Inside

INTELLIGENCE & SECURITY INVESTIGATIONS

InsideCyberSecurity

www.inside.agency • info@inside.agency

La tua nuova scelta nella gestione del rischio

CHI SIAMO

INSIDE, nel rispetto della compliance normativa, dei principi di etica professionale e delle regola della corporate governance, raccoglie informazioni, sul territorio nazionale ed internazionale, utili alle aziende nella gestione del rischio (c.d. risk management), quindi nella valutazione di rischi economici, finanziari e reputazionali di enti e persone fisiche con cui le stesse possono contrarre rapporti d'affari.

Tale insieme di notizie consente di **predisporre le strategie e le tecniche idonee a demolire le insidie** che connotano i vari settori del mercato (industrie farmaceutiche, automobilistiche, assicurazioni, finanziarie, pubbliche amministrazioni…) e che possono interessare tanto le piccole imprese quanto le società di dimensioni più consistenti.

I report rilasciati possono avere ad oggetto anche le cd. PEP, vale a dire le **persone politicamente esposte**, che ricoprono o che hanno in passato ricoperto cariche pubbliche, e che pertanto più facilmente sono esposte al rischio di commissione di particolari delitti quali corruzione, concussione, riciclaggio…

INSIDE **assiste le organizzazioni nella conoscenza dei propri partner commerciali**, orientando l'attività delle stesse a scelte più consapevoli, attraverso una serie di servizi che assicurano la compliance normativa e il mantenimento degli obblighi legali e di revisione (normative del Foreign Corrupt Practices Act - FCPA, Bribery Act del Regno Unito, norme antiriciclaggio – AML, Anti-Money Laundering, USA PARTRIOT Act e lotta al finanziamento del terrorismo – CFT, Countering the Financing of Terrorism); le ricerche effettuate - che possono avere ad oggetto tutti i settori di mercato e qualsiasi organizzazione, a prescindere dalla sua dimensione - consentono un controllo approfondito sulle possibili relazioni commerciali, mettendo in evidenza i rischi di corruzione derivanti da un'analisi geopolitica del caso.

I report forniscono ogni informazione concernente un'azienda e i suoi dirigenti, l'attività, la storia, l'amministrazione, i conflitti di interesse, le passività finanziarie, le vicende legali e giudiziarie (rischio di compliance), il rischio reputazionale. Sono inoltre comprensivi di verifiche delle dichiarazioni degli amministratori, compliance antiriciclaggio (AML), controlli anticorruzione e compliance alla normativa FCPA e UKBA, sanzioni contro l'Iran, procedure di due diligence internazionale e statunitense.

Il ricorso ai report INSIDE è consigliabile in generale per le verifiche su reati finanziari, ma non solo: le ricerche di INSIDE rappresentano **una valida soluzione in presenza di un rischio geopolitico** (Paese ad alto rischio) relativo ad una transazione o ad un individuo in esso coinvolto, per i controlli sulla supply chain e di due diligence, prima di investimenti importanti quali fusioni o acquisizioni, per **un programma di compliance integrato**.

INSIDE svolge in prima persona le indagini, consentendo in tal modo di mantenere alto il livello qualitativo e dei tempi, avvalendosi di un gran numero di **operatori dislocati nei cinque continenti, con oltre 60 lingue internazionali**; dispone inoltre di professionisti madrelingua, e che quindi possono apprendere quelle sfumature linguistiche spesso incomprensibili a chi non appartiene ad una determinata cultura. Tutte le informazioni e i dati raccolti «open source» sono numerosi e di qualità, poiché le varie fonti impiegate sono costantemente aggiornate da informazioni ufficiali estere.

La Divisione Cyber Security di INSIDE si propone di combattere il crimine informatico, e presta la propria assistenza non solo a supporto dell'attività delle forze dell'ordine, ma anche in ausilio delle aziende.

L'attenzione verso la **Sicurezza Informatica** è in forte espansione, dal momento che risulta ad oggi impossibile pensare di poter gestire le attività aziendali senza l'assistenza di sistemi informatici, ormai strumento imprescindibile all'interno dei processi produttivi delle aziende.

Per questa ragione è necessaria l'individuazione di una figura professionale che difenda dagli attacchi informatici che potrebbero seriamente mettere in pericolo il patrimonio più importante, il **Vostro know how**.

Attraverso la Divisione Cyber Security di INSIDE è possibile rilevare il **grado di vulnerabilità** dei Vostri sistemi e, a seguito di un'attenta analisi diagnostica, individuare gli interventi idonei alla messa in sicurezza della Vostra proprietà informatica.

Grazie all'esperienza maturata nel settore, agli elevati standard di qualità e sicurezza conseguiti e con il supporto del personale tecnico altamente qualificato di cui dispone, la Divisione Cyber Security di INSIDE ha come obiettivo principale quello di analizzare e potenziare la **sicurezza delle infrastrutture informatiche** delle Vostre aziende, approntando una serie di servizi a ciò preordinati.

Al termine di ogni attività, la Divisione Cyber Security di INSIDE rilascerà una relazione, all'interno della quale verranno dettagliati tutti gli interventi effettuati e fornite tutte le soluzioni necessarie per la sicurezza totale della Vostra azienda.

Servizi

I servizi offerti dalla Divisione Cyber Security di INSIDE sono preordinati al raggiungimento dei seguenti obiettivi:

VULNERABILITY ASSESSMENT AND MITIGATION
- Valutazione del grado di robustezza del sistema di sicurezza adottato
- Individuazione delle vulnerabilità note
- Adozione di contromisure

PENETRATION TEST
- Valutazione del grado di robustezza del sistema di sicurezza adottato
- Individuazione delle debolezze della piattaforma, mediante la simulazione di un attacco

WEB APPLICATION PENETRATION TESTING
- Individuazione delle vulnerabilità presenti sugli applicativi web
- Risoluzione delle problematiche rilevate

THREAT DETECTION & ANALYSIS
- Individuazione ed analisi di dispositivi hardware o software ostili

ETHICAL HACKING
- Individuazione del rischio di esposizione del sistema informatico rispetto ad eventi ostili di tipo tecnologico e/o umano

CODE REVIEW
- Rilevazione delle vulnerabilità presenti all'interno di un codice sorgente

SECURITY EVALUATION
- Valutazione del grado di sicurezza di applicazioni, processi, piattaforme hardware e software

IT RISK MANAGEMENT
- Individuazione dei rischi da investimenti aziendali in ambito IT
- Definizione delle strategie per governarli

SECURITY AUDIT
- Individuazione precisa delle vulnerabilità presenti nel sistema informatico
- Potenziamento dell'assetto di valutazione dei rischi in esso presenti

HIGH LEVEL SECURITY CONSULTING
- Fornitura di consulenza su tematiche riguardanti la sicurezza informatica

Nel prosieguo della presente documentazione saranno descritte le metodologie utilizzate e le caratteristiche dell'attività espletata, nonché le procedure da seguire nella consegna al Cliente della relazione conclusiva.

1. AMBITO DI APPLICAZIONE

Oggetto dell'intervento richiesto sarà la struttura tecnologica in dotazione del Cliente, ovvero:

- sistema informatico
- infrastruttura interna ed esterna
- rete
- dispositivo hardware/software
- applicazione web in uso al cliente

2. METODOLOGIA

La Divisione Cyber Security di INSIDE dispone di un gruppo di esperti specializzati nel settore, fregiati di un ventaglio di certificazioni accreditate a livello internazionale.

Immagine 1. Principali standard internazionali di riferimento

Nello specifico, svolge la propria attività professionale nel più ossequioso rispetto dei seguenti riferimenti normativi:

- ISO/IEC 19011:2003 – Guidelines for quality and/or environmental management
- ISO/IEC 20000-1:2005 – Service management – Part 1: Specification
- ISO/IEC 27002:2005 – Code of practice for information security management
- ISO/IEC27004:2009 – Information security management – Measurement
- ISO/IEC 27005:2008 – Information security risk management
- BS25999-2:2007 – Business continuity management – Specification
- COBIT v4.1 – Control Objectives for Information and related Technologies
- OSSTMM v3 – Open Source Security Testing Methodology Manual
- OWASP Testing Guide v3 – Open Web application Security Project Testing Guide
- CC v3.1 – Common Criteria
- CEM v3.1 – Common Methodology for Information Technology Security Evaluation
- ITIL v3 – Information Technology Infrastructure Library
- PCI-DSS v2.0 – Payment Card Industry Data Security Standard
- Basilea2 – International Convergence of Capital Measurement and Capital Standards
- SOX of 2002 – Public Company Accounting Reform and Investor Protection Act
- D. Lgs. 231/2001 – Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
- D. Lgs. 196/2003 – Codice in materia di protezione dei dati personali
- D. Lgs. 262/2005 – Tutela del risparmio e disciplina dei mercati finanziari
- D. Lgs. 81/2008 – Tutela della salute e della sicurezza nei luoghi di lavoro

2.1 RIFERIMENTI METODOLOGICI

2.1.1 OSSTMM

L'**OSSTMM** (Open Source Security Testing Methodology Manual) è una certificazione fornita da ISECOM (Institute for Security and Open Methodologies), Comunità internazionale di ricerca e collaborazione sulla Sicurezza, fondata nel Gennaio 2001.

Trattasi di un approccio metodologico di peer-reviewed, utilizzato nell'ambito dei sistemi di sicurezza informatica, che prevede l'esecuzione dei test di sicurezza e di analisi verso infrastrutture ed asset informatici, che si traducono in fatti verificati; questi fatti forniscono informazioni utili che possono migliorare, in termini di misurabilità, la sicurezza operativa.

L'utilizzo dello standard OSSTMM, nel rispetto della normativa prevista in materia, consente di ottenere risultati consistenti e ripetibili, e di capire quali sono le contromisure da adottare, quanto il sistema oggetto di analisi è esposto a possibili aggressioni, e dunque in che modo conseguire il massimo della sicurezza.

2.1.2 OWASP

L'**OWASP Testing Guide** è un framework per il test della sicurezza di applicazioni e infrastrutture di rete, elaborato da OWASP (Open Web Application Security Project), fondazione senza scopo di lucro, che incentra le sue attività sulla produzione di risorse, articoli e materiale relativo a problematiche collegate con la sicurezza informatica.

OWASP ha stilato una classifica delle minacce per la sicurezza ritenute maggiormente critiche:

- SQL Injection
- Broken Authentication and Session Management
- Cross Site Scripting
- Insicure Direct Object Reference
- Security Misconfiguration
- Sensitive Date Exposure
- Missing Function Level access Control
- Cross Site Request Forgery
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

2.2 MODALITÀ DI EROGAZIONE

2.2.1 SERVIZI DI SICUREZZA PROATTIVA

Attraverso i servizi della Divisione Cyber Security di INSIDE, siamo in grado di rilevare il grado di vulnerabilità dei Vostri sistemi e, a seguito di un'attenta analisi diagnostica, individuare gli interventi idonei alla messa in sicurezza della Vostra proprietà informatica.

PENETRATION TEST

Il Penetration Test è un servizio di valutazione della sicurezza di un sistema o di una rete, mediante la simulazione di un attacco da parte di un agente di minaccia esterno o interno. L'obiettivo è quello di evidenziare le debolezze della piattaforma, fornendo il maggior numero di informazioni sulle vulnerabilità tecnologiche che ne hanno permesso l'accesso non autorizzato: si tratta sostanzialmente di mettersi dalla parte dell'hacker, il quale, sfruttando le vulnerabilità rilevate, è in grado di ottenere ogni informazione necessaria per l'accesso all'infrastruttura informatica.

VAM – VULNERABILITY ASSESSMENT AND MITIGATION

Il metodo del Vulnerability Assessment and Mitigation (VAM), adottato dalla Divisione Cyber Security di INSIDE, si compone di una serie di attività non invasive volte a **valutare l'efficacia e il grado di robustezza dei sistemi di sicurezza** adottati dalla Vostra azienda, individuandone le vulnerabilità note in caso di attacco informatico. A queste prime fasi d'intervento segue l'adozione di contromisure finalizzate al miglioramento della sicurezza dei Vostri sistemi.

L'adozione del VAM deve essere organizzata periodicamente durante l'anno, in quanto la tecnologia è in continuo progresso e con essa anche gli strumenti per attaccare un sistema.

La Divisione Cyber Security di INSIDE sviluppa i seguenti livelli di VAM:

- **Data Base**: la nostra analisi si concentra in particolare sui DB maggiormente utilizzati dalle aziende (SQL Server Microsoft, Orcale, SyBase Server, etc..). L'intervento avviene attraverso l'uso di strumenti e software sofisticatissimi, e prevede una scansione automatica di queste banche dati, allo scopo di individuare e analizzare i punti deboli e quindi più facili da attaccare. Ogni azienda "conserva" le informazioni aziendali all'interno di questi DataBase che, essendo costantemente riorganizzati per una loro migliore fruibilità, sono esposti ad attacchi di malintenzionati, quali aziende concorrenti.
- **Rete Telefonica**: l'attacco alla rete telefonica è comunemente chiamato WarDial. Si tratta di un attacco informatico utilizzato frequentemente, poiché la rete telefonica risulta maggiormente vulnerabile per la presenza dei cosiddetti bachi (bug). L'intervento si focalizza sulla scansione di tutta la rete telefonica composta da centralini, modem, apparecchiature telefoniche, etc..

WEB APPLICATION PENETRATION TESTING

Con l'avvento dell'E-Commerce, le aziende sempre più spesso utilizzano il web per promuovere e vendere i propri prodotti e/o servizi. La Divisione Cyber Security di INSIDE svolge quindi attività di **prevenzione e sicurezza su tutti gli applicativi web** di cui le aziende sono munite.

L'intervento prevede una scansione ed un monitoraggio di tutte le sezioni presenti sull'applicativo web, con una particolare attenzione a quelle protette da username e password che, se bucate, permetterebbero l'accesso ai servizi offerti tramite i protocolli HTTP o HTTPS.

L'intervento coinvolge i seguenti campi di sicurezza:

- Scansione dei dati sensibili inviati tramite l'applicativo, esposti al rischio di intercettazione da parte di malintenzionati, tramite l'esame del codice HTML, degli script o di altre informazioni ottenibili da eventuali meccanismi di debugging;
- Approfondita analisi dei campi interattivi tra l'applicazione e l'utente, in modo da individuare eventuali falle create da input (in)volontariamente inseriti;
- Procedure di autenticazione;
- Risoluzione di problematiche relative ad una specifica sessione, come ad esempio timeout, logout, hijacking, login tramite indirizzi non verificati, etc..
- Validazione ed alterabilità dei dati;
- Esecuzione di comandi in zone impreviste dell'applicazione, che ad esempio, tramite specifiche stringhe SQL, possono portare alla diretta manipolazione del DataBase, con possibilità di acquisizione, modifica, cancellazione dei dati presenti;
- Interazioni inappropriate o non corrette con il Sistema Operativo (shell escare).

THREAT DETECTION & ANALYSIS

Con la procedura di Threat Detection & Analysis, la Divisione Cyber Security di INSIDE è in grado di rilevare ed analizzare eventuali dispositivi **hardware o software ostili** (come ad esempio virus), potenzialmente idonei a danneggiare o ad inoltrare verso l'esterno i dati sensibili presenti nei sistemi informatici colpiti da minacce.

ETHICAL HACKING

L'Ethical Hacking è un'attività consistente nella **simulazione di un attacco da parte di un malintenzionato**, esterno o interno, in funzione dell'individuazione del rischio di esposizione del sistema informatico, riguardante non solo l'aspetto tecnologico, ma anche quello umano, attraverso, ad esempio, il metodo del Social Engineering.

Il Social Engineering è un insieme di tecniche psicologiche che il Social Engineer (ingegnere sociale) utilizza allo scopo di indurre, con l'inganno, il destinatario a compiere determinate attività (quali ad esempio il rilascio di codici d'accesso, l'apertura di allegati malevoli o di un sito contenente dialer, etc..). L'attacco prevede una prima fase, detta footprinting, consistente nella raccolta di informazioni sulla vittima (e-mail, recapiti telefonici, etc..) e nella conseguente valutazione di attendibilità delle stesse. Nel momento in cui la vittima sarà caduta nel tranello, spinta dalla fiducia che il Social Engineer avrà nel frattempo generato in lei, il medesimo potrà accedere al sistema informatico e quindi violarlo.

Per svolgere questa attività non occorrono particolari competenze informatiche, essendo sufficiente la conoscenza della psicologia della persona (è peraltro possibile che gli ordinari strumenti di intrusione informatica siano già stati – senza successo – esperiti): il Social Engineer, infatti, fa leva su alcune sensazioni della vittima, quali la colpa, l'ingenuità, o l'ignoranza.

CODE REVIEW

Con il servizio Code Review, la Divisione Cyber Security di INSIDE rileva le **vulnerabilità presenti all'interno di un codice sorgente**, potendo in questo modo limitare i costi derivanti dalla produzione del relativo programma.

L'attività consta di una prima fase di analisi dell'applicazione, attraverso la simulazione, tramite dei tools, dell'esecuzione del codice e quindi di rilevazione delle vulnerabilità presenti. In un secondo stadio, saranno prese in considerazione quelle vulnerabilità che non è stato possibile individuare in prima battuta.

SECURITY EVALUATION

Con il servizio Security Evaluation, la Divisione Cyber Security di INSIDE, avvalendosi di tecnici ampiamente competenti, attesta, in ambiente di laboratorio, **il grado di sicurezza relativo ad applicazioni, processi, piattaforme hardware e software**, attraverso l'individuazione delle vulnerabilità presenti, e l'adempimento delle procedure di messa in sicurezza già esistenti da parte del personale.

IT RISK MANAGEMENT

Attraverso il processo IT Risk Management, la Divisione Cyber Security di INSIDE **individua i rischi** (vulnerabilità, minacce, etc..) derivanti dagli investimenti aziendali in ambito IT (cd. Risk Assessment) e definisce le strategie migliori per governarli (cd. Risk Treatment), amplificando in tal modo il livello di sicurezza che un'infrastruttura informatica richiede.

SECURITY AUDIT

Il servizio di Security Audit è un assessment tecnico della politica di sicurezza di un'organizzazione, che prevede la combinazione delle attività di Penetration Test e Risk Assessment: si tratta sostanzialmente di **individuare con precisione le vulnerabilità presenti nel sistema informatico**, mediante una puntuale ottimizzazione dell'esecuzione delle verifiche tecnologiche, e di potenziare così l'assetto di valutazione dei rischi in esso presenti.

HIGH LEVEL SECURITY CONSULTING

Il personale specializzato della Divisione Cyber Security di INSIDE offre **servizi di consulenza avente** ad oggetto qualsiasi tematica riguardante la sicurezza informatica, non altrimenti inquadrabile nell'ambito dei servizi descritti.

2.2.2 VETTORI DI ATTACCO - per i servizi di Penetration test e Web Application Penetration Test

Attraverso la tecnica dei vettori di attacco – che sono molteplici, a seconda del dispositivo sul quale è previsto l'intervento – la Divisione Cyber Security simula l'attività posta in essere da un agente di minaccia, che accede in maniera non autorizzata ad un sistema informatico.

Di seguito indichiamo alcuni dei vettori di attacco utilizzati:

- **Infrastruttura**: IP, VPN, Wi-Fi, SCADA, etc.
- **Applicazioni**: Web, Database, Client-Server, etc.
- **Telefonia**: PBX, RAS, APN, BlackBerry, VoIP, etc.
- **Altri**: Human, Physical, Videosorveglianza, Biometria, etc.

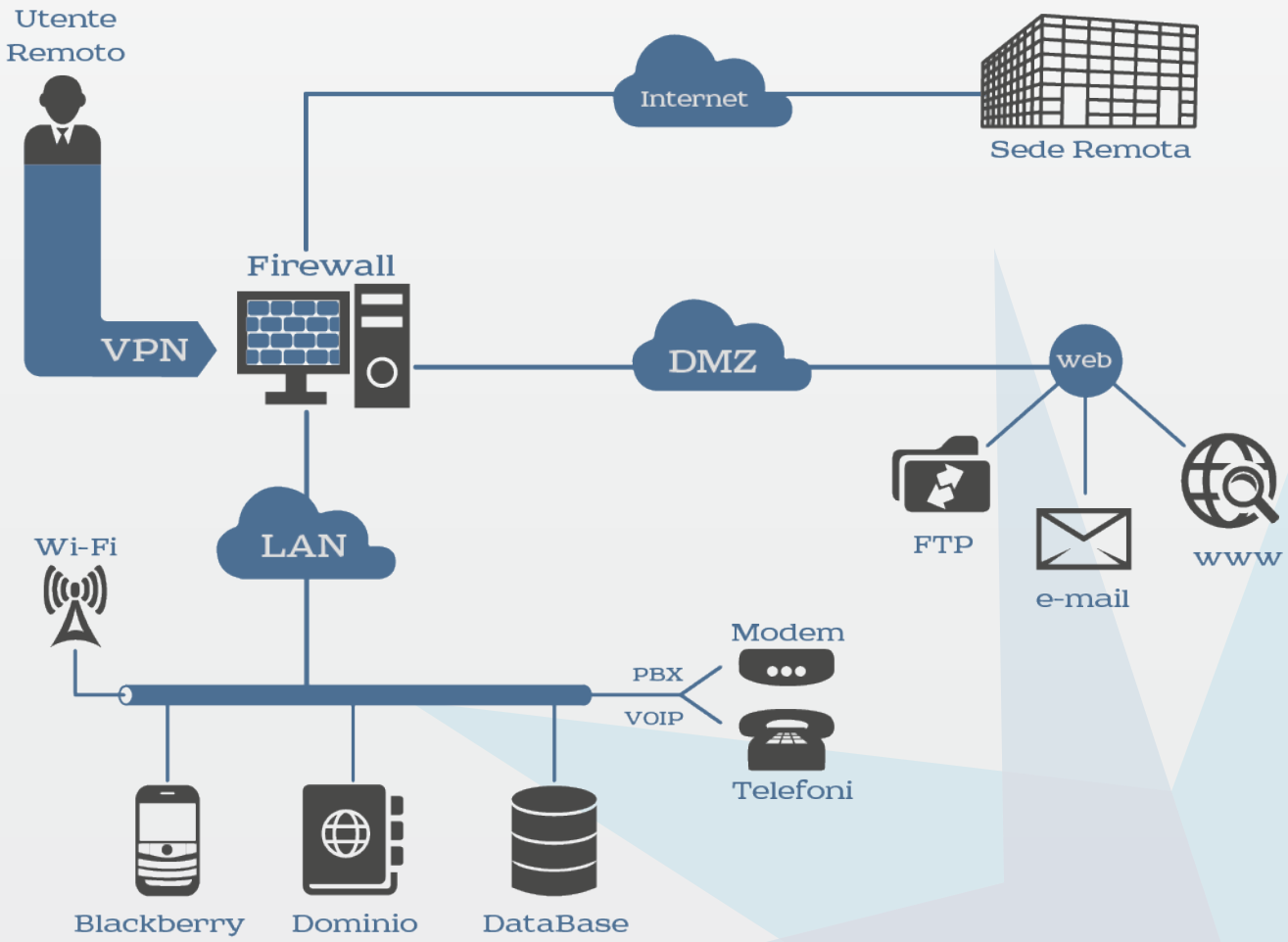

Immagine 3. Principali vettori di attacco

In alcuni casi preferiamo eseguire dei test da posizione privilegiata, ricorrendo a credenziali standard di accesso, per valutare l'eventualità di eludere i meccanismi di autenticazione ed autorizzazione realizzati.

2.2.3 APPROCCIO

L'approccio messo a punto dalla Divisione Cyber Security di INSIDE, sempre preordinato alla valutazione in merito al grado di sicurezza dell'infrastruttura informatica oggetto di analisi, avviene attraverso la modalità Blind, che prevede **la simulazione di un attacco "alla cieca"**, cioè senza conoscere i dettagli implementativi della infrastruttura medesima.

2.2.4 STRUMENTI

La Divisione Cyber Security di INSIDE si avvale degli strumenti di attacco maggiormente in uso sul mercato ovvero quelli elaborati dal Security Advisory Team, rientranti nelle categorie di seguito indicate:

- **Vulnerability Scanning** (nessus, nexpose, openvas, etc.)
- **Network Scanning** (nmap, unicornscan, singsing, arp-scan, ike-scan, p0f, etc.)
- **Web Testing** (burp suite, zed attack proxy, w3af, skipfish, nikto, etc.)
- **Wireless Testing** (aircrack-ng, kismet, karmetasploit, etc.)
- **Phone Testing** (minicom, warvox, ward, thc-scan, etc.)
- **Packet Forging** (hping, scapy, voiphopper, yersinia, isic, netcat, etc.)
- **Network Sniffing** (wireshark, cain & abel, ettercap, etc.)
- **Password Cracking** (john, rcrack, fgdump, thc-hydra, medusa, etc.)
- **Exploitation** (metasploit framework, exploit-db, private exploits, etc.)

È inoltre ammesso l'impiego di **exploit 0day**, attacco informatico particolarmente offensivo per l'integrità di un sito web o per il corretto funzionamento di un nodo di internet, previsto esclusivamente dietro espressa domanda del Cliente.

Saranno adoperati solo hardware e software di proprietà e, a conclusione di ogni progetto, verrà posta in essere una **procedura di sanitizzazione**, per la eliminazione di qualsiasi dato escusso nell'espletamento dell'incarico in oggetto.

2.2.5 DENIAL OF SERVICE

Si esclude dal presente progetto, salvo domanda del Cliente in tal senso, la verifica degli attacchi di tipo D**oS - Denial of Service** (letteralmente "negazione del servizio") che, come è noto, consiste in un malfunzionamento dovuto ad un attacco informatico, in cui deliberatamente **si esauriscono le risorse di un sistema informatico** che fornisce un servizio, fino a renderlo non più in grado di erogare il servizio medesimo.

3. PIANO DELLE ATTIVITÀ

3.1 Impostazione delle attività

Nella fase iniziale del progetto, è doveroso per il Security Advisory Team, attraverso l'interfaccia con il Cliente, la raccolta di ogni informazione indispensabile all'esecuzione dell'incarico, convenendo inoltre con il medesimo circa il programma e le modalità di intervento di ogni singola operazione di sicurezza.

3.2 VERIFICHE WEB ESTERNE - per web application penetration testing

La finalità dell'intervento è **l'analisi delle applicazioni web**, basate su tecnologie eterogenee (ASP.NET, PHP, JSP, etc.), per attestare il grado di robustezza delle componenti applicative, ed evitare ad eventuali agenti di minaccia provenienti dalla rete pubblica internet di accedere ai dati sensibili di cui il Cliente è in possesso.

3.3 VERIFICHE ESTERNE SU IP - per Penetration Test

La finalità dell'intervento è l'analisi dei sistemi esposti ad agenti di minaccia provenienti dalla rete pubblica internet, per attestare **il grado di robustezza dell'infrastruttura di rete** nel complesso, ed evitare accessi non autorizzati o sottrazione di informazioni riservate.

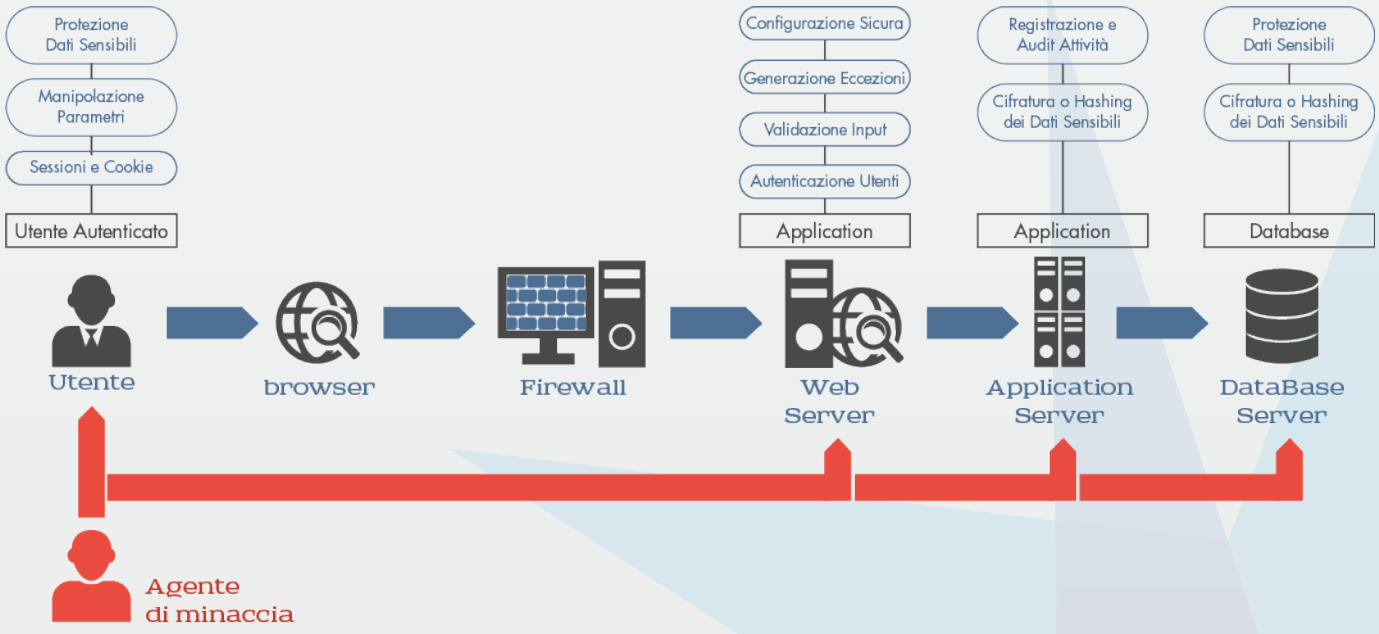

Immagine 4. Architettura di un'applicazione web e relative contromisure di sicurezza

3.4 VERIFICHE INTERNE SU IP - per Penetration Test

La finalità dell'intervento è l'analisi dei sistemi della rete privata del Cliente, per attestare il grado di robustezza dell'infrastruttura di rete nel complesso, ed **evitare accessi non autorizzati** o sottrazione di informazioni riservate.

4. DELIVERABLE

Nel prosieguo una serie di informazioni relative alle caratteristiche del documento finale rilasciato al Cliente, a conclusione della realizzazione del progetto.

4.1 RAPPORTO DI VERIFICA

Al termine di ogni attività, la Divisione Cyber Security di INSIDE rilascerà una relazione, dal contenuto strettamente confidenziale, all'interno della quale **verranno dettagliati tutti gli interventi effettuati** e fornite tutte le soluzioni necessarie per la sicurezza totale della Vostra azienda.

Il documento consta di due livelli di approfondimento:

- **Executive Summary**: è una sezione introduttiva che consente al Cliente di ottenere delle prime informazioni in grandi linee sul grado di sicurezza della struttura oggetto di verifica, corredata dall'indicazione dei rischi rilevati, dei danni prevedibili e delle contromisure da applicare per la risoluzione delle problematiche;
- **Relazione Tecnica**: è il documento finale vero e proprio, recante la descrizione tecnica delle operazioni compiute, le criticità evidenziate e il dettaglio delle contromisure da adottare.

5. TEMPI DI EROGAZIONE

Il grafico mette in evidenza i tempi di erogazione dei servizi richiesti.

Le attività oggetto della presente offerta saranno svolte presso la sede di INSIDE, ovvero, in caso di patto tra le contraenti in tal senso, presso la sede del Cliente.

Attività	Settimana 1	Settimana 2	Settimana 3	Settimana 4
Impostazione delle attività e Project Management				
Verifiche web esterne				
Verifica di follow/up				
Presentazione dei risultati				

6. FIGURE PROFESSIONALI

La Divisione Cyber Security di INSIDE dispone di **esperti considerevolmente specializzati**, in possesso di una serie di riconoscimenti e certificazioni in materia di verifica della sicurezza, attestanti requisiti di professionalità tecnica nonché il valore etico degli stessi:

- CISSP (Certified Information System Security Professional)
- CISA (Certified Information Security Auditor)
- CISM (Certified Information Security Manager)
- OPSA (OSSTMM Professional Security Analyst)
- OPST (OSSTMM Professional Security Tester)
- OWSE (OSSTMM Wireless Security Expert)
- GCFA (GIAC Certified Forensics Analyst)
- ITV3F (ITIL Foundation v3)
- ISFS (Information Security based on ISO/IEC 27002)
- ISO/IEC 27001:2005 Lead Auditor (diversi schemi)
- PCI-QSA (Payment Card Industry Qualified Security Assessor)
- PCI-ASV (Payment Card Industry approved Scanning Vendor)

6.1 SENIOR SECURITY ADVISOR

Questa figura vanta un'esperienza tecnico-organizzativa, nel settore della sicurezza, di 5 anni e pertanto dispone dei requisiti necessari per individuare l'attività di lavoro e pianificare le strategie di cui il Cliente necessita.

Conosce meticolosamente i servizi di sicurezza e le procedure da adottare per la risoluzione di ogni singolo problema in materia di sicurezza; in virtù di tali competenze e in forza del costante aggiornamento cui si sottopone, è in grado, quindi, di **intervenire in maniera dinamica in attività formative e di ricerca**.

6.2 SECURITY ADVISOR

La suddetta figura ha un'esperienza tecnico-organizzativa di 3 anni nel campo della sicurezza. È in grado di affiancare il Cliente nella scelta dei servizi da svolgere per la **messa in sicurezza dell'azienda**; dirige le attività dei Security Expert; partecipa attivamente a progetti formativi e di ricerca.

6.3 SECURITY EXPERT

Il Security Expert, grazie al biennio di esperienza tecnico-organizzativa maturata nell'ambito della sicurezza, ha sviluppato la capacità di **offrire consulenza e assistenza in materia**, a sostegno del lavoro del Security Advisor. È regolarmente coinvolto in attività di aggiornamento e di ricerca.

Inside
INTELLIGENCE & SECURITY INVESTIGATIONS

www.inside.agency • info@inside.agency •

SEDE CENTRALE

SVIZZERA
Via Maggio, 1/C
6900 Lugano
T +41 (0)91 260 16 42
F +41 (0)91 228 03 95

UFFICI NEL MONDO

REGNO UNITO
Crown House, 72 Hammersmith Rd
Hammersmith, London, W14 8TH
T +44 (0)20 75 59 13 11
F +44 (0)20 35 14 68 50

USA
6800 Jericho Turnpike, Suite 120W
Syosset, New York, 11791
T +1 (0)516 393 58 52
F +1 (0)516 393 58 19

RUSSIA
31st floor, stroenie 1, bld. 3,
Begovaya str, Moscow, 125284
T +7 (0)499 277 13 03
F +7 (0)499 287 66 00

ITALIA
Via Monte di Pietà, 21
20121 Milano
T +39 (0)2 86 33 73 42
F +39 (0)2 94 75 26 15

ITALIA
Via Ludovisi, 35
00187 Roma
T +39 (0)6 42 03 73 97
F +39 (0)6 94 80 17 11

EMIRATI ARABI UNITI
Building 3, Plot 598-676, Dubai Investment
Park, Green Community, DUBAI, 212880, EAU
T +971 (0)4 80 19 276
F +971 (0)4 80 19 101

HONG KONG
25 Westlands Road, Quarry Bay Berkshire
House, Unit 2402-07, 24th HONG KONG
T +852 (0)28 24 85 28
F +852 (0)37 19 81 11

SUD AFRICA
First Floor, Willowbridge Centre, 39
Carl Cronje Dr, Cape Town, 7530
T +27 (0)21 974 6276
F +27 (0)21 974 6101

BRASILE
Top Center Paulista, Paulista Avenue, 854
Bela Vista – 10° floor, São Paulo, 01310-913, Brasile
T +55 (0)11 21 86 04 42
F +55 (0)11 21 86 02 99