ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

ICC HRVATSKA MEĐUNARODNA TRGOVAČKA KOMORA
Svjetska poslovna organizacija

HGK 1852 HRVATSKA GOSPODARSKA KOMORA

VODIČ ICC-a ZA INFORMACIJSKU SIGURNOST U POSLOVANJU

Hrvatsko izdanje

diverto INSIG2 KING ICT span TRILIX

VODIČ ICC-a ZA INFORMACIJSKU SIGURNOST U POSLOVANJU

Hrvatsko izdanje

Zahvala

Vodič ICC-a za informacijsku sigurnost u poslovanju inspiriran je belgijskim vodičem za informacijsku sigurnost, odnosno inicijativom ICC-a Belgije i VBO-FEB-a te EY Belgium i Microsoft Belgium, s B-CCENTRE i ISACA-om Belgium. Iznimno cijenjen u Belgiji, ovaj je vodič ponuđen ICC-evoj komisiji za digitalnu ekonomiju ICC-a kao model koji bi se mogao prilagoditi i poslužiti, uz dopuštenje uključenih tvrtki i organizacija, kao globalni resurs.

ICC ljubazno zahvaljuje na doprinosu svima koji su bili uključeni u pripremu i izvedbu belgijskog vodiča te onim članovima ICC-eve radne skupine za sigurnost informacijskih sustava koji su osmislili ovaj vodič.

Publikacija ICC-a br. 450/1081-5
ISBN: 978-92-842-0336-9
ISBN: 978-953-7622-79-4

SADRŽAJ

PREDGOVOR

Predsjednik HGK i ICC-a Hrvatska, Luka Burilović

Hrvatska gospodarska komora i Međunarodna trgovačka komora (engl. International Chamber of Commerce—dalje u tekstu: ICC) Hrvatska s velikim zadovoljstvom donose i stavljaju na raspolaganje hrvatskoj poslovnoj zajednici prijevod ***Vodiča za informacijsku sigurnost u poslovanju*** koji su pripremili stručnjaci Komisije za digitalnu ekonomiju ICC-a.

Od samog osnutka, Hrvatska gospodarska komora uvijek je promicala dobru poslovnu praksu na korist svojih članica radi bolje zaštite poslovanja te podizanja ukupne konkurentnosti gospodarskog sustava Republike Hrvatske. Živimo i radimo u vremenu brzog razvoja IT sektora koji snažno utječe na poslovanje ne samo javnog, privatnog i državnog sektora nego ima utjecaj na potrošače, vlade i društvo u cjelini. Prednosti koje proizlaze iz većeg i olakšanog pristupa informacijama, robama i uslugama omogućio je globalni i otvoreni internet.

S druge strane, poduzeća su sve više suočena sa sigurnosnim ugrozama i rizicima koje internet donosi u poslovanju te činjenicom da su bez poduzimanja odgovarajućih mjera informacijske sigurnosti usluge na internetu izložene različitim sigurnosnim ugrozama i rizicima i predstavljaju značajnu prijetnju u elektroničkom poslovanju.

Mnoge studije pokazale su da su tvrtke koje su izgubile podatke ili doživjele sigurnosni proboj u informacijski sustav u kratkom roku prestale s poslovanjem jer su štete od gubitka ili krađe podataka bile nenadoknadive i u financijskom i reputacijskom smislu za njihov daljnji opstanak na tržištu.

ICC je upravo iz motiva temeljenih na doprinosu u području informacijske sigurnosti osmislio Vodič za informacijsku sigurnost u poslovanju radi osvještavanja poslovne zajednice diljem svijeta kako bi se uputilo na sigurnosne ugroze i rizike poslovanja na internetu te ponudio alat za efikasnije upravljanje rizikom u kriznim situacijama.

Namijenjen tvrtkama svih veličina i iz svih sektora, Vodič na pristupačan način pojašnjava osnove informacijske sigurnosti kako bi im olakšao rješavanje sve ozbiljnijeg pitanja sigurnosti poslovnih informacijskih sustava.

Čitajući Vodič upoznat ćete se s načelima i postupcima koji će vam pomoći u postizanju bolje informacijske sigurnosti, a upitnik za samoprocjenu pružit će vam uvid u stanje informacijske sigurnosti vašeg poduzeća.

PREDGOVOR

Unutar tvrtki, Vodič je namijenjen vlasnicima, menadžmentu i svim zaposlenicima te nije ograničen isključivo na organizacijske jedinice zadužene za informacijsku tehnologiju. Štoviše, Vodič za informacijsku sigurnost potiče poboljšanje dijaloga menadžmenta tvrke i IT specijalista te nalaže provedbu analize rizika i pripreme za otkrivanje i odgovor na sigurnosni proboj. Upravo bi se zbog toga Vodič trebao podijeliti s poslovnim partnerima u opskrbnom lancu roba i usluga i s javnim sektorom kako bi zaštita informacija bila što obuhvatnija. Suradnja privatnog i javnog sektora ključna je za ublažavanje rizika sigurnosti elektroničkog poslovanja na razini poduzeća, na nacionalnoj razini i društva u cjelini.

Vlade također imaju značajnu ulogu u intenziviranju međunarodne suradnje radi ublažavanja rizika *cyber*-kriminala.

Namjera je ICC-a Vodič distribuirati putem ICC-eve globalne mreže nacionalnih odbora, gospodarskih komora i tvrtki članica diljem svijeta, uz mogućnost prilagodbe nacionalnom kontekstu.

Stoga smo u hrvatsko izdanje uključili relevantne nacionalne partnere iz javnog sektora i dodali posebno poglavlje s poveznicama na njihove mrežne stranice te sponzore, renomirane tvrtke u Republici Hrvatskoj koji participiraju u pružanju proizvoda i usluga iz područja informacijske sigurnosti, kojima zahvaljujemo na potpori.

Vjerujemo da ćete ovaj Vodič prepoznati kao doprinos smanjenju sigurnosnih ugroza i rizika elektroničkog poslovanja na dobrobit svojih tvrtki i hrvatskoga gospodarstva u cjelini.

PREDGOVOR

Glavni tajnik ICC-a, John Danilovich

Međunarodna se trgovačka komora (ICC) ponosi činjenicom da gotovo sto godina tvrtkama osigurava alate i smjernice za samoregulaciju radi promicanja dobre poslovne prakse. Kao svjetskoj poslovnoj organizaciji, čiji su članovi tvrtke iz svih sektora i regija, ICC s osobitim zadovoljstvom tvrtkama svih veličina pruža ovaj jednostavan i jasan vodič kako bi im olakšao rješavanje sve ozbiljnijeg pitanja sigurnosti poslovnih informacijskih sustava.

ICC je organizacija posvećena poticanju trgovine i investicija, uključujući i poticanje povjerenja u digitalnu ekonomiju i povećanje značajnih mogućnosti koje ona donosi tvrtkama, potrošačima, vladama i društvu. Međusobna povezanost nije promijenila samo tržište, već i samu teksturu društva. Prednosti koje proizlaze iz većeg pristupa znanju, informacijama, dobrima i uslugama omogućio je globalni i otvoreni internet. On treba biti pouzdan i siguran. Stoga bi svaka strategija koja se odnosi na sigurnost informacijskih sustava trebala biti prikladna, opravdana i razmjerna kako bi očuvala ove prednosti.

S obzirom na to da je sigurnost—kao i savršenstvo—nedostižan cilj s više ustupaka, ona može biti i zastrašujuća tema. Strah ili nedostatak svijesti može biti zapreka tvrtkama da procjenjuju rizike i poduzmu odgovarajuće mjere. Ovaj vodič u nekoliko jednostavnih koraka osvještava o potrebi za brigom o informacijskoj sigurnosti i umanjuje strah od nepoznatog. ICC je izdao *Vodič za informacijsku sigurnost u poslovanju* kako bi se obratio širokoj publici, ciljajući pritom na svojih više od šest milijuna članova. Ovaj je vodič namijenjen da bude dostupan vlasnicima tvrtki, osoblju ili rukovoditeljima, a ne ograničen samo na službe za informacijsku tehnologiju te bi se trebao podijeliti s poslovnim partnerima u opskrbnom lancu dobrima i uslugama i s javnim sektorom kako bi zaštita informacija bila što obuhvatnija.

Vodič će se distribuirati putem ICC-eve globalne mreže nacionalnih odbora, tvrtki članica, poslovnih udruga, trgovačkih komora preko Svjetske federacije komora ICC-a i obuhvatit će 130 zemalja. ICC vjeruje da zajednički, globalni poslovni postupci njegove mreže partnera mogu značajno pridonijeti smanjenju rizika (elektroničkog) poslovanja na dobrobit tvrtki i društva u cjelini.

INFORMACIJSKA SIGURNOST POČINJE OD TEBE

Suvremena informacijska i komunikacijska tehnologija omogućuju tvrtkama svih veličina da budu inovativne, da prodiru na nova tržišta i potiču učinkovitost na dobrobit kupaca i društva. No sve se češće poslovna praksa i politika moraju prilagođavati izravnom i neizravnom utjecaju sveprisutnih komunikacijskih okružja i mrežnog protoka informacija koji su potrebni za isporuku usluga i dobara. U mnogim se tvrtkama usvajaju suvremene informacijske i komunikacijske tehnologije, a da se pritom nije u potpunosti razmotrila činjenica kako je zbog toga potrebno upravljati novim vrstama rizika.

Ovaj se vodič bavi upravo tom prazninom pa u glavnim crtama iznosi kako tvrtke svih veličina mogu utvrditi rizike u vezi s informatičkim poslovanjem i njima upravljati.

Propusti u sigurnosti informacijskih sustava konstantno su prisutni u medijima s izvješćima o zlonamjernim počiniteljima koji prodiru u tvrtke, velike i male—naizgled po volji i s lakoćom. Tvrtke su danas izložene sve većem riziku[1] jer počinitelji, hakeri, državni akteri i konkurenti postaju sve vještiji u iskorištavanju slabosti suvremenih informacijskih i komunikacijskih tehnologija. Kombinacija informacijskih sustava i raznih vanjskih uređaja[2] povećava razinu složenosti i broja prijetnji informacijskim sustavima tvrtki.

Tvrtke nisu izložene samo vanjskim prijetnjama, već moraju upravljati i rizicima unutarnjih prijetnji koje za njihove informacijske sustave predstavljaju osobe unutar same organizacije, kadre izmijeniti podatke ili zlorabiti resurse tvrtki iz udobnosti svojega doma ili lokalnog kafića. Iz poslovne je perspektive važno da tvrtka—mala ili velika—zna prepoznati rizike i učinkovito upravljati prijetnjama u vezi sa svojim informacijskim sustavima. Istodobno, svi menadžeri, uključujući rukovoditelje i direktore, moraju biti svjesni činjenice da je upravljanje rizicima poslovanja, koji su u vezi s njihovim informacijskim sustavima, trajni proces u kojemu nije i neće biti moguće postići apsolutnu sigurnost.

Za razliku od mnogih poslovnih izazova, upravljanje rizicima sigurnosti problem je za koji ne postoji jednostavno rješenje. Za to je potrebna dosljedna pozornost menadžmenta, toleriranje loših vijesti te jasna komunikacija. Premda su dostupni brojni odlični resursi koji pružaju sveobuhvatna objašnjenja o najčešćim prijetnjama, i dalje su rijetki prikladni postupci za pomoć menadžmentu u njihovu pristupu rješavanju problema sigurnosti informacijskog

1 Primjeri ugrožavanja sigurnosti informacijskih sustava koji su u porastu su zlonamjerni softveri (poput softvera za upadanje u druge informacijske sustave, softvera za iskorištavanje poznatih ranjivosti, crva, trojanaca itd.) napadi uskraćivanja usluge, kompromitacija podataka i drugi. Za mjerodavan popis vidi npr. ENISA Threat Landscape 2014, EL 2014 na http://www.enisa.europa.eu

2 Kao što su mobilni telefoni, modemi, platni terminali, automatsko ažuriranje softvera, industrijski sustavi nadzora, interakcija prodavatelja i kupca, kao i Internet stvari (IoT).

sustava. **Ovaj će dokument pomoći upravljačkoj strukturi** malih i velikih organizacija **u učinkovitijoj komunikaciji s njihovim menadžerima za informacijsku tehnologiju** te oko **razvijanja prakse upravljanja rizicima za sigurnost poslovnoga informacijskog sustava**.

Unapređenje sigurnosti informacijskog sustava organizacije moguće je kroz proces upravljanja rizicima. Poseban se naglasak ovdje stavlja na upravljanje. Zbog tehnološkog okružja koje se stalno mijenja te zbog novih izvora prijetnji, informacijski sustavi tvrtki neće nikada biti dovršeni, a niti sasvim sigurni. Kako bi bili učinkoviti u tako promjenjivom okružju, potrebno je imati dugoročan i konstantan pristup upravljanju rizicima. Ako menadžeri ne pristupe problemu smanjenja rizika s primjerenim očekivanjima, bit će frustrirani inicijativama u vezi s informacijskom sigurnošću jer bez prikladnih očekivanja tvrtke mogu brzo potrošiti sve raspoložive resurse u potrazi za ublažavanjem rizika. Od ključne je važnosti da se upravljanju rizicima sigurnosti informacijskih sustava pristupi procesom kojim će se tvrtki omogućiti da razumije i odredi prioritete bitne za organizaciju (fizička imovina i vrijedne informacije).

Iznimno je važno biti svjestan činjenice da **bez poduzimanja prikladnih mjera opreza, usluge na internetu, informacijske mreže i uređaji tvrtki nisu sigurni**. Moderni informacijski sustavi tvrtki cilj su raznih zlonamjernih počinitelja. Jedan koristan koncept kod određivanja očekivanja svih uključenih u upravljanje rizicima u vezi sa sigurnošću informacijskih sustava jest jednostavan postulat: “Ako je nešto vrijedno na mreži, onda je u opasnosti i vjerojatno je ugroženo.”

Srećom, ono što kakav zlonamjeran počinitelj smatra vrijednim nije uvijek povezano s imovinom (kako je slučaj s novcem, poslovnim tajnama i informacijama o kupcima) koju tvrtka smatra vrijednom. Premda postoje tehnike i procesi koji mogu pomoći u smanjivanju rizika, odlučan zlonamjerni počinitelj iskoristit će najslabiju kariku povezanih sustava jer postoji mnogo potencijalno ranjivih mjesta koja se odnose na organizaciju, zaposlenike ili tehnička rješenja.

Unatoč i najboljem radu proizvođača tehnoloških rješenja, pružatelja usluge pristupa internetu i zaposlenika unutar vaše organizacije, apsolutna sigurnost nije moguća. Stoga, procesi upravljanja rizicima sigurnosti informacijskih sustava moraju uključivati aktivnosti procjene prijetnji i slabosti specifičnih za vašu tvrtku i uskladiti ih s prioritetnom imovinom organizacije.

Unatoč navedenim sumornim izgledima za uspjeh, tvrtke svih veličina mogu razviti i njegovati ključne organizacijske sposobnosti kako bi bile uspješne u upravljanju rizicima sigurnosti informacijskih sustava.

- Prvo, menadžment mora provesti analizu rizika u svojoj organizaciji i odrediti prioritete odnosno vrijednost imovine kojoj je potrebna zaštita.
- Drugo, vodstvo mora poduzeti potrebne radnje i osigurati da tvrtka primijeni najbolju praksu u vezi s informacijskom sigurnošću.
- Treće, organizacije moraju biti spremne otkriti i odgovoriti interno i eksterno na sigurnosne događaje putem institucionaliziranih organizacijskih procesa.

Sposobnost odgovora na sigurnosni incident zahtijeva pojačanu komunikaciju sudionika u sigurnosnom događaju te s mjerodavnim vladinim akterima, vlastitim korisnicima, čak i konkurentima. Pripremom za bilo kakav sigurnosni incident u vezi s informacijskim sustavima izbjegavaju se mnoge pogreške koje bi komplicirale njegovo rješavanje. Konačno, mehanizmi na temelju kojih se iz sigurnosnih incidenata uči i mijenja praksa bitni su za pokretanje institucionalne promjene potrebne za širenje najbolje prakse upravljanja rizicima sigurnosti informacijskog sustava tvrtki.

KORIŠTENJE OVOG VODIČA

U posljednjem su desetljeću države, organizacije i pojedinci izdali brojne publikacije radi rješavanja problema informacijske sigurnosti. O toj temi postoji mnogo dokumenata i smjernica, pa je ponekad teško utvrditi što prvo čitati i koji je dokument prikladan upravo za vašu tvrtku. Raspon dostupnih materijala je golem, a uključuje sljedeće (prema rastućem stupnju specifičnosti):

- **Smjernice** su izjave o viziji na visokoj razini, a u njihovu je opsegu briga za informacijsku sigurnost i određivanje smjernica tvrtkama i pojedincima. Primjeri: Sigurnosne smjernice OECD-a, itd.
- **Nacionalne strategije** su dokumenti koji su često utemeljeni na smjernicama, a definiraju pristup informacijskoj sigurnosti te su prilagođeni određenom nacionalnom ili pravnom kontekstu. Primjeri: Međunarodna strategija za informacijsku sigurnost[3], nacionalne strategije Europe i drugih država[4], itd.
- **Okviri** su dokumenti koji nacionalne strategije vode korak dalje, a sadrže popis prioritiziranih ili ocijenjenih resursa te pomažu tvrtkama u ocjeni njihove zrelosti i napretka u upravljanju rizicima u vezi sa sigurnošću informacijskih sustava. Primjeri: Nacionalni institut za standarde i tehnologiju (NIST), Okvir za informacijsku sigurnost[5], itd.
- **Standardi poslovne prakse** su dokumenti na temelju kojih se unutar tvrtki upravlja procesima kako bi se osigurala trajna i dosljedna primjena dobre prakse informacijske sigurnosti. Primjeri: ISO 27001, 27002, 27032 standardi, PCI sigurnosni standardi, itd.
- **Tehnički standardi** su detaljne specifikacije za izvedbu sučelja kojima se ispunjavaju određeni uvjeti interoperabilnosti. Primjeri: HTTPS, AES, EMV, PCI standardi plaćanja, itd.

Utemeljen na globalnim smjernicama informacijske sigurnosti i nacionalnim strategijama, ovaj jednostavan vodič tvrtkama ponajprije nudi okvir za razmatranje pitanja sigurnosti na internetu. Namijenjene tvrtkama svih veličina, vodič na početku predstavlja **pet načela** koja poduzeća trebaju primijeniti radi postizanja informacijske sigurnosti. Zatim, u vodiču je utvrđeno **šest ključnih postupaka** prikupljenih iz raznih izvora i najboljih iskustava, koje bi tvrtka također trebala provesti. Vodič se konačno bavi pitanjem **kako navedenih pet načela primijeniti u okviru politika** i tako voditi razvoj postupaka za upravljanje rizicima u vezi s informacijskom sigurnošću. Digitalni dodatak relevantnih izvora služi kao dopuna ovom vodiču, odnosno kao živi resurs za pružanje preciznijih savjeta dok se vodič razvija—od standarda poslovne prakse do tehničkih standarda, itd. Premda apsolutna sigurnost nije moguća, koncepti upravljanja rizicima informacijske sigurnosti navedeni u ovom vodiču pomoći će tvrtkama u tome da se uhvate u koštac s izazovom informacijske sigurnosti u okružju koje se stalno mijenja. Ovaj vodič nije koristan samo za pojedinu tvrtku, već je zamišljen da ga podijelite s onima koji su u poslovnom odnosu s vašom tvrtkom, kako biste učinkovitije zaštitili sve točke ulaska i razmjene s vašim sustavima i postupcima.

3 https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace

4 https://www.enisa.europa.eu/topics/national-cyber-security-strategies

5 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

KORIŠTENJE OVOG VODIČA

Premda se pristupi informacijskoj sigurnosti mogu razlikovati od tvrtke do tvrtke ovisno o određenim čimbenicima[6], postoji niz važnih načela na kojima se temelji dobra praksa informacijske sigurnosti, neovisno o veličini ili gospodarskoj grani tvrtke. Ovaj vodič ističe **pet ključnih načela** podijeljenih prema dvjema kategorijama:

A. Vizija i način razmišljanja

B. Organizacija i procesi

Ova se načela nadopunjavaju s nizom od **šest ključnih sigurnosnih postupaka** te s **pet početnih elemenata za primjenu navedenih načela** i jačanje politika informacijske sigurnosti određene tvrtke.

Primjenom načela i postupaka iz ovog vodiča podiže se razina otpornosti tvrtke na prijetnje u vezi s informacijskom sigurnošću i smanjuju se poteškoće zbog povreda informacijske sigurnosti.

A. VIZIJA I NAČIN RAZMIŠLJANJA

Načelo br. 1: Usredotočite se na informaciju, a ne na tehnologiju

Vi ste prva linija obrane tvrtke od prijetnji informacijskoj sigurnosti i vi određujete način na koji će ona definirati svoj pristup informacijskoj sigurnosti. Stoga o informacijskoj sigurnosti razmišljajte u najširem smislu, a ne samo u kontekstu informacijske tehnologije.

Informacijska sigurnost obuhvaća ljude, procese i tehnologiju i tiče se cijele tvrtke, a ne samo službe za informacijsku tehnologiju (IT). Provedba sigurnosnih mjera ne bi trebala biti ograničena na službu za informacijsku tehnologiju, već bi se trebala odražavati na čitavu tvrtku u svim njezinim pothvatima. Dakle, opseg i vizija informacijske sigurnosti uključuju ljude, proizvode, postrojenja, procese, politike, postupke, sustave, tehnologije, uređaje, mreže i informacije.

Ljudi su ključ. Prepoznavanje i upravljanje ranjivostima i prijetnjama imovine i informacija može biti zahtjevan zadatak. Ipak, iskustvo je pokazalo[7] da je 35 posto sigurnosnih incidenata posljedica ljudske pogreške, a ne namjernih napada. Više od polovine preostalih sigurnosnih incidenata rezultat su namjernog napada **koji se mogao izbjeći** da su ljudi na sigurniji način raspolagali podacima.

Stoga svoje sigurnosne napore usmjerite ponajprije na zaštitu najvrjednijih podataka i sustava gdje bi gubitak povjerljivosti, cjelovitosti ili raspoloživosti ozbiljno naštetio tvrtki. Ovo, međutim, ne znači da se sigurnost ostalih informacija i imovine može zanemariti, već podrazumijeva da je pristup koji se temelji na riziku s naglaskom na "krunskim draguljima" organizacije učinkovit i djelotvoran pristup informacijskoj sigurnosti u praksi, priznajući istodobno da stopostotno uklanjanje rizika nije moguće, niti je potrebno s obzirom na troškove koje bi takav pristup uzrokovao.

6 uključujući, među ostalim, prirodu posla, stupanj rizika, okoliš, stupanj povezanosti, zakonske uvjete i veličine tvrtki.

7 EY — 2012. Globalno istraživanje o informacijskoj sigurnosti — *Fighting to close the gap*

Načelo br. 2: Neka otpornost postane vaš način razmišljanja

Cilj bi trebao biti otpornost tvrtke na rizik od gubitka ili oštećenja podataka. Tvrtke podliježu mnogim zakonima i propisima, od kojih mnogi nalažu provedbu odgovarajućih sigurnosnih kontrola. Poštovanje tih zakona, propisa i normi može dovesti do bolje informacijske sigurnosti, ali u trenutku kad se ti ciljevi postignu, može nastupiti samozadovoljstvo. Prijetnje u odnosu na informacijsku sigurnost mijenjaju se mnogo brže od zakona i propisa i tako predstavljaju dinamičan cilj za aktivnosti upravljanja rizicima. Stoga se postojeće poslovne politike i postupci mogu pokazati zastarjelima ili jednostavno neučinkovitima u praksi.

Periodična procjena otpornosti tvrtke na prijetnje informacijskoj sigurnosti i ranjivostima iznimno je bitna za ocjenu napretka upravljanja rizicima i adekvatnost mjera informacijske sigurnosti. Aktivnosti ocjenjivanja mogu se ostvariti internim i/ili neovisnim procjenama i revizijama, uključujući mjere poput penetracijskih testiranja i otkrivanja neovlaštenih upada.

Odgovornost za informacijsku sigurnost mora nadići IT odjel. Naime, zainteresirane strane koje donose odluke ne bi trebale biti uključene samo u utvrđivanje problema, već i u dugoročnu provedbu zdravog ekosustava unutar tvrtke. Ipak, prava vrijednost periodične revizije poslovanja postiže se ako se taj proces koristi radi poboljšanja kulture tvrtke te načina razmišljanja zaposlenika o postupcima upravljanja rizicima u vezi s informacijskom sigurnošću.

Usredotočenost na otporne informacijske sustave najvažnija je u trenutku kada tvrtka usvaja nova rješenja i uređaje. Tijekom takvog razdoblja potrebno je uzeti u obzir odgovarajuće mjere sigurnosti što je ranije moguće, a idealno vrijeme za to jest trenutak utvrđivanja poslovnih zahtjeva. Takva će "planska sigurnost" omogućiti zaposlenicima koji donose inovacije u tvrtke da budu usredotočeni na upravljanje rizicima u vezi s informacijskom sigurnošću.

B. ORGANIZACIJA I PROCESI

Načelo br. 3: Pripremite se na reakciju

U određenom će trenutku i najbolje pripremljena tvrtka doživjeti povredu informacijske sigurnosti. Živimo u okružju u kojemu je pitanje **kada** će se takvo što dogoditi, a ne **hoće li**. Stoga će vas se ocijeniti prema načinu na koji tvrtka reagira na povredu.

Kako bi se učinak sigurnosnih incidenata u vezi s informacijskim sustavima umanjio, potrebno je da, uz tehničke mjere, tvrtke osmisle i korporativne planove upravljanja incidentima. Planiranje upravljanja incidentima trebalo bi utvrditi putokaze menadžerima s uputom kada uključiti specijalizirane treće strane koji će znati spriječiti širenje i ublažiti sigurnosni incident i kada se valja obratiti drugim vanjskim stranama (uključujući tijela za provedbu zakona ili Vladinih nadzornih agencija). Imajte na umu da je informiranje odgovarajućih tijela način da se poboljša cjelokupno sigurnosno okružje, a u nekim slučajevima to može biti i obavezno kako bi se izbjegla povreda zakona ili kazna. Uspješno upravljanje incidentima uključuje komunikacijsku strategiju (internu i eksternu), koja vam može osigurati da, umjesto neugodnog pojavljivanja na prvoj stranici novina, vaša tvrtka uđe u sveučilišni program kao primjer uspješnog uklanjanja incidenata.

Premda su postupci upravljanja unutarnjim rizicima iznimno bitni, imajte također na umu da je u ovom trenutku potrebno odvojiti vrijeme za razgovore s kolegama i partnerima iz gospodarske grane vaše tvrtke, za razgovore sa širom poslovnom zajednicom, ali i regulatornim organima kako biste pridonijeli razumijevanju aktualnih i novih prijetnji te izgradili odnose s osobama na koje ćete se moći osloniti za vrijeme obrade incidenta.

Načelo br. 4: Pokažite predanost vodstva

Kako biste uspješno i učinkovito upravljali informacijskom sigurnošću, poslovno vodstvo mora razumijeti i podupirati aktivnosti upravljanja rizikom kao bitnim elementom za uspjeh vaše tvrtke. **Vi** i vaš tim menadžera trebate biti vidljivo uključeni u upravljanje i nadzor politika za upravljanje rizicima u vezi sa sigurnošću informacijskih sustava vaše tvrtke. Vodstvo tvrtke treba osigurati da se odgovarajući resursi—ljudski i financijski—dodijele za zaštitu imovine tvrtke. No samo resursi nisu dovoljni; potrebno je

osigurati funkciju za informacijsku sigurnost tvrtki, velikih i malih, kako bi na prijetnje i ranjivosti u odnosu na informacijske sustave bila zajamčena reakcija u cijeloj tvrtki.

O učinkovitosti i prikladnosti mjera korporativne informacijske sigurnosti potrebno je podnijeti službeno izvješće glavnom menadžeru, a barem jednom godišnje i timu menadžera, revizorima i upravi. Takvo bi redovito izvještavanje, utemeljeno na raznim sigurnosnim pokazateljima i mjerilima, trebalo pomoći u informiranju menadžmenta za donošenje daljnjih odluka o politici informacijske sigurnosti i investicija te osigurati uvid u stanje koliko dobro tvrtka štiti svoju imovinu.

Premda se u kontekstu informacijske sigurnosti ljude spominje kao najslabiju kariku, širenjem svijesti o informacijskoj sigurnosti razvit ćete kod zaposlenika djelotvorne vještine i osposobiti ih tako da oni postanu vaša najsnažnija karika za učinkovitu sigurnost poslovanja.

Načelo br. 5: Djelujte u skladu sa svojom vizijom

Nije dovoljno samo pročitati ovaj vodič—svoju jedinstvenu korporativnu viziju upravljanja rizicima u vezi s informacijskom sigurnošću trebate provesti u djelo stvaranjem (ili revidiranjem) raznih politika informacijske sigurnosti. Korporativne politike informacijske sigurnosti pružaju standardnu osnovu za usmjeravanje sigurnosnih postupaka unutar tvrtke za sve poslovne jedinice i osoblje, a pritom podižu i svijest o sigurnosti diljem tvrtke.

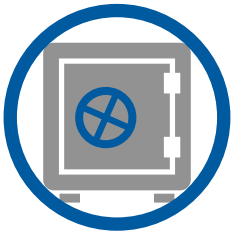
U pravilu, politike sigurnosti te prateće smjernice i norme sadržane su u okviru politike informacijske sigurnosti, koji se kasnije prenosi na uobičajene operativne postupke. Međutim, zbog sve većeg angažiranja i integriranja pružatelja usluga partnera u poslovne vrijednosti, organizacije moraju znati kakav je protok i međuovisnost njihovih informacija s vanjskim partnerima. Ako partner (ili njihovi informacijski sustavi na koje se oslanjate) ne štiti vaše podatke na prikladan način, **njihov** sigurnosni incident može postati ozbiljna odgovornost za **vaše** poslovne procese, ugled i vrijednost. Stoga potaknite partnere na to da usvoje barem informacije i načela informacijske sigurnosti koja se primjenjuju u vašoj tvrtki te, prema potrebi, provedite i revizije ili zatražite od partnera detalje o njihovoj praksi u pogledu informacijske sigurnosti kako biste se dodatno osigurali u odnosu na njihovu poslovnu praksu.

Vanjski partneri nisu samo izvori rizika—neki vam od njih mogu pomoći u smanjenju rizika i ostvarenju ciljeva upravljanja rizicima u vezi s informacijskom sigurnošću. Pružatelji informatičkih usluga mogu vam pomoći da unaprijedite infrastrukturu za upravljanje rizicima u vezi s informacijskom sigurnošću, sigurnosnim procjenama i revizijama te korištenjem uređaja informacijske sigurnosti i rješenja ili usluga, bila riječ o onima na licu mjesta, upravljanima izvana ili, pak, o onima iz oblaka („cloud“)[8].

8 Usluge iz oblaka jesu rješenja kojima se koriste vanjski davatelji usluga kako bi pohranili, obradili i upravljali podacima putem mreže kakva je internet, uz visok stupanj fleksibilnosti i nadzora u stvarnom vremenu.

Ovaj popis postupaka je skup praktičnih mjera koje tvrtke svih veličina mogu poduzeti radi smanjenja rizika pojave sigurnosnog incidenta. Premda popis nije sveobuhvatan i iscrpan, ako vaša tvrtka poduzme navedene postupke, bit će na dobrom putu da postigne izvrsnu informacijsku sigurnost.

Ne zaboravite da je upravljanje rizicima u vezi sa sigurnošću informacijskih sustava trajan proces. U trenutku kada budete zadovoljni time što su početne radnje u tijeku, pogledajte na internetskom portalu povezanim s ovim vodičem i utvrdite standarde i resurse koji će vas uputiti da poduzmete daljnje korake, kako biste dodatno unaprijedili program informacijske sigurnosti.



Postupak br. 1: Napravite pričuvnu kopiju (*back up*) poslovnih podataka; provjerite postupak povrata (*restore*)

Pripazite na to da zaštitite svoje poslovne podatke tako da napravite njihovu pričuvnu kopiju prije negoli se vaša tvrtka suoči s povredom sigurnosti i s posljedičnom krađom podataka, njihovom izmjenom, brisanjem ili gubitkom. Nije dovoljno napraviti samo pričuvnu kopiju[9]. Pravilno upravljanje postupcima izrade pričuvne kopije uključuje provjeru sadržaja poslovnih podataka i informacija sadržanih u arhiviranoj datoteci te ispitivanje postupaka povrata podataka. Ako se za pohranu podataka koriste treće strane (npr. usluge oblaka), pripazite na to da uključite odredbe i o izradi pričuvne kopije za takve podatke.

Imajte na umu da su fizički mediji poput diska, vrpce ili jedinice koji se koriste za pohranu pričuvne kopije podataka također podložni rizicima. Mediji korišteni za pričuvne kopije moraju imati jednaku razinu zaštite kao i izvorni podaci, osobito u pogledu fizičke sigurnosti, jer se predmeti za pohranu materijala pričuvne kopije lako prenose.

Postupak br. 2: Ažurirajte sustave informacijske tehnologije

Sustavi i softveri svih vrsta, uključujući mrežnu opremu i uređaje, trebali bi se ažurirati čim se pojave softverske nadopune („zakrpe“) i nadogradnje programskih datoteka. Takve

9 Postupak izrade pričuvne kopije jest tehnički postupak kojim se mora prikladno upravljati. Primjerice, samo korištenje više istodobno povezanih repozitorija za pohranu na istome mjestu nedovoljan je kao postupak izrade pričuvne kopije. Uspješna politika izrade pričuvne kopije mora uzeti u obzir višestruke vrste rizika uključujući gubitak podataka i gubitak operativne lokacije, među ostalim—brigama koje u pravilu nalažu da pričuvne kopije ne budu na istoj lokaciji.

nadogradnje i sigurnosne nadopune uklanjaju ranjivosti sustava koje bi napadači mogli zlorabiti. Mnoge su povrede uspjele kao posljedica ranjivosti sustava, premda su ažuriranja bila dostupna, često čak i više od godinu dana prije nastupa samog incidenta.

Kada je to moguće, koristite usluge automatskog ažuriranja, osobito za sigurnosne sustave kakvi su aplikacije protiv zlonamjernih softvera, alati za filtriranje sadržaja i sustavi otkrivanja neovlaštenih upada. Automatiziranjem postupaka ažuriranja možete pomoći tome da korisnici rabe važeća ažuriranja za sigurnosni softver neposredno od izvornog prodavatelja.

Postupak br. 3: Ulažite u obuku

Uspostavljanje osnovne svijesti o bitnim prijetnjama na informacijsku sigurnost te svijest o samom pitanju sigurnosti iznimno su bitni za osoblje vaše tvrtke i tu svijest treba stalno obnavljati. Obuka[10] osigurava da sve osobe koje imaju pristup informacijama i informacijskim sustavima razumiju svoju svakodnevnu odgovornost pri rukovanju, zaštiti i podršci aktivnostima informacijske sigurnosti tvrtke. Bez odgovarajuće obuke, zaposlenici mogu ubrzo postati izvor opasnosti unutar same tvrtke i izazvati sigurnosne incidente ili ranjivosti koje konkurenti mogu iskoristiti za povredu vaših mjera informacijske sigurnosti.

U svojoj tvrtki **vi** možete osmisliti kulturu upravljanja rizicima informacijske sigurnosti. Ako ulažete u obuku, s vremenom ćete zaposlenicima pojačati svijest o informacijskoj sigurnosti poslovanja i razvit ćete kod njih željene vještine i sposobnosti u vezi sa sigurnošću.

Postupak br. 4: Nadzirite svoj informacijski okoliš

Tvrtke moraju uspostaviti sustave i procese kako bi se osiguralo obavještavanje u slučaju nastupa incidenta informacijske sigurnosti unutar organizacije. Prečesto tvrtke nisu svjesne nastupa povrede sigurnosti; u nekim tvrtkama dođe do povrede ili zaraze čak nekoliko mjeseci ili godina prije negoli se upad otkrije.[11] Premda postoje razna tehnološka rješenja za pomoć oko

10 Opći podaci o sigurnosti informacijskih sustava i svijesti za krajnje korisnike dostupni su na www.staysafeonline.org. http://www.enisa.europa.eu/media/multimedia/material, kao inicijativi ENISA-e. Imate pravo koristiti sve te podatke, video i infografike u obrazovne svrhe unutar svoje tvrtke.

11 http://www.verizonenterprise.com/DBIR/2013/Verzija 2013. Izvješće o ispitivanju povrede podataka

ovog zadatka, uključujući sustave za otkrivanje i sprečavanje neovlaštenog upada i upravljanje sigurnosnim incidentima, samo instaliranje tih rješenja nije dovoljno. Kako bi se imalo koristi od tehnologije, potrebno je kontinuirano praćenje i analiziranje izlaznih podataka dobivenih iz tih sustava.

Mnoge tvrtke nemaju interne stručnjake ili resurse potrebne za praćenje bitnih sustava i procesa. Međutim, postoje različiti davatelji usluga koji pružaju usluge upravljanja sigurnošću na licu mjesta, nudeći različite poslovne modele, uključujući tehnologiju i usluge u oblaku.

Pronađite pravo rješenje za svoju tvrtku i zatražite pomoć od stručnjaka koji će vam dati savjet oko uključivanja odgovarajućih uvjeta u ugovore.

Ako je u tvrtki došlo do sigurnosnog incidenta u vezi s informacijskim sustavima, razmotrite mogućnost da o tome obavijestite odgovarajuće vladine agencije[12] i udruženja vaše gospodarske grane—komuniciranje s drugima može vam pomoći da utvrdite je li vaša tvrtka izoliran slučaj ili je dio većeg sigurnosnog incidenta.[13] Komuniciranjem s drugima često možete doći do informacija i savjeta koji mogu pomoći oko poduzimanja učinkovitih protumjera.

Postupak br. 5: Slojevita obrana radi smanjenja rizika

Sigurnost rubova mreže i tradicionalna kontrola pristupa više nisu dovoljni, osobito kada se informacijski sustav tvrtke spaja na internet, davatelje usluge pristupa internetu, na *outsourcing* i *cloud*-usluge, na dobavljače i partnere te na prijenosne uređaje, koji su izvan kontrole i dosega tvrtke. Za učinkovitu zaštitu od virusa, zlonamjernog sofvera ili uređaja te hakera, potrebni su slojevi obrambenih mjera, čime se smanjuje rizik od incidenta informacijske sigurnosti.

Kombiniranjem više tehnika[14] za rješavanje problema rizika u vezi s informacijskom sigurnošću moguće je značajno smanjiti vjerojatnost da se mala povreda pretvori u ozbiljan incident.

Slojevitom se obranom informacijske sigurnosti ograničava stupanj slobode dostupan napadačima, a korporativnim se sustavima kontrole povećava mogućnost otkrivanja povreda.

Osiguranje od rizika u vezi s informacijskom sigurnošću može biti način da tvrtke ublaže financijske posljedice incidenta, ali i da proaktivno upravljaju izloženošću te ojačaju interno upravljanje rizicima.

12 Žrtve kriminala (u vezi s informacijskim sustavima) trebale bi također podnijeti prijavu mjerodavnim tijelima za provedbu zakona. Lokalna je policija često najbolje mjesto za kontakt u slučaju klasičnih kaznenih djela, ali za slučajeve kaznenih djela u vezi s informacijskim sustavima (hakiranje, sabotaža, špijunaža) mogu postojati i specijaliziranija tijela za provedbu zakona.

13 Napad može biti horizontalan (cilj su tvrtke istog sektora) ili vertikalan (cilj su podizvođači) ili može biti riječ o sigurnosnoj prijetnji specifičnoj za poseban element softvera ili hardvera.

14 Uključujući filtriranje mrežnog prometa, antivirusne zaštite, proaktivne zaštite od zlonamjernog softvera, vatrozida, jake sigurnosne politike i obuke osoblja samo su neke od postojećih tehnika.

Postupak br. 6: Pripremite se za trenutak nastupa povrede

Upravljanje rizicima ne služi samo kako bi smanjilo vjerojatnost, već i potencijalnu štetu u trenutku kada povreda nastupi. To znači biti spreman da se incident brzo istraži, tako da prikladni resursi budu pri ruci te da sustavi i postupci budu prilagođeni za dohvat ključnih informacija. Ako je riječ o povredi uzrokovanoj upadom zlonamjernog programa, onda je takav program potrebno uništiti. Priprema također znači da postoji organizacijski plan radi brzog donošenja dobrih odluka i koordiniranja potrebnih radnji radi preuzimanja kontrole nad incidentom. Tko je odgovoran i kako?

Primjenom dobro osmišljenih postupaka te učinkovitom komunikacijom vaš tim može utjecati na ishod incidenta.

Konačno, pripremajući se unaprijed, moguće je umanjiti neke od najštetnijih učinaka povreda poput gubitka operabilnosti, nemogućnosti pristupa podacima, nemogućnosti nastavka rada unutar primjerenog roka. Takva se šteta može minimizirati planirajući postupak osiguravanja poslovnoga kontinuiteta i uz planiranje oporavka tako da budete usredotočeni na prioritete i da se za nastup incidenta unaprijed pripremite.

ELEMENTI ZA IZRADU POLITIKE INFORMACIJSKE SIGURNOSTI

Upravljačkoj se strukturi često povjerava zadatak da načela iz dokumenata poput ovog uključe u politiku i poslovnu praksu svoje tvrtke tako da budu od koristi upravo za nju. Svrha je ovog poglavlja pomoći menadžmentu u obavljanju tog zadatka. Osmišljeni na temelju pet ključnih sigurnosnih načela navedenih u ovom vodiču, sljedeći elementi nude polazišne točke za izradu politike i poslovne prakse upravljanja rizicima u vezi s informacijskom sigurnošću.

Usredotočite se na informacije, a ne na tehnologiju

- Osmislite funkciju i imenujte osobu koja će voditi i olakšavati provedbu inicijativa informacijske sigurnosti, pri čemu je odgovornost za sigurnost i dalje zajednička za cijelu tvrtku.
- Kod planiranja kako ostvariti ciljeve informacijske sigurnosti, svaka tvrtka treba odgovoriti na sljedeće:
  - Što će se učiniti?
  - Koji su potrebni resursi?
  - Tko je odgovoran?
  - Kada će se što obavljati?
  - Kako će se vrednovati rezultati?[15]
- U slučaju kada tvrtka nema dovoljno iskustva s pitanjima interne sigurnosti, potražite dodatne informacije i stručnjake za informacijsku sigurnost koji će vam pomoći oko uključivanja informacijske sigurnosti u izradu poslovnih procesa i informacijskih sustava.

Izaberite otpornost kao način razmišljanja

- Postupci informacijske sigurnosti trebali bi biti usklađeni s drugim naporima oko regulatornog usklađivanja i smanjenja rizika te bi, prema potrebi, trebali biti uključeni u njih kako bi se izbjeglo preklapanje inicijativa i odgovornosti.
- Averzija prema riziku ne bi smjela onemogućiti uvođenje novih tehnologija. Uz ostvarenje ciljeva upravljanja rizicima sigurnosti informacijskih sustava, pristupi informacijskoj sigurnosti mogu potaknuti tvrtku i na uvođenje novih i inovativnih tehnologija.
- Pripazite na to da sigurnost bude uvijek uključena u svakom projektu koje vaša tvrtka provodi, osobito u novim projektima. Kada je uključena od samog početka, uz ispravni poslovni angažman, sigurnost neće značajno povećati trošak i trajanje projekta. Međutim, kada se sigurnost dodaje kasnije ili, u najgorem slučaju, nakon nastupa povrede, onda dolazi do prekoračenja troškova, a kašnjenja kao i ostale posljedice za nekoliko su redova veličine veće.

15 ISO/IEC 27001:2013

- Odredite koji uređaji (ponajprije mobilni uređaji poput onih od vaših zaposlenika ili poslovnih partnera) smiju pristupiti mreži i/ili informacijama tvrtke[16] i razmislite o tome kako upravljati softverom i sigurnosnim postavkama na opremi tvrtke.
- Ocjenjujte pristup podacima kako biste osigurali da sustavi kontrole djeluju radi očuvanja povjerljivosti, cjelovitosti i dostupnosti informacija.
- Menadžeri bi u svojem odjelu trebali pregledati i odobriti korisnike (unutarnje i vanjske) koji imaju pristup aplikacijama i podacima—pristup je odgovornost i rizik pa je zato poželjna odgovarajuća kontrola pristupa zaposlenika podacima i informacijskim sustavima.
- Razvijajte postupke izvješćivanja za izgubljenu ili ukradenu opremu i, ako je moguće, osposobite funkcionalnost daljinskog brisanja podataka s opreme kako bi se s izgubljenih ili ukradenih uređaja mogli izbrisati svi korporativni podaci.

Budite spremni reagirati

- Svatko griješi, a tvrtka koja svoje pogreške u pogledu informacijske sigurnosti pretvori u priliku za otvorenu reviziju sigurnosnih incidenata, stvorit će kulturu u kojoj se zaposlenici neće bojati prijaviti sigurnosne incidente kada do njih dođe.
- Ovlastite odabrane osobe za razmjenu odgovarajućih informacija s kolegama i drugim zainteresiranim stranama unutar predmetne gospodarske grane, i to ne samo radi pomoći oko osmišljavanja vodeće poslovne prakse, već i radi upozorenja od potencijalnih nadolazećih napada.
- Odredite odgovornu osobu kako bi se osiguralo pravilno čuvanje dokaza od samog početka kod rješavanja sigurnosnog incidenta, a posebno u slučaju kaznenog djela u vezi s informacijskim sustavima.[17]
- Odredite kako i kada je potrebno prijaviti incident informacijske sigurnosti hitnoj službi za kaznena djela u vezi s informacijskim sustavima (poznatoj i kao CERT—cyber emergency response team), vladinim agencijama ili pravosudnoj policiji.

16 Tražite od korisnika da konfiguriraju odgovarajuće sigurnosne postavke na mobilnom uređaju kako biste spriječili krađu informacija putem uređaja.

17 Smjernice za dobivanje podataka u slučaju sigurnosnog incidenta radi istrage od ICT osoblja, ili u slučaju zaraze zlonamjernim softverom, dostupne su na: http://cert.europa.eu/cert/plainedition/en/cert_about.html

Vodstvo je bitno

- Osoblje bi trebalo biti odgovorno za informacije i njihovu zaštitu, a trebalo bi imati i odgovarajuće ovlasti, pristup top menadžmentu te alate i obuku kako bi bilo osposobljeno u odnosu na svoje odgovornosti i moguće prijetnje.[18]
- Male bi tvrtke trebale imati nekoga, unutar ili izvan tvrtke, tko redovito provjerava primjerenost informacijske sigurnosti i službeno preuzima odgovornost za informacijsku sigurnost. Premda to možda nije zadaća koja zahtijeva ulogu s punim radnim vremenom, ona je vrlo važna i može biti bitna za opstanak tvrtke.
- U velikim tvrtkama, dodjeljivanje dužnosti, uloga i odgovornosti trebaju biti postupak dobro promišljenog uključivanja pojedinaca i (virtualnih) radnih skupina i povjerenstava. Svaki član tima treba jasno znati koja je njegova osobna i hijerarhijska odgovornost. U ovom su slučaju pravilno dokumentiranje i komunikacija bitni.

Postupajte u skladu sa svojom vizijom

- Kontrolirajte pristup prema unutarnjoj mreži (intranetu) i iz nje dajući prednost pristupu uslugama i resursima koji su bitni za potrebe posla i zaposlenika.[19]
- Obvezujte druge na to da koriste kvalitetne lozinke i razmotrite mogućnost provedbe učinkovitih metoda provjere autentičnosti[20] koji za ulaz, uz lozinku, traže i dodatne informacije.
- Upotrijebite šifriranje gdje je to prikladno kako biste zaštitili pohranjene podatke te podatke koje prenosite,[21] s posebnim naglaskom na prenošenje podataka putem javnih mreža i prijenosnih uređaja poput prijenosnih računala, USB memorijskih ključeva i pametnih mobilnih telefona koji se mogu lako izgubiti ili ukrasti.

18 Važna prijetnja za koju osoblje treba osposobiti jest društveni inženjering. Riječ je o tehnici manipuliranja tako da obave radnje i otkriju osjetljive ili povjerljive informacije.

19 Razmislite o tome da filtrirate usluge i internetske stranice koje povećavaju sigurnosne rizike za resurse tvrtki, primjerice dijeljenje datoteka među kolegama i pornografske internetske stranice. Pravila za filtriranje trebaju biti potpuno jasna svim korisnicima u organizaciji i uključivati postupak za deblokiranje poslovnih internetskih stranica koje mogu biti omaškom odbijene.

20 U višefaktorskoj se autentifikaciji rabi kombinacija elemenata poput stvari koje znam (npr lozinke ili PIN-ovi), *stvari koje imam* (npr. pametna kartica ili SMS) i *što jesam* (npr. otisak prsta ili skeniranje šarenice).

21 Primjerice, s obzirom na to da se elektronička adresa putem interneta često šalje kao otvoreni tekst, tvrtke bi, kada prenose osjetljive informacije, trebale razmotriti načine za šifriranje elektroničke pošte.

ELEMENTI ZA IZRADU POLITIKE INFORMACIJSKE SIGURNOSTI

- Osmislite detaljnu politiku za izradu pričuvnih kopija i arhiviranja koja će biti u skladu sa zakonskim i regulatornim zahtjevima za pohranu informacija, a kojom će se detaljno definirati sljedeće:
  - od kojih podataka učiniti pričuvnu kopiju i kako to učiniti
  - koliko često se radi pričuvna kopija podataka
  - tko je odgovoran za stvaranje pričuvnih kopija i provjeru uspješnosti izrade pričuvnih kopija
  - gdje i kako se spremaju pričuvne kopije
  - tko ima pristup pričuvnim kopijama
  - kako rade postupci za povrat (*restore*) (i kako se testiraju)
- Razvijajte programe obuke o svijesti o informacijskoj sigurnosti, uključujući teme poput:
  - sigurnog i odgovornoga komuniciranja;
  - mudroga korištenja društvenih medija;
  - prijenosa digitalnih datoteka na siguran način;
  - pravilnoga korištenja lozinki;
  - izbjegavanja gubitka važnih podataka;
  - osiguravanja da samo ovlaštene osobe mogu pristupiti vašim podacima;
  - zaštita od virusa i drugih zlonamjernih programa;
  - koga obavijestiti ako primijetite potencijalni sigurnosni incident i
  - kako spriječiti da vas ne navedu na odavanje informacija.

UPITNIK ZA SAMOPROCJENU SIGURNOSTI

Sljedeće poglavlje sadrži jednostavan popis kao alat za menadžment koji će vam pomoći oko provedbe unutarnje revizije sposobnosti tvrtke da se zaštiti od prijetnji informacijskoj sigurnosti. Taj će vam alat osigurati da postavite prava pitanja službama koje su uključene u navedene inicijative te da utvrdite prednosti i nedostatke odnosno način na koji poboljšati informacijsku sigurnost tvrtke.

Istodobno, ovaj se upitnik za samoprocjenu sigurnosti može koristiti kao kontrolni popis za tvrtke koje su tek pokrenule inicijative za uvođenje informacijske sigurnosti, a žele koristiti informacije kao temelj za planiranje sposobnosti zaštite od prijetnji informacijskoj sigurnosti.

Za svako pojedino pitanje u nastavku valja utvrditi koja od pruženih mogućnosti najviše odgovara aktualnoj poslovnoj praksi vaše tvrtke. Svaki je odgovor označen jednom bojom, pri čemu je:

- ovo najnepoželjniji odgovor; svakako treba razmotriti kako poboljšati stanje.
- moguće dodatno poboljšati stanje, kako bi se poboljšala zaštita tvrtke.
- ovaj odgovor najbolji odraz zaštite u odnosu na prijetnje u vezi s informacijskim sustavima.

Odgovori na upitnik jedinstveni su rezultat za svakog procjenitelja, a detaljnija je kontrolna lista ispod svakog pitanja namijenjena kao pomoć oko utvrđivanja i dokumentiranja statusa informacijske sigurnosti tvrtke. Podacima koje prikupite ovim upitnikom moći ćete utvrditi nedostatke ili propuste te spoznati u kojem smjeru poduzeti sljedeći korak.

1

Provodite li analizu o tome kako postupati s osjetljivim informacijama unutar tvrtke?

✖ Ne, ali imamo vatrozid koji nas štiti od krađe informacija.

! Da, shvaćamo važnost svojih informacija i provodimo opće mjere sigurnosti.

✔ Da, imamo model za klasifikaciju podataka i znamo gdje se naši osjetljivi podaci pohranjuju i obrađuju. Provodimo mjere sigurnosti ovisno o osjetljivosti pojedine informacije.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Utvrđujete li i klasificirate svoje osjetljive podatke?		
Znate li koja je vaša odgovornost u odnosu na utvrđene osjetljive podatke?		
Jesu li najosjetljiviji podaci dobro zaštićeni ili šifrirani?		
Postoje li postupci za upravljanje osobnim privatnim podacima?		
Jesu li svi zaposlenici u stanju utvrditi i ispravno zaštititi osjetljive i neosjetljive podatke?		

2

Provodite li procjene rizika u vezi s informacijskom sigurnošću?

☒ Ne provodimo.

! Provodimo, ali ne o nekim određenim pitanjima u vezi s informacijskom sigurnošću.

☑ Provodimo za određena pitanja informacijske sigurnosti.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Bavite li se rezultatima ranjivosti u smislu klasifikacije visoke i niske razine rizika?		
Utvrđuju li se događaji koji bi mogli uzrokovati prekide u poslovnom procesu i procjenjuje li se učinak potencijalnih prekida?		
Imate li aktualni plan poslovnoga kontinuiteta koji se redovito provjerava i ažurira?		
Provodite li redovito procjene rizika kako biste ažurirali razinu zaštite potrebnu za podatke i informacije?		
Identificiraju li se u vašim poslovnim procesima područja rizika kako bi se kod obrade podataka spriječilo njihovo iskrivljavanje ili namjerna zloupotreba?		

3

Na kojoj se razini provodi upravljanje informacijskom sigurnošću?

✖ Nikakvo upravljanje informacijskom sigurnošću nije na snazi.

! Upravljanje informacijskom sigurnošću instalirano je unutar IT odjela jer je to mjesto gdje informaciju treba zaštititi.

✔ Upravljanje informacijskom sigurnošću instalirano je na korporativnoj razini kako bi se učinak osigurao za cjelokupnu tvrtku.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Dodjeljuju li članovi uprave i izvršni direktor budžet za informacijsku sigurnost?		
Je li informacijska sigurnost dio postojećeg upravljanja rizikom koje obavljaju direktori?		
Odobrava li menadžment politiku informacijske sigurnosti tvrtke i priopćava li je na prikladan način zaposlenicima?		
Jesu li članovi uprave i menadžment redovito informirani o najnovijem razvoju politika, standarda, postupaka i smjernica u području informacijske sigurnosti?		
Je li bar jedan djelatnik unutar strukture menadžmenta zadužen za zaštitu podataka i zaštitu privatnosti osobnih podataka?		

4

Postoji li unutar vaše tvrtke služba za informacijsku sigurnost ili funkcija posvećena informacijskoj sigurnosti?

✖ Ne postoji služba za informacijsku sigurnost, niti specifična uloga ili odgovornost u vezi s informacijskom sigurnošću.

! Nemamo službu za informacijsku sigurnost, ali smo unutar tvrtke definirali određene uloge i odgovornosti u vezi s informacijskom sigurnošću.

✔ Imamo službu za informacijsku sigurnost ili funkciju posvećenu informacijskoj sigurnosti.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Koordinira li određeni stručnjak ili služba za informacijsku sigurnost znanje unutar tvrtke i pruža li pomoć menadžmentu kod donošenja odluka?		
Jesu li određeni stručnjak ili služba za informacijsku sigurnost zaduženi za revidiranje i sustavno ažuriranje politike informacijske sigurnosti na temelju značajnih promjena ili incidenata?		
Jesu li određeni stručnjak ili služba za informacijsku sigurnost unutar tvrtke dovoljno vidljivi i imaju li potporu kako bi mogli intervenirati u svakoj inicijativi u vezi s informacijskom sigurnošću?		
Jesu li različiti menadžeri odgovorni za pojedine vrste podataka?		
Revidira li neovisno tijelo ili revizor redovito izvedivost i uspješnost politike informacijske sigurnosti i učinkovitost službe za informacijsku sigurnost?		

5

Kako se vaša tvrtka odnosi prema riziku za informacijsku sigurnost od dobavljača koji imaju pristup vašim osjetljivim informacijama?

✖ Sa svojim dobavljačima imamo odnos utemeljen na uzajamnom povjerenju.

! U neke ugovore uključujemo odredbe u vezi s informacijskom sigurnošću.

✔ Imamo postupke kojima dobavljačima validiramo pristup, a priopćavaju im se i određene sigurnosne smjernice koje oni potpisuju.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Identificiraju li se izvođači radova i dobavljači putem identifikacijske značke na kojoj je njihova novija fotografija?		
Imate li politiku koja se bavi provjerom izvođača radova i dobavljača?		
Prekida li se pristup sadržajima i informacijskim sustavima automatski kada izvođač ili dobavljač završi svoj zadatak?		
Znaju li dobavljači kome unutar tvrtke i kako bez odgode prijaviti bilo kakav gubitak ili krađu informacija?		
Osigurava li vaša tvrtka da dobavljači ažuriraju svoje softvere i aplikacije sigurnosnim nadopunama (“zakrpama”)?		
Jesu li u ugovorima s izvođačima radova/dobavljačima jasno definirani uvjeti sigurnosti?		

6

Procjenjuje li vaša tvrtka redovito računalnu i mrežnu sigurnost?

- ✖ Ne provodimo reviziju niti penetracijska testiranja kako bismo procijenili svoju računalnu i mrežnu sigurnost.
- ! Nemamo sustavni pristup za obavljanje sigurnosnih revizija i/ili penetracijskih testiranja, ali obavljamo određene *ad hoc* provjere.
- ✔ Redovite sigurnosne revizije i/ili penetracijska testiranja sustavni su dio našeg pristupa u procjeni računalne i mrežne sigurnosti.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Testirate li redovito i vodite li evidenciju o utvrđenim prijetnjama?		
Imate li postupke za procjenu prijetnji koje za vaše informacijske sustave predstavljaju ljudi, uključujući nepoštenje, društveni inženjering i zlouporabu povjerenja?		
Traži li vaša tvrtka od svojih pružatelja usluge informacijske tehnologije izvješća o sigurnosnoj reviziji?		
Procjenjuje li se tijekom sigurnosne revizije i korisnost svih vrsta pohranjenih podataka?		
Obavljate li reviziju svojih informacijskih procesa i postupaka radi usklađivanja s ostalim utvrđenim politikama i standardima unutar tvrtke?		

7

Procjenjuje li vaša tvrtka kod uvođenja novih tehnologija potencijalne rizike u odnosu na informacijsku sigurnost?

- Informacijska sigurnost nije dio postupka kod uvođenja novih tehnologija.
- U postupku uvođenja novih tehnologija informacijska se sigurnost provodi samo *ad hoc*.
- Informacijska je sigurnost uključena u postupak uvođenja novih tehnologija.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Kada razmatrate uvođenje novih tehnologija, procjenjujete li njihov potencijalni utjecaj na utvrđenu politiku informacijske sigurnosti?		
Imate li zaštitne mjere kojima smanjujete rizik kada uvodite nove tehnologije?		
Dokumentiraju li se postupci za uvođenje novih tehnologija?		
Može li se vaša tvrtka kod uvođenja novih tehnologija pouzdati u partnere i time omogućiti udruživanje napora i sudjelovanje u bitnim sigurnosnim informacijama?		
Sagledava li se politika informacijske sigurnosti vaše tvrtke često kao prepreka za tehnološke izazove?		
Upravlja li tvrtka novim tehnologijama koristeći metodologiju sigurnog razvoja unutar životnog ciklusa sustava?		

8

Održava li se unutar vaše tvrtke obuka iz informacijske sigurnosti?

✖ Imamo povjerenja u svoje zaposlenike i ne smatramo da je obuka iz informacijske sigurnosti dodana vrijednost.

! Samo osoblje IT odjela pohađa obuku radi osiguranja našeg IT okružja.

✔ Za sve se zaposlenike redovito organiziraju predavanja osviještenosti o informacijskoj sigurnosti.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Jesu li neka predavanja iz informacijske sigurnosti prilagođena području rada zaposlenika?		
Osposobljava li se zaposlenike da budu pripravni za slučaj povrede informacijske sigurnosti?		
Ima li vaša tvrtka upute za korisnike o tome kako prijaviti slabosti ili prijetnje za sigurnost sustava ili usluga?		
Znaju li zaposlenici kako primjereno upravljati podacima kreditnih kartica i privatnim osobnim podacima?		
Pohađaju li i treće osobe kao korisnici (ako je primjenjivo) prikladnu obuku iz informacijske sigurnosti i obavještava li ih se redovito o aktualnim politikama i postupcima tvrtke?		

9

Kako se unutar vaše tvrtke koriste lozinke?

✖ Dijelimo lozinke s drugim kolegama i/ili ne postoji nikakva politika za sigurno korištenje lozinki ili za njihovu redovitu promjenu.

! Svi zaposlenici, uključujući menadžment, imaju jedinstvene lozinke, ali se pravila o kompleksnosti ne primjenjuju. Promjene lozinki su izborne, a ne obavezne.

✔ Svi zaposlenici, uključujući menadžere, imaju osobne lozinke koje moraju ispunjavati određene uvjete i koje se redovito mijenjaju.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Je li vaša tvrtka utvrdila globalno prihvaćenu politiku za lozinke za svu svoju imovinu?		
Možete li potvrditi dolje navedeno za sve lozinke u vašoj tvrtki? – nisu pohranjene u lako dostupnim datotekama; – nisu slabe, ne ostavljaju se prazne lozinke, niti se ostavljaju kao zadana postavka; – ne ostaju neizmijenjene, niti se mijenjaju samo rijetko, osobito one za mobilne uređaje.		
Osjećate li se dobro zaštićeni od neovlaštenoga fizičkog pristupa sustavima?		
Jesu li korisnici i izvođači radova svjesni svoje odgovornosti da zaštite i onu opremu koja nije pod nadzorom (tj. da se odjavljuju)?		
Jesu li zaposlenici osposobljeni za prepoznavanje trikova socijalnog inženjeringa kojima se osobe navodi na otkrivanje sigurnosnih pojedinosti i znaju li kako reagirati na takvu prijetnju?		

10

Postoji li korporativna politika za primjereno korištenje interneta i društvenih medija?

✖ Ne postoji takva politika.

! Da, postoji, na centraliziranoj lokaciji dostupnoj svim zaposlenicima, ali je zaposlenici nisu potpisali

✔ Da, politika o primjerenom korištenju interneta dio je ugovora / svi zaposlenici su je potpisali.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Postoje li opće smjernice i procesi komunikacije za zaposlenike u tvrtki, uključujući odnose s tiskom i društvenim medijima?		
Postoje li disciplinski postupci za zaposlenike koji povrijede korporativne smjernice za komunikaciju?		
Provjerava li menadžer ili služba za komunikacije internet kako bi procijenili rizike i status e-ugleda?		
Je li vaša tvrtka procijenila svoju odgovornost za djela zaposlenika ili drugih internih korisnika ili napadača koji zlorabe sustav radi poduzimanja nezakonitih radnji?		
Je li vaša tvrtka poduzela mjere kako bi spriječila zaposlenike ili druge interne korisnike da napadnu druga internetska mjesta?		

11

Mjeri li, izvješćuje li i prati li vaša tvrtka pitanja u vezi s informacijskom sigurnošću?

✖ Ne nadziremo, ne izvješćujemo i ne pratimo učinkovitost i primjerenost provedenih sigurnosnih mjera.

! Naša je tvrtka instalirala alate i metode kako bi mogla nadzirati, izvješćivati i pratiti učinkovitost i prikladnost određenog broja naših provedenih sigurnosnih mjera.

✔ Naša je tvrtka instalirala potrebne alate i metode kako bi nadzirala, izvješćivala i pratila učinkovitost i prikladnost svih provedenih sigurnosnih mjera.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Kada su u pitanju incidenti, vode li se o tome revizijski zapisnici i poduzimaju li se proaktivne mjere kako se to ne bi ponovilo?		
Provjerava li vaša tvrtka usklađenost sa zakonskim i regulatornim uvjetima (npr. zaštita privatnosti podataka)?		
Je li vaše tvrtka razvila vlastite alate kojima pomaže menadžmentu u procjeni sigurnosti, kojima joj se omogućuje da ubrza svoju sposobnost ublažavanja potencijalnih rizika?		
Postoji li u vašoj tvrtki plan informacijske sigurnosti koji sadrži ciljeve, ocjenu napretka te mogućnosti suradnje?		
Iznose li se izvješća o praćenju i incidenti vlastima i drugim interesnim skupinama, poput udruženja određenog sektora?		

12

Kako se unutar vaše tvrtke ažuriraju sustavi?

✖ Za većinu se svojih rješenja oslanjamo na automatsko upravljanje nadopunama koje daje proizvođač.

! Sigurnosne nadopune sustavno se primijenjuju svakog mjeseca.

✔ Imamo postupak upravljanja ranjivošću i uvijek tražimo informacije o mogućim ranjivostima (npr. pretplatom na uslugu koja automatski šalje upozorenje o novim ranjivostima) i primjenjujemo nadopune na temelju rizika koji se njima ublažavaju.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Je li provjera ranjivosti predviđena kao redoviti zadatak unutar plana održavanja tvrtke?		
Pregledava li se i testira li se aplikacijski sustav nakon svake promjene u operativnom sustavu?		
Mogu li korisnici sami za sebe provjeravati postojanje nenadopunjenih aplikacija?		
Jesu li korisnici svjesni činjenice da su i oni dužni ažurirati operativni sustav i aplikacije te sigurnosni softver na svojim mobilnim uređajima?		
Jesu li korisnici osposobljeni za prepoznavanje opravdanih poruka upozorenja, poput traženja dopuštenja za ažuriranje (za razliku od lažnih antivirusnih zahtjeva) i znaju li na odgovarajući način obavijestiti sigurnosnu službu ako se nešto loše ili upitno dogodi?		

13

Revidira li se i upravlja li se redovito pravima pristupa aplikacijama i sustavima?

✖ Prava na pristup aplikacijama i sustavima ne oduzimaju se dosljedno, niti se dosljedno revidiraju.

! Prava na pristup aplikacijama i sustavima oduzimaju se samo onda kada zaposlenik napusti tvrtku.

✔ Utvrđena je politika kontrole pristupa, a dodijeljena se korisnička prava na pristup redovito revidiraju za sve relevantne poslovne aplikacije i sustave potpore.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Ograničavaju li politike i postupci pristup elektroničkim informacijskim sustavima i objektima?		
Oslanja li se vaša tvrtka na politiku zaštite privatnosti, navodeći podatke koje prikuplja (primjerice o svojim kupcima: adrese, elektroničke adrese, povijest pregledavanja, itd.) i što se s time radi?		
Određuju li politike i postupci metode koje će se koristiti za kontrolu fizičkog pristupa radi osiguranja područja (brave, sustavi kontrole pristupa i video nadzor)?		
Prekida li se zaposleniku pristup sadržajima i informacijskim sustavima automatski kada mu prestane zaposlenje?		
Klasificiraju li se osjetljivi podaci (vrlo povjerljivi, osjetljivi, samo za internu upotrebu) i jesu li popisani svi korisnici kojima je odobren pristup?		
Jesu li razvijeni procesi za reguliranje udaljenog pristupa elektroničkim informacijskim sustavima tvrtke?		

14

Smiju li zaposlenici u vašoj tvrtki koristiti svoje osobne uređaje, poput mobilnog uređaja ili tableta, za pohranu ili prijenos korporativnih informacija?

✖ Da, smijemo pohranjivati ili prenositi korporativne informacije na osobne uređaje bez provedbe dodatnih sigurnosnih mjera.

! Postoji politika kojom se zabranjuje korištenje osobnih uređaja za pohranu ili prijenos korporativnih informacija, ali je to tehnički moguće učiniti bez provedbe dodatnih sigurnosnih mjera.

✔ Na osobne se uređaje smiju pohraniti ili prenositi korporativni podaci tek nakon što su za te osobne uređaje provedene sigurnosne mjere i/ili je pronađeno određeno službeno rješenje.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Oslanja li se vaša tvrtka na dobro prihvaćenu politiku “ponesi vlastiti uređaj sa sobom”?		
Jesu li mobilni uređaji zaštićeni od neovlaštenih korisnika?		
Jesu li svi uređaji i priključci trajno identificirani na mreži?		
Je li šifriranje instalirano na svakom mobilnom uređaju kako bi se zaštitila tajnost i cjelovitost podataka?		
Je li korporativna razina svjesna toga da, dok pojedini zaposlenik može biti odgovoran za uređaj, tvrtka je i dalje odgovorna za podatke?		

15

Je li vaša tvrtka poduzela mjere za sprečavanje gubitka pohranjenih informacija?

✖ Nemamo nikakav postupak izrađivanja pričuvnih kopija / dostupnosti.

! Imamo postupak izrade pričuvne kopije / dostupnosti, ali nismo provjeravali funkcije povrata (*restore*).

✔ Imamo postupak izrade pričuvne kopije / dostupnosti koji uključuje testiranje povrata / otpornost. Imamo kopiju pričuvne kopije koja je pohranjena na drugoj sigurnoj lokaciji ili koristimo druga rješenja visoke dostupnosti.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Ima li dovoljno članova osoblja koji su u stanju stvoriti dohvatljive pričuvne i arhivske kopije?		
Je li oprema osigurana od kvarova napajanja tako što koristite trajno napajanje poput višestrukih izvora, neprekidnog napajanja (UPS), sigurnosnog generatora, itd.?		
Testira li se medij za pričuvnu kopiju redovito kako bi se osiguralo da se može obnoviti unutar roka predviđenog u postupku oporavka?		
Primjenjuje li vaša tvrtka postupke izvješćivanja za izgubljen ili ukraden mobilni uređaj?		
Znaju li zaposlenici što trebaju učiniti ako se informacije slučajno izbrišu te kako dohvatiti informacije u vrijeme katastrofa?		
Jeste li proveli mjere kako biste zaštitili povjerljivost i cjelovitost pričuvnih kopija na mjestu za njihovu pohranu?		

16

Je li vaša tvrtka spremna za rješavanje incidenata informacijske sigurnosti?

✖ Nećemo imati nikakvih incidenata. U slučaju da ih bude, naši su zaposlenici dovoljno sposobni da se s njima nose.

! Imamo postupke za upravljanje incidentima, no nisu prilagođeni za rješavanje incidenata informacijske sigurnosti.

✔ Imamo postupak posvećen obradi incidenata informacijske sigurnosti, s potrebnim mehanizmima eskalacije i komunikacije. Nastojimo rješavati incidente što je učinkovitije moguće jer tako učimo kako se bolje zaštititi u budućnosti.

Pitanja u nastavku ponuđena su kao kontrolna lista informacijske sigurnosti za vašu tvrtku kao pomoć u procjeni gdje se nalazite u tom procesu.	DA	NE
Bavi li se vaš postupak različitim vrstama incidenata, od uskraćivanja usluga, do povrede tajnosti itd. te načinima na koje ih se može riješiti?		
Ima li vaša tvrtka plan upravljanja komunikacijama u slučaju nastanka incidenta?		
Znate li koje vlasti obavijestiti i kako u slučaju incidenta?		
Ima li vaša tvrtka informacije za kontakt razvrstane i utvrđene za svaku vrstu incidenta?		
Oslanjate li se na internoga komunikacijskog menadžera za kontakte sa zaposlenicima i njihovim obiteljima?		
Postoji li postupak “naučenih lekcija” radi poboljšanja upravljanja incidentima nakon nastupa incidenta informacijske sigurnosti?		

RELEVANTNI NACIONALNI RESURSI I KONTAKTI

Želite li znati više o temi informacijske sigurnosti, u nastavku su navedena nadležna i stručna tijela i organizacije u Republici Hrvatskoj koja se bave tim područjem. Popis daje pregled korisnih poveznica i nudi vam alate za širenje znanja i suradnju s javnim sektorom i poslovnim udruženjima.

Agencija za zaštitu osobnih podataka
www.azop.hr

Hrvatska akademska i istraživačka mreža (CARNet) / Nacionalni CERT
www.CARNet.hr
www.cert.hr

Hrvatska gospodarska komora
http://www.hgk.hr/

Hrvatski nacionalni odbor Međunarodne trgovačke komore (ICC Hrvatska)
http://www2.hgk.hr/icc/ ; http://www.icc.hgk.hr/

Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)
www.hakom.hr

Hrvatska udruga banaka
https://www.sigurnostnainternetu.hr/

Ministarstvo unutarnjih poslova
www.mup.hr

Ministarstvo uprave
https://uprava.gov.hr

Ured Vijeća za nacionalnu sigurnost
www.uvns.hr/hr/normativni-akti/informacijska-sigurnost

Zavod za sigurnost informacijskih sustava
https://www.zsis.hr/

BILJEŠKE

MEĐUNARODNA TRGOVAČKA KOMORA (ICC)

ICC je svjetska poslovna organizacija, tijelo koje predstavlja poslovnu zajednicu iz svih sektora u svim dijelovima svijeta.

Misija je ICC-a promicati međunarodnu trgovinu i ulaganja te pomoći poslovnom sektoru u suočavanju s izazovima i prilikama globalizacije. Uvjerenje da je trgovina snažna sila za postizanje mira i napretka potječe još od samih početaka organizacije u ranim godinama 20. stoljeća. Mala skupina dalekovidnih poslovnih lidera koji su osnovali ICC nazivala se "trgovcima mira".

Tri su glavne djelatnosti ICC-a utvrđivanje pravila, rješavanje sporova i zagovaranje politika. Kako tvrtke i udruženja učlanjena u ICC-u i sama sudjeluju u međunarodnom poslovanju, ICC predstavlja neprikosnoveni autoritet u stvaranju pravila kojima se uređuje međunarodno poslovanje. Premda se ta pravila primjenjuju na dobrovoljnoj osnovi, ona se svakodnevno poštuju u nebrojenim transakcijama i postala su dijelom samog tkiva međunarodne trgovine.

ICC pruža i važne usluge, među kojima se ističe njegovo Međunarodno arbitražno sudište, vodeće svjetsko arbitražno tijelo. Tu su i usluge Svjetske federacije komora, ICC-eve globalne mreže trgovačkih komora koja potiče suradnju i razmjenu najbolje prakse među komorama. ICC nudi i specijalizirane programe izobrazbe i seminare, a na tom je području i vodeći izdavač praktičnih i obrazovnih vodiča za međunarodno poslovanje, bankarstvo i arbitražu.

Poslovni lideri i stručnjaci iz redova članstva ICC-a oblikuju poslovna stajališta o širokom rasponu tema trgovinske i investicijske politike te o relevantnim tehničkim pitanjima. To uključuje, među ostalim, borbu protiv korupcije, bankarstvo, digitalnu ekonomiju, etiku marketinga, okoliš i energetiku, politiku zaštite tržišnog natjecanja i intelektualno vlasništvo.

ICC blisko surađuje s Ujedinjenim narodima, Svjetskom trgovinskom organizacijom i međuvladinim forumima, uključujući G20.

ICC je osnovan 1919. godine. Danas njegovu globalnu mrežu čini više od 6 milijuna tvrtki, trgovačkih komora i poslovnih udruga u više od 130 zemalja. Nacionalni odbori s članovima ICC-a u svojim zemljama rade na rješavanju njihovih interesa te svojim vladama prenose poslovna stajališta ICC-a.

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 F +33 (0)1 49 53 28 59
E icc@iccwbo.org www.iccwbo.org

Publikacija ICC-a br. 450/1081-5
ISBN: 978-92-842-0336-9

Izdavač: Hrvatska gospodarska komora i ICC Hrvatska
Za izdavača: Luka Burilović

Naklada: 1000 primjeraka
Zagreb, studeni 2017.

ISBN: 978-953-7622-79-4