

Kako prijeći s
regulative na stvarnu
otpornost kritične
infrastrukture.

Štitimo ono što je važno

Nova pravila sigurnosti kritične infrastrukture



UVOD	4
BEZ GRANICA I ISPREPLETENE: NOVI HORIZONT SVE SLOŽENIJH PRIJETNJI	6
Studija slučaja: Tjelesna zaštita na lokaciji i tehnologija termalnih kamera za proizvođača električne energije	7
IZGRADNJA OTPORNOG SIGURNOSNOG PROGRAMA: OD RAZUMIJEVANJA RIZIKA DO MJERLJIVIH REZULTATA U 5 KORAKA	8
INTEGRIRANA FIZIČKA I DIGITALNA ZAŠTITA ZA OTPORNU KRITIČNU INFRASTRUKTURU	10
Studija slučaja: Tjelesna zaštita i usluge na daljinu pomažu nordijskom energetsom operateru u odgovoru na rizik od prelijetanja dronova	11
GLAVNI SEKTORI NA KOJE UTJEČE DIREKTIVA O OTPORNOSTI KRITIČNIH SUBJEKATA	12
Studija slučaja: Obavještajni podaci o rizicima usmjeravaju poslovanje organizacije iz prometnog sektora	12
USKLAĐENOST I KONTROLA: IMPERATIV NA RAZINI UPRAVE	14
Studija slučaja: Mobilno video sigurnosno rješenje štiti gradilište kritične infrastrukture	14
Studija slučaja: Nadzor u stvarnom vremenu i obavještajni podaci osnažuju globalnu finansijsku instituciju	17
SIGURNOSNI PRIORITETI ZA POSLOVNE LIDERE: OD USKLAĐENOSTI DO KONTINUITETA I OPORAVKA	18

Sadržaj

Uvod

Današnja kritična infrastruktura počiva na međuovisnosti. Energetika, vodoopskrba, promet, bankarstvo, digitalne platforme, javna uprava i druge usluge danas su toliko usko povezani da poremećaj u jednom području može brzo izazvati lančane posljedice u mnogim drugima. Ta povezanost donosi učinkovitost, ali istodobno povećava rizik. Lokalni čin vandalizma na nezaštićenom čvoru može pokrenuti posljedice na regionalnoj razini. Podmetanje požara na berlinskoj elektroenergetskoj mreži u siječnju 2026. dobar je primjer: jedan incident s tisućama pogođenih i prekidom više usluga.

U kontekstu pojačanih geopolitičkih napetosti, počinitelji prijetnji postali su raznolikiji i profesionalniji. Hibridni napadi koji spajaju digitalno i fizičko, od sabotaze na lokaciji do kibernetičkih upada i prelijetanja dronova, sve su češće osmišljeni tako da nadvladaju sustave detekcije i odgovora..

Organizacije kritične infrastrukture ulaze i u novo sigurnosno poglavlje s Direktivom Europske unije o otpornosti kritičnih subjekata (CER), koja obvezuje države članice da do srpnja 2026. utvrde kritične subjekte i propisuje strože sigurnosne zahtjeve. Prema analizama, do 2027. u Europi će biti više od **15.000¹** utvrđenih kritičnih subjekata, u odnosu na samo njih **100** prema prijašnjoj direktivi.

Kako regulatorni zahtjevi rastu, a prijetnje se spajaju kroz fizičku i digitalnu domenu, poslovni lideri moraju usvojiti integriraniji pristup sigurnosti vođen obavještajnim podacima. Ta promjena zahtijeva odgovornost na najvišoj organizacijskoj razini. Kritična infrastruktura okosnica je društvene otpornosti i gospodarske stabilnosti; njezina zaštita stoga nije samo operativno pitanje, nego zajednička odgovornost s posljedicama koje nadilaze pojedinačne organizacije.

Suradnici

Mike Evans
Direktor, Risk Intelligence Center,
Securitas

Claus Fibiger
Predsjednik za
Dansku, Securitas

Gaspard Fierens
Voditelj sigurnosnog
savjetovanja, Securitas
Europa

Benedikt Meyer
Odnosi s javnošću,
Securitas Njemačka

Morten Krohn Sommer Mikkelsen
Potpredsjednik za razvoj rješenja
Securitas Europa

Marc Moris
Voditelj grupne prevencije i zaštite,
Proximus

¹ [Implementing the European Directive on Critical Entity Resilience \(CER Directive\): Status, Challenges, and International Context - EU-CIP](#)



Bez granica i isprepletene – novi horizont sve složenijih prijetnji

Globalne geopolitičke konfrontacije, uključujući prvi veći europski sukob u više od 70 godina, podigle su razinu prijetnji za pružatelje **kritične infrastrukture**. NATO² danas sabotira kritične infrastrukture svrstava među najveće sigurnosne prijetnje. Hibridni ili “isprepleteni” pokušaji ometanja kritične infrastrukture dio su trenda koji se brzo razvija.

Hibridni napadi kreću se preko granica jednako brzo kao protok podataka i medija. Digitalizacija je proširila površinu napada, no i fizički rizici postali su sofisticiraniji, od proboja perimetra do bespilotnih letjelica koje ciljaju trafostanice i udaljenu imovinu. Mapiranje međuovisnosti, diversifikacija opskrbnih lanaca i izgradnja redundancije ključni su, ali funkcioniraju tek u sprezi s integriranim upravljanjem sigurnošću i rizicima koje može detektirati, provjeriti i reagirati u stvarnom vremenu.

Mike Evans, Director, Risk Intelligence Center, Securitas, kaže: “Danas je svaka vrsta počinitelja prijetnji motivirana

da cilja kritičnu infrastrukturu. Čak i najjednostavniji čini sabotaže i krađe mogu izazvati teške prekide. Neke su prijetnje sada uistinu bez granica zbog međuovisnosti moderne infrastrukture. Prijetnje kritičnoj infrastrukturi ne poznaju geografiju. Brzina kojom se problemi šire sama je po sebi čimbenik rizika. Naš savjet poslovnim liderima jest da nadzor regionalnih rizika u stvarnom vremenu postave kao najviši prioritet.”

“Prijetnje kritičnoj infrastrukturi ne poznaju geografiju.”

Mike Evans
Director, Risk Intelligence Center
Securitas

Marc Moris, Group Prevention & Protection Lead u tvrtki Proximus, koja se bavi informacijsko-komunikacijskim tehnologijama i digitalnim uslugama, upozorava na potrebu da organizacije budu proaktivne i agilne. Kaže: “Pripreme za prevenciju i zaštitu od rizika koji se razvijaju

su slučajevima još uvijek nedostatne. Tvrtke kritične infrastrukture moraju provoditi sveobuhvatne procjene rizika kako bi osigurale primjerene preventivne i zaštitne mjere te dinamičnije procjenjivale rizike.”

Mapiranje međuovisnosti i diversifikacija opskrbnih lanaca prioriteti su za organizacije koje nastoje ublažiti poremećaje i izbjeći zastoje, kao i ugradnja redundancije u kritične sustave. No to je potrebno povezati s integriranim upravljanjem sigurnošću i rizicima kako bi se odgovorilo na višeslojne prijetnje.

Morten Krohn Sommer Mikkelsen, VP Solutions Offering, Securitas Europe, ističe važnost procjene opskrbnog lanca i kaže: “Kritična infrastruktura živi unutar dugih i vrlo isprepletenih lanaca vrijednosti. Svaki dobavljač, podizvođač i pružatelj usluga postaje dio jednadžbe otpornosti. Ako je jedna karika u tom lancu krhka, posljedice ne ostaju ograničene, nego se šire. Zato odabir dobavljača više nije samo komercijalna ili nabavna odluka. To je odluka o otpornosti.”

Evans kaže: “Situacijska svjesnost važnija je nego ikad za kritičnu infrastrukturu, ali upravo će sposobnost da se u stvarnom vremenu smisleno razlikovati organizacije i omogućiti im da budu korak ispred.”

Situacijska svjesnost stoga je odlučujuća sposobnost. Organizacije koje objedinjuju fizičke podatke, poput videonadzora, evidencija pristupa ili podataka o ophodnjama, s kibernetičkim signalima i vanjskim obavještajnim podacima o prijetnjama, mogu postići bržu provjeru i eskalaciju te tako smanjiti operativne i društvene posljedice.

STUDIJA SLUČAJA

Tjelesna zaštita na lokaciji i tehnologija termalnih kamera za proizvođača električne energije

Vodeći privatni proizvođač energije, specijaliziran za izgradnju termoelektrana, hidroelektrana, solarnih i vjetroelektrana, trebao je nadogradnju sigurnosti kako bi poboljšao zaštitu perimetra, obnovio elektroničku zaštitu i osigurao mogućnost širenja na više lokacija.

Uvedeno je integrirano rješenje koje objedinjuje tjelesnu zaštitu na lokaciji, udaljeni videonadzor i analitiku, termalne kamere, zvučnike i bodycam kamere.

U ovo prilagođeno rješenje uključene su i usluge zaštite od požara i sigurnosti, čime je povećana robusnost i učinkovitost zaštite.

² <https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence?>

Izgradnja otpornog sigurnosnog programa

Većina operacija i imovine unutar okruženja kritične nacionalne infrastrukture (CNI) izrazito je kritična, za razliku od drugih operatera.



1. RAZUMIJEVANJE PREPOZNATI ŠTO JE VAŽNO

Mapirajte kritičnu imovinu poput ljudi, lokacija, opreme i procesa. Procijenite moguće posljedice kako biste razumjeli kako bi incidenti mogli utjecati na sigurnost života, kontinuitet, financijske gubitke ili ugled. Stvorite zajedničko razumijevanje prioriteta i prihvatljive razine rizika.



2. PROCJENA UTVRDITI PRIJETNJE I RANJIVOSTI

Koristeći obavještajne podatke iz otvorenih izvora, vlastite podatke i lokalne uvide, prepoznajte relevantne prijetnje i utvrdite kako se njihova vjerojatnost razlikuje među regijama. Procijenite postojeće mjere kontrole u pogledu ljudi, procesa i tehnologije.



3. UBLAŽITI PRIMIENITI PRAVE MJERE

Kombinirajte brze rezultate s dugoročnim poboljšanjima u tri područja: ljudi, procesi i tehnologija



4. UPRAVLJATI UGRADITI POBOLJŠANJA

Upravljanje treba uključivati preglede i praćenje ključnih pokazatelja uspješnosti (KPI) poput vrsta incidenata, vremena odgovora, dostupnosti sustava i usklađenosti s obukom.



5. RAZVIJATI SE PRATITI PROMJENE

Prijetnje i ranjivosti mijenjaju se kako organizacije rastu, a okruženja se razvijaju. Pratite nove trendove, ažurirajte procedure, ugradite naučene lekcije i revidirajte planove upravljanja rizicima dvaput godišnje.

Integrirana fizička i digitalna zaštita za otpornu kritičnu infrastrukturu

Iako su digitalizacija i povezanost s jedne strane povećale površine napada, i fizičke su prijetnje postale sofisticiranije, pa organizacije traže načine da ih ublaže. Kritični subjekti u ključnim sektorima morat će provoditi formalne procjene rizika, izrađivati planove otpornosti i provoditi tehničke mjere za ublažavanje poremećaja. CER naglašava važnost fizičke sigurnosti, od kontrole pristupa i zaštite lokacija do redundancija i postupaka u izvanrednim situacijama.

Benedikt Meyer, Public Affairs, Securitas Germany, kaže: “Ono što danas vidimo usklađen je i integriran zaokret prema cjelovitim arhitekturama fizičke i kibernetičke sigurnosti

te činjenica da ulaganje u stvari poput robusne zaštite perimetra, videonadzora i analize rizika postaje očekivani minimalni standard koji podliježe reviziji.”

Sigurnosna tehnologija također se razvija kako bi ponudila inovativna rješenja za zaštitu organizacija. Claus Fibiger, Country President, Securitas Denmark, kaže: “Sve je veći interes za tehnologiju koja ublažava rizike za organizacije kritične infrastrukture. U Danskoj i diljem Europe vidimo veći interes za mogućnosti detekcije dronova, a istodobno raste i interes za robotske sigurnosne ophodnje za udaljenu imovinu.”

Prijetnje s kojima se danas suočava kritična infrastruktura ne dolaze u urednim, odvojenim kategorijama. Mikkelsen kaže:

“Fizički rizici i digitalne prijetnje sve su isprepleteniji, a sigurnost popušta ondje gdje se njima još upravlja odvojeno, u silosima. Prava spremnost proizlazi iz integracije, iz povezivanja fizičke zaštite, tehnologije i obavještajnih podataka, uz sposobnost djelovanja u stvarnom vremenu. Ljudski element u tom lancu ostaje ključan za pokretanje odgovora na incidente.”

STUDIJA SLUČAJA

Tjelesna zaštita i usluge na daljinu pomažu nordijskom energetsom operateru u odgovoru na rizik od prelijetanja dronova

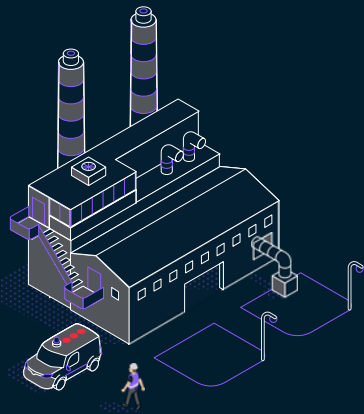
Veliki operater za prijenos energije u nordijskim zemljama bio je izložen nadlijetanju dronova.

Procjena prijetnje pokazala je da bi sigurnost na tim lokacijama povećala zaštita koja kombinira statičnu tjelesnu zaštitu i mobilne intervencijske timove za rješavanje eskalacija, uz obavještajne podatke i koordinaciju koje omogućuje Securitas Operations Center (SOC).

Ovo integrirano rješenje dovelo je do znatno brže provjere prijetnji za ovog važnog operatera i istodobno poboljšalo usklađenost organizacije s budućim zahtjevima direktiva CER i NIS2 (Network and Information Security).

Glavni sektori na koje utječe Direktiva o otpornosti kritičnih subjekata

Direktiva o otpornosti kritičnih subjekata (CER) okvir je na razini cijele EU koji obuhvaća 11 sektora: energetiku, promet, bankarstvo, financijska tržišta, zdravstvo, opskrbu pitkom vodom, otpadne vode, digitalnu infrastrukturu, javnu upravu, svemir i hranu.



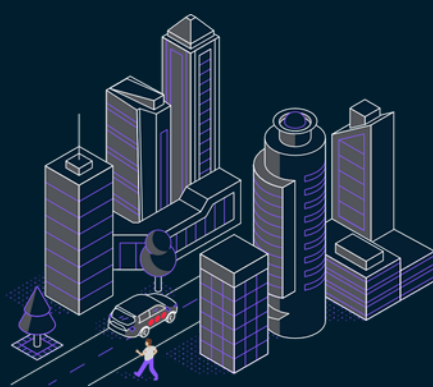
ENERGETSKI SEKTOR

Proizvodnja električne energije i skladištenje energije.



VODOOPSKRBNI SEKTOR

Opskrba pitkom vodom, distribucija pitke vode te usluge prikupljanja, obrade i odvodnje otpadnih voda.



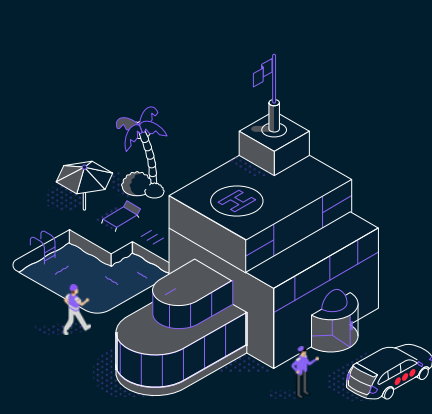
FINANCIJSKI I BANKOVNI SEKTOR

Usluge poput vođenja mjesta trgovanja i sustava poravnanja, uključujući bankarstvo s ključnim uslugama kao što su primanje depozita i kreditiranje.



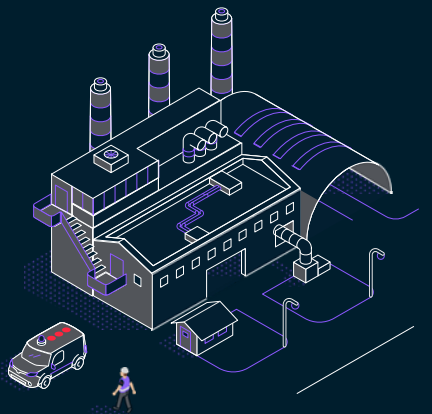
SEKTOR DIGITALNE INFRASTRUKTURE

Usluge poput pružanja i vođenja internetskih točaka razmjene (IXP), sustava naziva domena (DNS), vršnih domena, cloud računalstva i podatkovnih centara.



ZDRAVSTVENI SEKTOR

Distribucija, proizvodnja, pružanje zdravstvene skrbi i medicinskih usluga.



SEKTOR PROIZVODNJE, PRERADE I DISTRIBUCIJE HRANE

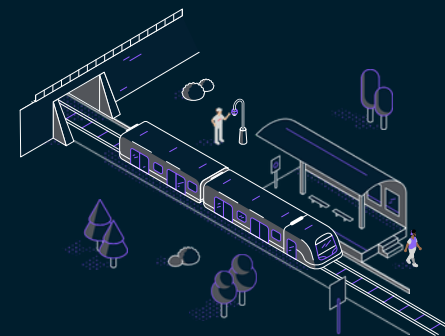
Industrijska proizvodnja i prerada hrane velikih razmjera, usluge opskrbnog lanca hrane i usluge veleprodajne distribucije hrane.

STUDIJA SLUČAJA

Obavještajni podaci o rizicima usmjeravaju poslovanje organizacije iz prometnog sektora

Poduzeće iz prometnog sektora upravlja s nekoliko lokacija i za oblikovanje sigurnosne strategije oslanja se na pouzdane procjene situacije. Operater redovito prima obavještajne podatke o rizicima vezane uz relevantna događanja u blizini svojih lokacija, poput prosvjeda, poremećaja ili drugih mogućih rizika.

Ti su obavještajni podaci omogućili rano prepoznavanje mogućih prijetnji i prilagodbu sigurnosnih mjera, čime su poboljšali operativnu spremnost i ojačali otpornost.



SEKTOR PROMETA

Usluge poput upravljanja i održavanja zračnih luka ili željezničke infrastrukture.



SEKTOR JAVNE UPRAVE

Države članice EU dužne su provesti nacionalnu procjenu rizika kako bi do srpnja 2026. utvrdile sve kritične subjekte, nakon čega organizacije mogu imati svega 10 mjeseci da dokažu usklađenost sa zahtjevima otpornosti.

Osnovni zahtjevi uključuju provođenje procjena rizika, provedbu tehničkih i organizacijskih mjera otpornosti te prijavu incidenata. Direktiva nastoji osigurati da operateri mogu spriječiti niz poremećaja, izdržati ih, odgovoriti na njih i oporaviti se od njih.

Usklađenost i kontrola - imperativ na razini uprave

Direktiva CER i drugi okviri imaju značajnu ulogu u razvoju sigurnosti kritične infrastrukture. Oni otpornost pretvaraju iz dobrovoljne “najbolje prakse” u zakonski propisanu obvezu vodstva i upravljanja. U svjetlu te dinamike, otpornost je iz tehničke mjere prerasla u strateški prioritet na razini uprave.

Fibiger kaže: “Važno je da se CER promatra šire od puke usklađenosti. Direktive nisu samo regulatorni

teret, one su strateški pokretači koji oblikuju odluke i ulaganja na razini uprave. To je pitanje vodstva, svijesti o rizicima i dugoročne konkurentnosti. Organizacije koje razumiju svoju ulogu unutar lanaca vrijednosti u kojima djeluju mogu otpornost iskoristiti kao poziciju snage, umjesto da je promatraju tek kao regulatorni zahtjev. Kada je otpornost ugrađena u prakse upravljanja i operativno razmišljanje, ona postaje strateška vrijednost.”

Iako je visoka razina otpornosti češća u sektorima poput energetike, robusna sigurnost i provedba sigurnosnih mjera mogu biti neujednačeni među sektorima, a spremnost na incidente nedostatna. Diljem Europe regulatorno okruženje postaje sve strože stupanjem na snagu nacionalnih provedbi Direktive CER, čega je izvrstan primjer njemački KRITIS³ krovni zakon (KRITIS-Dachgesetz).

STUDIJA SLUČAJA

Mobilno video sigurnosno rješenje štiti gradilište kritične infrastrukture

Tijekom planiranja velikog projekta modernizacije željezničke infrastrukture otkrivena su dva velika plinovoda koja su ometala planiranu izgradnju. Tu neočekivanu prepreku trebalo je hitno riješiti kako bi projekt ostao u planiranim rokovima. Postojeće plinovode trebala je premjestiti nacionalna plinska tvrtka, a bila je potrebna i zaštita gradilišta tijekom cijelog postupka.

Uvedeno je mobilno video rješenje s ugrađenom video analitikom te je uspostavljena veza na daljinu s lokalnim Securitas Operations Centerom. To je omogućilo neprekidan nadzor, uz SOC operatore dostupne 24/7 za odgovor na alarme u stvarnom vremenu.

U slučaju incidenta, operateri bi koordinirali odgovarajuće snage za intervenciju i mogli su davati obavijesti na lokaciji putem zvučnika povezanih sa SOC-om.

³ <https://www.bundesregierung.de/breg-en/news/cabinet-kritis-umbrella-law-2404992>



“Direktive nisu samo regulatorni teret, one su strateški pokretači koji oblikuju odluke i ulaganja na razini uprave.”

Claus Fibiger
Country President
Securitas Denmark

“Ako usklađenosti pristupate kao pukom ispunjavanju kvačica na popisu, to vas ne čini sigurnima.”

Mike Evans
Director, Risk Intelligence Center
Securitas

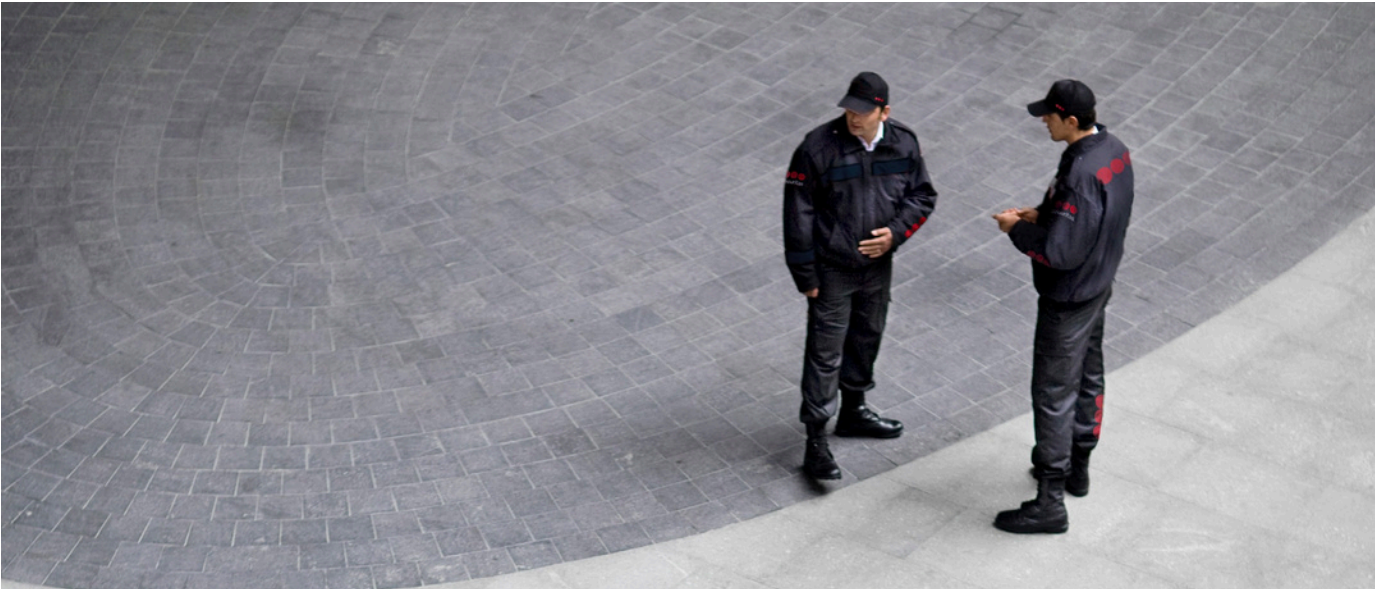
Okvir je prije svega namijenjen prepoznavanju kritičnih subjekata, pri čemu se organizacije koje opslužuju više od **500.000** ljudi označavaju kao KRITIS. Sudionici u toj kategoriji moraju prijaviti incidente u roku od 24 sata, a neusklađenost može dovesti do novčanih kazni do **milijun eura**.

Fizička sigurnost u središtu je usklađenosti sa zakonodavstvom poput direktive CER i KRITIS krovnog zakona. Ti okviri naglašavaju važnost primjerene zaštite perimetra, kontrole pristupa, nadzora i praćenja, tjelesne zaštite i alarmnih sustava. Meyer kaže,

“Zakonodavstvo nameće obveznu analizu rizika, obveze prijavljivanja i zahtjeve fizičke sigurnosti, ali, što je važno, vidimo i da usklađenost predstavlja velik korak prema sveobuhvatnoj, međusektorskoj zaštiti kritične infrastrukture.”

Moris kaže: “Europa je izvrsna u donošenju novog zakonodavstva, ali usklađenost ne smije postati sama sebi svrha za organizacije kritične infrastrukture. Poslovni lideri moraju imati na umu da kriminalci djeluju izvan zakonskih okvira te da rizike treba procjenjivati kontinuirano.”

Evans dodaje: “Usklađenost je nužna, a ti okviri koji se razvijaju plima su koja podiže sve brodove. Ako usklađenosti pristupate kao pukom ispunjavanju kvačica na popisu, to vas ne čini sigurnima. Kad je riječ o sigurnosti kritične infrastrukture, usklađenost treba shvatiti tek kao početak, a ne kao krajnji cilj.”



STUDIJA SLUČAJA

Nadzor u stvarnom vremenu i obavještajni podaci osnažuju globalnu finansijsku instituciju

Globalna organizacija na vrhu industrije finansijskih usluga suočavala se sa sve većim brojem incidenata, pri čemu su prijetnje pogađale zaposlenike, resurse i ključne poslovne procese.

Uočeni su nedostaci u postojećem sustavu izvješćivanja za praćenje prijetnji, što je bilo ograničavajući čimbenik i za otpornost i za buduću usklađenost.

Uspostavljena je prilagođena obavještajna usluga temeljena na praćenju uživo u stvarnom vremenu, s alarmom 24/7, ranim upozorenjima i podrškom u kriznim situacijama, što je omogućilo predviđajući pristup prijetnjama i snažan odgovor.

Uvedena su redovita obavještajna izvješća radi stalnog uvida u okruženje prijetnji. Uspostavljena je provjera radi zaštite rukovoditelja izloženih ciljanim prijetnjama. Uspostavljena je i

namjenska usluga zahtjeva za obavještajnim podacima (Request for Intelligence, RFI), putem koje su mogli angažirati stručnjake za informacije o konkretnim prijetnjama. Te prilagođene, integrirane usluge pomogle su u ublažavanju materijalne štete, prijetnji zaposlenicima i potencijalno ometajućih prosvjeda. Uz veću kontrolu i jasnoću u odlučivanju, organizacija za finansijske usluge izvijestila je o poboljšanjima u globalnom poslovanju.

Sigurnosni prioriteti za poslovne lidere - od usklađenosti do kontinuiteta i oporavka

Odgovor na spajanje fizičkih i digitalnih prijetnji glavni je prioritet za lidere u kritičnoj infrastrukturi. Sposobnosti nadzora, obavještajnog djelovanja i odgovora potrebno je objediniti u sklopu usklađenog pristupa sigurnosti. Sprječavanje svakog čina sabotaze, unutarnje prijetnje i kvara sustava postalo je nerealno, što naglašava važnost višeslojne otpornosti i djelotvornih odgovora.

Evans kaže: "U svijetu u kojem se isprepletene prijetnje osmišljavaju s namjerom da se društveni učinak maksimalno poveća, integrirana sigurnost koja obuhvaća i fizički i digitalni sloj nikada nije bila važnija."

Suradnja i usklađenost među dionicima također su važni čimbenici. Moris kaže: "Suradnja se mora protezati izvan podjele na javno i privatno te uključivati i partnerstva unutar privatnog sektora, iskorištavajući stručnost, resurse, inovacije i saveze među tvrtkama.

Usklađenost između operatera kritične infrastrukture, pružatelja usluga i javnih tijela ostaje ključna. Pružatelji sigurnosnih usluga imaju sastavnu ulogu u ublažavanju velikih incidenata i upravljanju njima."

Regulativu i okvire poput Direktive CER ne treba promatrati samo kao obveze usklađivanja, nego kao **strateške prilike za jačanje spremnosti i dugoročne konkurentnosti**.

Fibiger zaključuje: "Što su pripremljenije, tvrtke mogu učinkovitije odgovarati na sve strože zahtjeve. Najbolje pripremljene organizacije izlaze jače, vjerodostojnije u dijalogu s klijentima i pouzdanije u operativnoj isporuci."

Organizacije koje prihvate takav pristup, integrirajući sigurnost, učinkovito surađujući i koristeći regulativu kao polugu za otpornost, bit će najbolje pozicionirane u sve nestabilnijem okruženju rizika.

U Securitasu vodimo sigurnosnu industriju u budućnost. Objedinjujemo svoju stručnost u pojedinačnim uslugama poput usluga **Remote**, **Mobile** i **On-Site**, **Fire & Safety** te **Technology** u inovativna sigurnosna rješenja koja odgovaraju na različite potrebe naših klijenata. Baš kao i vaše poslovanje, naša su sigurnosna rješenja stvorena da se prilagođavaju i rastu. Uz uistinu globalnu prisutnost, ponosni smo što smo pouzdan sigurnosni partner tvrtkama diljem svijeta.

