Provjera informacijskih tehnologija

Zašto SIQ?

Stabilnost:

Naš se rad temelji na cjelovitim rješenjima, partnerskom odnosu, neovisnosti i nepristranosti. Sukladno tim načelima već više od 50 godina testiramo, certificiramo i kontroliramo proizvode i sustave, umjeravamo mjerne uređaje, ocjenjujemo i certificiramo sustave upravljanja te prenosimo iskustva i znanje. SIQ je uključen u međunarodno okruženje; imamo stranke iz cijelog svijeta te izdajemo globalno priznate izvještaje i certifikate.

Iskustva:

Ekipa smo iskusnih stručnjaka s dugogodišnjim iskustvom na području pregleda programske opreme, informacijskih sustava, sigurnosnih pregleda i osiguravanja cjelovite zaštite informacija. Stručnost kadrova potvrđuju ugledni međunarodni certifikati i mnogobrojne zadovoljne stranke.

Povjerenje:

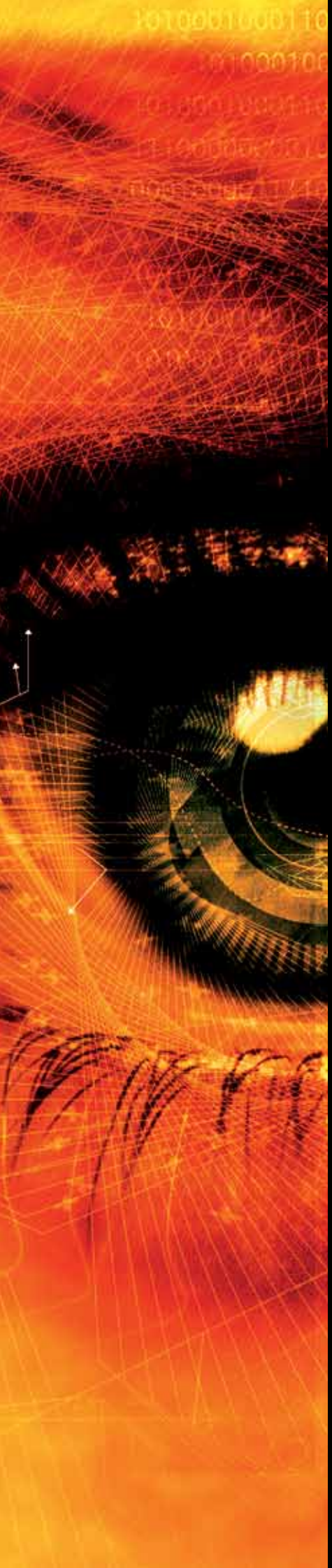
Za pregled od strane neovisne organizacije ključno je potpuno povjerenje stranke, jer stranka za vrijeme pregleda otkriva svoje najosjetljivije podatke, postupke i znanje. Takvo je povjerenje u SIQ opravdano:

- Imamo oko 140 zaposlenika i aktivno potičemo politiku niske fluktuacije.
- Imamo stroge odredbe u ugovorima o zaposlenju kad je riječ o povjerljivosti informacija.
- Naše su usluge akreditirane i priznate od strane mnogih međunarodno priznatih akreditacijskih tijela i shema.
- Redovito smo podvrgnuti najrazličitijim i često vrlo opsežnim provjerama naših postupaka, prostora i osoblja od strane različitih domaćih i stranih tijela i organizacija.
- Imamo dorađen prijedlog sporazuma o čuvanju informacija (NDA – Non-disclosure Agreement) koji možete oblikovati prema Vašim potrebama ili možete predložiti svoj oblik sporazuma.
- Profesionalnu odgovornost imamo odgovarajuće osiguranu.

Konkurentnost:

Znamo osluhnuti potrebe i želje stranka. Sistematičnim i učinkovitim pristupom naše usluge možemo ponuditi po konkurentnim cijenama i u brzim rokovima izvedbe.

SIQ
www.siq.hr



Sigurnosni pregled informacijskog sustava

Zaštitite svoje poslovanje

U današnjem svijetu elektroničkog poslovanja dolazi do sve više zloupotreba podataka, zato je njihova zaštita ključna za dugoročnu uspješnost organizacije. Najbolje je mogućnosti zloupotreba spriječiti i to odgovarajućim zaštićenim pristupom podatcima i uslugama unutar organizacije te javnim uslugama na internetu.

Sigurnosni pregled namijenjen je otkrivanju mogućih prijetnji i ranjivosti Vašeg informacijskog sustava te s njima povezanih rizika za sigurnost informacija. To je najučinkovitiji način provjere stvarnog stupnja sigurnosti jer se primjenjuju jednake metode, tehnike i alati koje u praksi primjenjuju hakeri. Obavljanjem sigurnosnog pregleda dobit ćete nedvojbeni odgovor jesu li sigurnosne kontrole u Vašem informacijskom sustavu odgovarajuće te time odgovarajuće zaštititi poslovanje Vaše organizacije.

Sigurnosnim pregledom dobit ćete odgovore na pitanja:

- Je li Vaš informacijski sustav odgovarajuće zaštićen kako ne biste postali žrtvom internetskog napada?
- Jeste li pravilno postavili politike Vaše sigurnosne infrastrukture da ih Vaši zaposlenici i ugovorni suradnici ne mogu zaobići te neovlašteno pristupati Vašim podatcima?
- Imaju li korisnici Vaših poslovnih aplikacija stvarno pristup samo onim podatcima koje trebaju?
- U što ulagati sredstva da izbjegnete ili smanjite troškove zbog gubitka ili krađe podataka, nedjelovanja usluge, kršenja zakona ili gubitka ugleda kod stranaka?
- Znate li koji su trendovi zloupotrebe informacijskih sustava u Sloveniji i inozemstvu i kakve su potrebne sigurnosne kontrole koje morate uvesti?

Glavni je cilj sigurnosnog pregleda ocijeniti koje sigurnosne kontrole u informacijskom sustavu još trebaju poboljšanja. Osim toga predstavljanjem rezultata sigurnosnog pregleda upravitelje i korisnike informacijskog sustava možemo upoznati s otkrivenim ranjivostima i osposobiti ih da se pobrinu za odgovarajuću zaštitu informacija pri svakodnevnom obavljanju svojeg posla.

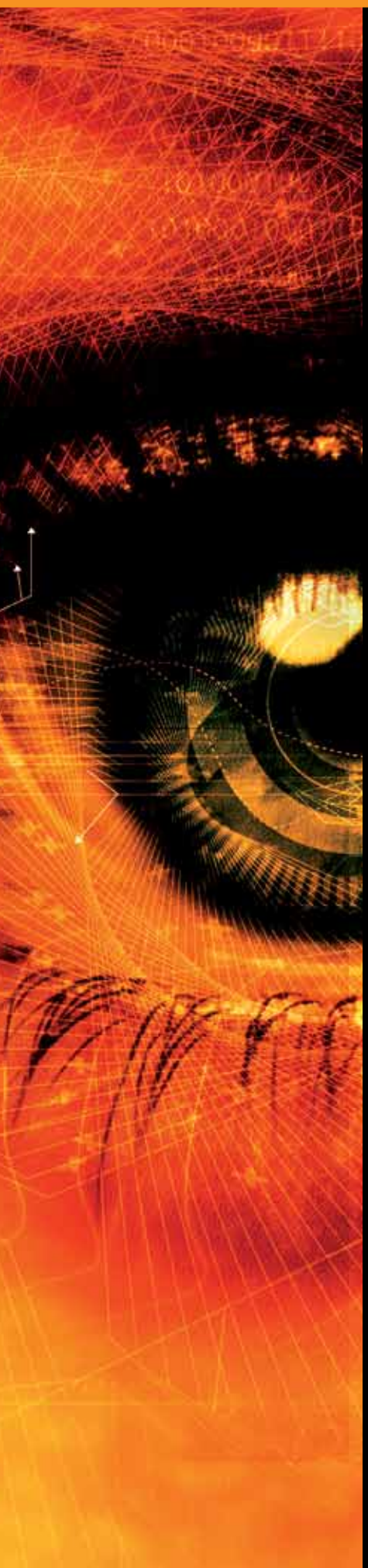
SIQ Ljubljana sa svojom ekipom iskusnih stručnjaka iz područja informacijske sigurnosti provodi cjelovit skup sigurnosnih pregleda koje prilagođavamo Vašim potrebama. Obavljamo standardne sigurnosne preglede (automatizirani pregled ranjivosti, vanjski i unutarnji sigurnosni pregledi) i specijalizirane preglede s obzirom na potrebe naručitelja (sukladnost s PCI DSS - ASV i QSA, sigurnosni pregled aplikacija, pregled mobilnih uređaja, pregled sustava za igranje, pregled izvornog koda, pregled sustava SCADA, pregled VoIP/IP telefonije, socijalni inženjering, revizijski pregled informacijskog sustava).

Informacije

SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

SIQ
www.siq.hr

PROVJERA SUKLADNOSTI S PCI-DSS-OM



Obrađujete li podatke o kartičnom poslovanju?

PCI-DSS (Payment Card Industry Data Security Standard) sigurnosni je standard međunarodnih sustava plaćanja (American Express, Discover Financial Services, JCB International, MasterCard i Visa). Pruža okvir za odgovarajuću zaštitu podataka korisnika kartičnog poslovanja. Sve organizacije koje obrađuju, prenose ili čuvaju kartične podatke moraju zadovoljiti zahtjeve PCI-DSS-a, što dokazuju godišnjim revizijama QSA, samoocjenjivanjem SAQ ili tromjesečnim pregledima ranjivosti ASV. Zahtijevani načini provjere ovise o godišnjem broju transakcija kartičnog poslovanja te su obvezni i za trgovce, financijske ustanove (issuer, acquirer) i procesne centre.

SIQ Ljubljana može vam pomoći u cijelom procesu uspostave i održavanja sukladnosti s PCI-DSS-om. Nudimo sljedeće usluge:

Analiza raskoraka

Analizom raskoraka utvrđujemo odstupanja trenutačnog stanja od zahtjeva standarda PCI-DSS. Naši iskusni i akreditirani revizori prepoznaju sva područja s manjkavostima i daju preporuke za postizanje usklađenosti. Rezultat analize jest i određivanje opsega infrastrukture koja je podvrgnuta zahtjevima PCI-DSS-a i potrebna je informacija pri samoocjenjivanju SAQ.

Pomoć pri samoocjenjivanju SAQ

Naši iskusni i akreditirani stručnjaci mogu vam pomoći pri samoocjenjivanju i ispunjavanju upitnika SAQ. Pritom vam daju i preporuke za postizanje sukladnosti s PCI-DSS-om.

Revizija QSA

Reviziju QSA provode naši akreditirani stručnjaci (Qualified Security Assessors) s dugogodišnjim iskustvom na području informacijske sigurnosti (CISA, CISM). Ona uključuje temeljit pregled informacijskoga okruženja, koji je dio kartičnog poslovanja, a završava izvještajem o sukladnosti (RoC).

Pregled ranjivosti ASV

Pregled ranjivosti ASV provode naši akreditirani stručnjaci (Approved Scanning Vendors) s dugogodišnjim iskustvom na području sigurnosnih provjera (EC CEH, GCIH, GPEN). Ona uključuje provjeru ranjivosti svih javno dostupnih sustava koji su dio kartičnog poslovanja ili ga omogućuju. Rezultat je izjava o sukladnosti (AoC) s detaljnim izvještajem ranjivosti razvrstanih prema ljestvici CVSS.

Informacije

SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

www.siq.hr

SIGURNOSNI PREGLED APLIKACIJA

Imaju li korisnici aplikacija stvarno pristup svojim podatcima?

Sigurnosni pregled aplikacija namijenjen je otkrivanju mogućih sigurnosnih prijetnji i manjkavosti pojedinih aplikacija. To kod zlonamjernog napada može omogućiti provedbu neovlaštenih promjena koje mogu utjecati na povjerljivost, raspoloživost i cjelovitost podataka u samoj aplikaciji (npr. neovlašten pristup, mijenjanje podataka, nedjelovanje aplikacije).

U pozadini djelovanja aplikacija mogu biti različite tehnologije (internetske, mobilne, klasične). Bez obzira na njihovu njihovo vrstu moguće su prijetnje na strani:

- korisnika
- mreže odnosno transportnog kanala
- infrastrukture poslužitelja

Cjelovit sigurnosni pregled aplikacija zato se provodi u više faza unutar kojih detaljno proučimo arhitekturu aplikacije, elemente i samo djelovanje aplikacije. Tipične manjkavosti aplikacija jesu:

- pristup podatcima bez prijave
- neodgovarajuće lokalno spremanje podataka
- provedba akcija u ime drugog korisnika, kao što je provedba transakcija, uključivanje/isključivanje usluga itd.
- promjena lozinke drugog korisnika i time preuzimanje njegova korisničkog računa
- eskalacija privilegija korisničkih prava koja korisniku omogućuje više mogućih aktivnosti, npr. promjenu cijena itd.
- pristup podatcima odnosno mijenjanje podataka drugog korisnika

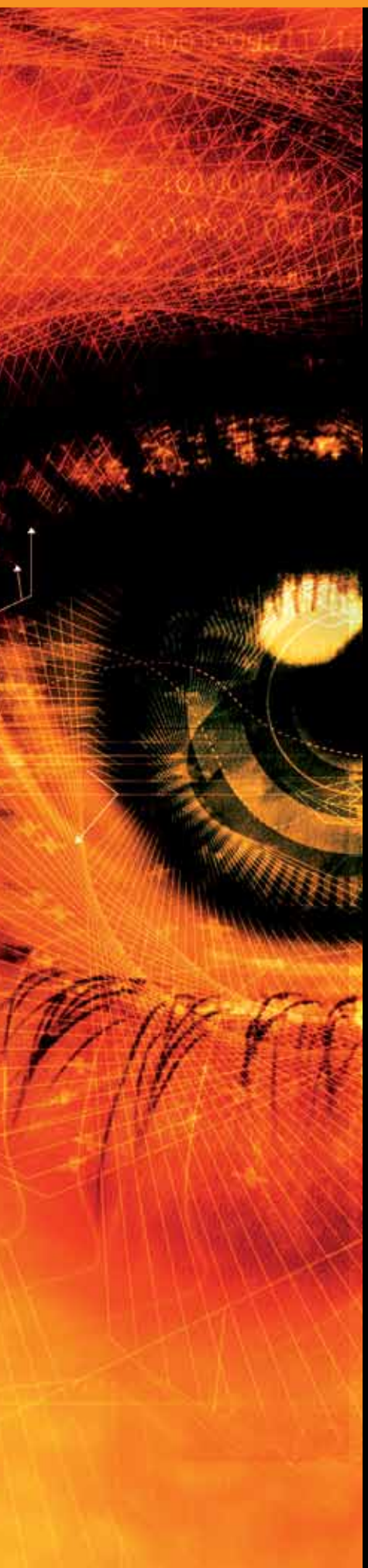
Detaljnim sigurnosnim pregledom, koji uključuje i korisničku prijavu, dobivate nedvojbeni odgovor jesu li sigurnosne kontrole u aplikaciji odgovarajuće.

Najdetaljnije sigurnosne nedostatke možemo otkriti pregledom izvornog koda aplikacija, jer su upravo greške u kodiranju primarni izvor problema. Pritom je važno da izvorni kod provjere neovisni stručnjaci za aplikacijsku sigurnost, koji nisu sudjelovali u razvoju aplikacije. Pregled izvornog koda aplikacije provodi se u više koraka, pri čemu naručitelj osigurava sve raspoložive informacije (princip »bijele kutije«). U prvom koraku primjenjuje se namjenski programski alat koji prepoznaje sigurnosno problematična mjesta u programskom kodu. On se nakon toga ručno detaljno provjerava u suradnji s razvojnim stručnjakom programske opreme na strani naručitelja te savjetnikom za sigurnost i razvojnim specijalistom na strani izvođača. U zadnjem koraku još se penetracijskim testom nedvojbeno potvrđuju utvrđeni sigurnosni nedostaci.

Informacije
SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

www.siq.hr

SIGURNOSNI PREGLED INFORMACIJSKE INFRASTRUKTURE



Vjerujete li svim članovima vašeg IT-a??

S punim razmahom elektroničkih komunikacija sigurnost informacijskih sustava postala je ključna za poslovanje organizacija. Sigurno postavljanje i održavanje informacijske infrastrukture posebno je važno jer s kompleksnošću i raznolikošću informacijskih sustava raste i mogućnost sigurnosnih propusta, a teže ih je i otkriti. Sigurnost cijelog informacijskog sustava ovisi naime o najslabijoj kariki. I jedan sigurnosni propust može uništiti mnogobrojne uvedene sigurnosne mjere (npr. preuzete administrativne lozinke).

Opći pregled ranjivosti

Takvim pregledom dobit ćete osnovnu informaciju o izloženosti Vaše informacijske infrastrukture zlonamjernom kodu i najčešćim prijetnjama koje zbog poznatih ranjivosti ili grešaka u konfiguraciji mogu iskoristiti i neiskusni napadači. Pregled će se provesti automatiziranim alatima koji raznim tehnikama i posebno kreiranim zahtjevima sustavno provjeravaju dostupnost usluga i poznate ranjivosti. Takvi se pregledi najčešće provode u organizacijama koje su obvezne redovito provjeravati stanje informacijske sigurnosti zbog zahtjeva IT revizora.

Vanjski sigurnosni pregled (penetracijsko ispitivanje)

Namijenjen je otkrivanju mogućih sigurnosnih prijetnji koje prijete informacijskoj infrastrukturi iz javno dostupne mreže. Pritom se primjenjuju metode i alati koji su prisutni kod stvarnih internetskih napada. Ciljani sustavi koji se provjeravaju su internetski poslužitelji i internetske poslovne aplikacije, poštanski poslužitelji i druge potporne usluge, upotrijebljeni sigurnosni sustavi i mehanizmi zaštite (požarni zidovi, IPS itd.) te ostale javno dostupne usluge organizacije.

Unutarnji sigurnosni pregled

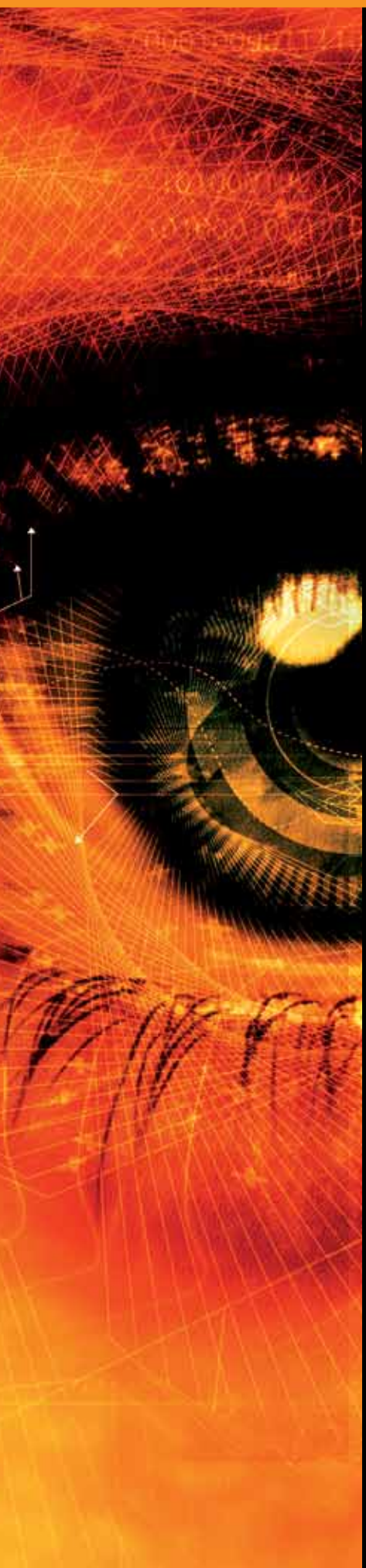
Svrha je otkriti moguće sigurnosne prijetnje i ranjivosti informacijske infrastrukture kod namjernih ili nenamjernih štetnih aktivnosti zaposlenika odnosno kod napada iz unutarnje mreže. Obuhvaća pregled odgovarajućeg planiranja informacijskog sustava, pregled dostupnosti te postavljanje strojne i programske opreme, pregled VoIP/IP telefonije, pregled bežične mreže i mobilnih uređaja, pregled adekvatnosti sigurnosne politike i pravila održavanja sustava te sigurnosni pregled ključne programske opreme.

Informacije

SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

SIQ
www.siq.hr

REVIZIJSKI PREGLED INFORMACIJSKOG SUSTAVA



Osiguravate sukladnost sa zakonodavstvom i dobrim praksama upravljanja informacijskim sustavom

Informacijski sustavi usko su povezani s poslovanjem svih vrsta organizacija. Bez pouzdanog, dobro upravljivog i sigurnog informacijskog sustava svakodnevno poslovanje više ne možemo zamisliti. Redoviti revizijski pregledi informacijskog sustava pridonose da se provedbom propisanih preporuka smanji mogućnost incidenata koji bi mogli utjecati na povjerljivost, raspoloživost ili cjelovitost podataka te organizaciji uzrokovati poslovnu štetu. Revizijski pregled informacijskog sustava predstavlja sistematičnu i stručnu procjenu tehničkih i organizacijskih kontrola u informacijskom sustavu. Svrha je provjeriti sukladnost s propisima, standardima i dobrim praksama na području informatike. Pregled se sastoji od ocjene stanja, analize rizika i procjene kontrola. Na osnovi pregleda utvrđujemo podupire li informacijski sustav u organizaciji poslovne ciljeve te djeluje li učinkovito, sigurno i pouzdano. Revizijskim pregledom dobivate neovisno stručno mišljenje u vezi s usklađenosti s propisima, standardima i dobrim praksama. Nudimo sljedeće usluge:

- revizijski pregled kompletne informacijske infrastrukture
- revizijski pregled informacijske sigurnosti (ISO/IEC 27001)
- revizijski pregled upravljanja uslugama IT (ISO/IEC 20000-1)
- revizijski pregled neprekidnog poslovanja (ISO 22301)
- revizijski pregled projektnog upravljanja u informatici
- pregled programske opreme (funkcionalnost, sigurnost)
- revizijske preglede poštivanja zakonodavnih odredbi s područja zaštite podataka

Revizijske preglede informacijskog sustava provode naši stručnjaci s dugogodišnjim iskustvom na području procjenjivanja i revidiranja (PRIS, CISA, CISM, VP ISO/IEC 27001, VP ISO/IEC 20000-1). Rezultat je revizijsko izvješće s detaljnim opisom svih zaključaka i prijedlozima za poboljšanja upravljanja informacijskim sustavom.

Informacije
SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

SIQ
www.siq.hr

SOCIJALNI INŽENJERING

Znaju li Vaši zaposlenici pravila informacijske sigurnosti?

Organizaciji koja se bavi većim brojem različitih profila zaposlenika, osiguranje odgovarajuće razine informacijske sigurnosti predstavlja velik izazov. Najučinkovitiji način provjere osviještenosti i obrazovanja zaposlenika jest provedba tzv. socijalnog inženjeringa.

Socijalni inženjering je skup tehnika kojima napadač nadmudri ili uvjeri korisnika da izvede određenu aktivnost (npr. otvori zlonamjernu elektroničku poštu, upotrijebi ključ USB zaražen štetnim kodom itd.) te mu time omogući pristup povjerljivim podatcima organizacije. Pritom napadač iskoristi odaziv korisnika na određenu situaciju (npr. na privlačnu ponudu, povjerenje, spremnost na pomoć itd.).
Poznato je više oblika socijalnog inženjeringa:

- tehničke metode
- osobni kontakt
- prijetnje i prisile

Za provedbu socijalnog inženjeringa potrebno je prikupiti mnogo informacija o organizaciji i potencijalnim metama (zaposlenicima). Informacije je moguće dobiti uz pomoć javno dostupnih informacija (internetske stranice, telefonski imenici itd.), posjetom organizaciji ili uspostavom prijateljskih kontakata sa zaposlenicima.

Primjeri scenarija provjere zaposlenika:

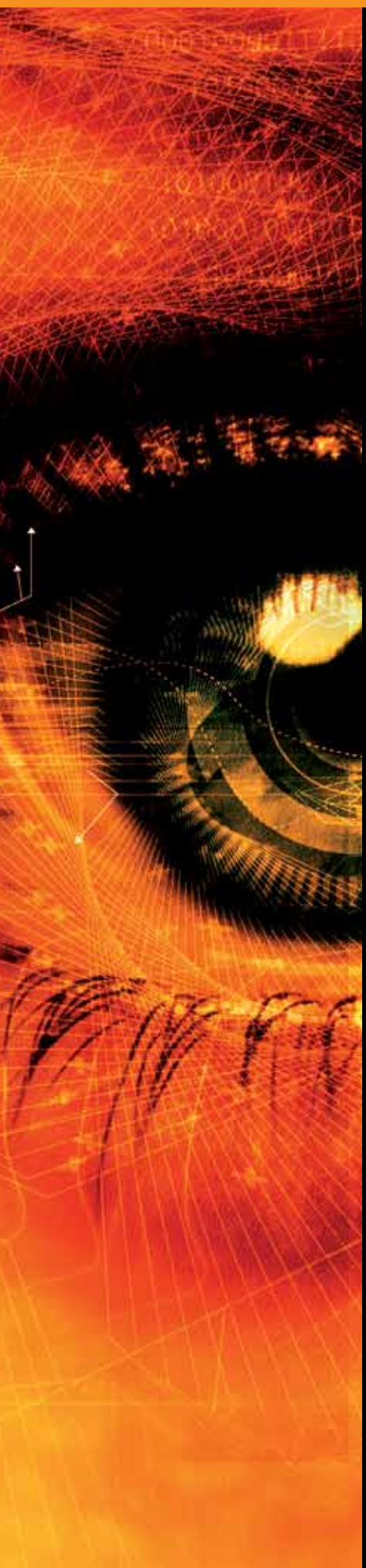
- slanje »zlonamjernih« elektroničkih poruka
- usađivanje štetnog koda na prijenosnom mediju
- postavljanje »zlonamjerne« aplikacije na mobilni uređaj
- priključivanje neautoriziranog uređaja u internu mrežu organizacije
- dobivanje informacija putem telefona, osobno, klasičnom ili elektroničkom poštom
- ulazak u poslovne prostore bez identifikacije na ulazu
- ulazak u zaštićeno područje davanjem identiteta drugoga

Na osnovi provedenih scenarija priprema se izvješće sa statistikom uspješnosti napada i prijedlozi za poboljšanje osviještenosti zaposlenika na području informacijske sigurnosti i nadgradnju postojećih sigurnosnih mehanizama.

Informacije
SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

SIQ
www.siq.hr

ANALIZA SLUČAJNOSTI, STATISTIČKA ANALIZA



Primjenjujete li u radu proces generiranja slučajnosti? Zanima li Vas postiže li stvarno svoju svrhu?

U poslovnom svijetu često se pojavljuje potreba za generatorom slučajnosti, na primjer kod primjene statističkih metoda u financijskoj ili istraživačkoj sferi, kod algoritama šifriranja, kod izbora pobjednika nagradnih igara, kod izbora rasporeda ekipa za natjecanja, kod izbora sudionika anketa u masi kandidata i slično.

Generator slučajnosti može biti mehanički/fizički (npr. kocke, loptice, kolo sreće, šumna dioda), algoritamski (programski kod) ili kombinirani.

Nudimo stručnu analizu generatora slučajnosti na osnovi koje utvrđujemo postiže li primijenjeni postupak ili oprema stvarno svoju svrhu. Analiza može obuhvaćati više sklopova:

- statistička analiza slučajnosti brojeva/rezultata (primjenjujemo mnogo poznatih statističkih metoda; izbor metoda možemo prilagoditi željama stranke)
- kod mehaničkog/fizičkog generatora analiza može uključivati detaljna dimenzijska mjerenja (npr. mjerenja razmaka na kolu sreće) i mjerenja težine (npr. jednaka težina loptica za izvlačenje)
- kod algoritamskog generatora analiza uključuje i potporne procese koji nisu dio generatora slučajnih brojeva, a vrlo su važni za konačnu slučajnost (npr. algoritam skaliranja brojeva, tzv. »seeding« algoritam, algoritam prijenosa generirane slučajne vrijednosti do krajnjeg korisnika itd.)

Uslugu statističke analize podataka nudimo i za slučajeve koji ne uključuju generiranje slučajnosti ni na kojim podatcima koje upotrebljava stranka.

Informacije
SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

SIQ
www.siq.hr

PREGLED PROGRAMSKE OPREME

Trebate li neovisan i stručan pregled programske opreme?

Ako trebate neovisno izvješće o radu programske opreme (softvera) koju su razvili Vaši programeri ili Vaši poslovni partneri, možemo Vam ponuditi stručni pregled programske opreme. Ciljevi pregleda mogu biti različiti; na primjer, potvrda:

- da programska oprema uistinu izvršava samo dokumentirane funkcije
- da programska oprema određene kritične funkcije obavlja pravilno (npr. obračunavanje novca, pretvaranje količina itd.)
- da programska oprema odgovarajuće podupire dogovorene protokole (npr. komunikacijske)
- da je programska oprema kompatibilna s drugom programskom ili strojnom opremom (tzv. »inter-operability« testiranja)
- ugrađenih razina pristupa, zaštita, upotrijebljenog šifriranja
- da moguća ugrađena slučajnost (RNG) postiže svoju svrhu
- da izvedbeni kod stvarno odgovara dostavljenom izvornom kodu
- ispunjava li programska oprema izabrane zakonske zahtjeve (na primjer zakonske zahtjeve u području poreznih blagajni, s obzirom na mjerne instrumente, s obzirom na sigurnost potrošačkih proizvoda itd.)
- nekih drugih specifičnih zahtjeva

Pregled provesti na dvije razine:

- provjera izvedbenog koda (tzv. »black box« testiranje)
- provjera izvedbenog koda i istodobno prevođenje u izvedbeni kod u suradnji s programerom (produbljena analiza)

Pregled u nekim slučajevima možemo obaviti i na daljinu.

Informacije
SIQ Croatia d.o.o.
Provjera informacijskih tehnologija
T: +385 1 65 51 305
E: info@siq.hr

SIQ
www.siq.hr