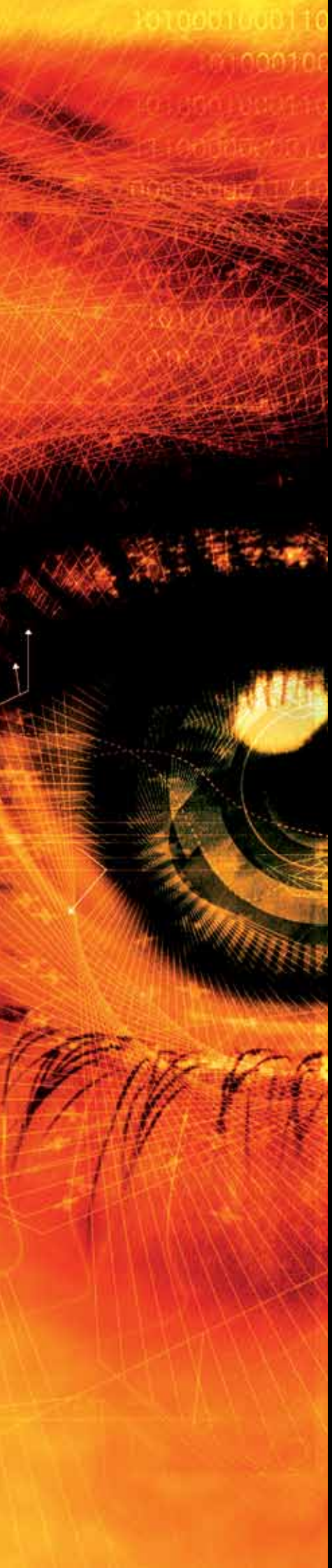


Controllo di sicurezza del sistema informatico

Proteggete la vostra attività

Oggigiorno, nel mondo dell'e-commerce, i casi di abuso di dati sono sempre più frequenti, pertanto per il successo di un'azienda la loro protezione è fondamentale. Considerata tale situazione la miglior soluzione è impedirne le possibilità di abuso, precisamente tramite opportune protezioni agli accessi ai dati ed ai servizi sia interni all'azienda che pubblici attraverso la rete.

Il controllo di sicurezza è focalizzato sulla scoperta di eventuali minacce e vulnerabilità del vostro sistema informatico e rispettivamente delle informazioni. Poiché vengono usati metodi, tecniche e strumenti uguali a quelli usati dagli hackers, questo sistema di verifica risulta il modo più efficace per verificare il grado effettivo della sicurezza del sistema informatico. Tramite il controllo di sicurezza avrete una risposta certa se i meccanismi di sicurezza del vostro sistema informatico siano adeguati, garantendo protezione all'attività stessa della vostra azienda.

Il controllo di sicurezza risponderà alle vostre seguenti domande:

- Il vostro sistema informatico è sufficientemente protetto per non diventare vittima di un attacco online?
- Le politiche della vostra infrastruttura di sicurezza sono tali da evitare che i vostri dipendenti e collaboratori possano eluderli accedendo di conseguenza ai dati per cui non hanno autorizzazione?
- Gli utenti delle vostre applicazioni aziendali possono di fatto accedere solo ai dati di cui hanno effettivamente bisogno?
- Come investire per evitare o ridurre i costi causati della perdita o dal furto di dati, malfunzionamenti del sistema, violazioni della legge o perdita di rispetto da parte dei clienti?
- Conoscete le attuali tendenze in ambito di sicurezza informatica e quali sono i controlli da introdurre?

L'obiettivo principale del controllo di sicurezza è valutare quali meccanismi del sistema informatico necessitano ancora di miglioramenti. Per di più, con la presentazione dei risultati dei controlli eseguiti, possiamo informare sia i gestori sia gli utenti del sistema delle vulnerabilità rivelate dandogli la possibilità di curare adeguatamente la protezione delle informazioni durante il quotidiano svolgimento del loro lavoro.

La società SIQ Italia S.r.l. con il suo team di esperti nel settore della sicurezza informatica esegue una serie completa di controlli di sicurezza adattabili alle vostre esigenze. Forniamo sia controlli standard (verifiche automatizzate della vulnerabilità, controlli di sicurezza interni ed esterni) che controlli specifici in base alle necessità del cliente (conformità con PCI-DSS – ASV e QSA, controlli sui meccanismi di sicurezza delle applicazioni, dei dispositivi mobili, dei sistemi di gioco, dei codici sorgenti, dei sistemi SCADA, della telefonia VoIP/IP, ingegneria sociale, revisione del sistema informatico).

Informazioni

SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

INGEGNERIA SOCIALE

I vostri dipendenti sono a conoscenza delle regole di protezione delle informazioni?

Garantire un adeguato livello di sicurezza delle informazioni presenta una grande sfida per un'organizzazione che ha a che fare con un gran numero di differenti profili di dipendenti. Il modo più efficace di verificare la consapevolezza e la formazione dei dipendenti è l'implementazione della così detta ingegneria sociale.

L'ingegneria sociale è un insieme di tecniche con cui l'hacker inganna o induce l'utente a eseguire una determinata attività (ad esempio: aprire una e-mail pericolosa, utilizzare una chiavetta USB contenente codice dannoso) consentendogli così l'accesso alle informazioni confidenziali dell'organizzazione. L'hacker infatti usufruisce solitamente delle reazioni degli utenti a una determinata situazione (un'offerta attraente, fiducia, disponibilità ad aiutare, ecc.). Ci sono diverse forme di ingegneria sociale:

- Metodi tecnici,
- Contatto personale,
- Minacce e ricatti.

Per realizzare l'ingegneria sociale è necessario raccogliere molte informazioni sull'organizzazione e sui suoi potenziali bersagli (dipendenti). Le informazioni possono essere ottenute utilizzando informazioni pubblicamente disponibili (pagine web, elenchi telefonici, ecc.), visite all'azienda o tramite contatti con i dipendenti stessi.

Esempi di scenari di verifiche dei dipendenti:

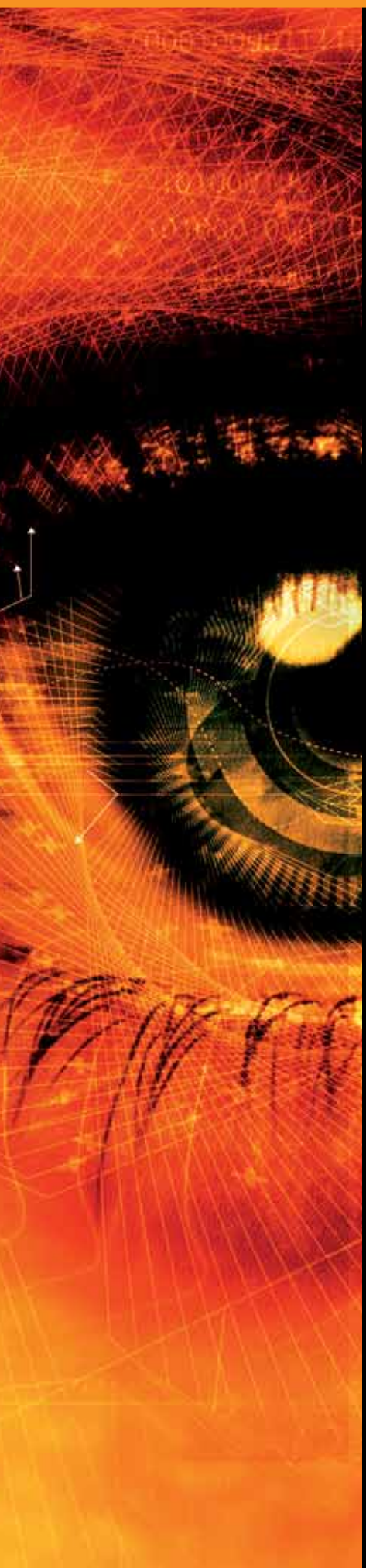
- invio di e-mail »ostili«
- installazione di codice dannoso su un mezzo di trasmissione
- installazione di un'applicazione »ostile« su un dispositivo mobile
- collegamento di un dispositivo non autorizzato nella rete interna dell'azienda
- acquisizione delle informazioni per telefono, di persona, via posta regolare o e-mail
- accesso ai locali di lavoro senza identificarsi all'entrata
- accesso alla zona protetta con il badge di un'altra persona.

In base ai scenari eseguiti viene preparato il rapporto comprendente la statistica sull'efficacia degli attacchi e i suggerimenti per il miglioramento della consapevolezza dei dipendenti nella protezione delle informazioni e dei meccanismi di sicurezza esistenti.

Informazioni
SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

CONTROLLO DI SICUREZZA DELLE APPLICAZIONI



Gli utenti delle applicazioni hanno davvero l'accesso solo ai propri dati?

Il controllo di sicurezza delle applicazioni è progettato per rilevare potenziali minacce di sicurezza e lacune delle singole applicazioni. In caso di attacco ostile infatti, queste possono permettere modifiche non autorizzate che potrebbero influire sulla riservatezza, disponibilità ed integrità dei dati nell'applicazione stessa (per esempio accesso non autorizzato, modifica dei dati, malfunzionamento dell'applicazione).

Le applicazioni possono funzionare in base a diverse tecnologie (web, mobile, classiche). Indipendentemente dal loro tipo, le minacce di sicurezza possono essere collegate a:

- Cliente
- Rete o percorsi di trasmissione
- Infrastruttura del server.

Il controllo di sicurezza delle applicazioni viene effettuato in più fasi all'interno delle quali studiamo in modo dettagliato l'architettura dell'applicazione, i suoi componenti e il suo funzionamento. Tipici difetti sono:

- accesso ai dati senza previa registrazione;
- archiviazione locale dei dati non idonea;
- esecuzione di azioni a nome di un altro utente, ad esempio attivazioni e disattivati azioni di sistemi
- modifica della password di un altro utente e il conseguente uso del suo account;
- aumento di privilegi dei diritti di utente che danno la possibilità di eseguire operazioni privilegiate (ad esempio variazione dii prezzi);
- accesso e modifica dei dati di un altro utente.

Con un controllo di sicurezza dettagliato, comprendente anche la registrazione degli utenti, riceverete una chiara risposta alla domanda se i controlli di sicurezza nell'applicazione sono adeguati.

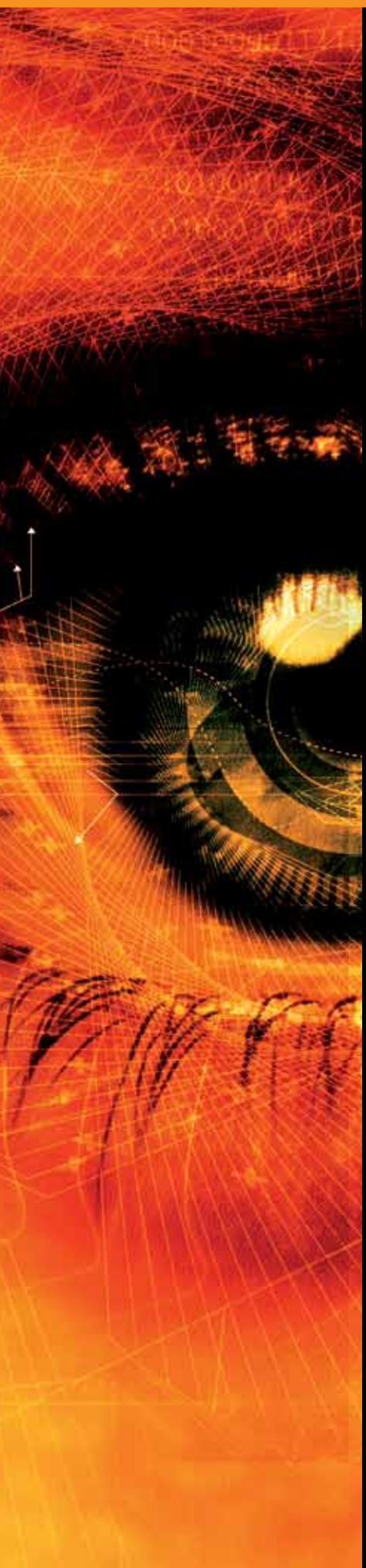
I difetti nella sicurezza possono essere rilevati nel modo più dettagliato tramite il controllo del codice sorgente delle applicazioni, essendo proprio gli errori di codifica la principale fonte di problemi. A questo punto è importante che il codice sorgente venga controllato dagli esperti di sicurezza applicativa che non hanno collaborato nello sviluppo dell'applicazione.
Il controllo del codice sorgente viene svolto in più fasi per cui il cliente fornisce tutte le informazioni disponibili (metodo »white box«). Nella prima fase viene usato un software specifico che identifica potenziali falle di sicurezza all'interno del codice sorgente. Dopodiché il risultato viene controllato dettagliatamente a mano assieme agli autori del software da parte del cliente e del consulente per la sicurezza e per evitare falsi positivi. Nell'ultima fase i difetti di sicurezza riscontrati vengono confermati con il test di penetrazione.

Informazioni

SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

REVISIONE DEL SISTEMA INFORMATICO



I tuoi sistemi IT sono conformi alla legge e alle norme pratiche?

I sistemi informatici sono parte integrante dell'attività di svariate organizzazioni. Senza un sistema informatico affidabile, ben gestito e sicuro non sono più immaginabili nemmeno le operazioni quotidiane. Le regolari revisioni del sistema informatico, come dalle istruzioni prescritte, riducono la possibilità di incidenti che potrebbero influire sulla riservatezza, disponibilità ed integrità dei dati, causando così dei danni commerciali all'organizzazione stessa. La revisione regolare del sistema informatico rappresenta la valutazione sistematica e professionale tramite controlli tecnici e organizzativi nel sistema stesso. L'obiettivo è la verifica della conformità con la regolamentazione, gli standard e le buone prassi nel settore informatico. La revisione consiste nella valutazione dello stato, nell'analisi dei rischi e nella valutazione dei controlli usati. In base alla revisione si verifica se il sistema informatico supporta gli obiettivi commerciali e funziona in maniera efficace, sicura ed affidabile. La revisione offre una perizia indipendente circa la conformità con la regolamentazione, gli standard e le buone prassi. Offriamo le seguenti prestazioni:

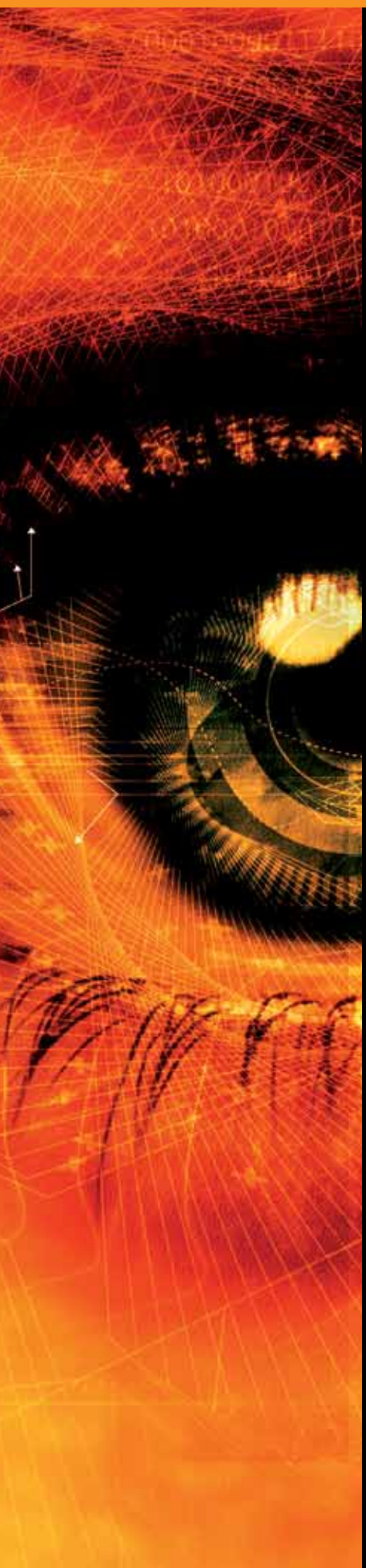
- Revisione dell'intera infrastruttura informatica
- Revisione della sicurezza informatica (ISO/IEC 27001)
- Revisione della gestione di servizi IT (ISO/IEC 20000-1)
- Revisione del funzionamento continuo (ISO 22301)
- Revisione della gestione dei progetti
- Revisione dei software (funzionalità, sicurezza)
- Revisione dell'osservanza delle disposizioni legislative nel settore della protezione dei dati

Le revisioni sono effettuate dai nostri esperti con anni di esperienza nel campo dell'analisi e revisione (PRIS, CISA, CISM, VP ISO/IEC 27001, VP ISO/IEC 20000-1). Il risultato è un rapporto contenente la descrizione dettagliata di tutte le constatazioni e proposte per migliorare la gestione del sistema informatico.

Informazioni
SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

CONTROLLO DI SICUREZZA DELL'INFRASTRUTTURA INFORMATICA



Vi fidate di tutti gli anelli della vostra IT?

Con la piena espansione delle comunicazioni elettroniche, la sicurezza dei sistemi informatici è diventata cruciale per la gestione dell'attività delle organizzazioni. Un'implementazione sicura e una buona manutenzione dell'infrastruttura informatica sono di estrema importanza, dato che la complessità e la diversità dei sistemi informatici aumentano la possibilità di difetti di sicurezza e ne rendono difficile la rilevazione. La sicurezza dell'intero sistema informatico dipende infatti dall'anello più debole: già un solo difetto può distruggere numerose misure di sicurezza (per esempio password amministrative).

Controllo generale della vulnerabilità

Tale controllo vi offrirà informazioni di base sull'esposizione della vostra infrastruttura informatica a codice maligno e altre minacce, che possono essere utilizzate dagli hackers a causa delle vulnerabilità o dei difetti nella configurazione del sistema informatico. Il controllo viene effettuato con degli strumenti automatizzati, i quali con diverse tecniche e richieste progettate ad hoc controllano sistematicamente l'accessibilità dei servizi e le vulnerabilità conosciute. I controlli di questo tipo sono per lo più eseguiti nelle aziende che devono controllare regolarmente lo stato di sicurezza informatica a causa delle esigenze dei revisori IT.

Controllo di sicurezza esterna (test di penetrazione)

Questo test è progettato per rilevare eventuali minacce alla sicurezza dell'infrastruttura informatica dalla rete esterna. Per tale scopo vengono usati i metodi e gli strumenti che sono tipicamente adottati negli attacchi web. I sistemi controllati sono i server e le applicazioni web, i server postali con i loro servizi di sostegno, i meccanismi di protezione (firewall, IPS, ecc.) ed altri servizi di pubblico accesso.

Controllo di sicurezza interna

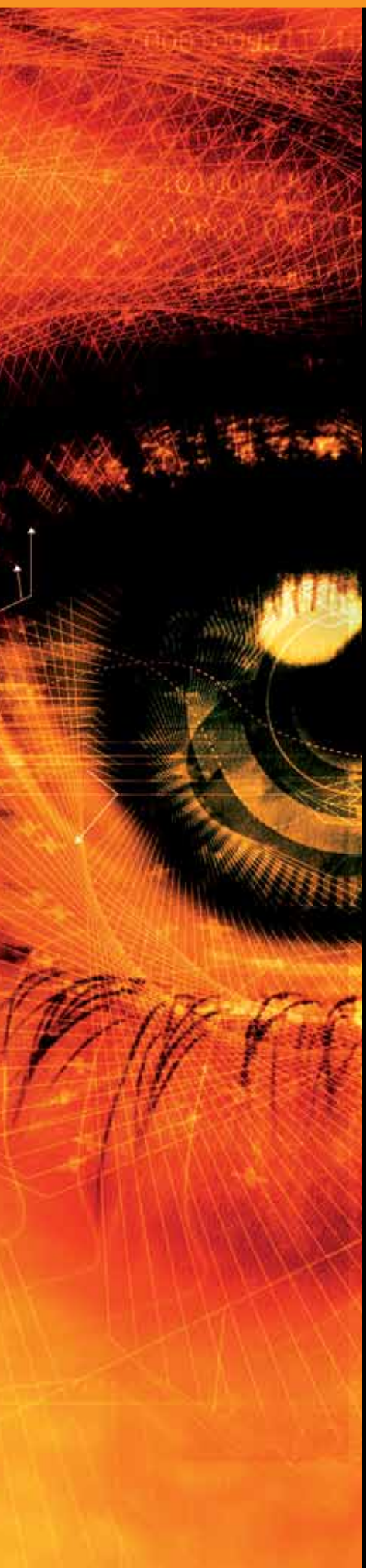
L'obiettivo è la rilevazione di eventuali minacce di sicurezza e vulnerabilità dell'infrastruttura informatica causate da attività dannose (premeditate o no) dei dipendenti, ovvero attacchi dalla rete interna. Il test comprende il controllo della corretta progettazione del sistema informatico, dell'accessibilità, delle impostazioni software e hardware, della telefonia VoIP/IP, della rete senza fili, dei dispositivi mobili, della politica di sicurezza e delle regole di manutenzione dei sistemi nonché il controllo di sicurezza del software chiave.

Informazioni

SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

VERIFICA DELLA CONFORMITÀ CON PCI-DSS



Elaborate i dati di commercio con carte elettroniche?

PCI-DSS (Payment Card Industry Data Security Standard) è uno standard di sicurezza dei sistemi di pagamento internazionale. Offre una piattaforma per la protezione appropriata dei dati degli utenti che utilizzano carte di pagamento. Tutte le organizzazioni che elaborano, trasmettono o archiviano i dati di carte di pagamento sono tenute ad adempiere ai requisiti PCI-DSS, provandolo tramite revisioni annuali QSA, autovalutazione SAQ o revisioni trimestrali della vulnerabilità ASV. Le modalità richieste dalla verifica dipendono dal numero annuo di transazioni con carte di pagamento e sono obbligatorie sia per i commercianti sia per le istituzioni finanziarie (issuer, acquirer) nonché i centri che ne processano i dati.

SIQ Italia S.r.l. può offrire il sostegno dell'intero processo di istituzione e manutenzione della conformità con PCI-DSS. Offriamo le seguenti prestazioni:

Analisi della divergenza

Tramite quest'analisi vengono constatate le divergenze dai requisiti dello standard PCI-DSS. I nostri esperti e accreditati revisori identificano tutte le aree difettose e propongono soluzioni per il raggiungimento delle conformità. Il risultato dell'analisi è anche la determinazione della quantità dell'infrastruttura soggetta alle esigenze PCI-DSS e presenta l'informazione necessaria per l'autovalutazione SAQ.

Supporto per l'autovalutazione SAQ

I nostri esperti ed accreditati professionisti possono offrirvi il supporto nell'autovalutazione e compilazione del questionario, presentandovi anche i suggerimenti per raggiungere la conformità con PCI-DSS.

Revisione QSA

La revisione QSA viene eseguita dai nostri esperti accreditati (Qualified Security Assessors) con delle esperienze pluriennali nel settore della sicurezza informatica (CISA, CISM). Questa comprende la revisione approfondita della piattaforma informatica parte del commercio con carte di pagamento, e sarà conclusa rilasciando un rapporto di conformità (RoC).

Controllo della vulnerabilità ASV

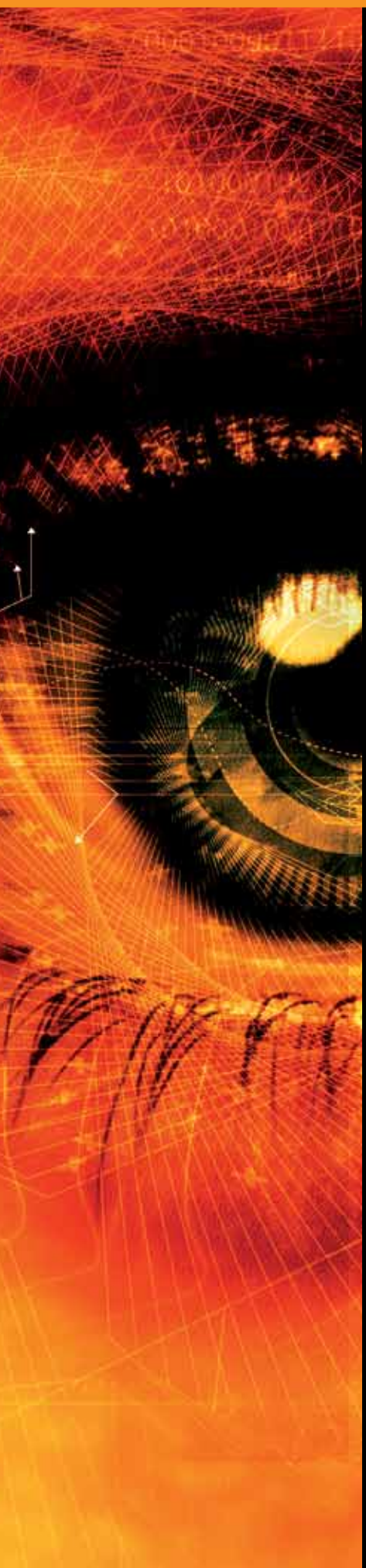
Il controllo della vulnerabilità viene eseguito dai nostri esperti accreditati (Approved Scanning Vendors) con lunghe esperienze nel settore dei controlli di sicurezza (EC CEH, GCIH, GPEN) e comprende il controllo della vulnerabilità di tutti i sistemi accessibili pubblicamente che fanno parte del commercio con carte di pagamento o che ne facciano collegamento in qualsiasi modo. Il risultato della verifica sarà la dichiarazione di conformità (AoC) con il rapporto dettagliato sulle vulnerabilità scoperte e classificate secondo la scala CVSS.

Informazioni

SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

ANALISI DELLA CASUALITÀ, ANALISI STATISTICA



Nel vostro lavoro dovete utilizzare numeri o eventi casuali? Vorreste verificare che la loro generazione sia adeguata alle vostre necessità?

Nel mondo del lavoro ci si scontra spesso con la necessità di una buona fonte di casualità, ad esempio nell'analisi statistica in ambito finanziario, negli algoritmi di cifratura, nel gioco d'azzardo, nella selezione di formazioni sportive, nella selezione degli intervistati per sondaggi, ecc.

La fonte principale di casualità (generatore di numeri casuali – RNG) può essere di tipo meccanico / fisico (dadi, palline, ruota della fortuna, rumore di un diodo, ecc.), algoritmico (codice software) oppure combinato.

SIQ fornisce un'analisi professionale del generatore di numeri casuali con la quale verifica che i processi e gli strumenti utilizzati per la generazione raggiungano effettivamente il loro scopo. L'analisi può basarsi su diversi approcci:

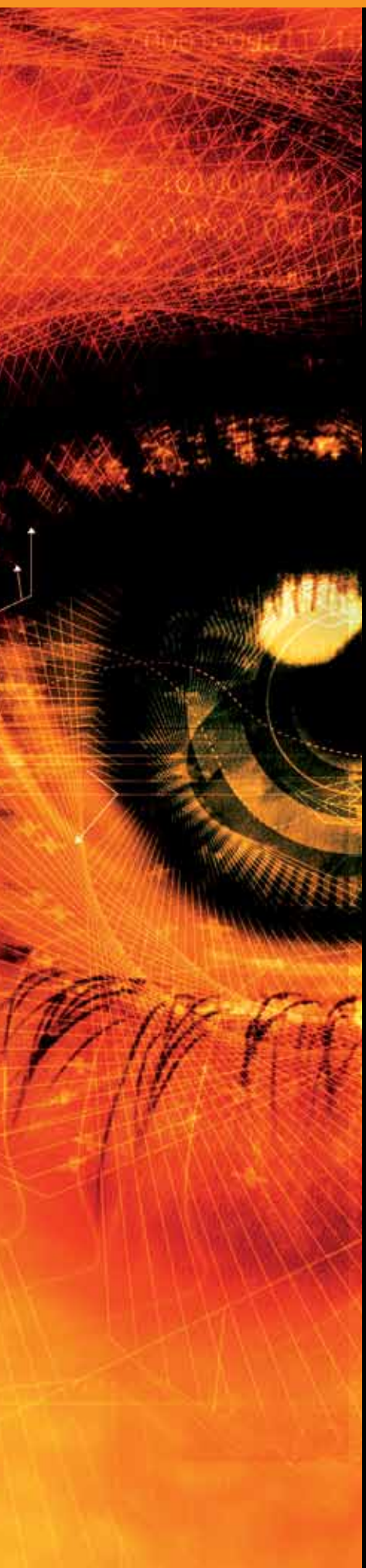
- analisi statistica della casualità dei numeri o dei risultati generati (utilizziamo una serie di metodi statistici consolidati che può essere personalizzata in base alle necessità del cliente),
- nel caso di generatori meccanici o fisici l'analisi può includere misurazioni dimensionali (es. misurazioni degli intervalli della ruota della fortuna) e misurazioni di peso (es. il peso delle palline da sorteggiare)
- per generatori algoritmici l'analisi comprende anche processi di supporto che non fanno parte del generatore di numeri casuali in sé, ma che sono importanti per la qualità della casualità prodotta (es. il ridimensionamento dei valori, l'algoritmo di generazione del seme, l'algoritmo di trasmissione dei valori generati fino al loro punto di utilizzo finale, ecc.).

SIQ offre inoltre servizi di analisi statistica su dati non basati sulla generazione di valori casuali, utilizzando processi e dati che meglio si adeguano alle necessità del cliente.

Informazioni
SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com

ANALISI SOFTWARE



Avete bisogno di un'analisi software indipendente e professionale?

Se avete bisogno di un resoconto indipendente sul funzionamento dei software sviluppati dai vostri programmatori o dai vostri partner commerciali, SIQ è in grado di offrirvi un'accurata analisi dei software stessi. Gli obiettivi della revisione possono variare, per esempio confermare che:

- il software fornisca solo le funzioni documentate,
- il software svolga correttamente tutte le funzioni critiche (es. contabilità , conversione degli importi, ecc.),
- il software supporti correttamente i protocolli concordati (es. quelli di comunicazione),
- il software sia compatibile con altri software o hardware (il cosiddetto test di "interoperabilità")
- integri diversi livelli di accesso, protezione e cifratura,
- l'eventuale fonte di casualità (RNG - generatore di numeri casuali) raggiunga il suo scopo,
- il codice eseguibile corrisponda effettivamente al codice sorgente fornito,
- il software soddisfi determinati requisiti di Legge (es. i requisiti legali per i registratori di cassa fiscali, strumenti di misura, sicurezza dei prodotti, ecc.),
- rispetti qualsiasi altro requisito specifico.

La revisione può essere di due tipi:

- controllo del codice eseguibile (analisi "black box"),
- controllo del codice sorgente e generazione del relativo codice eseguibile in collaborazione con gli sviluppatori del software stesso (analisi approfondita).

In alcuni casi SIQ può eseguire la revisione software anche da remoto.

Informazioni
SIQ Italia S.r.l.
Verifica delle tecnologie informatiche
T: +39 0481 209 50
E: info@siq-it.com

siq-it.com