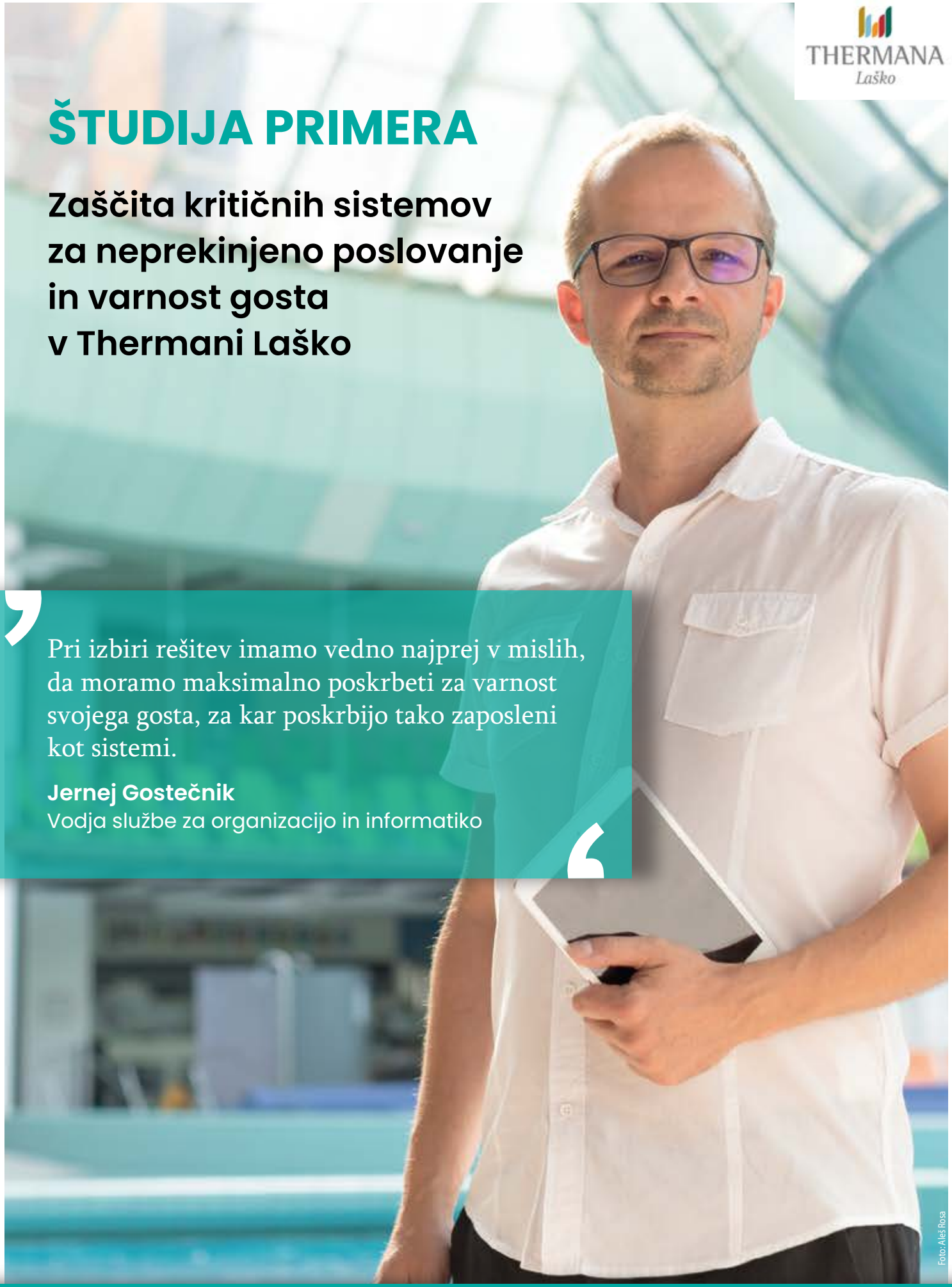
THERMANA
Laško

ŠTUDIJA PRIMERA

Zaščita kritičnih sistemov za neprekinjeno poslovanje in varnost gosta v Thermani Laško



> Pri izbiri rešitev imamo vedno najprej v mislih, da moramo maksimalno poskrbeti za varnost svojega gosta, za kar poskrbijo tako zaposleni kot sistemi.

Jernej Gostečnik
Vodja službe za organizacijo in informatiko

Foto: Aleš Rosa

SMART COM

TREND MICRO
Tehnološki partner

Thermana d. d. *je eden izmed najsodobnejših turističnih centrov v Sloveniji z več kot 160-letno tradicijo. S storitvami, ki temeljijo na vrhunskem znanju in bogatih izkušnjah priznanih medicinskih strokovnjakov ter na termalni vodi, gostom pomagajo ohranjati zdravje in omogočajo dobro počutje. Družba zajema tri ključne centre: Zdravilišče Laško, kjer se pretežno izvajajo medicinske storitve, turističen kompleks in kongresni center Thermana Park ter Dom starejših Laško.*

Skrb za varnost gostov, pacientov in oskrbovancev je na prvem mestu. Pri tem je ključno tudi delovanje in kontrola nad industrijskimi sistemi, kritičnih za poslovanje, med katerimi je najpomembnejši sistem bazenske tehnike za doziranja klora. Pri povezovanju industrijskih sistemov v poslovno okolje so se soočili z varnostnimi tveganji.

V skladu z varnostno politiko in politiko neprekinjenega poslovanja so iskali rešitev, s katero bi zagotovili varnost in nemoteno poslovanje integriranega sistema.

Uvedba dopolnjujoče se tehnološke rešitve proizvajalca Trend Micro, produktov Safe Lock in Portable Security 2, omogoča celovito zaščito navedenih sistemov pred škodljivo programsko kodo ter daje kontrolo nad tem, katere aplikacije se lahko izvajajo. S tem se zagotovi učinkovita zaščita kritičnih sistemov, brez internetne povezave ('offline').

Pri uspešni izvedbi projekta je sodelovala ekipa podjetja Smart Com.

Izziv

Kako poskrbeti za varnost industrijskih sistemov, ki krmilijo bazensko tehniko, ogrevanje itd., pri povezovanju v poslovno okolje pred tveganji zlonamerne kode, skladno s politiko neprekinjenega poslovanja.

Rešitev

Uvedba dopolnjujočih se produktov Trend Micro Safe Lock in Trend Micro Portabe Security 2 omogoča zaščito starejših, zaprtih sistemov, nepovezanih v internet, brez možnosti nameščanja protivirusne zaščite in varnostnih popravkov. Ključno je, da se s tem zagotovi kontrola pred nameščanjem nepooblaščenih aplikacij, s čimer se zagotovi varnost nadzornih sistemov.

Učinki

- Vpogled in kontrola nad izvajanjem upravljanja kritičnih industrijskih sistemov.
- Natančen popis sistema (krmilnikov) ter varnostnih in procesnih tveganj povezanih s tem.
- Popis programov, ki se jih ne spušča v sistem, kar je zelo pomembno za poslovanje in delo zunanjih izvajalcev.

Foto: arhiv Thermane Laško

V družbi Thermana d. d. dajejo velik poudarek kibernetski varnosti in obvladovanju varnostnih ter procesnih tveganj. Za to je odgovorna služba za organizacijo in informatiko, ki skrbi za poslovno in sistemsko informatiko ter organizacijo procesov. Jernej Gostečnik, vodja službe, skupaj s sodelavci skrbi za implementacijo in vzdrževanje sistemov, ki pokrivajo potrebe njihovih procesov.

Uveljavljajo varnostno politiko in politiko neprekinjenega poslovanja, v kateri so opredelili sisteme, ki so kritični in jih je potrebno na vsak način zaščititi in podvojiti, zato, da podjetje lahko posluje nemoteno. Prvi vidik varnosti je ta, da se varnostni incident prepreči oz. da do njega sploh ne pride. Drugi pa je v primeru, če se incident zgodi, mora za varnost podatkov poskrbeti redundantni sistem.

Povezovanje industrijskih sistemov v poslovno okolje prinaša nova varnostna tveganja

Celoten sistem temelji na virtualizaciji strežniških sistemov, nameščenih in upravljanih v centralnem sistemskem prostoru. Vsi trije objekti, za katere skrbi služba za organizacijo in informatiko, so povezani z optičnimi povezavami. Industrijski sistemi, ki krmilijo bazensko tehniko, ogrevanje itd. so bili do leta 2018 vedno ločeni od ostalih sistemov IT, ko so jih poenotili in postavili v virtualno okolje. Centralizacija je posledično prinesla nova varnostna tveganja, povezana z možnostjo nedovoljenih dostopov in nekontroliranega nameščanja aplikacij. Zato je bilo nujno okrepiti varnostne mehanizme.

Izziv pa ni bil povezati sisteme v tehnološke smislu temveč tudi v povezovanju med ekipama - službo za organizacijo in informatiko s službo vzdrževanja, ki je odgovorna za obvladovanje in pravilno upravljanje industrijskih sistemov, tudi v primeru nedelovanja zaradi varnostnega incidenta.

Zaprti, izolirani sistemi niso varni pred okužbo s škodljivo programsko kodo

Za zaščito industrijskih sistemov so poskrbeli z uvedbo rešitve tehnološkega ponudnika Trend Micro. Ker so v dnevni uporabi sistemi starejšega datuma, ki sicer delujejo ustrezno, kjer pa namestitev sodobne protivirusne zaščite ni mogoča, prav tako ne posodobitve za operacijski sistem, ki nadgradnjo sistemskih popravkov pogojujejo s povezavo v internet.

Z rešitvijo Trend Micro Portable Security 2 je zaščita možna, saj omogoča pregled sistemov pred škodljivo programsko kodo (antivirus, antimalware) in njihovo odpravo brez povezave v internet in je tako primerna za sisteme, kjer ni mogoče nameščati protivirusne zaščite. Na ta način obvladujejo nadgradnje (tudi nepričakovane), ki bi v primeru nekontroliranih posodobitev izpostavile delovanje kritičnih sistemov določenim tveganjem.

> Obstajala je možnost, da pride nekdo s ključkom USB in naloži novo verzijo aplikacije, posodobi krmilnik in tako ogrozi delovanje kritičnih sistemov.
>
> Ta izziv smo rešili z rešitvijo Trend Micro, ki poskrbi za zaščito starejših ('legacy') sistemov brez povezave v internet in onemogoča nekontrolirano nameščanje nepooblaščenih aplikacij.

Po drugi strani pa rešitev Trend Micro Safe Lock omogoča varovanje pred namestitvijo in zaganjanjem nepooblaščenih aplikacij, ki lahko privede do motenj v delovanju krmilnikov, kritičnih za delovanje sistemov. Rešitev med drugim omogoča tudi zaščito pred vnosom zlonamerne kode iz zunanjih diskov (mrežne mape, ključki USB).

Foto: Aleš Rosa

S tega vidika je v Thermani d. d. zelo pomembna zaščita sistema bazenske tehnike – krmilnikov za reguliranje doziranje klora, ki se uporablja za dezinfekcijo. V majhnih odmerkih je nenevaren, v prevelikih pa zdravju škodljiv.

Rešitev Trend Micro Safe Lock omogoča graditev baze dovoljenih aplikacij (izvršljive datoteke, različne sistemske knjižnice, gonilniki in druge datoteka, ki so potrebne za delovanje sistema), njihovo ročno ali avtomatsko upravljanje, aktivno spremljanje procesov in kontrolo nad zunanjimi diski.

> Pomembno je, da imamo kontrolo nad tem, kaj se dogaja na naših sistemih in da je izvajanje nedovoljenih programov onemogočeno.
>
> Ne moremo si privoščiti, da bi virus onemogočil uporabo programov, ki skrbijo za krmiljenje, kar glede na politiko neprekinjenega poslovanja lahko povzroči velike težave pri delovanju sistemov, neobratovanje, posledično pa poslovno škodo ali celo ogroža življenje oz. zdravje gosta.

Ponudnik in integrator rešitve Smart Com je za ekipo službe vzdrževanja izvedel tudi izobraževanje v obliki delavnice, kjer so se spoznali s praktično uporabo rešitve. Služba vzdrževanja je tista, ki skrbi za periodično preverjanje delovanja sistema, kontrolira stanje na sistemih in jih tudi posodablja. Zaradi 'offline' načina delovanja ter varnostne politike, se enkrat mesečno izvedejo posodobitve protokolov.

Z rešitvijo Trend Micro nad varnostna in procesna tveganja, ki lahko povzročijo motnje poslovanja in poslovno škodo

V Thermani d. d. so z uvedbo rešitve Trend Micro zmanjšali tveganja, ki so posledično nastala, ko so povezali industrijske sisteme s poslovnimi.

Z uporabo rešitve sedaj na enostaven način skrbijo za zaščito pred naprednimi kibernetskimi grožnjami sistemov. Rešitev omogoča preglede sistemov in morebitno odpravo škodljive programske kode ('malware') ter zaščito pred njenim izvajanjem in nameščanjem nedovoljenih aplikacij.

Popolna vidljivost v dogajanje v sistemu je prinesla večjo varnost in večje zaupanje v delo zunanjih izvajalcev, ko dostopajo do sistemov, katere vzdržujejo. Preverjanje njihovih sistemov in računalnika, s katerim se priklapljajo, ni več potrebno, saj rešitev Trend Micro poskrbi za to, da nepooblaščenih programov ne spušča v sistem.

Ob implementaciji rešitve sta bila narejena natančen popis in evidenca sistemov ter krmilnikov. S tem so ugotovili realno stanje, kar prinaša kontrolo nad elementi in preprečuje potencialna varnostna tveganja, povezana z nepoznavanjem razmer v omrežju.

Izkušnje

- Od namestitve rešitve Trend Micro ni bilo pritožbe o nedelovanju sistema.
- Nadzorni sistemi in upravljanje procesnega omrežja deluje brezhibno.

Glavne prednosti rešitve Trend Micro

- ✔ Enostavna uporaba in minimalna raba virov.
- ✔ Centralizirano ali samostojno upravljanje.
- ✔ Široka podpora različnim operacijskim sistemom Windows.
- ✔ Primerno za industrijske kontrolne sisteme ICS (SCADA), HMI ter namenske zaprte sisteme in terminale.

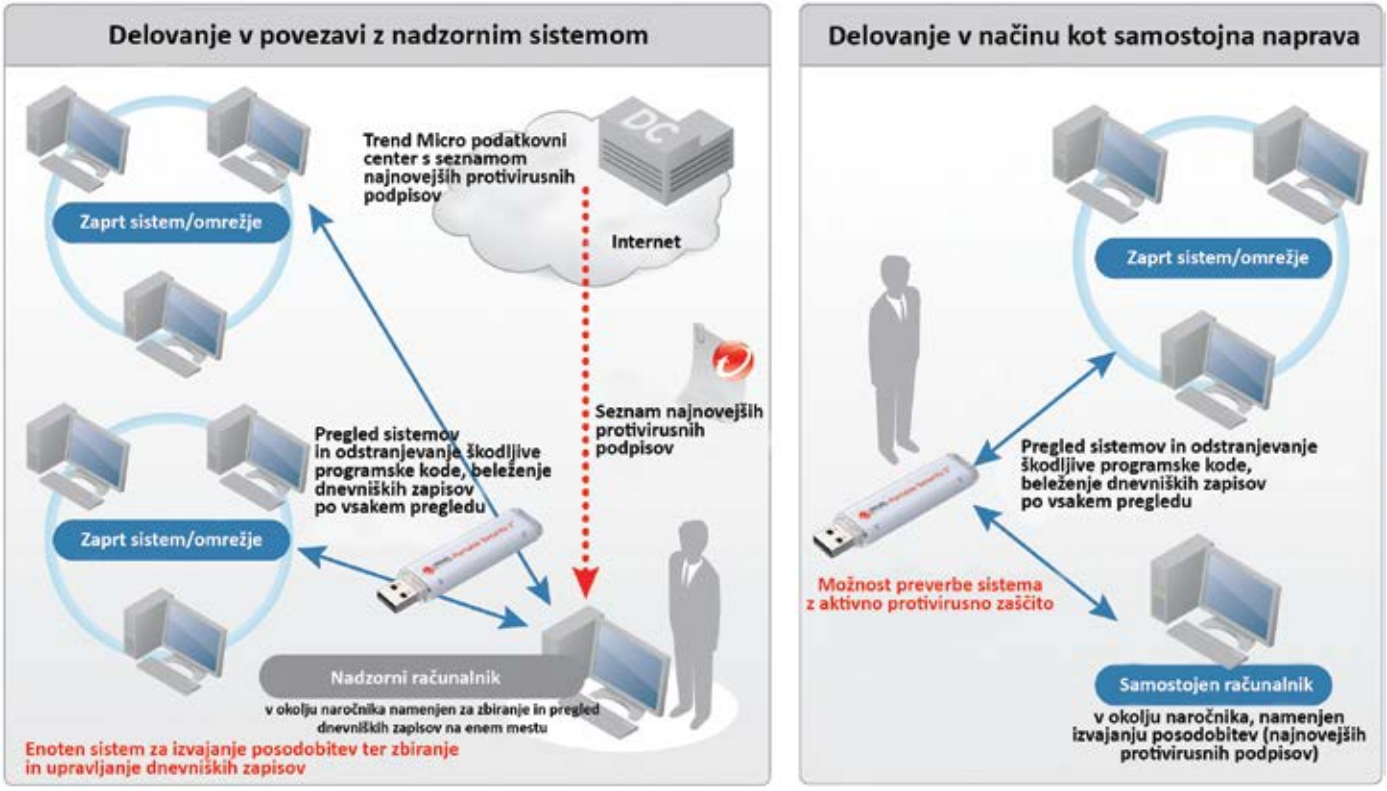
Trend Micro Portable Security 2

- ✔ Pregled sistemov in odstranjevanje škodljive programske kode.
- ✔ Tudi za sisteme, brez povezave v internet, kjer ni možno nameščati varnostnih popravkov in protivirusne zaščite.
- ✔ Brez nameščanja dodatne programske opreme, programska zaščita se zaganja neposredno s ključa USB.

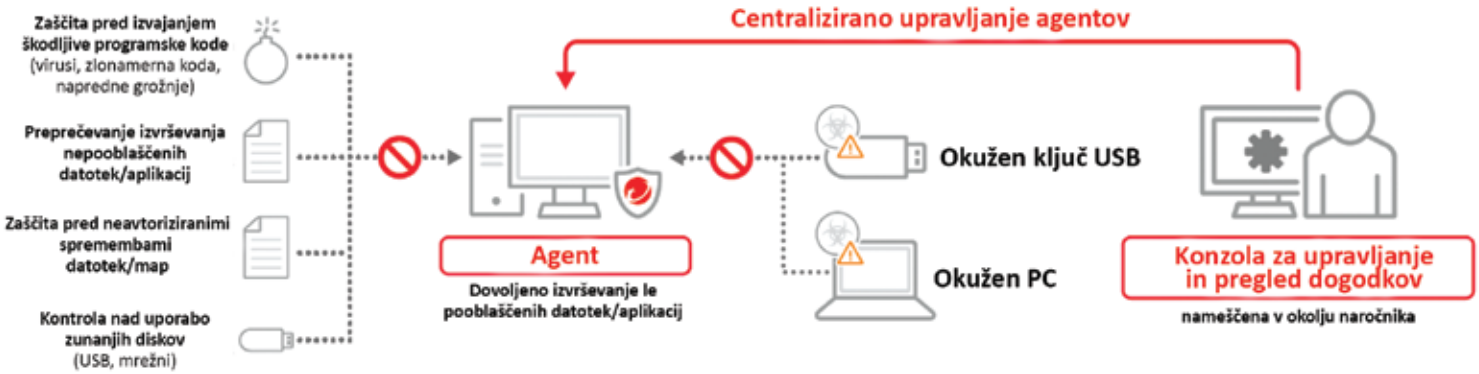
Trend Micro Safe Lock

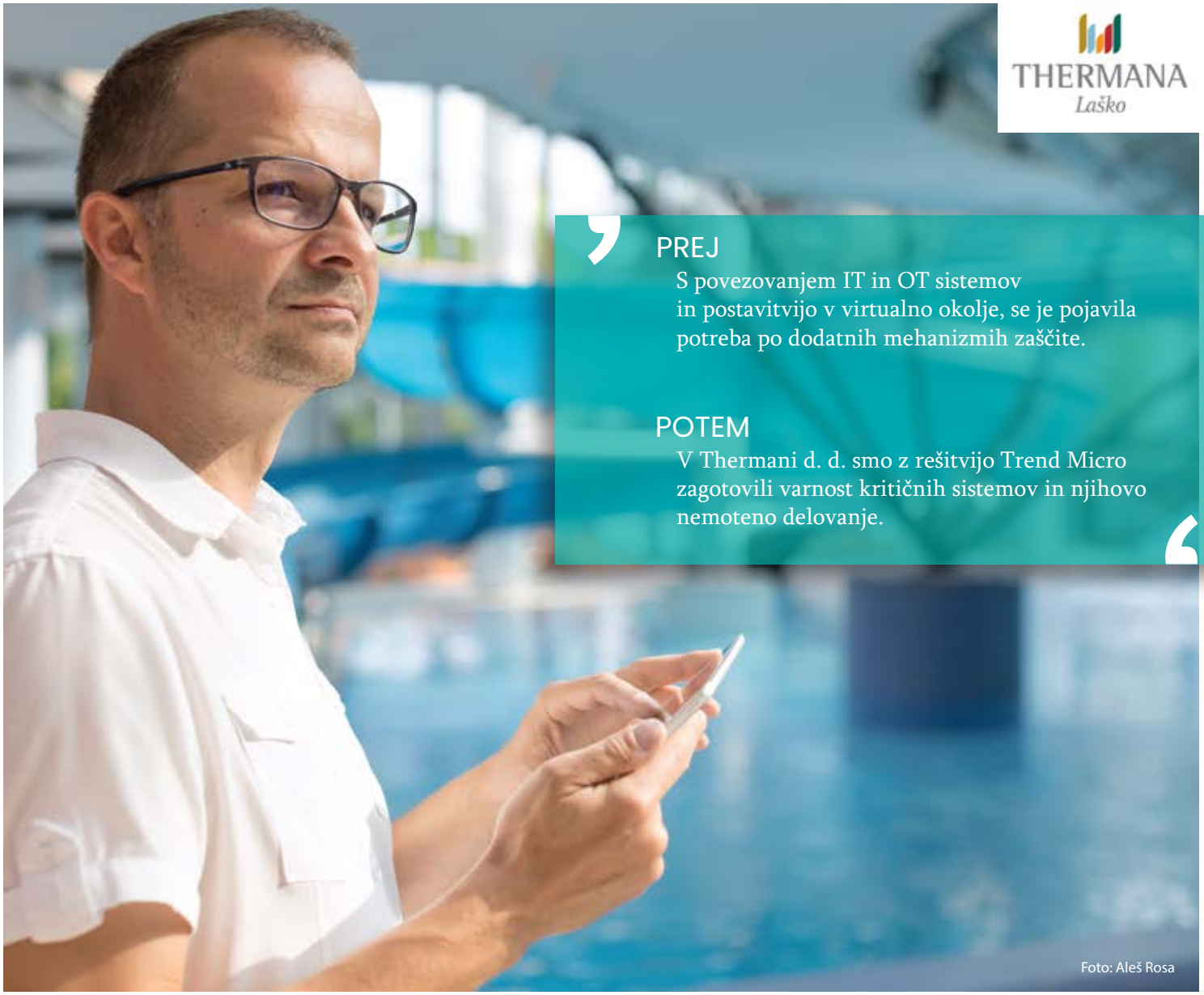
- ✔ Preprečevanje zaganjanja nepooblaščenih aplikacij.
- ✔ Zaščita pred izvajanjem škodljive programske kode (virusi, zlonamerna koda, napredne grožnje).
- ✔ Kontrola nad zunanjimi diski (USB, mrežni diski).
- ✔ Centralizirano upravljanje agentov:
  - pregled dogodkov (statusi agentov in kršitve),
  - avtomatizirana priprava poročil o stanju na sistemih in obveščanje preko e-pošte.

Prikaz vpeljave rešitve Trend Micro Portable Security 2



Prikaz vpeljave rešitve Trend Micro Safe Lock





Posledice nedelovanja posameznih sklopov ali celotnega industrijskega okolja in s tem kritičnih sistemov so za podjetje lahko katastrofalne.
Zaradi tega je pred združitvijo industrijskih in poslovnih procesov potrebno skrbno načrtovati ukrepe za informacijsko komunikacijsko varnost.
Pri tem vam lahko pomaga ekipa strokovnjakov podjetja Smart Com.

Če se srečujete s podobnimi izzivi, vam z veseljem svetujemo pri izbiri in izvedbi tehnološke rešitve, ki bo uporabniku prijazna, funkcionalno dovršena in cenovno sprejemljiva. Poleg svetovanja in implementacije sistema poskrbimo tudi za vzdrževanje sistema in tehnično podporo.

info@smart-com.si 01 5611 606 www.smart-com.si

SMART COM

TREND MICRO
Tehnološki partner