ISSN 2566-3690

www.bas.gov.ba

GLASNIK

INSTITUT ZA STANDARDIZACIJU BOSNE I HERCEGOVINE; GODINA XIII; BROJ 1, APRIL 2019

CYBER POVJERENJE

INSTITUT ZA STANDARDIZACIJU BOSNE I HERCEGOVINE
ИНСТИТУТ ЗА СТАНДАРДИЗАЦИЈУ БОСНЕ И ХЕРЦЕГОВИНЕ

www.bas.gov.ba

GLASNIK

INSTITUT ZA STANDARDIZACIJU BOSNE I HERCEGOVINE: GODINA XIII, BROJ 1, APRIL 2019

BAS

Glasnik
Instituta za standardizaciju BiH;
godina XIII, broj 1,
april 2019.
ISSN 2566-3690

Izdavač
Institut za standardizaciju
Bosne i Hercegovine
71123 Istočno Sarajevo,
Vojvode Radomira Putnika 34
telefon: +387 57 31 05 60;
fax: +387 57 31 05 75
e-mail: stand@bas.gov.ba;
www.bas.gov.ba

Glavni i odgovorni urednik
Aleksandar Cincar

Uređivački odbor
Borislav Kraljević, Goran Tešanović,
Dejana Bogdanović, Miljan Savić,
Biljana Maletić

Design/DTP
BAS

S A D R Ž A J

PET STVARI ZA KOJE NISTE ZNALI DA MOGU BITI HAKOVANE

Autor: Elizabeth Gasiorowski – Denis i Vivienne Rojas - ISOFocus #132

Uređaji koje svakodnevno koristimo sve su više povezani, što olakšava život ne samo nama već i hakerima. Da bismo se zaštitili od neželjenih upada, prvo moramo postati svjesni opasnosti koje sa sobom nosi umrežavanje uređaja.

Hakeri također napadaju djecu. Pitate se kako to haker može pronaći put do dječije sobe? Nažalost, svetinja dječije sobe je narušena ... od napadača koji vrebaju izvan vašeg doma. Poenta ove priče nije to da vaš bebi-monitor može biti hakovan. Poenta je da se to može desiti skoro svakom “povezanom” uređaju.

Kompanija Gartner, Inc. predviđa da će se do 2020. godine širom svijeta upotrebljavati 20,4 milijarde povezanih uređaja. Najveći dio korisnika povezanih uređaja odnosi se na potrošački segment i u 2017. godini iznosio je 5,2 milijarde jedinica, što predstavlja 63% ukupnog broja korištenih aplikacija. Mnoga domaćinstva su već opremljena sa više desetina povezanih uređaja u koje spadaju računari, mobilni telefoni i tableti, ali i mnogi tradicionalni kućanski proizvodi kao što su frižideri, televizori i sigurnosni sistemi.

Dok su provodili studiju o osjetljivosti IoT uređaja na hakovanje, istraživači na Univerzitetu Ben-Gurion u Beershebi, Izrael, došli su do zaključka da su mnogi proizvođači i vlasnici uređaja zapravo olakšali posao hakerima. Brojni proizvođači imaju iste lozinke za isti tip uređaja, a korisnici ih često i ne promijene. To znači da ako imate deset uređaja koji su povezani na mrežu i ako ste ostavili jedan bez nadzora, cijela vaša mreža je ugrožena. Zaista zastrašujuće.

Činjenica je da se sve što ima stabilnu Wi-Fi vezu može hakovati ili ga može kontrolisati “profesionalni” haker. Čak i kada nije direktno vezan za internet, uređaj može, na neki način ili u nekom obliku biti meta napada. Ovo obuhvata veoma širok spektar predmeta, pa pogledajmo pet stvari koje mogu biti hakovane!

Bebi-monitori i kamere

Šta je svrha bebi monitora: da nadgledaju malu djecu. Upravo zato ovaj uređaj predstavlja takvu prijetnju kada je hakovan i/ili eksploatisan. Bebe, pa čak i malu djecu, može sa velike udaljenosti posmatrati bilo ko ko uspije da preuzme kontrolu nad ovim uređajem.
Mnoge sigurnosne kamere se sada povezuju na internet da bismo omogućili ljudima da im pristupaju izvan kuće. Njujorška služba za zaštitu potrošača izdala je javno upozorenje o sigurnosti bebi-monitora nakon niza prijavljenih incidenata, gdje su se putem monitora čuli nepoznati glasovi.

Štampači i faksovi

U kućama ili kancelarijama štampači često imaju svoju internet vezu kako bi im se omogućila, često bežična, komunikacija sa drugim uređajima. Ovo veza za hakere predstavlja prvi korak koji im omogućava da daljinski pristupe vašoj mreži. Sve što treba da urade je da zaobiđu sigurnosne kontrole i upadnu u vaš štampač ili drugi uređaj koji je povezan s njim. Ranjivosti printera su veoma dobro dokumentovane, s tim da je jedan haker tvrdio da je „provalio“ u 150 000 štampača kako bi ukazao na njihovu nesigurnost.
Hakeri se također mogu infiltrirati u vašu mrežu jednostavnim slanjem faksa. S obzirom na to da je danas većina faksova integrisana u multifunkcionalnom štampaču, povezanom na Wi-Fi mrežu i telefonsku liniju, lako se mogu hakovati slanjem pažljivo dizajniranog slikovnog fajla koji sadrži zlonamjerni kod. Kada se ovaj skriveni kod konvertuje u podatke za prijenos unutar interne kompjuterske mreže, on može preuzeti kontrolu nad faksom, ukrasti lozinke i bankovne podatke i hakovati još više uređaja.

Dječije igračke

Da, taj slatki medo je pravi raj za hakere. Čini se da čim se bilo koji uređaj poveže sa internetom biva hakovan. To uključuje mnoge predmete i uređaje koje tradicionalno ne povezujemo sa ovom vrstom tehnologije... kao što su dječije igračke. Bilo koje igračke povezane sa internetom sa mikrofonima, kamerama ili praćenjem lokacije mogu ugroziti privatnost ili sigurnost djeteta. U pitanju bi mogla biti lutka koja govori ili tablet dizajniran za djecu. Maloprodavci su bili primorani da povuku veliki broj “povezanih” ili “inteligentnih” igračaka nakon što su otkrili sigurnosne kvarove u njihovim Bluetooth i Wi-Fi protokolima koji mogu dozvoliti strancu da razgovara sa djetetom ili da sluša razgovore. Kod svake od ovih igračaka Bluetooth veza nije bila zaštićena, što znači da napadaču nije bila potrebna lozinka, pin ili bilo koja vrsta autentifikacije da bi dobio pristup.

Pametni uređaji

Vaš frižider bi mogao biti vaš najgori neprijatelj kada je u pitanju sigurnost. Frižider koji vam omogućava da pošaljete listu za kupovinu direktno na vaš pametni telefon konfigurisan je tako da omogućava svakome da pronađe vašu Google prijavu za korisnika. Bilo koji uređaj ili aparat u vašoj kući koji je povezan može predstavljati ulaz u čitavu mrežu. Dakle, iako je zgodno da možete da kontrolišete temperaturu svoje kući dok ste vani - naprimjer, ako uključite grijanje kad krećete iz kancelarije - hakeri mogu kontrolisati vaš termostat i blokirati ga sve dok vlasnik ne plati otkupninu. Aparati za kafu su druga glavna meta cyber napada. Nedostatak u mobilnoj aplikaciji koja daljinski kontroliše vaš aparat za kafu može otvoriti vrata za kršenje prava vaše privatnosti ako hakeri ukradu vaše Wi-Fi lozinke i filtriraju podatke koji prolaze kroz vašu mrežu.

Pejsmejkeri i implantati

Hakiranje srca je moguće! Američka agencija za hranu i lijekove (FDA) je u 2017. godini opozvala 465 000 pejsmejkera iz straha da bi sigurnosni problemi mogli dovesti do toga da zlonamjerni hakeri mogu promijeniti ritam nečijeg srca - što može rezultirati smrću. A šta je sa dubokom stimulacijom mozga, gdje se mozak podvrgava elektroudarima radi kontrole epilepsije ili tremora kod Parkinsonove bolesti? Ova precizna kontrola mozga otvara hakerima mogućnost da naprave još veću štetu poput kontrolisanja inzulinskih pumpi ili srčanih implantata. Ciljani napadi na implantate u mozgu, ili “hakovanje mozga“, mogu izazvati oštećenje motoričke funkcije, promjenu kontrole impulsa, modifikaciju emocija ili afekata, indukciju boli i modulaciju sistema nagrađivanja. Dakle, postavlja se pitanje: Kada bežični moždani implantati postanu široko rasprostranjeni, kako omogućiti pristup mozgu doktorima, ali ne i cyber-kriminalcima?

Sačuvajte sigurnost

Postoji mnogo drugih naizgled nevjerovatnih načina na koje haker može pristupiti vašem sistemu. Čak i ako vam je glavni ulaz na internet dobro zaštićen, neko bi se mogao infiltrirati na mala vrata. Šta to znači za našu budućnost? Koliko trebamo biti zabrinuti ako imamo u vidu sve ove pametne proizvode priključene na internet? Odgovor je *veoma*. Ne moramo čekati do 2020. godine da bismo se uhvatili ukoštac sa ovim sigurnosnim propustima.

Zaštita našeg cyber prostora je prioritetnog značaja i neophodno joj je posvetiti neposrednu i stalnu pažnju. U velikom broju slučajeva, prave sigurnosne mjere mogu obeshrabriti hakere i zadržati oportuniste, a često su međunarodni standardi vaša prva linija odbrane. Standardi poput ISO/IEC 27001 i ISO/IEC 27002 daju zajednički jezik za rješavanje problema u vezi sa upravljanjem, rizicima i usaglašenošću koja se odnosi na sigurnost informacija, dok ISO/IEC 27031 i ISO/IEC 27035 pomažu organizacijama da efikasno odgovore, odbiju i oporave se od cyber napada. Također postoje mnogi drugi standardi koji definišu mehanizme enkripcije i potpisa koji se mogu integrisati u proizvode i aplikacije za zaštitu online transakcija, korištenje kreditnih kartica i pohranjenih podataka.
Standardi su dobri samo u onoj mjeri u kojoj se koriste. Sljedeći put kada kupite monitor za bebe ili bilo koji drugi umreženi uređaj, zapitajte se: Da li je proizvođač razmotrio mogućnost hakovanja? Da li je kompanija primijenila odgovarajuće međunarodne standarde? Ako je odgovor na oba pitanja ne, onda bi možda trebalo dvaput razmisliti o kupovini.

POTRAGA ZA CYBER POVJERENJEM

Autor: Robert Bartram - ISOFocus #132

S tehnologijom koja je sve sofisticiranija i koja nudi bolje mogućnosti ali i nove ranjivosti i prijetnje, različite vrste organizacije su u velikoj mjeri podložne zlonamjernim napadima ili kršenjima podataka. Upravljanje rizikom je, prema tome, jednako vitalno u *cyber* prostoru kao i u fizičkom svijetu. Koji su to *cyber* rizici? Kako ih međunarodni standardi mogu ublažiti? I da li je zaista jedini odgovor još sofisticiranija tehnologija?

Definicija iz Oxford English Dictionary definitivno je dovoljno jasna: „rizik", kaže se u rječniku, „jeste situacija koja uključuje izloženost opasnosti". Postizanje rezultata zahtijeva preuzimanje rizika, ali se rizikom mora upravljati kako bi se postigli pozitivni ishodi i izbjegle negativne posljedice.

Izbjegavanje rizika je nemoguće. Rizike je neophodno preuzeti i to je neizbježan i neophodan dio našeg života, kako lično tako i profesionalno. Zaista, ako bi bilo koja kompanija ili organizacija iz bilo koje industrije u današnjem visoko konkurentnom svijetu pokušala da se pretvara da nema rizika u onome čime se bavi – u stvari, da rizik nije ni postojao – onda osim toga što ona ne bi ispunjavala svoje zakonske i regulatorne obaveze, već bi vrlo brzo propala i nestala.

Ipak, rizik također može biti i koristan. Uspješno upravljanje rizicima može imati pozitivne rezultate, tako da kompanije moraju preuzeti rizike kako bi ostvarile svoje ciljeve. Naravno, organizacijama je potrebno da imaju određen stepen sigurnosti prije donošenja važnih strateških odluka. Važno je razumjeti da je rizik vjerovatan utjecaj nesigurnosti na te odluke. Ukratko, rizik leži u upravljanju odlukama u već složenom, nestabilnom i dvosmislenom svijetu, koji ubrzano postaje sve složeniji i nejasniji.

Digitalna prijetnja

Ovo pitanje je posebno istinito kada se radi o *cyber* riziku. U *cyber* prostoru, kada je u pitanju rješavanje sigurnosnih pitanja na nacionalnom i korporativnom nivou, neizvjesnost je veoma visoka. Prijetnja ne proističe iz konteksta i okolnosti na tržištu, već od „zlonamjernih aktera" koji pokušavaju izvesti ozbiljne napade. Oni su, u stvari, nevidljivi kao duhovi i fantomi iz drevnih legendi, a njihova nevidljivost samo pogoršava osjećaj prijetnje. Oni imaju i namjeru i sposobnost da nanose štetu, agilni su i prilagodljivi.

Štaviše, tehnologija postaje sve sofisticiranija iz dana u dan, ako ne i iz sata u sat. U prošlosti, biti uspješan industrijski kriminalac je uključivalo krađu dokumenata koji su ostavljeni na radnom stolu. Sada uz pomoć USB stika ili tehnikom eksfiltracije, isti kriminalac može ukrasti gigabajte informacija čiji bi ekvivalent predstavljao hrpu papirnih dokumenata tako visokih da mogu dohvatiti mjesec. Međutim, nije samo skladištenje podataka postalo hiper sofisticirano – od skladištenja papira do digitalnog skladištenja – već se promijenila i sama priroda i svrha podataka. Na primjer, ako kriminalac namjerava ukrasti zaštićene medicinske proizvode, više ne mora provaljivati u skladište, već može kopirati podatke u digitalnom formatu i klonirati proizvod 3D štampačem.

Očigledno je da organizacije svake vrste trebaju imati *cyber* zaštitu u bilo kojem obliku. I ne samo to, već im je potreban sistem koji je dovoljno robustan da ih upozori na svaki napad – stvaran ili zamišljen – što je brže moguće. Prijetnje u kibernetičkom prostoru spadaju u dvije široke kategorije: unutrašnje i vanjske. Da bi se dizajnirao i uspješno implementirao sistem zaštite od vanjskih prijetnji, treba se fokusirati na namjere i sposobnosti vanjskih zlonamjernih napadača – koje podatke traže, zašto ih traže i koje tehnologije su im dostupne.

Međutim, organizacije se također moraju pripremiti za prijetnju i od zlonamjernih insajdera i insajdera koji su slučajno ostavili sistem ranjivim na mogući napad. Nepažljiva upotreba ličnih podataka može izložiti pojedinca ucjenjivanju i zloupotrebi od strane organizacije koja ima zle namjere. Organizacije mogu imati najbolje *firewalle* na svijetu, ali oni ne znače ništa ako su suočeni s insajderom koji ima visok nivo pristupa informacijama i koji ih može ukrasti, a da ne bude otkriven.

Šta je zaista važno

Kako se vlade, preduzeća i pojedinci štite od tih prijetnji? Tehnički komitet ISO/TC 262, *Upravljanje rizicima*, izradio je ISO 31000, standard upravljanja rizikom koji kreira okvir principa i procesa za upravljanje rizikom uopšte. Jason Brown je predsjedavajući ISO/TC 262 i bio je, između ostalog, odgovoran za upravljanje procjenom *cyber* sigurnosti i osiguranje u australijskom ministarstvu odbrane. On ističe da, kao i kod upravljanja rizicima, ako se organizacija ozbiljno želi zaštititi od *cyber* rizika, onda se treba „vratiti ciljevima kojima teži i fokusirati se na ono što je zaista važno – drugim riječima, definisati najvažniji kapital".

Preduzeća i vlade moraju pažljivo procijeniti vrijednost i prirodu onoga što im je važno. Na primjer, ako je organizacija čuvar visokog tehničkog intelektualnog vlasništva u obliku podataka, očigledno je da bi curenje ili krađa takvih podataka imala ogromne posljedice, posljedice koje bi mogle biti još destruktivnije ako se te informacije čuvaju u ime drugih osoba koje se oslanjaju na tu organizaciju kao dio lanca snabdijevanja, jer bi narušavanje sistema moglo značiti uništenje čitavog lanca. Ono što je najbitnije, dakle, jeste strateški sistemski pregled, a ne procjena same tehnologije.

Ovakav pristup se poklapa s pristupom dr. Donalda R. Deutscha, potpredsjednika i šefa sektora za standarde u Oracle, sa sjedištem u Kaliforniji, i predsjedavajućim tehničkog komiteta ISO/IEC JTC 1, *Informaciona tehnologija*, potkomitet SC 38, *Cloud computing i distribuirane platforme*, grupe stručnjaka koji rade pod zajedničkom upravom ISO-a i Međunarodne elektrotehničke komisije (IEC). Cloud, i njegova pozicija u hijerarhiji rizika, možda ima najveći neposredni značaj za svakodnevne potrošače. Danas, ako koristimo računar, vrlo je vjerovatno da ćemo koristiti i cloud. Međutim, „cloud computing", kaže dr. Deutsch, „više je strategija implementacije i poslovanja nego tehnološka strategija". Definitivno postoje nedavna tehnološka poboljšanja koja su povezana s rizicima – kao što je automatsko osiguravanje računarskih resursa koje dijele višestruki korisnici – a ipak „rizici su slični onima koje biste imali u bilo kojem računarskom okruženju, ali su pogoršani i uvećani zbog povećanja obima".

Cijena otpornosti

Međunarodni standardi podržavaju ovaj strateški pristup *cyber* riziku. Kao što ističe Jason Brown, kada se radi o *cyber* rizicima, serija standarda ISO 31000 bi također trebala biti ocijenjena zajedno sa serijom ISO/IEC 27000 o sistemima upravljanja sigurnošću informacija, odnosno ISMS-om. Takav pristup predstavlja balans između tehnologije i „ljudskih faktora". ISO/IEC 27000 će pomoći organizaciji da procijeni svoje čisto tehnološke potrebe, dok će joj ISO 31000 pomoći da shvati vrijednost informacija ili proizvoda koje posjeduje u *cyber* prostoru, a samim tim i stepen tehnološke zaštite koji je potrebno da ima kako bi se spriječili bilo kakvi napadi. Drugim riječima: kroz temeljnu procjenu rizika pomoću ISO 31000 svaka organizacija može sebi uštediti značajne finansijske troškove kada je u pitanju stjecanje tehnološke sigurnosti. Loša procjena rizika može isto tako dovesti do toga da se previše plati za zaštitni sistem, odnosno da se ne plati dovoljno.

Ove dvije serije standarda nipošto nisu jedini standardi koji mogu pomoći u ublažavanju *cyber* rizika. *Cyber* sigurnost se također mora posmatrati u smislu kontinuiteta poslovanja, a serija standarda ISO 22301 za upravljanje kontinuitetom poslovanja je upravo za to predviđena. Ova serija ima za cilj uspostavljanje „dokumentovanog sistema upravljanja koji štiti od […] ometajućih incidenata kada se pojave" i omogućava organizaciji da procijeni kako njen informacioni i telekomunikacioni sistem podržava njene ciljeve i kakve bi bile posljedice u slučaju kolapsa. Ulaganje organizacije u *cyber* sigurnost može biti diktirano nivoom zavisnosti od sistema; mala organizacija će možda moći da nastavi s korištenjem (ili čak da se vrati) na papirne račune, dok div kao što je Amazon doslovno zavisi od povezanosti.

Isto tako, rad ISO/IEC JTC 1/SC 38 pomaže proizvođačima – i na kraju i potrošačima – da govore zajedničkim jezikom *cloud computinga*. Važno je napomenuti da potražnju za ovim setom standarda ne određuju sami proizvođači ili prodavci, kao što je to obično slučaj, već potrošači i kupci. Vlade i korporacije su naglasile da svaki proizvođač koristi sopstvenu

terminologiju, što onemogućava poređenje proizvoda i donošenje informisane odluke o kupovini. To je dovelo do objavljivanja standarda ISO/IEC 17789, *Informaciona tehnologija – Cloud computing – Referentna arhitektura*, koji je dao referentnu arhitekturu i okvir zajedničkog rječnika. Potkomitet SC 38 je nadgledao i izradu standarda ISO/IEC 19086, koji se sastojao od četiri dijela, od kojih su dva još u razvoju, o sporazumima o nivou usluga između pružalaca *cloud* usluga i njihovih klijenata.

Kvantni skok

Pozitivan utjecaj koji su svi ovi standardi imali na *cyber* sigurnost, a posebno na *cyber* rizike uopšte nije upitan. Oko 40 zemalja je usvojilo ISO 31000 kao nacionalni sistem za upravljanje rizicima. Štaviše, kada se u Google pretraživaču unese „ISO 31000", broj rezultata za 0,54 sekunde prelazi cifru od 6,5 miliona.

Međutim, s obzirom da se tehnologija razvija sve bržim tempom, tako i međunarodni standardi moraju držati korak s vremenom. Alati koji se danas koriste možda neće funkcionisati u budućnosti. Na primjer, s obzirom na činjenicu da mašinsko učenje doprinosi razvoju vještačke inteligencije, sistem će vjerovatno moći integrisati i adaptivne i „filozofske" sposobnosti učenja koji sada jednostavno ne postoje. Mogućnosti analize podataka se razvijaju do te mjere da se velike količine podataka mogu analizirati kako bi se identifikovali novi problemi koji se inače ne bi mogli otkriti. Osim toga, pojava kvantnog *computinga* će također eksponencijalno povećati brzinu *computinga*. Kombinacija ove tri promjene u *cyber* svijetu će „vjerovatno biti najveća revolucija koja se desila od otkrića struje ili atoma", kaže Jason Brown. A ovdje čak ne uzimamo u obzir nanotehnologiju ili sve veću međusobnu povezanost uređaja.

Kada se ti faktori konačno spoje, konkurentsko okruženje koje omogućava prednost u poslovanju, između zemalja i između protivnika bit će mnogo brže. Toliko da će ljudski doprinos vjerovatno i dalje predstavljati rizik u smislu ciljeva, ali će stvarna ljudska sposobnost da se bavi *cyber* prostorom biti zanemarljiva. ISO tehnički komitet ISO/TC 262 trenutno ispituje oblast koju je označila kao „*Upravljanje rizicima u nastajanju"*, fokusirajući se na one rizike koji će najvjerovatnije dovesti do poremećaja. Kao što Brown kaže, i potrošači i proizvođači moraju drugačije pristupiti budućnosti, i svi mi ćemo „morati biti mnogo otvoreniji prema ovom veoma nestabilnom i dvosmislenom svijetu".

OLAKŠATI PUTOVANJE PODATAKA SA ISO/IEC 20000-1

ISOFocus #132

Podaci, i oblak (cloud) koji ih hostuje, imaju skoro beskonačnu vrijednost za preduzeća koja znaju kako da ih tretiraju – dokle god postoji odgovarajuća strategija koja će osloboditi njihov pun potencijal. Kompanija *Orange Business Services* pomaže korisnicima da pretvore svoje podatke u posebnu poslovnu imovinu, zahvaljujući maloj pomoći ISO/IEC standarda za upravljanje IT uslugama.

U doba digitalne revolucije kompanije proizvode više podataka nego ikada. Ti podaci nisu ništa drugo nego sirovina, međutim ako su organizacije sposobne da ih transformišu u korisne informacije, to može otvoriti vrata cijelom nizu mogućnosti. Zahvaljujući *cloud computingu*, organizacije mogu imati pristup ogromnim IT mogućnostima – a s većom fleksibilnošću kompanije mogu eksternalizovati kompletne ili dio svojih informacionih sistema, radne prostore, servere, aplikacije i skladištenje.

Iako *cloud* postoji više od deset godina, najveća prepreka koja i dalje ometa njegovo usvajanje je stalna briga o sigurnosti i integritetu podataka. Integratori sistema koji mogu ponuditi efikasna rješenja za sigurnost cloud hostinga i kontrolu pristupa će u budućnosti biti dobro pozicionirani, jer će korisnicima moći ponuditi širok spektar usluga za daljinsko upravljanje uz istovremeno povećanje ukupne vrijednosti njihove kompanije. *Orange*

Business Services je jedna takva kompanija. B2B, kao ogranak Orange grupe, koji je globalni pružalac ICT usluga, koji ima 260 miliona klijenata u 28 zemalja i koji ostvaruje godišnji prihod od prodaje od 41 milijardu eura, teži da bude vodeći akter u takozvanom „putovanju podataka". Podržavajući organizacije u svakoj fazi njihove digitalne transformacije, B2B nudi klijentima stručnost u prikupljanju, prijenosu, sigurnosti, skladištenju, obradi, analizi i razmjeni podataka i stvaranju vrijednosti. Kako bi pružio podršku u jednom tako velikom poduhvatu *Orange Business Services* treba da vodi globalne procese u okviru modela korporativnog upravljanja koji se primjenjuje širom svijeta.

Implementacija standarda ISO/IEC 20000-1, *Informacione tehnologije – Upravljanje uslugama – Dio 1: Zahtjevi sistema za upravljanje uslugama*, stoga se nametnula kao logičan cilj. Vodeći standard ISO/IEC 20000 porodice, koji je izradio ISO i Međunarodna elektrotehnička komisija (IEC), pomaže organizacijama da integrišu strategiju životnog ciklusa usluga pružajući primjere najbolje prakse o tome kako upravljati svojim portfoliom usluga da bi one ostale aktuelne. Objavljivanje novog i poboljšanog izdanja standarda u 2018. godini potaknulo nas je da pitamo Jean-Pierre Girardina, iz sektora za Korisničke usluge i operacije u kompaniji *Orange Business Services*, kako će ovaj najnoviji ažurirani standard pomoći kompaniji u njenoj posvećenosti održavanju superiornih sveobuhvatnih usluga – gdje god njegovi klijenti posluju.

ISOfocus: Koji su razlozi za toliki entuzijazam vezan za standard ISO/IEC 20000-1 u *Orange Business Servicesu*?

Jean-Pierre Girardin: S klijentelom od preko tri hiljade renomiranih multinacionalnih korporacija širom svijeta i preko dva miliona profesionalaca, kompanija i lokalnih zajednica u Francuskoj, *Orange Business Services* se u svom radu uveliko oslanja na standarde za informacionu sigurnost. Kompanija je već deset godina certificirana prema standardu ISO/IEC 20000-1. Od početka je odlučeno da se standard uvodi na postepen i integrisan način. Izgradili smo inicijalne sisteme korporativnog upravljanja kvalitetom koji su zasnovani na ISO 9001 da bi poboljšali procese upravljanja uslugama u okviru koji se temelji na integraciji. To nam je omogućilo da uskladimo naše uslužne procese u svim operativnim centrima kompanije *Orange Business Services* širom svijeta. Za B2B kompaniju koja je orijentisana za pružanje usluga, dobijanje certifikata prema ISO/IEC 20000-1 u to vrijeme predstavljalo je zlatnu priliku. Omogućilo nam je da se usredsredimo na poboljšanje naših usluga i izvučemo korist od kombinovanja tri standarda za sisteme upravljanja – ISO 9001 (kvalitet), ISO/IEC 20000-1 (IT usluge) i ISO/IEC 27001[1] (informaciona sigurnost) – kao i od kontinuiranog poboljšanja koje je svojstveno za ta tri standarda.

Koje su glavne prednosti koje je ISO/IEC 20000-1 omogućio kompaniji *Orange Business Services*?

Implementacija ISO/IEC 20000-1 osigurala je niz ključnih prednosti, kako unutrašnjih tako i vanjskih. Naš trostruki certifikat, koji se obnavlja svake godine s redovnim novim proširenjima područja primjene, identifikuje *Orange Business Services* kao pouzdanog partnera i prepoznaje kvalitet našeg sistema upravljanja na globalnom nivou. Od tada smo uveli i standard ISO 14001 za upravljanje zaštitom okoline na tri naše lokacije. Svi naši indikatori pokazali su da se zadovoljstvo korisnika značajno povećalo kao rezultat tih

[1] ISO/IEC 27001:2013, *Informaciona tehnologija – Sigurnosne tehnike – Sistemi upravljanja informacionom sigurnošću – Zahtjevi*, zajednički je izradio ISO i Međunarodna elektrotehnička komisija (IEC).

napora. Štaviše, program certifikacije se pokazao kao odličan način za jačanje kohezije naših timova što nam je omogućilo da zadržimo ovaj tempo tokom godina.

Sve veća upotreba ISO/IEC 20000-1 nije posebno iznenađujuća ako se uzme u obzir trenutna zabrinutost za sigurnost. Možete li nam objasniti kako ovaj standard pruža dodatne koristi vezane za sigurnost?

Standard ISO/IEC 27001 za sigurnost informacija pokriva specifično područje primjene naših aktivnosti i entiteta (operacije, cloud usluge…), tako da tački 6.6 standarda ISO/IEC 20000-1 o upravljanju informacijskom sigurnošću možemo zahvaliti što nam je omogućila da osiguramo širinu naših procesa i aktivnosti na tri nivoa: zahtjevi u našim uslugama, sigurnosne kontrole u operacijama i portfolio o upravljanju sigurnosnim uslugama.

Na primjer, mi proaktivno nadgledamo i odgovaramo na sigurnosne incidente koji mogu utjecati na imovinu koja nam je povjerena. Da bismo to postigli, osiguravamo da su sve izmjene procijenjene prije implementacije kako bi se spriječili bilo kakvi udari na zaštitu sigurnosti. Također smo u naše procese i radne procedure uveli značajne sigurnosne kontrole koje su se pokazale veoma efikasnim. Dodatne sigurnosne karakteristike ISO/IEC 20000-1 također doprinose podizanju svijesti o sigurnosti kao sastavnom dijelu operativne prakse, a auditori su podržali primjer ponašanja našeg osoblja kada je u pitanju zaštita integriteta podataka.

Kako je ISO/IEC 20000-1 integrisan u procesni, operativni i strateški nivo unutar kompanije *Orange Business Services*?

Od samog početka projekta 2008. godine, ISO/IEC 20000-1 je u potpunosti integrisan u naš globalno koherentni sistem upravljanja sigurnošću. To je posebno važno jer se poklopilo s početkom certifikacije prema ISO/IEC 27001 našeg Egipatskog glavnog centra za usluge u u Kairu, a zatim Indijskog glavnog centra za usluge u Gurgaonu u blizini Delhija i, konačno, naših aktivnosti u Francuskoj, Brazilu i na Mauricijusu. Kao rezultat toga, zahtjevi standarda ISO/IEC 20000-1 su postali sastavni dio svih naših procesa i aktivnosti, bilo da se radilo o odnosima s kupcima, aktivnostima s dobavljačima ili životnom ciklusu usluga, od narudžbe pa do isporuke.

Na strateškom nivou, *Orange Business Services* provodi redovno preispitivanje upravljanja na lokalnom, regionalnom i globalnom nivou gdje se rezultati certifikacije pažljivo nadgledaju. Pratimo očekivanja kupaca i tome prilagođavamo naše područje djelovanja.

S obzirom da ste imali ogroman uspjeh u implementaciji ISO/IEC 20000-1 uglavnom internim resursima, možete li čitaocima ISOfocusa dati neke savjete?

Kada krenete u proces certifikacije, veoma je važno da idete korak po korak. Počeli smo tako što smo formirali vješt, informisan i posvećen tim za upravljanje projektom. U tu svrhu, na znanje stečeno u okviru ITIL-a, koji pomaže usklađivanje IT usluga s poslovnim potrebama, gledalo se kao na ogromnu prednost. Smatrali smo da je važno napraviti metodičku analizu nedostataka i studiju izvodljivosti prije uvođenja bilo koje nove usluge za certifikaciju kao i da ojačamo bazu internih auditora koji bi pomogli u potvrđivanju našeg napretka kroz godišnje audite svih naših procesa i entiteta.

Da bi se osoblje ohrabrilo da učestvuje u ovom projektu, organizovali smo sesije o ISO/IEC 20000-1 i svim aspektima vezanim za certifikaciju i standarde. S obzirom da smo

nastavili da budemo pragmatični, u svakom trenutku smo težili prenijeti prednosti certifikacije te osigurati da svi razumiju svrhu implementacije standarda. Izazov nije bio da se navedu zahtjevi standarda, nego da se koncentrišemo na demonstraciju važnosti primjene istih u korist naših klijenata, naših usluga i naših procesa. Cijeli poduhvat je, naravno, podržalo više rukovodstvo, što je bilo presudno za njegov uspjeh.

Nedavno je objavljena nova verzija standarda ISO/IEC 20000-1 – imate li ikakvu ideju o tome kako dalje ? Budući projekti/planovi?

Nova verzija ISO/ IEC 20000-1 pruža uzbudljivu perspektivu za našu kompaniju. Standard je usklađen s novom strukturom visokog nivoa koja se koristi u svim ISO standardima za sisteme upravljanja, uključujući ISO 9001:2015, ISO/IEC 27001:2013 i ISO 14001:2015, tako da će ova verzija biti još lakša za razumjeti.

U *Orange Business Services* već razmišljamo o tome kako da se prilagodimo promjenama i nastojimo da budemo jedna od prvih kompanija koja će uspješno implementirati novo izdanje standarda. To će biti naš izazov za 2019. godinu!

ARHITEKTURA POVEZANE BUDU.NO STI

Autor: Rick Gould - ISOFocus #132

Godine 2018. ISO je, zajedno s Međunarodnom elektrotehničkom komisijom (IEC), objavio ISO/IEC 30141, prvi harmonizovani standard referentne arhitekture za Internet stvari (Internet of Things – IoT) na svijetu – složeni skup milijardi pametnih uređaja povezanih putem Interneta. Primjena standarda učinit će Internet stvari učinkovitijim, sigurnijim, otpornijim i mnogo zaštićenijim.

Prošlo je dvije godine od trenutka kada je ISOfocus prvi put izvještavao o Internetu stvari (IoT) 2016. godine. Prvo, osnovan je novi potkomitet koji se u potpunosti fokusirao na razvoj standarda kao što je ISO/IEC 30141 za ovaj sektor koji se brzo širi. Drugo, nekoliko visokoprofilnih napada na Internet stvari jasno je pokazalo zašto su ti standardi neophodni. Prije gotovo 20 godina pionir RFID tehnologije u Velikoj Britaniji Kevin Ashton skovao je izraz „Internet of Things" kada je radio za kompaniju Procter & Gamble. Ashton je u prezentaciji pokazao kako kompanija može koristiti radiofrekvencijsku identifikaciju ili RFID – bežičnu tehnologiju koja se danas široko primjenjuje u beskontaktnim plaćanjima i pametnim ID karticama – za traženje i praćenje proizvoda. I fraza se zadržala.

Zvanična definicija IoT-a koju je formulisao ISO i Međunarodna elektrotehnička komisija (IEC) glasi: „infrastruktura međusobno povezanih entiteta, ljudi, sistema i izvora informacija zajedno s uslugama koje obrađuju i reaguju na informacije iz fizičkog i virtuelnog svijeta". Ali, jednostavno rečeno, Internet stvari je mreža kompjuterizovanih i često bežičnih uređaja koji nam omogućavaju, kao i mašinama, da vidimo, osjetimo i čak kontrolišemo veći dio svijeta oko nas, bilo na individualnom ili na širem, globalnom nivou. Zaista, IoT uređaji i sistemi igraju sve veću ulogu u većini, ako ne i u svim aspektima modernog života. Neki od njih su već dobro poznati i u svakodnevnom jeziku na domaćem i potrošačkom tržištu, a ipak najveći korisnici IoT-a rade u industrijskom, zdravstvenom i poljoprivrednom sektoru. Jednostavno rečeno, svaka tehnologija koja ima prefiks pametna vjerovatno će biti dio brzorastuće IoT porodice; naprimjer, pametna brojila, pametni automobili, pametne kartice, pametne fitnes narukvice, pametni gradovi, pametni telefoni, pametni satovi, pametne komunalne usluge, pametna poljoprivreda, pametna zdravstvena zaštita, pa čak i pametna proizvodnja, što će biti sljedeća industrijska revolucija.

Približavanje

Internet stvari može nas učiniti povezanijim, obrazovanijim, efikasnijim, efektivnijim i manje rasipnim. Ali ako se zloupotrijebi, može oslabiti sigurnost i otpornost naših računarskih mreža i podataka. Jer relativna jednostavnost IoT uređaja stvara onoliko problema koliko i prilika. „Prednosti su brojne, ali u isto vrijeme najveći rizici su otpornost i sigurnost", primjećuje Francois Coallier, predsjedavajući zajedničkog tehničkog komiteta ISO/IEC JTC 1, *Informaciona tehnologija*, potkomitet SC 41, *Internet stvari i srodne tehnologije*. ISO i IEC su osnovali JTC 1/SC 41 kako bi se fokusirali na standarde za IoT, dok je sam JTC 1 odgovoran za međunarodnu standardizaciju u oblasti IT-a i objavio je više od tri hiljade standarda od svog osnivanja 1987. godine.

Izazovi interoperabilnosti – ili sposobnost IoT uređaja da se neometano povežu jedni s drugima kao i s drugim sistemima – i sigurnost su povezani. „Tehnologije se stalno razvijaju i to izuzetno brzo", dodaje Coallier, „tako da se njihovo dodavanje mreži odvija veoma brzo i često *ad hoc* u zavisnosti od toga kako se nove tehnologije pojavljuju". Rast IoT-a je eksponencijalan, a procjenjuje se da bi do 2020. godine broj povezanih IoT uređaja mogao dosegnuti 50 milijardi, a tržište bi moglo vrijediti millijarde dolara.

Upečatljiva godina

Godina 2016, kada je osnovan JTC 1/SC 41, bila je upečatljiva kako u doslovnom tako i u figurativnom smislu za Internet stvari, zbog nekih visokoprofilnih napada na mreže kroz Internet stvari. U martu te iste godine, naprimjer, hakerski napad „Mirai Botnet" paralizovao je veći dio Interneta na istočnoj strani SAD-a, u najvećem udaru na internet do danas. Mnogi su bili iznenađeni brzinom kojom se širio zlonamjerni kod i koliko je hakeru bilo lako da provali u navodno sigurne mreže. Kako se to moglo dogoditi? Ciljanjem na najslabije karike u lancu ili, u ovom slučaju, na IoT uređaje na rubu mreže.

„Kreator malvera Mirai Botnet ciljao je uređaje kao što su bežične CCTV kamere i pametne televizije, koje se prodaju s ograničenim brojem podrazumijevanih administratorskih imena i lozinki", objašnjava Coallier. Proizvođač je proizveo milione takvih uređaja. „Napadajući Botnet je probao svaku kombinaciju imena administratora i lozinke, dok napad nije uspio, čime je omogućio Botnetu da preuzme kontrolu nad uređajem", kaže on. „S više od stotinu hiljada ovih uređaja pod svojom kontrolom, napadač je mogao izvesti intenzivne napade uskraćivanja usluga koje su uspjele privremeno srušiti dio interneta u SAD-u".

U drugom dobro dokumentovanom hakiranju, fabrika je sabotirana napadom na administrativne lične računare (PC-jeve). „U tom slučaju čini se da je preko tih računara bilo moguće pristupiti industrijskim proizvodnim sistemima”, dodaje Coallier, „što se ne bi desilo da su industrijski proizvodni sistemi izolovani od administrativnih računara koji su spojeni na internet putem pravilne segmentacije mreže”. Što je još značajnije, mreža je mogla biti mnogo sigurnija jednostavnom primjenom dobro dokumentovanih procesa i procedura koje su već opisane u mnogim standardima, kao što je ISO/IEC 27033 serija standarda za IT sigurnosne tehnike, odnosno standard koji propisuje segmentirane mreže za dodatnu sigurnost.

Iste godine kada se desio Mirai Botnet grupa izraelskih istraživača pokazala je da postoji potencijal za hakiranje mreže za rasvjetu pomoću modifikovanih zračnih bespilotnih letjelica i iskorištavanjem ranjivosti u popularnoj pametnoj sijalici. Jednostavno kroz zaobilaženje sigurnosnih mjera u samo jednoj lampi moguće je zaraziti susjedne, kompatibilne sijalice, a zatim ih kontrolisati. Istraživači su izjavili da ako u gradu postoji dovoljno pametnih sijalica koje koriste iste komunikacijske protokole, zlonamjerni napadači mogu lahko pristupiti i zaraziti cijelu mrežu sijalica za samo nekoliko minuta. Uprkos činjenici da bi to bio ekstremni scenario, ta demonstracijska vježba pokazala je potencijal za izvođenje masovnih zlonamjernih napada u naizgled sigurnim mrežama iskorištavanjem previđenih ranjivosti u jednostavnim uređajima na rubu mreže.

IoT standardi

Problem sa IoT uređajima leži u tome što je njihova jednostavnost povezana s nepažljivom *ad hoc* implementacijom otežana ako korisnici zanemare pitanje sigurnosti. Mnogi takvi uređaji su pojednostavljeni mini kompjuteri male snage, s kompaktnim operativnim sistemom zasnovanim na široko dostupnom Linuxu, sistemu koji je popularan kod kompjuterskih hakera. To znači da IoT uređaji imaju različite zahtjeve od drugih računara, tako da kada korisnici rigorozno ne primjenjuju standarde za sigurnost ti faktori omogućavaju da Internet stvari postane meta sve većih napada. „Kod IoT-a se sve svodi na pitanje ravnoteže. Mogućnosti su brojne, ali neophodno je pronaći pravu ravnotežu s pažljivom implementacijom i posvetiti mnogo više pažnje sigurnosti”, primjećuje Coallier.

U ovoj situaciji međunarodni standardi će podržati operabilnost i otpornost Interneta stvari. Kako se to može postići? Naprimjer, serija standarda ISO/IEC 29192 definiše tehnike lagane kriptografije koje su idealne za jednostavne uređaje male snage. U primjeru sijalice izraelski istraživači preporučili su specifičnu sigurnosnu tehniku opisanu u ISO/IEC 29192-5, koja određuje tri *hash* funkcije pogodne za aplikacije koje zahtijevaju lagane kriptografske implementacije. Ali, kao što je slučaj i u svakoj oblasti u razvoju, bit će nam potrebni i novi standardi, a to je upravo uloga JTC 1/SC 41, čije opsežno područje rada pokriva interoperabilnost, sigurnost i, prije svega, zaštićenost.

Potkomitet JTC 1 je do sada objavio 18 dokumenata, uglavnom fokusiranih na senzorske mreže. Također je izdao uputstvo u obliku tehničkog izvještaja ISO/IEC TR 22417, *Informacione tehnologije – Slučajevi upotrebe Interneta stvari (IoT),* koji osigurava kontekst za korisnike IoT standarda. Ovaj vodič pokriva važna pitanja kao što su osnovni zahtjevi, interoperabilnost i standardi koje su korisnici primijenili. Što je najvažnije, navedeni primjeri objašnjavaju ulogu koju postojeći standardi imaju i naglašavaju područja gdje je potreban daljnji rad na standardizaciji.

Uspostavljanje osnove

Standardi za Internet stvari uspostavljaju zajednički jezik o temama kao što su terminološke ili referentne arhitekture koje će pomoći razvojnim inženjerima da razviju interoperabilni ekosistem. ISO/IEC 30141 pruža osnovu i referentni okvir za mnoge primjenjive standarde koje je izradio JTC 1/SC 41. „Uvidjeli smo da postoji potreba za referentnom arhitekturom kako bi se maksimizirale koristi i smanjili rizici", objašnjava Coallier, koji je predsjedavajući ovog ISO-ovog potkomiteta. Još jedan osnovni standard je ISO/IEC 20924, *Informaciona tehnologija – Internet stvari (IoT) – Definicije i rječnik*. „Važno je da oni koji rade s Internetom stvari komuniciraju istim jezikom", dodaje Coallier. ISO/IEC 20924 i ISO/IEC 30141 daju taj neophodan jezik.

Radnu grupu koja je razvila ISO/IEC 30141 vodila je dr. Jie Shen iz Kine, uz podršku druga dva urednika Wei Wei iz Njemačke i Östen Frånberga iz Švedske. Zajedno, vođe ovog projekta imaju višedecenijsko iskustvo u ovoj oblasti, a podržalo ih je više od 50 drugih stručnjaka koji su direktno doprinijeli standardu. „Za IoT su vezani mnogi rizici i prilike", kaže dr. Jie Shen, dodajući da „moramo osmisliti savršen mehanizam održavanja kako bi prevazišli ove rizike; to je samo po sebi vrlo detaljan posao".

Većina detalja već je sadržana u mnogim standardima koje su objavili potkomiteti JTC-a 1, a ISO/IEC 30141 osigurava referentnu arhitekturu kako bi ih sve objedinio, zajedno s nekoliko novih standarda koje razvija JTC 1/SC 41. „ISO/IEC 30141 daje zajednički okvir za dizajnere i programere Interneta stvari", objašnjava Coallier. „Standard opisuje glavne karakteristike Interneta stvari, zajedno s konceptualnim modelom i referentnom arhitekturom", dodaje on. Opise prate brojni primjeri.

Lanac od šest domena

Standard ISO/IEC 30141 također uključuje novu i inovativnu strukturu poznatu kao model šest domena za referentnu arhitekturu Interneta stvari. Ovaj model daje okvir dizajnerima sistema da integrišu mnoštvo uređaja i operacija u IoT. Projektni tim je ustanovio da konvencionalni pristupi nisu pogodni za jednostavniju mrežu. Dr. Jie Shen objašnjava: „Komplikovanije je izgraditi ekosistem u Internetu stvari, povezati mnoge heterogene entitete kao što su ljudski korisnici, fizički objekti, uređaji, uslužne platforme, aplikacije, baze podataka, alati trećih strana i drugi resursi. Shvatili smo da je konvencionalni slojeviti referentni model koji se obično primjenjuje u IT sistemima bio nedovoljan. „Model sa šest domena, s druge strane, može pomoći da se jasno podijeli ekosistem IoT-a i usmjeri korisnike na uspostavljanje novog poslovnog modela Interneta stvari. Sam model će biti još efikasniji kada bude zasnovan na *blockchain* tehnologiji, odnosno visoko zaštićenoj tehnici koja se sve više koristi u finansijskim transakcijama.

Standard se također opsežno bavi interoperabilnošću – koja omogućava da različiti tipovi uređaja besprijekorno komuniciraju – i konceptom pouzdanosti Interneta stvari koji je definisan kao stepen pouzdanosti koji korisnici mogu imati da sistem funkcioniše kao što je planirano, istovremeno obezbjeđujući sigurnost, zaštićenost, povjerljivost, pouzdanost i otpornost na poremećaje kao što su prirodne katastrofe, kvarovi, ljudske greške i napadi. Već su objavljeni mnogi standardi za otpornost, sigurnost i zaštićenost, a ISO/IEC 30141 pruža referentnu arhitekturu za njihovu primjenu", obavještava Coallier. Istovremeno, kako Internet stvari nastavlja da se razvija i raste, JTC 1/SC 41 izrađuje devet dodatnih standarda za IoT, kako bi se osigurala veća pouzdanost, interoperabilnost, sigurnost i tehničke specifikacije.

KAKO SE POZABAVITI DANAŠNJIM IT SIGURNOSNIM RIZICIMA

Autor: Barnaby Lewis - ISOFocus #132

Stručnjaci za industriju procjenjuju da bi se godišnji gubici od *cyber* kriminala mogli povećati na 2000 milijardi dolara do sljedeće godine[1]. Mnoštvo mobilnih uređaja i drugih povezanih „stvari" svakodnevno se dodaje na listu potencijalnih meta, tako da je neophodno usvojiti zajednički pristup.

Privlačnost *cyber* kriminala za hakere je očigledna: zbog složenog mehanizma interakcije, relativno niskih kazni, nepovezanih pristupa pranju novca i potencijalno masovnih isplata. Ključni zadaci su priprema i identifikacija ranjivosti i otpornosti, u smislu interakcije s cjelokupnim sistemima upravljanja, a tu stupa na snagu standard ISO/IEC 27001 za sisteme upravljanja sigurnošću informacija (ISMS).

Vodeći standard iz porodice standarda ISO/IEC 27000 prvi put je objavljen prije više od 20 godina, a izradio ga je ISO/IEC JTC 1, zajednički tehnički komitet ISO-a i Međunarodne elektrotehničke komisije (IEC). Osnovan je kako bi omogućio formalnu standardizaciju u oblasti informacione tehnologije, stalno se ažurira i proširuje tako da uključuje više od 40

[1] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", Forbes Online

međunarodnih standarda koji pokrivaju sve od zajedničkog rječnika (ISO/IEC 27000), upravljanja rizikom (ISO/IEC 27005), sigurnosti clouda (ISO/IEC 27017 i ISO/IEC 27018) do forenzičkih tehnika koje se koriste za analizu digitalnih dokaza i istraživanje incidenata (IEC 27042 odnosno ISO/IEC 27043).

Stručnjaci za industriju procjenjuju da bi se godišnji gubici od *cyber* kriminala mogli povećati na 2000 milijardi dolara do sljedeće godine[2]. Mnoštvo mobilnih uređaja i drugih povezanih „stvari" svakodnevno se dodaje na listu potencijalnih meta, tako da je neophodno usvojiti zajednički pristup.

Privlačnost *cyber* kriminala za hakere je očigledna: zbog složenog mehanizma interakcije, relativno niskih kazni, nepovezanih pristupa pranju novca i potencijalno masovnih isplata. Ključni zadaci su priprema i identifikacija ranjivosti i otpornosti, u smislu interakcije s cjelokupnim sistemima upravljanja, a tu stupa na snagu standard ISO/IEC 27001 za sisteme upravljanja sigurnošću informacija (ISMS).

Vodeći standard iz porodice standarda ISO/IEC 27000 prvi put je objavljen prije više od 20 godina, a izradio ga je ISO/IEC JTC 1, zajednički tehnički komitet ISO-a i Međunarodne elektrotehničke komisije (IEC). Osnovan je kako bi omogućio formalnu standardizaciju u oblasti informacione tehnologije, stalno se ažurira i proširuje tako da uključuje više od 40 međunarodnih standarda koji pokrivaju sve od zajedničkog rječnika (ISO/IEC 27000), upravljanja rizikom (ISO/IEC 27005), sigurnosti clouda (ISO/IEC 27017 i ISO/IEC 27018) do forenzičkih tehnika koje se koriste za analizu digitalnih dokaza i istraživanje incidenata (IEC 27042 odnosno ISO/IEC 27043).

Pored toga što olakšavaju upravljanje sigurnošću informacija, ovi standardi će također pomoći da se identifikuju i procesuiraju hakeri. Naprimjer, ISO/IEC 27043 nudi smjernice koje opisuju procese i principe koji se primjenjuju na različite vrste istraga, uključujući neovlašteni pristup, korupciju podataka, pad sistema ili korporativna kršenja sigurnosti informacija, ali ne ograničavajući se na njih, kao i bilo koje druge digitalne istrage.

Budite korak ispred

Potkomitet SC 27, ISO/IEC JTC 1 odgovoran za tehnike IT sigurnosti ima veliku odgovornost da, kroz proces stalnog napretka, osigura da ova porodica standarda nastavi zadovoljavati potrebe malih i velikih preduzeća, što je u velikoj mjeri omogućeno zahvaljujući doprinosu ljudi kao što je prof. Edward Humphreys, koji predsjedava radnom grupom koja je odgovorna za razvoj ISMS-a, i koji se brine da ona i dalje bude jedan od najefikasnijih alata za upravljanje rizicima protiv milijardi napada koji se događaju svake godine[3], a koji također nastavljaju razvijati svoje ciljeve i metode.

Razgovarali smo s prof. Humphreysom, ekspertom za sigurnost informacija i upravljanje rizicima koji ima više od 37 godina iskustva u savjetovanju i edukativnom radu. Započeli smo s pitanjem o osnovama ISMS-a. Kako ti sistemi mogu konstantno biti korak ispred kriminalaca da bi zaštitili poslovanje i potrošače? „Istina je da se rizici koji ugrožavaju informacije, poslovne procese, aplikacije i usluge stalno razvijaju. ISO/IEC 27001 je standard koji se kontinuirano poboljšava, što znači da integrisani proces upravljanja rizikom omogućava preduzećima da ostanu ažurna u borbi protiv *cyber* kriminala."

[2] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", Forbes Online

[3] "Internet Security Threat Report", Volume 23, Symantec, 2018

Prema profesoru Humphreysu, aspekt stalnog poboljšanja ISO/IEC 27001 znači da organizacija može procijeniti svoje rizike, provesti kontrolne mjere za njihovo ublažavanje, a zatim pratiti i revidirati rizike i kontrole, poboljšavajući svoju zaštitu prema potrebi. Na taj način standard je uvijek spreman i pripremljen da reaguje na napade: „Ako se pravilno koristi, ISMS omogućava organizaciji da bude korak ispred kriminalaca, reagujući na rizike koji se javljaju u okruženju vezanom za Internet i *cyber* prostor."

Od prijetnji do mogućnosti

Na poslovnom nivou, modeliranje i ublažavanje prijetnji u svim njihovim oblicima je i dalje veliki zadatak. Postoji jasna potreba da se koristi jedinstveni, integrisani sistem sigurnosti u cjelokupnom poslovanju i, s obzirom na složenost međusobnih odnosa, pitali smo prof. Humphreysa da li se ISMS može primijeniti na mala i srednja preduzeća (SME).

„ISMS se primjenjuju na sve vrste organizacija i sve vrste poslovnih aktivnosti, uključujući i mala i srednja preduzeća. Mnoga mala i srednja preduzeća su dio lanaca snabdijevanja, tako da je od suštinskog značaja da kontrolišu i upravljaju sigurnošću informacija i *cyber* rizika kako bi zaštitili sebe i druge". Prof. Humphreys objašnjava da su obaveze preduzeća obično definisane sporazumima na nivou usluga (Service Level Agreement – SLA), ugovorima između partnera u lancu snabdijevanja koji detaljno opisuju obaveze i zahtjeve usluga i uspostavljaju zakonske obaveze, s tim da ISMS često čini sastavni dio takvih sporazuma.

Naravno, online poslovanje nesumnjivo predstavlja izazov za mala i srednja preduzeća, ali mogućnosti koje pruža internet su mnogo veće. Moglo bi se tvrditi da su mala preduzeća najviše favorizovana pojavom tehnologije, što je nedavno izjavio ambasador Svjetske trgovinske organizacije Alan Wolff. Govoreći na Generalnoj skupštini ISO-a 2018. godine, Wolff je istakao da „bilo ko – ko ima projekt, posjeduje računar, ko ima pristup internetu ili ima pristup platformi može postati dio međunarodne trgovine".

Prednosti za socio-ekonomski razvoj su brojne, jer internet omogućava sve većem broju prethodno izolovanih ljudi i zajednica da igraju ulogu na globalnom tržištu. Međutim, usvajanjem opreznog i dokazanog pristupa kao što je onaj koji se zasniva na ISMS-u neophodno je suprotstaviti se mogućim nedostacima. Gospodin Humphreys nas podsjeća da „*cyber* napad na jednom dijelu lanca snabdijevanja može poremetiti sve aktere" i imati posljedice ne samo na ciljnu kompaniju već i njene direktne klijente. To važi i za proizvođače igračaka na Baliju, kao i za nacionalne zdravstvene službe u Evropi.

Pravo na privatnost i klima povjerenja

Naša privatnost može biti manje složena od privatnosti u globalnom poslovnom okruženju, ali je pitanje jednako važno. Za mnoge od nas jednostavna činjenica da koristimo najbolje prakse da izaberemo lozinku i izvršimo sigurnosno ažuriranje (ne zaboravljajući da slijedimo svoju intuiciju kada slučaj izgleda mutno ili previše dobro da bi bio istinit) trebala bi da nas u većini slučajeva štiti od hakera. Međutim, sve više se postavlja pitanje o načinu na koji institucije i preduzeća skladište, analiziraju i monetiziraju ogromne količine podataka koje im manje-više dobrovoljno pružamo.

Pitali smo gospodina Humphreysa da li misli da porodica standarda ISO/IEC 27000 daje odgovore na te nepoznanice: „Nedavno je potkomitet SC 27 započeo razvoj standarda ISO/IEC 27552, koji proširuje standard ISO/IEC 27001 za rješavanje specifičnih potreba

za privatnošću”. Trenutno u fazi nacrta, ovaj dokument utvrđuje zahtjeve i formuliše smjernice koje treba slijediti za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje upravljanja zaštitom privatnosti u kontekstu organizacije.

Svaka prijetnja privatnosti, finansijama ili ugledu osobe ili kompanije narušava naše povjerenje i mijenja naše ponašanje i na internetu, i u stvarnom životu. ISO/IEC 27000 porodica standarda ima ključnu misiju: da nam omogući napredovanje. Dok je sve veća digitalizacija naših života razlog za zabrinutost, ohrabrujuće je znati da možemo računati na ovu porodicu standarda koji regulišu sisteme upravljanja sigurnošću informacija i da globalna grupa eksperata, kao što je i gospodin Humphreys, radi na tome da uvijek budemo korak ispred.

CILJ: SPASITI ŽIVOTE

Autor: Clare Naden - ISOFocus #133

Svake godine se širom svijeta daje oko 16 milijardi injekcija[1], a svaka nosi sa sobom rizik od prenošenja bolesti. Ponovna upotreba špriceva eksponencijalno povećava taj rizik. ISO se bavi ovim problemom tako što je izradio standarde za špriceve za jednokratnu upotrebu i definisao niz zahtjeva za sprečavanje nenamjernih povreda. Neki od tih standarda se ažuriraju kako bi još više odgovarali svojoj svrsi.

U studiji iz 2014. godine, objavljenoj pod pokroviteljstvom Svjetske zdravstvene organizacije - SZO (World Health Organization – WHO), koja se fokusirala na najnovije dostupne podatke, procijenjeno je da je u 2010. godini do 1,7 miliona ljudi zaraženo virusom hepatitisa B (HBV), do 315.000 virusom hepatitisa C (HCV) i čak 33.800 HIV-om kao rezultat upotrebe rizične injekcije. Dok se u razvijenom svijetu većina injekcija daje bezbjedno, prakse davanja injekcije širom svijeta se veoma razlikuju, a ponovna upotreba opreme za ubrizgavanje, loše rukovanje iglama nakon upotrebe i njihovo nedovoljno čišćenje i dalje predstavlja problem u nekim regionima.

Ovaj fenomen ne predstavlja ništa novo. Još 2000. godine SZO je pokrenula program za sigurnost injekcija i uspostavila Globalnu mrežu za sigurnost injekcija (SIGN), s namjerom da uspostavi sigurnu i odgovarajuću praksu upotrebe injekcija na globalnom nivou. Na početku programa smatralo se da je oko 40% injekcija dato s ponovno upotrijebljenom opremom za ubrizgavanje injekcija, što je rezultiralo milionima novih slučajeva HBV i HCV infekcije i stotinama hiljada slučajeva HIV-a.

[1] WHO tabela sigurnosti injekcija.

Inicijativa SZO-a dovela je do razvoja mnogih novih modela špriceva za koje se tvrdilo da će onemogućiti da se špric koristi nakon prve upotrebe. Međutim, nisu svi ti modeli postigli svoj cilj tj. jednokratnu upotrebu. ISO je već objavio standarde za konvencionalne tipove špriceva sa sistemom za samouništavanje, tako da se činilo sasvim prirodnim da se serija proširi novim standardima za špriceve s takvim karakteristikama.

Stručni komitet ISO-a za sisteme ubrizgavanja smatrao je da ponovna upotreba špriceva nije jedini rizik koji treba uzeti u obzir. Infekcija usljed slučajne povrede iglom je također veoma realna opasnost po zdravlje, posebno za zdravstvene radnike i ljude koji dolaze u kontakt s iglama ili drugim oštrim medicinskim predmentima[2] u medicinskim ustanovama ili na javnim mjestima.

Kako do prevencije

Na osnovu inicijativa SZO-a, ekspertska komisija ISO-a za špriceve je istraživala rizike povezane s ponovnom upotrebom špriceva i uzela u obzir činjenicu da se postojeći standardi za potkožne šprice za jednokratnu upotrebu (ISO 7886-1 i ISO 7886-2) i potkožne igle (ISO 7864) nisu posebno bavili rizikom od ponovne upotrebe. Komitet se složio da razvije nove standarde za smanjenje tih rizika i na taj način spriječi širenje smrtonosnih bolesti kao što su HBV, HCV i HIV.

Iako je rad na standardizaciji u ovoj oblasti započeo prije mnogo godina, postoji stalna potreba za borbom protiv nesigurnih praksi ubrizgavanja na globalnom nivou. Nije slučajno da je ukidanje špriceva s mogućnošću ponovne upotrebe ključni cilj u Agendi ciljeva održivog razvoja Ujedinjenih nacija (UN SDGs), koji su dio UN-ove Agende za održivi razvoj za 2030.godinu koju su svjetski lideri usvojili 2015.godinu Cilj održivog razvoja 3 o dobrom zdravlju i blagostanju planira da će do 2030. godine „okončati epidemiju AIDS-a, tuberkuloze, malarije i zanemarenih tropskih bolesti, i boriti se protiv hepatitisa, bolesti koje se prenose vodom i drugih zaraznih bolesti". Inicijative za sprečavanje ponovne upotrebe špriceva i izbjegavanje nenamjernih povreda iglom jasno će doprinijeti postizanju ovog cilja.

William Dierick, koji je prvobitno vodio aktivnosti na razvoju standarda za sisteme samouništavanja špriceva kao dio ISO-ovog tehničkog komiteta ISO/TC 84, *Uređaji za administriranje medicinskih proizvoda i katetera*, kaže da je filozofija komiteta bila – i ostala – da se fokusira na sigurnost pacijenata i osigura da su zahtjevi standarda što je moguće ažuriraniji. „Naš cilj je da budemo prisutni tamo gdje postoje nova tehnološka poboljšanja ili karakteristike, ili novi tipovi medicinskih proizvoda, kako bismo prilagodili standarde i osigurali da pacijenti dobiju najsigurniju i najefikasniju njegu", kaže on.

„Zbog toga u razvoj naših standarda uključujemo sve strane, uključujući zdravstvene organe kao što su Agencija za hranu i lijekove (FDA), međunarodne organizacije kao što su SZO i UNICEF, proizvođače lijekova i uređaja i krajnje korisnike kao što su pacijenti i zdravstveni radnici", dodaje on.

Ovaj inkluzivni pristup je jedan od razloga zašto je Danski institut za standardizaciju, koji vodi sekretarijat ISO/TC 84, pokrenuo twinning projekt s Institutom za standardizaciju Zimbabvea (SAZ) radi uključivanja afričkog kontinenta u razvoj standarda za sigurnije medicinske uređaje. To partnerstvo kojim je predsjedavao Zimbabve dovelo je do uspješnog izdavanja standarda ISO 23908 za zaštitu od oštrih medicinskih predmeta i

[2] Oštri medicinski predmet: medicinski instrument (skalpel, lanceta ili igla sa špricom) koji je oštar ili se razbijanjem može polomiti na oštre dijelove.

standarda ISO 23907 za kontejnere za odlaganje oštrih medicinskih predmeta, koji su dopunili druge standarde relevantne u ovoj oblasti, kao što su ISO 21649 (injektori bez igle) i standardi ISO serije 7886 (špricevi za jednokratnu upotrebu).

Sigurnije injekcije

Postoje mnogi razlozi za poboljšanje sigurnosti primjene injekcija. Cijena i hronična nestašica medicinskih sredstava zahtijevaju očajničke mjere, uključujući i sklonost za ponovnu upotrebu opreme za jednokratnu upotrebu. Štaviše, naučne studije pokazuju da davanje injekcija ne predstavlja samo rizik za medicinsko osoblje, već i za pomoćno osoblje kao što su čistači, radnici na pranju rublja ili laboratorijski tehničari.

U pokušaju da smanji rizik od povreda i prenošenja bolesti, SZO je 2015. godine pokrenuo novu politiku o sigurnosti ubrizgavanja, pozivajući međunarodnu zajednicu da do 2020. godine pređe na sigurnosno dizajnirane špriceve. Objavili su veoma detaljne smjernice za sigurnost šprica, koje su potcrtale brojne sigurnosne karakteristike špriceva koji ne samo da štite osobe koje primaju injekcije, već i zdravstvenog radnika koji ih daje.

SZO je naglasila da prijenos infekcije nije ograničen samo na zemlje u razvoju, jer se ponovna upotreba špriceva praktikuje na mnogim mjestima. „Usvajanje sigurnih šprica je apsolutno neophodno da bi se ljudi širom svijeta zaštitili od zaraze HIV-om, hepatitisom i drugim bolestima. To bi trebalo da bude hitan prioritet za sve zemlje”, rekao je dr. Gottfried Hirnschall, direktor odjela za HIV/AIDS u SZO-u, u saopštenju za javnost koje je objavljeno povodom objavljivanja smjernica.

Standardni jezik

Objavljene 2015. godine, *SZO smjernice o upotrebi sigurnih injekcionih špriceva za intramuskularne, intradermalne i potkožne injekcije u zdravstvenim ustanovama* daju osnovna pravila za špriceve s karakteristikama za „zaštitu od povreda od oštrih medicinskih predmeta”. Odnose se na definicije iz standarda ISO 23908, *Zaštitne mjere od povreda s iglama – Zahtjevi i metode ispitivanja – Mogućnosti zaštite od povrede hipodermalnim igalama za jednokratnu upotrebu, nastavaka za katetere i igala za uzimanje uzoraka krvi*, koji uspostavlja međunarodno dogovorene minimalne standarde za smanjenje rizika od povreda oštrim medicinskim predmetima. Osim toga, serija ISO 7886, koja definiše svojstva i zahtjeve za sterilne jednokratne potkožne šprice, također obuhvata automatske injekcije (ISO 7886-3) i špriceve sa sistemom samouništavanja (ISO 7886-4). To ga čini veoma korisnim alatom kako za proizvođače koji ih proizvode, tako i za korisnike koji mogu da se opuste, znajući da šprice ispunjavaju minimalne zahtjeve za kvalitet i sigurnost.

ISO standardi se redovno ažuriraju kako bi se osiguralo da zadovoljavaju potrebe proizvođača i korisnika, i uzimaju u obzir sve nove tehnologije koje će doprinijeti smanjenju rizika od prenosivih bolesti.

Pogled u budućnost

Čitav proces se ovdje ne zaustavlja. William Dierick kaže da komitet kontinuirano razvija i procjenjuje svoj rad kako bi razvio standarde koji zadovoljavaju potrebe korištenja injekcija u sve većem broju različitih okruženja. „Također imamo i druge standarde koji se

fokusiraju na zahtjeve za uređaje koje koriste određene grupe, kao što su bolesnici s oštećenim vidom i određene dobne grupe”, dodaje on.

Pored toga, naši standardi su prvobitno bili fokusirani na uređaje namijenjene zdravstvenim radnicima, ali s povećanim brojem uređaja za samostalno ubrizgavanje, odlučili smo proširiti svoj rad tako da uključimo pen-injektore, auto injektore i injektore koji se nose na tijelu. Ova inicijativa će omogućiti efikasnije i praktičnije ubrizgavanje medicinskih proizvoda, od kojih će sistemi zdravstvene zaštite i pacijenti imati velike koristi”.

Čitav taj proces će koristiti zemljama koje se približavaju krajnjem roku do 2020. godine, koji je postavio SZO i koji ih treba podstaknuti da pređu na sigurne špriceve kad god je to moguće. Također bi trebalo da pomogne u postizanju nekih od ciljeva održivog razvoja UN-a, dok spašavanje života u zemljama u kojima je ponovna upotreba šprice i dalje visoka ostaje široko rasprostranjena praksa.

NOVI POČETAK BORBE ZA KONTROLU BOLESTI

Autor: Ann Brady - ISOFocus #133

U našem sve složenijem, međusobno povezanom svijetu, sa zdravstvenim sistemima koji se suočavaju s novim izazovima i stresovima, upravljanje rizikom u zdravstvenom sektoru je važnije nego ikada. Tri ISO standarda igraju značajnu ulogu u usklađivanju kliničkog kvaliteta sa sigurnošću pacijenta i najboljom praksom, kako bi im pomogli ne samo da se nose s rizicima, već i da ih spriječe.

Samo srećnici prožive svoj život u dobrom zdravlju, bez bolova i bez svega onoga što nosi starenje. Mnogi od nas nemaju sreću da izbjegnu bolne i iscrpljujuće tegobe, kao što su bolovi u zglobovima koji u krajnjoj liniji zahtijevaju umjetne proteze, a većina nas, prije ili kasnije, mora se obratiti zdravstvenim radnicima i zdravstvenom sektoru radi liječenja.

Čini nam se normalnim da očekujemo da će nas ta rješenja i medicinski tretmani vratiti na noge i pomoći nam da se osjećamo bolje i vratimo se svakodnevnom životu. Kada smo najugroženiji, oslanjamo se na zdravstvene stručnjake koji, sa svoje strane, nastoje obezbijediti da sigurnost pacijenata bude na prvom mjestu i koji teže tome da najbolje prakse pomognu u smanjenju medicinskih pogrešaka.

Troškovi zdravstvene zaštite

Sektor zdravstvene zaštite je jedan od najbrže rastućih sektora u svijetu, koji obuhvata medicinu, biotehnologiju, medicinske uređaje, usluge i farmaceutske proizvode. Istraživanje The Economist Intelligence Unit i Deloitte ukazuje da, iako je globalna godišnja potrošnja za zdravstvo dostigla 707.700 milijardi dolara u 2015. godini, ta će se cifra do 2020. godine povećati na 873.400 milijardi dolara. Podaci pokazuju da će „povećanje starije populacije u SAD-u i inostranstvu, zajedno s visokim prosječnim troškovima pružanja kvalitetne zdravstvene zaštite članovima ovih grupa, dovesti do povećanja troškova u zdravstvu".

Prema magazinu Forbes, između 2015. i 2030. godine se očekuje da će broj ljudi u svijetu u dobi od 60 i više godina porasti za 56%, odnosno s nešto više od 900 miliona na skoro 1,5 milijardi ljudi. Predviđa se da će do 2050. godine globalna populacija starijih od 60 godina skočiti na 2 milijarde. Samo u SAD-u broj građana starijih od 65 godina do 2060.godine treba da dostigne cifru od skoro 100 miliona.

Suočeni s tako velikim procentom starijih ljudi, s bolestima povezanim sa starenjem, zdravstveni sektor će se suočiti s velikim izazovima. Stanovništvo širom svijeta stari – ali ne na isti način. Ishrana na bazi visokoprerađene hrane dovela je do povećanja bolesti na Zapadu, kao što su gojaznost, srčane bolesti i dijabetes, a zdravstvena industrija će morati da pronađe kreativna rješenja za problem hroničnih bolesti.

Kada su zdravstveni sistemi preopterećeni, mora se voditi računa da se sigurnost pacijenata održi na istom visokom nivou. Ipak, greške i neželjeni događaji su uvijek mogući u medicinskim procedurama. Podaci i statistika Svjetske zdravstvene organizacije (SZO) za Evropsku uniju, naprimjer, pokazuju da se „medicinske greške i neželjeni događaji povezani sa zdravstvenom zaštitom javljaju u 8% do 12% hospitalizacija". Prema SZO-u, infekcije povezane s njegom također uzimaju svoj danak, procenjuje se da u prosjeku jedan od 20 pacijenata na bolničkom liječenju oboli svake godine (4,1 milion pacijenata). Nacionalna kancelarija za reviziju u Velikoj Britaniji je procijenila da troškovi takvih infekcija iznose jednu milijardu funti godišnje.

Nema mjesta za greške

U SAD-u situacija nije ništa bolja. Studija koju su proveli doktori Makary i Daniel izazvala je kontroverzu kada je tvrdila da je medicinska greška treći vodeći uzrok smrti u ovoj zemlji. Međutim, jedan od pozitivnih rezultata ove kontroverze je to što je ona bacila novo svjetlo na ozbiljnu temu, čineći sigurnost pacijenta javnom brigom. To pitanje je nedavno ponovo izneseno na vidjelo objavljivanjem *Dosijea o implantatima*, nakon globalne istrage Međunarodnog konzorcija istraživačkih novinara (International Consortium of Investigative Journalists – ICIJ) o medicinskim implantatima – kao što su metalni kukovi, vaginalne mreže i pejsmejkeri – i njihov utjecaj na pacijente.

Istraga je provedena zbog zabrinutosti o adekvatnosti propisa koji se primjenjuju za medicinske implantate, od kojih neki, kako se tvrdi, nisu bili testirani prije nego što su se pojavili na tržištu. Međutim, ti medicinski uređaji postaju sve važniji u oblasti zdravstvene zaštite i mogu značajno poboljšati živote ljudi, posebno starijih. U eri takozvane Četvrte industrijske revolucije, nove tehnologije ne samo da omogućavaju inovacije u oblasti medicinskih implantata i uređaja, već i izazivaju zabrinutost zbog *cyber* sigurnosti i privatnosti podataka i čine upravljanje rizikom u zdravstvu još složenijim.
Sve to naglašava potrebu za efikasnim sistemima upravljanja rizikom. Koja sredstva su nam na raspolaganju da bi smanjili rizike povezane s medicinskim sredstvima, uključujući i

rizik od ljudske greške? Mnogi ISO standardi se bave upravljanjem rizicima u zdravstvenoj industriji – a tri su istaknuta u ovom članku. ISO 14971 je standard koji se bavi primjenom upravljanja rizikom u dizajniranju i proizvodnji medicinskih uređaja. Prema Jos van Vroonhovenu, šefu sektora za standardizaciju u multinacionalnoj elektronskoj kompaniji Philips, regulatorni organi su globalno prepoznali ovaj standard kao najbolji standard za upravljanje rizicima medicinskih uređaja. To je, kaže on, jedna od ključnih prednosti korištenja ISO 14971 za kompanije kao što je Philips.

Smanjiti izazove

Van Vroonhoven smatra da je trend uvođenja strožijih regulatornih zahtjeva veliki izazov za industriju. On kao primjer navodi Uredbu Evropske unije o medicinskim uređajima (EU) 2017/745 koja, kaže on, „postavlja sve strožije zahtjeve, ne samo u procesu upravljanja rizicima, već između ostalog, i u vezi s aktivnostima izvještavanja i nadzora nakon plasiranja na tržište". On je rekao da će u narednom izdanju ISO 14971 biti dati precizniji i detaljniji zahtjevi za proces upravljanja rizicima, koji su u skladu s promjenama regulatornih zahtjeva. „Prema tome, ISO 14971 će pomoći proizvođačima da pokažu usklađenost s regulatornim zahtjevima za upravljanje rizikom", dodaje on.

Van Vroonhoven kaže da će revidirani ISO 14971 ostati globalno priznati standard za upravljanje rizicima vezanim za medicinske uređaje i da je „opis procesa upravljanja rizikom poboljšan u nekoliko aspekata". Jedno poboljšanje, tvrdi on, odnosi se na precizniji opis procjene ukupnog preostalog rizika. „Objašnjeno je da doprinosi svih preostalih rizika moraju biti uzeti u obzir i procijenjeni u odnosu na koristi od predviđene upotrebe medicinskog uređaja".

Upravljanje rizikom u zdravstvenoj industriji se također proširuje na medicinske laboratorije, koje su ključna komponenta u zdravstvu. U tim laboratorijama se obavljaju osnovne aktivnosti na testiranju kliničkih uzoraka kako bi se dobile informacije o zdravstvenom stanju pacijenta u vezi s dijagnozom, liječenjem i prevencijom bolesti. Kredibilitet medicinskih laboratorija je najvažniji za zdravlje i sigurnost pacijenata koji se oslanjaju na usluge testiranja koje pružaju te laboratorije.

Drugi standard ISO 22367 (koji se trenutno razvija), bavi se smanjenjem grešaka u medicinskim laboratorijama kroz upravljanje rizikom i kroz kontinuirano poboljšanje. Willem Huisman, ekspert za medicinske laboratorije za kliničku hemiju u Evropi, stručnjak je za ovaj standard koji procjenjuje i integriše sve revizije koje je predložio projektni tim i odgovara na komentare primljene tokom različitih faza glasanja.

Huisman objašnjava da novo izdanje ISO 22367 u svojim dodacima dosta detaljno opisuje kako se upravljanje rizicima može primijeniti u medicinskoj laboratoriji. „Standard pomaže da razumijemo", kaže on, „kako pristup upravljanja rizikom može zaista doprinijeti sigurnosti pacijenata bez trošenja više novca i truda nego što je potrebno kao i da se usredsredimo na procese koji su najrizičniji." On navodi kao primjer učestalost internih uzoraka kontrole kvaliteta: česte tamo gde je potrebno i rjeđe gdje je to moguće. „Krajnji rezultati", kaže on, „mogu dovesti do smanjenja ukupnih troškova uz bolji kvalitet za pacijente".

Sve o tehnologiji

In vitro dijagnostika je važan sektor globalne zdravstvene industrije, koji ubrzano raste zahvaljujući tehnološkom napretku. Ovi medicinski uređaji i pribor pomažu u otkrivanju infekcija, dijagnosticiranju medicinskog stanja i sprečavanju bolesti. Huisman kaže da je

novi standard eksplicitniji i više u skladu sa standardom upravljanja rizikom za proizvođače *in vitro* dijagnostičkih medicinskih uređaja, naglašavajući zajedničku odgovornost za pouzdane laboratorijske rezultate. On također ističe da je naziv standarda „namjerno promijenjen u upravljanje rizikom za medicinske laboratorije umjesto ispitivanje u medicinskoj laboratoriji". To jasno ukazuje, kaže on, na značaj procesa koji prethode laboratorijskom ispitivanju (pravilno uzimanje uzoraka; uslovi transporta).

Huisman dodaje: „Novi standard ISO 22367 jasno će pokazati medicinskim laboratorijama kako će koncept upravljanja rizicima pomoći da se usredsredimo na sve laboratorijske procese koji to zahtijevaju, kako bi pružili usluge koje njihovi pacijenti zaslužuju. To pomaže laboratorijama da postanu profitabilnije i time poboljšaju dobrobit šire javnosti.

Treći standard, ISO 35001, koji je u fazi razvoja, fokusira se na upravljanje biološkim rizicima, odnosno upravljanje rizicima s kojima se organizacije suočavaju kada se bave biološkim agensima i toksinima. Pored proizvođača *in vitro* medicinskih sredstava, relevantne organizacije uključuju i medicinske centre, bolnice i klinike, univerzitete i istraživačke institute, veterinarske dijagnostičke laboratorije i objekte za smještaj životinja. Garry Burns, konsultant za biološku sigurnost i biobezbjednost i vođa radne grupe WG 5, *Laboratorijsko upravljanje biološkim rizicima*, tehničkog komiteta ISO/TC 212, *Klinička laboratorijska ispitivanja i in vitro dijagnostički ispitni sistemi,* naglašava brz rast biotehnoloških aplikacija, posebno u zemljama u razvoju: „Tehnički kapaciteti koji su ranije bili koncentrisani u visokorazvijenim zemljama sve više se koriste i u drugim zemljama širom svijeta. Ta ekspanzija je u velikoj mjeri posljedica potrebe za borbom protiv zaraznih bolesti prirodnog porijekla, koje ne poznaju nacionalne granice".

Borba protiv toksina i drugih rizika

U cilju rješavanja tih rizika, Burns napominje da će predloženi standard pomoći organizacijama da „kontinuirano poboljšavaju performanse i poštuju zakonske zahtjeve kroz dobrovoljnu politiku i procese upravljanja biološkim rizicima; implementiraju globalno prihvaćene pristupe za identifikaciju i kontrolu bioloških rizika; prate i ocjenjuju djelotvornost mjera kontrole bioloških rizika; i pomažu menadžmentu u donošenju odluka vezanih za te rizike".

Druge koristi za organizacije u implementaciji standarda, kaže on, uključuju smanjenje stope nezgoda i incidenata, usklađenost sa zakonskim obavezama i sposobnost da se vanjskim partnerima pokaže posvećenost visokom standardu u oblasti upravljanja biološkim rizicima. Još jedna prednost je da će „organizacije imati fleksibilnost da implementiraju standard na način koji je srazmjeran njihovoj veličini i složenosti" – što je dobra vijest za male i velike organizacije.

Kao što Burns kaže: „Rizici se stalno razvijaju, kako se novi patogeni neprestano pojavljuju". On navodi nedavne primjere nastalih bioloških agenasa koji su prouzrokovali izbijanje epidemija kod ljudi, uključujući „nekoliko patogenih sojeva virusa influence A (H1N1, H5N1 i H7N9), novi koronavirus koji je uzročnik srednjeistočnog respiratornog sindroma (MERS) i novi koronavirus koji je bio uzrok teškog akutnog respiratornog sindroma (SARS)".

Kako se broj organizacija koje rade s biološkim agensima i toksinima povećava i kako međunarodna saradnja među ovim organizacijama nastavlja rasti, Burns kaže da će se nastaviti i povećati potražnja za međunarodnim standardom za upravljanje biorizicima.

NOVOSTI

Pametna proizvodnja: novi ISO vodič za smanjenje rizika od *cyber* napada na mašine

Autor: Clare Naden

U današnjem sve povezanijem svijetu IT sigurnost se tiče ne samo naših podataka već i praktično svega što se pokreće – uključujući mašine. *Cyber* napadi ili IT kvarovi tokom proizvodnje mogu predstavljati rizike za postojeće sigurnosne mjere i tako utjecati na proizvodnju i ljude. Upravo su objavljene nove međunarodne smjernice za identifikaciju i rješavanje tih rizika.

„Pametna" proizvodnja, ili proizvodnja koja koristi internet i digitalne tehnologije, omogućava besprijekornu proizvodnju i integraciju duž čitavog lanca vrijednosti. Također omogućava daljinsko upravljanje parametrima – kao što su brzina, sila i temperatura. Ova vrsta proizvodnje ima mnogostruke prednosti, kao što je i mogućnost praćenja performansi, ali i povećava rizik od prijetnji IT sigurnosti.

Povećanje brzine ili snage mašine na opasne nivoe, ili smanjenje temperature kuhanja koja dovodi do kontaminacije hrane, samo su neki od primjera gdje *cyber* napadi ne samo da remete proizvodnju, već predstavljaju ozbiljan rizik za ljude. Srećom, novoobjavljeni ISO tehnički izvještaj (TR) pomoći će proizvođačima da se pripreme i ublaže takve rizike.

Tehnički izvještaj ISO/TR 22100-4, *Sigurnost mašina – Veza sa ISO 12100 – Dio 4: Smjernice proizvođačima mašina za razmatranje aspekata vezanih za IT-sigurnost (cyber sigurnost)*, osmišljen je da pomogne proizvođačima mašina da prepoznaju i odgovore na IT sigurnosne prijetnje koje mogu utjecati na sigurnost njihovog proizvoda. Njime se dopunjuje vodeći ISO standard za sigurnost mašina, ISO 12100, *Sigurnost mašina – Opšti principi za projektovanje – Procjena i smanjivanje rizika*, koji uspostavlja osnovne principe za procjenu rizika, analizu opasnosti i zahtjeve za dokumentaciju.

Otto Görnemann, predsjedavajući tehničkog komiteta ISO-a zaduženog za izradu ovog tehničkog izvještaja, kaže da se sigurnost mašina i *cyber* sigurnost uveliko razlikuju u smislu njihovih ciljeva, metoda i mjera, dok su u proizvodnji neraskidivo povezani.

„Tehnički izvještaj ISO/TR 22100-4 će pomoći proizvođačima mašina da integrišu odnos između *cyber* sigurnost i sigurnosti mašina", rekao je on.

„Ovim dokumentom će se obuhvatiti aspekti kao što su tipovi komponenti koje bi mogle biti potencijalne mete za *cyber* napade, dizajn mašine kako bi se smanjila njihova ranjivost na takve napade i informacije za operatera mašine o mogućim prijetnjama."

Tehnički izvještaj ISO/TR 22100-4 izradio je ISO-ov tehnički komitet ISO/TC 199, *Sigurnost mašina*, čiji sekretarijat vodi DIN, član ISO-a za Njemačku. Dostupan je kod Instituta za standardizaciju BiH ili preko ISO prodavnice.

Snažnija zaštita podataka s ažuriranim smjernicama za procjenu kontrola za sigurnost informacija

Autor: Clare Naden

Softverski napadi, krađa intelektualne svojine ili sabotaža samo su neki od mnogih rizika po informacionu sigurnost s kojima se organizacije suočavaju. A posljedice mogu biti ogromne. Većina organizacija ima uspostavljene kontrole za zaštitu, ali kako možemo osigurati da su te kontrole dovoljne? Upravo su ažurirane međunarodne referentne smjernice za procjenu kontrola za sigurnost informacija.

Za svaku organizaciju informacije su jedno od najvrednijih sredstava, a troškovi kršenja podataka mogu biti veoma visoki, kako u smislu gubitka posla tako i u smislu oporavka od štete. Stoga, postojeće kontrole moraju biti dovoljno rigorozne da bi zaštitile ovu imovinu i redovno nadzirane kako bi se uzeli u obzir promjenjivi rizici.

Standard ISO/IEC TS 27008, *Informaciona tehnologija – Sigurnosne tehnike – Smjernice za procjenu kontrola sigurnosti informacija*, koji je razvio ISO i Međunarodna komisija za elektrotehniku (IEC), daje smjernice za procjenu uspostavljenih kontrolnih mjera kako bi se osiguralo da su one odgovarajuće, djelotvorne, efikasne i u skladu s ciljevima kompanije.

Nedavno je ažurirana ova tehnička specifikacija (TS) kako bi se uskladila s novim izdanjima drugih komplementarnih standarda za upravljanje informacijskom sigurnošću, odnosno ISO/IEC 27000 (pregled i rječnik), ISO/IEC 27001 (zahtjevi) i ISO/IEC 27002 (kodeks prakse za kontrolu sigurnosti informacija).

Prof. Edward Humphreys, vođa radne grupe koja je razvila standard, rekao je da će ISO/IEC TS 27008 pomoći organizacijama da procijene i revidiraju svoje trenutne kontrolne mjere kojima se upravlja kroz implementaciju standarda ISO/IEC 27001.

„U svijetu u kojem *cyber* napadi nisu samo sve učestaliji, već i sve teži za otkrivanje i sprečavanje, procjenjivanje i revidiranje uspostavljenih sigurnosnih kontrolnih mjera treba redovno obavljati i da bude suštinski aspekt poslovnih procesa organizacije", rekao je on.

Standard ISO/IEC TS 27008 može pomoći organizacijama da budu sigurne da su njihove kontrolne mjere efikasne, adekvatne i prikladne za ublažavanje rizika s kojima se organizacija suočava."

Standard ISO/IEC TS 27008 koristi organizacijama svih vrsta i veličina, bilo javnim, privatnim ili neprofitnim, i dopunjuje sistem upravljanja informacijskom sigurnošću definisan u ISO/IEC 27001.

Tehničku specifikaciju je razvio ISO-ov tehnički komitet ISO/IEC JTC 1, *Informaciona sigurnost*, potkomitet SC 27, *IT sigurnosne tehnike*, čiji sekretarijat vodi DIN, član ISO-a za Njemačku. Može se kupiti kod Instituta za standardizaciju BiH ili preko ISO prodavnice.

*****

Bolja izgradnja s novim međunarodnim standardima za BIM

Autor: Clare Naden

Građevinska industrija je u procvatu širom svijeta, donoseći sa sobom globalne građevinske projekte i potrebu za efikasnim alatima kao što je Modeliranje informacija o građevinama (Building Information Modeling - BIM) za upravljanje informacijama. Upravo je objavljen novi set međunarodnih standarda koji će preko projekata i van utvrđenih granica doprinijeti razvoju BIM-a i koristiti industriji u cjelini.

S demografskim i ekonomskim rastom, raste i potreba za stanovanjem i infrastrukturom, a u prognozi rasta za globalnu građevinsku industriju očekuje se porast od 85% - ili 15,5 milijardi USD – do 2030 godine[1]). Veća izgradnja znači veću potrebu za efikasnim načinima rada, zbog čega BIM pristup zasnovan na 3D modelu u realizaciji građevinskih projekata postaje sve popularniji širom svijeta.

[1] PvC, „Globalna izgradnja 2030: globalna prognoza za građevinsku industriju do 2030".

BIM pruža arhitektima, inženjerima i građevinskim stručnjacima mogućnost da efikasnije planiraju, dizajniraju i upravljaju projektima izgradnje. On je sve popularniji što stvara potrebu za međunarodnim okvirom koji omogućava industriji da radi zajedno preko projekata i mimo nacionalnih granica.

Objavljena su prva dva dijela ISO 19650, *Organizacija i digitalizacija informacija o zgradama i građevinskim objektima, uključujući modeliranje informacija o građevinama (BIM) – Upravljanje informacijama uz korištenje modeliranja informacija o građevinama*, koji daju okvir za upravljanje informacijama kroz zajednički rad korištenjem BIM-a.

Jøns Sjøgren, predsjedavajući ISO-ovog potkomiteta koji je radio na razvoju standarda, rekao je da će standardi omogućiti šire korištenje BIM-a, a time i efikasnije građevinske i infrastrukturne projekte. „ISO 19650 je razvijen na osnovu ispitanog britanskog standarda BS 1192 i javno dostupne specifikacije PAS 1192-2, koji su već pokazali kako mogu pomoći korisnicima da uštede do 22% troškova pri izgradnji", rekao je on.

„Prelazak na međunarodni nivo ne samo da znači učinkovitiju saradnju na globalnim projektima, već omogućava dizajnerima i izvođačima koji rade na svim vrstama građevinskih radova da imaju jasnije i efikasnije upravljanje informacijama."

Budući standardi u seriji uključuju Dio 3 o upravljanju operativnom fazom imovine i Dio 5 koji je posvećen modeliranju informacija o građevinama, izgradnji digitalnih okruženja i pametnog upravljanja imovinom.
Standardi ISO 19650-1 i ISO 19650-2 izradio je ISO-ov tehnički komitet ISO/TC 59, *Građevinski objekti i građevinski radovi*, potkomitet SC 13, *Organizacija i digitalizacija informacija o zgradama i građevinskim objektima*, *uključujući modeliranje informacija o građevinama (BIM)*. Dostupne su kod Instituta za standardiazciju BiH ili preko ISO prodavnice.

*****

Održivi turizam: novi međunarodni standard za pružaoce usluga smještaja

Autor: Clare Naden

Turizam je jedan od najvećih i najbrže rastućih ekonomskih sektora na svijetu. Svake godine milijarde ljudi negdje putuju – a očekuje se da će do 2030. broj turista rasti za 3,3% godišnje. Smještaj za turiste je stoga od ključnog značaja, što znači da je njegov potencijalni utjecaj na održivi razvoj ogroman. Upravo su objavljene nove međunarodne smjernice za smještajne objekte koji će pomoći da se poboljša kvalitet usluge.

Ne samo da turizam raste iz dana u dan, već je to industrija koja promoviše razumijevanje i mir među zemljama i kulturama, osigurava milione radnih mjesta i idealno je mjesto koje može direktno doprinijeti mnogim od 17 ciljeva održivosti Ujedinjenih nacija.

Smještajni kapaciteti igraju vitalnu ulogu u svim turističkim aktivnostima i stoga imaju ogroman potencijal da mogu poboljšati svoj utjecaj na okolinu, promovisati društvenu interakciju i doprinijeti lokalnim ekonomijama na pozitivan način. Ipak, uprkos broju održivih turističkih programa koji postoje širom svijeta, a koje vode organizatori putovanja ili druge organizacije s komercijalnim interesima, nikada nije postojao zaista nepristrasan međunarodni standard za smještaj. Do sada.

Standard ISO 21401, *Turizam i srodne usluge – Sistem upravljanja održivošću smještajnih objekata – Zahtjevi*, specificira ekološke, društvene i ekonomske zahtjeve za implementaciju sistema upravljanja održivošću u turističkom smještaju. On se bavi pitanjima kao što su ljudska prava, zdravlje i sigurnost zaposlenih i gostiju, zaštitom okoline, potrošnjom vode i energije, stvaranjem otpada i razvojem lokalne ekonomije.

Manuel Otero, predsjedavajući tehničkog komiteta ISO-a koji je izradio standard, rekao je da na tržištu postoje brojne inicijative koje bi pružaoci smještaja mogli koristiti da poboljšaju svoje prakse u zaštiti okoline, ali nijedna koja bi takođe integrisala društvene i ekonomske aspekte ili bi bila oslobođena komercijalnih interesa.

„Činjenica da u različitim zemaljama i organizacijama postoji mnoštvo shema za održivi smještaj može takvim objektima otežati da uvide šta im je korisno i pouzdano i kako mogu ispuniti svoje zahtjeve", rekao je on.

„Ovaj međunarodno dogovoreni standard osigurava jasnoću na konfuznom tržištu, odnosi se na sve vrste smještaja i može poslužiti kao alat za poboljšanje održivog upravljanja. On će također pomoći u stimulaciji tržišta za veću održivost kako u sektoru smještaja tako i u turističkoj industriji u cjelini."

Osnivač radne grupe koja je uključena u razvoj standarda Alexandre Garrido dodao je da će oni koji implementiraju sistem upravljanja održivošću baziran na ISO 21401 moći pokazati svojim klijentima i čitavom tržištu da su dio održivog poslovanja.
„Standard ISO 21401 će koristiti smještajnim objektima kako bi ojačali sistem upravljanja i poboljšali reputaciju, pružanjem kvalitetnijih usluga klijentima i poboljšanjem odnosa s dobavljačima, zaposlenicima i lokalnom zajednicom."

Standard ISO 21401 je izradio ISO-ov tehnički komitet ISO/TC 228, *Turizam i srodne usluge*, čiji sekretarijat zajednički vode UNE, član ISO-a za Španiju i INNORPI, član ISO-a za Tunis. Dostupan je kod vašeg nacionalnog člana ISO-a ili preko ISO prodavnice. Saznajte više o ISO/TC 228, *Turizam i srodne usluge*, u ovom kratkom videu: https://www.youtube.com/watch?v=zDkaM4-foQg

*****

Novi ISO međunarodni standard za izvještavanje o ljudskom kapitalu

Autor: Clare Naden

Vrijednost organizacije zavisi od toga koliko vrijede njeni ljudi – zbog toga na radnu snagu kompanije često otpada najveći postotak njenih troškova. Mjerenje isplativosti ulaganja kompanije u zaposlene nije lak zadatak i trebao bi biti olakšan objavljivanjem prvog međunarodnog standarda za izvještavanje o ljudskom kapitalu.

Dobro je poznato da efikasne strategije ljudskih resursa (Human Resources – HR) mogu imati pozitivan utjecaj na učinak organizacije. A s obzirom da troškovi radne snage mogu iznositi i do 70% troškova organizacije, veoma je važno imati relevantnu strategiju.

Postoji mnogo različitih sistema i procesa upravljanja ljudskim resursima koji imaju za cilj maksimiziranje povrata investicija u osoblje, ali oni variraju od kompanije do kompanije i od zemlje do zemlje, što otežava precizno određivanje referentne tačke koje su relevantne na međunarodnom nivou. Novi ISO standard koji je upravo objavljen nudi globalno dogovorene načine da se to postigne.

Standard ISO 30414, *Upravljanje ljudskim resursima – Smjernice za interno i eksterno izvještavanje o ljudskom kapitalu*, prvi je međunarodni standard koji omogućava organizaciji da dobije jasan pregled stvarnog doprinosa svojih zaposlenih. Primjenjuje se na preduzeća svih vrsta i veličina, pruža smjernice o osnovnim oblastima upravljanja ljudskim resursima kao što su organizaciona kultura, regrutovanje i promet, produktivnost, zdravlje i sigurnost i liderstvo.

Dr. Ron McKinley, predsjedavajući ISO-ovog tehničkog komiteta koji je razvio standard, izjavio je da će ISO 30414 omogućiti organizacijama da bolje razumiju svoj utjecaj na zaposlene i pomoći da se maksimizira doprinos zaposlenika dugoročnom uspjehu organizacije.

„Izvještavanje o radnoj snazi se odnosi na promišljanje o tome kako treba razumjeti i procijeniti organizacionu vrijednost, te omogućiti donošenje odluka koje se zasnivaju na više podataka u upravljanju radnom snagom", objasnio je on.

Štaviše, pružanjem niza relevantnih ključnih mjera koje su prepoznatljive na međunarodnom nivou, multinacionalne kompanije mogu lakše prenijeti informacije o ljudskom kapitalu, bolje kontrolisati svoje međunarodne aktivnosti vezane za ljudske resurse i pružiti veću transparentnost svim svojim zainteresovanim stranama ", rekao je on.

„Ali ovaj standard ne odnosi se samo na multinacionalne kompanije. Organizacije svih veličina, uključujući mala i srednja preduzeća, mogu imati koristi od toga da mogu izabrati mjere koje smatraju najrelevantnijima.

Vlade i kreatori politike također imaju koristi od njega, rekao je McKinley, jer stiču više znanja o razvoju ljudskog kapitala u organizacijama svoje zemlje u poređenju s drugim zemljama, što je važno za političke inicijative na tržištu rada.

Standard ISO 30414 razvio je ISO-ov tehnički komitet ISO/TC 260, *Upravljanje ljudskim resursima*, čiji sekretarijat vodi ANSI, član ISO-a za SAD. Može se kupiti kod Instituta za standardizaciju BiH ili preko ISO prodavnice.

*****

Upaljači su postali sigurniji zahvaljujući revidiranim ISO standardima

Autor: Barnaby Lewis

Da bi se smanjio rizik od plamena, ISO je izradio standarde za džepne kao i višenamjenske upaljače s dužom cijevi. U oba slučaja fokusiralo se na sigurnost korisnika.

Bilo da se koriste za paljenje svijeće, ili logorske vatre, upaljači ostaju jedna od najpopularnijih i najkorisnijih sprava svih vremena. S obzirom da se svakodnevno proda nekoliko miliona upaljača, potreba za standardima u ovoj oblasti je neosporna.

Zajednički element za džepne i višenamjenske tipove upaljača je plastični rezervoar ispunjen zapaljivim plinom pod pritiskom. Ovaj rezervoar predstavlja realnu opasnost ako nije dizajniran i proizveden na odgovarajući način. Rizik od nezgoda povezanih sa nestandardizovanim upaljačima potvrđuje i šokantna statistika. Samo u Evropi, upaljači su odgovorni za gotovo 30.000 teških nesreća svake godine. Osim ljudskih troškova, ekonomski utjecaj ovih nesreća iznosi skoro 1 milijardu eura.

Standard ISO 9994 definiše osnovne sigurnosne zahtjeve za džepne upaljače, posebno maksimalnu visinu plamena, otpornost na pad, otpornost na visoke temperature, unutrašnji pritisak i kontinuirano sagorijevanje. Prvi put je objavljen 1989. godine i, kao i svi međunarodni standardi, revidiran je i ažuriran kako bi držao korak s najnovijom tehnologijom. Standard ISO 22702 je prvobitno objavljen 2003. godine kako bi obuhvatio upaljače koji imaju dužu cijev, koji su obično poznati kao višenamjenski upaljači, upaljači za roštilj, upaljači za kamine ili plinske šibice.

Prema Steveu Burkhartu, rukovodiocu projekta i vođi ISO-ove radne grupe zadužene za izradu oba ova međunarodna standarda, nove revizije daju značajan doprinos smanjenju opasnosti. „ISO 9994 sada uključuje zahtjeve za visinu plamena kao i maksimalnu količinu plina koja se može pohraniti, dok ISO 22702 pruža dodatne zahtjeve za ispitivanje koji se odnose na specifičan način na koji se koriste.”

Standard ISO 9994, *Upaljači – Specifikacije o sigurnosti* i ISO 22702, *Višenamjenski upaljači – Specifikacije o sigurnosti*, razvio je tehnički komitet ISO/TC 61, *Plastika*, potkomitet SC 4, *Ponašanje pri gorenju*, čiji sekretarijat vodi BSI, član ISO-a za Veliku Britaniju. Mogu se kupiti kod Instituta za standardizaciju BiH ili preko ISO prodavnice.

IoT Tech Expo Europe 2019

Amsterdam, Holandija, 19-20. juni 2019.

Naučite nešto novo od stručnjaka o decentralizovanoj obradi podataka na rubu mreže tzv. edge computingu, rješenjima IoT povezanosti, 4.0/5.0 industriji, upravljanju objektima i automatizaciji zgrada, pametnim brojilima/pametnim mrežama, izgradnji povezanog lanca snabdijevanja, automatizaciji procesa, infrastrukturi pametnog grada, praćenju i upravljanju imovinom, cloudu, upravljanju IoT podacima i još mnogo toga.

https://www.iottechexpo.com/europe/

Jicable 2019

Deseta Međunarodna konferencija o izolovanim električnim kablovima

Pariz - Versaj, Francuska 23-27. juni 2019

Pridružite se stručnjacima u području istraživanja, industrijskog razvoja, instalacija, rada i dijagnostike u vezi sa izolovanim električnim kablovima i njihovom opremom, od niskonaponskih i specijalnih kablova do kablova za ultra visoki napon i kablova nove tehnologije.

https://www.iottechexpo.com/northamerica/

Početni sastanak CEN-CENELEC fokus grupe za vještačku inteligenciju 24. aprila

Početni sastanak novoosnovane CEN-CENELEC-ove fokus grupe za vještačku inteligenciju održat će se u srijedu, 24. aprila, u sjedištu danskog instituta za standardizaciju u Kopenhagenu, koji vodi sekretarijat grupe.

Tokom jednodnevnog sastanka učesnici će donijeti neke važne odluke za osnivanje grupe, kao što su imenovanje komiteta za izbor vođe grupe i određivanje prioriteta za naredne godine.

CEN-CENELEC-ova Fokus grupa za vještačku inteligenciju (Artificial Intelligence – AI) osnovana je u decembru 2018. godine. Osnovao ju je Tehnički odbor CEN-a i CENELEC-a (Technical Board – BT). Odluka o osnivanju Fokus grupe uslijedila je nakon Radionice o angažmanu zainteresovanih strana „Pouzdana vještačka inteligencija – izgradnja okvira sa standardizacijom" koju su organizovali CEN i CENELEC u septembru 2018. godine, s ciljem pokretanja rasprave na visokom nivou o standardizaciji u oblasti AI-ja i postizanja dogovora o mapi puta za standardizaciju AI-ja do 2020. godine.

Također možete preuzeti i ove dokumente:

- Nacrt dnevnog reda za početni sastanak (pdf)
- CEN-CENELEC mapa puta za standardizaciju AI (pdf)

*****

CEN i CENELEC su objavili dva nova standarda o aspektima materijalne efikasnosti za ekodizajn

Mnoga prirodna bogatstva naše planete iscrpljuju se velikom brzinom. Osim toga, količina gasova koji oštećuju ozonski omotač i uzrokuju klimatske promjene također nastavlja da raste. Da bi pokušala zaustaviti ove efekte, Evropska komisija je uvela niz inicijativa i zakonodavnih mjera, uključujući uvođenje Akcionog plana za kružnu ekonomiju.

Iako je zakonodavstvo osnovno sredstvo za osiguravanje jednakih uslova koji određuju kriterije koje proizvodi moraju ispunjavati, ono obično ne propisuje kako se trebaju mjeriti limiti. Dakle, tu standardi stupaju na scenu. Zakonodavstvo podržano standardima već duže vrijeme omogućava potrošačima korištenje proizvoda koji su energetski efikasniji, čime se smanjuje potrošnja el. energije i smanjuje količina ugljika koji se emituje u atmosferu. Kružna ekonomija će zahtijevati da proizvodi budu štedljiviji u količini materijala koji se koriste, čime se održava vrijednost i korisnost što je duže moguće.

Evropska komisija prepoznaje činjenicu da su evropski standardi osnovni komplementarni instrumenti zakonodavstva EU za kružnu ekonomiju, podržavajući, između ostalog, Uredbe o ekološkom dizajnu i energetskom označavanju. U skladu s tim, Evropska komisija je zatražila od tri evropske organizacije za standardizaciju – CEN-a, CENELEC-a i ETSI-ja – da izrade standarde o efikasnosti materijala koji bi utvrdili buduće zahtjeve za ekološkim dizajnom o, između ostalog, trajnosti, mogućnosti popravljanja i reciklaže proizvoda.

Da bi se odgovorilo na zahtjev za standardizaciju koji je izdala Komisija, odlučeno je da se osnuje zajednički tehnički komitet CEN-CENELEC 10 o proizvodima vezanim za energiju – aspekti efikasnosti materijala za ekološki dizajn (CEN-CLC/JTC 10).

U skladu s mandatom Evropske komisije, CEN-CLC/JTC 10 priprema (s jednim izuzetkom, standardom EN 45558) opće standarde sa širokom primenljivošću kako bi se osigurao zajednički okvir za razvoj budućih standarda koji su specifični za određeni proizvod.

Prva dva standarda koje je razvio CEN-CLC/JTC 10 objavljena su 1. marta 2019. godine. To su:

- EN 45558:2019, *Opća metoda za deklarisanje upotrebe kritičnih sirovina u proizvodima povezanim s energijom*

U samoj srži cirkularnosti i efikasnosti resursa su kritične sirovine, koje su ključne za evropsku ekonomiju i neophodne za održavanje i poboljšanje kvaliteta života. Pružanje informacija o upotrebi kritičnih sirovina (Critical Raw Materials – CRMs) u okviru proizvoda povezanih s energijom olakšat će na taj način prelazak na ekonomiju koja je u većoj mjeri kružna.

Standard EN 45558:2019 pravi razliku između regulisanih i neregulisanih CRM-ova i pomaže korisnicima (proizvođačima i njihovim dobavljačima) da izrade CRM deklaracije, dajući lancu snabdijevanja određeni nivo sigurnosti o tome šta da izvještavaju, kako da izvještavaju kao i standardizovan mehanizam za prijenos podataka kroz lanac snabdijevanja. Da bi se to postiglo, EN 45558 se zasniva na standardu EN IEC 62474 o deklaraciji materijala.

- EN 45559: 2019, *Metode za pružanje informacija o aspektima efikasnosti materijala proizvoda povezanih s energijom*

Da bi društvo, potrošači i industrija maksimizirali potencijal za upotrebu materijala koji se nalazi u proizvodima na efikasan način, potrebno je da imaju odgovarajuće informacije. Takve informacije mogu se dati dobrovoljno ili propisati zakonima. Standard EN 45559 uspostavlja opću metodu, uključujući pravila i formate, za pružanje informacija koje se odnose na aspekte efikasnosti materijala vezanih za energiju.

Ova metoda se može koristiti kao osnova za razvoj publikacija proizvoda u prikupljanju svih relevantnih informacija o aspektima efikasnosti materijala na jedinstven i strukturiran način, uzimajući u obzir ne samo temu efikasnosti materijala, već i osjetljivost podataka, ciljanu publiku i najprikladniju metodu komunikacije.

Prema tome, EN 45559 podržava razvoj efikasne komunikacione strategije za efikasnost materijala, osigurava efikasnu komunikaciju od strane pružalaca informacija i, zauzvrat, povećava vjerovatnoću da ih primaoci tih informacija razumiju na pravi način. Također opisuje kako bi trebalo da se uzme u obzir ciljana publika (krajnji korisnici, profesionalci ili organi za nadzor nad tržištem), zajedno s nivoima osetljivosti podataka, kao i najprikladniji način komunikacije i medija za pružanje informacija o efikasnosti materijala.

Pored toga, ovaj standard je namijenjen tehničkim komitetima za proizvode kao input za razvoj komunikacione strategije u horizontalnim, generičkim, specifičnim proizvodima ili publikacijama grupe proizvoda. CEN i CENELEC su upravo objavili dva nova standarda o aspektima materijalne efikasnosti za ekodizajn.

Ova dva standarda izradio je zajednički tehnički komitet CEN-CENELEC-a 10, čiji sekretarijat vodi NEC, holandski komitet za elektrotehniku.

Poboljšanje života pacijenata na hemodijalizi zahvaljujući EN ISO 23500

Novoodobrena serija standarda EN ISO 23500, *Priprema i upravljanje kvalitetom tečnosti za hemodijalizu i srodne terapije*, bavi se tretmanom vode i proizvodnjom tečnosti za dijalizu. Ova serija standarda trenutno je sastavljena iz četiri dijela, odnosno dijela posvećenog općim zahtjevima (EN ISO 23500-1), opremi za tretman vode za primjenu hemodijalize (EN ISO 23500-2), vodi (EN ISO 23500-3) i koncentratima za hemodijalizu (EN ISO 23500-4).

Odavno je poznato da hemijska i mikrobiološka kontaminacija tečnosti za dijalizu predstavlja za pacijente na hemodijalizi rizik od akutnih i hroničnih problema. Jedan od glavnih izazova bio je uključiti zahtjeve za kvalitet tečnosti u dokument usmjeren na proizvođače opreme za obradu vode ili aparata za hemodijalizu. Upravo ovdje do izražaja dolazi serija standarda EN ISO 23500. Njihov cilj je da pruže korisnicima uputstva za rukovanje vodom i koncentratima i za proizvodnju i nadzor kvaliteta tečnosti za dijalizu koja se koristi za hemodijalizu. Potreba za takvim uputstvima zasniva se na ključnoj ulozi kvaliteta tečnosti za dijalizu u obezbjeđivanju sigurne i efikasne hemodijalize, kao i na prepoznavanju da je svakodnevni kvalitet tečnosti za dijalizu pod kontrolom medicinskih stručnjaka koji daju terapiju.

Ova serija usmjerena je na medicinske stručnjake koji su uključeni u upravljanje ili rutinsku brigu o pacijenatima na hemodijalizi i koji su odgovorni za kvalitet tečnosti za dijalizu. Uzima se u obzir da opremu koja se koristi u različitim fazama pripreme tečnosti za dijalizu obično prodaju specijalizovani prodavači, a stručnjaci za dijalizu su obično odgovorni za održavanje opreme nakon njene instalacije. Prema tome, EN ISO 23500 daje smjernice za kontrolu kvaliteta i održavanje opreme kako bi se osiguralo da je kvalitet tečnosti za dijalizu prihvatljiv u svakom trenutku. Korisniku se preporučuje da se pridržava uputstava proizvođača u vezi s radom i održavanjem opreme. U onim slučajevima u kojima oprema nije nabavljena od specijalizovanog prodavača, odgovornost korisnika je da potvrdi njene performanse i osigura da su dostupni odgovarajući priručnici za rad i održavanje.

Novoodobreni standardi odražavaju napore medicinskih stručnjaka, pacijenata i proizvođača medicinskih uređaja da poboljšaju tretman vode i koncentrata i proizvodnju i nadzor tečnosti za dijalizu koji se koriste u hemodijalizi, kako bi se pacijenti na hemodijalizi zaštitili od neželjenih efekata koji potiču od poznatih hemijskih sredstava i mikrobioloških zagađivača.

Seriju standarda EN ISO 23500 usvojio je na evropskom nivou CEN/TC 205, *Neaktivni medicinski uređaji*, čiji sekretarijat vodi DIN, njemačko nacionalno tijelo za standardizaciju.

*****

Novi CEN standardi: EN 589:2018 – Goriva za motorna vozila – LPG – Zahtjevi i metode ispitivanja

Upotreba tečnog naftnog gasa, mješavine propana i butana, poznatog kao LPG, kao motornog goriva je proteklih godina u stalnom porastu na globalnom nivou, a očekuje se da će još više rasti. Postoji niz razloga za ovaj trend: na primjer, LPG je jeftiniji i lakši za skladištenje i transport od benzina ili dizela. Nadalje, popularnost LPG-a leži u njegovoj (relativnoj) održivosti, jer ima niže stope emisije CO_2 od ostalih fosilnih goriva.

Ova sve veća popularnost, jer je LPG u svakom slučaju gas, zahtijeva stalno usavršavanje i ažuriranje, kako bi se obezbijedilo da su automobili na putu sigurni i da se emisije održavaju što je moguće nižim, u kontekstu tehnologija koje se brzo razvijaju. Nedavno odobreni standard EN 589:2018 – *Goriva za motorna vozila – LPG – Zahtjevi i metode ispitivanja,* ima za cilj da osigura takav okvir. Standard uvodi specifikacije za kvalitet LPG-a za upotrebu u automobilskoj industriji, osiguravajući minimalni nivo kvaliteta širom Evrope. Standard naglašava da je LPG (i njegova moguća varijanta na bazi biomase) izvodljivo alternativno gorivo.

Verzija iz 2018. godine je najnovija verzija standarda. U poređenju s prethodnom verzijom, u EN 589:2018 su date neke tehničke izmjene i pojašnjenja. Primjeri toga su smanjenje granične vrijednosti sumpora na 30 mg/kg, poboljšana zaštita ubrizgivača od ostataka i uvođenje nove oznake za potrošačke informacije.

Važnost ovog ažuriranja leži u činjenici da niži sadržaj sumpora omogućava održavanje prednosti LPG-a kao goriva niske cijene i niske emisije. To je upoređeno sa sve čistijim dizelskim gorivima koja dolaze na tržište. Za tu svrhu razvijena je nova metoda ispitivanja sumpora. Pored toga, tekst standarda omogućava zemljama da, pored standardizovane, izaberu alternativne metode otkrivanja mirisa čime se smanjuju troškovi proizvodnje i održava sigurnost. Pošto je LPG gas, miris gasa mora da bude karakterističan kako bi potrošač ili operater na benzinskoj pumpi mogao otkriti curenje.

EN 589:2018 je pripremio Tehnički komitet CEN/TC 19, *Gasna i tečna goriva, maziva i srodni proizvodi od nafte, sintetičkog i biološkog porijekla*. Sekretarijat TC 19 vodi NEN, holandsko nacionalno tijelo za standardizaciju.

*****

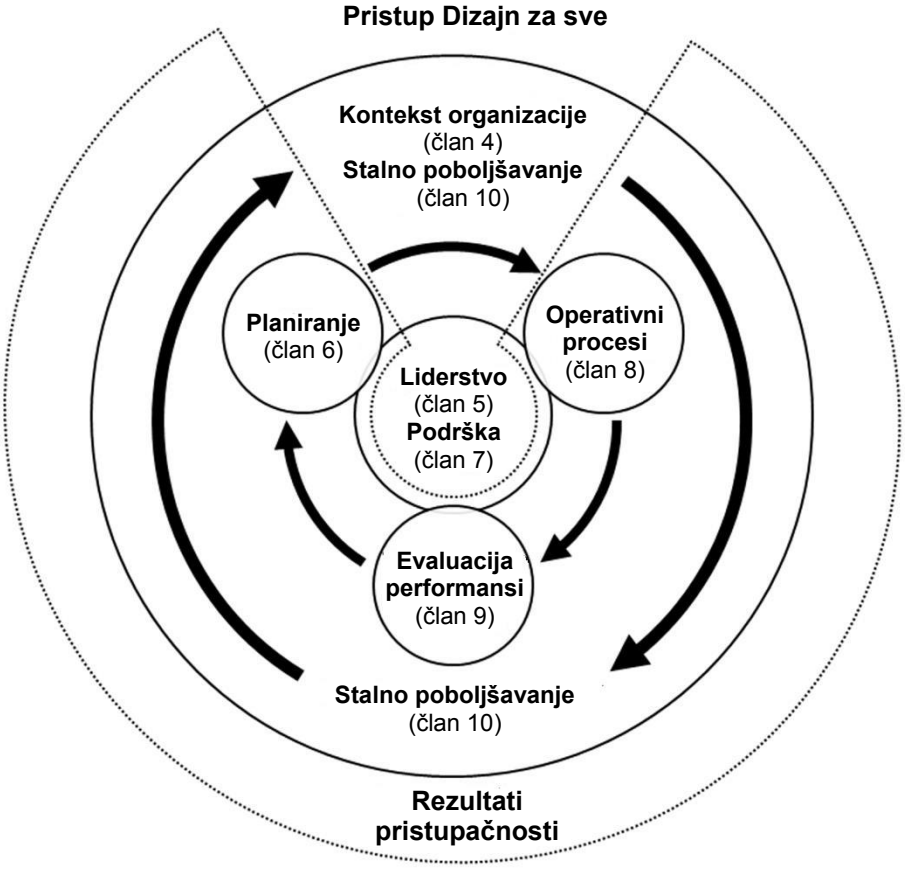
Novi CEN standard: EN 17161:2019 o pristupačnosti

Svaki individualni korisnik ima svoj profil potreba, karakteristika, sposobnosti i preferencija. Tu činjenicu treba uzeti u obzir prilikom razvoja proizvoda i usluga široke potrošnje. Posebno je neophodna dostupnost proizvoda i usluga da bi se osobama s invaliditetom osigurao pristup na ravnopravnoj osnovi s drugima. Pristup „Dizajn za sve" priznaje te varijacije i ima za cilj da zadovolji njihove zahtjeve u najvećoj mogućoj mjeri kako bi se postigli pristupačni proizvodi i usluge.

U tom kontekstu, nedavno objavljeni evropski standard EN 17161:2019, *Dizajn za sve – pristupačnost nakon pristupa dizajnu za sve u proizvodima, proizvodima i uslugama – proširenje spektra korisnika*, ima za cilj da pomogne organizacijama da se usklade s konzistentnim pristupom za rješavanje pristupačnosti za osobe s invaliditetom. On specificira zahtjeve koji mogu omogućiti organizaciji da dizajnira, razvije i osigura proizvode, robu i usluge kojima mogu pristupiti, razumjeti i koristiti najširi mogući krug korisnika, uključujući osobe s invaliditetom.

Ovaj standard je rezultat Zahtjeva za standardizaciju M/473 Evropske komisije da uključi „Dizajn za sve" u relevantne standardizacijske inicijative.

Zahtjevi dati u ovom standardu su generički i imaju namjeru da budu primjenljivi na sve relevantne dijelove svih organizacija, bez obzira na tip, veličinu ili proizvod(e), robu ili uslugu(e).



Slika 1 – Integrisanje pristupa „Dizajn za sve" u kontinuirane procese dizajniranja, razvoja i pružanja proizvoda, robe i usluga

Slika 1 pokazuje, kroz koncentrične krugove, međusobne odnose između procesa, procedura i aktivnosti predviđenih ovim standardom kako bi se postigla pristupačnost zasnovana na primjeni pristupa „Dizajn za sve".

Ovaj evropski standard EN 17161 definiše zahtjeve na način koji je u skladu s organizacionim planiranjem i upravljanjem procesima, tj.

- Razumijevanje konteksta organizacije, potreba i očekivanja zainteresovanih strana, osiguravanje uključivanja osoba s invaliditetom i integracija pristupa „Dizajn za sve" u uspostavljene sisteme i procese;
- Liderstvo, politiku i odgovornosti u podršci pristupu „Dizajn za sve" kako bi se osiguralo postizanje ciljeva pristupačnosti;
- Planiranje ciljeva „Dizajna za sve" i kako ih postići;
- Organizovanje podrške i drugih resursa, uključujući ljude i informacije potrebne za implementaciju pristupa „Dizajn za sve" za postizanje rezultata pristupačnosti;
- Operativne procese vezane za zadovoljavanje potreba korisnika, uključujući osobe s invaliditetom, i razvoj pristupačnih proizvoda i usluga u cijelom lancu, u skladu s pristupom „Dizajn za sve";
- Procese za praćenje, mjerenje, analizu i procjenu efikasnosti i ispravnosti pristupa „Dizajn za sve" i njegovih ishoda pristupačnosti;
- Stalno poboljšanje pristupa i pristupačnosti „Dizajna za sve".

Standard EN 17161 može pomoći organizacijama da se usklade s dosljednim pristupom rješavanja problema pristupačnosti u čitavom nizu aplikacija. Konkretno, standard omogućava organizacijama da se bave „pristupačnosti", kako je navedeno u Konvenciji Ujedinjenih nacija o pravima osoba s invaliditetom.

Prednosti koje organizacije ostvaruju u implementaciji ovog standarda su višestruke.

Pristupačnost može maksimizirati raspon potencijalnih korisnika proizvoda, robe i usluga. On također ima ogromnu društvenu vrijednost, jer može pomoći da se poveća udio stanovništva koje je u stanju potpuno i nezavisno da učestvuje u društvu.

Kako je istakao James Hubbard, vođa EN 17161: „Dok radimo zajedno na postizanju pravednijeg društva, bila je privilegija učestvovati u standardizaciji pristupa koji unapređuje pristupačnost i upotrebljivost za sve, da donosimo bolje informisane odluke o svijetu koji dizajniramo".

Standard EN 17161 izradio je CEN-CENELEC-ov Zajednički tehnički komitet 12 (CEN/CLC/JTC 12) - „Dizajn za sve", čiji sekretarijat vodi NEN, holandsko nacionalno tijelo za standardizaciju uz finansijsku podršku Evropske komisije.

*****

Novi CEN standard: Sigurno prekogranično putovanje, zahvaljujući CEN/TS 17262:2018

Letenje je sve popularniji način putovanja u našem globalizovanom svijetu. Prema procjenama, u 2018. godini komercijalne aviokompanije su redovnim letovima prevezle preko 4,3 milijarde putnika. Međutim, putovanje ne obuhvata samo letenje: milioni ljudi svake godine prelaze državne granice širom svijeta. Stoga je od strateškog značaja obezbijediti da takva vrsta putovanja bude sigurna. Zaista, zahvaljujući tehnološkom razvoju, posljednjih godina su pokrenute mnoge inicijative za poboljšanje provjera na aerodromima (i drugim graničnim prijelazima) i za smanjenje rizika na minimum uz istovremeno osiguravanje što lakšeg putovanja.

Jedno od najnovijih dostignuća u ovoj oblasti u Evropi je tehnička specifikacija CEN/TS 17262:2018, *Lična identifikacija – robusnost protiv napada na biometrijske prezentacije – primjena na evropsku automatsku kontrolu granica*. Objavljen u decembru 2018. godine, CEN/TS 17262 je tehnička specifikacija koja pruža profil primjene na osnovu međunarodnog standarda ISO/IEC 30107, *Informaciona tehnologija – Detekcija napada na biometrijsku prezentaciju – Dio 1: Okvir za automatsku kontrolu granica*. Preciznije, dokument sadrži zahtjeve i preporuke za implementaciju sistema automatske kontrole granica (ABC) u Evropi, na osnovu analize biometrijskih podataka putnika (kao što su slika lica ili otisci prstiju).

Da bi se razumjelo kakav je konkretan doprinos ove tehničke specifikacije, bilo bi korisno napraviti korak nazad i pogledati širi kontekst u kojem se ona primjenjuje. Danas je uobičajeno da države članice EU izdaju elektronske pasoše (ePasoši) koji sadrže pametni čip koji čuva biometrijske podatke. Kako bi se nosile sa sve većim sigurnosnim potrebama, brojne države članice EU-a su uvele sisteme automatizovane kontrole granica (ABC) koji automatizuju granične provjere za građane EU-a koji posjeduju ePasoš.

U praksi, ABC sistem funkcioniše tako što koristi biometrijske podatke koji se čuvaju u ePasošu radi provjere identiteta putnika. Sistem potvrđuje da ePasoš odgovara njegovom vlasniku upoređivanjem biometrijskih karakteristika pojedinca s biometrijskim podacima koji se čuvaju u ePasošu, pretraživanje evidencije granične kontrole (moguće uključujući biometrijsku identifikaciju putnika koji su na listama za praćenje) i konačno određuje prihvatljivost graničnih prijelaza, gdje ne intervenišu graničari. Međutim, graničari i dalje mogu intervenisati kad god nešto nije u redu ili ako nešto ne ide prema planu.

Bez obzira na njihovu preciznost, ABC sistemi su potencijalno podložni napadima na biometrijske prezentacije (poznate i kao spoofing), koji imaju za cilj lažiranje biometrijskih karakteristika kako bi se prevario proces prepoznavanja. Iz tog razloga, uspostavljene su tehnike za automatizovanu detekciju napada na prezentacije (takozvani Presentation Attack Detection (PAD)). Tehnička specifikacija CEN/TS 17262:2018 se fokusira na te tehnike, dajući preporuke za implementaciju PAD mehanizama u Evropi – gdje se međunarodni zahtjevi koje postavlja ISO trebaju prilagoditi određenim nivoima sigurnosti i procesa.

Tehnička specifikacija CEN/TS 17262: 2018 je izradio tehnički komitet CEN/TC 224, *Lična identifikacija i srodni lični uređaji sa sigurnim elementima, sistemima, operacijama i privatnošću u multisektorskom okruženju*. Sekretarijat TC 224 trenutno vodi AFNOR, francusko nacionalno tijelo za standardizaciju.

CWA 17379: 2019: Novi CEN-ov Sporazum s radionice za čistiji zrak

CEN-ov Sporazum s radionice CWA 17379:2019 „Opće smjernice o metodologiji ispitivanja stvarne emisije izduvnih gasova za prikupljanje uporedivih podataka o emisijama" je najnoviji primjer aktivne uloge standardizacije u poboljšanju kvaliteta zraka za sve Evropljane, posebno u urbanim područjima. Prvi put ikada, publikacija pruža metodologiju ispitivanja i smjernice koje se širom Evrope priznaju za provođenje testiranja tokom vožnje automobila i kombija radi prikupljanja podataka o emisijama urbanih azotnih oksida (NOx). Tačnije, metode i zahtjevi opisani u ovom sporazumu osiguravaju da se dosljedno primjenjuje testna procedura provedena pomoću prijenosnih sistema za mjerenje emisija (PEMS). Tako prikupljeni podaci će omogućiti da se performanse emisija različitih vozila, u različitim centrima za testiranje, mogu pravedno porediti.

Od 1. septembra 2017. godine tipska odobrenja za sve novouvedene automobile uključuju testiranje tokom vožnje kao dio najnovijeg standarda za emisije poznatog kao Stvarne emisije izduvnih gasova (RDE – Real Driving Emissions). Ovaj evropski certifikacioni proces je razvijen i primijenjen kako bi se osiguralo da moderna vozila ne prelaze propisane granične vrijednosti emisija izduvnih gasova pri normalnoj upotrebi u različitim uslovima vožnje.

CWA 17379:2019 se zasniva na RDE metodama i opisuje proces za ispitivanje stvarnih emisija izduvnih gasova zabilježenih tokom gradske vožnje, s ciljem da se pravedno porede performanse emisija različitih vozila tokom vožnje. Uvedeni strogi zahtjevi zahtijevaju ispitivanje najmanje dva odgovarajuća primjera za svaki model, tokom tri odvojena putovanja, uključujući najmanje pet putovanja od 10 km na asfaltiranim cestama, s prosječnom brzinom između 20 km/h i 40 km/h.

Rezultati dobijeni upotrebom ove metodologije pružaju transparentnost u pogledu NOx emisija na putevima koja proizvedu vozila tokom gradske vožnje. To omogućava kupcima automobila, kreatorima politika i drugim zainteresovanim stranama da donesu bolje odluke o izboru vozila i posljedicama po kvalitet zraka u gradu.

CEN CWA 17379:2019 objavio je 30. januara 2019. godine CEN/WS 090 „Metoda ispitivanja tokom vožnje za prikupljanje emisija". Sporazum je rezultat kolektivnog dijaloga između više od 40 naučnika, grupa potrošača, kreatora politike, inženjera, nevladinih organizacija i Evropske komisije, čijim radom je predsjedavao Nik Moldena, osnivač Emission Analytics i koosnivač Allow Independent Road-Testing (AIR). Sekretarijat CEN-ovog radnog potkomiteta CEN/WS 090 vodi UNI, italijansko nacionalno tijelo za standardizaciju.

*****

Novi tehnički komitet za javne nabavke (CEN/TC 461)

CEN je nedavno osnovao novi tehnički komitet CEN/TC 461, *Javne nabavke*, s ciljem da se definiše evropski standard za integritet i odgovornosti u kontekstu javnih nabavki u EU. Ova nova standardizacijska aktivnost proizilazi iz diskusija u okviru aktivnosti JIS[1]-a 11 „Povećana upotreba standarda u javnim nabavkama" i potrebe koju su izrazile zainteresovane strane (preduzeća iz EU i javni organi) da se utvrde novi zahtjevi za nabavke koji se zasnivaju na Direktivi 2014/24/EU o javnim nabavkama i Direktivi 2014/25/EU o nabavkama subjekata koji djeluju u sektoru voda, energije, transporta i poštanskih usluga.

Ako ste zainteresovani da učestvujete u radu budućih tehničkih komiteta, kontaktirajte vaše nacionalno tijelo za standardizaciju.

Sekretarijat CEN/TC 461 vodi SIS, švedski institut za standardizaciju.

[1] JIS – Japanska industrijska standardizacija

Novi CENELEC standard: EN 50068:2018 za visokonaponsku sklopnu i upravljačku opremu – Kućišta od kovanog čelika

Brisel, Belgija, 15. 1. 2019.

Upravljačka i sklopna oprema je važno čvorište u modernim elektroenergetskim sistemima i koristi se u različitim aplikacijama. Termini, definisani u standardu EN IEC 60947, odnose se na električne prekidače, osigurače i prekidače koji se koriste za kontrolu, zaštitu i izolaciju električne opreme, kako bi se obezbijedila sigurnost električne infrastrukture i pojedinaca koji ih koriste.

Za izolaciju električnih pogona razvijene su različite tehnike koristeći različite izolacione materijale, od jednostavnog zraka do nafte ili gasa. Jedan od najnaprednijih i najsigurnijih mehanizama sastoji se od korištenja gasa SF6: u ovom rješenju visokonaponski provodnici, prekidači, strujni transformatori i naponski transformatori su uronjeni u gas unutar uzemljenih metalnih kućišta, tzv. podstanice izolovane gasom (GIS).

Nedavno ažurirani evropski standard EN 50068:2018,"*Visokonaponska sklopna i upravljačka oprema – Kućište od kovanog čelika punjeno gasom*", posvećen je obezbjeđivanju visokog nivoa sigurnosti u ovim infrastrukturama. Standard se primjenjuje na specifičnu vrstu GIS-a, zavarena kućišta od kovanog čelika pod pritiskom inertnih gasova, koji se koriste za izolaciju u instalacijama visokonaponske rasklopne opreme s nazivnim naponima iznad 1 kV, pri čemu se upotrijebljeni gas uglavnom bira za dielektrična svojstva.

Standard EN 50068 je iteracija široko rasprostranjenog standarda, koji je prvi put objavljen 1991. godine. U ovom standardu se uvode određena ažuriranja koja su neophodna da bi se uzeo u obzir tehnološki razvoj. Standard se posebno odnosi na uspostavljanje konzistentnih zahtjeva širom Evrope za projektovanje, konstrukciju, ispitivanje, inspekciju i certifikaciju kućišta pod pritiskom koji se koriste u visokonaponskoj sklopnoj i upravljačkoj opremi, na osnovu člana 2. Direktive 2014/68/EU, također poznatoj kao Direktiva za „opremu pod pritiskom". Standard se bavi specifičnim zahtjevima evropske industrije, pomaže joj da ostane konkurentna i smanji prepreke u trgovini unutar jedinstvenog tržišta.

Standard EN 50068 je objavio CLC TC 17AC, čiji sekretarijat vodi DKE, Njemački nacionalni odbor za standardizaciju u elektrotehnici.

*****

Novi CENELEC standard: Sa EN IEC 63000: 2018, evropski standardi za zaštitu okoliša osvajaju svijet

Brisel, Belgija, 31. 1. 2019.

Evropska unija (EU) ima jedno od najnaprednijih zakonodavstava vezano za zaštitu okoliša u svijetu. Ono je zaista neophodan korak za dostizanje ambicioznog cilja: postati lider u zaštiti okoliša. Dobra je vijest, kako za Evropu, tako i za okoliš, da se ponekad evropski standardi ili prakse o pitanjima zaštite okoliša usvajaju na međunarodnom nivou i priznaju kao globalno vrijedni.

To je slučaj s nedavno odobrenim standardom EN IEC 63000. CENELEC je usvojio standard koji je izradio IEC, a koji je posvećen pružanju smjernica o tehničkoj dokumentaciji za procjenu električnih i elektronskih proizvoda (EEE) u pogledu ograničavanja opasnih supstanci. EN IEC 63000 se u velikoj mjeri zasniva na EN 50581:2012, potpuno harmonizovanom evropskom standardu razvijenom radi provedbe Direktive EU 2011/65/EU o ograničenju upotrebe određenih opasnih supstanci u električnoj i elektronskoj opremi , također poznatoj kao RoHS direktiva.

Za više informacija posjetite web stranicu CEN-CENELEC-a.

Institut za standardizaciju BiH je usvojio sljedeće standarde metodom prijevoda u periodu od 1. 1. 2019. do 31. 3. 2019.

Putem Tehničkog komiteta BAS/TC 6, *Oprema za eksplozivne atmosfere*, usvojen je sljedeći standard:

BAS EN 13237:2019, *Potencijalno eksplozivne atmosfere – Termini i definicije za opremu i zaštitne sisteme namijenjene za korištenje u potencijalno eksplozivnim atmosferama, usvojen je motodom prijevoda.*

Bosanskohercegovački standard BAS EN 13237:2018 identičan je evropskom standardu EN 13237:2012, *Potentially explosive atmospheres – Terms and definitions for equipment and protective systems intended for use in potentially explosive atmospheres.*

Ovaj evropski standard izrađen je u svrhu pomoći projektantima, proizvođačima i drugim zainteresiranim stranama pri korištenju usklađenih termina i definicija (rječnika) za opremu i zaštitne sisteme, namijenjene za korištenje u potencijalno eksplozivnim atmosferama.

Putem Tehničkog komiteta BAS/TC 19, *Električne instalacije u zgradama*, usvojeni su sljedeći amandmani:

BAS HD 60364-5-52/A11:2019, *Električne instalacije niskog napona – Dio 5-52: Izbor i montaža elektroopreme – Sistemi ožičenja*

Amandman **BAS HD 60364-5-52/A11:2019** bavi se izborom i montažom sistema ožičenja. Dio 5-52 serije IEC 60364 bavi se izborom i postavljanjem električnog razvoda. Ovaj standard se primjenjuje u općem slučaju i na zaštitne provodnike, dok standard IEC 60364-5-54 sadrži dodatne zahtjeve za te provodnike.

BAS HD 60364-5-54/A11:2019, *Električne instalacije niskog napona – Dio 5-54 : Izbor i ugradnja električne opreme – Sistemi uzemljenja i zaštitni provodnici*

Amandman BAS HD 60364-5-54/A11:2019 razmatra sisteme uzemljenja i zaštitne provodnike, uključujući i provodnike zaštitnog izjednačavanja potencijala, kako bi se zadovoljili zahtjevi za sigurnost električne instalacije.

BAS HD 60364-5-559/A11:2019, *Električne instalacije niskog napona – Dio 5-559: Izbor i ugradnja električne opreme – Svjetiljke i instalacije osvjetljenja*

Zahtjevi amandmana BAS HD 60364-5-559/A11:2019 primjenjuju se na izbor i postavljanje svjetiljki i instalacija za osvjetljenje koje su predviđene da budu dio fiksne instalacije.

Osim navedenih amandmana, usvojen je i sljedeći standard:

BAS HD 60364-5-56:2019, *Električne instalacije niskog napona – Dio 5-56: Izbor i montaža elektroopreme – Sigurnosni sistemi*

Standard BAS HD 60364-5-56:2019 obuhvata opšte zahtjeve za sigurnosne usluge, odabir i montažu električnih sistema napajanja za sigurnosne usluge i izvore električne sigurnosti. Sistemi za napajanje u pripravnosti su izvan okvira ovog dijela. Ovaj dio se ne odnosi na instalacije u opasnim područjima (BE3), za koje su zahtjevi navedeni u IEC 60079-14.

Putem Tehničkog komiteta BAS/TC 44, *Bibliotekarstvo*, usvojen je standard

BAS ISO 3297:2019, *Informacije i dokumentacija – Međunarodni standardni broj serijske publikacije – ISSN.*

Standard definiše i promoviše upotrebu standardnog koda za jedinstvenu identifikaciju serijskih publikacija i ostalih kontinuiranih izvora.

Standard BAS ISO 3297:2019 opisuje mehanizam „vezivnog ISSN-a (ISSN-L)" koji omogućava lokaciju ili povezivanje između različitih verzija medija istog kontinuiranog izvora. ISSN se može primjenjivati na serijske publikacije i druge kontinuirane izvore, neovisno o datumu njihovog izdavanja, tj. neovisno o činjenici da li je publikacija prestala da se izdaje ili se nalazi u procesu izdavanja ili će se tek izdati u bliskoj budućnosti, bez obzira na medij publikacije ili proizvodnje.

OSTALE VIJESTI IZ BAS-a

Posjeta delegacije ÚNMZ-a

Institut za standardizaciju Bosne i Hercegovine su u periodu između 19. i 21. marta 2019. godine posjetili predstavnici Češkog ureda za standarde, mjeriteljstvo i ispitivanja (ÚNMZ) Miroslav Chloupek, Jindra Kafková i Klara Popadičová, te Lubomir Keim iz Istraživačkog centra za građevinarstvo – kompanija za certificiranje iz Praga.

Više na: http://www.bas.gov.ba/pages/page_6678.html

Digitalizacija bosanskohercegovačkog društva

U Sarajevu je od 18. do 20. marta 2019. godine održana konferencija „Digitalizacija bosanskohercegovačkog društva".

Cilj konferencije je da se napravi presjek stanja u BiH kada je u pitanju digitalizacija i iskorištenost bh. IKT industrije, te iniciraju aktivnosti koje će pokrenuti promjene u društvu. U Institutu za standardizaciju Bosne i Hercegovine je prepoznat značaj spomenute teme te su predstavnici Instituta uzeli aktivno učešće u radu konferencije.

Više na: http://www.bas.gov.ba/pages/page_6677.html

15. mart – Svjetski dan prava potrošača

Obilježavanje 15. marta – Svjetskog dana prava potrošača je prilika da se traži poštovanje i zaštita prava svih potrošača, kao i da se iskaže protest protiv zloupotreba tržišta i socijalnih nepravdi koje ugrožavaju ta prava.

Više na: http://www.bas.gov.ba/pages/page_6675.html

INSTITUT ZA STANDARDIZACIJU NA NOVOJ LOKACIJI

Trg Ilidžanske brigade 2B
Dobrinja IV
71123 Istočno Sarajevo
Bosna i Hercegovina

Tel: +387 (0)57 310 560
Fax: +387 (0)57 310 575
e-mail: stand@bas.gov.ba