PRIVATNOST I SIGURNOST PODATAKA U HT CLOUDU

Siječanj 2015.

ŽIVJETI ZAJEDNO

SADRŽAJ

SAŽETAK

Ako vas brine sigurnost vaših podataka u cloudu, pročitajte ovaj dokument pa saznajte koje su osnovne komponente sigurnih sustava te provjerite je li i vaš informacijski sustav čuvan na svim potrebnim razinama.

Ako ste odabrali Hrvatski Telekom za svog pružatelja ICT usluga, uvjereni smo da ste napravili odličan izbor jer HT-u je sigurnost implementirana duboko u organizacijsku strukturu, a sigurnost informacija vidimo kao svoju stratešku prednost.

Stalna edukacija zaposlenika i podizanje razine svijesti o važnosti sigurnosti i zaštite podataka, pažljivo planiranje i projektiranje svih sustava, vrhunski alati za borbu protiv prijetnji s interneta — i još mnogo toga — pružaju garanciju da su vaši podaci u sigurnim rukama.

Naš je posao sačuvati vaše podatke od vanjskih prijetnji s interneta, ali i od svih eventualnih neželjenih događaja unutar vaših kompanija.

UVOD

Svaki odnos zasniva se na povjerenju. To je posebno izraženo u poslovnim odnosima, a izuzetno je važno u internetskom poslovanju. Gubitak važnih ili curenje osjetljivih podataka može ugroziti opstanak tvrtke na tržištu. Stoga je nužno da **IT sustavi** budu uvijek **dostupni, a podaci sigurni.** Također, niti koncept računalstva u oblaku ne bi mogao uspjeti bez povjerenja u čitav sustav.
Ako se neki pružatelj cloud usluge pokaže nepouzdanim, on sigurno neće opstati na tržištu.

Kada se računalstvo u oblaku razmatra kao opcija za upravljanje vašim podacima, među ključnim su pitanjima sigurnost i privatnost podataka. Upravo se te značajke u istraživanjima tržišta spominju kao glavni razlozi za i protiv računalstva u oblaku. Primjetno je da računalni stručnjaci koji prate tehnološke trendove među glavnim osobinama računalstva u oblaku navode sigurnost i privatnost. Također, u promotivnim materijalima često možete pročitati da su vaši podaci u cloudu zaštićeni i sigurni. Ovaj dokument pokazat će zašto vjerujemo da su vaši podaci kod nas sigurniji nego u lokalnom IT okruženju te na koji način HT čuva vaše podatke i upravlja sigurnosnim mehanizmima i procedurama.

VLASNIŠTVO I SMJEŠTAJ INFRASTRUKTURE

Kada govorimo o informacijskim sustavima i podatkovnim centrima, možemo razmatrati tri varijante smještanja opreme i vlasništva nad opremom:

- vlastita oprema u vlastitim prostorijama (engl. on-premise)
- vlastita oprema u tuđim prostorijama (kolokacija, engl. collocation)
- tuđa oprema u tuđim prostorima (najam infrastrukture, platforme ili softvera).

Tradicionalan pristup upravljanju informacijskim sustavima pretpostavljao je nabavku potrebne opreme i njezin smještaj unutar prostorija tvrtke. U prošlosti telekomunikacijska infrastruktura nije niti omogućavala drugačije načine rada ako govorimo o transakcijskim sustavima koji se koriste u svakodnevnom poslovanju. Računala i računalni resursi unajmljivali su se za povremene veće obrade podataka još od njihova nastanka, kada su računalni resursi bili vrlo oskudni i rijetki.

Kada opremu držimo u vlastitim prostorijama, potrebno je osigurati adekvatan prostor, električnu energiju iz mreže te pričuvne izvore, hlađenje, mrežne resurse, kao i ljude — zaštitare koji će se brinuti o fizičkoj sigurnosti sustava, IT stručnjake koji će održavati opremu u uporabnom stanju te svoje ili vanjske certificirane stručnjake za održavanje građevine i elektrostrojarskih resursa. Ovi troškovi rastu proporcionalno potrebnoj razini **sigurnosti i dostupnosti sustava.** Ako se želi postići **neprekidan rad,** potrebno je imati **redundantne sustave** tako da rezervni sustav uvijek može preuzeti funkciju u potpunosti i bez prekida (npr. ako dođe do kvara ili je potrebno servisirati neki sustav). Kontrola pristupa također je jedan od neophodnih uvjeta za sigurnost sustava.

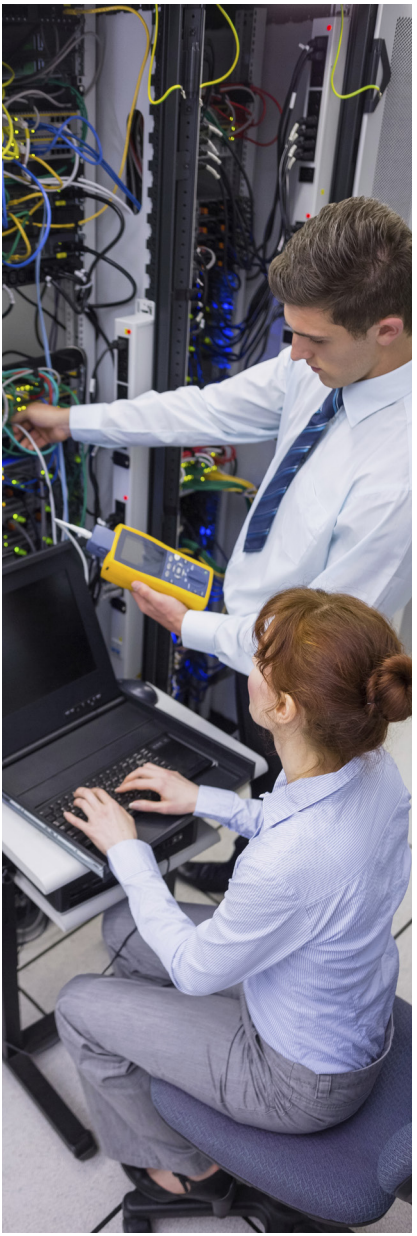
Upravo je manjak resursa za takve velike investicijske projekte, uz povećanje propusnosti interneta, iznjedrio novu uslugu — smještaj opreme u **dobro opremljenim i čuvanim podatkovnim centrima** sa širokopojasnim pristupom internetu. Ta usluga poznata je pod nazivom kolokacija. Ona podrazumijeva da svoja računala smjestite u podatkovni centar pružatelja usluga, koji jamči iznimnu fizičku sigurnost, neprekidno napajanje, kontinuirano odvođenje topline, adekvatne mrežne resurse i sve ostale uvjete potrebne za siguran, stabilan i neprekidan rad. Izgradnja adekvatne infrastrukture za smještaj opreme — od prostorija preko električnih instalacija do mrežne opreme — velika je kapitalna investicija, pa si samo najveće organizacije mogu priuštiti takva ulaganja. Kod kolokacije pružatelj usluge dužan je osigurati sve navedene resurse, a korisnik usluge mora se brinuti za sigurnost IT sustava: šifriranje podataka, obranu od internetskih napada, sigurnost aplikacija i održavanje vlastitog hardvera.

Kada govorimo o računalstvu u oblaku, usluge možemo podijeliti na tri osnovna tipa — infrastrukturu (engl. infrastructure as a service ili IaaS), platformu (engl. platform as a service ili PaaS) i softver (engl. software as a service ili SaaS).

Za razliku od kolokacije, gdje unajmljujete prostor, a hardver je vaš, pri najmu infrastrukture vaši se sustavi nalaze na hardveru pružatelja usluge. No ovdje korisnik zadržava kontrolu nad operacijskim sustavima i konfiguracijom poslužitelja, što mu daje značajnu kontrolu nad sigurnošću sustava, ali i odgovornost za pravilno rukovanje sustavom.

U slučaju najma platforme, što pojednostavljeno možemo prikazati kao razvojno okruženje u oblaku, pružatelj usluge brine se za hardver, ali i operacijski sustav na kojem se temelji aplikativna platforma. Tako se dodatna kontrola prebacuje na pružatelja usluge. Također, pružatelj usluge odgovoran je za sve aspekte raspoloživosti sustava, odnosno skaliranje resursa prema potrebama vaših aplikacija.

Prilikom korištenja **softvera kao usluge** gotovo sva briga o **sigurnosti** odgovornost je pružatelja usluge, a **korisnik brine** samo **o pravima pristupa** te o softveru koji se koristi. Logično je pretpostaviti da onaj koji brine o sigurnosti za velik broj korisnika, sustava i aplikacija ima razvijene sofisticirane sigurnosne sustave te su vaši podaci u njegovoj infrastrukturi sigurniji nego kod vas.



Prikaz 1 Odgovornost za sigurnost sustava ovisno o modelu korištenja IT-a

	MODEL KORIŠTENJA IT-A	FIZIČKA SIGURNOST I DOSTUPNOST	ODRŽAVANJE HARDVERA, VIRTUALIZACIJA	OPERACIJSKI SUSTAVI I PLATFORMA	SIGURNOST APLIKACIJA	UPRAVLJANJE IDENTITETIMA KORISNIKA
Vlastita oprema	U vašim prostorima					
	Kolokacija					
Cloud usluge	Infrastruktura (IaaS)					
	Platforma (PaaS)					
	Softver (SaaS)					

Odgovornost pružatelja usluge

Odgovornost korisnika

Pružatelj usluga mora osigurati sve da onemogući pristup neovlaštenim osobama, bilo fizički ili putem mreže, ali korisnik određuje pravila pristupa te politike za upravljanje podacima i čuvanje njihove sigurnosti i privatnosti budući da je korisnik uvijek vlasnik podataka.

Na **Prikazu 1**. primjetno je da je obim posla korisnika oko održavanja željene razine sigurnosti i dostupnosti najviši u slučaju kad svoju opremu drži u svojim prostorima, a najniži kada koristi softver kao uslugu. Slično je i s troškovima održavanja, posebno onim koji se odnose na plaće, edukacije i troškove vezane uz zapošljavanje IT stručnjaka. Primijetite kako i u slučaju korištenja softvera kao usluge trebate nekoga tko će se baviti upravljanjem pravima pristupa (obično i nabavom softvera) te obavljati administrativne zadatke kao što je promjena naprednih postavki softvera koji koristite. Dakle, ako imate bilo kakvih specifičnosti i **želite upravljati svojim informacijskim sustavima,** zaboravite na ideju da vam ne trebaju informatičari, razlika je samo u broju i razini stručnosti ljudi koje trebate. Ako unajmljujete platformu, smisleno je imati nekoga tko će razvijati aplikacije na toj platformi, a već kod najma infrastrukture nije na odmet imati sistemskog administratora koji će upravljati virtualnim poslužiteljima. Čim iz oblaka izađete u kolokaciju, potrebni su vam i hardverski stručnjaci, dok ćete za opremanje podatkovnog centra i održavanje njegove sigurnosti trebati i električare i zaštitare.

EKONOMIJA RAZMJERA I UTJECAJ NA SIGURNOST

Kada opremate podatkovni centar prema najvišim standardima, to je značajna investicija. Stoga je ekonomija razmjera ključ efikasnosti podatkovnih centara. Što je podatkovni centar veći, jedinični su **troškovi** po virtualnom poslužitelju **niži,** a isto vrijedi i za ostale resurse. Zato veliki podatkovni centri mogu ponuditi resurse po povoljnijim uvjetima nego mali.

Kako bi se postigla troškovna efikasnost, manji podatkovni centri često rade kompromise na području sigurnosti i dostupnosti, pa ne osiguravaju fizičku zaštitu cijelo vrijeme, nemaju razvijene sustave za kontrolu pristupa opremi, nemaju adekvatne sustave za održavanje povoljnih atmosferskih uvjeta, redudantne privode električne energije, pristup internetu i slično.

Kako bi korisnici znali o kakvom se podatkovnom centru radi, koristi se kategorizacija koju je donio Američki nacionalni standardizacijski institut (ANSI — American National Standards Institute).

ČETIRI RAZINE POUZDANOSTI PODATKOVNIH CENTARA

ANSI je podatkovne centre podijelio u četiri razine (engl. tier). Osim kao specifikacija, ovaj se standard koristi i kako bi se korisniku moglo brzo opisati o kakvom je podatkovnom centru riječ.

Tier 1 u osnovi predstavlja tradicionalnu serversku sobu bez ikakve redundancije. Očekivana dostupnost sustava je 99,671 % vremena.

Tier 2 koncipiran je tako da sustav od više elemenata ima instaliran po jedan pričuvni uređaj. Sve su instalirane komponente u količini N+1. Očekivana dostupnost je 99,741 % vremena.

Tier 3 koncipiran je tako da sva IT oprema ima dvostruko neovisno napajanje i hlađenje u konceptu 2N. Bazični energetski sustavi (transformatori i agregati) koncipirani su u redundanciji N+1. Očekivana dostupnost je 99,982 % vremena.

Tier 4 koncipiran je tako da svi dijelovi sustava moraju biti otporni na greške, odnosno svaki sustav ima instaliran kompletan i potpuno neovisan redundantni sustav. Oba sustava imaju još dodatno instaliran po jedan pričuvni uređaj. Sve su instalirane komponente u količini 2(N+1). Očekivana dostupnost je 99,995 % vremena.

HT-ovi podatkovni centri odgovaraju Tieru 3 s elementima Tiera 4, što znači da im je jamčena dostupnost 99,982 % vremena. Korištenjem **HT Cloud usluga** imat ćete na raspolaganju **visoko dostupan i skalabilan sustav,** uz smanjenje kompleksnosti vašeg IT okruženja i ukupnih troškova. Uz to, mijenja se i odnos prema informacijskoj tehnologiji — u tradicionalnom pristupu s vlastitim sustavom kupujete IT po visokoj cijeni koju potom morate opravdati korištenjem tehnologije, a u HT Cloudu platit ćete samo ono što koristite.

SIGURNOST OBLAKA

Kada govorimo o sigurnosti u cloudu, nekoliko je područja sigurnosti na koja treba obratiti pozornost kako bi sustav bio siguran.

> To su upravljanje identitetima, fizička sigurnost, sigurnost osoblja, dostupnost i neprekidnost poslovanja, sigurnost aplikacija, privatnost i pravna pitanja. Sustav je onoliko siguran koliko je sigurna najslabija karika u ovom lancu.

Ova se područja često isprepliću, pa im je nužno sustavno pristupiti. Primjetno je da se osim tehničkih i stručnih pitanja izdvajaju dva pitanja organizacijske razine, a to su zaposlenici i zakonodavni okvir. Stoga je nužno da čitava organizacija bude svjesna važnosti sigurnosnog sustava i da postupa u skladu s pravilnicima, politikama i, na kraju krajeva, u skladu sa zakonom.

Dobar primjer sustavnog pristupa pitanjima sigurnosti i privatnosti predstavlja Hrvatski Telekom. Za ostvarivanje sigurnosnih ciljeva te adekvatnu implementaciju sigurnosnih mjera T-HT Grupa utvrdila je proces upravljanja sigurnošću koji se temelji na **standardu ISO IEC 27001,** kao i odgovarajuću organizaciju upravljanja sigurnošću. Ona uključuje i obvezujuće sigurnosne zahtjeve postavljene ugovornim partnerima HT Grupe.

Sigurnosne mjere temelje se na ciljevima zaštite te uključuju elemente ljudskih resursa, organizacijske i tehničke elemente. Pristup upravljanju sigurnošću i učinkovitost mjera sigurnosti kontroliraju se periodički i u posebnim prilikama od strane nezavisnih osoba. Mjere se dodatno razvijaju na prikladan način. Na prikazu 2 je prikazana struktura ključnih dokumenata kojima se definira pristup kompanije pitanju sigurnosti.

Cilj ovakve strukture nije zaštititi samo informacijske sustave — upravo suprotno, **prvi je cilj zaštititi ljude,** odnosno njihov integritet, a tek potom opremu i podatke.

Krovni dokumenti u strukturi su Opća politika sigurnosti i Kodeks za zaštitu privatnosti. Hijerarhijski, ispod njih su politike za pojedina područja (Sigurnost informacija i zaštita osobnih podataka, IT/NT sigurnost, Upravljanje kontinuitetom poslovanja i situacijama, Fizička sigurnost, Sigurnost ljudskih resursa, Zaštite osoba i događanja, Istraga). Na sljedećoj nižoj razini nalaze se sigurnosni zahtjevi kojima se detaljnije propisuju minimalne sigurnosne mjere za uža područja i tehnologije. Tu su i pravilnici, upute i druga tehnička dokumentacija. Sve vrste dokumenata moraju biti u skladu s onima koje su u strukturi iznad njih. Ovakav pristup, struktura politika i pravila prema kojima se treba ponašati rezultat su dugogodišnjeg rada i unapređenja na organizacijskoj razini DT grupe i predstavljaju značajnu organizacijsku intelektualnu imovinu. Uz to, i u politikama je istaknuto da obzirom na vodeću ulogu HT Grupe u području informacija i komunikacija, informacije i podaci predstavljaju temeljnu imovinu HT-a te se stoga upravljanju istima posvećuje posebna pozornost. Međutim, upravo provedba tih pravila i politika donosi pravu dodanu vrijednost kroz sigurne sustave i povjerenje korisnika. U tome pomažu mnogobrojni alati i propisani procesi, a za našu temu najvažniji je **PSA** (engl. privacy & security assessment) **proces,** koji definira kako se rješava

Prikaz 2 Struktura politika sigurnosti u Hrvatskom Telekomu (Izvor: Opća Politika sigurnosti, Glasnik HT d.d., 2011)

problematika sigurnosti i privatnosti u projektima, s ciljem pravodobnog prepoznavanja i ispunjavanja mjera zaštite osobnih podataka te kibernetske i podatkovne sigurnosti.

Tri su glavne faze unutar PSA procesa — kategorizacija projekta, definiranje primjenjivih zahtjeva i testiranje. Unutar kategorizacije projekta određuje se njegova relevantnost u pogledu sigurnosti i privatnosti te se u skladu s tim definira potreban angažman. Kriteriji za kategorizaciju sastoje se od procjene osjetljivosti podataka, potrebnog zahvata na sustavima te poslovne važnosti. Potom, u skladu s kategorizacijom, slijedi određivanje zahtjeva u okviru dizajniranja sustava, implementacija zahtjeva u fazi izvedbe te konačna provjera i testiranje je li sve učinjeno prema specifikacijama. Na taj se način pristupa svim projektima, od izgradnje infrastrukture do izrade aplikacija. Još neka načela također pomažu u osiguravanju sustava.

PRAVNA PITANJA

Prvo načelo HT-ove Opće sigurnosne politike jest zakonito poslovanje. Tu se HT obvezuje poštovati sve zakonske propise vezane uz sigurnost. Osim zaštite radnika, zaštite od požara i drugih elementarnih nepogoda, za informacijske sustave to znači i obvezu čuvanja zapisa za potrebe istraga. Ovo se odnosi i na zapise u poslovnim informacijskim sustavima i na zapise niže razine, o prijavama u sustav, o IP adresama s kojih se pristupalo i slično.

Budući da promjene zakona mogu utjecati na ono što treba zapisivati i koliko dugo to čuvati, potrebno je napraviti prilagodbe koje propisuje zakon. One su ponekad neočekivani trošak koji ne možete izbjeći jer ste dužni prilagoditi svoje sustave zakonu, a u slučaju upravljanja vlastitom IT infrastrukturom ove prilagodbe predstavljaju vaš dodatni trošak.

Osim brige za **fizičku sigurnost,** HT se obvezao i **prilagođavati informacijske sustave zakonskim promjenama.** To znači da su korisnici HT-ovih Cloud usluga osigurani od dodatnih troškova prilagodbe sustava.

O izboru usluge ovisit će razina vaše odgovornosti. Ako koristite infrastrukturu u oblaku, sami ćete biti odgovorni za prilagodbu aplikacija, a ako koristite softver, nećete uopće imati brigu o troškovima prilagodbe uzrokovanim promjenama zakona.

I na taj način HT pokazuje kako mu sigurnost predstavlja mnogo više od pukog ispunjavanja zakonskih obveza — sigurnost je definirana kao **strateška prednost Hrvatskog Telekoma**.

SIGURNOST OSOBLJA

Danas daleko najveći broj sigurnosnih incidenata uzrokuju ljudi, a ne tehnika. Naljepnice s pristupnim podacima na monitoru, otključana vrata koja bi trebala biti zaključana, iskopčan kabel prilikom čišćenja samo su neki od banalnih uzroka potencijalnih incidenata bez zle namjere. Uzrok tomu može biti neznanje ili nepažnja.

HT veliku pozornost pridaje **edukaciji svih zaposlenika** i podizanju svijesti o važnosti svih elemenata sigurnosti sustava. Stoga su svi ranije navedeni dokumenti iz strukture politika sigurnosti prilog svim ugovorima o radu za stalne i privremene zaposlenike Hrvatskog Telekoma. Također, provode se provjere poznavanja sigurnosnih pravila i politika te svijesti zaposlenika o važnosti zaštite podataka. Sustavan pristup pokazuje se uspješnim, jer je vidljiv stalan napredak u rezultatima ovih provjera.

Kada razmišljate o sigurnosti, razmišljajte i o tome tko ima pristup vašem sustavu kao administrator. Osim što mora biti stručna za posao koji obavlja (na primjer za servisiranje opreme ili administraciju operacijskog sustava), ta osoba mora biti i osoba od povjerenja, upoznata sa svim pravilima i propisima, moralna i etična. Uz to, potrebna je kontrola pristupa koja može pokazati tko je, kada i gdje bio u prostorima koji su strogo čuvani i tko je, kada i gdje pristupio sustavu putem mreže te se ovdje isprepliće više područja sigurnosti (sigurnost osoblja, fizička sigurnost i IT/NT sigurnost). U većim organizacijama kao što je HT to se naziva sigurnost ljudskih resursa. Politika sigurnosti u području ljudskih resursa definira kako upravljati zaposlenicima od njihove prijave na posao do prekida radnog odnosa. Ona se temelji i poziva na standard ISO 27001 koji propisuje stvari poput procesa provjere kandidata za radna mjesta koja su klasificirana kao sigurnosno osjetljiva ili obveza čuvanja osjetljivih podataka nakon prekida radnog donosa.

I ovdje se primjenjuju načela da zaposlenici smiju imati pristup samo onim prostorima, sustavima i podacima koji su im neophodni za obavljanje zadataka, da se podaci ne smiju koristiti na način da budu vidljivi drugim osobama kojima ne trebaju te se obvezuju da će provoditi druge mjere iz strukture sigurnosnih politika. Posebno se naglašava i važnost **stalne edukacije zaposlenika.** Na ovaj način HT štiti podatke od ljudske greške. Neovisno je li riječ o podacima korisnika ili o vlastitim podacima.

ZAPOSLENIK BANKE OTUĐIO PODATKE

Da niti najsigurniji IT sustavi nisu 100 % sigurni ako ljudi s pristupom podacima nisu od povjerenja govori nam sljedeća priča. HSBC, jedna od vodećih svjetskih institucija u bankarskom i financijskom sektoru, priznao je krađu osobnih podataka svojih 24 000 klijenata početkom 2010. godine.

Herve Falciani, bivši zaposlenik IT odjela HSBC-a, pobjegao je iz Švicarske u Francusku s podacima o klijentima pouzdane financijske institucije Swiss bank. Francuske vlasti zaplijenile su podatke i predale ih švicarskom tužilaštvu. U vrijeme objave čak 15 000 tih računa bilo je još aktivno, a 9 000 ih je zatvoreno. Prema izvješću, HSBC postao je svjestan veličine propusta tek kad su francuske vlasti podatke predale Švicarskoj. Švicarski regulator financijskog i bankarskog sektora pokrenuo je postupak vezan uz ovaj sigurnosni incident, a HSBC izjavio je da su u sigurnosni sustav uložili dodatnih 100 milijuna švicarskih franaka od kada su saznali za slučaj krajem 2008. godine.

Ovakva ulaganja u sigurnost informacijskih sustava premašuju mogućnosti većine organizacija u Hrvatskoj, a uz to ne jamče stopostotnu sigurnost ako se ne pridaje dovoljna pažnja zaposlenicima, kao i dostupnosti podataka onima kojima ti podaci nisu potrebni za obavljanje svakodnevnih zadataka. Izvornu vijest možete pronaći na http://news.bbc.co.uk/2/hi/business/8562381.stm

FIZIČKA I INFRASTRUKTURNA SIGURNOST

Osnova sigurnosti informacijskih sustava jest njihov smještaj u sigurnim, čuvanim i održavanim prostorijama kako bi se osigurao njihov nesmetan rad. Prema Politici fizičke sigurnosti HT-a, koja uvažava europske i ISO standarde, fizička sigurnost obuhvaća zaštitu imovine i opreme te sukladno tome uključuje:

- zaštitu građevina, građevinskih dijelova i prostora, sredstava i opreme koji su u njima smješteni, i/ili poslovnih procesa koji se u njima provode od neovlaštenog pristupa, štete i drugih oštećenja uslijed napada ili elementarnih nepogoda i sila prirode, uključujući i zaštitu od požara,
- zaštitu sklopovlja logičke korporativne infrastrukture, kao što su npr. mreže (u daljnjem tekstu: „imovina“), od kvara i ostalih oštećenja,
- zaštitu opreme (naročito pokretne radne opreme i drugih materijalnih sredstava,

kao i informacija koje su u njima sadržane) od neovlaštenog pristupa, štete, krađe i gubitka.

Kada govorimo o sigurnosti građevina, treba početi od **okružja objekta.** Od posebne su važnosti rizici — mogućnost požara, uključivo i eksplozije, što bi moglo ugroziti podatkovni centar, na primjer ako je u blizini benzinska postaja ili prometnica kojom se prevoze opasni tereti. Također, važno je procijeniti opasnost od više sile i otpornost objekta na poplavu, potres i slične nepogode.

Potom je važno osigurati **perimetar.** Ograda i druge barijere, alarmi, videonadzor, protuprovalna zaštita, sustav kontrole pristupa — sve to potrebno je implementirati kako bi se osigurala zaštita od neovlaštenog pristupa.

Tu je i tjelesna zaštita, odnosno **zaštitarska služba** koja nadzire lokaciju i provodi mjere zaštite. Pravila pristupa i dozvole moraju biti jasno definirana, kao i pravila postupanja u slučaju alarma, dolaska gostiju i drugih događanja. Na kraju treba osigurati svaku pojedinu prostoriju sukladno sigurnosnim zahtjevima, i od neovlaštenog pristupa i od požara, poplave i drugih mogućih nepogoda. Uz to prostori moraju ispunjavati i druge uvjete, isprepletene s područjem koje se bavi **dostupnošću sustava,** kao što je **neprekidno napajanje i kontinuirano odvođenje topline.**
Svi HT-ovi objekti u kojima su smješteni podatkovni centri udovoljavaju svim ovim uvjetima. Objekti su otporni na velika opterećenja i utjecaj voda te imaju osiguranu stalnu fizičku zaštitu, pri čemu se misli na zaštitarsku službu potpomognutu sustavom za kontrolu pristupa i upozoravajućim sustavima. Osim standardnih mjera kao što su protupožarna vrata, zaštita od požara uključuje i vatrodojavni sustav te automatsko gašenje požara plinom.

Nadzor infrastrukturnih elemenata obavlja se 24 sata dnevno. Sustavi za napajanje koncipirani su na način da postoje dva ili tri HEP-ova visokonaponska energetska voda te najmanje jedan redundantni transformator. Također je osigurano rezervno napajanje putem stacionarnih dizelskih elektroagregata, od kojih je jedan redundantan, a zalihe energenata dostatne su za neovisan rad u trajanju od više dana. Budući da agregati kao izvor rezervnog napajanja nisu u mogućnosti osigurati potpunu besprekidnost napajanja, jer im je potrebno određeno vrijeme za startanje i preuzimanje opterećenja, u tu su svrhu instalirani sustavi koji u svojem sastavu imaju baterije. Postoje dva tipa sustava — sustavi za besprekidno napajanje izmjeničnim naponom (UPS sustavi) i sustavi za besprekidno napajanje istosmjernim naponom (DC sustavi). Sustavi su koncipirani u 2N redundanciji, tako da postoje dvije neovisne paralelne grane, pri čemu svaka može preuzeti cjelokupno opterećenje u slučaju kvara u drugoj grani napajanja.

Autonomija sustava osigurana je korištenjem više paralelnih baterija, za minimalno 45 minuta rada pri punom opterećenju. U sistemskim salama instalirani su rashladni ormari koji istovremeno odvode toplinsku energiju iz prostora putem tekućeg i putem plinovitog medija — ovisno o opterećenju i vanjskim temperaturnim uvjetima. Također se koristi „free cooling“, način rada u hladnijem periodu godine, kako bi se smanjili troškovi energije i time postigla povoljnija cijena za korisnika. Radi dodatnog racionaliziranja potrošnje u sistemskim salama instalirani su ormari (rackovi) za smještaj opreme, tako da su odvojene hladne od toplih zona. Temperatura zraka u hladnoj zoni, odnosno na mjestu usisa zraka u server održava se na 24 ± 20 °C, a vlažnost zraka u serverskim salama je 50 ± 20 %. Svaka sistemska sala ima ugrađen sustav za dovod svježeg kondicioniranog zraka. Prilikom nabave infrastrukturnih sustava i elemenata primarni uvjet bila je energetska učinkovitost i održivost sustava u cjelini, kao i svakog njegova dijela zasebno. Sve su to proizvodi renomiranih proizvođača, s višegodišnjom zajamčenom proizvodnjom i isporukom rezervnih dijelova.

Zahvaljujući adekvatnoj opremljenosti i procedurama, **HT-ovi podatkovni centri imaju certifikat ISO/IEC 27001.** Posjedovanje ovog certifikata omogućuje korisnicima da sami lakše ishode njima potrebne sigurnosne certifikate (samo korištenje sustava po standardu ISO 27001 ne znači da ste spremni za certifikaciju).

DOSTUPNOST SUSTAVA

Dvije su razine mjera kojima se osigurava dostupnost i neprekidnost poslovanja. Prve su **infrastrukturne,** a druge su usmjerene **k redundanciji sustava, sigurnosnoj pohrani i procedurama za povratak sustava u stanje prije eventualne havarije.**

Računalstvo u oblaku (engl. Cloud computing) prema svojim glavnim odrednicama olakšava poslove kojima se osigurava dostupnost sustava i njegovo održavanje. To su grid (engl. grid computing), virtualizacija (engl. virtualisation), računalstvo kao usluga (engl. utility computing) i autonomno računalstvo (engl. autonomic computing). Svi ovi koncepti, a posebno autonomno računalstvo, osiguravaju veću dostupnost sustava u odnosu na klasične poslužitelje. HT se dodatno osigurao nabavivši svu opremu od renomiranih proizvođača, s garancijom i osiguranom podrškom, čime je **pouzdanost sustava podignuta na višu stepenicu.**

Za primjer, ispred HT Oblaka postavljen je vatrozid Palo Alto. On može filtrirati promet po tipu, a upozorava na gotovo sve prijetnje, od virusa nadalje. To je **vodeći svjetski vatrozid,** i performansama i cijenom, koji daje dodatnu sigurnosnu vrijednost sustavima u HT Cloudu. To je vrlo važno jer najveći broj prijetnji i napada dolazi upravo s interneta, a razmišljajući o cloudu, korisnici najčešće vide upravo neovlašteni pristup putem interneta kao glavnu prijetnju.

HAKTIVIZAM

Prošle je godine američka centralna banka Federal Reserves objavila da je kontaktirala s korisnicima čiji su podaci kompromitirani, a potom je haktivistička zajednica Anonymous objavila pristupne podatke 4 000 izvršnih direktora američkih banaka.

Dokument koji je objavio Anonymous sadržavao je imena i radna mjesta, telefonske brojeve te zapise koji su izgledali kao pristupni podaci nekoliko desetaka zaposlenika banaka, kredit-nih udruga i drugih pozajmljivača. Središnja banka objavila je da lozinke nisu ugrožene te da je objavljeni dokument zapravo popis kontakata za slučaj elementarnih nepogoda. Glasnogovornik Središnje banke izjavio je da je sustav kompromitiran putem ranjivosti za koju je odgovoran izvođač web-stranica. Ranjivost je pokrpana čim se za nju saznalo, a incident nije utjecao na kritične sustave banke.

Anonymous je povezao ove napade s prosvjedima koji su uslijedili nakon smrti Aarona Swartza , računalnog programera, pisca i borca za slobodu Interneta.

Ovo nije jedini prijavljeni incident vezan uz Federal Reserves. 2010. godine Malezijac je proglašen krivim za ubacivanje malicioznog koda u mrežu centralne banke putem jedne od regionalnih banaka.

Ova priča pokazuje da i najsigurniji sustavi mogu pokleknuti pod silinom napada. Stoga je važno posvetiti iznimnu pozornost zaštiti od prijetnji s interneta. Iako je dobra vijest da se Hrvatska, za sad, nalazi izvan središta interesa raznih hakerskih skupina koje predstavljaju realnu prijetnju.

Izvornu vijest možete pronaći na http://www.bbc.com/news/technology-21351081

SIGURNOST APLIKACIJA

Sigurnosne propuste potrebno je otkriti čim prije **u ranijim fazama razvoja sustava,** jer je tad njihovo otklanjanje jeftinije, a sustav sigurniji. Ako se greške pronađu u produkcijskom sustavu, odnosno onom koji rabi prave podatke, riječ je o pravom sigurnosnom riziku. Zbog toga se prilikom razvoja aplikacija u koje je uključen HT primjenjuje ranije opisani **PSA** proces, unutar kojeg se aplikacija kategorizira, postavljaju se sigurnosni zahtjevi i provjerava jesu li ti zahtjevi ispunjeni.

Kategorizacija se temelji na pitanjima kao što su osjetljivost podataka, vrijednost projekta i broj korisnika aplikacije. Rezultat odgovara na pitanje na koji će se način odsjek za sigurnost uključiti u razvoj. Ako projekt nema utjecaja na sigurnost sustava, odjel za sigurnost nije potreban. Ako je riječ o standardnom projektu, sigurnosna pitanja kao što su postavljanje zahtjeva i provjera može pokriti tehnički odjel. Ako je riječ o kritičnom sustavu,

potrebno je uključiti ljude iz odsjeka za sigurnost.
Ovisno o kategorizaciji, vrsti aplikacije i funkcionalnostima propisuju se određeni tehnički zahtjevi koje aplikacija mora ispuniti. Izjava o usklađenosti (engl. statement of compliance ili SOC) još je jedan alat koji pomaže u procesu. Ovom izjavom dobavljač sustava potvrđuje sukladnost sa sigurnosnim zahtjevima. Na temelju izjave lako je pratiti zahtjeve i provjeriti je li aplikacija s njima usklađena. Također, lakše je pratiti ključne zahtjeve koji moraju biti ispunjeni.

Osim sustavnog pristupa sigurnosti i privatnosti prilikom razvoja aplikacija, redovno se obavljaju i testiranja sigurnosti od hakerskih napada. Budući da ovaj posao traži stručne ljude i dosta njihova vremena, za penetracijska testiranja angažira se sigurnosni centar DT grupe ili lokalni dobavljači.

DT-ov sigurnosni centar koji radi za cijelu grupu pruža i usluge testiranja izvornog koda, što je još jedna dodana vrijednost koju HT nudi razvojnim inženjerima. Kod se testira alatima koji upozoravaju na eventualne sigurnosne propuste.

PRIVATNOST

Zaštita osobnih podataka, tj. zaštita privatnosti, postiže se primjenom niza **organizacijskih, procesnih i tehničkih mjera zaštite.** Tako već prethodno spomenuti PSA proces omogućuje pravovremeno i sustavno osiguravanje zahtjeva zaštite privatnosti u svim projektima, odnosno uslugama i proizvodima koji su relevantni s aspekta zaštite privatnosti. PSA proces uključuje kategorizaciju, tj. procjenu relevantnosti projekta (usluge, proizvoda) s obzirom na potrebu zaštite privatnosti, postavljanje obveznih zahtjeva za zaštitu privatnosti — sve u ranim fazama projekta — te po završetku provjeru je li udovoljeno traženim zahtjevima po pitanju zaštite privatnosti. Na taj se način osigurava da konačan produkt projekta bude siguran prema pravilima zaštite privatnosti.

Osim toga, HT primjenjuje visoke standarde zaštite privatnosti podataka i povrh važećih propisa, a u skladu sa standardima DT Grupe. Zaposlenici HT-a kontinuirano se educiraju o zaštiti privatnosti, uključujući obvezne edukacije. Također, redovno se provode i provjere usklađenosti poslovanja sa zahtjevima za zaštitu privatnosti. HT još od 2009. godine ima zasebnu organizacijsku jedinicu za zaštitu privatnosti, kojoj je na čelu Povjerenica za zaštitu osobnih podataka, a čija je osnovna zadaća osigurati odgovarajuću zaštitu privatnosti u kompaniji. Pri tome aktivno surađuju s nadležnim tijelom za zaštitu osobnih podataka (Agencija za zaštitu osobnih podataka — AZOP) te se vode najboljom praksom.

Nadalje, zaštita privatnosti osigurava se i izborom tzv. podizvođača, koji moraju ispuniti visoke standarde zaštite privatnosti HT-a, što se osigurava i sklapanjem vrlo strogih ugovora upravo po pitanju zaštite privatnosti. U slučaju povrede osobnih podataka, HT o tome pravovremeno obavještava nadležna tijela (AZOP i HAKOM), odnosno korisnika. HT osobitu pažnju pridaje obvezama vezanim uz iznošenje podataka u druge zemlje. U pravilu riječ je o državama članicama EU-a za koje je na europskoj i hrvatskoj razini utvrđeno da osiguravaju zaštitu osobnih podataka. No u situacijama kada je potrebno podatke iznositi i u neke druge zemlje, koje a priori ne osiguravaju odgovarajuću zaštitu, tada se ona osigu-rava upravo kroz vrlo stroge ugovore s tzv. podizvođačima u tim zemljama te je naravno, u pravilu, podložna odobrenju AZOP-a.

Od niza načela kojima se HT ravna pri zaštiti privatnosti korisnika valja istaknuti sljedeća: **načelo „potrebno je znati“** znači da HT obrađuje isključivo one osobne podatke koji su mu nužni u legitimnu svrhu. **Načelo „određene svrhe“** znači da se osobni podaci koriste za svrhu radi koje su prikupljeni, a bilo koja druga uporaba u pravilu zahtijeva izričitu privolu osobe na koju se podaci odnose. **„Određeno vrijeme čuvanja“** znači da se podaci čuvaju onoliko koliko je to nužno ili zakonski obvezno, a u protivnom se anonimiziraju ili brišu. **„Pristup ovlaštenim osobama“** znači da pristup podacima nemaju svi zaposlenici HT-a, već isključivo ovlaštene osobe te je takav pristup kontroliran itd. Ako imate potrebu sigurnog čuvanja većih količina podataka unutar Hrvatske, a nemate adekvatan diskovni prostor, spremanje unutar HT Clouda optimalan je izbor.

UPRAVLJANJE IDENTITETIMA

Međutim, koliko god vaš pružatelj usluga osigurao informacijski sustav, njegova **sigurnost** u rukama je **krajnjih korisnika.** Uzalud svi napori oko protuprovalne i antivirusne zaštite, implementacije autonomnog računalstva i redundantne instalacije ako korisnik ne čuva vlastite pristupne podatke. Kriva osoba s pristupnim podacima i pravima na pristup sustavu može učiniti mnogo štete. Stoga je nužno stalno ukazivati na važnost čuvanja pristupnih podataka, educirati zaposlenike i upravljati identitetima odnosno pravima pristupa pojedinim podsustavima i podacima. Kako je upravljanje krajnjim korisnicima usluge uvijek obveza korisnika usluge, morate osigurati da se osobama pravovremeno ukidaju prava na podatke koji im više nisu potrebni te da se na pravovaljan zahtjev odmah omogući pristup potrebnim podacima u sustavu. Razne su mogućnosti povećanja sigurnosti na ovom području. Uobičajeno je inzistirati na dužim i složenim lozinkama. Moguće je izdavanje jednokratnih lozinki uz pomoć uređaja i uz unos osobnog

identifikacijskog broja (PIN) ili slično. Neovisno o tome, zajedničko svim sustavima jest da ne smijete dijeliti vlastite pristupne podatke niti ih ostavljati dostupnima drugim osobama. Krađe identiteta moguće su i na brojne druge načine, od obične prevare i krađe do sofisticiranih načina putem malicioznog softvera. Uz to, u slučaju hibridnih rješenja u specifičnim slučajevima moguće je koristiti i direktorije osoba u privatnom dijelu za prijavu u javnom dijelu clouda.

HT omogućuje pristup svim administracijskim resursima s istim pristupnim podacima (engl. single sign on ili SSO), kako korisnici ne bi morali za svaku uslugu pamtiti različit skup korisničkog imena i lozinke.

Budući da neovlaštenim pristupom s valjanim pristupnim podacima druge osobe mogu načiniti znatne štete neovisno o tome koliko je brige i pažnje posvećeno sigurnosti cjelokupnog sustava, nužno je da korisnik educira svoje zaposlenike o važnosti upravljanja korisnicima i važnosti čuvanja tajnosti osobnih pristupnih podataka. Isto vrijedi i za privatnost i sigurnost podataka.

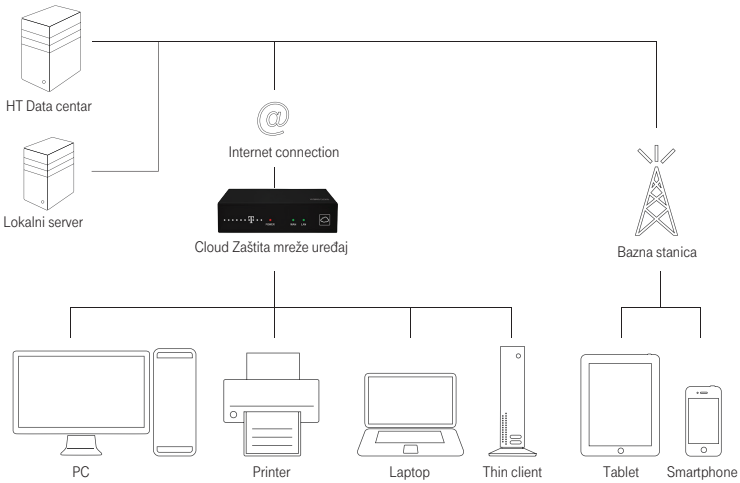
Čuvanje osjetljivih podatka ne odnosi se samo na informacijske sustave, već i na ispisane podatke, njihov prikaz na ekranu dok su neovlaštene osobe u blizini i slično.

SIGURNOST KOMUNIKACIJSKOG KANALA

Ništa što se nalazi na internetu nije apsolutno sigurno. Toga mora biti svjestan svaki korisnik. Čak i ako je sigurnost u podatkovnom centru izvedena na najbolji mogući način te korisnik pazi na pristupne podatke, komunikacijski kanal od korisničkog uređaja do poslužitelja može biti kompromitiran. Stoga je pametno šifrirati promet koji razmjenjujete putem interneta kako nitko kome nije namijenjen ne bi mogao pročitati sadržaj. To je moguće napraviti na više razina i na više načina.

Osim virtualnih privatnih mreža (VPN) i tuneliranja putem softvera namijenjenog za sigurnu komunikaciju internetom, moguće je koristiti uslugu Cloud Zaštita mreže s uređajem koji nudi mnogo više od sigurne komunikacije unutar vaše mreže. Uređaj usluge Cloud Zaštita mreže može se spojiti na internet putem fiksne i mobilne mreže, pa tako u slučaju ispada fiksne mreže možete nastaviti s radom putem mobilne mreže, i to bez zastoja u radu. Uređaj omogućuje određivanje

propusnosti internetske veze te jednostavno dodavanje lokacija u Cloud. Aplikacija kojom upravljate uređajem omogućuje i postavljanje ograničenja u internetskom prometu. Istovremeno pruža i antivirusnu zaštitu i vatrozid, a koristiti je možete i bez fizičkog uređaja.



SIGURNOST MOBILNIH UREĐAJA

Ako su vaši sustavi u oblaku, jedna od prednosti je što su vaši podaci dostupni a svakog mjesta i svakog uređaja koji ima pristup internetu. U praksi to znači da se sve veći broj osjetljivih podataka koristi i nalazi na mobilnim uređajima poput pametnih telefona i tableta. Kako većina aplikacija omogućuje pristup sustavima tako da se samo prilikom prvog korištenja unose pristupni podaci (korisničko ime i lozinka), dok svako sljedeće korištenje ne zahtijeva ponovan unos, gubitak mobilnog uređaja predstavlja ozbiljan sigurnosni rizik.

Uz to što vam omogućuje nadzor nad svim mobilnim uređajima unutar vaše organizacije i uprav-ljanje softverom na njima, usluga Cloud Upravljanje mobilnim uređajima povećava i sigurnost vašeg mobilnog uređaja. Usluga omogućuje kontrolu pristupa nesigurnim mrežama i aplikacijama, daljinsko zaklju-čavanje uređaja i brisanje podataka, čime se smanjuje rizik od gubitka ili curenja poda-taka prilikom gubitka ili krađe mobilnog uređaja. Aplikacija za upravljanje uslugom dostupna je na svakom uređaju koji ima pristup internetu, tako da

će administratori moći reagirati odmah po prijavi, čak i kada nisu na radnom mjestu.

ZAKLJUČAK

Ovisno o načinu korištenja cloud usluga, odgovornosti za sigurnost pojedinih dijelova sustava mogu biti na pružatelju usluge ili na korisniku. U svakom slučaju potrebno je educirati ljude o osnovama sigurnosnih mjera kroz pravilnike i procedure, jer samo **zajednički napori korisnika i pružatelja usluga mogu rezultirati sigurnim sustavom.**

HT kao pružatelj usluga već **godinama s** posebnom pozornošću **čuva podatke svojih korisnika** te svoju **ekspertizu** koristi i u pružanju **sigurnih Cloud usluga.** U svrhu štićenja informacija osmišljene su politike za pojedina sigurnosna područja, koje jamče sustavan pristup svim područjima te istovjetan pristup zaštiti podataka korisnika. Privatnost i sigurnost podataka smatramo našim posebnim odgovornostima, kojih smo svjesni svaki put kad pružamo uslugu svojim korisnicima te uvijek nastojimo postaviti nove i više standarde u ovom području. Odabirom HT Cloud usluga svoje podatke i svoje IT sustave dajete u sigurne ruke — profesionalcima koji imaju adekvatne resurse za efikasnu zaštitu od svakodnevnih prijetnji s interneta.

Razina IT znanja u vašoj organizaciji odredit će način konzumiranja ICT usluga što ih nudi HT. Najam infrastrukture u obliku proizvoda, kao što je Cloud Server ili Cloud Data Centar, koristit će tvrtke koje imaju IT odjele i adekvatna znanja za administriranje poslužiteljskih operacijskih sustava ili IT partnera za projektiranje, implementaciju, podešavanje i održavanje sustava.

Tvrtkama bez IT odjela namijenjene su aplikacije i softver kao što je Microsoft Office 365 ili Nadzor vozila. Gotovo rješenje za koje se administracija svodi na davanje prava pristupa korisnicima. Za to je obično potrebno elementarno informatičko znanje. Sve ostale odgovornosti oko IT sustava prepustit ćete stručnjacima Hrvatskog Telekoma, kojima je osigurana stalna edukacija i usavršavanje.

U svakom slučaju **HT će štititi vaše podatke** kao vlastite, **vrhunskom tehnologijom i educiranim stručnjacima.** Pri tom će uspostaviti potpunu sigurnost i privatnost podataka dajući pristup samo osobama koje imaju odgovarajuća prava. Korištenjem ovih usluga vaši sustavi dobit će zaštitu koja je većini cijenom nedostižna — i to po prihvatljivoj i predvidivoj cijeni, na načelu „plati koliko koristiš“.

Posjetite **https://ictmarketplace.hr** za više informacija o HT Cloud uslugama i proizvodima.

HRVATSKI	ENGLESKI
Pregledni dokument	White paper
Računalstvo u oblaku	Cloud Computing
Šifriranje	Encryption
Pristupni podaci	Credentials
Pružatelj usluga	Provider
U vašim prostorijama	On-premise
Kolokacija	Collocation
Virtualizacija	Virtualization
Maliciozni softver	Malware
Vatrozid	Firewall
Najam infrastrukture	Infrastructure as a service (IaaS)
Najam platforme	Platform as a service (PaaS)
Najam softvera	Softver as a service (SaaS)

InfoCumulus je neovisna savjetodavna tvrtka koja spajanjem tehnoloških i poslovnih znanja ostvaruje najbolje poslovne učinke za svoje klijente.