SPECIJALNI DODATAK ČASOPISA PC PRESS

PC PRESS

www.pcpress.rs

Mikro data centri
rešenja prilagođena potrebama

Sprečite sajberpretnje
da ih ne biste lečili

Data centri & Cyber security

Uloga softvera u povećanju efikasnosti i održivosti data centara

Cyber security danas
prilika ili neprilika

Ransomware pošast
kako da organizacije sačuvaju svoje podatke

Pet najboljih praksi
za dizajn data centra

Bezbednosni izazovi QR koda

Mikro data centri: rešenja prilagođena potrebama

Napredak digitalizacije u mnogim oblastima postavlja nove zahteve u svim industrijama. Traži se veća brzina protoka i obrada sve veće količine podataka i to što bliže procesu koji je izvor i korisnik ovih servisa

Zbog toga se javlja sve više zahteva za mikro *data* centrima u proizvodnji, u fabričkim halama ili tik pored njih. Mikro *data* centri obezbeđuju kratku latenciju i prostor za obradu većeg obima podataka tu, nadohvat mašina. Veliki, centralizovani *data* centri ne mogu biti od velike pomoći kod ovakvih zahteva.

Zahtev 1

Pouzdana i moćna infrastruktura

Mikro *data* centar i megazahtevi: napajanje i klimatizacija ne smeju zaostajati po kvalitetu, kapacitetu i pouzdanosti od sistema u velikim *data* centrima. Zbog toga se mikro *data* centri uobičajeno opremaju redundantnim sistemima napajanja i klimatizacije.

Varijante *Rittal* rešenja za IT klimatizaciju odgovaraju svim zahtevima: od minijaturnih *data* centara sa disipacijama reda kilovata, do onih koji zahtevaju moćna 53 kW rashladne snage u jednoj rashladnoj jedinici.

Ako imate mikro *data* centar smešten u jednom reku, *Blue e+* klima-uređaji će zadovoljiti svojom snagom i pouzdanošću, uz najveću uštedu energije i smanjenje ukupnih troškova. Provereni koncept neprikosnovenih *Rittal* industrijskih *Blue e+* klima-uređaja našao je mesto i u IT aplikacijama. Primena hibridnog pasivnog hlađenja omogućava i do 30 odsto ušteda u energiji, dok je smanjenje ukupnih troškova nabavke, eksploatacije i održavanja od neverovatnih 75 odsto u odnosu na klasične klima-uređaje.

Provereni koncept neprikosnovenih Rittal industrijskih Blue e+ klima-uređaja našao je mesto i u IT aplikacijama

Za mikro *data* centre koji imaju nešto veći obim opreme, a time i disipacije, preporučuje se primena LCU jedinica koje se montiraju direktno u serverski rek, tako da ceo sistem ostaje izolovan od uticaja okoline. LCU jedinice s direktnom ekspanzijom mogu da obezbede do 6,5 kW snage hlađenja, uz opcionu 1+1 redundansu u istom uređaju. LCU jedinice imaju optimizovani protok vazduha za efikasno hlađenje servera: struja hladnog vazduha ravnomerno je raspoređena po celoj visini reka u prednjoj zoni, tako da svaki server dobija potrebnu količinu vazduha.

Za još veće snage na raspolaganju su LCP jedinice s direktnom ekspanzijom ili vodom kao rashladnim fluidom, kao i hibridne jedinice, snage do 53 kW po jednom uređaju. Posebna prednost su minimalne dimenzije za optimalno iskorišćenje skupog prostora u *data* centru. Sistemi s vodenim hlađenjem rade u režimu temperatura 15/20°C, što omogućava *free cooling* režim u dužim periodima u odnosu na sisteme s nižom temperaturama rashladnih fluida.

Zahtev 2
Zaštita od uticaja okoline

Fabričko okruženje neretko nosi i rizike okoline: zaprljanu atmosferu, prisustvo vodene pare, vlage i agresivnih isparenja. Zbog toga je stepen zaštite od spoljašnjih uticaja bitan element. Osnovni zahtevi se mogu ispuniti jednostavnim, standardnim rešenjima: smeštaj opreme u serverske rekove zaptivene u stepenu IP55, što je uobičajen industrijski nivo zaštite. Ovako zaptiveni rekovi su idealni za okruženja s prašinom, vlagom i drugim problematičnim uticajima. Ako to nije dovoljno, *Rittal* nudi i dodatnu zaštitu koja uključuje viši nivo zaštite u vidu protivpožarnih obloga. *Rittal* MDC zapravo predstavlja „sef" koji je zaptiven i otporan na požar uz sve potrebne sertifikate. Dodatno opremljen unutrašnjim sistemom rane detekcije i automatskog gašenja obezbeđuje punu zaštitu od požara spolja i iznutra.

Zahtev 3
Modularno, skalabilno, proširivo, podesivo...

Zahtevi se menjaju, ponekad prebrzo, pa treba biti spreman. Mikro *data* centri moraju pratiti razvoj proizvodnje, nove programe i tehnologije. Zbog toga je princip modularnosti veoma važan: sva *Rittal*-ova rešenja omogućavaju proširenja u koracima koji odgovaraju korisniku, laku montažu i intervencije bez zaustavljanja rada IT opreme. Moguća je i demontaža i preseljenje na novu lokaciju prema potrebi.

Razvoj *data* centra mora svojom skalabilnošću da prati i oprema za napajanje i klimatizaciju: modularni UPS, konfigurabilni sistem napajanja, proširiva i promenljiva distribucija u samim rekovima.

Zahtev 4
Sve pod kontrolom

Nadzor i upravljanje radom *data* centra je strateška stvar, ne samo da biste imali punu kontrolu nad radom opreme. Podjednako je važno pratiti vitalne parametre infrastrukture kako biste predupredili havarijske situacije i reagovali na vreme u slučaju potrebe. Nije dovoljno imati samo direktan pristup do svakog uređaja koji je deo sistema napajanja ili klimatizacije već je preporučljivo imati nezavisan sistem merenja i nadzora.

Praćenje temperature i vlažnosti vazduha u karakterističnim tačkama *data* centra je osnovni i minimalni zahtev. Kontrola pojave kondenzata ukoliko postoji podignuti pod, nadzor i upravljanje sistemima za zabravljivanje kod rekova sa ograničenim pristupom, veza sa protivpožarnim sistemom… Daljinski nadzor nad svim ovim parametrima preko DCIM softvera čuva miran san.

Posebnu ulogu sistem daljinskog nadzora parametrima infrastrukture ima kod planiranja održavanja. Pravilnim izborom i praćenjem parametara može se predupredi havarija i smanjiti troškovi održavanja, prelaskom s redovnog na preventivno održavanje bazirano na praćenju vitalnih pokazatelja kvaliteta rada opreme. Primer je praćenje rada ventilatora i zaprljanosti filtera kako bi se intervencije na čišćenju svele na potrebnu meru, bez nepotrebnih odlazaka kada za tim ne postoji potreba.

Zahtev 5
Energetska efikasnost

Energetska efikasnost najviše zavisi od primenjene opreme i tehnoloških rešenja. Ne može se ići protiv prirode, ali se možete približiti granicama koje ona postavlja. Još je važnije iskoristiti svaku priliku i mogućnost da se smanji potrošnja energije.

Oprema za napajanje je sada tako efikasna i s tako malim gubicima da je tu jedva ostalo šta za uštede. Kod sistema klimatizacije, međutim, bitka još traje. Klasične kompresorske klime imaju snagu električne potrošnje koja odgovara trećini snage hlađenja ili više od toga. Korišćenje invertorskih pretvarača za napajanje omogućava da se izbegne neefikasni i stresni *on-off* režim uključenja kompresora i primeni precizna regulacija rada u skladu s trenutno potrebnom snagom hlađenja. Preko toga malo se može učiniti sa samim klima-uređajem.

Tu, međutim, stupa na snagu korišćenje drugih načina hlađenja. Hibridni uređaji, kakav je *Rittal Blue e+*, koriste inteligentno upravljanje radom, kombinovanjem precizno regulisanog kompresorskog režima i pasivnog hlađenja primenom posebno konstruisanog sistema s poboljšanim karakteristikama hlađenja okolnim vazduhom (*heat pipe*). Kada se smanji potrebna snaga hlađenja ili dovoljno padne temperatura spoljnog vazduha, pasivni sistem preuzima sve više ulogu hlađenja od kompresorskog agregata, smanjujući potrošnju.

Pravilnim izborom i praćenjem parametara može se predupredi havarija i smanjiti troškovi održavanja, prelaskom s redovnog na preventivno održavanje bazirano na praćenju vitalnih pokazatelja kvaliteta rada opreme

Sistemi s vodom kao rashladnim fluidom imaju takođe mogućnost efikasnog korišćenja spoljnog vazduha za hlađenje, bez uključivanja kompresora: indirektni *free cooling* u periodima nižih spoljnih temperatura može drastično da smanji ukupnu količinu energije utrošenu tokom godine. Ovo je posebno pogodno kod sistema koji mogu da koriste nešto više radne temperature fluida za hlađenje: *Rittal* LCP s radnom temperaturom 15/20°C može da radi u *free cooling* režimu već od temperatura koje su iznad 10°C, i sve su efikasniji kako temperatura ide dole. To je znatno efikasnije od sistema s radnim režimom 7/12°C, koji rade u punom *free cooling*-u kada temperatura priđe bliže nuli.

Još jedna bitna stvar: prema SRPS EN 50600 bitan segment implementacije energetske efikasnosti je praćenje parametara potrošnje u što više tačaka sistema napajanja kako bi se precizno odredili pravi parametri potrošnje. Dakle, odvojeno merenje aktivne potrošnje produkcione opreme od potrošnje sistema hlađenja, pumpi i drugih pratećih tehničkih potrošača. Jedino tako razgranato i precizno merenje i beleženje može predstavljati valjanu osnovu za kasniju analizu, optimizaciju potrošnje i smanjenje troškova.

Vesimpex.rs

Pet najboljih praksi za dizajn data centra

Data centri su klimatski kontrolisana okruženja posebno dizajnirana za smeštanje, napajanje i zaštitu osetljive IT opreme na koju se vaše poslovanje oslanja iz dana u dan

Ovi prostori su temelj kontinuiteta poslovanja, tako da se projektovanje i izgradnja *data* centara ne smeju shvatati olako. Zaista, uspeh dizajna modernog *data* centra zavisi od sposobnosti IT osoblja i objekata da uspešno uravnoteže često konkurentne potrebe za većom gustinom i poboljšanom agilnošću s većom efikasnošću i nižim troškovima, imajući pritom na umu najnovije standarde dizajna *data* centara.

Projektovanje *data* centara nije lak zadatak i zahteva veliko ulaganje vremena i resursa, ali ipak postoje neke temeljne prakse koje se primenjuju na bilo koji tip projektovanja/izgradnje. Radi što većeg uspeha projekta, bilo bi poželjno pratiti ove smernice:

- Odlučite koliki vam je prostor potreban i gde. *Data* centri dolaze u svim oblicima i veličinama, od jednostavnih serverskih soba, tradicionalnih objekata s podignutim podovima do kolokacije i hibridnih *cloud* rešenja. U današnje vreme, potreba za premeštanjem računarskih i skladišnih kapaciteta bliže krajnjim korisnicima dovela je do brzog rasta rešenja *edge data* centara i mikro *data* centara. Iako se *edge* mreže brzo širi, kompanijama su i dalje potrebni objekti *data* centra. Vlasnici i operateri moraće da odluče hoće li izgraditi nove *data* centre ili proširiti, naknadno opremiti ili nadograditi postojeće objekte. Kolokacija i *cloud* rešenja u oblaku nude još više izbora za IT i timove specijalizovane za objekte.

Projektovanje data centara nije lak zadatak i zahteva veliko ulaganje vremena i resursa, ali ipak postoje neke temeljne prakse koje se primenjuju na bilo koji tip projektovanja ili izgradnje

Data centar ne čine samo serveri

Bez obzira na arhitekturu *data* centra kojoj vaša kompanija teži, trebaće vam dovoljno prostora ne samo za servere, police za servere i mrežnu opremu, već i za neračunarske komponente infrastrukture *data* centra (napajanje, hlađenje i nadzor). Ne zaboravite da razmišljate izvan okvira i već sada planirate buduće potrebe za kapacitetom.

Pažljivo razmotrite ceo niz zahteva. Projektovanje *data* centara je toliko složeno zbog osetljive prirode opreme. Ona zahteva stalni izvor pouzdanog napajanja ili neprekidno napajanje (UPS), pravi sistem upravljanja toplotom za optimizaciju temperature i vlažnosti, solidne fizičke sigurnosne mere i mogućnost praćenja spoljnih uslova 24 sata dnevno. Skalabilno hlađenje, napajanje i „white space“ takođe su ključni kako bi se osiguralo da se *data* centar može proširiti prema vašim potrebama.

Dobra je ideja okupiti lidere IT-ja, objekata, mreže i sigurnosti u ranim fazama projektovanja *data* centra kako bi se definisao čitav skup zahteva za prostor. Finalni dokument sa zahtevima poslužiće kao nacrt za izradu detalja vašeg dizajna.

Neke stvari su već spremne

Predintegracija, prefabrikacija i fleksibilni dizajn pomoći će vam da budete efikasniji. Projektovanje tradicionalnih data centara često

dovodi do specifikacije proizvoda od više dobavljača, a zatim do upravljanja integracijom različitih rešenja, što može dovesti do poteškoća pri puštanju u rad i kašnjenja implementacije, a da ne pominjemo probleme s izvođenjem. Uz sve veću potrebu za računarskim kapacitetom, tradicionalna gradnja od cigle i maltera postaje sve ređa. Prefabrikovana modularna rešenja mogu osigurati bolji put do uspeha u mnogim slučajevima, smanjujući ukupne troškove i rizik, istovremeno ubrzavajući dizajniranje *data* centra i izgradnju.

S prefabrikovanim rešenjem *data* centra, sistemi se sastavljaju, integrišu i testiraju u fabričkom okruženju izvan lokacije kako bi se ubrzala implementacija i poboljšala predvidljivost rasporeda dizajna/izrade. Korišćenjem ponovljivih blokova podsistema, prefabrikovani pristup nudi efikasniji proces projektovanja s niskim rizikom. Dizajn je takođe obično skalabilan, što omogućava brz odgovor u slučaju povećane potražnje.

Prefabrikovana i unapred integrisana rešenja mogu uključivati podsisteme, kao što su upravljanje toplotom, zaštita i distribucija energije, kontrole i softver za upravljanje i usluge, ali i pomoćne sisteme, kao što su rasveta, zaštita od požara, fizička sigurnost i obrada vode.

Standardi su važni

Kao i svaki novi projekat izgradnje objekta, dizajn zgrade *data* centra mora da sledi kodove i standarde. Uz međunarodne, nacionalne i lokalne propise i zahteve koji se primenjuju na građevinske projekte svih vrsta, neki od najvažnijih standarda koje

treba uzeti u obzir za dizajn *data* centra uključuju:

Uptime Institute Tier Standard: standard za otpornost, redundansu i pouzdanost *data* centra koji pruža smernice za faze projektovanja, izgradnje i puštanja u rad projekta.

ANSI/TIA-942: određuje fizičke aspekte *data* centara, uključujući telekomunikacionu infrastrukturu, lokaciju, arhitekturu, električne i mehaničke sisteme, zaštitu od požara i sigurnost.

EN 50600: kao prva evropska transnacionalna norma, ova serija ima holistički pristup planiranju, izgradnji i radu *data* centra.

Započnite definisanjem najboljih praksi dizajna data centra

Iako su dizajn i izgradnja bilo kog *data* centra složeni procesi, poznavanje najboljih praksi uveliko će doprineti boljoj organizaciji vašeg projekta. Objedinjavanje zahteva i standarda uz uključivanje ključnih igrača u definisanje i dokumentovanje kritičnih potreba (uključujući efikasnost i fleksibilnost) od samog početka, pomoći će u postavljanju pravih temelja i postizanju uspeha.

Iako su dizajn i izgradnja bilo kog data centra složeni procesi, poznavanje najboljih praksi uveliko će doprineti boljoj organizaciji vašeg projekta

Vertiv™ rešenja za dizajn data centra

Vertiv™ pomaže kompanijama da izgrade i prošire *data* centre bilo gde u svetu, uključujući *edge data* centre, *data* centre i rešenja za kolokaciju i *cloud* rešenja. Neka od najpopularnijih rešenja za dizajn *data* centara dostupna u *Vertiv*™-u uključuju:

Vertiv™ SmartMod™ modularna infrastruktura *data* centra. Ove prefabrikovane strukture idealne su za razne primene i industrije. Dizajnirana kao lako prenosivi, prefabrikovani moduli za brzu implementaciju, kućišta su temeljni građevni blok za moderni modularni dizajn *data* centra.

Vertiv™ Power Module 1000/1200. Ova rešenja omogućavaju implementaciju izolovanih, energetski gustih, kritičnih infrastrukturnih kapaciteta tačno na vreme kako bi zadovoljili vaše poslovne zahteve. Možete brzo da izgradite redundantne blokove kritične energetske infrastrukture za vaš novi ili postojeći objekat, što vam omogućava da se usredsredite na osetljiva područja objekta koja zahtevaju najviše upravljanja.

Saznajte više o Vertiv™ integrisanim rešenjima na Vertiv.com ili nas kontaktirajte na croatia.hello@Vertiv.com da biste saznali kako možemo da sarađujemo na vašem sledećem projektu dizajna data centra.

Uloga softvera u povećanju efikasnosti i održivosti data centara

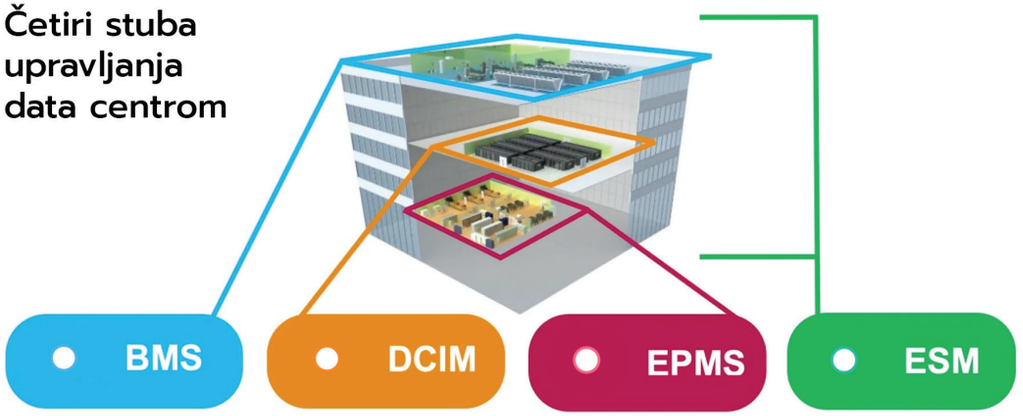
Industrija data centara dugo se smatrala pionirom u razvoju novih načina povećanja energetske efikasnosti i uključivanja obnovljive energije u svoju strategiju nabavke energije. Uprkos tome, sve veća potražnja za digitalnom infrastrukturom znači da će potrošnja energije data centara nastaviti da raste

Aleksandar Bukva, Key Account Manager Secure Power

Ispunjavanje ovih sve većih zahteva često izgleda kontradiktorno ciljevima održivosti *data* centara, ali se oba mogu rešiti digitalizacijom. Prema Svetskom ekonomskom forumu, preduzeća na vodećim pozicijama u digitalizaciji ostvarila su povećanje produktivnosti od 70 odsto, u poređenju s povećanjem od 30 odsto za organizacije koje su sporije digitalizovali svoje poslovanje. *Data* centri mogu da iskoriste digitalizaciju kako bi povećali produktivnost i takođe se pozabavili unapređenjem održivosti. Obično se operateri *data* centara suočavaju sa četiri glavna izazova - smanjenje potrošnje energije, smanjenje troškova energije, povećanje produktivnosti i održavanje pouzdanosti, što se sve može poboljšati digitalizacijom.

Operativni podaci i analitika su u osnovi održivosti svakog *data* centra. Napredna softverska rešenja mogu istovremeno da podrže inteligentno nadgledanje i kontrolu napajanja, celog objekta i IT sistema za rad, efikasnost i održivost. Za hiperskalere i *colocation* provajdere, digitalizacija i inteligentno korišćenje podataka su već sastavni deo implementacije i rada *data* centara. Na primer, pre više od šest godina, *Google* je govorio o tome kako su koristili *DeepMind* mašinsko učenje da bi smanjili količinu energije za hlađenje do 40 odsto.

Bez obzira na primenu najsofisticiranijih tehnologija od strane hiperskalera, neadekvatan softver koji se



tradicionalno primenjuje u industriji *data* centara ne dozvoljava vizuelizaciju u realnom vremenu i isporuku uvida potrebnih za poboljšanje performansi do nivoa potrebnih za *colocation* operatere. Operaterima je potreban pristup inteligentnim kontrolnim interfejsima da bi bili upozoreni na probleme i brzo prepoznali rešenja.

Četiri stuba podataka

Operateri *data* centara moraju se u isto vreme suočiti sa inherentnom složenošću objekata *data* centara i izazovima upravljanja geografski udaljenim lokacijama. Da bi odgovorili ovim izazovima, operateri se oslanjaju na softverske alate za upravljanje, kao što su sistemi za upravljanje zgradom/objektom (BMS), sistemi za nadzor električne energije (EPMS) i upravljanje infrastrukturom *data* centra (DCIM). Ovi sistemi obezbeđuju vidljivost i mogućnost praćenja svih udaljenih lokacija IT infrastrukture i *data* centara.

Ova tri stuba upravljanja *data* centrom omogućavaju pružanje usluga i obezbeđuju efikasnu primenu, rad i održavanje infrastrukture i IT opreme. Međutim, sve veći fokus među pružaocima usluga *data* centara na održivost životne sredine dovodi do pojave četvrtog stuba upravljanja *data* centrom: upravljanja održivošću životne sredine (ESM). Efikasan ESM softver treba da podrži upravljanje energijom, vodom i drugim uticajima na životnu sredinu unutar svakog objekta i kroz čitavu IT infrastrukturu.

Operativni podaci i analitika su u osnovi održivosti svakog data centra. Napredna softverska rešenja mogu istovremeno da podrže inteligentno nadgledanje i kontrolu napajanja, celog objekta i IT sistema za rad, efikasnost i održivost

Efikasna softverska rešenja

Najnovije softverske platforme za monitoring mogu da zadovolje sve potrebe koje su potrebne u prva tri stuba. Na primer, *EcoStruxure* rešenje kompanije *Schneider Electric* primenjuje softver, analitiku i usluge u tri glavna domena: *EcoStruxure Power*, *EcoStruxure Building* i *EcoStruxure* IT, omogućavajući korisnicima vidljivost svih parametara infrastrukture unutar njihove organizacije. Ova povećana vidljivost daje operaterima uvid koji im pomaže da poboljšaju energetsku efikasnost i napore za održivost. Da bi se pozabavio četvrtim stubom izveštavanja o održivosti, *Schneider Electric* u svom portfelju nudi i *EcoStruxure Resource Advisor.*

Platforma *EcoStruxure Resource Advisor* podržava naprednu analitiku podataka o snabdevanju, potrošnji i performansama resursa. Ovo podrazumeva varijable koje nisu uključene u drugi softver za upravljanje *data* centrom, kao što su emisije gasova staklene bašte, troškovi nabavke energije i kombinacija izvora energije. Širok spektar prikupljenih podataka može imati koristi iznad i izvan izveštavanja o održivosti. Inteligentna analiza punog spektra podataka o energiji i održivosti koji dolaze iz različitih sistema takođe može pružiti uvid koji će vam pomoći u krajnjoj liniji.

Obezbeđivanje kvaliteta podataka

Svaki sistem može biti dobar onoliko koliko je kvalitet podataka koji analizira. Izreka „kako seješ tako ćeš i žeti“ veoma je relevantna za mnoge tokove podataka o održivosti. Bez kvalitetnih podataka ne možemo imati jasnu sliku celokupne infrastrukture i ne možemo donositi kvalitetne odluke o poboljšanju efikasnosti, što rezultira nepotrebnim troškovima bilo po pitanju niske efikasnosti ili investicije u pogrešno odabrana rešenja.

Ecostruxure softverske platforme omogućavaju baš to, prikupljanje svih relevantnih podataka koji su kvalitetni i dostupni u realnom vremenu, kako bi se na osnovu njih donosile kvalitetne odluke u cilju povećanja energetske efikasnosti i održivosti. Tačni, čisti i dinamični podaci mogu se zatim koristiti u celom vašem preduzeću da biste uštedeli novac i povećali efikasnost i transparentnost.

Kao samo jedan od primera, DCIM softver *EcoStruxure* IT *Expert* omogućava menadžerima da optimizuju performanse upoređujući performanse svoje infrastrukture s performansama svojih kolega širom sveta i dobijaju preporuke zasnovane na podacima o tome kako da se poboljšaju. Još jedna komponenta DCIM rešenja nove generacije kompanije *Schneider Electric*, *EcoStruxure* IT *Advisor*, pruža dodatne pogodnosti, uključujući optimizaciju kapaciteta. Pomaže menadžerima da odluče gde da postave dodatne servere i drugu IT opremu, u smislu optimalne operativne efikasnosti iz perspektive napajanja i hlađenja.

Otkrijte kako softver može da poveća efikasnost data centra

Kako *data* centri postaju sve veći, složeniji i sve važniji za funkcionisanje društva, operaterima *data* centara je potreban odgovarajući softver koji će im pomoći da skaliraju dok optimizuju operacije za smanjenje potrošnje energije. To je balansiranje koje se može postići pravilnom strategijom. Da biste saznali više o tome kako softver može pomoći operacijama vašeg *data* centra da postignu ovu ravnotežu, pogledajte *Poglavlje 4* u vodiču za izazove održivosti.

se.com

Opravdanost i isplativost free cooling-a

Free cooling je rešenje koje za odvođenje toplote iz data centra koristi nisku temperaturu spoljašnjeg vazduha, a u zavisnosti od lokalnih klimatskih uslova, može se koristiti tokom većeg dela godine

Free cooling je ekonomični metod korišćenja temperature spoljašnjeg vazduha, u asistenciji s hlađenjem vode. Kada spoljna temperatura postigne vrednost koja je niža u odnosu na normativnu vrednost temperature, ovaj sistem koristi spoljašnji vazduh kao rashladni izvor. Pomoću ovog principa maksimalno se smanjuje potrošnja električne energije za rad sistema klimatizacije jer se koristi već hladan spoljašnji vazduh. To znači da ovakvo rešenje, kada se koristi na lokacijama s niskim do umerenim ambijentalnim temperaturama, može da postigne potrebnu rashladnu snagu veoma energetski efikasno i ekonomično, jer se automatski koristi indirektni *free cooling* kada su spoljašnje temperature niske. Upotreba *free cooling*-a izuzetno smanjuje operativne troškove.

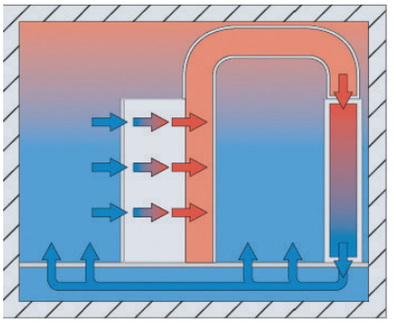
Rittal koncepti kontrole klime visoke efikasnosti

Nemačka kompanija *Rittal GmbH & Co*. koja se bavi celokupnom proizvodnjom, izradom, konsaltingom i instalacijom data centara, između ostaloga, bavi se i savremenim rešenjima klimatizacije data centara.

Rittal-ov koncept klima kontrole usmerava hladni vazduh direktno do opreme preko fizički formirane hladne zone. Hladni vazduh je usmeren na celoj visini rek ormara, osiguravajući da nema vrućih tačaka, a vrući vazduh se izvlači iz sistema. Zbog hladne zone koja je fizički odvojena od tople zone, topli izduvni vazduh se ne može pomešati sa hladnim ulaznim vazduhom, pa dolazi do povećanja efikasnosti sistema. Optimalna temperatura unutar hladne zone je između 22° C i 25° C. Izuzetna energetska efikasnost *Rittal*-ovog koncepta hladne zone ima jednostavno i verodostojno objašnjenje:

- Ulazni hladan vazduh i otpadni vruć vazduh se ne mogu mešati.
- Sistemom može da se upravlja na značajno višem temperaturnom nivou.
- Kao rezultat povećane razlike temperature između usisnog i otpadnog vazduha, klima uređaji rade na optimalnoj toplotnoj razlici.

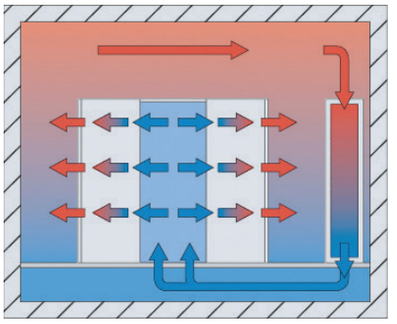
Slika 2. Standardni koncept klimatizacije data centara



Na primerima može se uočiti razlika koncepta kontrole standardnih klima uređaja i *Rittal*-ovih klima uređaja. Na slici 2. je prikazan standardni koncept klimatizacije data centara gde se vrši izvlačenje vrućeg vazduha pomoću sistema kanala:

- Složen i skup sistem kanala.
- Veći zahtevi za površinom i visinom prostorije.
- Ograničenje visine podignutog poda.
- Nema ravnomernog dovoda vazduha za hlađenje u prostoriju.
- Upravljanje kablovima je otežano.
- Izuzetno visok gubitak pritiska sa vazdušne strane, što dovodi do povećane potrošnje energije ventilatora.

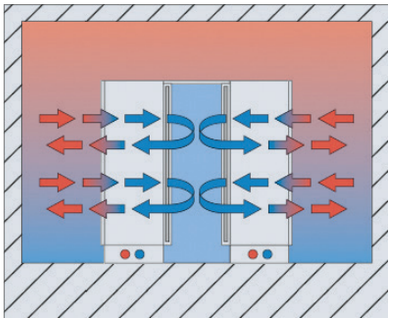
Glavni potrošač u server salama, ako se izuzme ICT oprema, su sistemi klimatizacije. Upravo najveća ušteda električne energije nalazi se u unapređenju ovog sistema



Slika 3. Rittal-ov koncept sa podignutim podom

Na slici 3. je prikazan *Rittal*-ov koncept klima uređaja sa fizički formiranom hladnom zonom i podignutim podom:

- Upotreba standardnih jeftinih jedinica za cirkulaciju hladnog vazduha. Pozicioniranje izvan područja servera.
- Nesmetana i ujednačena raspodela protoka vazduha za hlađenje u hladnoj zoni garantuje visoku efikasnost
- Povoljni uslovi rada u hladnoj zoni zbog uslova niske temperature, protoka i buke.
- Rek ormari koji nisu fizički povezani sa kućištem klima uređaja



Slika 4. Rittal-ov koncept bez podignutog poda

ne smanjuju efikasnost hlađenja hladne zone.
- Visina prostorije igra minimalnu ulogu jer je formirana hladna zona data centra.

Na slici 4. je prikazan *Rittal*-ov koncept klima uređaja sa fizički formiranom hladnom zonom i bez podignutog poda:

- Direktno povezivanje LCP-ova (*Liquid Cooling Package*) na spoljni dovod hladne vode.
- Jednostavno polaganje cevovoda u postolje/podnožje reka.
- Homogena raspodela vazduha za hlađenje u hladnoj zoni garantuje visok nivo efikasnosti
- Povoljni uslovi rada u hladnoj zoni zbog uslova niske temperature, protoka i buke.
- Rek ormari koji nisu fizički povezani sa kućištem klima uređaja ne smanjuju efikasnost hlađenja hladne zone.
- Visina prostorije igra minimalnu ulogu.

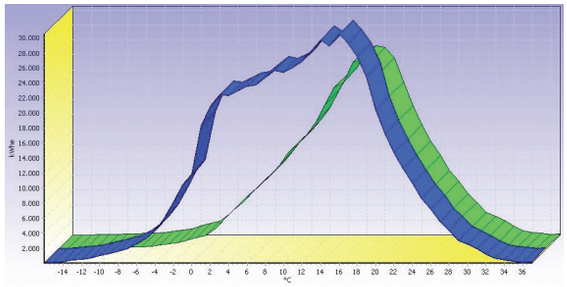
Iz navedenog se može zaključiti da uvođenje vertikalnih izmenjivača isključuje korišćenje prostora ispod podignutog poda za strujanje vazduha. Postojeće ploče sa prostrujnim rešetkama se zamenjuju punim pločama. Redundansa se postiže ugradnjom dovoljnog broja LCP jedinica u pogodnom rasporedu.

Izmenjivači se instaliraju između rekova. Izduvavanje hladnog vazduha je spreda, a povratak toplog vazduha sa zadnje strane uređaja. Uređaji imaju redundantne ventilatore koji su jedini deo koji se eventualno može pokvariti. Zamena je brza i jednostavna, bez prekida i ugrožavanja funkcionisanja uređaja.

Uvođenje free cooling režima rada

Free cooling predstavlja korišćenje spoljašnjeg vazduha za hlađenje rashladnog fluida u periodima niskih spoljnih temperatura. Kada je temperatura dovoljno niska, smanjuje se ili isključuje hlađenje kompresorima a fluid se prebacuje u tzv. FC konturu gde se hladi okolnim vazduhom. Umesto potrošnje električne energije u kompresorima, rade samo ventilatori daleko manje snage. Efikasnost *free cooling*-a zavisi od sledećih parametara:

- Klimatski uslovi, odnosno dijagram srednjih vrednosti temperatura tokom dana, u toku godine. Što su temperature niže, veće je iskorišćenje ovog režima.
- Kvalitet i efikasnost sistema, odnosno sposobnost FC konture da efikasno hladi već pri malim razlikama između temperature fluida i okolnog vazduha.

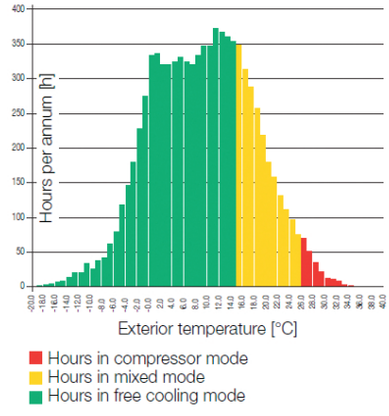


Slika 5. Komparacija energetske efikasnosti u free cooling režimu rada

Značaj implementiranja *free cooling*-a se može uočiti na slici 5. Free cooling režim rada se u chiller-ima može javiti u sledećim oblicima:

- Integrisan ili kao eksterni hladnjak (*dry cooler*) za individualne *chiller*-e
- Eksterni hladnjak povezan na dva *chiller*-a
- Eksterni hladnjak povezan na tri *chiller*-a

U svim *chiller*-ima, u kojima nije fabrički integrisan *free cooling* sistem, isti se može naknadno ugraditi bez potrebe za zamenom sistema za podešavanje, već samo primenom hidrauličkog sistema. U jednom sistemu se može povezati maksimalno osam *chiller*-a. U *Rittal*-ovoj ponudi standardno postoje spoljne *chiller* jedinice rashladne snage od 15 do 481 kW, a po potrebi i snažnije.



Raspodela raznih režima rada chiller-a tokom godine, Minhen

Oprema koja je implementirana u *chiller*-ima je sledeća:

- Pumpa sa regulacijom brzine ili konstantna
- Rezervne pumpe
- Hidraulični moduli
- *Free cooling* (opciono)
- SNMP/*Modbus* monitoring
- Zimska oprema (opciono)
- Oprema merenja efikasnosti rada (opciono)

Sve zavisi od snage data centra

Angažovana snaga ICT opreme unutar data centara je unapred određena i ne može se mnogo uticati na nju. Iz ovog razloga sistemi uštede energije koji se primenjuju u industriji, optimizacija potrošnje selektivnim isključivanjem pojedinih potrošača i korigovanje dnevnog dijagrama potrošnje nisu primenjivi. ICT oprema mora da radi neprestano i bez kompromisa. Zbog toga, mogućnosti za uštedu energije u data centru svode se na uštedama u potrošnji energije prateće opreme i merama za njeno efikasno iskorišćenje. Smanjivanje tzv. PUE faktora (*Power Usage Effectiveness*) je ključni zadatak. PUE se može smanjiti na različite načine, koji su određeni konkretnim uslovima u data centrima i mogućnostima primene efikasnijih i „štedljivijih" sistema fizičke IT infrastrukture.

Glavni potrošač u server salama, ako se izuzme ICT oprema, su sistemi klimatizacije. Upravo najveća ušteda električne energije nalazi se u unapređenju ovog sistema. Dizajn i sistem upravljanja linije *Rittal TopTherm* LCP čine ga posebno energetski efikasnim. Efikasno hlađenja postiže se čak i pri visokim spoljnim temperaturama. Ovo omogućava povećanje udela indirektnog besplatnog hlađenja (*free cooling*), što zauzvrat značajno smanjuje potrošnju energije, povećava energetsku efikasnost i pomaže u zaštiti životne sredine.

Uštede postignute ovom vrstom rada su ogromne, a efikasnost hlađenja je značajno poboljšana. LCP-ovi koji se koristi zajedno sa *chiller*-ima imaju znatno veći odnos energetske efikasnost (*Energy Efficiency Ratio* - EER). EER je odnos između uložene snage, u obliku potrošnje električne energije i izlazne snage, u obliku rashladne energije.

Rittal.com


EDGE
Data
Centri
SVE IZ JEDNE RUKE
Vesimpex
Patrijarha Dimitrija 24, 11090 Beograd,
tel. 063 33 90 90
• www.itinfrastruktura.rs
• www.vesimpex.rs
• info@vesimpex.rs
RITTAL

Cambium Networks™

Network Service Edge 3000

SD-WAN

- Routing
- WAN Load-Balancing
- WAN Failover
- Bandwidth control
- WAN QoS
- L2TP-IPsec VPN

SECURITY

- Firewall
- IDS/IPS
- VPN with MFA
- IoT Security
- LAN security assessment
- Zero Trust Network Access
- Geo-IP filters

SERVICES

- DHCP server
- RADIUS server
- Directory connectors
- DNS server

- cnMaestro Cloud Management
- Zero-touch provisioning
- Reusable group configuration
- Network security audit
- Dashboard widgets with comprehensive device overview and network health
- Intrusion attempts - severity, details, country of origin, remedial measures

INGRAM MICRO
E: igor.jurican@ingrammicro.com
T: +385 91 4692 261
A: Štefanovečka cesta 10, Zagreb

Posjetite nas!

http://cambium.ingrammicro.hr

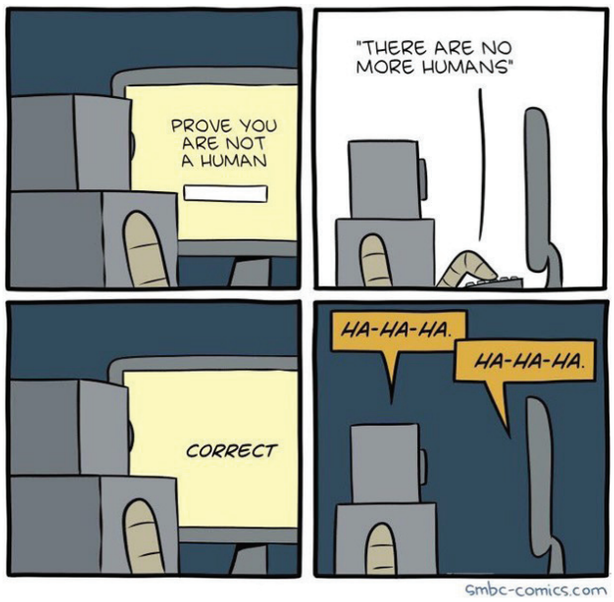
Cyber security danas: prilika ili neprilika

Krajem marta veliku pažnju javnosti privuklo je otvoreno pismo koje je napisao profesor MIT-a Max Erik Tegmark, tvrdeći da smo svi u opasnosti od nekontrolisanog razvoja veštačke inteligencije

Kristijan Lazić

Pismo profesora *Tegmark*-a prostire se na nekoliko strana i može se svesti na sledeće: ukoliko se nastavi ovakav model razvoja veštačke inteligencije, dakle model vođen prilagođen interesima kompanija a ne društva u celini, može nam se dogoditi da nas veštačka inteligencija nadvlada i istisne iz tokova evolucije, slično kao što je *Homo sapiens* istisnuo neandertalce.

Navikli smo da diskusije o računarskoj bezbednosti obiluju „argumentima“ koji u sebi sadrže elemente straha, neizvesnosti i sumnje (engleska skraćenica FUD, *Fear, Uncertainty and Doubt)*, ali uglavnom se „mračna komponenta“ diskusije odnosila na visok rizik od (značajne) štete po računarske sisteme, podatke i reputaciju. Ovog puta lestvica je podignuta na najviši mogući nivo – upozoreni smo da je ugrožen čovek kao vrsta! Otvoreno pismo je do sada potpisalo više od 27.000 visokoobrazovanih stručnjaka, među kojima su brojni istraživači veštačke inteligencije, kao i niz „zvučnih“ imena iz IT zajednice, kao što je *Steve Wozniak*.



Ubrzana evolucija?

Počeci *cyber* bezbednosti kao tehničke discipline neodvojivi su od razvoja ostalih računarskih nauka. Otkako su prvi IT sistemi postali „opremljeni“ mogućnošću razmene podataka, počeli su i simptomi prvih „prehlada“. Pioniri ere kućnih računara, pre svega prvih *desktop* PC-ja, dobro se sećaju računarskih virusa koji su stizali putem zaraženih disketa i zadavali ozbiljne glavobolje tadašnjoj (za današnje pojmove) skromnoj IT zajednici. Napredak kome smo svedočili širenjem Interneta u okviru univerzitetskih zajednica, a koji se za svega par godina „uvukao“ u sve privatne i poslovne aspekte društva, doneo je nam je i mrežne crve, trojanske konje, makro viruse u *Word* i *Excel* fajlovima, kao i prve „zaražene“ *Web* sajtove.

Najvažnija prednost koju smo stekli u odnosu na ostali živi svet, sposobnost sticanja i primene složenih znanja i veština koju nazivamo inteligencijom, je „napadnuta“! I to ne direktno od drugog čoveka, već od njegovog pažljivo razvijanog proizvoda – algoritama veštačke inteligencije

Period u kome su meta bili pretežno računarski sistemi zamenila je era u kojoj su cilj zlonamernih aktera postali podaci i informacije. Iz perspektive 2023. godine, prvobitne krađe platnih kartica izgledaju kao sitne krađe slatkiša u velikim trgovinskim lancima u odnosu na godine koje su sledile i donele krađu identiteta, ličnih podataka, masovne odlive poverljivih poslovnih informacija pa čak i vojnih tajni. *Julian Assange* i *Edward Snowden* mesecima su bili planetarna tema broj jedan i u stručnoj zajednici i u medijima uopšte, ali smo ih zaboravili brže nego viruse poput „Mikelanđela“ ili mrežnih crva kao što je *WannaCry.*

A onda nam se „desio“ COVID-19, *online* rad od kuće i, za mnoge, trajna promena načina poslovnog angažovanja. Pandemiju ćemo pamtiti i kao period u kome smo bili preplavljeni neistinama, poluinformacijama, dezinformacijama pa i potpunim besmislicama, u kojima je istinu bilo gotovo nemoguće pronaći. Bezbednosni perimetar korporacija postao je „difuzan“, jasna granica između zaštićenog IT okruženja koje se čuva i Interneta u praksi je nestala. Obuke iz informacione bezbednosti polako su počele da iz svojih obaveznih segmenata potiskuju module, poput „Recimo ne zaraženom USB drajvu!“, *Click before you think!* sa „Ne verujte (skoro pa ničemu) što vidite i čujete!“. Uznemireni i uplašeni, ljudi su postali podložniji socijalnom inženjeringu koji je, uz napredak sistema za *online* prevođenje, postajao sve uspešniji u pronalaženju lakovernih.

Kao da sve to nije bilo dovoljno, poslednji element IT bezbednosti, čovek, je bio fizički ugrožen i naglo izmešten iz namenskog radnog okruženja u svoj privatni prostor. Jedva primetno, najvažnija prednost (?) koju smo stekli u odnosu na ostali živi svet, sposobnost sticanja i primene složenih znanja i veština koju nazivamo inteligencijom, je „napadnuta“! I to ne direktno od drugog čoveka, već od njegovog pažljivo razvijanog proizvoda – algoritama veštačke inteligencije.

ChatGPT (r)evolucija

Napredak i softverski razvoj u modelima neuronskih mreža poznatijih kao

Generative Pre-trained Transformers, skraćeno GPT, doneo nam je softverski servis kojim je većina planete fascinirana poslednjih meseci – *ChatGPT*. Verujem da nema osobe koja nije iznenađena mogućnostima ove platforme, najpopularnije, ali ipak samo jedne u nizu mnogih o kojima se neprestano priča. Naša čula i um su oduševljeni ali i zbunjeni. IT esnaf je „iz naftalina izvadio" Tjuringov test, jednu od prvih metoda za određivanje da li je računar sposoban da razmišlja kao ljudsko biće, pokušavajući da utvrde koji od sistema nas je „pobedio". Teoretičari zavera su dodatno preplavili već zagađen medijski prostor. Mnogi su se uplašili za budućnost svojih profesija i setili se „trošne dedine kuće" pored koje može da se gaji povrće. Školarci manje „spavaju nad knjigom" i već su počeli da koriste neke od sistema za rešavanje domaćih zadataka; problem, ipak, i dalje predstavlja kada treba objasniti nastavnicima neke od međukoraka, a „rešenje" se traži bežanjem na *online* nastavu.

Manje spavaju i kriminalci, barem onaj deo koji je i do sada koristio tehnologiju, pokušavajući da osmisle nove načine kako da zaobiđu logičke barijere kod ljudi i navedu ih da urade nešto što im nije u interesu. Modeli su različiti, od pojave (gotovo) savršenih neželjenih *spam* i *phishing* poruka, tekstova za koje je gotovo nemoguće odrediti da li ih je pisao čovek ili ih je sastavio AI softver, do računarski generisanih slika ljudi, bića ili predela koji ne postoje, a koje su u stanju da obmanu i ozbiljna imena iz sveta fotografije. Stara šala: „Je l' više veruješ meni ili svojim očima?" u današnje vreme zvuči kao ozbiljno pitanje.

Najmanje spavaju, ili je barem to subjektivni utisak autora ovog teksta, oni kojima je posao da zaštite sva tri „sveta" tog neraskidivog ekosistema bezbednosti – IT tehnologiju, podatke i čoveka koji ih koristi. Dovoljno je složeno podesiti tehničke mere zaštite i uskladiti se s rastućom regulativom u oblasti zaštite podataka, neophodno znanje za uspeh zahteva i godine iskustva. Bezbednost je uvek bila igra mačke i miša, ali nikada pre miš nije imao ovoliku prednost. Zato i ne čudi vapaj poznatog profesora, apel da se mora stati, bar za trenutak, i promisliti kuda to idemo u odnosu na to gde želimo da stignemo.

Regulativa

Prvi korak ka tome da „vratimo duha u bocu" jeste uspostavljanje jasnog dogovora između svih nas, koji će biti artikulisan u formi zakonske regulative sa ciljem da barem načelno spreči mogućnost da se napredak u razvoju algoritama veštačke inteligencije koristi protiv opštih načela čovečanstva. U našem okruženju, prvi značajan korak načinila je Evropska unija donošenjem predloga Zakona o veštačkoj inteligenciji *(Artificial Intelligence Act* – AIA), o kome smo pisali avgusta 2022, a slična inicijativa pokrenuta je i u SAD početkom ove godine.

Važno je istaći i da je među prvim zemljama koje su prepoznale značaj veštačke inteligencije i Srbija, koja je, prateći svetsku praksu, februara ove godine usvojila dokument naziva „Etičke smernice za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije". Osnovni postulat svih zakonskih formi, ma gde bile usvojene, veoma je jasan – sprečavanje sistema veštačke inteligencije koji uzrokuju ili bi mogli da nanesu fizičku ili psihološku štetu čoveku. U toku je značajan napor da se novi zakoni usklade s već postojećom regulativom iz oblasti zaštite privatnosti, a neki od aktuelnih predloga o kojima se vodi javna stručna diskusija treba da urede način obaveznog označavanja slika generisanih veštačkom inteligencijom.

Administrativne mere trebalo bi da odvrate pojedince i grupe od zloupotrebe sistema veštačke inteligencije, ali kao za i svaki propis, jedino dosledna primena može (pomalo) dati praktične rezultate. S druge strane, veliki put je pred svima kada su u pitanju tehničke mere, za koje se u ovom trenutku može konstatovati da praktično ne postoje. „Hladne obloge" koje većina korporacija trenutno primenjuje, predstavljaju prostu zabranu pristupa sajtovima koji nude AI servise, ali takav sistem kontrole je privremen. Zabrinjava činjenica da ćemo se protiv zlonamernog korišćenja AI tehnologije verovatno boriti nekim sličnim sistemima koji će biti pod strogom kontrolom. Opet, najvažnija od „utešnih" činjenica je i ta da je tehnologija veštačke inteligencije jednako nepoznata i akterima na „tamnoj strani", pa ćemo, nažalost, učiti jedni od drugih u hodu.

„Hladne obloge" koje većina korporacija trenutno primenjuje, predstavljaju prostu zabranu pristupa sajtovima koji nude AI servise, ali takav sistem kontrole je privremen

Bezbednost je uvek bila igra mačke i miša, ali nikada pre miš nije imao ovoliku prednost

Bezbednost je jedna od osnovnih ljudskih potreba, pa je pitanje vremena kada ćemo „ukrotiti" AI sisteme tako da nam budu isključivo na korist, a ne na štetu. Do tog zamišljenog trenutka, iskoristite priliku da uskočite u voz koji je već krenuo!

Sinergija veštačke inteligencije i robotike

Razvoj robotike, 3D štampe i autonomnih sistema koji bez čoveka za upravljačem mogu da lete, plove ili voze, uskoro će se spojiti sa svetom veštačke inteligencije. Teško je proceniti kada će se to desiti u komercijalnom ekosistemu i kako će ta integracija izgledati, a ako je suditi po trendovima, brzo ćemo početi da srećemo pametne robote. Rojevi malih letećih dronova koji nose pakete i autonomno sleću bez intervencije centralnog sistema, komunicirajući međusobno, prateći jednostavna pravila poput onih inspirisanih prirodnim rojevima, na korak su da iz SF romana postanu svakodnevica, poput mobilnih telefona pre tridesetak godina.

Još manji aparati, bazirani na nanotehnologiji, možda će pretraživati naše telo i rešavati medicinske probleme za koje danas morate da se prijavite na listu čekanja. Grupa terenskih dronova biće u stanju da, koristeći „inteligenciju" povorke mrava, ruševine koje su posledica neke prirodne katastrofe, autonomno obiđu u potrazi za preživelima. Nažalost, nema sumnje da će i ponašanje rojeva koji (pametno) napadaju pronaći svoju primenu u vojnim sistemima.

Pomalo paradoksalno, krug bezbednosti ovde se (možda?) zatvara. Fizička bezbednost, koja odavno ne predstavlja fokus informacije bezbednosti, možda će postati primarna u decenijama koje dolaze. Trenutno zvuči smešno obuka na temu „Kako se odbraniti od pogrešno podešenog roja mikrodronova", uz glavni savet: „Ne gledajte ih u oči (kameru) i nosite zaštitni plašt!", ali smejali smo se i obukama koje su nas učile da ne treba uplaćivati novac „nigerijskom princu" da bismo mu pomogli da „oslobodi zarobljene milione dolara".

Ma koliko budućnost izgledala svetlo ili tamno, iskustvo nas uči da ljudska vrsta ipak ima ugrađene razne mehanizme opstanka, što pruža nadu da ćemo i ovaj tehnološki stepenik iskoristiti na bolji način. Ipak, bezbednost je jedna od osnovnih ljudskih potreba, pa je pitanje vremena kada ćemo „ukrotiti" AI sisteme tako da nam budu isključivo na korist, a ne na štetu. Do tog zamišljenog trenutka, iskoristite priliku da uskočite u voz koji je već krenuo!

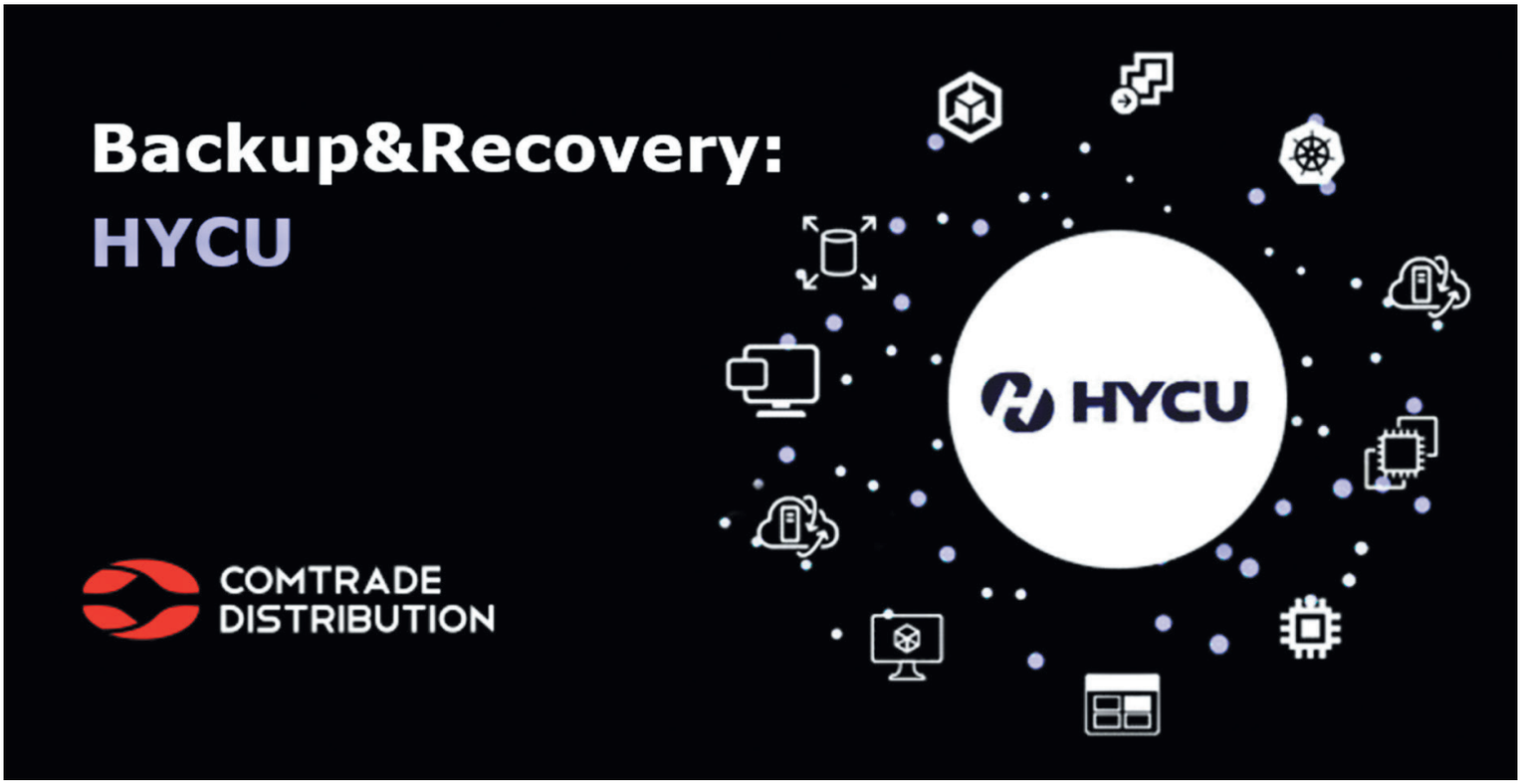
HYCU – novo ime u Comtrade Distribution portfoliju

U periodu sazrevanja svako od nas je pre ili kasnije imao dilemu u kom pravcu da se razvija, za koje oblasti da se opredeli, tj. kojim putem da krene. Slobodno možemo da kažemo da i oni koji ne analiziraju, već se lako prepuste nekom toku, ali i oni koji detaljno prolaze kroz svaki segment problema imaju jednu zajedničku osobinu – za siguran ili pravi put potreban je kontinuitet

Miodrag Nikolić i Aleksandar Gagović, Comtrade Distribution

Ukoliko se kontinuitet definiše kao preduslov za pravi put ka željenom, onda bi analogija u svetu *data* centar infrastrukture svakako bila sigurnost koja se ostvaruje kroz fenomen bekapa podataka. Dakle, stvorila bi se jednakost: kontinuitet = bekap. Ako ovu jednakost posmatramo iz ugla sistem integratora koji se brine da se poslovanje korisnika obavlja neometano, potrebno je naći takvo rešenje koje će biti dostupno, sigurno, prijemčivo i lako za upotrebu.

Sve opisane karakteristike rešenja sistem integratorima može da pruži neko ko ima pravilan uvid u tržište i ko posluje u skladu sa aktuelnim dešavanjima i trendovima. Ta uloga namenjena je distributeru koji je, pored osnovnih osobina, sposoban da



pruži i neke dodatne. S obzirom na to da distributer praktično predstavlja sponu između proizvođača i sistem integratora, jedan od dodatnih zadataka je i pravilan odabir rešenja koje će predstavljati ključ za stvaranje kontinuiteta.

Pouzdan partner

Proizvođač, odnosno vendor koji može da zadovolji potrebe korisnika u pogledu kontinuiteta poslovanja svakako je **HYCU**. Ovaj proizvođač bekap rešenja empirijski je dokazao da se i vrlo kompleksni sistemi mogu ukrotiti i svesti na nivo jednostavnosti, a to pokazuju brojne uspešne instalacije kod različitih tipova korisnika. Osnovni proizvod ove kompanije je **HYCU Protégé**, platforma za zaštitu podataka koja za cilj ima da integriše različita mesta na kojima se skladište podaci: lokalno, u *cloud*-u i unutar SaaS aplikacija. Koristeći *HYCU Protégé*, korisnici mogu dobiti jednake nivoe zaštite podataka, bez obzira na to gde se podaci čuvaju i to kroz jedinstveni interfejs.

Poslednjih godina u svetu informacionih tehnologija desile su se određene promene koje su promenile svest profesionalaca i poimanje akronima IT. Negativnu stranu sveprisutnog napretka predstavljaju sajbernapadi koji onemogućavaju pristup podacima tokom određenog perioda. Stepen napada ne može se sa sigurnošću utvrditi, a oporavak može potrajati danima ili nedeljama. Sajbernapadi imaju trenutni uticaj na poslovanje, ali mogu imati i trajni uticaj na reputaciju kompanije ukoliko oporavak traje duže od očekivanog.

Ransomware napadi dešavaju se svakih 11 sekundi, a samo u prvoj polovini 2022. bilo je 236 miliona napada. Prema HYCU izveštaju o spremnosti za *ransomware* napad, 63 odsto organizacija povećava ulaganja za otkrivanje, prevenciju i oporavak, a ujedno i shvataju da je bekap jedino rešenje da bi zaštitili svoje podatke od tih napada. Koliko god da su prevencija i otkrivanje važni u borbi protiv *ransomware*-a, organizacije će biti spremne za neizbežan napad samo kada mogu brzo da povrate podatke iz bekapa – za nekoliko minuta, a ne nedelja.

Spremna rešenja

Comtrade Distribution u svom portfoliju korisnicima nudi sledeća rešenja: **HYCU Protégé for Private Cloud & Data Centers:** *Backup and recovery for Nutanix and VMware*; **HYCU Protégé for M365:** *Backup and Archiving for Office 365* i **HYCU Protégé for Google Cloud, Azure and AWS:** *Data Protection, Data Migration and DR*. HYCU rešenja su namenski napravljena za svaki zaštićeni izvor bekapa i omogućavaju korisnicima da zaštite podatke koji se nalaze u okviru infrastrukturnih platformi, aplikacija i baza podataka. Ipak, to im takođe daje slobodu da migriraju svoje podatke na različite platforme ili da implementiraju isplativ oporavak od katastrofe.

Koristeći HYCU Protégé, korisnici mogu dobiti jednake nivoe zaštite podataka, bez obzira na to gde se podaci čuvaju i to kroz jedinstveni interfejs

Kao zvanični ekskluzivni distributer HYCU proizvoda na području Srbije, Crne Gore, Bosne i Hercegovine, Albanije i Severne Makedonije, **Comtrade Distribution** pruža rešenja koja pomažu korisnicima da oporave svoje podatke uz minimalan uticaj na poslovanje.

Za dodatne informacije, posetite *hycu.com* ili kontaktirajte *Comtrade Distribution*, ovlašćenog ekskluzivnog HYCU distributera na mejl:

hycu.distribution@comtrade.com.

Ransomware pošast: kako da organizacije sačuvaju svoje podatke

Ransomware napadi pune naslovne strane već nekoliko godina. U potrazi za profitom, napadači ciljaju gotovo sve tipove organizacija, od javnih preko zdravstvenih i obrazovnih institucija do pružalaca usluga i industrijskih preduzeća, utičući na skoro svaki aspekt života

Dragan Davidović, direktor kompanije Kaspersky za istočnu Evropu

Sajberkriminalci koji stoje u pozadini ovih napada još uvek uspevaju da smisle nove, sofisticirane i razrađene tehnike ili čak repliciraju pristupe karakteristične za neke od trenutno neaktivnih grupa koje su smatrane vrhunskim igračima.

Nedavno istraživanje kompanije *Kaspersky* potvrdilo je da se u prethodnoj godini više od 40 odsto kompanija suočilo s najmanje jednim *ransomware* napadom. Direktan finansijski trošak oporavka od ovih napada je, za male i srednje kompanije, u proseku iznosio 6000 evra, dok je oko 91.500 evra prosečan trošak za oporavak velikih kompanija.

Napadi ne prestaju

U prethodnoj godini, *Kaspersky* rešenja su detektovala i sprečila više od 74,2 miliona pokušaja *ransomware* napada, što je povećanje od 20 odsto u odnosu na 2021, kada je detektovano 61,7 miliona ovakvih napada. *Ransomware* napadi su najčešće ciljali javni sektor i vladine organizacije (19,39 odsto slučajeva), finansijski sektor (18,37 odsto) i industriju (17,35 odsto), za kojima slede sektor telekomunikacija (9,18 odsto) i IT (9,18 odsto). Iako je duži niz godina region jugoistočne Evrope bio donekle van fokusa organizovanih grupa koje koriste ovaj tip napada, on postaje sve prisutnija ozbiljna pretnja. Posebno privlačne su državne institucije i lokalne samouprave, kao i finansijski i telekomunikacioni sektor - dovoljno je da se podsetimo slučajeva koji su na određeno vreme paralisali rad pojedinih javnih institucija u Severnoj Makedoniji, Crnoj Gori i Srbiji.

Eksperti kompanije *Kaspersky* su otkrili da je u gotovo 43 odsto slučajeva *ransomware* napad otpočeo eksploatacijom aplikacija name-

njenih javnom korišćenju. Pored ovoga, najčešći vektor preko kojeg je *ransomware* našao svoj put do podataka kompanije su podaci vezani za prethodno kompromitovane korisničke naloge (u 24 odsto slučajeva) kao i zlonamerne *e-mail* poruke (u 12 odsto slučajeva). Primarni cilj napadača često nije bio samo iznuda ili šifrovanje podataka, već krađa ličnih podataka, intelektualne svojine i drugih osetljivih informacija.

Preventiva i lečenje

Ove brojke otkrivaju da su *ransomware* napadi i dalje rasprostranjeni i da mogu pogoditi bilo koju kompaniju u bilo kom trenutku. Da bi se efikasno zaštitile od ovog tipa napada, kompanije bi trebalo da slede sledeće savete:

- Uvek ažuriraju softver na svim uređajima koji imaju pristup kompanijskoj infrastrukturi, kako bi sprečili napadače da iskoriste ranjivosti i infiltriraju se u mrežu.

- Fokusiraju svoju strategiju odbrane na otkrivanje lateralnih pomeranja i eksfiltraciju podataka na Internet. Posebno treba obratiti pažnju na odlazni saobraćaj da bi se otkrile veze sajberkriminalaca s kompanijskom mrežom. Rezervne kopije podataka treba držati van mreže kako uljezi ne bi mogli da ih menjaju. Pri tome, važno je osigurati da tim rezervnim kopijama može brzo da se pristupi kada je to potrebno ili u hitnim slučajevima.

- *Ransomware* zaštita mora biti obezbeđena za sve *endpoint* uređaje. *Kasperski Anti-Ransomware Tool for Business* i u besplatnoj verziji štiti računare i servere od *ransomware*-a i drugih vrsta malvera, sprečava korišćenje eksploita i kompatibilna je s svim već instaliranim bezbednosnim rešenjima.

- Instaliranjem anti-APT i EDR rešenja, organizacije stiču mogućnosti za napredno otkrivanje i definisanje pretnji, istragu i blagovremeno otklanjanje incidenata. SOC tim organizacije mora redovno unapređivati svoje veštine kroz profesionalnu obuku. Sve gore navedeno je dostupno u okviru *Kaspersky Expert Security Framework* seta.

- SOC tim organizacije mora imati pristup najnovijim obaveštajnim podacima o pretnjama (TI). *Kaspersky Threat Intelligence Portal* je jedinstvena tačka pristupa za ove izveštaje, pružajući podatke o sajbernapadima i uvide koje je prikupljao naš tim duže od 20 godina. Da bi pomogao preduzećima da postave efikasnu odbranu u ovim turbulentnim vremenima, *Kaspersky* omogućuje pristup nezavisnim, kontinuirano ažuriranim informacijama sa globalnih izvora o tekućim sajbernapadima i pretnjama i bez naknade.

Kaspersky.rs

Sprečite sajberpretnje da ih ne biste lečili

Svetska privreda je usled sajbernapada u 2021. izgubila šest biliona dolara, a predviđanja su da će nas 2025. propusti u bezbednosnim merama koštati 10 biliona dolara, objavio je nedavno CB Insights. Gotovo dvostruko...

Jasno je da u toj ogromnoj sumi najveće gubitke beleži poslovni sektor. Razloge za ovakvo povećanje sajberpretnji i napada treba pre svega tražiti u opštem trendu u poslednjih nekoliko godina, kada organizacije ubrzano digitalizuju svoje procese, prelaze u *cloud* i održavaju rad zaposlenih na daljinu.

Isto tako, mnoge kompanije se suočavaju s velikim izazovom pronalaženja i privlačenja stručnjaka za sajberbezbednost, budući da je i na globalnom nivou manjak talenata u toj oblasti. Time se dodatno povećava rizik za kompanije da pretrpe potencijalno veliku poslovnu štetu, i stoga su prinuđene da izvan svoje organizacije potraže rešenje za podršku u domenu sajberbezbednosti, gde je prevencija od ključnog značaja.

Centar za bezbednost

Sajberpretnje su uveliko naša realnost, sve su sofisticiranije, dok su tehnike napada sve složenije i zato je adekvatna odbrana korporativnih digitalnih podataka od ključnog značaja. Te pretnje nemaju neki utvrđeni raspored, mogu se desiti u bilo kom trenutku, pri čemu tradicionalni sistemi zaštite (*firewall*, *endpoint*) nisu dovoljni. Zato je važan stalan uvid u dešavanje unutar mreže - 24/7, što omogućava predviđanje svakog potencijalnog napada, adekvatno vreme za reagovanje i kontrolu u svakom momentu.

U tom kontekstu, značajan iskorak u poboljšanju sajberbezbednosti predstavljaju bezbednosno operativni centri (*Security Operations Center* - SOC), koji zapravo čine vrhunska tehnološka rešenja i stručni timovi posvećeni praćenju događaja u sistemu neke kompanije u svakom trenutku, 365 dana u godini. Njihov prevashodni zadatak je da pravovremeno i adekvatno reaguju, čim se identifikuje neka sumnjiva aktivnost u sistemu.

Tri nivoa rešenja

Jedno takvo rešenje dostupno je poslovnim korisnicima u Srbiji, kao rezultat partnerske saradnje kompanija *Telekom Srbija* i PULSEC, u okviru koje se nalazi najveći bezbednosno-operativni centar na ovim prostorima - PULSOC. Zahvaljujući sinergiji njihovih ekspertiza, poslovnim korisnicima je ponuđen premijum servis - bezbednosno-operativni centar (SOC), koji čine tri paketa usluga za konstantnu podršku i nadzor podataka i IT sistema. Pored monitoringa i detekcije potencijalnih pretnji, ovaj servis je u stanju da odgovori na

potencijalne incidente (*Incident Response*) i pronalaženje prikrivenih pretnji (*Threat Hunting*), tako što se analizira svaka anomalija u sistemu i otklanjaju njeni uzroci.

Poslovnim korisnicima je tako na raspolaganju pouzdan sistem koji kontinuirano prati ponašanje u mreži, korišćenjem naprednih alata i tehnika za otkrivanje neobičnog ponašanja i identifikovanje potencijalnih pretnji, nakon čega se donose procene i upravlja definisanim pravilima, rangiraju upozorenja i analiziraju incidenti. Na taj način, omogućeno je pravovremeno reagovanje, budući da se ranjivi i ugroženi delovi u sistemima korisnika otkrivaju na vreme.

Bezbednosna premijum usluga

Ovaj sistem je zasnovan na *Next Generation SIEM* (*Security information and event management*) rešenju - IBM *QRadar* platformi i njenim naprednim funkcionalnostima, koje čine integrisanu celinu i omogućavaju centralizovani uvid u stanje IT bezbednosti informacionog sistema. Isto tako, njime se obezbeđuje međusobno povezivanje događaja sa svih krajnjih tačaka, 360° pogled na incidente, njihova analiza i dublje istraživanje. Zato su SIEM rešenja od ključnog značaja za organizaciju koja želi potpunu vidljivost i kontrolu nad onim što se dešava u njihovoj mreži u realnom vremenu. Dodamo li tome stručni tim analitičara koji nudi *mts* SOC servis, dobijamo premijum uslugu koja korisnicima istovremeno pruža podršku u tehnologiji i vrhunskoj ekspertizi, a iznad svega sigurnost jer su njihovi podaci bezbedni.

Mts.rs

SOC PREMA VAŠIM POTREBAMA

Odabirom SOC servisa, vaša organizacija dobija pristup naprednim tehnologijama i proverenoj ekspertizi PULSOC inženjera sajberbezbednosti. Na raspolaganju su vam tri opcije:

Osnovni SOC paket, koji uključuje monitoring i detekciju, kao i reagovanje na incidente tokom radnih dana (po modelu osam sati, pet radnih dana).

Premium SOC paket, koji uključuje 24-časovni monitoring i detekciju, reagovanje na incidente (24x7) i uslugu *Threat Hunting*-a (8x5).

Custom SOC paket, gde je, osim usluga monitoringa i detekcije, reagovanja na incidente, moguće odabrati i usluge *Internal Vulnerability Assessment*, *Penetration Testing*, *Virtual* CISO ili *Security Awareness* program.

Bezbednosni izazovi QR koda

Iako je uveden u upotrebu još pre 30 godina, QR kod tek u poslednje 2-3 godine doživljava naglu ekspanziju u pogledu broja onih koji ga upotrebljavaju. Velika popularnost donela je i niz bezbednosnih problema sa kojima se nije lako nositi

Dušan Katilović

QR kodovi su 2D slike („dvodimenzionalni bar-kodovi“) odštampane na nekom fizičkom predmetu ili prikazane na ekranu uređaja, koje se mogu skenirati kamerom mobilnog telefona. Pomoću specijalizovanog softvera, *Web browser* prevodi zapis unutar koda na konkretnu *Web* adresu (URL), čime se internet saobraćaj koji potiče od osobe koja je kod skenirala usmerava na određen naziv domena, tj. sajt.

QR slikom direktno na Web

Ove sve prisutnije „sličice“ su danas najčešći način povezivanja virtuelnog sveta interneta sa fizičkim svetom. Više skorašnjih fenomena je zaslužno za njihovu sve veću popularnost, ali se dva izdvajaju – promovisanje beskontaktnih plaćanja i evolucija pametnih mobilnih uređaja među kojima praktično svaki ima kvalitetnu i brzu kameru, kao i odgovarajući softver za skeniranje QR kodova.

Ovu evoluciju svesrdno su prihvatili bankari i marketari koji QR kod vide kao najlakši oblik obavljanja plaćanja, odnosno instant povezivanja korisnika sa brendom koji se prezentuje.

Brendovi i kompanije uočljivo prikazuju QR kodove na pakovanjima proizvoda, bilbordima, u časopisima... na bilo kom fizičkom medijumu gde će QR privući pažnju. Njega susrećemo i na TV ekranima, displejima elektronskih uređaja, reklamama na stajalištima javnog prevoza, ali i na nalepnicama na najrazličitijim površinama koje su izraz „gerila marketinga“.

QR sigurnosna pretnja

Upravo zbog svoje raširenosti, QR kodovi su novi „favorit“ među sajber-kriminalcima koji ih koriste u svrhe širenja malicioznog softvera i krađe osetljivih podataka. Za razliku od običnih, jednodimenzionalnih kodova, QR kodovi su nosioci dugačkih nizova podataka, što ih čini savršenim za čuvanje URL adresa. Svako ko skenira kod biva direktno odveden na neku *Web* lokaciju, bez potrebe da ručno unosi adresu sajta.

Postoje dve glavne vrste eksploatacije QR kodova koje koriste sajber-kriminalci. Prvi je *phishing* napad zasnovan na QR kodu, koji se ponekad naziva i *quishing*. Ova vrsta napada koristi kod da bi se žrtva namamila na *Web* stranicu koju su hakeri napravili sa namerom da ukradu žrtvin novac, lične podatke ili druge osetljive informacije.

Drugi tip napada na QR kod se naziva *QRLjacking*, gde hakeri koriste kod za plasiranje zlonamernog softvera na uređaj žrtve. Napadač navede korisnika da skenira QR kod, čime uređaj korisnika usmerava na zlonamernu URL adresu na kojoj se uređaj inficira malverom.

QR kodovima se mogu pokrenuti i druge vrste akcija na nivou uređaja. Na primer, haker može da koristi kod kako bi automatski uputio telefonski poziv ili poslao tekstualnu poruku sa uređaja koji je skenirao kod. Hakeri su u stanju čak i da kodovima iniciraju plaćanje sa zaraženog uređaja korisnika ili da ga silom povežu na određenu *Wi-Fi* mrežu.

Zaštita kompanija i brendova

Zaštita od ovih novostvorenih onlajn bezbednosnih pretnji zasniva se na brendiranju QR kodova, pravilnom izboru domena (sajta) na koji oni

PRODOR QR KODOVA ŠIROM SVETA

U obimnoj studiji sprovedenoj u SAD, UK, Japanu, Nemačkoj, Kini i Francuskoj, bezbednosna kompanija *Ivanti* publikovala je sledeće nalaze:

- 47% ispitanika zna da QR kod može da odvede na *Web* adresu.
- 37% je svesno da se kodom može preuzeti aplikacija
- 22% njih zna da se putem QR koda može otkriti nečija fizička lokacija
- 39% anketiranih veruje da ume da prepozna zlonamerni QR kod
- 49% je iznelo da nema ili ne zna da li ima instalirano sigurnosno rešenje na svom mobilnom uređaju.

vode, izboru dobrog provajdera za njihovo generisanje, kao i na stalnu edukaciju korisnika i kupaca.

Brendirajte svoje QR kodove Verovatno ste primetili da QR kod ne mora da bude u potpunosti crno-beli i da može da sadrži određene boje, oblike i slike koje dodatno privlače pažnju. Zato QR kod predstavlja novi predmet brendiranja. Kada budete dizajnirali sopstveni QR kod, obavezno integrišite boje i logotipe povezane sa vašim brendom.

Nadalje, trebalo bi da prilagodite internet link unutar koda tako da on vodi na osnovni domen vaše kompanije. Iako se pojedini marketari odlučuju da za individualne kampanje pokrenu zaseban („jednokratan“) sajt na koji QR kod upućuje, daleko bezbednije rešenje je da osoba koja skenira kod prvo bude upućena na stranicu na matičnom sajtu posvećenu kampanji, odakle će potom moći da pređe na drugi kompanijski sajt, ukoliko on postoji. Brendiranjem koda i pravilnim linkovanjem umanjuje se rizik od lansiranja uspešnog *phishing* napada.

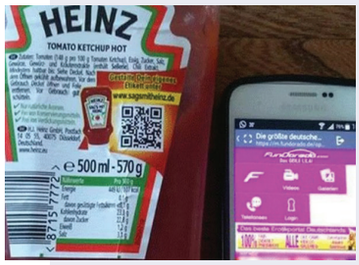
Izaberite bezbednu QR kod platformu Adekvatna platforma za generisanje QR kodova je ona koja primenjuje dobre bezbednosne prakse i time štiti svoje klijente. Poštovanjem bezbednosnih standarda, QR kod provajderi sprečavaju mogućnost da loši akteri hakuju vaš poslovni nalog, pristupe vašem QR kodu i preusmere ga na svoj domen.

Edukujte svoju publiku

Ne propuštajte nijednu priliku da svoje korisnike podsetite da QR kod može predstavljati bezbednosni rizik, da na svojim uređajima treba da imaju instaliran ažuriran bezbednosni softver protiv preuzimanja kontrole nad njim od strane hakera. Takođe se preporučuje da se posetioci na vaše onlajn platforme loguju pomoću višefaktorske autentikacije umesto klasične lozinke, s obzirom na to da je veliki deo napada putem QR koda usmeren upravo ka krađi lozinki.

domen.rs

BOCA KEČAPA EKSPLICITNOG SADRŽAJA



Poznati slučaj sa QR kodom desio se 2015, a žrtva je bio proizvođač kečapa *Heinz.* Kod koji se nalazio na pakovanju proizvoda služio je da korisnike odvede na mikrosajt kompanije posvećen jednokratnoj, vremenski ograničenoj promociji. Grubim propustom, registracija naziva domena tog mikrosajta je istekla i nije obnovljena od strane Heinza, a šansu da registruje nanovo slobodan naziv domena iskoristili su vlasnici jednog sajta za odrasle što je uzrokovalo to da svi oni koji su od jednog momenta skenirali QR kod sa boce kečapa budu usmereni na sajt sa eksplicitnim sadržajem. Zato treba biti vrlo oprezan sa „domenima za jednokratnu upotrebu“ i registrovati ih na duži period od trajanja same kampanje ili projekta, da ne bi dolazilo do ovakvih situacija.

GERILA TEHNIKE NAPADA

U prošlosti, omiljen alat kriminalaca za *phishing* napad je bila e-pošta. Problem (za kriminalce) u vezi sa ovim pristupom je u tome što postoje znakovi da e-pošta nije legitimna, kao što su pogrešno napisane reči ili linkovi koji dižu alarm. Sem toga, *phishing* poruka često od žrtve traži da preduzme radnje koje izgledaju potpuno nelogično – da plati robu koju nije naručila ili pošalje novac nepoznatoj osobi ili firmi.

Čak i kada je *phishing* poruka uverljiva, uvek postoje pokazatelji da je nelegitimna. Svako ko zna šta da traži i ko odvoji vreme da pažljivo prouči takvu poruku neće imati problema da utvrdi da je poruka lažna. Ovo nije slučaj sa QR kodovima. Kada osoba skenira QR kod, nema načina da unapred sazna da li je kod legitiman i to je ono što napade zasnovane na QR kodu čini efikasnim. Kako žrtva ne može da proceni validnost koda, veća je verovatnoća da će uspeti napad zasnovan na QR kodu nego napad zasnovan na e-pošti.

Još jedan problem sa ovim kodovima je taj što hakeri mogu lako zameniti legitimni kod zlonamernim. Na primer, ako restoran sačini kod koji posetioca povezuje sa njegovim menijem, napadač bi mogao da napravi nalepnice koje sadrže zlonamerni QR kod i zatim da ih prelepi preko originalnih.

Zabeleženi su slučajevi gde se prevarni QR kodovi postavljaju na javna mesta, za slučaj da je neko dovoljno radoznao da skenira kod.

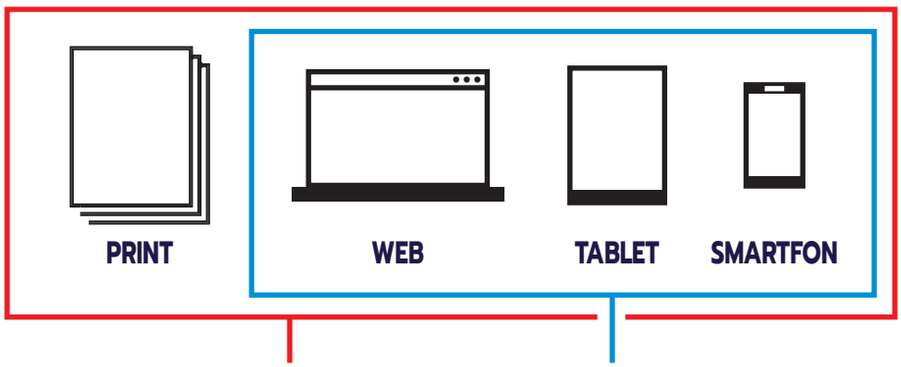
NAJPOPULARNIJI QR KOD PROVAJDERI

Monika Adarsh, stručnjak za QR kodove, tvrdi da su najbolje platforme za generisanje QR kodova u 2023. godini:

- Beaconstac’s QR Code solution (9.8/10)
- QR-Code-generator.com (8.2/10)
- QR Code Monkey (8/10)
- Scanova (7.4/10)
- the-qrcode-generator (6/10)
- GoQR (5/10)
- Shopify’s QR Code generator (5/10)
- QR Stuff (4/10)

NAJBOLJA SELEKCIJA INFORMACIJA O TEHNOLOGIJI I BIZNISU

Pretplatite se na print izdanje magazina PC Press po ceni od **3.990** dinara za godinu dana i dobićete na poklon **godišnju pretplatu na digitalno izdanje**



Print izdanje
Godišnja pretplata
3.990 dinara

Digitalno izdanje
Godišnja pretplata
1.990 dinara

Pozovite **Nevenku** na broj **(011) 276 55 33** ili posetite **prodavnica.pcpress.rs**