studio consi

sicurezza digitale

Sicuri di essere sicuri?

Indice

Il nostro studio

Red Team
Studio Indipendente

Offensive Mode Cyber Security. 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 le peculiarità che li contraddistinguono. Particolare attenzione va ai 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 atto ad un lavoro più piacevole e più proficuo. Questo stesso spirito anima i nostri rapporti con i clienti. Lavorare in un clima armonico favorisce la cooperazione e la collaborazione tra le parti e consente un lavoro più preciso e puntuale, anche nel rispetto degli obiettivi fissati in sede di accordo. 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 consolidati, continuativi e fidelizzati. Rispettiamo il principio della **Segregation of Duties** e dunque vendiamo solo servizi di consulenza specifica, **non commercializziamo hardware o software di nessun genere**. La nostra convinzione è che **chi fa sicurezza non dovrebbe "controllare se stesso".**

Siamo un **Red Team**: i nostri tecnici hanno certificazioni internazionali specifiche rilasciate da enti preposti alla formazione in ambito offensive mode cyber security.

È meglio che le vulnerabilità vengano scoperte durante un penetration test che durante un vero attacco criminale.

I nostri servizi

Dato che ogni Società ha un proprio DNA, i propri assets e i propri know-how, è imprescindibile effettuare ogni attività con parsimonia e attenzione inserendo tutte le informazioni nella loro contestualizzazione aziendale: ogni nodo o endpoint viene analizzato inserendolo nel più grande panorama aziendale dai nostri professionisti. Ciò consente di avere un'**analisi strutturata e non appiattita** su informazioni tecniche che rischiano altrimenti di risultare obsolete in pochi mesi.

Offriamo un set di servizi completi ma caratterizzati da una metodologia altamente sartoriale: la sicurezza aziendale è il nostro focus e perciò ogni progetto viene valutato in fase d'analisi ed eventualmente integrato – anche step by step – sulle necessità specifiche rilevate.

Quello che offriamo non è un servizio di configurazione e gestione dei sistemi: le nostre attività si costuituiscono dal **punto di vista offensivo** e sono mirate ad identificare i punti di sicurezza tecnici, logici o umani di un'infrastruttura che possono o che devono essere migliorati per **difendere il Core Business** aziendale. Il nostro obiettivo è l'analisi oggettiva e ciò ci impone, ovviamente, d'evitare ogni possibile **conflitto d'interesse** come autoanalisi, vendita di soluzioni concorrenti, etc.

Noi non ci fermiamo ad eseguire una scansione con un software apposito ma integriamo questi dati fondamentali con le nostre conoscenze tecniche e le nostre analisi manuali: controlliamo capillarmente ogni singolo nodo e riduciamo, di conseguenza, i possibili **falsi positivi dei test automatizzati** mantenendo la necessaria contestualizzazione.

Quello che proponiamo è un controllo completo e specifico sulla vostra infrastruttura dal punto di vista di un potenziale attaccante, simulando i vari scenari di criticità. Dalla semplice verifica al **Cyber Risk Government**.

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 knowhow, 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

Awareness of Digital Security

L'Azienda conta nella propria struttura diversi assets:

- Infrastruttura hardware
- Software
- Risorse

Il più importante è rappresentato proprio dalle Risorse che "fanno l'Azienda" che con ogni metodologia si interfacciano tra loro per un obiettivo Aziendale comune. Essi scambiano informazioni, dati, contenuti di ogni genere, ma sempre di alto valore per tutti. L'informazione prende forma dall'aggregazione di tanti piccoli dati, notizie, scambio di conoscenze.

Quest'ultima – processata, validata, condivisa, ed archiviata– è già un patrimonio dell'Azienda e come tale abbiamo l'obbligo di proteggerla. Potremmo predisporre infrastrutture all'avanguardia, sofisticate, automatiche nei processi ma se i fruitori di questo grande patrimonio non fossero formati doverosamente allora gli investimenti potrebbero essere verosimilmente visti quali costi superflui.

Dobbiamo **formare** le nostre Persone affinché abbiano gli strumenti culturali adeguati. Tutti gli asset si comprano. La **knowledge** in questo specifico ambito si alimenta e non può e non deve essere di pochi.

OSINT

Conoscere quali e quante informazioni sono pubblicamente disponibili in rete e che potrebbero essere usate contro di noi è un aiuto fondamentale nel contrastare le minacce reali e cercare di controllarle. Bisogna conoscersi per proteggersi. Lo Studio Consi offre questo servizio di ricerca avanzata delle informazioni concernenti l'azienda o i top manager che potrebbero, appunto, essere usate contro di essa, fornendo una scheda dettagliata comprensiva di tutte le fonti rinvenute.

Soluzioni offerte

Analisi OSINT: Acronimo di OpenSource INTelligence, rappresenta il controllo delle informazioni pubblicamente disponibili concernenti un'infrastruttura come, ad esempio:

- **Credenziali** e/o informazioni dei vostri utenti disponibili su siti specializzati nella rivendita dati e piattaforme di sharing varie (Pastebin, ControlC).
- **Mis-configurazioni** che potrebbero aver comportato l'indicizzazione di file contenenti informazioni più o meno sensibili.
- **Vulnerabilità indicizzate** e verifica DNS
- Analisi di **dati involontariamente resi noti**
- Ricerche tramite **Dorks**
- Domini **omomorfi**
- Analisi **metadati**

Statisticamente, le principali possibilità di attacco potrebbero essere derivanti da tre possibili fonti:

- **Supply Chain** ovverosia un attacco derivante da un **fornitore** coinvolto compromesso;
- Compromissione di un **account di dominio**, specialmente nel caso in cui le risorse non siano state sufficientemente formate sui rischi del **password reuse**;
- Ritrovamento di **informazioni pubblicamente disponibili** come, ad esempio, moduli intestati che potrebbero aver consentito l'esecuzione del tentativo di phishing nei confronti dei Vostri clienti.

CLOSINT Analysis

La maggior parte degli incidenti di sicurezza ha avuto luogo a seguito di attacchi mirati al fattore umano: credenziali trafugate e riutilizzate e campagne di phishing sono il principale rischio per la sicurezza aziendale. L'analisi CLOSINT rappresenta un baluardo della sicurezza informatica preventiva: tramite l'analisi delle fonti presenti nel DarkWeb è infatti possibile monitorare la presenza dell'azienda o la comparsa della stessa in real time per prevenire il verificarsi di rischi relativi alle credenziali degli utenti, accessi VPN trafugati e/o informazioni aziendali disponibili.
Studio Consi verifica la presenza di tali informazioni (email, username, password, numeri di telefono, indirizzi ip, etc) sul darkweb su black market sites, P2P Networks, chat nascoste, botnets e siti privati e ti informa di tali rischi prima che possano divenire una minaccia per la tua azienda.

Phishing, Smishing e Malware Execution Simulation

Un evergreen: moltissimi attacchi informatici vengono effettuati attraverso l'interazione con gli utenti e, in particolare, attraverso attacchi di tipo phishing e smishing redatti mediante l'utilizzo di tecniche d'ingegneria sociale. Esiste però una grossa disinformazione su cosa sia un phishing reale: l'utente medio pensa allo spam che arriva nella sua casella di posta elettronica personale non al criminale organizzato che vuole ottenere una manipolazione di un comportamento.
Per aiutare l'azienda a formare i propri utenti a riconoscere questi vettori di rischio, Studio Consi offre un servizio di phishing targettizzato sull'azienda: questo aiuterà a mostrare agli utenti il vero rischio dando un'idea esatta del livello di preparazione degli utenti che potranno quindi toccare con mano, in un ambiente sicuro, la problematica relativa al phishing.

Phishing

Test mirato alla verifica del grado di resilienza Aziendale a mezzo email e più specificatamente:

- Il riconoscimento da parte degli utenti di minacce introducibili;
- Uso consapevole delle apparecchiature;
- Comportamenti congrui con le proprie mansioni e funzioni Aziendali;
- Attività da esterno o smart working.

Smishing

Test mirato alla verifica del grado di resilienza Aziendale a mezzo messaggistica SMS

Malware Execution Simulation

Test mirato alla verifica del grado di resilienza aziendale a mezzo email, con allegati con contenuto specifico ma ovviamente depotenziato.

Possibile timing di progetto Simulazione Phishing

Preparazione progetto

In coordinamento con il cliente predisposizione dei gruppi utenti aggregati:

- Studio modelli/format in base alla numerosità, composizione ed eterogeneità dei gruppi stessi.
- Preparazione server, domini e certificati SSL/TLS 1.2 o 1.3
- Mini serie di prova
- Pianificazione e schedulazione attività

Phishing mirato

Tali test possono essere svolti secondo tre livelli possibili:

- **Livello Base:** test di phishing effettuato mediante un test ovvio ed evidente. Tale test ha il più alto livello di possibile rilevazione (quindi di fallimento) da parte di software specifici come anti-spam e antivirus;
- **Livello Standard:** test di phishing effettuato mediante una targhettizzazione ad hoc della Vostra società effettuato per mezzo di classiche tipizzazioni e relativi attachments. Tale livello ha buone possibilità di verificare la formazione degli Utenti;
- **Livello Avanzato:** test di sicurezza mirato e realizzato esattamente al fine di verificare la formazione della singola risorsa effettuato per mezzo di format custom;
- **Livello Elevato:** test di sicurezza effettuato per mezzo di profilazione delle risorse Societarie in ambito Dirigenziale e da formare in eseguito attraverso format ad hoc dopo analisi personalizzata delle risorse stesse.

Analisi risultati aggregati

Data la vostra struttura e le vostre necessità, la nostra offerta mira ad analizzare esattamente ed oggettivamente il livello di formazione delle vostre Risorse mediante un test avanzato. Al termine di questa attività, verrà redatto un report complessivo in forma statistica aggregata ed anonimizzata sul livello di consapevolezza delle vostre Risorse Societarie.

Formazione Utenti

Uno dei punti più rischiosi allo stato attuale, nel panorama italiano e non solo, è il fattore umano. Iniziare un programma di awareness costituisce la principale difesa contro le tecniche d'attacco che più affliggono il tessuto aziendale italiano. È necessario trasmettere non solo l'idea del rischio ma le competenze necessarie per riconoscerlo ed evitarlo

Programma

Introduzione

- Mondo digitalizzato globalizzato:
  - Perimetro Aziendale
  - Perimentro Personale
- Alfabetizzazione digitale
- Hacker e mentalità criminale:
  - Chi sono questi hacker
  - Chi sono le vittime

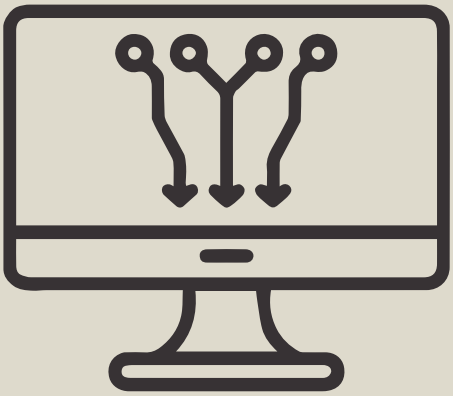
Sicurezza digitale in Azienda

- Il nostro patrimonio:
  - Il valore della nostra infrastruttura
  - Il valore del nostro patrimonio
- Vulnerabilità informatiche e tecniche d'attacco:
  - Le vulnerabilià hardware e software
  - Cyber attack
- Identificazione principali minacce:
  - Phishing
  - Smishing
  - Vishing
  - Altre minacce

Sicurezza digitale Personale

- Social Network
- Internet delle cose
- Ingegneria sociale

Se necessario, la fruizione dei contenuti formativi può avvenire online ma è caldamente consigliata – ove possibile – l'esecuzione dell'attività in presenza.
Il contatto con le risorse aiuta la veicolazione specifica delle informazioni fondamentali e consente – abbattendo il muro della distanza tra sconosciuti – ad affrontare insieme le casistiche pratiche e di rispondere, quindi, alle vere domande delle risorse aziendali. Si consiglia di prevedere sessioni di massimo 20/30 Persone.



Attack Simulation

I vantaggi che derivano dall'esecuzione delle attività offensive (come Vulnerability Assessments e Penetration Tests) sono molteplici: innanzitutto, permettono all'azienda di identificare e risolvere problemi relativi alla sicurezza informatica, riducendo così il rischio di perdite finanziarie e reputazionali. Inoltre, consentono di aumentare la consapevolezza del personale aziendale riguardo alle minacce informatiche e alle buone pratiche da seguire per prevenire gli attacchi. Infine, un Vulnerability Assessment e un Penetration test possono essere richieste dai clienti o dalle autorità competenti come requisiti obbligatori per garantire la conformità della sicurezza informatica dell'azienda rispetto agli standard esistenti nel settore.

Vulnerability Assessment

Cos'è un Vulnerability Assessment?

Cos'è una vulnerabilità? Il microcosmo di un sistema informatico è composto da molteplici ambiti, ognuno con le proprie peculiarità e le proprie caratteristiche tecniche. In questo campo non concorrono solamente evoluzioni tecnologiche, risorse, budget su investimenti, etc. ma anche sistemi c.d. legacy, software obsoleti, comunicazioni esterne sempre più avanzate e sempre meno sotto il nostro controllo, hardware dimenticati, comportamenti lavorativi non congrui o magari funzionali al solo risultato e non alla sicurezza, etc.

In tutto questo marasma tecnologico le vulnerabilità scoperte circa un software, OS, protocollo, etc., vengono catalogate in alcuni databases pubblicamente disponibili: le CVE. Queste, quindi, rappresentano le vulnerabilità già note al pubblico relative ad una soluzione commercialmente molto diffusa. Per quanto utili e fondamentali, questi elenchi non sono e non saranno mai completi poiché, appunto, contengono dati relativi alle soluzioni più diffuse al mondo e non considerano misconfigurazioni di rete o di sistema, applicativi minori o custom, etc. Tutte queste vulnerabilità non possono essere rilevate tramite un generico scanner ma devono essere analizzate da **personale qualificato**. L'immagine più vicina a questo scenario è quella di un "**check-up completo**": il nostro lavoro è quello di "fotografare" – in un determinato momento – lo status e il livello di sicurezza di una struttura, non di risolverlo.

Soluzioni offerte

Un Vulnerability Assessment (VA) può essere effettuato sia sul perimetro esterno che sul perimetro interno di una società, quindi sia su ciò che è raggiungibile tramite internet da chiunque sia quanto è raggiungibile esclusivamente dall'interno della rete aziendale.

Per quanto riguarda il **perimetro esterno**, si parte da una prima fase di analisi OSINT: si identificano i domini e i sottodomini aziendali, gli applicativi esposti – come VPS per siti showcase, **e-commerce**, **CRM** e **portali collaborativi** – e le relative configurazioni alla ricerca di vulnerabilità che potrebbero essere utilizzate per accedere ai dati trattati o, in alcuni casi, addirittura al network aziendale.

Le analisi relative al **perimetro interno**, invece, cercano di identificare le misconfigurazioni di rete, di sistema, di dominio, etc., i software e i sistemi operativi obsoleti ancora raggiungibili e attaccabili, l'utilizzo di credenziali deboli, etc., che potrebbero comportare dei rischi per la **sicurezza aziendale**, il **blocco produttivo** e il danno d'**immagine aziendale**. Tutto ciò, ovviamente, comporta l'analisi di una gran mole di dati riguardanti non solo i Personal Computer utilizzati dalle risorse aziendali ma anche centralini **VoIP**, **videosorveglianze**, sistemi **SCADA** e **Industria 4.0**.

L'attività si conclude con un report dettagliato diviso in due sezioni: una prima parte **Directional** rivolta alla Direzione che si sofferma sull'analisi complessiva più che sui dettagli tecnici e, una seconda parte, c.d. **Executive**, comprendente tutte le mitigazioni tecniche necessarie per ovviare alle rilevazioni effettuate.

Penetration Test

Cos'è un Penetration Test?

Un Penetration Test (PT) differisce da un Vulnerability Assessment (VA) in quanto si richiede espressamente di cercare una possibile "strada" che possa condurre ad una compromissione di un'infrastruttura, piattaforma, etc., e di verificare dove e fino a che punto tale vulnerabilità può o potrebbe essere spinta.

Per verificare un possibile scenario di compromissione, dunque, è necessario ragionare e muoversi come un Hacker ma con la consapevolezza e l'obiettivo di aiutare la società ad evitare che tali scenari si verifichino realmente. Per tale motivo, quindi, i nostri test – ove tecnicamente possibile ovviamente – cercano di rispettare anche un requisito ulteriore ovverosia la realizzazione di quello che viene chiamato **PoC** (Proof of Concept), quindi un programma appositamente redatto per aiutare gli sviluppatori a replicare i nostri test e verificare d'aver dunque risolto una segnalazione.

Un Penetration Test viene solitamente diviso in tre possibili livelli: White Box, Grey Box e Black Box e cioè, rispettivamente, con una conoscenza completa, conoscenza parziale o nessuna conoscenza pregressa dell'infrastruttura.

Privilege escalation, sql inection, movimento laterale ecco alcuni degli scenari di compromissione (basato sullo standard internazionale **Mitre ATT&CK®**) che un nostro Professionista verifica. Diversamente dal check-up del VA, dunque, nel PT si simula a tutti gli effetti un attacco informatico.

Soluzioni offerte

Similmente a quanto già detto per il Vulnerability Assessment, anche nel caso del Penetration Test si parte da una analisi OSINT preliminare, limitata ma funzionale alla **simulazione reale d'attacco**. Le uniche cose che ci servono, di fondo, sono l'identificazione di cosa si vuole testare, le autorizzazioni a procedere, una presa elettrica e un cavo di rete.

Il Responsabile del progetto sarà reperibile durante tutta la durata del progetto per ogni necessità tecnica urgente e al termine del progetto illustreremo – punto a punto – ogni vulnerabilità rilevata e daremo indicazione su come andrebbe risolta allegando, dove possibile, il codice informatico necessario per replicare un determinato comportamento.

Che si tratti di sistemi SCADA, Industry 4.0, un network aziendale o una nuova web application, il Penetration Test stabilisce un test fondamentale per la sicurezza dei dati trattati e il soddisfacimento di specifici obblighi legali.

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

Window Snyder

Responsabile della sicurezza delle informazioni presso Square, Inc., Apple, Fastly, Intel, Mozilla Corporation.

Check AD Hash

Delle credenziali degli utenti salvate nei Domain Controller, quante di queste sono veramente vulnerabili? Spesso, quando si effettuano attività come Vulnerability Assessment e Penetration Test si cerca di verificare le credenziali degli utenti. Tuttavia, svolgendolo in ambiente di produzione, questo comporta, in molti casi, il blocco temporaneo degli utenti testati.

Per evitare ogni eventuale disservizio alla struttura, è possibile **estrarre le password** degli utenti e verificarle "**offline**" sui nostri sistemi. In questo modo viene effttuata un'analisi dettagliata, indicando quali utenti e quali informazioni potrebbero risultare più utili in una sessione di formazione oltreché a fornire il supporto pratico per forzare la sostituzione delle credenziali e **ridurre**, quindi, uno dei **principali rischi** per la sicurezza informatica.

Ambienti produttivi SCADA/ICS/PLC

Nel mondo della spinta verso l'industria 4.0, l'integrazione fra macchina e infrastrutture digitali interne ed esterne è sempre più oggetto di attenzione ed investimenti. Questi assets e le misure a loro protezione rappresentano i trend con un tasso di crescita maggiore a livello internazionale. Nel corso del 2021 le aziende manufatturiere italiane hanno subito statisticamente un 10,8% in più di attacchi volti proprio a manomettere questa specifica risorsa aziendale.

I punti di contatto tra le infrastrutture interne e il mondo esterno sono delle ottime opportunità ma possono anche rappresentare potenziali vulnerabilità: riusciamo a fare il computo del **costo giornaliero** di un fermo produttivo o di distribuzione? Analizzare la sicurezza degli ambienti produttivi vuole evidenziare quali potrebbero essere gli scenari più probabili, i vettori di rischio e quali le conseguenze del verificarsi delle minacce più diffuse.

Interazioni e possibili incidenti

Interazioni: Remote Support, Supply Chain, Customer Support, Logistic Chain.

Incidenti

- Un **malware generico** si insinua nella rete industriale e lascia il segno nei dispositivi Windows. Ad esempio, le recenti epidemie dei ransomware WannaCry ed ExPetr.
- **Attacchi mirati** come Stuxnet, Havez o Industroyer, piattaforme malware e procedure d'attacco progettate specificatamente per colpire gli ICS.
- **Operazioni fraudolente di persone interne** all'azienda con lo scopo di arrecare danno senza l'uso di tecniche hacker, solo mediante la conoscenza dell'infrastruttura.
- **Errori e configurazioni erronee** di hardware e software degli ICS.

Soluzione offerta

La soluzione che offriamo è l'esecuzione di **Vulnerability Assessment** che vada a verificare non solo quali problematiche tecniche sono riscontrabili all'interno della rete di produzione ma anche – e forse soprattutto – **come ci si potrebbe arrivare,** quali azioni potrebbero essere compiute per arrecare un danno all'infrastruttura e quali, invece, potrebbero essere poste in essere per **evitare che si verifichino questi scenari.**

Monitoring Mitigation

Il servizio di monitoring mitigation si estrinseca in un controllo della progressiva risoluzione delle problematiche precedentemente riscontrate, e in un **regression test**, anche con cadenza periodica in sinergia con le risorse preposte all'attività.

Efficiency Monitoring SOC

Un **SOC** o **Security Operation Center**, è una centro dove vengono **centralizzate** tutte le informazioni sullo stato di **sicurezza dell'IT** di un'azienda o di più aziende (nel caso che il SOC appartenga a un **Managed Security Service Provider**, MSSP).
Può essere creato in azienda, fruito come servizio gestito esempio **SOCaaS** ovvero SOC as a Service, oppure implementato in modo ibrido. Nelle Aziende aventi strutture di grandi dimensioni o di particolare importanza strategica si è soliti inserire questo servizio continuativo di monitoraggio e difesa. In altre parole un insieme di sonde e sentinelle che monitorano tutto quello che succede e, a seconda del grado di filtraggio degli eventi, segnala ed interviene con funzioni di blocco automatico o manuale.

Proprio la calibrazione dei criteri di filtro può essere misconfigurata: rilevare il c.d. "rumore di fondo" e non rilevare un vero attacco informatico può spingere a sottovalutare i reali livelli di rischio.

Il servizio di Efficiency Monitoring SOC prevede quindi l'esecuzione di analisi finalizzate non tanto alla rilevazione di vulnerabilità quanto dei tempi e qualità di reazione del nucleo SOC per evidenziare eventuali carenze e possibili implementazioni. Ogni attività viene effettuata nell'ottica di identificare i "trigger" che vengono dispiegati dal SOC con livelli decrescenti di complessità.

Questo "modus operandi" viene usato per **verificare nel tempo l'efficienza** richiesta.

Framework Legal Compliance

Un servizio di analisi del livello di compliance societaria ai requisiti normativi cogenti in materia di protezione dei dati personali e cybersecurity può offrire numerosi vantaggi alle aziende, tra cui:

- Identificazione dei punti critici: L'analisi permette di individuare i punti deboli dell'organizzazione in termini di gestione e protezione dei dati personali e della sicurezza informatica.
- Miglioramento della trasparenza: L'azienda può dimostrare la propria conformità alle norme sulla privacy e sulla sicurezza informatica, migliorando la trasparenza nei confronti dei clienti, dei partner commerciali e delle autorità competenti.
- Miglioramento della reputazione: Essere conformi alle norme sulla privacy e sulla sicurezza informatica può aumentare la fiducia degli utenti e migliorare la reputazione dell'azienda.
- Riduzione del rischio legale: L'adeguamento alle norme sulla privacy e sulla sicurezza informatica può ridurre il rischio di sanzioni amministrative o azioni legali da parte degli utenti o delle autorità competenti.
- Risparmio economico: L'analisi permette di individuare eventuali inefficienze o costi superflui nella gestione dei dati personali e della sicurezza informatica.
- Miglioramento delle politiche interne: L'analisi può fornire indicazioni utili per migliorare le politiche interne dell'azienda in materia di gestione dei dati personali e della sicurezza informatica.
- In generale, un servizio di analisi del livello di compliance societaria ai requisiti normativi cogenti in materia di protezione dei dati personali e cybersecurity può fornire all'azienda una visione chiara della propria situazione attuale in materia di privacy e sicurezza informatica, consentendo di migliorare la propria conformità alle norme, ridurre i rischi associati alla gestione dei dati personali e migliorare la reputazione dell'azienda.

Gap Analysis 27001/CIS18 - CIS20

Effettuare una GAP Analysis sulla certificazione UNI EN ISO 27001:2022 e/o sullo standard CIS18/CIS20 offre numerosi vantaggi, tra cui:

- Identificazione delle lacune: la GAP Analysis aiuta a identificare le lacune nella conformità alle norme ISO 27001 e allo standard CIS18/CIS20 rispetto alle attuali pratiche aziendali.
- Miglioramento della sicurezza delle informazioni: l'analisi aiuta ad individuare le aree in cui è necessario migliorare la sicurezza delle informazioni, permettendo di porre in atto misure di sicurezza più efficaci.
- Rispetto dei requisiti normativi: l'effettuazione dell'analisi consente di verificare la conformità alle normative vigenti, garantendo il rispetto dei requisiti normativi previsti dalla legge.
- Miglioramento della gestione del rischio: l'analisi aiuta a comprendere i rischi presenti nell'ambiente aziendale e a definire le azioni necessarie per mitigarli, contribuendo al miglioramento della gestione del rischio.
- Identificazione di opportunità di miglioramento: grazie all'analisi è possibile individuare opportunità per migliorare i processi aziendali, aumentando l'efficienza ed il livello di sicurezza delle informazioni.
- Aumento della fiducia dei clienti: ottenere la certificazione secondo le norme UNI EN ISO 27001 ed effettuare GAP Analysis sullo standard CIS18/CIS20 dimostra agli stakeholder che l'azienda si impegna nella protezione delle informazioni sensibili e nella tutela della privacy dei clienti, aumentando la loro fiducia nella società.
- Miglioramento della reputazione: la certificazione ISO 27001 e dei controlli CIS è riconosciuta a livello internazionale e dimostra l'impegno dell'azienda per la sicurezza delle informazioni. Ciò può contribuire ad aumentare la reputazione dell'azienda nel mercato.

Compliance GDPR

L'effettuare un'analisi sul livello di compliance GDPR offre numerosi vantaggi, tra cui:

- Identificare le aree in cui l'organizzazione non è conforme al GDPR: l'analisi aiuta a identificare le aree in cui l'organizzazione non rispetta le normative del GDPR, fornendo un quadro completo delle attuali pratiche e procedure.
- Pianificare e implementare azioni correttive: una volta identificate le aree di non conformità, l'organizzazione può pianificare e implementare azioni correttive per garantire la conformità al GDPR.
- Minimizzare i rischi di sanzioni e multe: identificando le aree di non conformità e agendo tempestivamente per correggerle, l'organizzazione può minimizzare il rischio di sanzioni e multe da parte delle autorità competenti.
- Miglioramento della sicurezza dei dati: l'analisi consente all'organizzazione di valutare la sicurezza dei dati e fornire un livello più elevato di protezione dei dati personali dei propri clienti.
- Aumento della fiducia del cliente: dimostrando la conformità al GDPR, l'organizzazione può aumentare la fiducia dei propri clienti nella protezione dei loro dati personali.
- Miglioramento dell'immagine dell'azienda: dimostrando un impegno per la privacy dei dati personali, l'azienda può migliorare la propria immagine nei confronti del pubblico e degli investitori.
- In sintesi, effettuare un'analisi sul livello di compliance GDPR consente all'organizzazione di garantire il rispetto delle normative e dei regolamenti in materia di protezione dei dati personali, minimizzando i rischi e migliorando la sicurezza dei dati.

Security Consultancy

Un servizio di consulenza per la sicurezza delle informazioni offre assistenza alle aziende per garantire la protezione dei loro dati sensibili. Gli esperti della sicurezza informatica valutano i rischi, identificano le vulnerabilità e sviluppano strategie personalizzate per ridurre al minimo le minacce alla sicurezza dei dati. Questo servizio include anche la formazione del personale sull'importanza della sicurezza delle informazioni e sulle procedure da seguire per prevenire le violazioni della sicurezza. La consulenza per la sicurezza delle informazioni aiuta le aziende a proteggere i loro dati e a mantenere la fiducia dei clienti e degli investitori.

Ci sono diversi vantaggi nell'avere un consulente per la sicurezza informatica imparziale. Eccone alcuni:

- Obiettività: un consulente imparziale non ha alcun interesse personale nella scelta di determinati prodotti o soluzioni. Questo significa che le sue raccomandazioni saranno basate esclusivamente sulla sua esperienza e conoscenza del settore, senza essere influenzate da fattori esterni.
- Conoscenze specialistiche: un consulente per la sicurezza informatica imparziale avrà una vasta conoscenza delle minacce informatiche e delle migliori pratiche per prevenirle o mitigarle. Questo significa che sarà in grado di fornire consigli preziosi sulle soluzioni più efficaci per proteggere i dati e i sistemi dell'azienda.
- Risparmio di tempo e denaro: assumere un consulente interno per la sicurezza informatica può essere costoso, soprattutto se l'azienda è di piccole dimensioni. Inoltre, potrebbe richiedere molto tempo trovare la persona giusta con le giuste competenze e conoscenze del settore. Assumere un consulente esterno può aiutare l'azienda a risparmiare tempo e denaro, in quanto non ci sarebbe bisogno di formare internamente una figura specializzata.
- Flessibilità: assumere un consulente per la sicurezza informatica esterno offre all'azienda flessibilità nella scelta dei servizi necessari. Ad esempio, l'azienda potrebbe richiedere solo una valutazione della sicurezza dei propri sistemi o una revisione degli accessi ai dati. Un consulente esterno può fornire solo i servizi necessari, senza dover essere assunto a tempo pieno o per un periodo prolungato.
- Aggiornamento costante: la tecnologia informatica è in continua evoluzione e le minacce informatiche cambiano regolarmente. Un consulente per la sicurezza informatica imparziale sarà sempre aggiornato sulle ultime tendenze e minacce, garantendo all'azienda di avere sempre le migliori soluzioni per minimizzare i rischi e i relativi impatti.

Rating Preventiva

La nostra costante ricerca della più assoluta oggettività e l'esperienza in moltissime aziende diverse e con necessità differenti ci ha consentito di maturare una conoscenza delle infrastrutture e delle soluzioni sistemistiche piuttosto particolare. Possiamo assistere in via consulenziale circa l'acquisto o la sostituzione di soluzioni di sicurezza dando un rating esterno alle possibili soluzioni senza incorrere nel rischio del conflitto d'interessi.

IT Security Consultant

Un consulente esterno può offrire una visione imparziale e una prospettiva esterna che può aiutare l'azienda a prendere decisioni informate. Grazie all'esperienza acquisita in altri settori, i consulenti possono offrire una conoscenza più ampia rispetto a quella disponibile in-house e fornire un'analisi obiettiva delle alternative di investimento tecnologico.

Inoltre, i nostri consulenti possono quindi aiutare a identificare le minacce o le opportunità tecnologiche che possono influenzare la strategia dell'azienda e fornire suggerimenti su come affrontarle. I consulenti possono anche esaminare le prestazioni attuali e future delle tecnologie installate per sostenere la crescita o creare nuovi flussi di reddito. Inoltre, possono offrire l'accesso ad alcune tecnologie innovative di cui l'azienda potrebbe non essere al corrente.

Infine, un esterno imparziale può monitorare attentamente lo stack tecnologico installato per assicurarsi che soddisfi i requisiti dell'azienda, specialmente quando si tratta di nuove soluzioni. Questo può garantire che il business abbia gli strumenti di cui ha bisogno per rimanere competitivo nel mercato.

Infrastructure Inventory

Effettuare un Infrastructure Inventory consente di:

- Conoscere in modo preciso quali sono i beni aziendali presenti in azienda
- Monitorare l'utilizzo degli asset, la loro manutenzione e la loro sostituzione.
- Identificare le aree di miglioramento dell'azienda per quanto riguarda l'utilizzo degli asset.
- Migliorare la gestione del budget aziendale, evitando acquisti non necessari o duplicati di beni già presenti in azienda.
- Aumentare la sicurezza dell'azienda, avendo una visione completa dei beni presenti e dei relativi rischi associati.
- Facilitare la gestione delle garanzie e delle assicurazioni dei beni aziendali
- Agevolare le attività contabili e fiscali dell'azienda, avendo una visione completa del patrimonio aziendale

SCHEDA TECNICA

Timing di progetto

PERIMETRO ESTERNO

- Verifica della configurazione DNS e relativo test di sicurezza
- Enumerazione dei servizi esposti
- Enumerazione directories e permessi d'accesso non autenticati
- Identificazione delle versioni installate
- Verifica attinenza d'eventuali CVEs
- OSINT e verifica dei dati pubblicamente disponibili
- Verifica della presenza di eventuali filtri di validazione degli input e test di bypass
- Exploit
- Report
  Directional section:
  - Dati preliminari e scope del progetto;
  - Esito del Penetration Test;
  Executive section:
  - Metodologia utilizzata e step eseguiti;
  - Analisi dettagliata di quanto rilevato;

PERIMETRO INTERNO

- Fingerprinting di tutti i nodi di rete
- Verifica dei servizi esposti e della relativa configurazione
- Verifica dell'esistenza di CVE
- Test applicabilità CVE
- Test sulla politica delle credenziali
- Test su possibilità di movimento laterale
- Test phishing mirato su utenti
- Privilege escalation
- Report
  Directional section:
  - Dati preliminari e scope del progetto;
  - Esito del Penetration Test;
  Executive section:
  - Metodologia utilizzata e step eseguiti;
  - Analisi dettagliata di quanto rilevato;

Cyber Risk Government

ANALISI DELLA SICUREZZA ESTERNA

- Analisi OSINT
- Vulnerability Assessment
- Penetration Test
- Awareness

ANALISI DELLA SICUREZZA INTERNA

- Vulnerability Assessment
- Penetration Test
- Privilege Escalation
- SCADA/PLC

CONCLUSIONE

- Discussione tecnica finale
- Analisi possibili 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

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 **ridefinizione** 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

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 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.

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: Via G. Verdi 15 Asolo 31011 (TV)
Sede operativa: P.zza Serenissima 40/101
Castelfranco Veneto 31033 (TV)
Punto ufficio: Via Sanseverino 95 Trento
38122 (TN)

0423 57 08 84
0423 19 90 486

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

studioconsi.com

Sponsor