SI

INFORMACIJSKA VARNOST

Preverjanje
informacijskih
tehnologij

Zakaj SIQ?

Stabilnost:

Naše delo sloni na celovitih rešitvah, partnerskem odnosu, neodvisnosti in nepristranskosti. Skladno s temi načeli že več kot 50 let preskušamo, certificiramo in kontroliramo proizvode in sisteme, umerjamo merilne naprave, ocenjujemo in certificiramo sisteme vodenja ter prenašamo izkušnje in znanje. SIQ je vpet v mednarodno okolje; sodelujemo s partnerji s celega sveta ter izdajamo globalno priznana poročila in certifikate.

Izkušnje:

Smo ekipa izkušenih strokovnjakov z dolgoletnimi izkušnjami na področju pregledov programske opreme, informacijskih sistemov, varnostnih pregledov in zagotavljanja celovitega varovanja informacij. Strokovnost kadrov potrjujejo ugledni mednarodni certifikati in številne zadovoljne stranke.

Zaupanje:

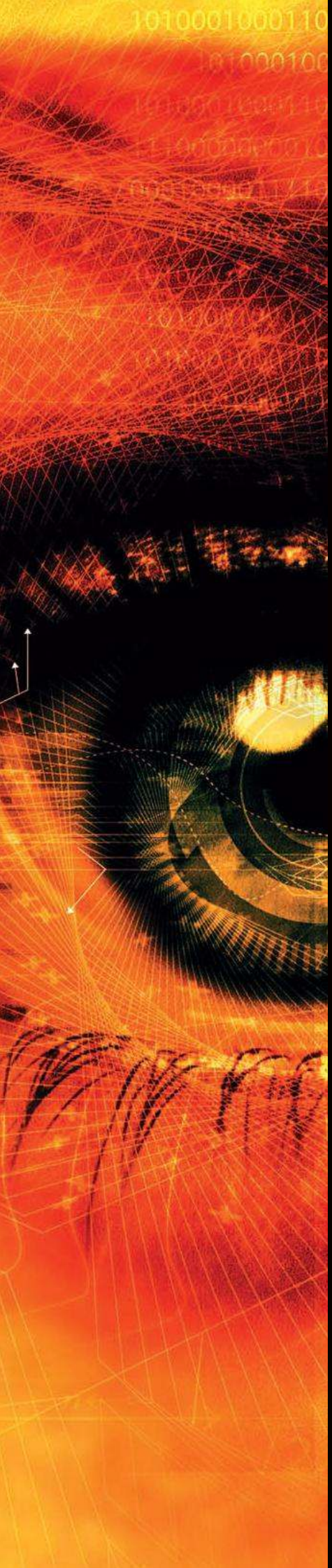
Za pregled s strani neodvisne organizacije je ključno popolno zaupanje stranke, saj stranka med pregledom razkriva svoje najobčutljivejše podatke, postopke in znanje. V SIQ je tako zaupanje upravičeno:

- Imamo okoli 140 zaposlenih in aktivno spodbujamo nizko fluktuacijo zaposlenih.
- Imamo stroga določila v pogodbah o zaposlitvi glede zaupnosti informacij.
- Naše storitve so akreditirane in priznane s strani številnih mednarodno uveljavljenih akreditacijskih organov in shem.
- Redno smo podvrženi najrazličnejšim in pogosto zelo obsežnim preverjanjem svojih postopkov, prostorov in osebja s strani različnih domačih in tujih organov in organizacij.
- Imamo dodelano predlogo sporazuma o nerazkrivanju informacij (NDA – Non-disclosure Agreement), ki jo lahko prikrojite po svoje, lahko pa tudi uporabite svojo.
- Poklicno odgovornosti imamo ustrezno zavarovano.

Konkurenčnost:

Znamo prisluhniti potrebam in željam strank. S sistematičnim in učinkovitim pristopom lahko naše storitve ponudimo po konkurenčnih cenah in v hitrih izvedbenih rokih.

SIQ
www.siq.si



Varnostni pregled informacijskega sistema

Zaščitite svoje poslovanje

V današnjem svetu elektronskega poslovanja prihaja do vse več zlorab podatkov, zato je njihovo varovanje ključnega pomena za dolgoročno uspešnost organizacije. Najbolje je možnosti zlorab preprečiti, in sicer z ustrezno varovanimi dostopi do podatkov in storitev znotraj organizacije ter do javnih storitev na spletu.

Varnostni pregled je namenjen odkrivanju morebitnih groženj in ranljivosti vašega informacijskega sistema ter z njimi povezanih tveganj za varnost informacij. To je najučinkovitejši način preverjanja dejanske stopnje varnosti, saj se uporabljajo enake metode, tehnike in orodja, kot jih v praksi uporabljajo hekerji. Z izvedbo varnostnega pregleda boste dobili nedvoumen odgovor, ali so varnostne kontrole v vašem informacijskem sistemu ustrezne, in s tem ustrezno zaščitili poslovanje vaše organizacije.

Z varnostnim pregledom boste dobili odgovore na vprašanja:

- Ali je vaš informacijski sistem ustrezno zaščiten, da ne boste postali žrtev spletnega napada?
- Ali ste pravilno postavili politike vaše varnostne infrastrukture, da jih vaši zaposleni in pogodbeni sodelavci ne morejo zaobiti ter nepooblaščeno dostopati do vaših podatkov?
- Ali imajo uporabniki vaših poslovnih aplikacij res dostop le do tistih podatkov, ki jih potrebujejo?
- V kaj vlagati sredstva, da se izognete stroškom ali zmanjšate stroške zaradi izgube ali kraje podatkov, nedelovanja storitve, kršitve zakonodaje ali izgube ugleda pri strankah?
- Ali veste, kakšni so trendi zlorab informacijskih sistemov v Sloveniji in tujini ter kakšne so potrebne varnostne kontrole, ki jih morate uvesti?

Glavni cilj varnostnega pregleda je oceniti, katere varnostne kontrole v informacijskem sistemu še potrebujejo izboljšave. Poleg tega lahko s predstavitvijo rezultatov varnostnega pregleda upravljavce in uporabnike informacijskega sistema seznanimo z odkritimi ranljivostmi in jih usposobimo, da poskrbijo za ustrezno varovanje informacij pri vsakodnevnem izvajanju svojega dela.

SIQ Ljubljana s svojo ekipo izkušenih strokovnjakov s področja informacijske varnosti izvaja celovit nabor varnostnih pregledov, ki jih prilagodimo glede na vaše potrebe. Izvajamo standardne varnostne preglede (avtomatizirani pregled ranljivosti, zunanji in notranji varnostni pregledi) in specializirane preglede glede na potrebe naročnika (skladnost s PCI DSS – ASV in QSA, varnostni pregled aplikacij, pregled mobilnih naprav, pregled igralniških sistemov, pregled izvorne kode, pregled sistemov SCADA, pregled VoIP/IP telefonije, socialni inženiring, revizijski pregled informacijskega sistema).

Informacije

SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

www.siq.si

VARNOSTNI PREGLED INFORMACIJSKE INFRASTRUKTURE

Ali zaupate vsem članom vaše IT?

S polnim razmahom elektronskih komunikacij je postala varnost informacijskih sistemov ključnega pomena za poslovanje organizacij. Varna postavitev in vzdrževanje informacijske infrastrukture sta še posebej pomembna, saj s kompleksnostjo in raznolikostjo informacijskih sistemov narašča možnost varnostnih pomanjkljivosti, težje pa jih je tudi odkriti. Varnost celotnega informacijskega sistema je namreč odvisna od najšibkejšega člena. Že ena varnostna pomanjkljivost lahko izniči številne vpeljane varnostne ukrepe (npr. privzeta administrativna gesla).

Splošni pregled ranljivosti

S takšnim pregledom boste dobili osnovno informacijo o izpostavljenosti vaše informacijske infrastrukture zlonamerni kodi in najpogostejšim grožnjam, ki jih zaradi znanih ranljivosti ali napak v konfiguraciji lahko izkoristijo že neizkušeni napadalci. Pregled se izvede z avtomatiziranimi orodji, ki z različnimi tehnikami in posebno oblikovanimi zahtevki sistematično preverijo dostopnost storitev in znane ranljivosti. Tovrstni pregledi se najpogosteje izvajajo v organizacijah, ki so dolžne redno preverjati stanje informacijske varnosti zaradi zahtev IT revizorjev.

Zunanji varnostni pregled (vdorno testiranje)

Namenjen je odkrivanju morebitnih varnostnih groženj, ki pretijo informacijski infrastrukturi iz javno dostopnega omrežja. Pri tem se uporabljajo metode in orodja, ki so prisotna ob dejanskih spletnih napadih. Ciljni sistemi, ki se preverjajo, so spletni strežniki in spletne poslovne aplikacije, poštni strežniki in druge podporne storitve, uporabljeni varnostni sistemi in mehanizmi zaščite (požarni zidovi, IPS itd.) ter druge javno dostopne storitve organizacije.

Notranji varnostni pregled

Namen je odkriti morebitne varnostne grožnje in ranljivosti informacijske infrastrukture ob namernih ali nenamernih škodljivih aktivnostih zaposlenih oziroma ob napadu iz notranjega omrežja. Zajema pregled ustreznega načrtovanja informacijskega sistema, pregled dostopnosti ter nastavitev strojne in programske opreme, pregled VoIP/IP telefonije, pregled brezžičnega omrežja in mobilnih naprav, pregled ustreznosti varnostne politike in pravil vzdrževanja sistemov ter varnostni pregled ključne programske opreme.

Informacije

SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

SIQ
www.siq.si

VARNOSTNI PREGLED APLIKACIJ

Ali imajo uporabniki aplikacij res dostop le do svojih podatkov?

Varnostni pregled aplikacij je namenjen odkrivanju morebitnih varnostnih groženj in pomanjkljivosti posameznih aplikacij. Le-te lahko ob zlonamernem napadu omogočijo izvedbo nepooblaščenih sprememb, ki lahko vplivajo na zaupnost, razpoložljivost in celovitost podatkov v sami aplikaciji (npr. nepooblaščen dostop, spreminjanje podatkov, nedelovanje aplikacije).

V ozadju delovanja aplikacij so lahko različne tehnologije (spletne, mobilne, klasične). Ne glede na njihovo vrsto so lahko varnostne grožnje na strani:
- odjemalca,
- omrežja oz. transportne poti ter
- strežniške infrastrukture.

Celovit varnostni pregled aplikacij zato poteka v več fazah, znotraj katerih podrobno preučimo arhitekturo aplikacije, gradnike in samo delovanje aplikacije. Tipične pomanjkljivosti aplikacij so:
- dostop do podatkov brez prijave;
- neustrezna lokalna hramba podatkov;
- izvedba akcij v imenu drugega uporabnika, kot so izvedba transakcij, vklop/izkop storitev itd.;
- sprememba gesla drugega uporabnika in s tem prevzem njegovega uporabniškega računa;
- eskalacija privilegijev uporabniških pravic, ki uporabniku omogočijo več možnih aktivnosti, npr. spremembo cen itd.;
- dostop do podatkov oziroma spreminjanje podatkov drugega uporabnika.

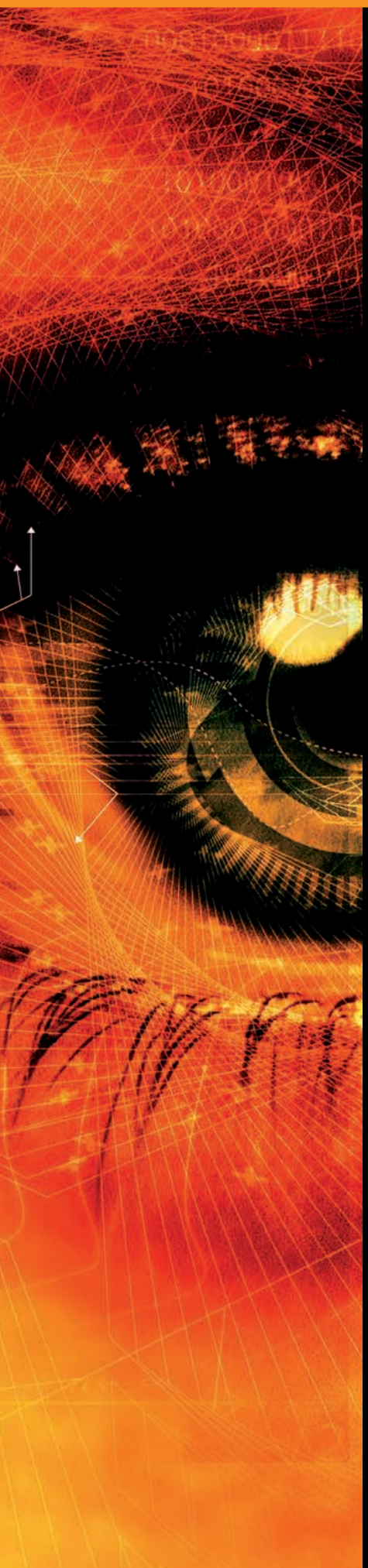
S podrobnim varnostnim pregledom, ki vključuje tudi uporabniško prijavo, dobite nedvoumen odgovor, ali so varnostne kontrole v aplikaciji ustrezne.

Najpodrobneje pa lahko varnostne pomanjkljivosti odkrijemo s pregledom izvorne kode aplikacij, saj so prav napake v kodiranju primarni vir težav. Pri tem je pomembno, da izvorno kodo preverijo neodvisni strokovnjaki za aplikacijsko varnost, ki niso sodelovali pri razvoju aplikacije. Pregled izvorne kode aplikacije poteka v več korakih, pri čemer naročnik zagotovi vse razpoložljive informacije (princip »bele škatle«). V prvem koraku se uporabi namensko programsko orodje, ki prepozna varnostno problematična mesta v programski kodi. Le-ta se nato ročno natančno preveri v sodelovanju z razvijalcem programske opreme na strani naročnika ter svetovalcem za varnost in razvojnim specialistom na strani izvajalca. V zadnjem koraku se s penetracijskim testom nedvoumno še potrdi ugotovljene varnostne pomanjkljivosti.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

SIQ
www.siq.si

REVIZIJSKI PREGLED INFORMACIJSKEGA SISTEMA



Zagotavljate skladnost z zakonodajo in dobrimi praksami upravljanja informacijskega sistema?

Informacijski sistemi so neločljivo vpeti v poslovanje vseh vrst organizacij. Brez zanesljivega, dobro upravljanega in varnega informacijskega sistema si vsakodnevnega poslovanja ne moremo več predstavljati. Redni revizijski pregledi informacijskega sistema pripomorejo, da se z izvajanjem predpisanih priporočil zmanjša možnost incidentov, ki bi lahko vplivali na zaupnost, razpoložljivost ali celovitost podatkov ter organizaciji povzročili poslovno škodo. Revizijski pregled informacijskega sistema predstavlja sistematično in strokovno presojo tehničnih in organizacijskih kontrol v informacijskem sistemu. Namen je preveriti skladnost s predpisi, standardi in dobrimi praksami na področju informatike. Pregled je sestavljen iz ocene stanja, analize tveganj in presoje kontrol. Na podlagi pregleda ugotovimo, ali informacijski sistem v organizaciji podpira poslovne cilje ter ali učinkovito, varno in zanesljivo deluje. Z revizijskim pregledom pridobite neodvisno strokovno mnenje glede skladnosti s predpisi, standardi in dobrimi praksami. Nudimo naslednje storitve:

- Revizijski pregled celotne informacijske infrastrukture
- Revizijski pregled informacijske varnosti (ISO/IEC 27001)
- Revizijski pregled upravljanja storitev IT (ISO/IEC 20000-1)
- Revizijski pregled neprekinjenega poslovanja (ISO 22301)
- Revizijski pregled projektnega vodenja v informatiki
- Pregled programske opreme (funkcionalnost, varnost)
- Revizijski pregled upoštevanja zakonodajnih določil s področja varovanja podatkov (ZVOP, ZTP, ZVDAGA, ZEKOM)

Revizijske preglede informacijskega sistema izvajajo naši strokovnjaki z dolgoletnimi izkušnjami na področju presojanja in revidiranja (PRIS, CISA, CISM, VP ISO/IEC 27001, VP ISO/IEC 20000-1). Rezultat je revizijsko poročilo s podrobnim opisom vseh ugotovitev ter predlogi za izboljšave upravljanja informacijskega sistema.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

www.siq.si

ZAUPANJE V ELEKTRONSKE TRANSAKCIJE (eIDAS)

Izvajanje zakonodajnih določil s področja elektronske identifikacije

SIQ nudi celovito certifikacijo storitev zaupanja po uredbi eIDAS po zadevnih standardih ETSI za:

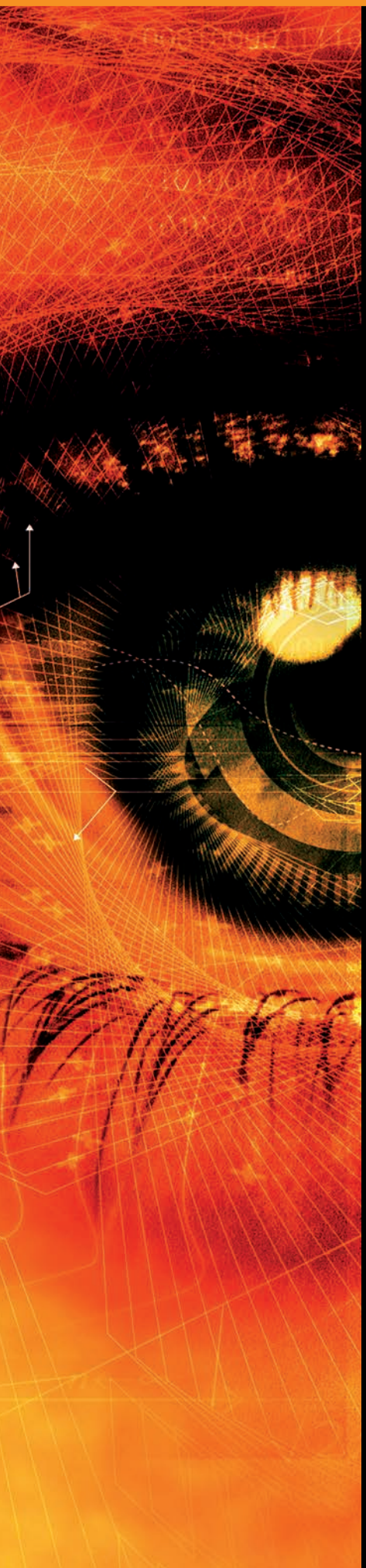
- elektronski podpis,
- elektronski žig,
- elektronski časovni žig,
- storitev elektronske priporočene dostave,
- avtentikacijo spletišč.

Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (eIDAS) je bila sprejeta s ciljem krepitve zaupanja v elektronske transakcije na notranjem trgu, tako da se zagotavlja skupni temelj za varne elektronske interakcije med državljani, podjetji in javnimi organi, s čimer se povečuje učinkovitost javnih in zasebnih spletnih storitev, elektronskega poslovanja ter elektronskega trgovanja v Uniji.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

SIQ
www.siq.si

VARSTVO OSEBNIH PODATKOV (GDPR)



Pregled upoštevanja zakonodajnih določil s področja varovanja podatkov

Če v vaši organizaciji upravljate z osebnimi podatki vam v SIQ Ljubljana lahko pomagamo v celotnem procesu vzpostavitve in vzdrževanja skladnosti z GDPR.

Naše storitve zajemajo:

- Pregled skladnosti pravilnikov in politik podjetja
- Pregled privolitev posameznika
- Pregled hrambe podatkov
- Pregled evidenc dostopa do podatkov
- Tehnični in organizacijski ukrepi (revizija, vdorni testi, testi ranljivosti)
- Pregled pogodb (obdelovalec)
- Ocena učinka
- Kodeksi ravnanja
- Preverjanje programske in strojne opreme
- Večkratni pregledi skladnosti v obdobju veljavnosti certifikata
- Izobraževanje

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

www.siq.si

PREVERJANJE SKLADNOSTI S PCI DSS

Ali obdelujete podatke o kartičnem poslovanju?

PCI DSS (Payment Card Industry Data Security Standard) je varnostni standard mednarodnih plačilnih sistemov (American Express, Discover Financial Services, JCB International, MasterCard in Visa). Ponuja okvir za ustrezno zaščito podatkov uporabnika kartičnega poslovanja. Vse organizacije, ki obdelujejo, prenašajo, hranijo ali omogočajo dostop do kartičnih podatkov, morajo zadostiti zahtevam PCI DSS, kar dokazujejo z letnimi revizijami QSA, samoocenjevanjem SAQ ali četrtletnimi pregledi ranljivosti ASV. Zahtevani načini preverjanja so odvisni od letnega števila transakcij kartičnega poslovanja in so obvezni tako za trgovce, finančne ustanove (issuer, acquirer) kot procesne centre.

SIQ Ljubljana vam lahko pomaga v celotnem procesu vzpostavitve in vzdrževanja skladnosti s PCI DSS. Nudimo naslednje storitve:

Analiza razkoraka

Z analizo razkoraka ugotovimo odstopanja trenutnega stanja od zahtev standarda PCI DSS. Naši izkušeni in akreditirani revizorji prepoznajo vsa področja s pomanjkljivostmi in podajo priporočila za doseganje skladnosti. Rezultat analize je tudi določitev obsega infrastrukture, ki je podvržena zahtevam PCI DSS in je potrebna informacija pri samoocenjevanju SAQ.

Pomoč pri samoocenjevanju SAQ

Naši izkušeni in akreditirani strokovnjaki vam lahko pomagajo pri samoocenjevanju in izpolnjevanju vprašalnika SAQ. Pri tem vam podajo tudi priporočila za doseganje skladnosti s PCI DSS.

Revizija QSA

Revizijo QSA izvajajo naši akreditirani strokovnjaki (Qualified Security Assessors) z dolgoletnimi izkušnjami na področju informacijske varnosti (CISA, CISM). Vključuje temeljit pregled informacijskega okolja, ki je del kartičnega poslovanja, in se zaključi s poročilom o skladnosti (RoC).

Pregled ranljivosti ASV

Pregled ranljivosti ASV izvajajo naši akreditirani strokovnjaki (Approved Scanning Vendors) z dolgoletnimi izkušnjami na področju varnostnih preverjanj (EC CEH, GCIH, GPEN). Vključuje preverjanje ranljivosti vseh javno dostopnih sistemov, ki so del kartičnega poslovanja ali omogočajo povezavo do le-tega. Rezultat je izjava o skladnosti (AoC) s podrobnim poročilom o odkritih ranljivostih, razvrščenih po lestvici CVSS.

Informacije

SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

PCI Security Standards Council

SIQ
www.siq.si

SOCIALNI INŽENIRING

Ali vaši zaposleni vedo, kakšna so pravila varovanja informacij?

Organizaciji, ki ima opravka z večjim številom različnih profilov zaposlenih, predstavlja zagotavljanje ustreznega nivoja varovanja informacij velik izziv. Najučinkovitejši način preverjanja ozaveščenosti in izobraževanja zaposlenih je izvedba t. i. socialnega inženiringa.

Socialni inženiring je nabor tehnik, s katerimi napadalec prelisiči ali prepriča uporabnika, da izvede določeno aktivnost (npr. odpre zlonamerno elektronsko pošto, uporabi ključ USB, okužen s škodljivo kodo, itd.) in s tem napadalcu omogoči dostop do zaupnih podatkov organizacije. Pri tem napadalec izkoristi odziv uporabnika na določeno situacijo (npr. na vabljivo ponudbo, zaupanje, pripravljenost pomagati itd.).
Poznamo več oblik socialnega inženiringa:

- tehnične metode,
- osebni stik,
- grožnje in izsiljevanja.

Za izvedbo socialnega inženiringa je potrebno zbrati veliko informacij o organizaciji in potencialnih tarčah (zaposlenih). Informacije se lahko pridobivajo s pomočjo javno dostopnih informacij (internetne strani, telefonski imeniki itd.), obiskov organizacije ali navezovanja prijateljskih stikov z zaposlenimi.

Primeri scenarijev preverjanja zaposlenih:

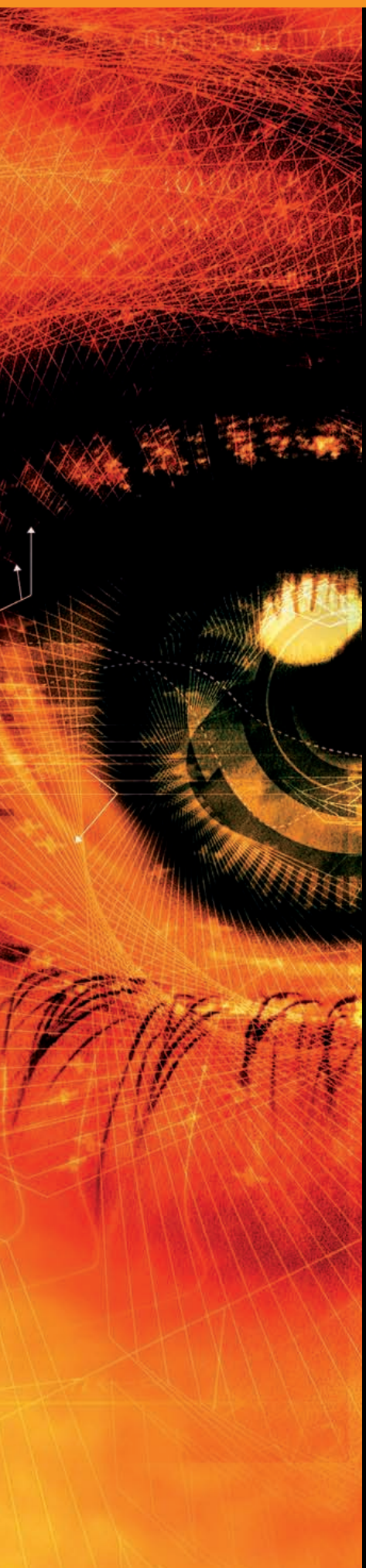
- pošiljanje »zlonamernih« elektronskih sporočil,
- podtikanje škodljive kode na prenosnem mediju,
- namestitev »zlonamerne« aplikacije na mobilni napravi,
- priklop neavtorizirane naprave v interno omrežje organizacije,
- pridobivanje informacij preko telefona, osebno, po klasični ali elektronski pošti,
- vstop v poslovne prostore brez identifikacije pri vhodu,
- vstop v varovano območje z izdajanjem identitete drugega.

Na podlagi izvedenih scenarijev se pripravi poročilo s statistiko uspešnosti napadov ter predlogi za izboljšanje ozaveščenosti zaposlenih na področju varovanja informacij in za nadgradnjo obstoječih varnostnih mehanizmov.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

www.siq.si

ANALIZA NAKLJUČNOSTI, STATISTIČNA ANALIZA



Ali pri delu uporabljate proces generiranja naključnosti? Vas zanima, če v resnici dosega svoj namen?

V poslovnem svetu se pogosto pojavi potreba po generatorju naključnosti, na primer pri uporabi statističnih metod, algoritmih šifriranja, pri izbiri zmagovalcev nagradnih iger, razporejanju tekmovalnih ekip, pri izbiri anketirancev in drugje ...

Generator naključnosti je lahko mehanski/fizični (npr. kocke, žogice, kolo sreče, šumna dioda), algoritmični (programska koda) ali kombinirani.

Nudimo strokovno analizo generatorja naključnosti, na podlagi katere ugotavljamo, ali uporabljeni postopek in oprema resnično dosegata svoj namen. Analiza lahko obsega:

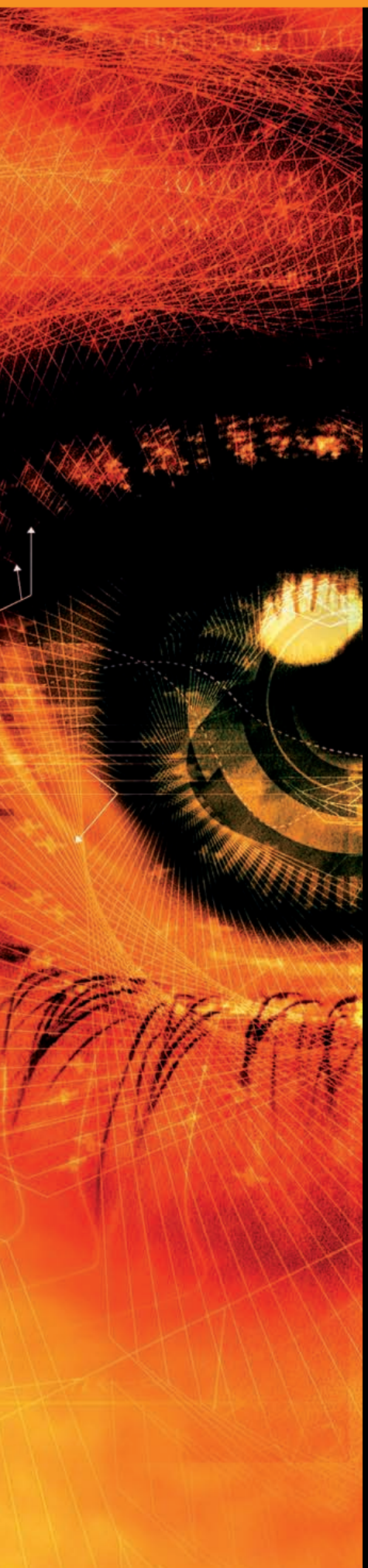
- statistično analizo naključnosti števil/izidov (uporabljamo vrsto uveljavljenih statističnih metod; izbor metod lahko prilagodimo željam stranke);
- pri mehanskem/fizičnem generatorju lahko analiza vključuje natančne dimenzijske meritve (npr. meritve razmikov na kolesu sreče) in meritve teže (npr. enaka teža žrebalnih žogic);
- pri algoritmičnem generatorju analiza vključuje tudi podporne procese, ki niso del generatorja naključnih števil, so pa prav tako pomembni za končno naključnost (npr. algoritem skaliranja števil, t. i. »seeding« algoritem, algoritem prenosa generirane naključne vrednosti do končnega uporabnika itd.).

Storitev statistične analize podatkov nudimo tudi za primere, ki ne vključujejo generiranja naključnosti, na kakršnih koli podatkih, ki jih uporablja stranka.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

SIQ
www.siq.si

PREGLED PROGRAMSKE OPREME



Potrebujete neodvisen in strokoven pregled programske opreme?

Če potrebujete neodvisno poročilo o delovanju programske opreme, ki so jo razvili vaši programerji ali pa vaši poslovni partnerji, vam lahko ponudimo strokoven pregled programske opreme. Cilji pregleda so lahko različni, na primer potrditev:

- da programska oprema resnično izvaja le dokumentirane funkcije;
- da programska oprema določene kritične funkcije izvaja pravilno (npr. obračunavanje denarja, pretvarjanje količin itd.);
- da programska oprema ustrezno podpira dogovorjene protokole (npr. komunikacijske);
- da je programska oprema združljiva z drugo programsko ali strojno opremo (t. i. »inter-operability« preskusi);
- vgrajenih nivojev dostopa, zaščit, uporabljenega šifriranja;
- da morebitna vgrajena naključnost (RNG) dosega svoj namen;
- da izvedbena koda dejansko ustreza dostavljeni izvorni kodi;
- da programska oprema izpolnjuje izbrane zakonske zahteve (na primer zakonske zahteve glede davčnih blagajn, merilnih instrumentov, varnosti potrošniških izdelkov itd.);
- kakršnih koli drugih specifičnih zahtev.

Pregled lahko izvedemo na dveh nivojih:

- preverjanje izvedbene kode (t. i. »black box« preskušanje);
- preverjanje izvorne kode in hkratno prevajanje v izvedbeno kodo v sodelovanju z razvijalcem programske opreme (poglobljena analiza).

Pregled lahko v nekaterih primerih izvedemo tudi na daljavo.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

SIQ
www.siq.si