



WWW.CYBERSECURITYBOX.IT



Soluzioni informatiche per rendere le aziende sicure.

La nostra Mission è garantire sempre soluzioni tecnicamente eccellenti, affidabili e progettate secondo le reali necessità del cliente permettendoci così di esprimere il massimo livello di competitività e di efficienza.

**Sei consapevole
della quantità
di rischi legati
alla sicurezza
a cui sei
sottoposto
ogni
singolo
giorno?**





Indice

IL TARGET

_____ 4

SMART WORKING
VS. SICUREZZA

_____ 6

INTRODUZIONE
ALLA SOLUZIONE

_____ 7

I 6 PUNTI CARDINE

_____ 9

ANALISI E RISULTATI

_____ 10

FAQ E DUBBI

_____ 12

MAI SOTTOVALUTARE
IL PROBLEMA

_____ 15

RIEPILOGO

_____ 16

TESTIMONIANZE

_____ 18

Il Target

Piccole e medie imprese sotto attacco

L'azienda per cui lavori (o di cui ne sei titolare) gestisce ogni giorno elevate quantità di dati con frequenti scambi tra i dipendenti utilizzando differenti luoghi di accesso (pratica in grande aumento data la diffusione dello smart working). A seguito di questa premessa vorremmo porti una domanda: **Sei consapevole della quantità di rischi legati alla sicurezza a cui l'impresa viene sottoposta ogni singolo giorno?**

Sai di quanto sono aumentati i rischi legati alla sicurezza informatica con la diffusione dello smart working? Ad oggi, ben il 64% delle piccole medie imprese italiane si dichiara più esposto a minacce informatiche ed eventi critici legati alla partita dei propri dati rispetto al passato.

Dall'arrivo del COVID, i cyber attacchi contro aziende, studi legali, professionisti ma anche singoli utenti si sono moltiplicati con una frequenza sbalorditiva.

Oggi, in Italia, avviene un attacco informatico ogni 11 secondi.



Violazione dei dati o della sicurezza, attacchi hacker, malfunzionamenti di servizio, errori legati alla scarsa preparazione digitale dei dipendenti...

Questi e molti altri motivi portano oggi gravi conseguenze nelle imprese, andando dalla semplice perdita di tempo causata dall'interruzione dell'attività, fino alla vera e propria perdita di dati molto importanti.

IL VERO PROBLEMA? LA SCARSA PERCEZIONE DEL RISCHIO

Ma tra tutto questo, sai qual è il principale problema che mette rischio la sicurezza di un'azienda?

La scarsa consapevolezza del pericolo. Il pericolo informatico non si vede, non si percepisce. Non ce ne si accorge fino a che non accade, ed è proprio questo il rischio maggiore: sottovalutare il problema.



La scarsa percezione del rischio e la **convizione di possedere già tutto il necessario per proteggersi e di avere tutto sotto controllo** illude ogni giorno le PMI.

Naturalmente, le conseguenze sono molteplici: **rallentamenti del lavoro, mancanza di digitalizzazione** dei processi critici nelle aziende, **furti di identità digitale**, attività quotidiane svolte senza appropriati **supporti analogici** come ad esempio **annotare le credenziali di accesso su un'agenda**, ecc...

Il tuo obiettivo dovrebbe quindi essere quello di implementare nella tua azienda un sistema di **cyber risk management** all'avanguardia ed attuare una **strategia di gestione della sicurezza** informatica efficace.



SMART WORKING VS. SICUREZZA

Si stima che in Italia, durante il lockdown, siano stati circa 554.754 i lavoratori che hanno dovuto lavorare da casa, in smart working.

Nonostante questo abbia portato alcuni **vantaggi e benefici** alle aziende, purtroppo ha generato anche parecchi pericoli legati alla sicurezza. Immagina: tutti i dipendenti hanno iniziato a lavorare da casa, diventando **inconsapevolmente** un punto di accesso ulteriore ai dati aziendali da parte degli hacker.

Lavorare da casa, inoltre, spesso significa utilizzare una **rete wifi poco sicura**, un **pc non adatto** al lavoro svolto, ed un dispositivo maggiormente vulnerabile con **password poco sicure** poiché senza il doppio fattore di autenticazione e con dati non cifrati. **Conseguenza: in poco tempo, gli attacchi di phishing sono quasi triplicati. Per tutti questi motivi, oggi è indispensabile poter avere la certezza di essere al sicuro! Come?**

L'IMPORTANZA DELLA CONOSCENZA

**Le parole chiave sono:
formazione,
conoscenza,
continuità.**

Conoscere e sapere come muoverti ti porterà a ridurre i rischi legati alla sicurezza informatica per la tua azienda, permettendoti di evitare l'utilizzo di dispositivi poco sicuri e digitalizzare tutti i processi maggiormente critici.

Ad esempio, ti sei mai chiesto come si capisce se un'azienda è in pericolo?

Sono **grandissimi i vantaggi** che si ottengono conoscendo le caratteristiche che dovrebbe avere un sistema di gestione della sicurezza, sono altresì **grandissimi i pericoli** che porta con se il non conoscere tali caratteristiche.



I consigli che possiamo darti, sono i seguenti:

Evita di utilizzare dispositivi poco sicuri

Cerca sempre di formare al meglio i tuoi dipendenti riguardo a come comportarsi e cosa evitare

Cerca sempre di digitalizzare i processi critici

Introduzione

ALLA SOLUZIONE

Perché la tua soluzione è unica?

Dopo aver parlato a lungo dei rischi informatici corsi oggi da ogni azienda e dell'importanza di non sottovalutarli, è giunto il momento di parlare della soluzione a questi problemi.

Informatica95 può fornirti questa soluzione, ma prima di parlarne vorremmo spendere due parole per spiegarti perché dovresti affidarti a noi per proteggere la tua impresa.



Perché Informatica95 è diversa dalle altre aziende?

La lunga esperienza ottenuta dal 1995 ad oggi, l'assistenza garantita 24 ore al giorno 7 giorni su 7, le relazioni stabili con fornitori nazionali ed internazionali, la consulenza e la realizzazione di soluzioni personalizzate, il backup costante dei servizi e la possibilità di interagire con un interlocutore a te dedicato **sono soltanto alcuni dei vantaggi che Informatica95 può offrirti.**



Il principale motivo per cui abbiamo successo nel proteggere i dati sono esattamente le caratteristiche indispensabili a cui abbiamo fatto cenno poco fa: continuità e formazione.

La maggior parte delle aziende operanti in questo settore infatti, quanto ti forniscono connettività e sicurezza si **limitano ad installarti i sistemi necessari per farlo**, ed il tutto finisce lì. In Informatica95 invece, siamo da sempre convinti che **informare e formare il cliente** riguardo a cosa gli stai proponendo **per salvaguardare la sua sicurezza sia il primissimo passo da compiere** per riuscire al meglio in questo intento.

IL PUNTO DI PARTENZA: ANALISI INTERNA

Nel momento in cui deciderai di affidare la tua sicurezza nelle nostre mani, il primo passo da compiere per avvicinarsi alla soluzione sarà effettuare un'attenta ed accurata analisi del tuo sistema attuale, volta a comprenderne punti deboli e fragilità. **Ricorda: chiunque voglia venderti connettività e sicurezza senza partire da un'analisi del tuo sistema, non sta svolgendo un buon lavoro.**



Com'è possibile comprendere quale sia la soluzione più adatta a ciascuno senza prima analizzare la sua situazione attuale?

Un'altra grande differenza tra noi e la maggior parte delle aziende del settore sta nel modo in cui svolgiamo questa analisi: **DALL'INTERNO!**

Devi sapere infatti che quasi tutti gli operatori, nel momento in cui ti forniscono connettività e sicurezza, lo fanno dotandoti di un firewall che ti protegge dall'esterno.

Conseguenze? Fatica, dispersione di energia e perdita di tempo. È proprio questo il motivo per cui noi cerchiamo di proteggere e valutare ogni debolezza sempre agendo dall'interno.

Ciò che realmente ci differenzia dai nostri competitor durante l'analisi di un sistema quindi è proprio questo: grazie al nostro metodo, siamo in grado di comprendere aspetti che la maggior parte delle volte non vengono notati, e ci riusciamo proprio agendo dall'interno invece che dall'esterno. Non solo: in questo modo riusciamo a farlo in maniera più rapida ed efficace.

Obiettivo: comprendere la base delle vulnerabilità e fragilità di quel sistema. Da dove è arrivato il problema? Cosa lo ha causato? Cosa comporta al cliente?

Cyber Security Box

ECCO I 6 PUNTI CARDINE



Installazione Plug&Play

Installazione semplificata. Il BOX arriva già configurato. Collega alimentazione e cavo di rete, al resto pensiamo noi.



Fino a 254 Host Scansionati

Non devi scegliere quali dispositivi analizzare. Cyber Security Box scansiona l'intera rete, silenziosamente e senza impatto sulle prestazioni dei sistemi.



21 Giorni di Analisi Continua

Non tutti i dispositivi sono accesi tutti i giorni, per questo facciamo un'analisi ripetuta nell'arco di tre settimane. Vogliamo essere sicuri di intercettare tutte le vulnerabilità possibili.



Report Dettagliato

Elenco dei dispositivi scansionati, elenco delle vulnerabilità, elenco delle correzioni. Non manca nulla nel nostro report. Avrai così visibilità completa della sicurezza informatica nella tua azienda.



1 ora di Consulenza Inclusa

Facciamo del nostro meglio per rendere il report il più semplice possibile. Se alcune cose non sono chiare non preoccuparti, abbiamo pensato anche a questo. Un tecnico specializzato sarà a tua disposizione per spiegartelo al meglio.



Espansione Futura

L'analisi di vulnerabilità è solo un primo passo. Attraverso Cyber Security Box potrai aumentare la sicurezza della tua azienda nel tempo. Questo grazie ad uno sviluppo continuo e focalizzato a contrastare le future minacce informatiche.

Analisi e Risultati

Abbiamo finalmente compreso quanto sia importante svolgere l'analisi di un sistema per poter intervenire annullandone i punti deboli e le vulnerabilità. **Ma quali sono effettivamente i risultati che sarà possibile ottenere grazie a tutto questo?**

Importanza dell'Analisi

Innanzitutto, dopo aver completato l'analisi potremo finalmente **attribuire un livello di rischio al tuo sistema**. In secondo luogo, potremo finalmente conoscere e studiare la tua specifica situazione riuscendo così a proporre **una soluzione mirata e personalizzata** per proteggere la tua azienda dagli attacchi informatici.



RISCHIO BASSO

Un rischio viene dichiarato basso quando **esistono delle vulnerabilità che non sono sfruttabili o che richiedono passaggi aggiuntivi, come il social engineering**.

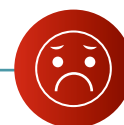
In questo caso, si consiglia comunque di predisporre un piano di azione ed aggiornamento dopo che i problemi ad alta priorità sono stati risolti.



RISCHIO MEDIO

Lo sfruttamento di questa vulnerabilità è più difficile ma, se riuscito, potrebbe causare una **potenziale perdita di dati o lunghi tempi di inattività**.

In caso di rischio medio quindi, si consiglia di strutturare un **piano d'azione ed aggiornamento** il più presto possibile.



RISCHIO ALTO

Lo sfruttamento di questo tipo di vulnerabilità è semplice e di solito comporta la **compromissione totale del sistema coinvolto**.

In caso di rischio alto quindi, si consiglia di strutturare immediatamente un piano d'azione e di correzione dei sistemi vulnerabili.



RISULTATI OTTENUTI

Dopo aver concluso l'analisi ed aver steso così un piano di azione ideato apposta per le tue necessità, potrai finalmente godere di numerosi vantaggi:



Business continuity più alta ed efficace grazie a data center all'avanguardia.



Processi più fluidi grazie alla presenza di un personale costantemente formato ed aggiornato direttamente da noi.



Assistenza personalizzata e dedicata a te che può arrivare anche a 24 ore al giorno, 7 giorni su 7.



Continuità e formazione costante del tuo personale riguardo agli aspetti informatici legati alla protezione dei tuoi dati.



Sicurezza certa nello scambio di dati tra differenti sedi, fornitori, clienti e dipendenti, anche in smartworking

Questi sono solamente alcuni dei vantaggi che possiamo garantirti qualora decidessi di affidare la sicurezza del tuo sistema a Informatica95!



FAQ e dubbi

LE RISPOSTE AI TUOI DUBBI

Ecco qui la lista delle domande più frequenti che riceviamo. Se ne hai altre saremo lieti di risponderti al telefono o per email.

Il BOX crea problemi di connettività una volta installato sulla rete?

Assolutamente no, il sistema si comporta come un normalissimo dispositivo che si collega in Internet. L'unico traffico che genera verso la connettività è quello di aprire un collegamento sicuro e cifrato verso i nostri datacenter di Torino ed Umbertide finalizzato alla telegestione.

Potrei avere disservizi utilizzando questo BOX?

No, il sistema non abilita nessun servizio di rete e si comporta come un client che chiede l'autoconfigurazione da parte dei sistemi esistenti. Anzi, ricevere i parametri della rete è una prerogativa, in quanto il prodotto non fa nessun servizio interno alla rete.

Il BOX può spiare o acquisire dati sensibili aziendali, amministrativi o altro?

No, il box ha il solo scopo di collegare la rete privata alle sonde di scansione nei nostri datacenter senza installare nessuna intelligenza di analisi nel box stesso. Le analisi da parte delle sonde sono solo in relazione alle vulnerabilità di sistema, non si richiedono credenziali di accesso per poter analizzare, ci si comporta come un qualsiasi dispositivo di rete collegato (es. una stampante, uno scanner, un orologio marcatempo, una telecamera etc...)

Il BOX può accedere a comunicazioni private su dispositivi? (e-mail / chat ecc.)

No, il box senza avere le credenziali di accesso dei dispositivi non può accedere ad alcun dato.

Quanto tempo dovrà rimanere il BOX in azienda e dopo quando potrà dare risposte?

Saranno necessarie all'incirca 3 settimane per analizzare e produrre il report.

Il BOX può accedere in qualunque modo nella privacy delle persone in azienda?

No, il box analizza solo ed esclusivamente gli indirizzi ip della classe di rete di appartenenza alla ricerca di vulnerabilità.

Tutti i macchinari o altri dispositivi in azienda possono essere bloccati dall'utilizzo di questo prodotto?

No, il box analizza le vulnerabilità e non tenta in alcun modo di fare test di penetrazione dei sistemi.

Per quanto tempo è valida l'analisi prodotta dal BOX?

L'analisi è valida solo per il momento in cui è stata fatta.

È possibile avere un monitoraggio continuo?

Sì, è sufficiente fare un abbonamento e scegliere una frequenza tra bimestrale, trimestrale, quadrimestrale, semestrale ed annuale.

Può il BOX produrre nel tempo la richiesta di soluzioni più avanzate?

Sì, oltre all'analisi di vulnerabilità è possibile attivare dei monitoraggi dei sistemi con la possibilità di gestire delle notifiche in caso di errore, come per esempio sapere se una telecamera non è più raggiungibile e ricevere un alert via email che avvisa il cliente riguardo a questo .

Può il BOX rallentare i flussi di lavoro? Ad esempio avere minore banda, download più lenti, operazioni più complesse?

No, perché in condizione di inattività non interagisce con internet se non tenendo una sessione aperta di pochi kbs per la telegestione. In condizioni di attività si procede con una scansione che non occupa mai più di 256Kbs al secondo, velocità gestibile da qualsiasi connessione internet senza creare disservizi interni.

Il BOX analizza la rete LAN o anche Wi-Fi / Altro?

Il box può analizzare qualsiasi dispositivo di rete dotato di un indirizzo della sua stessa rete.

Può il BOX analizzare dispositivi collegati via bluetooth?

No, non può farlo.

Può in qualche modo questo dispositivo cambiare le impostazioni o settaggi vari in azienda?

No, può solo eseguire la lettura degli stati della rete e le sue eventuali vulnerabilità.

Il BOX ha accesso a documenti nel cloud, HD, client di posta ecc?

No, il box analizza solo le vulnerabilità che sono oggetto di attacco da parte di hacker e non accede ai sistemi.

Perché il BOX dovrebbe garantire maggiore sicurezza rispetto ad altri sistemi o a non averlo?

Gli altri sistemi solitamente eseguono la scansione da esterno e non riescono a simulare scansioni interne. Le aziende concorrenti spesso forniscono un software da installare in sistemi interni attraverso il quale poi eseguono la scansione, non potendo confinare realmente il sistema di analisi dal sistema messo a disposizione dall'azienda per installare il software.

Con la cifra richiesta in installazione del BOX io in effetti cosa pago o acquisto?

Si paga la professionalità di sistemisti che analizzano e categorizzano le vulnerabilità dei sistemi, prima che queste possano essere sfruttate da malintenzionati. Si avrà quindi l'analisi di vulnerabilità su cui poi i vari fornitori potranno intervenire.

Cosa succede poi a seguito dell'analisi che il BOX farebbe alla mia azienda?

Verrà fornito un report su cui si evidenzieranno le criticità rilevate, facendole collimare ai rischi per l'azienda e producendo l'elenco delle soluzioni necessarie a risolvere il problema.

Cosa succede

SE ACQUISTI PRODOTTI SENZA AVER EFFETTUATO PRIMA L'ANALISI DELLE VULNERABILITÀ?

Mai sottovalutare il problema!

Come abbiamo già visto in precedenza, il problema principale che porta le aziende ad essere sottoposte a rischi informatici è quasi sempre la scarsa consapevolezza del pericolo. Sottovalutare il problema è molto più semplice e comune di quanto tu possa pensare. Ricorda che il pericolo informatico non è un qualcosa che si può percepire mentre arriva: ce ne si accorge solamente quando è ormai in atto. Come fare quindi per risolvere questo problema?

01.

Innanzitutto, è fondamentale mettere al corrente il proprio personale riguardo a questi argomenti, ed è proprio per questo che noi, insieme al nostro prodotto, offriamo formazione ai nostri clienti.

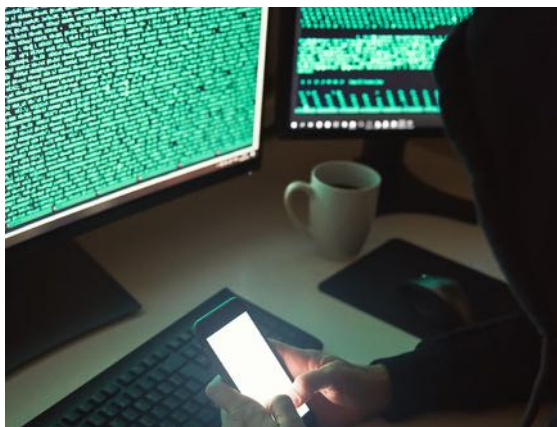
02.

In secondo luogo è poi importante svolgere una manutenzione periodica e regolare dei sistemi informatici, ed è proprio per questo che noi, insieme al nostro prodotto, offriamo continuità ai nostri clienti.

Cosa succede se acquisti prodotti senza aver prima fatto l'analisi?

La mancanza dell'analisi di vulnerabilità è uno **svantaggio molto grosso** per le imprese che vogliono mettere in sicurezza i propri dati. Il motivo è molto semplice: ogni azienda presenta dei punti deboli. Si tratta di quelle **fragilità che gli hacker sfruttano** per potersi infiltrare in un sistema, e per questo è importantissimo conoscerle per poter porre un rimedio.

Questi punti deboli però cambiano e sono differenti per ogni impresa!



Ed è proprio questo il motivo per cui è praticamente impossibile risolvere il problema senza prima effettuare un'analisi accurata di ogni singolo sistema. **Grazie all'analisi effettuata con il Cyber Security Box invece, potrai finalmente acquistare un prodotto in maniera consapevole e sicuro che sia quello giusto per risolvere il tuo problema!** Per farti un piccolo esempio, immagina di stare male ed andare da un medico che ti prescrive delle medicine da prendere senza però che prima ti sia stata effettuata una visita.

Cosa succede? Naturalmente, tu continui a prendere medicine a caso ma non sai quale sia la vera origine del male, quindi sarà difficile guarire.

Con i sistemi informatici accade la stessa identica cosa: **per mettere in sicurezza un'impresa è fondamentale comprenderne le vulnerabilità prima**, e questo può essere fatto solamente tramite analisi.

Riepilogo

Metti al sicuro la tua Azienda

Avrai ormai capito quanto sia importante essere certi che la propria azienda sia protetta da qualsiasi eventuale attacco. Scegliere i sistemi di sicurezza offerti da Informatica95 significa scegliere un prodotto

veloce, sicuro e realizzato su misura per tutte le vostre esigenze!



Ricorda sempre una cosa importante: oggi non puoi nemmeno immaginare di fare a meno di connettività e dispositivi informatici adeguati se vuoi stare al passo con i tempi.



Conosciamo meglio il prodotto



Oggi ogni sistema è smart e connesso alla rete, conoscere le eventuali vulnerabilità è assolutamente indispensabile.

Se queste non vengono identificate in tempo qualche malintenzionato potrebbe sfruttarle per crearti un danno irrimediabile.





Come è fatto?

Il nostro Box di sicurezza ha delle dimensioni di circa 10x6x2cm con attacchi di rete e della corrente.



A cosa serve?

Il prodotto serve per veicolare l'analisi effettuata dai nostri datacenter verso la rete del cliente in totale sicurezza.



Come funziona?

Il Box deve semplicemente essere collegato alla rete tramite i cavi di rete e della corrente forniti da noi.

Il dispositivo si collegherà al nostro datacenter, ed attraverso di lui i nostri sistemi effettueranno le scansioni di vulnerabilità.

Una volta conclusa l'analisi, il report ti verrà consegnato di persona o illustrato in videoconferenza.



I benefici del prodotto

- ♥ Ricezione dell'elenco completo dei dispositivi rilevabili presenti nella rete
- ♥ Presa di coscienza riguardo a quali di questi dispositivi presentano criticità
- ♥ Spiegazione di quale soluzione adottare per risolvere le vulnerabilità individuate
- ♥ Una volta messe in atto le soluzioni, il livello di sicurezza aziendale potrà crescere esponenzialmente
- ♥ Possibilità di accesso a molte altre soluzioni e prodotti forniti da noi in totale sicurezza attraverso lo stesso hardware utilizzato per l'analisi

Se hai ancora dei dubbi

sul nostro prodotto, inquadra questo QR Code e visita il sito www.cybersecuritybox.it per ottenere maggiori informazioni.



Testimonianze

DICONO DI NOI..

Autocentri Giustozzi srl



"È ormai da ben 8 anni che collaboriamo con Informatica95 e devo dire che ci siamo trovati decisamente bene fin da subito.

Sono tutti molto disponibili ed il tecnico che ci assiste personalmente, Federico Grilli, si dimostra sempre capace, tempestivo nelle risoluzioni ed efficiente in tutti gli ambiti, seppur diversi tra loro, per i quali ci presta assistenza.

La consulenza di Informatica95 mi supporta sempre molto, specialmente per quanto riguarda la risoluzione dei problemi che si presentano riguardo alla parte IT. Inoltre, il nostro tecnico ci supporta in ogni singolo aspetto, e questo fa sì che io non sia costretto ad interfacciarmi con persone diverse a seconda del problema che devo risolvere."

RD Amministrazioni srl



"Collaboro con Informatica 95 da un paio d'anni e mi trovo molto bene. Sono molto bravi e preparati a supportare i propri clienti, specialmente per quanto riguarda la sicurezza dei sistemi.

Ciò che mi soddisfa maggiormente di questa collaborazione sono la disponibilità, la prontezza e l'estrema capacità di risolvere qualsiasi problema."

Alfa Spa



"Collaboriamo con Informatica95 da circa 10 anni, e ci troviamo molto bene coi loro tecnici.

La consulenza informatica mi supporta parecchio, e l'assistenza è fatta sempre da personale competente"

GruppoEIL ELETTROMECCANICA – LOGITEC SRL



"Collaboro con il Team di Informatica95 da ormai ben 15 anni e mi trovo molto bene con tutti i tecnici. Sono sempre molto disponibili, in caso di urgenza anche fuori dall'orario di lavoro.

Mi sono sempre sentito molto supportato nella gestione dei problemi più importanti, per questo la gestione dei nostri server e della rete è completamente affidata a loro.

Il rapporto che si è instaurato in questi anni con i tecnici di Informatica95 è molto informale e diretto. Infine, propongo sempre soluzioni tecniche molto professionali."

Marco Ceresara



"Collaboro con il Team di Informatica95 da circa 3 anni e mi trovo benissimo. Sono molto puntuali e competenti, in grado di supportarti riguardo ad ogni problematica inerente l'informatica.

Ma il vero aspetto per cui mi trovo così bene con quest'azienda è che, pur trattando argomenti complessi, riescono sempre a farmi comprendere ciò che devo fare in modo molto semplice."

Moretti Ottaviano

DITTA INDIVIDUALE



"Collaboriamo con il team Informatica95 da oltre 10 anni. Sono molto professionali e mi sono sempre trovato molto bene.

Un aspetto grazie al quale mi sono sempre sentito molto supportato è la loro velocità nella comprensione del problema con relativa risoluzione. Tutto il team è molto competente."

TI-EMME



"Collaboro con Informatica95 da 24 anni e mi sono sempre trovato bene con i loro tecnici, sempre disponibili e molto professionali.

Mi supportano specialmente in ciò che riguarda il networking e si vede che hanno grande conoscenza in materia."

Giuliano Tartufi Spa



"Collaboro con Informatica95 da 3 anni e mi trovo molto bene.

Sono molto competenti nel fornire assistenza ai loro clienti, dando sempre risposte pronte ed efficienti.

Sono molto soddisfatto della garanzia del loro servizio."



Contattaci

Per avere maggiori informazioni e
procedere all'analisi della tua Azienda
non esitare a contattarci!

Per ulteriori informazioni:
E-mail: info@informatica95.net
Tel: +39 075 941 7850

WWW.CYBERSECURITYBOX.IT
WWW.INFORMATICA95.NET