mogu sprječiti vanjske napade pomoću firewalla i sigurnih gatewaya. Kada je riječ o internim prijetnjama, operateri mogu upravljati, nadzirati i revidirati sve dobavljače i partnere kako bi sve elementi njihove mreže učinili sigurnim. Na kraju, kao industrija, svi moramo raditi na standardima. Ovo je naša zajednička odgovornost. Da bismo

izgradili sistem u koji svi možemo vjerovati, trebaju nam definisane odgovornosti, jedinstveni standardi te jasna i nediskriminatorna regulativa.

**a&s Adria:** Nedavno ste kao predavač na Virtual Security Summitu spomenuli nekoliko velikih sigurnosnih izazova s kojima se suočavamo u domenu razvoja softvera, među kojima je i potreba za standardom za siguran razvoj. Je li Evropski zakon o kibernetičkoj sigurnosti postavio dobre temelje za to?

**Klein:** Mislim da svi, kao ICT industrija, moramo raditi zajedno kako bismo unaprijedili svoju cyber sigurnost i digitalnu otpornost. Samo zajedničkim radom i koordinacijom napora na evropskom nivou, ali i šire, možemo se uspješno nositi s budućim prijetnjama. Industriji nedostaje jedinstven set tehničkih standarda za sigurnost, a stanje je isuviše fragmentirano. I zato vjerujem da nedavni evropski Zakon o kibernetičkoj sigurnosti može i hoće donijeti jasnou dodatnu vrijednost na ovom polju. Donošenjem GDPR-a Evropa je već pokazala da, kada se postigne konzensus država članica, ona može utrti put globalno prihvaćenim sigurnosnim pravilima i smjernicama. Štavše, Agencija Evropske unije za cyber sigurnost (ENISA) također je temeljitim i sveobuhvatnim publikacijama, kao što je "Dobre prakse za sigurnost IoT-a – siguran životni ciklus razvoja softvera", koja je objavljena u novembru 2019. godine, pokazala da posjeduje stručnost da vodi industriju kada je u pitanju siguran razvoj softvera.

**a&s Adria:** Prema Vašem mišljenju, softverska industrija ulaže snažne napore u certificiranje proizvoda, ali ne i u procje-

**Jedna od naših osnovnih vrijednosti je rast pogonjen akumuliranim iskustvom i promišljanjem. Zbog toga je dijeljenje i razmjena informacija s trećim stranama tokom cijelog razvoja proizvoda i prihvatanje izazova od vitalnog značaja.**



nu samog procesa. Kako možemo balansirati između to dvoje i zašto je evaluacija procesa podjednako važna?

**Klein:** Ne kažem da softverska industrija ne evaluira sam proces, već da je količina napora uložena u certificiranje proizvoda i procjenu procesa nejednaka. Očigledan način da se to promijeni je da se u sadašnjim i budućim standardima jača dio evaluacije razvojnog procesa. Ne treba izmišljati topalu vodu. Već postoje smjernice poput BSIMM-a ili SDLC-a. Zapravo sam vrlo zadovoljan kad vidim da Evropski zakon o kibernetičkoj sigurnosti uključuje procjenu procesa. Još jedan dobar primjer je NESAS, koji obuhvata evaluaciju nekih ključnih procesa (npr. rješiti ranjivosti koje se pojavljuju tokom životnog ciklusa proizvoda). Izazov je kako izbjegći dodavanje dodatnog tereta ionako velikim zahtjevima vezanim za certificiranje. No, optimističan sam jer vjerujem da evaluiranje i eventualno jačanje pouzdanosti u razvojnim procesi-

## U Huaweiju su istraživanje i razvoj fokusirani na sigurnost tokom razvoja proizvoda, uz pridržavanje principa sigurnosti ugrađene u dizajn i sigurnosti u razvojnom procesu

ma može pomoći u smanjenju napora za ponovnu certifikaciju.

**a&s Adria:** Treće strane moraju igrati ključnu ulogu u omogućavanju sigurnog razvoja, budući da su partner ne samo na kraju već i tokom procesa razvoja proizvoda. Kako je Huawei ovo implementirao kroz svoj integrirani razvoj proizvoda (IPD)?

**Klein:** Pravilno prikupljanje povratnih informacija neophodno je za plodnu saradnju. Jedna od naših osnovnih vrijednosti je rast pogonjen akumuliranim iskustvom i promišljanjem. Zbog toga je dijeljenje i razmjena informacija s trećim stranama tokom cijelog razvoja proizvoda i prihvatanje izazova od vitalnog značaja.

To potiče naš kontinuirani proces usavršavanja. Konkretno, u našem IPD-u imamo namjenski proces koji nazivamo "upravljanje zatvorenom petljom". Iskoristavanje povratnih informacija podrazumijeva i primjenu adekvatnog modela upravljanja. Kombinovani pristup od vrha prema dolje i odozdo prema gore je najefikasniji način za uspješno korištenje povratnih informacija trećih strana. Kao primjer rezultata, prije nekoliko godina smo pokrenuli novi program softverskog inžinjeringu. Uspostavili smo kontinuiran i konstruktivan dijalog sa zainteresovanim stranama da bismo shvatili kako možemo dodatno unaprijediti razvoj softvera, a sada te promjene primjenjujemo u našoj organizaciji. ◀

S rastom pametnih zgrada

# MODERNIZACIJA VATRODOJAVE

ZA RAZLIKU OD DRUGIH INDUSTRIJA, POTRAŽNJA ZA ZAŠTITOM OD POŽARA NE JENJAVA ZBOG NJENE ULOGE U SPAŠAVANJU ŽIVOTA. PREMA ISTRAŽIVANJU VIŠE AGENCIJA, TO BI TRŽIŠTE MOGLO ZABILJEŽITI STABILAN RAST U NAREDNIM GODINAMA BUDUĆI DA VLADE ŠIROM SVIJETA ŽELE POOŠTRITI REGULATIVE I POVEĆATI SIGURNOST. NO, DANAS SE MODERNIZIRAJU I SAME ZGRADE KOJE SE TREBAJU ZAŠTITITI

■ Izvor: a&s International  
redakcija@asadria.com

**Tržište pametnih** zgrada će, kako navodi Fortune Business Insights, rasti po složenoj godišnjoj stopi od 12,6 posto do 2026. godine. Napori na smanjenju emisije ugljika i stvaranju energijski efikasnijih zgrada mogli bi biti glavni pokretač. A kako raste broj pametnih zgrada tako se povećava i potreba za njihovom zaštitom od požara. Dugo vremena razvoj u sektoru zaštite od požara nije bio brz kao u videonadzoru ili drugim oblastima

sigurnosti. Tome je doprinijelo nekoliko faktora, od zadovoljstva kupaca onime što već imaju do slabog interesa za ulaganje u ovaj segment. Međutim, sada se vide značajne promjene u zaštiti od požara, među kojima je sve veća digitalizacija. Zbog toga bi industrija zaštite od požara trebala sve više usvajati pametnu tehnologiju.

## Brže usvajanje IP-a

“Zaštita od požara se tokom posljednje decenije transformirala rastom adresabilnih uređaja zasnovanih na IP-u unutar umrežene infrastrukture sistema za do-

javu požara”, kaže Andreas Kahl, voditelj softverskog inžinjeringu i vatrodojavnih sistema u Bosch Building Technologies. “Skalabilnost i modularna arhitektura digitalnih sistema za vatrodojavu otključali su novu razinu zaštite, npr. određivanjem tačnog mesta aktiviranog detektora dima u alarmnoj situaciji ili povezivanjem sa sistemima razglosa za faznu evakuaciju zgrada. Za sistem-integratora instalacija i održavanje alarmnih sistema dostigli su novi nivo efikasnosti – uključujući automatizirana servisna upozorenja i mnogo manje lažnih alarma – uz veliku uštedu troškova”, objašnjava on.





Andreas Kahl, voda razvoja softvera i protupožarnih alarm sistema u Bosch Building Technologies



Ray Dotts, projektni menadžer u Telgian Engineering and Consulting



Rodger Reiswig, saradnik i potpredsjednik za industrijske odnose u Johnson Control



Thomas Dols, globalni projektni menadžer u Siemens Smart Infrastructure

## Prelazak na IoT

Kahl kaže da će uskoro sve veći broj umreženih vatrodojavnih sistema biti povezan s internetom stvari (IoT). To je dio većeg trenda u svim industrijama, uključujući pametne domove i pametne zgrade automatizirane kombinacijom podataka prikupljenih pomoću senzora i vještacke inteligencije (AI). Očekuje se da će broj IoT povezanih uređaja u svijetu premašiti 14 milijardi do 2022. godine, što je više od polovine od 28,5 milijardi povezanih uređaja na svijetu.

## Adresabilni uređaji za slanje obavijesti

Jedno od najznačajnijih dostignuća u sistemima za zaštitu života je adresabilno obavlještavanje. Prema Rodgeru Reiswigu, potpredsjedniku kompanije Johnson Controls, iako industrija već nekoliko decenija ima adresabilne ulazne uređaje za vatrodojavu, uređaji za obavlještavanje su to počeli pratiti tek prije nekoliko godina. "Budući da se notifikacijski uređaji, uključujući sirene i zvučnike, sada mogu adresirati, njihova mogućnost da se selektivno aktiviraju softverom, a ne načinom na koji su fizički ožičeni, pruža veću fleksibilnost vlasniku ili upravitelju zgrade. Također, uz selektivnu kontrolu takvi uređaji mogu izvršiti automatizirano samotestiranje. U osnovi, ako se uređaj može samostalno funkcionalno testirati, oponašati funkcionalni test, prijaviti je li prošao ili nije i izvesti to u istom intervalu koji zahtijeva NFPA 72, tada se to smatra ekvivalentnim slanju osobe da testira svaki uređaj. Ova mogućnost nudi vlasniku ili upravitelju mogućnost testiranja svog sistema mnogo brže i uz znatno manje ometanja stanara", rekao je Reiswig.

## Komunikacija je ključna za zaštitu od požara. Značajna promjena kroz koju industrija trenutno prolazi je prestanak korištenja telefonskih linija u centralnim nadzornim stanicama

### Novi komunikacijski sistemi

Komunikacija je ključna za zaštitu od požara. Značajna promjena kroz koju industrija trenutno prolazi je prestanak korištenja telefonskih linija u centralnim nadzornim stanicama kako se analogno prenošenje telefonskog signala ukida. Mobilni i IP komunikatori su tehnologija koja se trenutno najviše koristi. "Sistem koji nije vatrodojavni, ali često spada pod odgovornost izvođača vatrodojavnih sistema, je ERRCS, radiosistem za hitne slučajeve. Ovi sistemski zahtjevi se iz dana u dan sve više provode. Hitna pomoć, policija i vatrogasci ovise o radiokomunikacijama, a ako komunikacije u zgradbi ne rade, životi su ugroženi", rekao je Ray Dotts, projektni menadžer u Telgian Engineering and Consultingu.

### Rastuća uloga IoT-a u zaštiti od požara

Nema sumnje da IoT polako revolucionizira većinu tradicionalnih industrija. Prema Thomasu Dolsu, način na koji radimo, štitimo se od požara i pružamo usluge zaštite od požara promijenio se tokom posljednjih godina. "Digitalizacija je pokrenula ovu promjenu, pretvarajući tradicionalnu zaštitu od požara u moderni i produktivan biznis. S ovom novom ponudom smo u srcu IoT-a, s jasnim ciljem da sigurno povežemo što više naših proizvoda za zaštitu od požara. Za kupce će to značiti bolje korištenje stručnjaka u

tom segmentu, bolji servis, pa čak i nove poslovne mogućnosti", rekao je Dols.

### Prednosti IoT-a

Internet stvari omogućio je sistemima za zaštitu života da se povežu sa svijetom. Vlasnici ili upravitelji zgrada sada se mogu povezati sa svojim sigurnosnim sistemima s bilo kojeg mesta na svijetu telefonom, tabletom ili bilo kojim povezanim uređajem. "lako se sistemi mogu povezati sa svijetom, ipak moramo postaviti pitanje – može li se sistem kompromitovati zlonamjernim aktivnostima hakera? Zbog toga moraju biti primjenjene zaštitne mjere kako bi se spriječila preuzimanja te vrste. Ovo je postalo pitanje kojim se bave Underwriters Laboratory i Nacionalna asocijacija za zaštitu od požara i poduzimaju mjere kako bi primijenili cyber sigurnosne standarde i instalacijske prakse", rekao je Rodger Reiswig, potpredsjednik za industrijske odnose u Johnson Controlsu. Vlasnici i upravitelji objekata sada mogu integrisati svoje sigurnosne sisteme bez potrebe da budu na lokaciji, što štodi vrijeme i resurse, ali i dozvoliti instalateru ili serviseru da to učini i dijagnosticira bilo kakav problem prije nego što uopće dođe na mjesto događaja.

Većina velikih kompanija istražuje šta još mogu učiniti da iskoriste snagu IoT-a. Bosch je, naprimjer, postavio strateški cilj da sve kategorije elektronskih proizvo-



da podržavaju IoT do kraja 2020. Riječ je o tzv. 3S viziji povezivanja: senzora, softvera i usluga (services). Razvijajući i implementirajući usluge i rješenja za povezani svijet, Boschevi kupci imaju koristi od stručnosti te kompanije u razvoju softvera i senzorskoj tehnologiji, kao i širokog portfolija njenih usluga i proizvoda. "Što se tiče uvođenja IoT-a u segment zaštite od požara, Bosch ima viziju budućnosti u kojoj povezani uređaji i njihovi podaci otvaraju nove vrste usluga koje krajnjim kupcima i sistem-integratorima nude značajne prednosti. Ovo putovanje ka digitalnoj transformaciji već je uveliko u toku, jer IoT aplikacije već unapređuju usluge zaštite od požara na nekoliko načina. Kao preduslov, mrežna arhitektura sistema, koji čine vatrodojavne centralne i senzori, mora se na siguran način povezati s internetom putem pristupnih čvorista, hubova i gatewaya. S ovakvom konekcijom, sistem može komunicirati s poslužiteljem aplikacija u oblaku putem IP protokola za slanje podataka u stvarnom vremenu, poput onih o stanju uređaja, potrošenosti baterije i liste događaja", rekao je Andreas Kahl, voditelj softverskog inženjerstva i vatrodojavnih sistema u kompaniji Bosch Building Technologies. Iako IoT usluge daljinskog upravljanja integratorima već omogućavaju veću efikasnost, tek grebemo po površini moguće ga. Temelj za sljedeću generaciju usluga povezanih u internet stvari izliven je već

## Cloud rješenja

Rješenja bazirana na cloudu sada prodiru u svaki segment, a industrija zaštite od požara nije iznimka. Prema Thomasu Dolsu, globalnom menadžeru softverskih proizvoda u Siemens Smart Infrastructureu, najviši nivo zaštite objekta od požara je brza, pouzdana i pametna komunikacija vatrodojavnog sistema i interfejsa koji prikuplja podatke. "Sve počinje omogućavanjem da su svi podaci kontinuirano dostupni na daljinu, tako da se rad sistema može nadzirati i njime upravljati putem bilo kojeg računara, laptopa ili mobilnog uređaja – bilo kada i bilo gdje", rekao je Dols.

danasa kako se povećava integracija između senzora, softvera i usluga. Da bi se ostvarila prednost u odnosu na konkurenčiju, neće biti presudno samo da uređaji rade međusobno unutar iste mreže već i da se u procesu izgradnje cijelovitih vatrodojavnih sistema spremnih za povezivanje s IoT-om omogući bespriječorna integracija s aplikacijama i platformama trećih strana putem API-ja. Bit će još važnije da sistemi mogu komunicirati s aplikacijama ili softverom za upravljanje zgradama. Istovremeno, sposobnost pružanja integrisanih IoT usluga, sigurnih od hakera i zlonamernih napada, bit će nezamjenjiva, jer su sistemski podaci najvažniji resurs. Ti podaci sadrže ključ za ono što slijedi.

## Važnost videonadzora u vatrodojavni

Pomoću kamere centralna nadzorna stanica može vidjeti požar. Nakon oba-

vještavanja vatrogasne službe sistem će prenijeti relevantne informacije, poput činjenice da je riječ o stvarnom požaru, njegovoj veličini i tačnoj lokaciji, tako da vatrogasci mogu znati gdje trebaju doći i adekvatno se spremiti za gašenje vatre.

Najvažnija prednost upotrebe nadzornih kamera za potvrdu požara je smanjenje broja lažnih uzbuna. Međutim, upotreba ovog rješenja kupcu nudi i više. Tradicionalni sistemi za otkrivanje požara rade samo kad dim ili toplota dođu do senzora, koji su najčešće postavljeni na plafonu. Kamere, s druge strane, mogu otkriti požar netom nakon što izbije i ubrzati odgovor najmanje nekoliko sekundi. "Detekcija požara putem videa je mnogo brža u usporedbi sa standardnim vatrodojavnim rješenjima, jer se požar može otkriti direktno na izvoru, što omogućuje pokretanje alarmu mnogo ranije. Uz to, takve se kamere mogu instalirati na mjestima



**Najočitija prednost upotrebe nadzornih kamera za provjeru požara je smanjenje broja lažnih alarma. Međutim, upotreba ovog rješenja kupcu nudi više. Kamere mogu otkriti požar netom nakon što izbije i pružiti barem nekoliko sekundi dodatnog vremena za odgovor**

na kojima se konvencionalni sistemi ne mogu efektivno koristiti, poput prašnjavog i vlažnog okruženja ili u zgradama s visokim plafonima ili na otvorenim površinama. Videosnimak omogućava jednostavan način potvrde alarmu", objašnjava Theresa Grunewald, menadžerica za globalni razvoj poslovanja za AVIOTEC u Bosch Building Technologies. Videoverifikacija se tradicionalno koristi u svijetu sigurnosti, ali se tek počela koristiti u vatrodajavnim sistemima.

#### Zakonski propisi

Propisi o protivpožarnoj sigurnosti razlikuju se od države do države, a pri korištenju bilo koje nove tehnologije postoji određena zabuna u vezi s njenom pravnom valjanosti. Reiswig je objasnio da je NFPA 72 prvi počeo rješavati ove probleme provjerom s nadzornom stanicom. Ako nadležna vlast odobri, postoji mogućnost da kompanija za nadzor protivpožarnog sistema prvo kontaktira vlasnika imovine, i ako on potvrdi da postoji potreba, nadzorna stanica može pozvati vatrogasce da preduzmu određene mjere. Naravno, protivpožarna zaštita uglavnom je tradicionalna industrija u kojoj su rješenja poput kamera još u početnoj fazi. Za Reiswig je ovo dobar početak, ali i dokaz da je putovanje tek počelo. "Treba se desiti još mnogo toga, ali ovo je osnova za provjeravanje alarma. Videoverifikacija sljedeći je korak ka većoj sigurnosti.

Važno je imati na umu da su vatrodajjni sistemi postali više sistemi za zaštitu života jer detektuju plin, integrišu liftove, šalju masovne obavijesti itd.", rekao je Reiswig.

Izraz "pametne zgrade" ljudi različito poimaju. Reiswig objašnjava da je za neke to samo "zelena inicijativa", tj. da li zgrada ima mogućnost da bude samodrživa i smanji emisiju ugljika, može li ponovo iskoristiti vodu i generisati električnu energiju pomoću solarnih ćelija i

vjetroturbina. Druga definicija pametnih zgrada temelji se na senzorima: je li zgrada dovoljno pametna da zna uključiti ventilaciju, klimatizaciju i grijanje nakon što prva osoba ujutro provuče karticu, može li samostalno paliti svjetla, može li prilagoditi žaluzine tako da dopusti ulazak sunca, može li pozvati lift, jer zna da je osoba u predvorju i da ide na deseti sprat? Sve je u tome kako se sistemi međusobno integrišu, ne samo razmjenjuju informacije već i komuniciraju,





uzrokujući pokretanje lanca događaja iz sistema u sistem.

## Element pametnog u vatrodojaví?

IP vatrodojava je posljednji krik tehnologije. Umreženi u digitalnu infrastrukturu, adresabilni sistemi, sačinjeni od centrala i detektora, pružaju zaštitu od požara u najranijoj fazi, a uz to daju i tačnu lokaciju izvora požara i integrišu se sa drugim bitnim sistemima, kakvi su prskalice, videonadzor i kontrola pristupa. Također, mogu se kombinovati sa sistemom za glasovnu evakuaciju kako bi se ljudi brže i preciznije sklonili iz opasnih područja. "IP vatrodojavni sistemi su skalabilni i lako prilagodljivi zahtjevima kupaca. Za maksimalnu pouzdanost IP sistemi potpuno podržavaju redundantno umrežavanje putem IP-a i/ili CAN veze između centrala, čime sistem održava operativnim u slučaju greške. Kao uobičajen korak, IP vatrodojavni sistemi integrišu se u arhitekturu sistema za upravljanje zgradama kao što je Boschev sistem za integraciju objekata (BIS) ili neko rješenje treće strane kako bi operatorima pružili jedinstven pregled i uvid u stvarnom vremenu", kaže Andreas Khal. Za centralizirano upravljanje zgradama vatrodojavni sistem u pametnoj zgradi mora se povezati s drugim sistemima kao što su videonadzor, kontrola pristupa i razglas. Spoj vatrodojave i glasovne evakuacije postao je uobičajen

tokom posljednjih nekoliko godina na velikom broju lokacija, od hotela do trgovачkih centara i aerodroma. Studije su pokazale da glasovni alarm s jasnim uputama znatno skraćuje vrijeme evakuacije za vrijeme požara u usporedbi sa standardnim alarmima i čak do 30 posto ubrzava reakciju timova za hitne intervencije.

## Popularnost zaštite od požara u pametnim zgradama

Reiswig ističe da njegova kompanija već nekoliko godina radi integraciju sa sistemima za ventilaciju, klimatizaciju i grijanje ili, pak, rasvjetu. Sada, naprimjer, mogu koristiti položaj sunca kako bi maksimalno iskoristili sunčevu svjetlost da zimi zagrijavaju zgradu. "Jedan od najvećih izazova u pametnim objektima su protokoli ili topologije na osnovu kojih jedan sistem komunicira s drugim. Vatrodojavni sistem koristi određeni protokol ili jezik, HVAC neki drugi. Stvaranje okruženja u kojem sistemi mogu međusobno komunicirati i ne samo slati već i primati informacije je teži dio", kaže Reiswig.

## Kako bi se upravitelji trebali pripremiti za budućnost

Prije ulaganja u nove sisteme zaštite od požara upraviteljima zgrada se savjetuje da razmotre održivost svojih sistema u budućnosti, a tu se IT arhitekture na-

hode kao jedini put naprijed. "Trenutna legislativa, poput Međunarodnog vatrogasnog zakona iz 2015. godine, već propisuje adresabilne sisteme u kojima umreženi uređaji mogu signalizirati svoj tip uređaja, lokaciju i status upozorenja. Što se tiče održivosti, IT vatrodojavni sistemi mogu besprijekorno integrisati sljedeću generaciju videonadzornih uređaja za otkrivanje požara koji se oslanaju na algoritme mašinskog učenja za otkrivanje vatre i dima u manje od 30 sekundi", kaže Kahl. Istovremeno, operateri će možda htjeti prilagoditi svoja rješenja i integrisati ih u svoje sisteme za upravljanje zgradama, što se može olakšati pomoću paketa za razvoj softvera (SDK) kao što je interfejs Boschevog vatrodojavnog sistema (FSI) ili otvorenih IT standarda poput OPC-a. Osim ovog nivoa održive integracije, IP rješenja lako se prilagođavaju proširenjima zgrade ili instalacijama u više objekata.

## U konačnici

U srži pametne zgrade je umreženost, kaže Thomas Dols. Živimo u digitalnom dobu punom novih informacija, gdje se performanse stalno poboljšavaju pomoću podataka, a interakcije s pametnim interfejsima nam pomažu da donosimo pametnije odluke. Ova potreba za stalnom optimizacijom leži u srcu pametnih zgrada, čija je svrha poboljšati korisničko iskustvo. ◀

Pet-friendly kamere

# SIGURNIJI DOM ZA KUĆNE LJUBIMCE

**ZAŠTO SU KAMERE ZA NADZOR KUĆNIH LJUBIMACA POSTALE VAŽNE NJIHOVIM VLASNICIMA, KAKVE OPCIJE NUDE I DA LI ZAISTA MOGU POMOĆI UKOLIKO IH ODLUČITE INSTALIRATI U SVOM DOMU, PROČITAJTE U NASTAVKU TEKSTA**



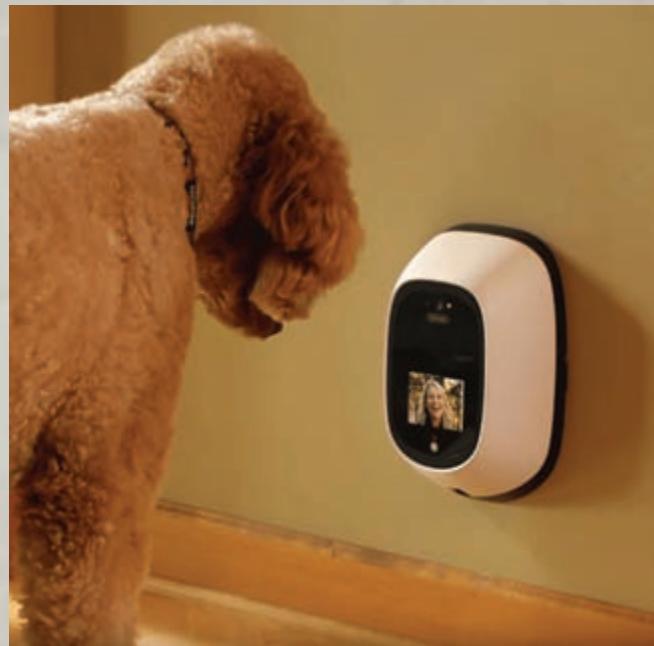
■ Piše: Vesna Matić Karić  
redakcija@asadria.com

**Iz straha** da duži boravak vlasnika van kuće može izazvati određenu dozu stresa kućnog ljubimcu, vlasnici ih često odlučuju ostavljati same kod kuće. U tom slučaju pas, koji je izrazito društvena životinja, često reagira na načine koji mogu uključivati i uništavanje imovine, pa se mogućnost nadgledanja i kontrole kućnog ljubimca čini veoma korisnom. S obzirom na to da živimo u moderno vrijeme, tu na scenu stupaju kamere namijenjene za kućne ljubimce. One ne samo da vlasnicima omogućavaju da ih stalno nadziru već imaju i dvosmjerni audiosignal zahvaljujući kojem je moguća i komunikacija. Vlasnici tako mogu svoje ljubimce umiriti ukoliko su uplašeni ili uzremeni, a mogu jednostavno detektovati i postojanje bilo kojeg drugog problema. Pošto na tržištu postoji veći broj ovih kamera, najbitnije je da vlasnici razmisle šta im tačno treba i da, u zavisnosti od svojih potreba, izaberu onu koja će im najviše odgovarati.

### Na šta obratiti pažnju

Postoji nekoliko osnovnih funkcija koje kamere za nadzor kućnih ljubimaca nude: detekciju pokreta, daljinski video nadzor putem mobilne aplikacije, dvosmjerni audiosignal, noćno snimanje, Wi-Fi konekciju i PTZ funkcionalnost. Prije svega, treba obratiti pažnju na rezoluciju i ugao snimanja, jer se oni razlikuju od kamere do kamere. Tako, naprimjer, ako imate mladog i razigranog kućnog ljubimca, ugao snimanja je bitna stavka jer pokazuje koliko je vidno polje kamere. Što je veći ugao snimanja, to više njegovih aktivnosti može pokriti. S druge strane, ako imate starijeg kućnog ljubimca, koji se baš i ne kreće previše, onda ugao snimanja nije od presudne važnosti kod izbora kamere.

Kada ste to pokrili, bitno je da kamera ima i dvosmjerni sistem komunikacije koji smo na početku teksta već spominjali, jer mogućnost da samo vidite šta vaš pas radi više nije dovoljna. Pošto sada imate i kamere sa zvučnikom i mikrofonom, zašto ne iskoristiti pogodnosti "razgovora" s njim u slučaju da je to neophodno ili nešto što jednostavno želite? Opcija noćnog snimanja idealna je za ljudе koji često rade noćne smjene i žele provjeriti kako se njihov ljubimac snalazi dok je sam u stanu, a nudi mogućnost snimanja i nadziranja čak i u uslovima slabe vidljivosti. I, naravno, tu je još i dodatak u vidu senzora pokreta i zvuka, koji funkcioniše tako da dobijate upozorenja putem mobilne aplikacije u slučaju da senzori zabilježe sumnjivo kretanje ili zvukove.



### Pohrana podataka

Još jedna bitna stavka na koju vrijedi obratiti pažnju pri kupovini ovih kamera jeste način pohrane podataka, jer vjerovatno snimljeni materijal nećete moći provjeravati baš svakog dana. Zato su u ponudi tri opcije: čuvanje zapisa u cloudu, na SD kartici ili internoj flash memoriji. Na vama je da izaberete najbolju opciju za vas i vaše potrebe. Ako se nećkate oko neophodnih opcija, samo da nglasimo da stručnjaci iz oblasti veterine najveći naglasak stavljuju na dobru rezoluciju i dvosmjernu komunikaciju, jer se zahvaljujući njoj briše fizička barijera između vlasnika i kućnog ljubimca, tako da trebate i to uzeti u obzir.

### Sigurnosna kamera ili nešto drugo?

Prije nego što krenemo pojašnjavati specifikacije kamera namijenjenih nadzoru kućnih ljubimaca, prvo želimo pojasniti razliku između sigurnosnih kamera i onih o kojima u ovom tekstu pišemo. Jer, možda bi neko pomislio: a zašto bih ja kupio kameru koja će snimati mog psa kada mogu uzeti standardnu sigurnosnu kameru i tako ubiti dvije muhe jednim udarcem? Poenta je u sljedećem:

## Kamere za kućne ljubimce kao pomoć pri osiguranju

Kada je riječ o Sjedinjenim Američkim Državama, zanimljivo je istaći da mnogi posjednici kuća dobijaju i popust kod osiguravajućih kuća ukoliko imaju uređaje koji smanjuju rizik od nanošenja štete domu. To može uključivati protivprovalna vrata, ali i instaliranje sigurnosnih ili, u ovom slučaju, kamere namijenjenih nadgledanju kućnih ljubimaca. Čak i ako ne živate u Americi, zgodno bi bilo provjeriti s osiguravajućom kućom da li nude popuste ukoliko imate neki nadzorni sistem, jer biste u tom slučaju mogli uštedjeti dosta novca, a istovremeno biste učinili nešto dobro za svog kućnog ljubimca.

iako vam sigurnosne kamere omogućavaju da pratite i snimate svog kućnog ljubimca dok niste kod kuće, one ne mogu učiniti ništa na uspostavljanju odnosa s njim, što, pretpostavljamo, želite. Moderne kamere za kućne ljubimce vam omogućavaju da im se obraćate, da se gledate preko kamere, a neke čak imaju i opciju da s vremena na vrijeme izbace poslasticu za vašeg četveronožnog člana porodice. One mogu rješiti problem anksioznosti kod ljubimca ili dosade jer je predugo ostavljen sam, što nerijetko dovodi i do pojave uništavanja namještaja, odjeće, obuće itd. Da ne govorimo o porastu nivoa stresa koje neki ljubimci doživljavaju kada su ostavljeni sami. U nastavku donosimo kamere koje se mogu naći na tržištu.

### Furbo

Ova kamera je namijenjena i kreirana isključivo za pse, a u sebi sadrži i Amazonovog glasovnog asistenta Alexa. Kamera vlasnicima šalje upozorenje u stvarnom vremenu svaki put kada njihov pas počne lajati (tzv. barking alert), s tim da možete podešiti nivo osjetljivosti samog upozorenja, a možete i filtrirati druge zvukove kako bi se spriječila njegovaa bespotrebna aktivacija. Treba naglasiti da vam kamera neće slati notifikacije svaki put kada vaš pas zalaje, jer bi to bilo suludo. Riječ je o tome da je kamera u stanju prepozнатi kada vaš pas laje jer je u nevolji ili je nesretan, tako da tek u tim slučajevima dobijate notifikaciju ili upozorenje, a sve to bez prijeke potrebe za konstantnim nadgledanjem.

Kao što smo ranije u tekstu već napomenuli, neke kamere imaju sposobnost da vašem ljubimcu dobace igračku ili neku poslasticu, a Furbo je upravo jedna od njih. Prije nego što izbaci poslasticu, kamera će pustiti zvuk "klik-klik" (što se u praksi zove click trening), što znači da zahvaljujući njoj možete trenirati svog psa da prepoznae zvuk i šta slijedi nakon njega. Furbo nudi još neke usluge uz



### Pawbo+

Pawbo je dizajnirana tako da nadgleda pse i mačke, a uključuje HD video feed, dvosmjerni komunikacijski sistem, a tu je i opcija za instantno dijeljenje fotografija vašeg ljubimca na društvenim mrežama. A kako se on ne bi previše ulijenio dok vi niste tu, Pawbo se pobrinuo da ima lasersku igru ugrađenu u svoj sistem, mada treba imati na umu da se u prošlosti ovakve igre nisu preporučivale psima, ali su za mačke sasvim uredi. U svakom slučaju, na svakom vlasniku je da sam istraži temu i odabere najbolju kameru za sebe i svog kućnog ljubimca. Ukoliko ste zainteresovani za ovaj tip kamere, možete je naručiti putem Amazona i web-stranice Chewy za 150 dolara.

doplatu kao što je Dog Nanny usluga, ali i bez toga ovo je dobra kamera koja je dobrodošao stanar u vašem domaćinstvu.

### Petcube Bites 2

Ovdje je riječ o tzv. dog treat kameri, koja je zadužena za davanje poslastica kućnom ljubimcu. Bites 2 dolazi s opremom za monitoranje, tako da je možete postaviti na zid, a to opet znači da ne zauzima mnogo prostora u kući. Kamera ima ugrađen laser i Alexa tehnologiju, a može puštati muziku te nudi 1080p video s vidnim poljem od 160 stepeni. Sama kamera je, kao što joj ime i kaže, u obliku kocke, s tim da se u donjem aluminijskom dijelu nalazi dispenzer za dijeljenje poslastica. Osim toga, Bites2 ima četiri mikrofona i zvučnika, što znači da je zvuk bolji nego kod većine drugih kamera. I njega, kao i Furbo, možete kontrolisati pomoću Alexe, koja je u ovom slučaju kod Bitesa 2 ugrađena, ali nije i aktivirana. Još jedna od stvari koju nudi jeste premium pretplata od četiri dolara mjesečno, s tim da moramo naglasiti da se ona plaća godinu dana unaprijed, a nudi mogućnost dodavanja drugih kamera, kao i skidanja videa. Ukoliko se odlučite na kupovinu, Petcube Bites 2 košta oko 250 dolara na Amazonu.

### Petcube Play 2

Još jedna Petcubeova kamera, ovaj put naziva Play 2, namijenjena je nadzoru vlasnika mačaka. Riječ je o kameri kockastog oblika, rezolucije 1080p, koja dolazi s dodatkom dvosmjeren komunikacije u stvarnom vremenu. Uz pomoć Petcube aplikacije u svakom



**Istraživanja potvrđuju da psi doživljavaju vrijeme na isti način kao i ljudi, a oni koji provode najviše vremena daleko od svojih vlasnika skloni su iritabilnosti, anksioznosti uslijed razdvajanja, pa čak i depresiji**



trenutku možete provjeriti šta vaš krvnjeni prijatelj radi, možete razgovarati s njim i tako ostvariti odnos pomoću moderne tehnologije. Zanimljivo je da u okviru aplikacije postoji opcija zahvaljujući kojoj možete prevlačiti prstom preko ekrana osjetljivog na dodir za vrijeme snimanja uživo, dok će ugrađeni laser pratiti putanju kretanja vašeg prsta, omogućavajući vam da se izdaleka igrate sa svojom mačkom. A kako kamera dolazi s ugrađenom Alexa tehnologijom, to znači da će ona započeti partiju ako joj kažete da se poigra s vašim kućnim ljubimcem umjesto vas. Dakle, ukoliko niste raspoloženi za to da se igrate s laserom, Amazonov glasovni asistent će rado preuzeti taj zadatok na sebe. Međutim, ovdje moramo napomenuti da su prijavljeni određeni problemi s vidljivošću lasera i slaboj pokretljivosti u stanovima u kojima ima dosta prirodnog osvjetljenja, pa ga kućni ljubimac ponekad ne može ni vidjeti. Kao i druga Petcubeova kamera opisana u ovom tekstu, i ova košta oko 150 dolara.

### Tri razloga za pet-friendly kamere

Ukoliko već neko vrijeme razmišljate i trudite se da odvagate trebate li ovaku kameru ili ne, nudimo vam tri legitimna razloga zbog kojih je ovaj tip kamera dobra odluka i investicija. Prvi je i najočigledniji, a to je udaljeni nadzor. Ovaj tip nadzora sigurno bi pomogao u slučajevima kada ste na poslu ili idete u kupovinu, jer čak su i najposlušniji ljubimci skloni nepoželjnom ponašanju,

a kamera bi vam omogućila da barem znate gdje nestaju stvari iz domaćinstva ili na čemu trebate poraditi. Pored toga, ovakve kamere su dobar odabir i u slučaju da ste unajmili nekoga da vam se brine za kućne ljubimce dok vi niste tu, jer će na diskretan način snimati i ponašanje date osobe. I na kraju, nije zanemarljivo napomenuti i to da ovakva kamera može pomoći i u slučaju provale u stan, jer će ostati zabilježeno ko je provalio, kada i kako, a vi ćete imati lagan pristup svim navedenim snimcima. Drugi razlog jeste bolji nadzor zdravlja vašeg kućnog ljubimca. Za mnoge vlasnike njihov kućni ljubimac je i član porodice čije zdravlje je od velike važnosti. Nažalost, mnoge bolesti kod životinja se prekasno otkriju, a to je upravo polje na kojem kamere namijenjene nadzoru kućnih ljubimaca mogu pomoći. Nekad je jednostavno teško odrediti da li je vaš kućni ljubimac letargičan, pospan, odbija li hranu ili je jednostavno bolestan. Kamere namijenjene ljubimcima mogu vam pomoći da otkrijete obrasce ponašanja koje možda drugačije ne biste otkrili. Tako biste, recimo, prilikom pregledanja snimaka od prije nekoliko dana mogli primijetiti da nešto ne štima i taj snimak pokazati svome veterinaru koji će znati šta treba dalje raditi. I u slučaju da dođe do operacije, kamera će vam ponovo pomoći pri nadgledanju ljubimca tokom njegovog oporavka.

### Interakcija i posvećenost

I treći razlog koji ide u prilog nabavci kamere za kućne ljubimce zasigurno je pojačana interakcija i posvećenost. Naime, mnogi vlasnici imaju određeni stepen griže savjesti ili se pitaju nedostaju li svojim ljubimcima kada nisu tu. Stručnjaci kažu: da, nedostajete im, a to posebno važi ukoliko imate psa. Zapravo, ne samo da im nedostajete, nego čak znaju i koliko dugo ste bili odsutni. Istraživanja potvrđuju da konkretno psi doživljavaju vrijeme na isti način kao i ljudi, a oni koji provode najviše vremena daleko od svojih vlasnika skloni su iritabilnosti, anksioznosti uslijed razdvajanja, pa čak i depresiji. Zbog toga su ove kamere jedan od načina da se vašem ljubimcu popravi raspoloženje kada niste tu. Kako većina nabrojanih kamera nudi dvosmjernu komunikaciju i neku vrstu surogata Skype poziva, treba iskoristiti prednosti koje nam donosi nova tehnologija kako bismo usrećili i svog ljubimca, ali i sebe, jer onda znamo da smo učinili sve što je u našoj moći da svog psa ili mačku učinimo zadovoljnim. Jer, ipak smo mi birali njih, a ne oni nas. ◀





Videonadzorne kamere za noćno snimanje

# KAKO ODABRATI ONU NAJBOLJU?

**VIDEONADZORNE KAMERE ZA NOĆNO SNIMANJE** POSLJEDNJIH **SU** GODINA DOŽIVJELE VELIKI USPON ZAHVALJUJUĆI SENZORIMA SLIKE I TEHNOLOŠKOM NAPRETKU KOJI IM OLAKŠAVA RAD PRI SLABOM OSVJETLJENJU. SIGURNOSNE KAMERE ZA NOĆNO SNIMANJE DANAS SU MNOGO SNAŽNIJE I, ZA RAZLIKU OD ZRNASTIH MONOHROMATSKEHLI SLIKE S NOĆNIH KAMERA, MODERNI UREĐAJI OVOG TIPOA SADA MOGU PONUDITI JASNE SLIKE U PUNOJ BOJI I UZ MINIMALNO OSVJETLJENJE

■ Izvor: a&s International  
redakcija@asadria.com

**Prava sigurnosna** kamera za noćno snimanje može biti dragocjena komponenta svakog sigurnosnog sistema za rad na otvorenom. Ipak, uz veliki broj modela dostupnih na tržištu, odabir pravog rješenja može biti veoma složen proces. Pravilno razumijevanje faktora koje treba uzeti u obzir pri odabiru kamere može predstavljati razliku između uspješne i neuspješne instalacije. U nastavku teksta govorimo o boji prikaza, ambijentu i osvjetljenju kao nekim od najvažnijih faktora koje treba uzeti u obzir prilikom biranja najbolje kamere za noćno snimanje.

## Noćno snimanje u boji vs. crno-bijeli režim rada

Tradicionalne sigurnosne kamere za noćno snimanje s infracrvenim filterima (poznate i kao IR-cut modeli) nude crno-bijelu sliku. Međutim, napredak tehnologije izrade kamera, senzora slike i podrške za rad u uvjetima slabog osvjetljenja unaprijedili su mogućnosti kamera za noćno snimanje u boji. Budući da je sada dostupan širi izbor modela, prvo što treba utvrditi prilikom odabira najbolje kamere za noćno snimanje jeste da li vam treba ona s prikazom u boji ili vam je dovoljan crno-bijeli video. Iako se ovo može činiti

kao jednostavna stavka za razmatranje, Andres Vigren, globalni menadžer proizvoda u kompaniji Axis Communications, navodi da odgovor na ovo pitanje uveliko određuje koje je rješenje najbolje za vas. "Za prikaz kvalitetnog videa u boji potreban vam je adekvatan izvor svjetlosti koji odgovara potrebama kamere. Na tržištu su dostupni noviji modeli s naprednim tehnologijama za rad pri slabom osvjetljenju koji zahtijevaju manje svjetlosti", kaže on. Max Fang, direktor za IP proizvode u kompaniji Hikvision Digital Technology, naglašava da dužina trajanja prikaza u boji zavisi od sposobnosti kamere da izade na kraj sa slabim osvjetljenjem. U protivnom, kamere će se prebaciti u infracrveni (IC) način rada kada osvjetljenje postane nedovoljno (npr. kada padne mrak), a zaslon će se prebaciti na crno-bijeli prikaz.



Andres Vigren, globalni menadžer proizvoda, Axis Communications

U slučajevima slabog osvjetljenja važno je provjeriti je li IC svjetlo na kameri odgovarajuće ili vam je potreban zasebni

IC uređaj. Ako ugrađeno IC svjetlo nije dovoljno za ravnomjerno osvjetljenje, to bi moglo dovesti do toga da na slici imate crne uglove.

Osim toga, morat ćete provjeriti i je li IC svjetlo potpuno ili djelimično skriveno. Ako krajnji korisnik želi da kamere budu potpuno neprimjetne, prikladna opcija je skriveno IC svjetlo koje je nevidljivo za ljudsko oko. Međutim, Vigren navodi da je ono manje osjetljivo kada je u pitanju rad ka-

mere i da će biti potrebno dodatno osvjetljenje u okruženju kako bi se došlo do najbolje slike.

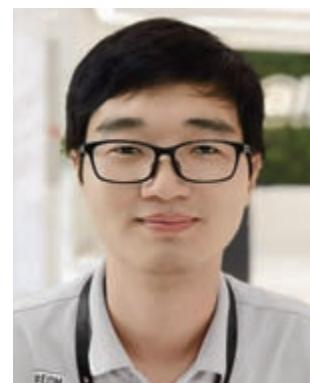
## Dodatni faktori važni za noćno snimanje

Promjene u nivou osvjetljenja tokom godišnjih doba su još jedan od ključnih faktora prilikom odabira kamere za noćno snimanje. U idealnoj situaciji, kamere koje kvalitetno rade pri slabom osvjetljenju trebale bi jednako dobro raditi i tokom dana. Istovremeno, postavke koje se koriste za noćno snimanje možda neće biti optimalne u nekom

drugom dobu dana. "Kako se godišnja doba mijenjaju, sunčeva svjetlost pada na kamere na različite načine, posebno tokom jeseni i proljeća. Zato je jako bitno osigurati da se kamera može automatski prilagoditi ambijentu. To znači da ona mora moći mijenjati režime rada u uvjetima slabog osvjetljenja i koristiti široki dinamički opseg (WDR) u zavisnosti od ambijentalnog osvjetljenja", kaže Vigren.

## Napredni senzori slike

Nadzorne kamere za noćno snimanje kontinuirano se ažuriraju pomoću novih tehnologija. Fang navodi da danas uključuju više objektiva, fuziju dvostrukog svjetla i prateće tehnologije, objektive sa širim otvorom blende, namjenske senzore za veće površine i inteligentniju tehnologiju za rad pri slabom osvjetljenju. "Što se tiče senzora slike, došlo je do



Eaden Xie, direktor IPC serije proizvoda, Dahua Technology

kako bi ih se učinilo osjetljivijim na svjetlost i omogućila obrada slike u stvarnom vremenu. Implementacija ovako snažnih čipova nudi i veći kapacitet za obradu slike, što u konačnici podiže i njihov kvalitet. Ovakav razvoj situacije doveo je do pojave kvalitetnijih kamera za rad pri slabom osvjetljenju s prikazom u znatno višim rezolucijama. U odnosu na period od prije deset godina, kada su kamere za rad pri slaboj svjetlosti bile dostupne samo u SVGA i D1 rezoluciji, sada se ista osjetljivost nudi sa 4K ka-

## Analizirajte okruženje koje nadzirete

Okruženje u kojem se koristi kamera također je bitan faktor pri odabiru pravog uređaja za noćno snimanje. Pri tome treba razmotriti faktore kao što su veličina pokrivenog područja i postojanje potrebe za otkrivanjem, identifikacijom i prepoznavanjem objekata. Na taj način možemo utvrditi specifikacije buduće kamere za noćno snimanje i ustanoviti da li nam je potrebna podrška dodatnih tehnologija, poput termalnih sistema ili radara. Mjesto postavljanja također igra značajnu ulogu tokom procjene potrebnih karakteristika kamere. Naprimjer, ako je postavljena nisko i lako joj se može pristupiti, može biti izložena neovlaštenom rukovanju i vandalažmu. U tom slučaju krajnji korisnici trebaju uzeti u obzir i IK standard otpornosti na udare. Ako će kamera biti izložena nepovoljnim vremenskim uvjetima (npr. kiši, snijegu itd.), potrebno je osigurati kvalitetnu zaštitu od nepogoda i vlage za prednje staklo uređaja. Kapljice na staklu mogu uzrokovati pojavu odsjaja kod uključenog IC svjetla, što u konačnici smanjuje jasnoću i kvalitet slike.



merama”, objašnjava Vigren. Eaden Xie, direktor IPC serije proizvoda u kompaniji Dahua Technology, navodi da njihove kamere koriste senzor slike osjetljiv na noćne izvore svjetla, koji omogućava modelima u boji da ponude veće dimenzije piksela i pozadinsko osvjetljenje za njih, kao i veći stepen konverzije svjetla (HCG) pri slabom osvjetljenju. “Korištenje HCG tehnologije može ponuditi viši stepen konverzije svjetla unutar senzora. Ovakvo pojačanje se dešava u prednjem segmentu signalne veze, što može smanjiti utjecaj pozadinskog šuma i tako donijeti kvalitetniji omjer signala i šuma”, objašnjava Xie.

### Kako vještačka inteligencija i duboko učenje pomažu kamerama?

Napredak u segmentu hardverskih i softverskih tehnologija omogućio je primjenu inteligentnih načina rada s kamerama za noćno snimanje. Stalnim poboljšanjem algoritama vještačke inteligencije i smanjivanjem sistemskih zahtjeva za njihovu primjenu, u sve više scena sada se koristi cijeli spektar boja i vještačka inteligencija. “Kada je riječ o kamerama za noćno snimanje, ljudi mogu pomisliti da je slika dovoljno dobra ako je prikaz jasan, dobro osvijetljen i u boji. Kod inteligencije se više pažnje posvećuje pribavljanju kvalitetnih informacija o praćenom subjektu, a ne samo o prikazu boja, poboljšanju svjetline i smanjenju šuma. Krajnji cilj stalne optimizacije učinaka noćnog snimanja je primjena algoritama dubokog učenja za podršku reagiranju na konkretne situacije uz dovoljnu količinu i detaljnost prikazanog videa”, kaže Xie. U budućnosti bi interna i eksterna primjena vještačke

### Specifikacije i tehnički podaci nisu ključni!

Još jedna uobičajena zabluda je izjednačavanje proizvođačevih brojki s konkretnim performansama. Krajnji korisnici se često previše oslanjaju na tehničke specifikacije kada odlučuju o nabavci kamere. Ustvari, tehnički podaci ih često zavaraju i zbog njih donose odluke bez fokusiranja na načine na koje kamera, zapravo, radi. Ako ne uspoređujemo modele istog proizvođača, tehničke specifikacije mogu zavarati jer one ne daju nikakve garancije u vezi s kvalitetom kamere ili njenim performansama u praksi. Osim toga, ograničavanjem izbora kamera prema određenom rasponu specifikacija vi iz postupka odabira možete isključiti i druge pogodne i kvalitetne opcije, što može dovesti do neželjenih ishoda. “Ako se oslanjaju samo na suhe podatke, krajnji korisnici mogu nabaviti rješenje za koje smatraju da će ponuditi očekivane performanse, a onda ih ono može iznevjeriti na duže staze jer se specifikacije ne podudaraju s realnošću. Jedini način da se to izbjegne je testirati kameru na terenu prije donošenja konačne odluke”, objašnjava Vigren. On vjeruje da vrijedi uložiti dodatno vrijeme u testiranje i procjenu potencijalne kamere, odnosno provjeriti kvalitet njihovog rada tokom dana i noći, jer na taj način krajnji korisnici mogu donijeti odluku na osnovu konkretnih pokazatelja o performansama.

inteligencije mogla igrati važnu ulogu u poboljšanju mogućnosti tehnologija za rad pri slabom osvjetljenju. To uključuje poboljšanje kvaliteta videa koji kamera prikazuje, snima i prenosi.

### Bolje performanse traže više procesorske snage

Bilo da je riječ o dovoljnom dostupnom infracrvenom (IC) svjetlu, nivou osv-

jetljenja (lux) ili drugim komponentama, sve navedeno utječe na kvalitet rada kamere za noćno snimanje i domet u kojem ona može obavljati svoj posao. Osim toga, dostupna procesorska snaga može utjecati ne samo na daljinu vidokruga kamere nego i na kvalitet slike. Procesorska snaga, međutim, ima svoju cijenu i njen iznos je obično takav da će krajnji korisnici morati dobro razmislići da li je

**Tehnološko unapređenje senzora slike i procesa njene obrade radi poboljšanja osjetljivosti na svjetlost u infracrvenom opsegu povećava osjetljivost infracrvene (IC) svjetlosti na kameri, a to joj omogućava da bolje “vidi” na daljinu uz istu količinu IC svjetla**

mogu priuštiti i žele li platiti za nju. Razlika u cijeni između ulaznog i vrhunskog modela kamere za noćno snimanje može se kretati u rasponu od 200 do 5.000 američkih dolara. Vigren naglašava da kompanijama s manjim prostorijama nije isplativo ulagati u vrhunske modele, jer bi troškovi premašili njihov budžet, a da pritom ne bi nužno ponudili dodatnu vrijednost. "Na kraju, odabir kamere zavisi od ukupnih troškova ulaganja i konkretne primjene. Ulazni modeli fiksnih fokalnih kamera često nude područje pokrivenosti od oko 10 metara. Za manje prostorije s ograničenim budžetom, ovaj tip kamere može biti dovoljan", kaže on, dodavši da je za veće prostore bolja opcija standardna 1080p kamera s dometom od 30-ak metara.

### **Veći domet traži dodatno IC svjetlo**

Količina svjetlosti koju kamera dobija je još jedan faktor koji u velikoj mjeri može utjecati na njene performanse u pogledu dometa. "Općenito govoreći, više svjetla donosi kvalitetniju sliku i to je još važnije na većim udaljenostima. Za postizanje visokog kvaliteta slike potrebna vam je dovoljna količina ugrađenog IC svjetla koje troši više energije.

U ovom slučaju može biti isplativije osigurati izvor dodatnog IC svjetla koje će podržati performanse kamere", kaže Vigren. Za scenarije primjene u kojima je potreban veći domet (npr. mostovi, ceste, pogranična kontrola itd.) Vigren preporučuje korištenje kamera s vrhunskim zoomom. On naglašava da takve kamere mogu pokriti udaljenost i do 400 metara podešavanjem infracrvene zrake prema nivou zuma kamere. "Za korisnike koji moraju pratiti objekte na velikim udaljenostima kombinirano rješenje u vidu dodatnih radara ili termalnih kamera



Max Fang, direktor IP proizvoda, Hikvision Digital Technology



može ponuditi najbolje rezultate, jer te tehnologije ne zavise od količine svjetla da bi bile efikasne", kaže on.

### **Česte zablude povezane s kamerama za noćno snimanje**

Postoji više zabluda koje se tiču rada nadzornih kamera za noćno snimanje i njih se potrebno riješiti prije ulaska u proces odabira. One mogu dovesti do nabavke pogrešne kamere i loših rezultata pri njihovom korištenju. Ideja noćnog snimanja obično zaziva asocijacije na crno-bijele monohromatske slike

ili snimke u zelenkastim nijansama koje često viđamo na televiziji. To danas više nije slučaj. Moderne kamere tokom noćnog snimanja nude prikaz u

cijelom spektru boja. Mnoge kompanije naporno rade na poboljšanju tehnologije za rad pri slabom osvjetljenju kako bi tokom noćnog rada ponudile realnije i jasnije videozapise u boji. Iako mnoge kamere za noćno snimanje danas mogu prikazivati boje, njima je i dalje potrebna dovoljna količina svjetla kako bi se to postiglo. Zbog toga su opremljene izvorom infracrvenog (IC) svjetla, koji im omogućava da se prebace na crno-bijeli prikaz ako osvjetljenje postane nedovoljno za efikasnu primjenu prikaza u boji. Kompanije kao što je Dahua Technology lansirale su proizvode koji podržavaju prikaz u punoj boji i nude cjelodnevni nadzor u boji u uvjetima slabog osvjetljenja. Kako kaže Xie, "u poređenju s drugim kamerama, kod ovih modela nema mjesta zabrinutosti zbog gubitka kvaliteta videa/boje uslijed prebacivanja na crno-bijeli režim rada".

Jedna od uobičajenih zabluda u vezi sa sigurnosnim kamerama za noćno snimanje jeste da one "vide" bolje tokom dana u odnosu na noć. "Dnevne performanse snimanja zavise od brojnih faktora, poput dubinske oštirine, širokog dinamičkog opsega (WDR), rezolucije itd. Njih treba sveobuhvatno procijeniti. Ovo su glavni faktori koji utječu na kvalitet videa tokom dana. Tehnologija za rad pri slabom osvjetljenju ne poboljšava kvalitet slike tokom dana", objašnjava Fang. ▲

**Čipseti se neprestano unapređuju. To će s vremenom omogućiti sve većem broju kamera za noćno snimanje da pokreću složene algoritme i ponude dodatni kapacitet za obradu koji je potreban za kreiranje jasnog i preciznog prikaza u boji**



IZAZOVI PANDEMIJE

# BESKONTAKTNA SIGURNOST I POVRATAK NA RADNA MJESTA

**DA BI RADNIKE VRATILI NA RADNA MJESTA, ORGANIZACIJE SE MORAJU PRILAGODITI NOVIM UVJETIMA,** primijeniti nove postupke i iskoristiti tehnologiju kako bi pomogle zaposlenicima da se osjećaju sigurnije. U fokusu je fizički pristup. Pretrpani ulazi, liftovi i zajednički radni prostori ugrožavaju sigurno socijalno distanciranje. Isti tako, neki sigurnosni procesi, poput izдавanja akreditiva, uvek su se oslanjali na direktni kontakt

■ Piše: Jaroslav Barton, direktor marketinga proizvoda, HID Global  
jbarton@hidglobal.com

Upravljanje kontrolom pristupa može pomoći u usmjeravanju kretanja zaposlenika paralelno s aktivnostima na organizaciji radnog vremena. Fizički sistemi za kontrolu pristupa (PACS) mogu koristiti funkcije lociranja kako bi podržali praćenje kontakata i smanjili stvaranje gužvi. Isti sistemi mogu se iskoristiti i kao podrška pametnom upravljanju posjetiocima.

## Kontrola pristupa bez dodira

Automatski pokretači vrata, rotirajuća i klizna vrata mogu pomoći u smanjenju kontakta na prometnim ulaznim i izlaznim tačkama. Oni se mogu kombinirati s beskontaktnim akreditivima i čitačima kako bi se došlo do veće sigurnosti, uz minimiziranje površinske kontaminacije. Druga strategija uključuje primjenu čitača s velikim dometom koji koriste Bluetooth Low Energy (BLE) vezu za bolje performanse čitanja na daljinu. S dometom čitanja do nekoliko metara, BLE može dodatno udaljiti zaposlenike koji bi se inače mogli naručiti oko čitača i vrata. Beskontaktni akreditivi također podržavaju higijenske protokole za prijavljivanje na mreže, plaćanje ili korištenje štampača.



Jaroslav Barton

zgradi. Tu postoji i potreba za potencijalnim praćenjem kontakta. Kvalitetna politika i napredne tehnologije mogu osigurati sigurno kretanje posjetilaca. Rješenja za upravljanje posjetiocima mogu se koristiti samostalno ili u kombinaciji sa sistemom kontrole pristupa na nivou organizacije. Posjetioci se sami registriraju u predvorju, a domaćini se obavještavaju o njihovom dolasku. Skeneri vozačkih dozvola i bar-koda, kamere i štampači pomažu u pružanju podrške procesima koji se odvijaju na recepciji.

## Usluge lociranja

Ključnu ulogu u držanju fizičke distance među ljudima ima svijest o tome gdje se oni nalaze u svakom trenutku. Slično načinu na koji se GPS koristi na otvorenom, usluge lociranja koriste BLE odašiljače koji šalju signale do gatewaya. Ti mrežni prolazi mogu prepoznati lokaciju pojedinaca u fizičkom prostoru. Identitet osobe može biti zabilježen na ID kartici koja kontinuirano šalje signale, čime se kreira virtualna mapa lokacije u odnosu na fiksne mrežne

## Bežično izdavanje akreditiva

Moderno sistemi s bilo koje lokacije mogu slati akreditive na svaki ovlašteni uređaj, što znači da zaposlenici i posjetioci mogu dobiti svoje akreditive bez potrebe za kontaktom. Posjetioci uvode novu varijablu u ovaj proces. Njihovi akreditivi se provjeravaju prilikom ulaska, a iz sigurnosnih razloga se mora pratiti njihovo kretanje u

**Na aplikaciju se mogu spojiti sve Previdia vatrogodjavne centrale koje su spojene na IP mrežu i prijavljene u Inim Cloud. Prijaviti ih može osoba koja ima otvoren instalaterski ili korisnički račun na Inimovim web-stranicama**

prolaze. Usluge lociranja menadžmentu daju alat u ruke da može djelovati proaktivno, a ne reaktivno u svojim nastojanjima da promovira fizičko distanciranje. Na taj način se u svakom trenutku može znati broj ljudi u određenom prostoru. Povezani odašiljači šalju informacije i o popunjenošći prostorija. To, npr., znači da se osoblje informira o tome koji su prostori slobodni, a koji zauzeti. Štaviše, ovi sistemi mogu automatizirati praćenje kontakta jer se pomoću njih zna je li neko stupio u kontakt s osobom čiji je test pozitivan na COVID-19.

## Iskorištavanje PACS tehnologije

Za osoblje zaduženo za primjenu i nadzor kontrole pristupa, ovo vrijeme nosi velike izazove. Na licu mjesta danas može biti manje osoblja, ali oni koji se zateknu tamo će biti vrlo opterećeni. Da bi se došlo do sigurnih prostora, potrebno je optimizirati operacije, osigurati da osoblje dođe do pravih informacija i da osobe koje ulaze u zgradu budu svjesne politika koje se primjenjuju. Iako tehnologija može igrati značajnu ulogu u kontroli socijalne distance i ostalih potreba povezanih s pandemijom, politike su ključne za uspješan fizički povratak na posao. Jako bitno je, npr., imati kvalitetne sisteme vođenja evidencije. PACS sistemi generišu zapisnike, izvještaje i arhivski materijal. Ako se dobro iskoriste, to mogu biti neprocjenjive informacije. Upravitelji zgrada mogu iskoristiti ove ključne podatke da prate ko je bio u objektu i kada i tako dobiti potpuniju sliku o operativnim rizicima.

## Najbolje prakse

Da bi ove mjere bile efikasne, poslodavci će morati primijeniti općeprihvaćene najbolje prakse u vezi s iskorištavanjem prostora, a naročito higijenom. U nastavku su neke od ključnih politika.

*Vizuelna komunikacija* – kao ključ za provođenje novih politika i postupaka, vizuelna komunikacija je dobar način da se ljudima predstave nova očekivanja.

*Dezinfekcija ruku* – stanice za dezinfekciju ruku moraju biti dostupne svim zaposlenim i osoblje treba podsjećati da često



## Priprema za budućnost

Iako pandemija nosi velike izazove za upravljanje zgradama i sigurnost, ona je i jedinstvena prilika. U zadovoljavanju novih potreba u vezi sa socijalnim distanciranjem, praćenjem kontakata i iskorištenosti prostora leži i prilika da se detaljno ispitaju praksu kontrole pristupa. Holistički pogled na PACS tehnologiju može pomoći u kreiranju sigurnih radnih okruženja. Time se upraviteljima zgrada nude novi uvidi koji mogu poslužiti u smanjenju gužvi, praćenju pojedinaca i boljem iskorištenju prostora u skladu s kvalitetnom definisanom najboljom praksom.

pere ili dezinficira ruke.

*Održavanje fizičke distance* – rasporedite mesta za sjedenje kako biste omogućili odgovarajuće socijalno distanciranje, dodajte natpise na zidovima i oznake na podu kako biste preusmjerili protok ljudi, zabranite nenajavljenе sastanke u sobama i privremeno onemogućite sadržaje u zajedničkim prostorima.

*Beskontaktnе tehnologije* – gdje god je to moguće, obustavite procese koji zahtijevaju dodirivanje ili ih ograničite na jednu osobu. Sarađujte s dobavljačima usluga kako biste identificirali i implementirali tehnologije i procese koji ne podrazumijevaju dodirivanje, posebno u zonama gdje je to često, poput vrata i dizala.

*Lična zaštitna oprema (LZO)* – medicinski stručnjaci širom svijeta preporučuju svima da nose masku preko usta i nosa.

Poslodavci bi maske trebali staviti na raspolaganje svim zaposlenim.

*Pojačano redovno čišćenje* – sve površine koje se često dodiruju trebaju se čistiti i dezinficirati nekoliko puta dnevno. To može uključivati stolove i kvake, prekidače za svjetlo i telefone. PACS tehnologije kao što su tastature i biometrijski čitači također se moraju često dezinficirati. Gde je moguće, konfigurišite uređaje za kontrolu pristupa za rad s beskontaktnom karticom ili mobilnom tehnologijom umjesto otiska prsta ili ekrana osjetljivog na dodir. *Ažurirane politike za posjetioce* – implementirajte politike pristupa za posjetioce koje ograničavaju kontakte tokom boravka u prostoriji. To uključuje upitnik o zdravstvenom stanju, ekrane za mjerjenje temperature i ograničavanje nepotrebnog kretanja. ◀



Cambium Networks

CAMBIUM NETWORKS PREDSTAVIO CNVISION

# PROFESSIONALNO BEŽIČNO RJEŠENJE ZA VIDEOONADZOR

**NOVO RADIJSKO RJEŠENJE TVRTKE CAMBIUM NETWORKS, CNVISION, POSEBNO JE PRILAGOĐENO ZA TRŽIŠTE VIDEOONADZORA.** OVA LINIJA PROIZVODA STVORENA JE S NAMJEROM VISOKE ISPLATIVOSTI, JEDNOSTAVNOSTI KORIŠTENJA I PREDVIDLJIVOSTI U PERFORMANSAMA S PRAVIM IZBOROM ZNAČAJKI SPECIFIČNIH ZA POSLOVE VIDEOONADZORA

■ Piše: Kristijan Fabina, regionalni predstavnik za Jadransku regiju, Cambium Networks  
kristijan.fabina@cambiumnetworks.com

Rješenje cnVision koristi prednosti jakog pedigreea bežičnosti tvrtke Cambium Networks, a služi kao bežična okosnica mreže u povezivanju nadzornih videosustava u točka-točka ili točka-više točaka konfiguraciji. Rješenje je dizajnirano na način da uklanja kompleksnost konfiguracije te partnerima osigurava besplatan i jednostavan alat za planiranje linkova i cjelovitih bežičnih mreža. Zato su ključni kupci cnVision rješenja integratori svih oblika i veličine. cnVision ima visoku razinu otpornosti u pružanju podrške implementaciji sustava od kritične važnosti i vrlo je otporan na smetnje. Ugrađeni mehanizam za ponavljanje paketa osigurava isporuku kritičnih videozapisa u manje ili više izazovnim situacijama. Algoritam bežičnog prijenosa optimiziran je primarno za prijenos videosadržaja, pa je tehnička izvedba predvidljiva i osigurava dosljedno iskustvo, dok je gubitak kritičnog videosadržaja neprihvatljiv. S protokolom dizajniranim za najvišu razinu kvalitete prijenosa videosadržaja, visokom otpornošću na smetnje i ugrađenim mehanizmom za ponavljanje paketa, cnVision se



Sakid Ahmed, potpredsjednik cnVision inženjeringu, na nedavnoj ISC East konferenciji pokazuje primjer integracije cnVision radijskih uređaja u Hanwha VMS s Hikvisionovim kamerama, kao i pregled alarma i događaja na mreži

lako prilagođava promjenjivim i izazovnim okruženjima na spektru.

## ONVIF i integracija u VMS

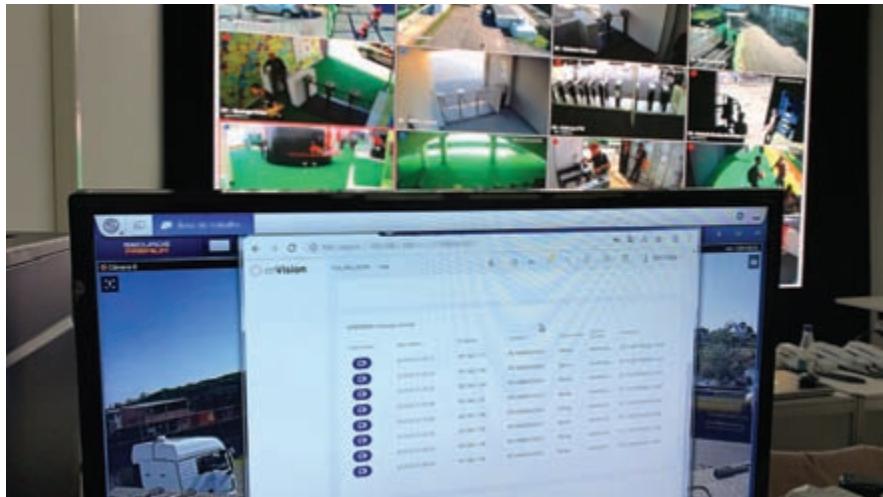
Dvije su ključne značajke cnVision rješenja. Svi radijski uređaji iz cnVision serije imaju u softveru integriran ONVIF klijent (Open Network Video Interface Forum), koji omogućuje otkrivanje prijenosa videosadržaja putem radijskog linka, naziv proizvođača i modela kamera, IP i MAC adresu kamera te potrošnju mrežnog prometa. Mogućnost

otkrivanja prijenosa videosadržaja dodatno omogućuje i gledanje snimke uživo unutar administracijskog web-sučelja cnVision uređaja. Takav pristup omogućuje otkrivanje poteškoća u mreži ili zastoj u radu određenih kamera, što je veliki korak prema rješavanju potencijalnih problema na terenu. Druga važna značajka je mogućnost integracije cnVision radijskih uređaja u VMS raznih proizvođača koji upravlja kamerama, kao što su Milestone, Genetec i Hanwha, u kojima možemo u stvarnom vremenu vidjeti ne samo kamere određenih proizvođača i videosadržaj već i informacije o radijskim uređajima kroz koje prolazi videosadržaj, potrošnji prometa, brzini prijenosa, modelima kamera, alarmima i događajima.

**Rješenje dolazi s tri godine garancije kao vodeći standard u industriji, a modeli uređaja imaju IP55 ili IP67 certifikat**



cnVision profesionalni radijski uređaji za prijenos videosadržaja korišteni su nedavno za potrebe video nadzora Formule1 u Brazilu



Pregled nadzornih kamera u VMS-u i u cnVision nadzornom sučelju s modelima, nazivom proizvođača, IP i MAC adresama te potrošnjom prometa

### Primjer izbor rješenja

Pouzdanost i fleksibilnost ovog rješenja dolazi s primjerenim izborom modela uređaja koji se mogu koristiti za povezivanje dvije ili više lokacija na kojima se nalaze kamere. Temperaturni raspon je od -30°C do +60°C, a u portfelju su još dvije bazne stanice i tri klijentska uređaja za krajnje lokacije. Klijentski uređaji su Micro, Mini i MAXr i vrlo su robusno rješenje. Micro klijent je kompaktan uređaj malih dimenzija s ugrađenom usmjerrenom antenom 13 dBi pojačanja prikladan za kraće udaljenosti do 150

Nadzorni centar Formule1 u Brazilu prima videosadržaj najviše kvalitete putem cnVision profesionalnih radijskih rješenja



metara i montažu na semaforima i sličnim lokacijama gdje ne želimo zauzimati previše mesta. Mini klijent dolazi s ugrađenom usmjerrenom antenom uskog snopa i 16 dBi pojačanja i koristi se u dometu kratkih i srednjih udaljenosti do 1-2 km. MAXr klijent je IP67 uređaj s ugrađenom antenom 19 dBi pojačanja za udaljenost i do 10 kilometara.

### Sigurnost komunikacije

Sigurnost je od ključne važnosti za prijenos kritičnih videozapisa. cnVision uključuje privatni zatvoreni komunikacijski protokol koji je razvio Cambium Networks poboljšavajući sigurnost uz šifriranje podataka putem AES 128 ili alternativno AES 256 bitova. Dodatne mјere su administrativni pristup s različitim privilegijama za određene osobe, HTTPS i SSH pristup, L2/L3 kontrola prometa (vatroid), mogućnost filtriranja po

### Softver i podrška

Softverska strana nosi nekoliko dobrih značajki. Besplatna Cambium cnMaestro platforma za nadzor i upravljanje mrežom dolazi u tri inačice: Cloud, softver/kontroler za virtualizaciju ili kao fizički kontroler za smještaj u mrežni ormar. LinkPlanner je besplatan alat za prodajno osoblje i inženjere, a služi za brzu i jednostavnu provjeru izvedivosti povezivanja dvije ili više lokacija, kao i očekivane vrijednosti za radijske veze. cnCompanion je također sveobuhvatan besplatan alat s kojim partneri mogu sa sigurnošću planirati postavljanje kamera i točno znati koje cnVision proizvode odabratite predviđeni kapacitete. Na taj način partneri mogu unaprijed pripremiti opremu, a kasnije izvršiti održavanje sustava i nadogradnje softvera. Uz trogodišnje jamstvo za cnVision rješenje, Cambium Networks osigurava 24/7 podršku putem telefona, e-pošte, Support portala i foruma, a na raspolaganju su i ovlašteni stručni regionalni distributer i Cambiumovo osoblje zaduženo za regiju.

MAC adresama, RADIUS i WPA2 autentifikacija. Brojači mrežnih paketa žičnog i bežičnog dijela mreže otkrivaju kvalitetu radijske veze i poduzimaju korektivne mјere na osnovu statistika. Distribucija modulacije paketa poboljšava kvalitetu linka na osnovu distribucije paketa u mreži. cnVision nudi i dodatne servise poput Wireless links testa, koji provjerava stvarne RF performanse, watchdog servisa, koji automatski resetira link na osnovu definiranih kriterija, te QoS-a, kvaliteta servisa koji prioritizira videoprijenos. ◀



KONTROLA DOGAĐAJA U VREMENU NOVE NORMALNOSTI

# NOVO RJEŠENJE ZA SPAJANJE LJUDI

**ORGANIZATOR KONFERENCIJA HOTELRESERVIERUNGS UND TAGUNGSMANAGEMENT (HUT) IZ NJEMAČKE TRAŽIO JE PRIVREMENO RJEŠENJE ZA PONOVNU ORGANIZACIJU DOGAĐAJA. LOKALNI PARTNER MICHAEL TELECOM AG PONUDIO JE TEHNOLOGIJU KOMPANIJE HIKVISION**

■ Pripremio: Odjel marketinga za Evropu, Hikvision  
marketing.eu@hikvision.com

**Kompanije u vremenu nove normalnosti moraju biti inovativne kako bi opstale na tržištu.** One iz ugostiteljstva i konferencijskog turizma suočene su sa svijetom u kojem mnogo manje ljudi putuje. To se svekoliko odrazilo i na događaje poput sajmova i konferencijskih događaja, koji su otkazani ili odgođeni u cijelom svijetu. Njemački organizator konferencija Hotelreservierungs und Tagungsmanagement (HUT) tražio je privremeno rješenje za ponovnu organizaciju događaja, a našao ga je u ponudi kompanije Hikvision.

## Izazov

HUT organizira događaje za EHI Retail Institute, njemačko tijelo nadležno za maloprodajne subjekte. Prije uvođenja karantina taj institut je u februaru 2020. uspješno održao jedan od najvećih maloprodajnih sajmova u Evropi – EuroShop u Düsseldorfu. Tokom godine su ponovo procijenili situaciju i odlučili da će se budući događaji odvijati isključivo u hibridnom formatu. To je značilo da će se više aktivnosti odvijati na internetu i da je trebalo poduzeti stroge higijenske i mjere za kontrolu pristupa. HUT-u je bio potreban način da unaprijed testira sve posjetioce, uključujući učesnike, izlagачe i zaposlenike, te da osigura da svi nose maske. Kao dio strogog režima nadzora, bilo je potrebno omogućiti i da se te informacije prikažu na šalteru s informacijskim terminalom na kojem osoblje može nadgledati situaciju i djelovati po potrebi. Iako privremeno karaktera, ponuđeno rješenje moralo



se postaviti na sve ulaze i izlaze za vrijeme održavanja događaja. To je uključivalo i vrijeme montaže i demontaže.

## Rješenje

Rješenje koje je ponudio Michael Telecom sastojalo se od tri Hikvisionova MinMoe terminala za mjerjenje temperature (DS-K1T671TM-3XF), koji su postavljeni na ulazu u objekat radi kontrole prijema. Svaki terminal opremljen je vlastitim Wi-Fi ruterom kako bi se uspostavila komunikacija sa 7-inčnim monitorom, a svi uređaji su fleksibilni i mogli su se koristiti u pokretu. MinMoe terminali uključuju širokougaoni objektiv od 2 MPx i termalni senzor, koji omogućava mjerjenje temperature na površini kože dok neka osoba gleda u ekran. Temperatura se može prikazati na ekranu, a svaka vrijednost koja

je veća od unaprijed određenog nivoa šalje se operateru u vidu obavještenja. Pametna funkcija kamere podrazumijeva mogućnost praćenja da li neka osoba nosi masku ili ne. Status se može prikazati na ekranu, uz upozorenje o odsustvu maske koje se šalje osobljiju. Na informativnom šalteru instalirana je 7-inčna unutrašnja stanica s dodirnim ekranom (DC-KC001), koja osobljiju pruža mogućnost detaljnog praćenja situacije. Osoblje po potrebi može djelovati na temelju upozorenja i držati na oku situaciju na ulazu. "Proizvodi su se pokazali veoma fleksibilnim i ponudili su nam mnoštvo mogućnosti kako bismo ispunili sve naše potrebe u različitim scenarijima. Dodatni bonus je činjenica da su jednostavniji za upotrebu i postavljanje", kaže Bauer. ▲



SLUČAJ IZ PRAKSE

# RJEŠENJE ZA ZAŠTITU OBJEKATA, LJUDI I OKOLINE

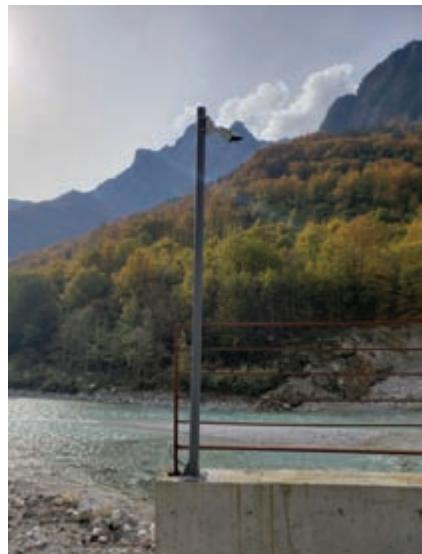
**ENERGETSKI SEKTOR VAŽAN JE DIO PORTFOLIJA GENERA 2, A HE DRAGOBIA JE NJEGOV NAJNOVIJI PROJEKAT NA RIJECI VALBONA, U SJEVERnim ALPAMA ALBANIJE. SASTOJI SE OD DVije MALE RIJEČNE HIDROELEKTRANE S UKUPNOM SNAGOM OD 21,9 MW. KOMPLEKS JE ZAŠTIĆEN NAPREDNIM AXISOVIM SISTEMOM**

■ Piše: Predrag Aćimov, proizvodni menadžer za tehničku sigurnost i telematiku za Jugoistočnu Evropu, Ingram Micro predrag.acimov@ingrammicro.com M: + 381 64 822 75 61

Sistem su implementirali Ingram Micro, najveći distributer IT i sigurnosnih sistema na svijetu, i Synapse ATS, lokalni partner Ingram Microa i Axis Communicationsa. Synapse ATS je albanski sistem-integrator, prepoznatljiv po stručnosti na polju umrežavanja, tehničke sigurnosti i rješenja za podatkovne centre. Odabrali su Axis Communications kako bi ponudili pouzdana i kvalitetna nadzorna rješenja za kritičnu infrastrukturu i industrijska postrojenja. To je bio jedini proizvođač koji je bio u stanju efikasno odgovoriti na složene zahtjeve klijenata i zadobiti njihovo povjerenje. Sistem je instaliran u dvije faze u skladu s procesom izgradnje obje hidroelektrane. Veliki izazov bilo je pronaalaženje odgovora na potrebe dva nova objekta, što nije bilo moguće bez tehničkog i sigurnosnog znanja i logističke podrške kompanije Ingram Micro, uključujući globalnu infrastrukturu i fokus na opskrbu i životni ciklus sigurnosnih sistema.

## Korišteni proizvodi

Videonadzorno rješenje temeljilo se na Axisovim mrežnim kamerama i dodacima, serverima i sistemu zaštite perimetra. Ukupno 42 kamere pokrivaju dvije elektrane, dva usisnika vode, dva tlačna kanala, ogradu i razvodno postrojenje. Kamere se koriste za zaštitu perimetra i objekata te praćenje da li se osoblje pridržava si-



gurnosnih i operativnih propisa. Najbolje iskoristene mrežne kamere bile su modeli AXIS P1435-LE s IC svjetlima i odličnim režimom rada noću, a korištene su i AXIS P3245-LV kamere za unutrašnje prostorije, PTZ kamere P5655-E s vrhunskim performansama i termalne kamere AXIS Q1941-E zbog izvanredne mogućnosti detekcije i kvalitetne videoanalitike, kao i razglasni zvučnici AXIS C1310-E i sistem zaštite perimetra. Sve sigurnosne kamere lokalno pohranjuju podatke na 64 GB microSD kartice, a snimanje se vrši pomoću dva AXIS S1132 servera stанице kamera. Kamere su postavljene unutar i izvan svih objekata i povezane su sa centraliziranim nadzornim sobama putem optičke mreže i infrastrukture industrijske klase.

## Integrisana zaštita

Izvedene su tri različite primjene korištenog CCTV sistema: zaštita perimetra i objekta, nadgledanje kritičnih operacija, procesa i zaštite radnika te osiguravanje pridržavanja zdravstvenih i sigurnosnih propisa. Zaštitom perimetra i objekta upravlja sigurnosno osoblje koje ima pristup zaštićenom objektu. Za drugu i treću primjenu odgovorni su menadžeri u kontrolnoj sobi i prateće osoblje, koje može pratiti kritične komponente i provjeravati jesu li radnici ugroženi, npr. tokom rada u blizini ventilacijskih otvora u slučaju hitnog ispuštanja vode, kao i jesu li kvalitetno opremljeni ličnom zaštitnom opremom u skladu sa zdravstvenim i sigurnosnim pravilima. ◀



Smart Building Technology Germany

VRIJEME JE ZA "VIRTUELNE" KABLOVE

# JEDNOSTAVNI, BEŽIČNI I SIGURNI PAMETNI OBJEKTI

**FROGBLUE POTROŠAČIMA I INSTALATERIMA NUDI NOVI I JEDNOSTAVAN NAČIN ZA PRISTUP RJEŠENJIMA ZA PAMETNE DOMOVE.** SVE SE ODVIJA BEZ KABLOVA I CENTRALNE UPRAVLJAČKE JEDINICE, BEZ DUGOTRAJNIH RADOVA, IT TEHNOLOGIJE I UPRAVLJAČKOG ORMARIĆA, KAO I BEZ PROSTORA U PODDISTRIBUTERU I CLOUDA

■ Piše: Aleš Polajnko, direktor, ORG. TEND  
ales.polajnko@tend.si

Ovaj zanimljivi sistem zasnovan je na tzv. žabicama, koje se mogu ugraditi čak i iza prekidača za svjetlo. Instalacija se može izvesti u duboko postavljenoj kutiji, spuštenom plafonu, izlazu sijalice, razvodnoj kutiji ili kutiji motora. Žabice čine osnovu bežične frogblue Bluetooth mreže koja nosi "virtuelne kablove" za druge žabice. Zbog automatskog slanja šifriranih poruka od žabice do žabice nema problema s dometom. Ovi intelligentni upravljački moduli povezani su na napajanje od 230 V i nude sve što je jednoj kući ili zgradi potrebno za normalno funkcioniranje.

## Bluetooth LE

Revolucionarno jednostavan i jeftin pametni dom je vizija mlade dinamične kompanije frogblue, čiji su proizvodi 100% rađeni u Njemačkoj. Bilo da je riječ o kontroli svjetla u zatvorenom i vani, automatiziranom zasjenjivanju ili složenim logičkim funkcijama za veću udobnost, sigurnost i održivost – s frogblue rješenjem svim navedenim možete upravljati na jednostavan način, tj. putem konvencionalnog prekidača/dugmeta za svjetlo te u kombinaciji s pametnim telefonom, tabletom i tehnologijom frogDisplay i frogKey. Kućna kontrola putem uspostavljenog Bluetooth LE (Low Energy) standarda postavlja nove trendove, posebno s obzirom na njenu energijsku efikasnost i održivost. Bilo da se automatski kontrolira samo jedno vanjsko

svjetlo ili pametno umrežava cijela kuća, sve je izvedivo bez ograničenja.

## Scenariji primjene

U jednom domu dovoljna su, npr., tri zatamnjivača kao osnova opreme za kuhinju, trpezaru i dnevni boravak. Oni se mogu konfigurirati tako da se naizmjenično aktiviraju za sve tri sobe. To znači da se prekidač za svjetlo u dnevnoj sobi može koristiti i za aktiviranje ili zatamnjivanje kuhinje i trpezare. Dodatne funkcije za veću udobnost omogućene su višestrukim dodjeljivanjem prekidača za svjetlo. Funkcija centralnog isključivanja može se aktivirati dvostrukim klikom i sve instalacije u kući će se pouzdano isključiti. Isto važi za dječiju sobu: ako noću svjetla trebaju svijetliti sa samo 30 posto snage, dovoljan vam je tek integrirani prekidač za prigušivanje svjetla, tj. prekidač opremljen žabicom. Osim toga, moguće je isključiti zvono na vratima tokom noći ili u nekom drugom terminu. Svjetlo u dnevnoj sobi će jednostavno zatreperiti, što omogućava djeci da nesmetano spavaju. Također, kada naruštate dom, svjetla u cijeloj kući moguće je isključiti jednim pritiskom na dugme, kao i spustiti roletne i prebaciti gri-

## Partneri u regiji

U saradnji s partnerskom kompanijom TEND, frogblue radi na predstavljanju svog rješenja na području Jadranske regije, pri čemu će se odabranim partnerima pružiti cijelovita podrška u oblasti prodaje, tehničke pomoći i projektnog planiranja. Svi zainteresirani partneri su dobro došli. Kontakt: frogblue@tend.si, www.frogblue.si



janje na način rada u odsustvu stanara. Ako su instalirani odgovarajući senzori, treperenje svjetla u hodniku može biti signal da ste ostavili otvoren prozor prije izlaska iz kuće. Osim toga, moguće je podesiti i alarm u slučaju da neko aktivira prekidač za svjetlo ili otvori unutrašnja vrata tokom vašeg odsustva. To pametni dom čini još sigurnijim. ▲





SVESTRANI SENZORI

# BEŽIČNI PREDAJNICI ZA OPTEX SENZORE

**OPTEX JE PROIZVODAČ VIŠOKOKVALITETNE SENZORSKE TEHNOLOGIJE, KOJI VEĆ 40 GODINA  
UŽIVA POVJERENJE HILJADA KUPACA ŠIROM SVIJETA ZBOG PRECZNOSTI I POUZDANOSTI SVOJIH  
DETEKCIJSKIH SISTEMA**

- Pripremio: OPTEX Security  
optex@optex.com.pl  
www.optex-europe.com

**B**aterijski napajani senzori kompanije OPTEX mogu raditi s bežičnim predajnicima bilo kojeg proizvođača, a većina predajnika se može smjestiti čak i u kućište senzora. Pojedini proizvođači bežičnih panela razvili su posebne predajnike s podrškom za dublju integraciju s OPTEX senzorima. No, ako pitate koji protivprovalni senzor tačno odabratiti, iz kompanije preporučuju sve baterijski napajane PIR senzore aktivne infracrvene i zrake s dvostrukom tehnologijom. Hoćete li koristiti jednokanalni ili dvokanalni bežični predajnik, to zavisi od primjene. Za "chime" notifikacije, pri kojima će detekcija osobe ili vozila biti označena putem zvučnog ili vizuelnog upozorenja, može se koristiti jednokanalni predajnik, dok bi se u sigurnosnoj primjeni trebao koristiti dvokanalni kako bi se pratili pokušaji onesposobljavanja senzora.

## Šta treba imati u vidu?

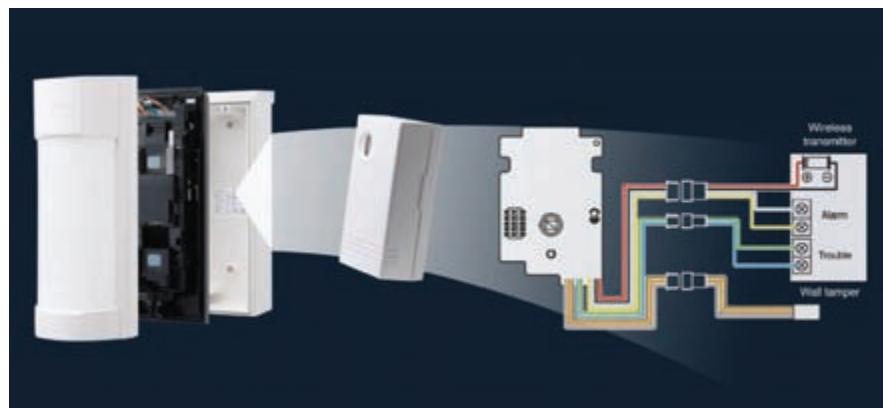
Prije implementiranja vanjskog bežičnog protivprovalnog sistema bitno je ispitati mogućnosti korištenja bežične tehnologije na datoј lokaciji. U naseljenijim okruženjima, u kojima se nalazi veliki broj građevina i metalnih objekata, postoji šansa da će domet bežičnog signala biti smanjen. Ukoliko jačina signala nije dovoljno dobra, preporučuje se korištenje bežičnog pojačivača signala. Ispitivanje bežičnog signala trebalo bi provesti pomoću odgovarajuće opreme. Prije izlaska na teren najbolja praksa podrazumijeva programiranje bežičnog predajnika u bežičnom

prijemniku. Na taj način tehničari mogu provjeriti da li oba uređaja – predajnik i prijemnik – rade kako treba i da li se alarmni i signal za prevenciju onesposobljavanja senzora ispravno emituju. Ukoliko je alarmni signal prethodno testiran, a ne funkcioniše na terenu, tehničari će znati da je to povezano s okruženjem te da nije u pitanju pokvaren uređaj ili greška u programiranju.

## Povezivanje bežičnog predajnika

OPTEX PIR-ovi i senzori sa dvostrukom tehnologijom mogu se napajati iz predajnika, a u tu svrhu su dostupna dva kabloska voda, jedan sa dva kabla i drugi sa četiri. Onaj sa dva kabla koristi se za prijenos signala za prevenciju onesposobljavanja senzora, a sa četiri za prijenos energije i alarmnog signala. Crveni i crni kablovi imaju konektore koji su smješteni između kontakata baterije i predajnika kako bi napajali uređaj. Bijeli i žuti kablovi se koriste za prijenos alarmnog signala. Kada su u pitanju ak-

tivne infracrvene zrake, situacija je drugačija – bežični predajnik ne bi mogao omogućiti dovoljno energije za napajanje i bežičnog predajnika i infracrvenih senzora. Međutim, bežični predajnik se može napajati pomoću bežične zrake ukoliko se koristi baterijski dodatak. Ukoliko imate dva bežična predajnika, to vam omogućava da pratite pokušaje onesposobljavanja senzora i nivoa napunjenošt baterije infracrvene predajničke zrake i primalačke zrake, kao i DQ dodatka za pojačavanje signala u nepovoljnim vremenskim uslovima ukoliko je dostupan. OPTEX-ove zrake dolaze s različitim kabloskim opcijama, tako da je potrebno pogledati uputstvo za svaku od njih. AX serija (dvostrukе zrake) nema kabloske vodove, dok SL-TNR serija (dvostrukе i hibridne zrake) ima dva kabloska voda za alarm i signal za prevenciju onesposobljavanja, a SL-QFR/QNR serija (četverostrukе zrake) ima tri kabloska voda za alarm, prevenciju onesposobljavanja i pojačavanje signala u nepovoljnim uslovima. ◀



## ASSA ABLOY

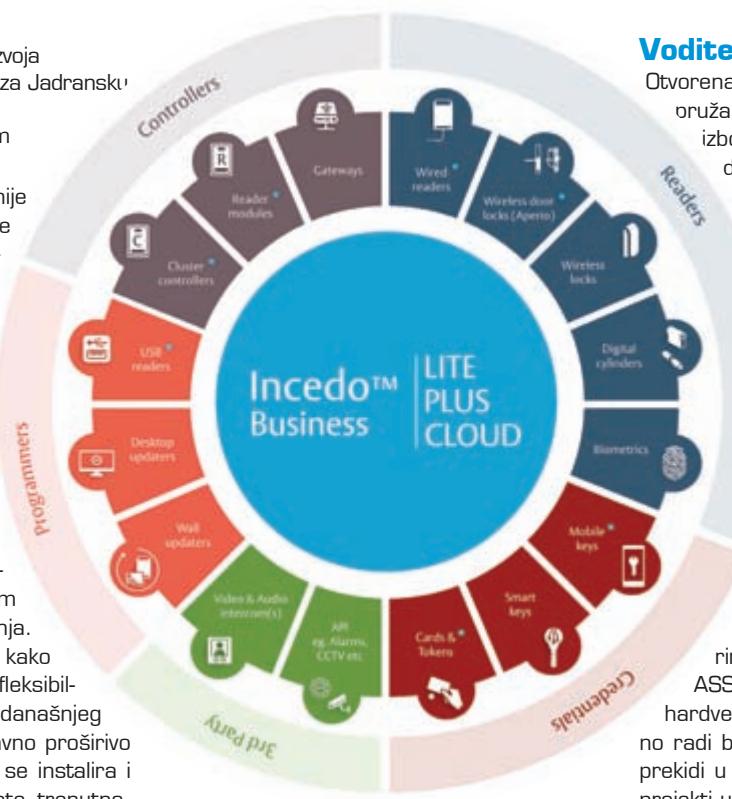
INCEDO BUSINESS PLATFORMA

# KONTROLA PRISTUPA KOJA VAM JE POTREBNA

**OVAJ UNIVERZALNI SIGURNOSNI SUSTAV KOMBINIRA HARDVER I SOFTVER U JEDNOM RJEŠENJU KONTROLE PRISTUPA.** INCEDO BUSINESS JE OTVORENA PLATFORMA DIZAJNIRANA ZA POBOLJŠANJE PRIKUPLJANJA PODATAKA OKO KONTROLIRANIH VRATA, ALI OSMIŠLJENA I KAKO BI OSIGURALA BESPRIJEKORNU INTEGRACIJU SA SVIM INCEDO HARDVEROM I DRUGIM PROIZVOĐAČIMA

■ Piše: Robin Vukelić, šef razvoja poslovanja za DAS proizvode za Jadransku regiju, ASSA ABLOY  
Robin.Vukelic@assaabloy.com

Uloga tehnologije nije samo slijediti trendove već i postavljati nove koji donose pametniju budućnost za sve. Organizacijama je potrebna jedinstvena, sveobuhvatna platforma koja uključuje usklađivanje, povezivanje i jednostavnost. Tu nastupa Incedo Business, sa sustavom koji kombinira svjetski vodeći ASSA ABLOY raspon pristupa hardvera i sigurnosnih rješenja s fleksibilnim softverom uz više mogućnosti upravljanja. Incedo sustavi su dizajnirani kako bi osigurali upotrebljivost, fleksibilnost i ažurnost zahtjeva današnjeg užurbanog svijeta. Jednostavno proširivo i beskrajno skalabilno, brzo se instalira i nadograđuje, a daje rezultate trenutno. Agilan je sustav koji se prilagođava najnovijim tehnološkim promjenama, intuitivno kombinirajući sigurne, povezane pristupne točke s inteligentnim tehnologijama



identifikacije, što ga čini idealnim rješenjem usmjerenim na budućnost. Incedo Business čini život lakšim i učinkovitijim za sve, od instalatera do krajnjih korisnika.

**S Incedo Businessom svijet je postao jednostavniji. Sada je moguće stvoriti potpune, integrirane sigurnosne sisteme brzo, jednostavno i isplativo**

### Voditelji postrojenja

Otvorena platforma Incedo Business oruža voditeljima postrojenja najširi izbor tehnologija i funkcija koje zadovoljavaju današnje i buduće sigurnosne potrebe, dok fleksibilni pretplatnički paketi nude i veću kontrolu nad troškovima. Osim toga, najsuvremenija povezivost poboljšava prikupljanje podataka i, u vezi s tim, donošenje odluka, tako da možete potaknuti kontinuirana i isplativa poboljšanja sigurnosti i učinkovitosti zgrada bez ugrožavanja kvalitete. Novi sustav koji povezuje sigurnosne i ostale sustave upravljanja zgradama, olakšava jednostavnu instalaciju, ažuriranja i nadogradnje - ne samo za ASSA ABLOY Incedo hardver već i hardver drugih proizvođača. Sve zajedno radi bespriječno kako bi se smanjili prekidi u radu te učinkovito održali ljudi i projekti u stalnom pokretu.

### Instalateri

Rješenja često zahtijevaju višestruke tehnologije i dobavljače, a poslovanje s više dobavljača može uvesti u nesigurnost i dovesti do većeg rizika i kašnjenja projekta. To su izazovi s kojima se instalateri suočavaju pri radu sa sigurnosnim sustavima. S Incedo Businessom svijet

je postao jednostavniji. Sada je moguće stvoriti potpune, integrirane sigurnosne sustave brzo, jednostavno i isplativo. Incedo je kompatibilan i s proizvodima drugih proizvođača te pruža snažnu i kvalitetnu platformu za mnogobrojne primjene, uz koju se sve kreće zajedno, bez dugotrajnog kašnjenja, rasprava ili gnjavaže. Omogućavanje besprijeckorne, početne integracije ASSA ABLOY uređaja za zaključavanje s hardverom i softverom drugih proizvođača pojednostavljuje instalaciju i isporuku projekta, pomaže vam uštedjeti vrijeme i trud, ispuniti rokove i premašiti očekivanja kupaca. S Incedom se sve kreće zajedno. Integracija je također moguća i s podsustavima kao što su video nadzor te grijanje, ventilacija i klimatizacija.

### Sistem-integratori

Savršena integracija i povezivost zahtijevaju jednostavno rješenje bogato funkcijama. To rješenje je ASSA ABLOY Incedo Business. Dizajniran kako bi osigurao besprijeckornu integraciju sa svim ASSA ABLOY Incedo hardverom, razvijat će se zajedno s proizvodima drugih proizvođača kako bi se osigurala laka proširivost i beskrajno skalabilno rješenje koje ima i dodatnu prednost: mogućnost upravljanja s jednog mesta. Uz Incedo Business moguće je upravljanje većim brojem zaposlenika, uključujući IT instalacije, sigurnost i ljudske resurse. Kombinirajući sustav otvorene platforme s prilagođenim paketom pametnih softverskih rješenja, sada je moguće stvoriti potpune integrirane sigurnosne sustave brzo, jednostavno i isplativo. Incedo će uskoro biti kompatibilan s proizvodima drugih proizvođača kako bi se osigurala snažna platforma za višestruku primjenu, tako da se sve kreće zajedno i bez dugotrajnih kašnjenja.

### Sistem-administratori

Provedba, upravljanje i praćenje sigurnosnih sustava specifičnih za korisnika i praćenje ažuriranja na svim lokacijama uz Incedo će biti znatno olakšano. On pruža i praktično rješenje i za zaboravlje-



### Krajnji korisnici

Krajnjim korisnicima Incedo Business omogućuje besprijeckorno povezivanje hardvera i softvera iz ASSA ABLOY assortimenta, ali i drugih pružatelja usluga, stvarajući kompletan, moderan sustav koji predstavlja vrhunsku praksu zaštite ljudi, imovine i informacija. Incedo Business radi s vama i za vas, pazeći da sve zajedno besprijeckorno funkcionira. Najbolji je omjer uloženog i dobivenog i zadovoljava trenutne, ali i buduće potrebe većine korisnika. Uz to, potpuno je certificirano rješenje temeljeno na cloud rješenju, koje omogućuje upravljanje sustavom i s mobilnih uređaja.

ne lozinke, stalni protok korisnika koji dolaze i odlaže, redovita ažuriranja i izazove praćenja sigurnosnih sustava specifičnih za korisnika, osiguravanje centralizirane



vidljivosti i kontrole usklađenosti u stvarnom vremenu – tko ima pristup i kako ga upotrebljava. Omogućujući povezivanje i upravljanje većim hardverskim i softverskim elementima unutar jedne platforme bogate funkcijama, Incedo Business poboljšava prikupljanje podataka kako bi se poboljšala vidljivost i performanse uz istodobno smanjenje složenosti i dugotrajnih aktivnosti, uključujući ažuriranja i upravljanje većim brojem sudionika. Osigurava sustav i lude koji se i dalje učinkovito kreću zajedno, povećavajući produktivnost, ali i zadovoljstvo svih unutar sistema.

Platforma Incedo Business također ispunjava očekivanja s dostupnim budžetom i daje najširi izbor tehnologija i značajki koje zadovoljavaju današnje i buduće sigurnosne potrebe. ▲

Nova vrsta hakerskih napada

# GLASOVNA KONTROLA BEZ KORIŠTENJA GLASA

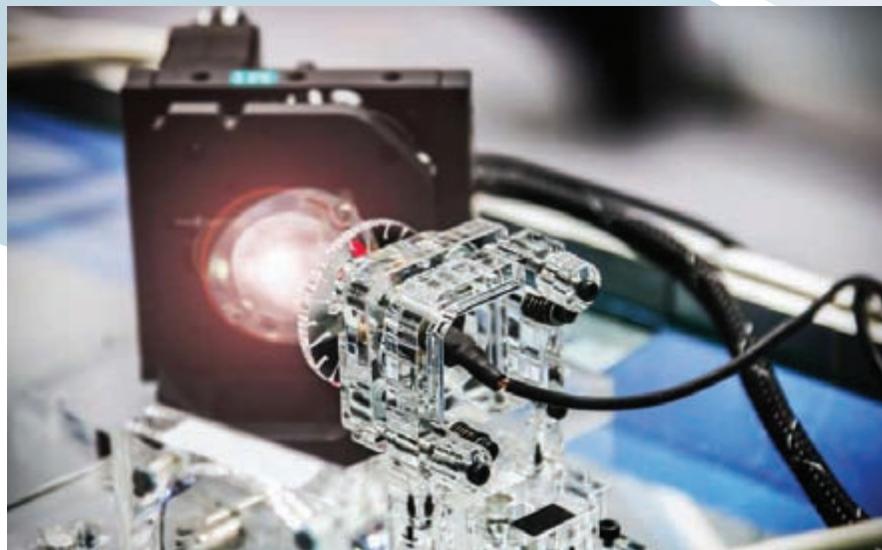
**PROTEKLIMA NEKOLIKO GODINA OTKIVEN JE NOVI METOD CYBER NAPADA – LASERSKO UBACIVANJE KOMANDI U UREĐAJE KONTROLISANE GLASOM.** NAIME, CYBER SIGURNOSNI ISTRAŽIVAČI SU OTKRILI DA MIKROFONI REAGUJU NA SVJETLOST ISTO KAO I NA ZVUK. KELLY JACKSON, DIREKTOR CYBER SIGURNOSNOG PORTALA DARK READING, ISTRAŽIO JE KAKO SU POKUŠAJI HAKIRANJA PAMETNIH DIGITALNIH KUĆNIH ASISTENATA POMOĆU LASERSKIH POKAZIVAČA POKRENULI NIZ NOVIH PITANJA O SIGURNOSTI TIH UREĐAJA

■ Izvor: Dark Reading  
redakcija@asadria.com

**Sigurnosnim istraživačima** s Univerzitetom u Michiganu i Univerziteta za elektronske komunikacije u Tokiju i dalje je misterija šta im je to tačno fizički omogućilo da pomoću laserskih pokazivača ubace komande u ugrađene mikrofone Amazon Alexa, Google Homea i drugih digitalnih glasovnih asistenata. Pretprošle godine uspešno su iskoristili novi tip hakerskih napada – ubacivanje komandi pomoću svjetlosti – kako bi kontrolisali Amazonovog digitalnog asistenta Alexa, Facebook Portal i Apple Siri. Pri tome su iskoristili propust u takozvanim MEMS mikrofonima tih uređaja, koji im je omogućio da svjetlosne zrake iskoriste za ubacivanje nevidljivih i nečujnih komandi u digitalne asistente, kao i glasovno kontrolisane pametne telefone i tablete. Čak im je pošlo za rukom da to urade s udaljenosti od 110 metara, kroz prozore, što znači da se razni sigurnosni sistemi i druge funkcije pametnih domova mogu relativno lako modifikovati i isključivati iz susjednih objekata, preko ulice i sl.

## Kako je moguće?

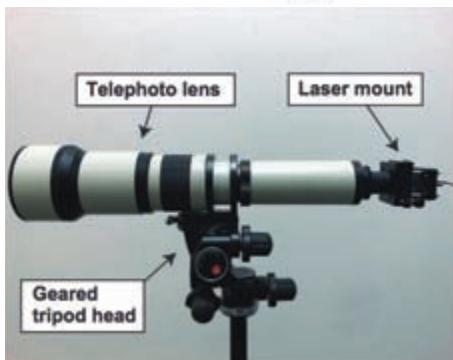
Sada isti tim provodi detaljniju istragu da bi otkrili kako je to moguće. „Još postoji određena misterija vezana za način kako ovo funkcioniše. Detaljnije istražujemo ovu problematiku“, kaže Benjamin Cyr, student na doktorskom studiju na Univerzitetu u Michi-



**Sigurnosni stručnjaci ističu kako čitav ekosistem glasovno kontrolisanih asistenata, koji obuhvata pametne brave, prekidače u pametnim domovima i automobile, ima zajedničke sigurnosne propuste koji svjetlosne hakerske napade čine još opasnijim**

ganu, koji je s istraživačicom Sarom Rampazzi predstavio najnovija saznanja na Black Hat Europe konferenciji 10. decembra. „Zašto mikrofoni reaguju na svjetlost kao da je zvuk? Želimo otkriti šta se to dešava na fi-

zičkom nivou, tako da u budućnosti hardver bude zaštićen od hakerskih napada pomoći svjetlosti“, pita se on. Sada proučavaju sigurnost sličnih sistema, uključujući i one koji se nalaze u medicinskim uređajima, autono-



mnim vozilima, industrijskim sistemima – pa čak i sistemima u svemirskoj tehnologiji.

Cyr, Rampazzi, koja je asistentica na Univerzitetu u Floridi, i Daniel Genkin, asistent na Univerzitetu u Michiganu, demonstrirali su kako se sigurnosnom kamerom može manipulisati pomoću hakiranog glasovnog asistenta s kojim je povezana. Tačnije, demonstrirali su svjetlosni hakerski napad na Echo 3, noviji model Amazonovog pametnog zvučnika, koji nije bio dostupan prošle godine kada su prvi put testirali novi tip napada na Echo, Siri, Facebook Portal i Google Home. Cyr kaže da istraživači još nisu imali prilike da testiraju četvrtu generaciju Echo zvučnika.

### Širok spektar slabih tačaka

Ovi sigurnosni stručnjaci su se dotakli i toga kako čitav ekosistem glasovno kontrolisanih asistenata, koji obuhvata pametne brave, prekidače u pametnim domovima i automobile, ima zajedničke sigurnosne propuste koji svjetlosne hakerske napade čine još opasnijim. Njihov tim, ukratko, pokazuje kako korištenje digitalnih asistenata kao kontrolne tačke pametnog doma može napadačima omogućiti da preuzmu kontrolu nad drugim uređajima u kući. Osim toga, Cyr je demonstrirao kako tačno laserska zraka zvuči kada dođe do mikrofona digitalnog asistenta. U korijenu istraživanja se nalazi problem eksplozivnog rasta popularnosti interneta stvari

### Napadi iz susjednih zgrada

Propust u glasovno kontrolisanim uređajima koji omogućava korištenje laserskog pokazivača za hakiranje glasovnih asistenata i pametnih telefona prvo je bio u 2019. otkrili Takeshi Sugawara s Univerziteta za elektronske komunikacije u Tokiju te Benjamin Cyr, Sara Rampazzi, Daniel Genkin i Kevin Fu s Univerziteta u Michiganu. Jedan od napada koje su uspješno proveli obuhvatao je usmjerenje laserske zrake s obližnjeg tornja u kancelariju kroz prozor na četvrtom spratu uredske zgrade. Modulirana laserska zraka uspješno je izdala komandu Google Home uređaju, nakon čega je dočinio otvorio vrata garaže u zgradama i tako omogućio lagan ulaz napadačima.

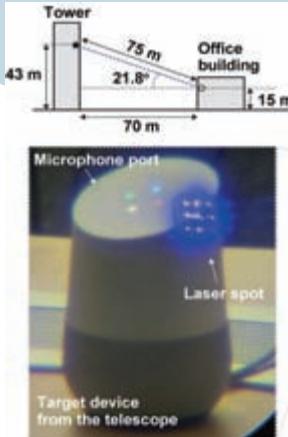
na tržištu, koje u principu nije izgrađeno na osnovu sigurnosnih aspekata i principa. "Želimo razumjeti na koji se način možemo braniti od ovih propusta. Naš krajnji cilj je zaštititi sistem i učiniti ga otpornijim, ne samo na vrste napada koje smo otkrili nego i na buduće koji još nisu otkriveni", kaže Rampazzi.

### Svetlosne komande i igračke

Istraživači su potrošili samo 2.000 dolara na opremu za izvođenje ovih napada, koje su opisali kao "napadi pomoću svjetlosti". U tu opremu spadaju laserski pokazivači, laserski kontroleri i zvučna pojačala. Međutim, oni nagađavaju da je to moguće izvesti i za samo 100 dolara, koristeći jeftini laserski pokazivač za mačke koji se može kupiti na Amazonu. "Laseri s Amazona koje smo kupili bili su za mačke", objašnjava Cyr. Za napade s većim

udaljenosti kupili su teleobjektiv, koji im je omogućio da lasersku zraku precizno usmjeri ka metu te su enkodirali laserski moduliran signal za mikrofon. "Lasersku zraku usmjeravate prema akustičnom dijelu mikrofona, nakon čega se ona konvertuje u akustični signal. Stoga voltažni signal izgleda potpuno isto kao da je uzrokovani akustičnim signalom", kaže Cyr. To omogućava davanje komandi glasovno kontrolisanim uređajima, kao što su uređaji za otvaranje garažnih vrata, pametne brave i kamere u okviru sigurnosnog sistema pametnog doma. Istraživači su podijelili svoja saznanja s Amazonom, Googleom i drugim kompanijama prije nego što su ih objavili u okviru početnog ispitivanja prethodne godine. Rampazzi kaže da je Amazon od tada nadgradio softver Alexa na način koji onemogućuje potencijalnom napadaču da metodom sirove sile otkrije PIN uređaja. "Nova generacija uređaja također ima zaštitu na mikrofonu", ističe Rampazzi, mada istraživači još ne znaju da li ta promjena predstavlja odgovor na informacije o novoj vrsti napada laserom. Ta zaštita otežava pronalaženje tačnog mesta na kojem se nalazi mikrofon s ciljem svjetlosnog ubacivanja komandi u uređaj.

Ona kaže da bi proizvođači mogli napraviti i druge promjene na hardveru kako bi zaštitili uređaje od svjetlosnih hakerskih napada, kao što je dizajniranje mikrofona tako da ne budu podložni svjetlu ili dodavanje autorizacijskih tehniku u softver, tako da neovlašteni korisnik ne može upravljati glasovnim asistentom. ◀



Izazovi cyber sigurnosti

# VAŽNOST KONVERGENCIJE FIZIČKE I CYBER SIGURNOSTI

**CYBER SIGURNOST OSTAJE VISOKO NA POPISU SIGURNOSNIH PRIORITETA, POSEBNO U VREMENU KADA JE PANDEMIA KORONAVIRUSA NATJERALA BROJNE ORGANIZACIJE DA ZAPOSLENICIMA OMOGUĆE DALJINSKI PRISTUP POSLOVNIM RESURSIMA. OVAJ TREND JE PRATIO I RAST SVIJESTI O VAŽNOSTI KONVERGENCIJE FIZIČKE I CYBER SIGURNOSTI, ŠTO PODRAZUMIJEVA ŠIRU SARADNUJU TIMOVА ZADUŽENIH ZA OBA SEGMENTA NA NIVOU KOMPANIJA**

■ Piše: Mirza Bahić  
mail: redakcija@asadria.com

**Kako se situacija** s pandemijom neće promjeniti preko noći, donosimo vam pregled mjera i praksi koje možete početi primjenjivati praktično od sutra, a sve s ciljem jačanja segmenta cyber sigurnosti kod kojeg već jedna greška može imati skupe i dugoročne posljedice po poslovanju.

## Ranjivost organizacija na cyber napade

Problem cyber sigurnosti posljednjih godina je dobijao na važnosti na gotovo linearan način. Uspon novih tehnologija poput interneta stvari (IoT) i sveprisutne povezanosti uređaja svih profila na mrežu pratio je i rast interesa za ovaj vid nefizičkih prijetnji sigurnosti kompanija i domova. Ipak, izbjeganje pandemije skrenulo je pažnju na slabosti cyber sigurnosti na jedan posve neočekivan način, a sve se odvijalo paralelno s masovnim širenjem IoT uređaja. Od lokalnog mikronivoa, poput pojedinačnih pametnih domova, sve do velikih korporacija pomama za mrežnim funkcijama odškrinula je vrata novim mogućnostima, ali i slabim tačkama koje hakeri mogu lako zloupotrijebiti. Kako se većina poslova prebacila na rad na daljinu, timovi za cyber sigurnost morali



**Pojedinačna cyber sigurnost svakog uređaja postaje prednost tek ako su ostale karike u tom lancu podjednako otporne na napade, što potvrjava važnost detaljne provjere proizvođača**

su svjesno oslabiti zaštitne mjere kako bi radnicima na daljinu omogućili pristup poslovnim mrežama. Hard diskovi s osjetljivim

podacima morali su postati otvoreniji za pristup, a kompanije su bile prinudene zatvoriti jedno oko na sigurnosne mjere kako

bi uopće bile u stanju nastaviti poslovati. Hakeri su priliku prepoznali i u činjenici da je dosta poslovnih zgrada u ovoj eri ostalo poluprazno. Pri tome je na terenu ostala infrastruktura ranjiva na cyber napade, s tim da je ona sada dodatno izložena zbog odsustva osoblja zaduženog za njenu zaštitu. Manje radnog osoblja znači i manju vidljivost same opreme, što smanjuje prostor za blagovremenu detekciju napada i njihovu prevenciju. Istovremeno, sigurnosni ambijent domova iz kojih zaposlenici rade već je po definiciji ranjiviji u odnosu na poslovno okruženje i to dodatno usložnjava situaciju. No, je li ona doista beznadežna? Odgovor je, srećom, negativan, ali traži proaktivni pristup i inteligentno upravljanje resursima za cyber sigurnost.

### **Je li pametno ujedno i sigurno?**

U poslednjih nekoliko mjeseci zabilježen je do sada najveći nivo ulaganja u IoT sisteme u pametnim domovima i kompanijama. Više uređaja je povezano na mreže nego ikada ranije, a uprkos ovom povoljnem investicijskom trendu, ulaganje u cyber sigurnost i dalje se tretira kao manje važna stavka. Istovremeno, hakerski upad u samo jedan sistem ovog tipa može uzrokovati štetu čija vrijednost premašuje svaku investiciju u cyber sigurnost. Važna stvar koju treba imati na umu je da vas naljepnica s oznakom "pametno", koja se koristi za brojne umrežene uređaje, ne smije zavarati da je tretirate kao sinonim za "sigurno". Zapravo, posve je moguće da vaš pametni uređaj uopće nije zaštićen od cyber napada, pri čemu je važno znati da se danas i sistemi koji se tradicionalno koriste za tehničku sigurnost (poput kamera) moraju tretirati kao IoT uređaji. Prilikom cyber napada u jednom kasinu u Las Vegasu u 2018. hakeri su probili zaštitu ovladavanjem običnim, pametnim termometrom. Zato, ako niste u stanju zaštiti svaki umreženi uređaj, onda nema potrebe nići na umrežavanje sve dok se kriterij sigurnosti u potpunosti ne zadovolji i to ovaj slučaj zorno prikazuje. Tu se javlja i jedna kvaka, jer možete nabaviti uređaj koji je označen kao otporan na cyber napade, ali ga priključivanjem na pametnu, ali neosiguranu mrežu zapravo činite nezaštićenim.

### **Neophodna saradnja sektora**

Priča o konvergenciji dvije ključne komponente sigurnosti kao cjeline već dugo je u centru pažnje stručne javnosti i korisnika, a u vezi s njom postoje i brojne zablude i



### **Sigurnost ugrađena u dizajn i provjera ponuđača**

Koncept sigurnosti ugrađene u dizajn (secure-by-design) potencijalni je lijek za sve slabe tačke cyber sigurnosti u svijetu sveprisutnog rada od kuće i proliferacije IoT uređaja. Ukratko, sa cyber zaštitom se počinje od samog postupka odabira ponuđača usluga ili tehnologija. Oslanjanje na kriterij cijene kao jedini otvara vrata nabavci uređaja ranjivih na hakerske napade, čija upotreba zbog samog karaktera IoT mreže može lančano ugroziti i ostale sisteme. Svakog proizvođača opreme neophodno je detaljno provjeriti u smislu pridržavanja koncepta sigurnosti ugrađene u dizajn i primjene politika i smjernica iz oblasti cyber sigurnosti. Pri tome morate znati da, makar univerzalni, ovi koncepti i politike imaju drugačije značenje za uređaje koji se koriste u poslovnom okruženju i one u, naprimjer, pametnim domovima. Svaki proizvod mora biti provjeren u odnosu na temeljne standarde cyber sigurnosti. Fondacija za sigurnost interneta stvari (IoT Security Foundation), naprimjer, nudi smjernice prilagođene za različite sektore, a slično rade i specijalizirane kompanije kao što su CSI i druge. Tu su i različiti vodići i politike za otklanjanje ranjivosti na cyber napade.

pogrešne percepcije. Za početak, osoblje iz oba sektora sigurnosti unutar organizacija mora predstaviti tehnologiju koju koristi svojim kolegama i postati dio specijalističkog sigurnosnog tima s integriranim nadležnostima. Menadžeri sigurnosti moraju se potruditi da steknu barem osnovna znanja o cyber sigurnosti, ako ne putem plaćenih obuka i obrazovnih programa, onda barem pomoću besplatnih kurseva i certifikata. Isto važi i obrnuto, pri čemu se vrata komunikacije otvaraju već običnim odlaskom "na kafu" kao neformalnim uvodom u održavanje redovnih sastanaka o temi integralne sigurnosti. U ovoj eri pristup svakom tipu sigurnosti kao silosu ili dvorcu koji treba zaštititi više ne može dati želje-

ne rezultate. Kompanije će, umjesto toga, morati osnovati sigurnosne centre u kojim fizička i cyber sigurnost moraju biti objedinjene, uz razmjenu informacija o sigurnosnim trendovima, razvoju IoT-a, zaštiti privatnosti, usklađenosti s GDPR direktivom i drugim pitanjima. Razmatrane politike moraju obuhvatiti i tehnička pitanja poput dinamike promjene lozinki, integracije s rješenjima drugih proizvođača, HTTPS enkripcije, zabrane pristupa na daljinu, korištenja pouzdanih platformi i zaštićenih elemenata, strategije primjene firmvera i slično. Na kraju, do objedinjavanja dva sigurnosna svijeta pod jedan krov će neminovno doći, jer će kroz integraciju obje komponente svaka od njih postati sigurnija. ◀

Smart Home

# UMJETNOST, NAUKA I SIGURNOST U PRIVATNOSTI DOMOVA

KUĆNE NADZORNE KAMERE  
POPULARNIJE SU NEGO IKADA.  
PREMA IZVJEŠTAJU KOMPANIJE  
GRAND VIEW RESEARCH, TO JE TRŽIŠTE  
DOSTIGLO VRIJEDNOST 3,7 MILIJARDI  
DOLARA U 2019. GODINI, A OČEKUJE SE I RAST OD  
15,7% DO 2027. GODINE. ALI, POVEĆANJE NJIHOVE  
POPULARNOSTI DOVODI DO OPASNOSTI OD INVAZIJE NA  
NAŠU PRIVATNOST. NEKOLIKO STUDIJA POKAZUJE DA SU IP  
KUĆNE KAMERE NAJRANJIVIJE NA HAKERSKE NAPADE



■ Izvor: a&s International  
redakcija@asadria.com

**Tehnologije** za pametne domove dizajnirane su da učine život jednostavnijim i udobnijim. Ali, nove udobnosti donose i nove probleme. Bilo da je riječ o kućnoj IP kameri ili baby monitoru, kamere dolaze s rizikom od narušavanja naše privatnosti koji se, čini se, ne može izbjegći. Zato preporučujemo nekoliko jednostavnih koraka prije kupovine i ugradnje kućne sigurnosne kamere.

## Istražite ranjivosti

Prije kupovine uređaja potražite na internetu vijesti o potencijalnim ranjivostima tog uređaja. Vitaly Kamluk, direktor Global Research and Analysis tima za Azijsko-pacifičku regiju u kompaniji Kaspersky, tvrdi da je IoT goruća tema te da istražitelji daju sve od sebe kako bi pronašli sigurnosne probleme u proizvodima ovog tipa. Sigurnosni analitičari su možda već pregledali uređaj koji želite kupiti, a velika je mogućnost i da je eventualni problem u uređaju već "zakrpljen". Joe Tham, suosnivač kompanije Simshine Intelligent Technology, dodaje da prije kupovine sigurnosne kamere možete preuzeti njihovu aplikaciju i pročitati njihovu politiku o zaštiti privatnosti te saznati koje će podatke kompanija prikupljati i kako će ih koristiti. Proizvođači bi trebali koristiti vaše podatke u skladu s GDPR-om. "Kompanija bi trebala koristiti AES enkripciju kako bi zaštitila lozinke i tokove korisnikovih videopodataka. Ako korisnik želi naprednije funkcionalnosti, kao što su detekcija osoba ili prepoznavanje lica, preporučuje se da odabere nadzornu kameru koja obrađuje podatke na samom uređaju. Proizvođači koji prave kamere s obradom podataka u cloudu često koriste fotografije i videoe korisnika za unapređenje svoje vještačke inteligencije", kaže Tham, ustvrdivši da bi korisnici zato trebali imati opciju da sačuvaju video direktno na uređaj, umjesto postavljanja svega na cloud server.

## Izbjegavajte "novo na tržištu" proizvode

Ponekad nije najbolja ideja kupiti proizvode koji su tek došli na tržište, tvrdi Kamluk. Osim standardnih bugova koje obično dobijete uz proizvod, on može imati i sigurnosne probleme koji još nisu otkriveni. Najbolji savjet bi bio kupiti proizvode koji su već dobili nekoliko softverskih ažuriranja. "Bilo bi mudro pri odabiru uređaja koji će prikupljati podatke iz našeg privatnog

i života naših porodica, naprimjer sigurnosnih kamera, odabratи najjednostavniji RF model na tržištu. Takav uređaj će, bez pristupa internetu, emitovati samo zvučni signal", dodaje Kamluk.

## Upoznajte svoj uređaj

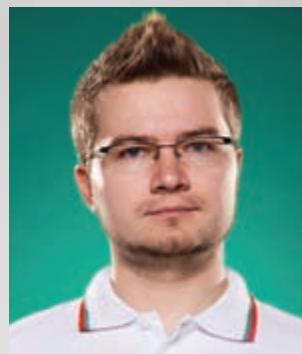
Naučite što više o uređaju koji posjedujete kako biste smanjili rizik od napada. Nekoliko alata, koji su dostupni online, mogu pomoći u ovome. Kaspersky je lansirao aplikaciju IoT Scanner – besplatno pametno rješenje za uređaje koje će provjeriti vašu Wi-Fi mrežu i reći vam jesu li spojeni uređaji sigurni ili ne.

## Završna riječ

Martin Hron, viši istraživač u kompaniji Avast Software, dodaje da je ključno izabrati renomiranog prodavača kako bi se osigurala privatnost podataka. Druga i možda najbitnija stvar je pravilno postavljanje uređaja, neostavljanje fabričke postavke i fabričke lozinke. Ostavljanje IoT uređaja na fabričkim postavkama i šifri je najčešći uzrok hakiranja uređaja. "Danas su mnoge kamere opremljene cloud funkcionalnostima, što može biti još jedan od uzroka napada jer se snimci i privatni podaci koji napuštaju perimetar vašeg doma pohranjuju na serverima trećih strana. U ovom slučaju više nego bitno je izabrati brend koji provjerovali koristi sigurnu cloud infrastrukturu. Ako niste sigurni u cloud sigurnost ili imate određene sumnje, potražite kamere u kojima je cloud funkcionalnost opcionalna", kaže Hron.

## Kako kućna nadzorna kamera narušava privatnost

Znati na koji način haker vrši upad je prvi korak ka zaštiti vaših podataka. Ali, ako



Vitaly Kamluk, Direktor tima za globalna istraživanja i analizu (GReAT) APAC, Kaspersky



Joe Tham, Suosnivač, Simshine Intelligent Technology



Martin Hron, Viši istraživač u polju sigurnosti, Avast Software

pitate Vitalija Kamluka, direktora tima za globalno istraživanje i analitiku (GReAT) za APAC regiju u kompaniji Kaspersky, većina IP kamera na tržištu nema sistem za zaštitu podataka. "Prosječna IP kamera dolazi skoro bez ikakve zaštite. Veoma je jednostavno hakirati sistem i ukrasti njen zapis. Svaka kamera koja je dostupna online posjeduje svoj mali web-sajt koji vam omogućava da je gledate na drugom kraju svijeta. Ovaj web-interfejs dolazi sa samostalnom upravljačkom konzolom i ima mogućnost promjene ugla snimanja, korištenja zooma, čak i zvuka. Ali, ova napredna konzola dolazi s rizikom. Specijalizirani sistemi za pretragu mogu jednostavno upratiti zapis iz nje", kaže Kamluk. Joe Tham, suosnivač kompanije Simshine Intelligent Technology, objašnjava da će haker provoliti u sistem kompanije i dobiti pristup korisničkoj bazi podataka i njihovim lozinkama. Onda će pokušati iskoristiti ovu informaciju pri logiranju u korisničke naloge u sigurnosnim kamerama. Mnogi ljudi iznova koriste isto korisničko ime.

## Česti scenariji

Martin Hron iz Avast Softwarea tvrdi da su dva scenarija najizglednija kada je curenje privatnih podataka u pitanju. Prvi može biti pogrešna konfiguracija rutera i neosiguranje kamere promjenom.

Neke kamere također koriste (obično fabrički) UPnP servis, koji, u saradnji s ruterom, dozvoljava pristup kameri direktno putem interneta, zaobilazeći pri tome ruter. "Problem je da ako vi kao korisnik zadržite fabričku konfiguraciju kamere, onda niste ni svjesni da je uređaj dostupan direktno putem interneta, na istoj IP adresi na kojoj je i vaš ruter. U kombinaciji s već postojećim ranjivostima

uređaja ili fabričkog korisničkog imena ili lozinke, ovo može pružiti jednostavan pristup kamери, a u nekim slučajevima i dublji pristup vašoj mreži", kaže Hron. Drugi scenario je preuzimanje vaših zapisa ili čak streamova koji se prenose uživo direktno s cloud servera, u slučaju da kamera posjeduje cloud pohranu. U tom slučaju upad i curenje privatnih podataka mogu biti ozbiljni, jer napadač uspijeva dobiti pristup cloud serveru i obično preuzeće podatke sa svih kamera istovremeno.

### Višefaktorska autorizacija kao spas

Još bolja ideja bila bi korištenje dvostrukе provjere autentičnosti, ukoliko je uređaj dozvoljava. Proizvođači koriste različite metode za pružanje višestruke provjere autentičnosti. Tham objašnjava da proizvodi njegove kompanije dolaze s LAN načinom zaštite korisnika od hakerskih upada. U LAN načinu korisnik može gledati video samo kada je njegov telefon povezan na isti Wi-Fi na koji je povezana i kamera. Ovaj način se može isključiti samo pomoću šeme za otključavanje telefona. Ako bi haker ušao u vaš nalog, ne bi vido ništa osim crnog ekrana. Glasnogovornik kompanije Canary Connect rezimira najbolje prakse ističući važnost korištenja snažnih lozinki i njihovog čestog mijenjanja. "Ažuriranje firmvera sigurnosne kamere je još jedan način zaštite uređaja. Naprimjer, uređaji kompanije Canary automatski ažuriraju svoj firmver kako bi osigurali korisnicima najnovije sigurnosne postavke. Ažuriranja se instaliraju na uređaju putem mobilnog interneta", kaže Tham.



**Kamere su danas opremljene cloud funkcionalnostima, što može biti još jedan od uzroka napada budući da se snimci i privatni podaci koji napuštaju perimetar vašeg doma pohnuju na serverima trećih strana**

### Je li vaša nadzorna kamera hakirana?!

Martin Hron tvrdi da je danas najveći izazov s IoT uređajima znati je li vaša kamera hakirana ili ne. Teško je zaštiti IoT, a samim time i sigurnosne kamere od hakiranja. Ali, prateći nekoliko osnovnih pravila, možete smanjiti rizik, pa čak i otkriti je li uređaj kompromitovan ili ne.

Ipak, to je prilično težak zadatak. Golim okom možete zapaziti čudna ponašanja. Naprimjer, ako je kamera opremljena funkcijama nagiba i naklona, možete zapaziti pokrete kamere bez razloga. Vitaly Kamluk navodi pet znakova pomoću kojih možete znati je li vaš uređaj hakiran:

1. Čudni zvukovi ili glasovi – u nekim slučajevima cyber kriminalac želi da znate da je prisutan. Oni čak mogu pokušati



kommunicirati s vama putem funkcije za dvosmjernu komunikaciju. Većina kućnih sigurnosnih kamera omogućava ljudima da komuniciraju s gostima s druge strane vrata. Ali, ako čujete čudne zvukove ili glasove, to vam je jasan pokazatelj.

2. Kad se LED svjetlo upali usred ničega, u slučaju unutrašnjih kamera, to je znak da se nešto čudno dešava. LED svjetlo u hakiranoj kamери može se ponašati abnormalno, mijenjajući status svjetla bez posebnog razloga. Ako se ovo desi, po-brinite se za zaštitu.

3. Pomicanje okna ili promjena ugla – većina kamera ima opciju podešavanja sigurnosnog okvira i uglova. Ali ako primijetite da su se ove postavke automatski promjenile, to bi vas trebalo zabrinuti. Bilo koja promjena u postavci kamere, koja je drugačija od one koju ste vi postavili, može biti znak da je kamera kompromitovana.

4. Promjena lozinke – ovo je, vjerovatno, najstrašniji scenario za kućnu sigurnosnu kameru. Ako ne možete pristupiti korisničkom nalogu kamere zbog promjene lozinke, a ne sjećate se promjene, to je čest znak da je uređaj hakiran.

5. Historija prijave na mrežu na aplikaciji – vaša historija konekcije u većini

## Problemi fabričkih lozinki

"Proizvođači i ponuđači cloud servera trebali bi vrijedno raditi na sprečavanju upada u njihove servere. Preporučuje se da ljudi izbjegavaju brendove sigurnosnih kamera koji su već bili meta hakerskih napada i odabratи kameru koja radi lokalno i posjeduje lokalnu pohranu podataka", kaže Tham. On dodaje da se problemi narušavanja privatnosti ne mogu u potpunosti izbjegći sve dok je uređaj povezan na Wi-Fi mrežu. Korisnici bi trebali kreirati komplikovane i jedinstvene lozinke, ne koristiti fabričke.

slučajeva može vam pokazati neodobrene aktivnosti. Provjeravajte historiju kako biste se uvjерili da nema pokušaja upada. I drugi eksperti dijele slična mišljenja, dodajući da je praćenje prijenosa podataka pouzdan metod za praćenje neovlaštenih upada. "Možete provjeriti da li kamera mijenja status LED svjetla, proizvodi zvučne, pomicne okno ili se zakrivilje sama od sebe. Drugi način je praćenje prometa na kameri koristeći funkciju praćenja na ruteru. Ako kamera prenosi ogromnu količinu podataka kada je ne koristite, to može značiti da je haker kontroliše", kaže Joe Tham. Hron objašnjava da je najbolja strategija praćenja na nivou mrežnog prometa. U tom slučaju potreban vam je dodatni uređaj za praćenje mrežnog pro-

meta sposoban da uoči nepravilnosti u radu vašeg uređaja (sigurnosna kamera ili neki drugi IoT uređaj). Takve nepravilnosti mogu značiti da se kamera povezuje na druge IP adrese, pored originalne u cloudu, ili na druge uređaje u vašem domu ili je neobično velik promet podataka koji vrši kamera.

## Kako integrisati pametni dom bez ugrožavanja privatnosti

Postoji citat koji se često koristi u IoT sigurnosti koji kaže da je mreža sigurna koliko i njena najslabija karika. To se nedovjedno primjenjuje na sigurnosne kamere. Općenito, uz kameru, ključni dio vaše mreže je ruter, jer je on poveznica



### ISTRAŽIVAČKI RAD

- izrada studija i analiza o funkcionalnosti i optimalnosti predviđene preventivne zaštite kroz investiciono tehničku dokumentaciju



### PREGLED I NADZOR

- pregled, ovjera i pružanje konsultantskih usluga za projekte iz oblasti zaštite od požara i zaštite na radu



### NORMATIVNA DJELATNOST

- izrada pravilnika iz oblasti zaštite od požara i zaštite na radu
- izrada planova zaštite od požara za preduzeća, javne ustanove, društveno političke zajednice i njihove organe



### PROIZVODNJA, MONTAŽA I SERVISIRANJE

- proizvodnja hidrantskih crijeva prema zahtjevu kupca
- izrada elemenata stabilnih sistema za gašenje požara
- montaža svih tipova automatskih sistema za gašenje požara



### OBRAZOVANJE

- obuka uposlenika iz oblasti zaštite na radu, zaštite od požara i rukovanja zapaljivim tečnostima i gasovima u prometu
- stručno usavršavanje za obavljanje poslova i radnih zadataka projektovanja, montaže, rukovanja i održavanja sistema



### PROJEKTOVANJE

- projektovanje specifičnih objekata sa aspekta zaštite od požara i zaštite na radu
- projektovanje automatskih stabilnih sistema za gašenje požara
- projektovanje sistema za dojavu požara i detekciju gase



### EKSPOZIIONA ZAŠTITA

- izrada elaborata o prostornom rasprostiranju i kategorizaciji zona opasnosti sa rješenjima protuexplozijske zaštite električnih uređaja i instalacija u tim zonama u svim slučajevima mogućih pojava eksploziono ugrožavajućih paro-gaso-prašinastih smjesa



### PRODAJA

- prodaja aparatova za gašenje početnih požara
- prodaja hidrantske opreme
- prodaja opreme i komponenti za stabilne uređaje za gašenje i dojavu požara
- prodaja opreme za zaštitu na radu



**PROVING**  
Društvo za protivpožarni inžinjering,  
marketing, istraživanje i razvoj

**PROVING d.o.o. Sarajevo**

UI. Milana Preloga bb, 71000 Sarajevo, BiH  
Tel/Fax: + 387 33 610 264; 663 100; 664 100  
E-mail: [info@proving.ba](mailto:info@proving.ba) - [www.proving.ba](http://www.proving.ba)



vaše privatne mreže i javnog interneta. "Pogrešna konfiguracija ruter, posebno ostavljanje fabričkog korisničkog imena i lozinke i neažuriranje su i dalje glavni uzročnici upada u mrežu. Odaje vam osjećaj da je kućna mreža u potpunosti sigurna jer je izolirana od ostatka interneta. No, barem jedan pogrešno konfigurisan uređaj može potencijalno ugroziti kompletну mrežu. Moderni trend u mrežnoj sigurnosti je mikrosegmentacija. To znači da biste trebali osigurati svaki uređaj povezan direktno na internet, a to podrazumejava jaku lozinku, gašenje uređaja koji se ne koriste i stalna ažuriranja", objašnjava Martin Hron. Druga opcija, koja je također preporučena, jeste izoliranje na druge mreže (segmente), tako da u slučaju upada ovi uređaji ne bi dotalici jedan drugog. Držati sve sigurnosne kamere odvojene od ostatka IoT uređaja i posjedovanje dodatne mreže za vaš kompjuter i NAS pohranu je preporučen setup.

## Pogrešna konfiguracija ruter, a posebno ostavljanje fabričkog korisničkog imena i lozinke i neažuriranje, i dalje su glavni uzročnici upada u mrežu. Barem jedan pogrešno konfigurisan uređaj može potencijalno ugroziti kompletну mrežu

### Izolirajte da biste zaštitali

Izoliranje od ostatka mreže ključni je korak u osiguranju doma. Ovo je relativno lako učiniti tako što ćete, npr., postaviti mrežu za goste vaših IoT kućnih uređaja. Naprimjer, vaš frižider može biti hakiran i postati dio botneta koji šalje spame ili rudari kriptovalute. "Međutim, budući da zauzima vlastitu mrežu, neće moći pristupiti vašem e-mailu ili bankovnom računu. Korištenje mreže za goste može poboljšati sigurnost vaše kućne mreže i na druge načine", objašnjava Vitaly Kamluk. Također osigurajte da su uređaji za pristup, nadzor i isporuku na vašoj mreži sigurni. To može uključivati pametne zvučnike, ruter, računar i pametni telefon. Ako vaš pametni telefon bude hakiran ili ukraden, mogao bi ugroviti cijelokupni sigurnosni sistem vaše kuće.

### Rizik oblaka i antivirusna rješenja

Sve dok integracija radi u oblaku, postoji i mogućnost ugrožavanja privatnosti. Zato neki entuzijasti za pametne domove radije grade lokalnu integraciju. Ako je vlasnik kuće inžinjer, on može povez-

ati dva uređaja pomoću API-ja sam ili putem privatne platforme treće strane. "Različite kompanije za pametne domove mogu stupiti u partnerstvo i integrisati svoje uređaje prije nego što ih korisnici dobiju. Jedna od misija naše kompanije je izgradnja ugrađenog AI sistema pametne kuće na intranetu", kaže Joe Tham iz Simshine Intelligent Technologyja. Korištenje pouzdanog antivirusnog i antimalverskog softvera na računaru, kao i mobilnim uređajima, također je dio cyber sigurnosti. Nekoliko većih kompanija danas nudi pametne programe za kibernetičku sigurnost za domove zajedno sa svojim cijelovitim paketima zaštite, a to bi uveliko moglo pomoći u zaštiti podataka. ◀



# ADRIA SECURITY SUMMIT

Sarajevo, Bosnia and Herzegovina, 15-16 Sep. 2021

powered by **intersec**



# See You in September



# SAVE DATE



## AGENCIJE ZA ŽAŠTITU LJUDI I IMOVINE SECURITY AGENCIES



88260 ČITLUK, Tromeđa bb  
tel/fax: (036) 650 052  
mob: 063 327 297  
e-mail:  
delta.security@tel.net.ba  
www.deltasecurity.org

d.o.o. Agencija za zaštitu ljudi i imovine

### TJELESNA ŽAŠTITA:

Zaštita osoba i objekata, usluge osiguranja vrijednosti u prijevozu, prijevoz i pratnja novca, usluge recepcionara, portira i čuvara.

### TEHNIČKA ŽAŠTITA:

Protuprovala i protuprednapna zaštita, vatrodojava, video nadzor, kontrola pristupa i radnog vremena, nadzorni centar - 24 sata.



## TEHNIČKA ŽAŠTITA TECHNICAL PROTECTION



Distribucija opreme za tehničku zaštitu  
Videonadzor • Vatrodojava  
Protuprovala • Kontrola prolaza  
Satelitsko praćenje  
Interfoni • Commax  
Quiko automatika

Obilazna cesta 23  
88220, Široki Brijeg  
tel.: +387 39 700 700  
fax: +387 39 700 701  
www.afp.ba; sales@afp.ba



**BOSCH**

Invented for life

**Bosch empowers you to build a safer, more secure and enjoyable world**

Bosch Security and Safety Systems Offices in the Region:

Croatia, Zagreb: Tel.: +385 1 295 8072  
Serbia, Belgrade: Tel.: +381 11 2052 381

[www.boschsecurity.com](http://www.boschsecurity.com)

**HIKVISION**

Video surveillance products and solutions



Hybrid DVR Digital Video Server



Speed Dome Network Camera Compression Card

UL CE FC Rohs ISO9001:2000 ISO14001

[www.hikvision.com](http://www.hikvision.com)

**INGRAM** MICRO®

Globalni i najveći IT distributer

### Hrvatska

Ingram Micro d.o.o. Zagreb  
<https://hr.ingrammicro.eu>

### Slovenija

Ingram Micro Ljubljana d.o.o.  
<https://si.ingrammicro.eu>

### Srbija, Bosna i Hercegovina, Makedonija, Albanija, Crna Gora

Ingram Micro d.o.o Beograd  
<https://rs.ingrammicro.eu>



## SECTOR SECURITY

Preduzeće za fizičko i tehničko obvezivanje i zaštitu

A: Siniša Mijatovića 9, 78 000 Banja Luka  
T: +387 51 461 115; F: +387 51 424 142

A: Dr. Silve Rizvanbegović b-1/13  
71 000 Sarajevo  
T: +387 33 782 985; F: +387 33 809 193

[www.sectorsecurity.org](http://www.sectorsecurity.org)

Nama Vjeruju.



### Regionalni lider u tehničkoj zaštiti

Alarm automatika d.o.o.  
Džemala Bijedića 156  
71000 Sarajevo  
Tel: +387 33 218 872  
Fax: +387 33 217 237  
sarajevo@alarmautomatika.com  
www.alarmautomatika.com

**ahua** Dahua Technology Co., Ltd.



1187 Bin'an Rd., Binjiang, Huangzhou, Zhejiang 310053, China  
Tel: (86-571)8768 8883, 2893 9666 | Fax: (86-571)8768 8815  
Email: overseas@dahuatech.com | www.dahuatech.com

CE FC CCC UL RoHS ISO 9001:2000

**D-Link®**

Building Networks for People

II Cijetno naselje 18, 10000 Zagreb Croatia  
Tel: +385 1 61 89 145; Fax: +385 1 61 89 144  
Email: ad-info@dlink.com; www.dlinkadria.eu



Wireless - Preklopniči - IP video nadzor  
Mrežna pohrana - Sigurnost - Podrška



- Standalone Access Control Readers
- Simple Access Control Hardware and Software
- Advanced Access Control and Time & Attendance Systems
- Time & Attendance Kits For Small Companies
- Key Management Systems



**Jantar**  
[www.jantar.si](http://www.jantar.si)



1313

[www.unilab.ba](http://www.unilab.ba) 033 / 657 999

**antenall**

ANSEC UNV FIRECLASS  
HIKVISION PARADOK ROGER  
ZKTeco CyberPower Ultracell

### ANTENALL d.o.o.

Ljiljana Krstić 24, 11000 Beograd  
Telefon: +381 11 6 356 356  
e-mail: office@antenall.rs; www.antennal.rs

### Antenal d.o.o.

Caru Dušana 149a, 78252 Trn, Laktasi, BIH  
Telefon: +387 51 586 094  
e-mail: office@antenal.ba; www.antenal.ba

**EVONA®**  
ALARM SYSTEMS

JABLOTRON  
CREATING ALARMS

### SMART ALARM



Dr. Ante Starčevića 62  
88000 Mostar, BIH  
+387 (0)34 348 033  
evona@evona.net  
www.evona.ba | www.jablotron.ba

**KAMIR**  
agencija

### AGENCIJA ZA USLUGE TEHNIČKE ŽAŠTITE



88220 Široki Brijeg, Obilazna cesta 23  
Tel: +387 (0)39 700 700; Fax: 700 701  
[www.kamir.net](http://www.kamir.net), [kamir@kamir.net](mailto:kamir@kamir.net)

**Advanced**

The Standard in Fire Systems



Tel: +44 (0)345 894 7000  
Email: [sales@advancedco.com](mailto:sales@advancedco.com)  
Web: [www.advancedco.com](http://www.advancedco.com)

**ASSA ABLOY**

The global leader in door opening solutions

### Slovenia

Tel.: +386 (0)4 280 77 44

[info@assaabloy.si](mailto:info@assaabloy.si)

### Croatia

Tel.: +385 51 684 710

[info@assaabloy.hr](mailto:info@assaabloy.hr)

**FUJIFILM**

Fujinon. To see more is to know more.



e-mail: [cctv\\_eu@fujifilm.com](mailto:cctv_eu@fujifilm.com)  
[www.fujifilm.eu/fujinon](http://www.fujifilm.eu/fujinon)

**KROBEL**

VELIKI IZBOR SIGURNOSNE OPREME

Visonic, HIKvision, Golmar, Teletek

### KROBEL PROMET d.o.o.

Remetinečka cesta 13, 10000 Zagreb  
Tel: +385(0)1 3640 343, Fax: 3664 134  
[krobel@krobel.hr](mailto:krobel@krobel.hr); [www.krobel.hr](http://www.krobel.hr)

### KROBEL d.o.o. Sarajevo

Ul. Safeta Zajke 115c, 71000 Sarajevo  
Tel: +387(0)33 466 800; Fax: 466 808  
E-mail: [dzemal@krobel.eu](mailto:dzemal@krobel.eu)



**LUNATRONIK**

INTEGRISANI SISTEMI  
BEZBEDNOSTI

Lunatronik doo  
Požeška 36, 11030 Beograd, Srbija  
Tel. +381-11-30-55-172;  
+381-11-35-58-446  
GSM: +381-63-499-331  
Email: office@lunatronik.co.rs  
www.KLT.rs



**PRO ALARM RJEŠENJA**  
**solutions 4 security**

[www.proalarmhr.com](http://www.proalarmhr.com)



**TEHNOZAVOD  
MARUŠIĆ**

ZAŠTITA - SIGURNOST - KOMUNIKACIJA

Automatika prolaza • Evakuacijsko ozvučenje  
• Konferencijski sustavi • Kontrola prolaza •  
Ozvučenje • Plinodjavo • Portafoni • Protuprovala  
• Sustavi za simultano prevođenje • Vatrodjavo •  
Videonadzor • Videoprezentacijski sustavi

Tehnozavod Marušić d.o.o.  
XIII Podbrežje 26, 10020 Zagreb  
Tel: +385 1 6599 600  
Fax: +385 1 6539 666  
E-mail: info@tehnozavod.hr  
www.tehnozavod.hr



**HULK-HUDINY LOCK**

ZAŠTITA ZA VOZILA  
BLOKADA VOLANA  
ALARMI  
BLINDIRANA VRATA  
SIGURNOSNE BRAVE  
CILINDRI

Milana Preloga 10, 71000 Sarajevo  
Tel: +387 33 616 975  
Mob: +387 61 147 262  
E-mail: info@hudiny.ba  
www.hudiny.ba



**MASTER BC**  
DISTRIBUTER

P A R D O X 

MASTER BC, Braće Podgornika 63 Banja Luka  
Tel/Fax: +387 (0)51 306 301, 345 130  
[www.masterbc.com](http://www.masterbc.com); [masterbc@teol.net](mailto:masterbc@teol.net)



**PROTEKTA** Integralna zaštita

Tehnička zaštita osoba i imovine Protekta d.o.o.,  
I. Šibla 9 - 10000 Zagreb, HR  
Tel: +385 1 66 36 444;  
Fax: +385 1 66 36 999  
e-mail: [info@protekt.hr](mailto:info@protekt.hr)  
[www.protekt.hr](http://www.protekt.hr)

KONTROLA PRISTUPA • ZAŠTITA OD  
RASBOJNIŠTVA • OPREMA ZA PRIJENOS I TRANS-  
PORT NOVCA • SEFOVSKO TREZORSKA OPREMA  
• VATROTOPORNI ORMARI I ARHIVE • OPREMA  
ZA SKENIRANJE I DIGITALNO POKRUVANJU  
DOKUMENATA • ZAŠTITA OD TERORIZMA



**UNV**  
World-leading IP Video  
Surveillance Manufacturer



[www.uniview.com](http://www.uniview.com)  
Sales : [fengjunqing@uniview.com](mailto:fengjunqing@uniview.com)  
Technical support: [chenxin@uniview.com](mailto:chenxin@uniview.com)



**BIROSAFE d.o.o.**  
Ul. Gocé Delčeva 121, Strumica, Makedonija  
Telefon: +389 34 330 290  
E-mail: [info@birosafe.com](mailto:info@birosafe.com); [sales@birosafe.com](mailto:sales@birosafe.com)  
Web: [www.birosafe.com](http://www.birosafe.com)



**Middle point**  
ELECTRONICS d.o.o.

AGENCIJA ZA TEHNIČKU I FIZIČKU ZAŠTITU  
71 000 SARAJEVO - ČEZMALA BIJEĆINA 35 - +387 33 697 155 / 697 157

VIDEOADZOR  
PROTIPROVALA  
VATRODOJAVA  
KONTROLA PRISTUPA  
KOMUNIKACIJSKI SISTEMI  
SPECIJALNI SISTEMI ZAŠTITE  
DUGOROČNO OSIGURAN SERVIS  
ZA SVE INSTALIRANE SISTEME



[www.mpoint.ba](http://www.mpoint.ba) [info@mpoint.ba](mailto:info@mpoint.ba)



**SALTO**  
inspired access

ELECTRONIC  
LOCKING SOLUTIONS  
FOR HOSPITALITY

Tel.: +34 943 344 550  
Email: [hospitality@saltosystems.com](mailto:hospitality@saltosystems.com)  
[www.saltohospitality.com](http://www.saltohospitality.com)





**VANDERBILT**  
**comnet**  
Communication Networks



ACCESS CONTROL    INTRUSION DETECTION    TRANSMISSION SOLUTIONS

ComNet, Suite 4, 2 Turnberry Park Road  
Gildersome, Leeds, LS27 7LE, UK  
Tel: +44 (0)113 307 6400  
Fax: +44 (0)113 253 7462  
E: [info-europe@comnet.net](mailto:info-europe@comnet.net)  
W: [www.comnet.net](http://www.comnet.net)



**PROTIVPOŽARNA  
ZAŠTITA I ZAŠTITA  
NA RADU**  
FIRE PROTECTION AND  
PROTECTION AT WORK



**Stay Untouched.**  
[www.cactusconcept.com](http://www.cactusconcept.com)

BeyondHumanVision **MOBOTIX**



**SPICA**

- » Kontrola pristupa
- » Cloud tehnologija
- » HID čitači i Špica kontroleri
- » Kontrola pristupa bez čitača
- » Bežične Aperio brave

Špica international d.o.o.,  
Pot k sejmisuču 33, 1000 Ljubljana,  
Tel: +386 01 568 08 00  
E-mail: [info@spica.si](mailto:info@spica.si)  
Web: [www.spica.si](http://www.spica.si)



**VIVOTEK**



See More in Smarter Ways  
[alarmautomatika.com](http://alarmautomatika.com)





**ARCUS d.o.o.**  
TEHNIČKA ZAŠTITA OBJEKATA

Dojava požara  
Detekcija gasova  
Sistemi automatskog gašenja  
Ostali sistemi tehničke zaštite

Arcus d.o.o. Sarajevo  
Bulevar Meše Selimovića 81A  
71000 Sarajevo, Bosna i Hercegovina  
tel: +387 33 777 757; fax: 777 767  
e-mail: [arcus@bih.net.ba](mailto:arcus@bih.net.ba)  
[www.arcus.ba](http://www.arcus.ba)



**OPTEX**

A global player  
in sensing technologies

- Indoor intrusion sensors
- Outdoor beam sensors
- Outdoor intrusion sensors
- Vehicle detector for gate and parking systems
- People counting

[www.optex-europe.com](http://www.optex-europe.com)



**SPSC GROUP**

Adresa: Vogošća, Braće Halač 16,  
71200, BIH  
Telefon: +387 33 869 873  
Mobilni: +387 66 223 169  
Email: [info@spscgroup.com](mailto:info@spscgroup.com)

Pametni & sigurnosni sistemi  
[www.spscgroup.com](http://www.spscgroup.com)



**MEHANIČKA ZAŠTITA,  
SPECIJALNA OPREMA  
I SREDSTVA**  
MECHANICAL  
PROTECTION AND  
SPECIAL EQUIPMENT





**PROVING D.O.O. SARAJEVO**

Preduzeće za protivpožarni inžinjering, marketing, istraživanje i razvoj

Ul. Milana Preloga bb  
71000 Sarajevo, BiH  
Tel/Fax: +387 33 610 264;  
663 100; 664 100  
E-mail: [proving@bih.net.ba](mailto:proving@bih.net.ba)  
[www.proving.ba](http://www.proving.ba)

# PREGLED AKTUELNIH DOGAĐAJA I SAJMOVA SIGURNOSTI MART/OŽUJAK - JUNI/LIPANJ 2021.

## ISAF Fuari

Istanbul, Turska. 4–7. mart

[www.isaffuari.com](http://www.isaffuari.com)



## Secutech Taiwan

Taipei, Tajvan. 21 – 23. april

<https://secutech.tw.messefrankfurt.com/taipei/en.html>



## IFSEC International

London, Velika Britanija. 18–20. maj

[www.ifsec.co.uk](http://www.ifsec.co.uk)



## Technobank

Beograd, Srbije. 14–15. april

[www.technobank.rs](http://www.technobank.rs)



## Security Summit Virtual Event

Sarajevo, Bosna i Hercegovina. 4–6. maj

<https://vsecuritysummit.com>



## Integrated Systems Europe

Barcelona, Španija. 1–4. juni.

[www.iseurope.org](http://www.iseurope.org)





Magazine



asadria.com

a&s Adria Newsletter



Social Networks



## PRETPLATA U 2021. GODINI

- Mjesečna publikacija
- Jadranska regija (Bosna i Hercegovina, Hrvatska, Kosovo, Crna Gora, Sjeverna Makedonija, Srbija i Slovenija.)
- Stručna publikacija za kompletan sigurnosni rješenja
- Godišnja pretplata: Printano izdanje: **60 EUR**   Digitalno izdanje: **40 EUR**

## NOVOGODIŠNJI PROMO PAKET

Osnovni paket promocije Vaše kompanije u magazinu a&s Adria.



Paket promocije uključuje:

- Oglas u rubrici Tržište i kontakti (42x55mm),
- Preplatu\* na dva primjerka sa dostavom na Vašu adresu,
- Preplatu na jedan primjerak sa dostavom na adresu po vašem izboru,
- Vijest o vašoj kompaniji ili proizvodu (online i print),
- Promo tekst o proizvodima ili uslugama vaše kompanije (online i print),
- Registraciju na b2b mrežu sa mogućnošću 20 video konferencijskih poziva.

\* cijena godišnje preplate iznosi 60€ s uključenim troškovima poštarine;

\*\* vrijednost usluge prema cjenovniku: 1.200€.

# Indeks oglašivača Index of Advertisers

| STR.                      | OGLAŠIVAČ                    | ZEMLJA              | E-MAIL                         | WEB STRANICA   |
|---------------------------|------------------------------|---------------------|--------------------------------|--|
| <b>PROIZVODI I USLUGE</b> |                              |                     |                                |  |
| 4, 5,                     | ALARM AUTOMATIKA             | HRVATSKA            | sarajevo@alarmautomatika.com   | <a href="http://www.alarmautomatika.com">www.alarmautomatika.com</a>         |
| 63                        | AGENCIJA KAMIR               | BOSNA I HERCEGOVINA | afp@afp.ba                     | <a href="http://www.kamir.net">www.kamir.net</a>                             |
| 3                         | DAHUA TECHNOLOGY             | KINA                | overseas@dahuatech.com         | <a href="http://www.dahuatech.com">www.dahuatech.com</a>                     |
| 2                         | HID GLOBAL                   | SAD                 | customerservice@hidglobal.com  | <a href="http://www.hidglobal.com">www.hidglobal.com</a>                     |
| 64                        | HIKVISION DIGITAL TECHNOLOGY | KINA                | overseasbusiness@hikvision.com | <a href="http://www.hikvision.com">www.hikvision.com</a>                     |
| 9                         | INGRAM MICRO                 | HRVATSKA            | marko.peica@ingrammicro.com    | <a href="https://hr.ingrammicro.eu">https://hr.ingrammicro.eu</a>            |
| 15                        | KROBEL                       | HRVATSKA            | kobel@kobel.hr                 | <a href="http://www.kobel.hr">www.kobel.hr</a>                               |
| 17                        | MIDDLE POINT                 | BOSNA I HERCEGOVINA | info@mpoint.ba                 | <a href="http://www.mpoint.ba">www.mpoint.ba</a>                             |
| 13                        | PROTEKTA                     | HRVATSKA            | info@protekta.hr               | <a href="http://www.protekta.hr">www.protekta.hr</a>                         |
| 7                         | SPSC GROUP                   | BOSNA I HERCEGOVINA | info@spscgroup.com             | <a href="http://www.spscgroup.com">www.spscgroup.com</a>                     |
| <b>OSTALO</b>             |                              |                     |                                |  |
| 11                        | SECURITY SUMMIT              | BOSNA I HERCEGOVINA | summit@asadria.com             | <a href="http://vsecuritysummit.com">http://vsecuritysummit.com</a>          |
| 57                        | ADRIA SECURITY SUMMIT        | BOSNA I HERCEGOVINA | summit@asadria.com             | <a href="http://www.adriasecuritysummit.com">www.adriasecuritysummit.com</a> |
| 55                        | PROVING                      | BOSNA I HERCEGOVINA | proving@bih.net.ba             | <a href="http://www.proving.ba">www.proving.ba</a>                           |

## Teme magazina Magazine Topics

### Fizička zaštita

### Tehnička zaštita

- Videonadzor
- Kontrola pristupa
- Protivprovala
- Zaštita artikala od krađe
- IP i mrežna rješenja
- Perimetarska zaštita
- Vatrodojava
- Plinodojava

### Mehanička zaštita

### Transport novca i dragocjenosti

### Informacijska zaštita

### Digitalna forenzika

### Softverska rješenja

### Pametni domovi

### Internet stvari

### Menadžment sigurnosti

### Istražne radnje

### Upravljanje objektima

### Istraživanja tržišta

### Zakonodavstvo i standardi

### Private security

### Technical protection

- Video surveillance
- Access control
- Intrusion detection
- Item theft protection
- IP and network solutions
- Perimeter protection
- Fire detection
- Gas detection

### Mechanical protection

### Cash/valuables-in-transit

### Cyber security

### Digital forensics

### Software solutions

### Smart home

### Internet of things

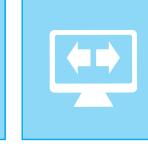
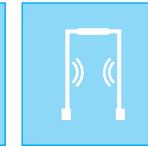
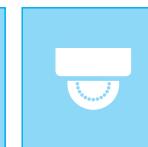
### Security management

### Investigations

### Building management

### Market research

### Legislation and standards





# New ColorVu Cameras Enhanced by

## AcuSense technology



**ColorVu**  
Cameras

See in color and focus on what matters.  
Even in darkness.