sinattica
SERVIZI EVOLUTI PER L'AZIENDA

PROGRAMMA SICUREZZA

Programma Sicurezza Sinattica

Per la difesa informatica delle Imprese

PROGRAMMA SICUREZZA SINATTICA

Per la difesa informatica delle imprese

Quattro fasi, un solo obiettivo: **ridurre a zero tutte le vulnerabilità informatiche all'interno delle infrastrutture aziendali** che hacker e cyber criminali potrebbero sfruttare per compiere attacchi, frodi e violazioni dalle estreme conseguenze.

PROGRAMMA SICUREZZA SINATTICA

Indice dei contenuti

Difesa informatica per le Imprese	pag. 01
Le 4 fasi del PSS	pag. 02
IT Risk Assessment	pag. 03
Advisory e Strategy	pag. 05
Vulnerability Assessment (V.A.)	pag. 07
Penetration Test (PenTest)	pag. 09
Business Continuity & Disaster Recovery	pag. 11

PROGRAMMA SICUREZZA

PROGRAMMA SICUREZZA SINATTICA

Difesa informatica per le Imprese

Ogni giorno i media riportano notizie di violazioni di sistemi informatici con conseguente sottrazione di dati sensibili che coinvolgono multinazionali, istituzioni e banche. Quel che si legge più raramente è che **gran parte del bottino di hacker e cyber crimiminali deriva da attacchi rivolti a imprese di qualsiasi dimensione**.
Uno scenario critico in cui la posizione dell'Italia risulta aggravata da una poco invidiabile seconda posizione all'interno della Classifica dei Paesi più colpiti dell'Unione Europea stilata lo scorso anno da Check Point Research.

Perché le Imprese sono nel mirino dei criminali informatici?

Nel 2021 l'84% delle aziende italiane è stata dichiarata a rischio di attacchi ad alto impatto. La causa principale è da ricondursi a criticità informatiche apparentemente latenti. A causa dei ridotti o mancati investimenti in materia di cybersecurity, tali attività risultano **impreparate di fronte alle conseguenze operative ed economiche di un blocco informatico**. Pertanto, negli anni si sono dimostrate le **più propense a cedere a richieste di riscatto**. Organizzazioni che quotidianamente gestiscono copiose quantità di dati sensibili relative a clienti, dipendenti, fornitori, manuali e processi. Ne consegue che senza investimenti in strumenti e procedure di tutela efficaci, indipendentemente dalle dimensioni, dal fatturato annuale e/o dal settore di riferimento, per ognuna di esse aumenta esponenzialmente la probabilità di subire un fermo forzato a causa di un attacco informatico.

PROGRAMMA SICUREZZA SINATTICA

Le 4 fasi del PSS

È difficile comprendere autonomamente gli effettivi rischi a cui la propria infrastruttura è esposta. Per questo prova a domandarti: *Quanto mi costerebbe in termini di tempo e reputazione un fermo forzato? Esistono dati che posso permettermi di perdere? Sarei finanziariamente pronto ad affrontare le conseguenze di un attacco?*
Per poterti garantire piena operatività, abbiamo affinato una strategia in grado di mantenere la tua impresa al sicuro da rischi e minacce cyber: il **Programma Sicurezza Sinattica**. Un piano di difesa articolato in 4 fasi.

PSS:

1. **IT Risk Assessment**
   analisi dei rischi informatici dell'infrastruttura

2. **Advisory e Strategy**
   consulenza e strategia di difesa personalizzata

3. **Vulnerability Assessment**
   valutazione delle vulnerabilità della rete aziendale

4. **Penetration Test**
   simulazione di attacchi hacker provenienti dall'esterno

FASE 1

IT Risk Assessment

Analisi dei rischi informatici dell'infrastruttura

Per definire ed attuare un piano di protezione a lungo termine, è fondamentale avere una visione chiara dei rischi a cui la propria infrastruttura informatica è esposta.

A tale scopo, la FASE 1 del PSS si divide in 3 step:

1. **Analisi dei processi di gestione dei dati**
2. **Identificazione dei rischi dell'infrastruttura IT**
3. **Qualificazione dei rischi identificati**

Il processo di analisi inizia con la somministrazione di un **IT&Process Strategic Survey**, un questionario sottoposto da un consulente Sinattica a uno o più referenti aziendali a seconda dei relativi ambiti di competenza.

Tra le categorie oggetto dell'indagine:

- Sistema Informativo Aziendale
- Applicativi e Modalità di autenticazione
- Networking fisico e logico
- Backup e Business Continuity
- CED e Accesso fisico
- Marketing e Visibilità Web
- Videosorveglianza e Gestione delle intrusioni
- Sicurezza alla persona

Terminata la procedura di somministrazione, i consulenti Sinattica esamineranno le risposte fornite con l'obiettivo di **tracciare un profilo dettagliato ed esaustivo in merito alle procedure e alle modalità di gestione dati da parte dell'impresa e dei suoi collaboratori**.

Ad analisi conclusa, l'azienda riceverà un **report relativo a quanto emerso durante l'indagine** e **alle minacce** a cui l'infrastruttura informatica e l'intera organizzazione risultano esposte in termini di corretta gestione dei dati trattati.

Lo scopo del documento è mettere a tua disposizione una fotografia completa e facilmente leggibile della situazione riscontrata nel corso della FASE 1 del PSS.

I rischi elencati all'interno della relazione **verranno categorizzati a seconda della loro portata e dell'urgenza con cui**, da un punto di vista tecnico, **è opportuno porvi rimedio**. Le contromisure necessarie e il loro iter di esecuzione saranno definiti nel corso della FASE 2 del Programma Sicurezza Sinattica.

Indipendentemente dalle soluzioni proposte, le stesse dovranno ottemperare ai 5 requisiti fondamentali del GDPR (Reg. UE 2016/679) riportati a seguito.

CONOSCERE i propri dati e mapparne la posizione.

REGOLAMENTARE l'accesso ai dati in termini di procedure e autorizzazioni.

PROTEGGERE i dati trattati attraverso le soluzioni più idonee.

DOCUMENTARE l'adempimento alle norme vigenti.

AGGIORNARE con continuità le misure di protezione adottate.

FASE 2

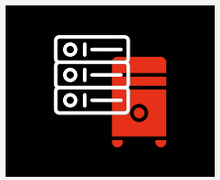
Advisory e Strategy

Consulenza e Strategia di difesa

Una volta identificati i rischi legati ai processi di gestione aziendale, il PSS procede con la FASE 2. Dedicata alla **mappatura delle componenti IT** e alla **stesura di un piano di ristrutturazione** finalizzato al potenziamento della protezione informatica dell'impresa, la seconda fase del Programma Sicurezza Sinattica si sviluppa in 3 azioni:

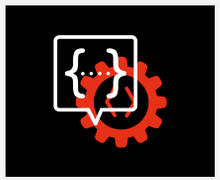
1. **Identificazione di software e device in uso**
2. **Analisi delle componenti identificate**
3. **Elenco e dettaglio delle soluzioni proposte**

Il primo step della FASE 2 prevede la mappatura di tutte le componenti che, nell'insieme, costituiscono l'infrastuttura informatica aziendale, ovvero:



HARDWARE

Server, client e dispositivi



SOFTWARE

Sistemi operativi, app e programmi

RETI & WIFI

Concentratori e access point

Terminato il processo di mappatura, verranno analizzate funzioni, caratteristiche, servizi e falle di ogni potenziale punto di accesso all'infrastruttura.

Per provvedere alle criticità riscontrate e prevenire danni o blocchi futuri delle componenti, i consulenti Sinattica procederanno con la **definizione di un piano di carattere risolutivo** la cui attuazione, in termini di tempistiche e modalità di intervento, sarà invece concordata insieme al cliente.

Ragionando in ottica proattiva, durante l'esecuzione degli interventi verranno installati degli **agent di monitoraggio** su tutti i sistemi informatici dell'azienda.

Attraverso il **Servizio di Monitoraggio Proattivo**, Sinattica potrà verificare con continuità la stabilità, il grado di aggiornamento e le anomalie di ciascuna componente. In questo modo sarà possibile preservare nel tempo il grado di efficienza dell'intera infrastruttura sia in termini di performance che di sicurezza.

> **"L'obiettivo di Sinattica è evitare quanto più possibile disagi o fermi di lavoro consentendo allo stesso tempo la conclusione di tutte le operazioni in tempi certi e modi celeri.**

Luoghi e tempisitiche di intervento saranno definiti in virtù dei seguenti fattori:

Tipologia di vulnerabilità

Portata delle criticità

Prestazioni di rete e device

Previsioni di riavvio

Aggiornamenti disponibili

Backup necessari

FASE 3

Vulnerability Assessment (V.A.)

Valutazione delle vulnerabilità della rete aziendale

Un piano proattivo di sicurezza informatica prosegue con il monitoraggio diretto dell'intera infrastruttura.

Per questa ragione, la FASE 3 del PSS, dedicata alla valutazione approfondita delle vulnerabilità della rete e dei dispositivi ad essa connessi, si prefigge lo scopo di **individuare nuove o potenziali criticità della rete informatica aziendale**.

Denominato **Vulnerability Assessment** (**V.A.**), questo processo consente di testare il proprio livello di cybersecurity interna, prevenire nuove minacce e salvaguardare la piena operatività dell'azienda. Se eseguito con continuità prende il nome di **Continuous Vulnerability Assessment** (**C.V.A.**)

Attraverso l'installazione di un apposito dispositivo locale sarà possibile avviare il processo di scansione, il quale permetterà di esaminare tutti gli apparecchi fissi e mobili collegati alla rete, anche da remoto.

Scansioni, analisi e valutazione delle vulnerabilità svolte da Sinattica interesseranno nello specifico:

- Sistemi Operativi di Client e Server
- Apparati e Dispositivi di rete
- Software e Web Applications
- Codici di sviluppo delle Applicazioni
- Procedure di Archiviazione dati
- Informazioni condivise in Rete

Le operazioni descritte permetteranno di individuare apparati e utenti a rischio, ovvero tutte le componenti e i collaboratori che potrebbero subire attacchi a causa delle falle individuate.

Ogni vulnerabilità riscontrata verrà poi categorizzata al fine di stimare il grado di sicurezza di tutti i sistemi informatici. Tale classificazione costituirà il punto di partenza per la definizione e l'applicazione di un **Piano Organizzato di Rimedi**.

Si riportano a lato degli esempi di tipiche **Remediations**:

- Installazione di Patch e Aggiornamenti
- Revisione delle Policy di Protezione dati
- Installazione di Dispositivi di Sicurezza
- Applicazione di Filtri di Navigazione

FASE 4

Penetration Test (Pen Test)

Simulazione di attacchi provenienti dall'esterno

Terminata la valutazione delle vulnerabilità interne, la FASE 4 del PSS consiste nel **testare il livello di sicurezza raggiunto in seguito all'applicazione delle contromisure previste dalle fasi precedenti**.

Tale processo prende il nome di **Penetration Test** (**PenTest**) e prevede il coinvolgimento di una o più figure tecniche specializzate in interventi di sabotaggio a scopo preventivo, gli ethical hacker.

Durante il Penetration Test gli ethical hacker coinvolti **progetteranno e simuleranno una cyber-irruzione al fine di verificarne l'impatto e le effettive conseguenze**.

Tale procedura sarà supervisionata dai consulenti Sinattica e consentirà di **identificare nuovi e potenziali punti di debolezza dell'infrastruttura e della rete aziendale**. Inoltre, l'esecuzione di queste operazioni sarà utile per certificare i punti di forza noti e testare l'efficacia delle soluzioni implementate tramite gli interventi precedentemente svolti nell'ambito dell'intero Programma Sicurezza elaborato da Sinattica.

A simulazione conclusa, ti verrà consegnato un report contenente recap ed esiti dei vari test svolti. Nello stesso saranno evidenziati:

- Mezzi impiegati e Processi attuati
- Criticità riscontrate
- Remediations utili
- Piano operativo di Applicazione dei rimedi

> **"Il PSS è concepito per fornire alle Imprese una risposta concreta e attuabile in termini di cybersecurity. Un investimento per guardare al futuro della propria azienda tutelandone passato e presente.**

Le 4 fasi del PSS sono indipendenti ma la loro applicazione sequenziale permette di ridurre di oltre il 90% il rischio di un blocco forzato e di:

Proteggere con continuità i dati dell'azienda

Tutelare la piena operatività dei reparti

Rafforzare la reputazione dell'impresa

Business Continuity e Disaster Recovery

Continuità Operativa e Recupero in caso di Disastro

In ogni settore, operatività e produttività di ogni reparto, ufficio e collaboratore dipendono dall'efficienza dei sistemi informatici.

La **capacità dell'impresa di proseguire nella propria attività anche in seguito a eventi imprevisti** quali danni, disastri ambientali o attacchi informatici, prende il nome di **Business Continuity**.

Ragionando in quest'ottica, è chiaro che il Programma Sicurezza Sinattica possa essere inserito all'interno di un contesto molto più ampio e complesso.

Analisi ed esiti di tutte e 4 le FASI del PSS risultano elementi chiave ai fini dell'ottimizzazione del processo di gestione della continuità operativa della tua impresa. Inoltre gli stessi costituiranno il punto di partenza per la redazione di un **Business Continuity Plan,** ovvero il piano da applicare nel caso in cui la tua azienda fosse costretta a fronteggiare e risolvere imprevisti di qualsiasi entità. La stesura di un **Piano di Continuità Operativa** può avvenire solo in seguito a un'accurata analisi dei rischi informatici, ovvero la FASE 1 del Programma Sicurezza.

A quale scopo redarre un Business Continuity Plan?

- **ASSICURARE** la prosecuzione delle attività essenziali dell'organizzazione.
- **IDENTIFICARE** gli eventi che ne ostacolano la continuità operativa.
- **DEFINIRE** procedure e modalità di reazione tempestive ed effecaci.
- **RIDURRE** i rischi mediante l'applicazione di specifici strumenti e processi.

Per contrastare al 100% il rischio di un blocco forzato e preservare la propria continuità operativa è utile associare alle 4 FASI del Programma Sicurezza Sinattica una strategia personalizzata di **Disaster Recovery**.

Elaborare un **Piano di Recupero in caso di Disastro** significa identificare gli strumenti da adottare e le procedure da applicare in seguito a eventi o incidenti di qualsiasi natura e portata. Si tratta quindi di una serie di regole, strumenti e tutele attraverso cui l'impresa può **riacquistare il controllo dei propri sistemi IT senza subire fermi o perdite di dati.**

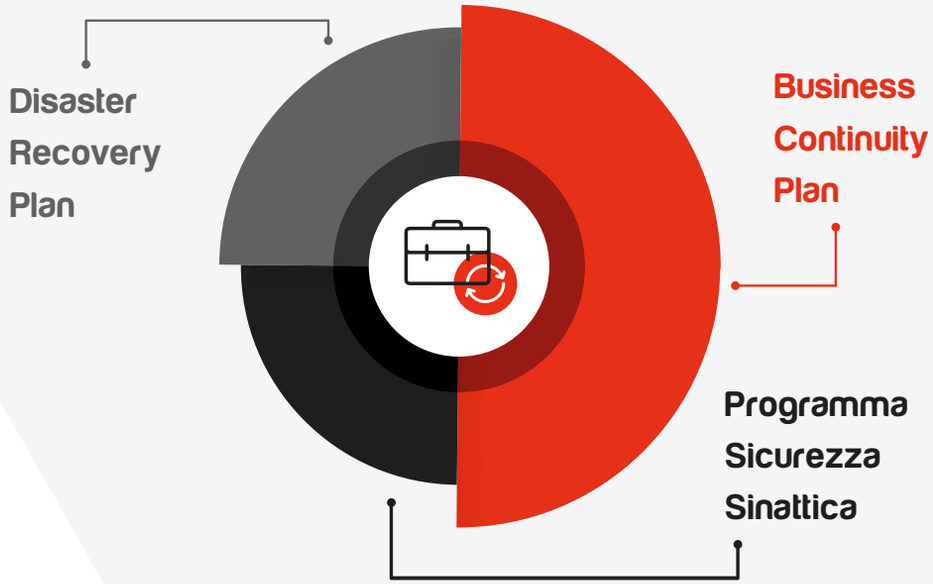
La **strategie di Disaster Recovery** attuabili dipendono strettamente dalle specifiche esigenze dell'azienda. Tra le principali si evidenziano:

Backup in Cloud

Riduce i tempi di fermo mediante il ripristino di una copia di dati precedentemente salvata in un'unità di web storage.

Iperconvergenza

Elimina i tempi di fermo mediante il trasferimento immediato dell'infrastruttura IT su una piattaforma cloud di un provider.



> **Sinattica è partner certificato Achab, azienda leader in soluzioni di Backup, Disaster Recovery e Business Continuity progettate per preservare l'operatività delle imprese in caso di disastri crash di sistema e perdite di dati.**

datto

Rev. Luglio 2022

sinattica
SERVIZI EVOLUTI PER L'AZIENDA

PROGRAMMA SICUREZZA SINATTICA

Per la difesa informatica delle Imprese

Il piano di protezione informatica progettato per mantenere la rete dati delle Imprese al sicuro da rischi e attacchi hacker.

Via Cremona, 10
25025, Manerbio (BS)

Tel. 030 777 8487
pss@sinattica.com

pss.sinattica.com
www.sinattica.com