studio consi
sicurezza digitale

Sicuri di essere sicuri?

Indice

Il nostro studio

Red team
Offensive Cyber Security

Servizi di qualità certificati.
Solo consulenze di professionisti.
Pensare, agire come un Hacker ed operare in modo etico.

Il nostro team, nato quale aggregazione di professionisti quali **Lead Auditor**, **consulenti Aziendali**, **informatici**, **Privacy Officer**, **legali**, e **DPO**, offre una varietà di servizi di alto livello, con particolare attenzione agli specifici fabbisogni integrando soluzioni altamente specializzate per consulenze informatiche, organizzazione aziendale e sistemi di gestione della qualità. Questo è svolto cercando di rispettare le singole competenze che contraddistinguono ogni professionista, rispettando il codice etico-morale di ciascuno e creando dunque un clima sereno e proficuo atto ad un lavoro più piacevole e più proficuo. Ognuno di noi, coinvolto in questo progetto porta il massimo della propria professionalità e passione.

Una peculiarità del nostro gruppo in tutti i servizi offerti è per prima cosa l'**indipendenza** perché non abbiamo fornitori di soluzioni. Noi vendiamo solo servizi di consulenza, non commercializziamo hardware o software di nessun genere.

I nostri servizi

Seguendo la naturale evoluzione sociale, produttiva e non ultima quella tecnologica abbiamo scelto la ricerca della qualità in tutti i nostri servizi mettendoci professionalità certificata, passione e correttezza.
I nostri ambiti d'azione rispecchiano le **necessità** del mercato e i relativi **trend**.

CYBERSECURITY

I Sistemi Informativi rappresentano, in tutte le loro componenti, punti nevralgici e vincolanti del progetto Aziendale. Proprio questa loro necessità aumenta la loro **sensibilità** a possibili compromissioni: una **verifica proattiva** non mediata da interessi personali non è un costo ma un **investimento** sulla resilienza del cuore pulsante dell'organizzazione stessa. La verifica della sicurezza non può essere fatta da chi fa la sicurezza stessa.

PRIVACY

La riservatezza dei dati rappresenta un tema complicato e nevralgico dell'intera organizzazione societaria di cui è facile perdere il controllo. Dove sono le Nostre informazioni personali, come sono custodite e chi vi può accedere? Queste sono le domande fondamentali. Essere **compliant** alle norme vigenti non è tanto una sfida di facile risoluzione quanto un **processo** sempre in **fieri**.

CONSULENZA FUNZIONALE

I processi aziendali possono essere di tipologie diverse ma rappresentano il know-how, il **core business** dell'intera struttura. Tuttavia, in un mondo globalizzato in costante evoluzione rimanere sempre fedeli ad un'unica metodologia può essere talvolta limitante. Quali metodi, quali visioni potrebbero aiutare la tua azienda a crescere?

Cybersecurity

SERVIZI DI CYBERSECURITY

Vulnerability Assessment

Cos’è un Vulnerability Assessment?

Cosa si intende per **vulnerabilità**? Il macrocosmo informatico è composto da molteplici ambiti: evoluzioni tecnologiche, risorse, budget d’investimento, sistemi di comunicazione avanzati e molto altro. In questo panorama complesso ed articolato si annidano delle possibili fonti di rischio: le vulnerabilità.
Che si tratti di questioni **pubblicamente note** o di **misconfigurazioni** operative, nel panorama moderno queste devono essere conosciute e mitigate.
Un Vulnerability Assessment è dunque la ricerca, eseguita non solo con tool informatici ma, e forse soprattutto, anche con l’ausilio della **competenza professionale**.
La definizione che più s’avvicina all’idea del Vulnerability Assessment è quella di un **check-up completo** sulle possibili problematiche che potrebbero compromettere il processo produttivo.

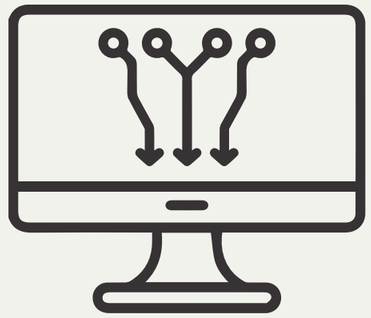
Soluzioni offerte

Il Vulnerability Assessment si può dipanare sia sul perimetro esterno che su quello interno.

Dall’esterno vi sono le principali minacce, per questo motivo è **utile** e, sul lungo periodo, **imprescindibile** effettuare analisi di sicurezza su tutta la presenza online di una società: dall’analisi dei domini e dei sottodomini, server privati ospitanti e-commerce e CRM alla Supply Chain e web app di varia natura. Questi sono solo alcuni esempi di ciò che può essere considerato a rischio.

Tuttavia, spesso si sminuisce l’importanza della sicurezza interna ad una struttura. Il perimetro interno rappresenta un punto particolarmente delicato in cui, dietro alla corretta operatività, potrebbero annidarsi problematiche di **business continuity**: dall’adozione di Sistemi Operativi non aggiornati e, magari, non aggiornabili, a software outdated, passando per protocolli e politiche deboli di sicurezza.

Un Vulnerability Assessment verifica tutto questo e si conclude con un report composto di **due sezioni**: una sezione Directional e una Executive.
La prima espone chiaramente e discorsivamente l’esito della valutazione ed è finalizzata a rendere chiaro lo status quo anche alla Direzione, la seconda espone i dettagli tecnici e le relative risoluzioni necessarie.
Da qui, l’azienda potrà porre rimedio a tutte le eventuali vulnerabilità rilevate in totale **autonomia**.



Penetration Testing

Cos’è un Penetration Test?

Quali potrebbero essere le conseguenze del verificarsi di un rischio informatico e quali potrebbero essere i percorsi che lo consentirebbero? Queste sono le domande fondamentali a cui una simulazione **etica** d’attacco deve rispondere.

Un Penetration Test deve utilizzare, per essere effettivamente veritiero, la **metodologia** e la **tecnologia** che potrebbe essere usata a fini distruttivi.
In questo contesto, dunque, si verificano tutte le principali tipologie di vulnerabilità: Cross Site Scripting (CSS), SQL Injection (SQLi), XXE, RCE, etc.

Tali verifiche si distinguono in tre livelli a seconda del grado di conoscenza pregressa data all’attaccante e cioè, in via progressivamente crescente: BlackBox, GreyBox e WhiteBox.

La differenza **fondamentale** tra un Vulnerability Assessment e un Penetration Test è che la prima si ferma alla rilevazione di possibili vulnerabilità, il secondo verifica tecnicamente che queste siano effettivamente **utilizzabili** e praticamente fattibili.

Soluzioni offerte

Il test di penetrazione è un test **oggettivo** finalizzato effettivamente alla verifica delle potenziali vulnerabilità.

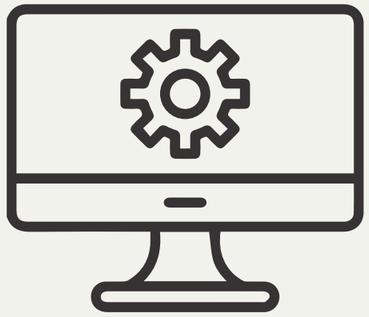
La soluzione di Studio Consi si rivolge ovviamente sia alla struttura esterna che a quella interna, così come per quanto concernente i Vulnerability Assessment.

I nostri test simulano **attacchi reali** per cui ciò di cui abbiamo bisogno è esattamente ciò di cui avrebbe bisogno un Hacker.

Per la soluzione esterna, tutto ciò di cui abbiamo bisogno sono i domini coinvolti e/o gli indirizzi IP o, se s’intende verificare possibili problematiche relative alla segregazione dei profili utente, di relativi account di test.

Per la soluzione interna, invece, ci basta un accesso cablato o wireless e una presa elettrica. Di default andiamo a verificare anche parziali potenziali compromissioni di dati pregresse ed informazioni pubbliche che potrebbero consentire la realizzazione di attacchi in modalità facilitata mediante quella che viene chiamata analisi **OSINT**.

SERVIZI DI CYBERSECURITY



Sistemi SCADA / ICS

Cos’è un’analisi di sicurezza SCADA?

I sistemi SCADA (Supervisory Control And Data Acquisition) sono sistemi informatici, in genere un’architettura distribuita con gestione più o meno centralizzata, incaricati di monitorare elettronicamente sistemi industriali e/o logistici.

L’analisi SCADA sostanzialmente è tesa a verificare la presenza di possibili vulnerabilità all’interno di questa segmentazione del più vasto perimetro interno societario al fine di verificare la possibilità di compromissioni e/o paralisi da personale non autorizzato.

Soluzioni offerte

Sia che la rete sia costituita mediante PRP (Parallel Redundancy Protocol) sia tramite HSR (High-availability Seamless Redundancy), l’analisi di sicurezza offerta si costituisce in un Vulnerability Assessment mirato esplicitamente alla rilevazione di condizioni logiche deboli e alla presenza di possibili compromissioni dell’infrastruttura che potrebbero comportare, tra le altre, furto di know-how aziendale, disservizi (DoS) o, addirittura, paralisi dell’intera infrastruttura, sia internamente alla rete SCADA sia per mezzo dei punti di contatto destinati alla gestione in tempo diretto della stessa.

Awareness of digital security

Il punto più importante di un’azienda sono le sue **risorse societarie**: lo sappiamo bene.
Tuttavia, proprio queste devono conoscere i rischi a cui sono esposte mediante l’uso dei server e-mail e di navigazione web. Sono loro le prime misure di sicurezza e come tali dovrebbero essere trattate. Soluzioni software di sicurezza, infatti, possono fare ben poco quando le prime linee non possono contrastare anche le più semplici forme di attacchi.
Molti asset si possono comprare ma la **knowledge** necessaria non può essere di pochi.

Training timing

Dunque, perché non formare correttamente le risorse societarie? Studio Consi non offre solo la classica formazione in aula ma, soprattutto, **formazione pratica** focalizzata al riconoscimento della gravità di una minaccia.
Per far ciò si può ricorrere a test di phishing via via più complessi ed articolati finalizzati a far prendere confidenza con la **mentalità TNO** (Trust No One).
La nostra proposta è quella di effettuare i test di **phishing** via via più complessi per comprendere, hands on, il livello delle risorse da formare.
Dall’analisi aggregata dei risultati, dunque, si potrà effettuare una **formazione mirata** alla risoluzione delle carenze specifiche del personale.

Argomenti

- Vulnerabilità informatiche e tecniche d’attacco;
- Hacker e mentalità criminale;
- Il valore della nostra infrastruttura e del nostro patrimonio;
- Come riconoscere le principali minacce e come evitarle.

SCHEDA TECNICA

Timing di progetto

PERIMETRO ESTERNO

- Verifica della configurazione DNS e test di trasferimento
- Enumerazione ed identificazione dei servizi esposti
- Verifica misconfigurazioni delle directories;
- Identificazione di eventuali CVE e verifica della relative applicabilità;
- Analisi OSINT;
- Test di bypass delle attuali politiche in essere e verifica di eventuali vulnerabilità custom;
- Realizzazione del report:
  Sezione **“Direction”**:
  - Dati preliminari e di contatto;
  - Esito dei test eseguiti.
  Sezione **“Executive”**:
  - Metodologia e step per la riproduzione;
  - Analisi dettagliata e relative mitigazioni.

PERIMETRO INTERNO

- Scansione atta all’identificazione dei servizi esposti e al fingerprinting dei device connessi;
- Verifica della configurazione (dall’esterno) dei singoli servizi e protocolli;
- Identificazione di eventuali CVE e verifica della relative applicabilità;
- Verifica diffusa della politica delle credenziali;
- Analisi pratica della possibilità di movimento laterale;
- Test di privilege escalation e di bypass delle attuali politiche in essere;
- Realizzazione del report:
  Sezione **“Direction”**:
  - Dati preliminari e di contatto;
  - Esito dei test eseguiti.
  Sezione **“Executive”**:
  - Metodologia e step per la riproduzione;
  - Analisi dettagliata e relative mitigazioni.

Sistemi SCADA / ICS

- Studio della toponomia della rete;
- Analisi dei protocolli e delle condizioni logiche sottese al corretto funzionamento della rete stessa;
- Verifica dell’esistenza di vulnerabilità in SCADA nativi e programmi PLC custom quali, ad esempio:
- - Bypass dell’autenticazione,
- - Abusi dei privilegi assegnati, etc.;
- Realizzazione del report:
  Sezione **“Direction”**:
  - Dati preliminari e di contatto;
  - Esito dei test eseguiti.
  Sezione **“Executive”**:
  - Metodologia e step per la riproduzione;
  - Analisi dettagliata e relative mitigazioni.

SCHEDA TECNICA

Estratto del Portfolio software utilizzabili

Le attività previste possono essere eseguite con una serie di tools che a contesto ed esigenza sono specifici allo scopo.

Routersploit	Software per la verifica della presenza di vulnerabilità nel firmware di router e videocamere (test anche del riutilizzo di credenziali standard/default)
Hydra	Software per attacco dictionary brute force
Metasploit	Software per l'exploit (attacco attivo)
Msfvenom	Software per la scrittura di payloads (standard e custom)
Burp Suite	Software per l'analisi di web applications
Nessus	Software per l'analisi di vulnerabilità interne ad una WLAN/ LAN ed installazione di patch
Nikto	Software per l'analisi di vulnerabilità web application
Golismero	Software per l'analisi di vulnerabilità web application
Netdiscover	Software per l'analisi di vulnerabilità WLAN/LAN

John	Software per realizzazione attacchi dictionary bruteforce e/o bruteforce
Nmap	Software per la mappatura della rete ed analisi vulnerabilità (anche exploit)
Powershell Empire	Software per la realizzazione e criptazione payload specifico per Windows
Saint	Software per analisi vulnerabilità ed exploit in WLAN/LAN
Maltego	Software per analisi OSINT
Theharvester	Software analisi OSINT
Dmitry	Software analisi OSINT DNS
Unix Privesc Check	Software analisi file per sistemi UNIX
Sqlmap	Software per attacchi SQLi
ZAP	Software analisi vulnerabilità Web application
Aircrack Suite	Software analisi vulnerabilità ed exploit reti WLAN
Wireshark	Software (sniffer) analisi vulnerabilità reti WLAN/LAN
Kismet	Software (sniffer) analisi vulnerabilità reti WLAN
Netsniff Ng	Software (sniffer) analisi vulnerabilità reti WLAN
Powerspolit	Software per la realizzazione di exploit custom per Windows
Analisi Exifs	Utilizzati vari programmi finalizzati all'analisi dei metadati della documentazione pubblicata e/o rinvenuta online

Privacy

SERVIZI DI PRIVACY

Adeguamento privacy

In cosa consiste un adeguamento privacy?

La riservatezza dei dati rappresenta un tema complicato e nevralgico dell'intera organizzazione societaria di cui è facile perdere il controllo.
Dove sono le Nostre informazioni personali, come sono custodite e chi vi può accedere? Queste sono le domande fondamentali.
Essere **compliant** alle norme vigenti non è tanto una sfida di facile risoluzione quanto un **processo** sempre **in fieri**: migrazioni tra soluzioni, acquisizioni di personale, strutturazione di nuovi servizi e/o ammodernamenti, anche parziali, rendono la riservatezza un **processo societario** trasversale che, se mal configurato, può rendere l'operatività farraginosa.

Soluzioni offerte

Le soluzioni di Studio Consi vanno dalle **verifiche** dell'affidabilità e della robustezza del Sistema di Gestione Privacy svolte in simulazione d'ispezione degli organi verificatori alla realizzazione dei sistemi dinamici d'adeguamento.
I nostri Esperti vi possono aiutare in questo percorso di **ri-definizione** dell'asset societario dal punto di vista legale, operativo e di mantenimento del livello di **compliance**.
Ciò può arrivare anche alla gestione dell'incarico di Responsabile della Protezione dei Dati (DPO) sia per le società obbligate alla nomina che per quelle che, per motu proprio, decidono d'avvalersene.

SCHEDA TECNICA

Timing di progetto

PROGETTAZIONE ATTIVITÀ
- Studio dei processi Aziendali e definizione dei relativi strumenti idonei
- Definizione della metodologia al fine della formazione specifica;
- Timing di progetto con Gantt

AUDIT DI PRIMA PARTE
- Locations e sicurezza fisica
- Informatizzazione e relativa sicurezza dei dati
- Presenza online della società
- Tipologia di dati raccolti e trattati
- Metodologia dei trattamenti

REDAZIONE DELLA DOCUMENTAZIONE
- Modulistica (informative, atti di nomina ad autorizzati e responsabili dei trattamenti);
- Registri delle attività di trattamento ex art. 30, par. 1 e par. 2, GDPR;
- Procedure organizzative;
- Documentazione del livello di compliance:
  DPRA - Valutazione dei rischi
  DPIA - Valutazioni d'impatto

FORMAZIONE
Formazione continua

SERVIZI DI CONSULENZA FUNZIONALE

Consulenza funzionale

In cosa consiste una consulenza funzionale?

I software gestionali potremmo rappresentali come centri nevralgici che controllano e gestiscono la nostra idea di Azienda. Quest'ultimi ci informano degli eventi preventivati o in corso e, forse, di quelli futuri.

Per avere queste caratteristiche ci devono prima di tutto conoscere, capire, ed essere adatti a Noi. Altrimenti sono essenzialmente gangli che ci imbrigliano, che ci richiedono risorse, risorse senza restituirci che dati magari anche difficilmente interpretabili.

Soluzioni offerte

Dalla conoscenza degli ambiti Aziendali, delle soluzioni del mercato e delle problematiche insite in questo microcosmo nasce la suite di servizi che la nostra realtà mette a disposizione dei propri Clienti.

I processi aziendali possono essere di tipologie diverse ma rappresentano il know-how, il **core business** dell'intera struttura. Tuttavia, in un mondo **globalizzato** in costante evoluzione rimanere sempre fedeli ad un'unica metodologia può essere talvolta limitante.
Quali metodi, quali **visioni** potrebbero aiutare la tua azienda a crescere?

Oltre a ciò, tuttavia, a volte possono sorgere delle **controversie** con vari fornitori come, ad esempio, fornitori di software CRM o gestionali HR, etc. La presenza di un terzo indipendente può dirimere la questione e risolvere l'**impasse**.

Domande frequenti

1- Siamo una piccola azienda, cosa potrebbero volere da me?

Ad un criminale **non interessa** quale sia il target che sta colpendo, importa solo l'obiettivo finale. All'Hacker non necessariamente interessa conoscere le proprie potenziali vittime. Forse le nostre informazioni, disegni industriali, lista Clienti non avranno una rilevanza internazionale però possono essere **vendute**, come le password rubate, e -magari- a qualcuno potrebbero interessare. L'esempio più eclatante è un attacco phishing. Viene "buttata" la rete e chi risponde in qualche modo diventa un potenziale "pagatore", statisticamente il **2%**. Lo stereotipo dell'hacker con felpa e cappuccio non corrisponde alla verità: il vero problema sono le **organizzazioni criminali** composte di veri e propri professionisti del crimine informatico che, sistemicamente, lanciano attacchi massivi.

2- Il nostro fornitore si occupa di tutto

Chi fa sicurezza non può fare la verifica, sarebbe come chiedere ad uno studente di **auto-esaminarsi**, si porrebbe domande solo domande su quello che ha studiato.

3- Siamo sicuri che fatto questo sia tutto a posto?

No, queste attività servono a verificare se vi sono, al momento attuale, delle vulnerabilità. Ma la sicurezza informatica è un'attività continua, non un'attività a spot. Questo è il primo passo, non l'ultimo.

4- Noi lavoriamo in cloud per cui i rischi sono minori

Il Cloud rappresenta una comodità per tutti noi: potersi connettere e lavorare ovunque si sia è stata davvero una gran rivoluzione. Tuttavia, se possiamo farlo noi, può farlo chiunque. È necessario verificare che questo non possa accedere alle informazioni contenute nei server esposti.

5- Abbiamo una polizza assicurativa

La necessità d'effettuare un ripristino dei dati non è l'unico danno che si subisce a seguito di un attacco: fermi produttivi, danni d'immagine e così via non sono fattori da dimenticare e non v'è assicurazione che tenga alla perdita di fiducia dei clienti.

6- Cosa centra la privacy con gli attacchi hacker?

Un data breach può comportare l'esposizione e il furto di dati personali. In questi casi è legalmente obbligatorio notificare al Garante l'avvenuto incidente, con tutte le conseguenze del caso.

7- Abbiamo appena installato un nuovo antivirus

I software antivirus non sono una panacea a tutti i mali. Esistono tecniche di bypass – ad esempio mediante l'offuscamento pesante del codice sorgente – che vengono regolarmente utilizzate dai virus più avanzati per evitare che vengano riconosciuti dalle più comuni misure di sicurezza, appunto come gli antivirus.

8- I dipendenti sono responsabili e lo sanno

Non si può delegare l'intera sicurezza di un'azienda alle risorse societarie e ai soli software di protezione, come gli antivirus. I primi responsabili sono sempre gli Amministratori della società: CED, Amministratori Delegati, Amministratori di Sistema, etc.

9- Ci sono programmi automatizzati che simulano attacchi

I programmi automatizzati fanno esattamente quello che gli si dice: non potranno dedurre o intuire altro che quello che gli viene chiesto. Serve un professionista che abbia senso critico e l'intuizione di leggere i dati e, molte volte, oltre i dati stessi.

"Una singola vulnerabilità è tutto ciò di cui un hacker ha bisogno"

Window Snyder

10- Vulnerabilità su sistemi SCADA notoriamente più isolati?

I sistemi SCADA necessariamente collegati ad altre reti Aziendali, hanno introdotto vulnerabilità legate principalmente all'utilizzo di standard aperti per i protocolli di comunicazione interna.

11- Quali ambiti di vulnerabilità su SCADA?

Le tipologie si possono riepilogare in -hardware, software, nodi, autorizzazioni, elettronica bordo macchina.

12- Quali ambiti sono a rischio?

I primi ambiti oggetto di attacchi inizialmente erano soprattutto quelli energetici, successivamente qualsiasi sistema industriale con apparecchiature collegate a reti, non ultimo l'ambito logistico distributivo sia interno che esterno.

Contatti

Studio Consi S.a.s.
di Dal Broi Antonio & C.

Sede legale: 31011 Asolo (TV) Via G. Verdi, 15
Sede operativa: 31033 Castelfranco Veneto
(TV) P.zza Serenissima 40/101

0423 1990486
0423 1886218

info@studioconsi.com
privacy@studioconsi.com
amministrazione@studioconsi.com

studioconsi.com

Sponsor

FEDERPRIVACY

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica