IT•NEWS

N. 18 MAR./APR. 2024

L'indispensabile road-book

per rendere sempre più digitale e competitiva la tua impresa

IN QUESTO NUMERO

L'EDITORIALE

A cura di **Alessio Angioli**

Piano Transizione 5.0:

continuano le agevolazioni per le imprese

Pubblicato in Gazzetta Ufficiale il decreto che dà il via al credito d'imposta alle imprese che aderiscono al piano Transizione 5.0, l'insieme delle agevolazioni volte a favorire l'efficientamento energetico e la digitalizzazione delle aziende.

Cos'è la Transizione 5.0?

La Transizione 5.0 è un piano di incentivi per la digitalizzazione e la sostenibilità delle imprese italiane. È stato approvato dal Consiglio dei Ministri il 31 gennaio 2024 e si inserisce nel quadro del PNRR, il Piano Nazionale di Ripresa e Resilienza. Si tratta dell'evoluzione dei precedenti decreti nominati Industria 4.0, Impresa 4.0 e Transizione 4.0.

Quali sono gli obiettivi della Transizione 5.0?

- Incrementare l'efficienza energetica e promuovere l'adozione dell'autoproduzione di energia rinnovabile, con l'obiettivo di conseguire un risparmio cumulativo di 0,4 Mtep (tonnellate equivalenti di petrolio) nei consumi energetici nel periodo 2024-2026
- Sostenere la digitalizzazione delle imprese, attraverso l'adozione di tecnologie innovative, come la robotica avanzata, l'intelligenza artificiale, l'Internet of Things, la stampa 3D e il cloud computing
- Promuovere la competitività delle imprese italiane sui mercati internazionali.

Chi sono i beneficiari della Transizione 5.0?

I beneficiari della Transizione 5.0 sono le imprese di qualsiasi dimensione, incluse le micro, piccole e medie imprese (MPMI)

Quali sono le tipologie di investimenti agevolabili dalla Transizione 5.0?

- Beni strumentali nuovi che consentano di migliorare l'efficienza energetica dei processi produttivi riducendo il consumo di energia e i costi operativi
- Tecnologie innovative, come la robotica avanzata, l'intelligenza artificiale, l'Internet of Things, la stampa 3D e il cloud computing
- Soluzioni innovative per la produzione e l'utilizzo di energia da fonti rinnovabili.

Qual è l'incentivo e l'aliquota del credito previsto dalla Transizione 5.0?

In totale, i fondi sono 6,3 miliardi di euro di cui 3,78 miliardi per i beni strumentali e 630 milioni per la formazione. Le imprese potranno beneficiare di progetti che includono l'innovazione digitale per risorse di 4,4 miliardi di euro per i prossimi due anni.

L'incentivo previsto dalla transizione 5.0 è un credito d'imposta, che può essere utilizzato in compensazione con le imposte a debito o in forma di sconto sul corrispettivo dovuto al fornitore dei beni strumentali.

Il credito d'imposta è articolato in fasce:

35%

è destinato agli investimenti fino a 2,5 milioni di euro

15%

si applica agli investimenti superiori a 2,5 milioni di euro e fino a 10 milioni di euro

5%

è riservato agli investimenti superiori a 10 milioni di euro fino al limite massimo di 50 milioni

Può raggiungere percentuali più elevate, arrivando fino al 40% e 45% della spesa, se dimostrato che l'investimento consente di ridurre i consumi energetici oltre al 6% e 10%.

Perché approfittarne del bonus Transizione 5.0 ?

Il futuro delle aziende è digitale e il decreto si propone di guidare le imprese italiane verso una nuova era di digitalizzazione, ma anche di sostenibilità ambientale.

L'I-TEAM è pronto ad offrirti soluzioni personalizzate per ogni tua esigenza di innovazione digitale e sicurezza

A cura di
Marco Melucci

HIJACKING DELLE eSIM: la nuova minaccia per la sicurezza dei conti bancari

Una delle ultime truffe digitali che si sta diffondendo in tutto il mondo è l'Hijacking: si tratta di una tecnica che sfrutta le SIM telefoniche virtuali, le eSIM, il cui utilizzo può mettere a rischio gli accessi gestiti da verifica telefonica della vittima, come quelli bancari.

Come avviene la truffa?

Gli hacker "dirottatori" sfruttano la funzione di sostituzione o ripristino della scheda SIM digitale e trasferiscono il numero di telefono della vittima sul proprio dispositivo, dotato di eSIM; in questo modo, l'accesso all'account della vittima presso l'operatore di telecomunicazioni o servizi governativi viene controllato dagli hacker.

Una volta che gli aggressori hanno ottenuto il controllo del numero di telefono della vittima, **possono inserirsi non solo nei conti bancari online**, ma anche negli account di messaggistica. Questo apre la porta a una serie di potenziali attacchi, tra cui **richieste di denaro fraudolente** o ricatti, sfruttando i contenuti multimediali presenti nella corrispondenza della vittima e l'utilizzo di strumenti di intelligenza artificiale.

Questa tecnica è piuttosto recente, ma si teme sia in grande espansione e possa diventare una minaccia globale.

Come proteggersi

Le best practice consigliate dagli esperti di cyber security sono rigorose:

- usare password complesse e uniche per ogni servizio
- attivare l'autenticazione a due fattori (2FA)
- monitorare i messaggi SMS relativi al blocco o al trasferimento della carta SIM
- aggiornare regolarmente i software dei dispositivi mobili con le ultime versioni firmware e patch
- evitare connessioni wi-fi pubbliche non sicure
- evitare link e allegati sospetti

Le organizzazioni finanziarie sono in prima linea

Il problema, ovviamente, interessa anche gli istituti finanziari, che devono essere pronti nell'affrontare questo tipo di minaccia. Per questo motivo gli istituti bancari stanno adottando **strumenti avanzati di antifrode** capaci di **rilevare comportamenti anomali e di attivare protocolli di risposta tempestiva** per proteggere i conti bancari dei clienti.

Il consiglio di I-TEAM è di seguire attentamente le Best Practice indicate, dato che il panorama digitale sta diventando sempre più ostile: è fondamentale monitorare i propri account e adottare misure proattive per difendere la propria sicurezza online, grazie anche e soprattutto alla conoscenza dei metodi criminali.

A cura di
Marco Cecchi

CYBER SECURITY:
quando e come il cloud computing fa la differenza

Con l'aumento dei rischi associati alla gestione dei dati sensibili, le aziende stanno cercando soluzioni innovative per proteggere le loro informazioni critiche. L'affermarsi del cloud computing ha cambiato completamente il paradigma della cyber security: ecco le caratteristiche principali:

Flessibilità e scalabilità

I volumi dei dati da trattare sono in continua crescita in ogni settore. Il cloud computing permette di adattarsi rapidamente alle esigenze di sicurezza in evoluzione, consentendo l'espansione o la riduzione delle risorse informatiche in base alle necessità. Ciò significa che le aziende possono implementare misure di sicurezza in modo più rapido ed efficiente rispetto alle soluzioni tradizionali.

Protezione evoluta e sempre aggiornata

I dati sono uno dei beni più preziosi per le imprese. Proteggere i propri dati è essenziale per garantire la continuità operativa e mantenere la fiducia dei clienti. Le piattaforme di cloud computing sono dotate di strumenti di crittografia, autenticazione multifattoriale e controlli di accesso granulari, che aumentano significativamente la protezione dei dati. Inoltre, i provider di servizi cloud investono continuamente in tecnologie innovative per proteggere i dati dei loro clienti.

Monitoraggio continuo e risposta agli incidenti

La tempestività è fondamentale per affrontare gli incidenti di cyber sicurezza. Il cloud computing fornisce funzionalità avanzate di monitoraggio e risposta agli incidenti, con strumenti automatizzati che rilevano e mitigano le minacce in tempo reale.

Disaster Recovery e Business Continuity

Le aziende dovranno affrontare sempre più frequentemente una varietà di minacce che potrebbero interrompere le loro operazioni. Il cloud computing offre soluzioni affidabili di disaster recovery e business continuity, creando in cloud duplicati dei dati e delle applicazioni necessarie, garantendo, in caso di incidente o interruzione, il pieno e immediato ripristino delle operazioni. Inoltre, il cloud computing offre la flessibilità di scegliere la posizione geografica dei dati, consentendo alle aziende di rispettare le normative sulla privacy e la conformità.

Collaborazione e condivisione sicura dei dati

I team di lavoro posizionati in diverse sedi geografiche, anche non stabilmente, con il cloud computing possono collaborare a tutte le operazioni aziendali. Il cloud computing facilita la condivisione sicura dei dati tra i membri autorizzati, consentendo di lavorare in piena sicurezza. Attraverso l'uso di strumenti di crittografia e di autorizzazioni di accesso, le imprese possono garantire la massima protezione dei dati sensibili.

Il cloud computing continuerà a evolversi e offrire ancora più funzionalità avanzate per imprese di ogni dimensione, proteggendole al tempo stesso dagli attacchi informatici. Tuttavia, è importante sottolineare che la sicurezza dipende anche dall'adozione di buone pratiche da parte delle persone, dato che il "fattore umano" è una delle cause principali di rischio.

I-TEAM offre soluzioni evolute per la protezione dei dati, di risposta agli incidenti, di continuità operativa e di condivisione sicura delle informazioni, per costruire insieme la migliore strategia di sicurezza informatica per la tua impresa.

A cura di
Paolo Vannini

Il tuo sito WordPress è stato hackerato? È possibile ripristinarlo!

WordPress, essendo probabilmente il CMS più utilizzato nel mondo, è soggetto a numerosi attacchi hacker.

Quando il proprio sito viene violato e infettato da malware, è normale andare nel panico, soprattutto se non si è del mestiere, ma non ci si deve preoccupare troppo. Esistono procedure per ripristinare il proprio sito.

A INDIVIDUARE LE RED FLAG: capire il problema dai segnali

1) Se noti reindirizzamenti sospetti verso altre pagine, oppure se ricevi avvisi sul tuo browser su possibili violazioni, prendili sul serio.
Forse il tuo sito WordPress è stato hackerato.

2) Se, ad un certo punto non riesci a loggarti - a meno che tu non abbia digitato la password sbagliata – molto probabilmente sei stato hackerato.

3) Supera la fase del panico e mantieni la calma; chiama il tuo consulente esperto in sicurezza e gestione di WordPress. Una soluzione è spesso possibile.

B NON ALZARE BANDIERA BIANCA: cosa farà l'esperto

1) Come prima operazione metterà offline il sito; in questo modo gli hacker non avranno l'opportunità di accedere.

2) Verificare i backup del sito e dei contenuti. Se il backup è stato eseguito regolarmente, ripristinare la versione precedente prima dell'incidente; non è difficile e spesso non si perde alcun dato.

3) Identificare le modalità di hackeraggio. Potrebbe essere dipeso da un plugin, una configurazione errata o una vulnerabilità del tema. Capire cosa e come è accaduto l'incidente è utile per fare in modo che non succeda di nuovo.

4) Una volta individuata la causa della violazione, a volte difficile, c'è spesso la possibilità di rimuovere i file compromessi.

5) Testare il sito ripulito; nelle operazioni di ripristino, a volte, può saltare qualche codice; fare ulteriori test è sempre utile per verificare il corretto funzionamento del sito.

C SVENTOLARE BANDIERA VERDE: risolvere i problemi con I-Team

1) Ripulire WordPress e risolvere i problemi. I-TEAM utilizza software come ISPProtect, PHP antivirus Wordfence, All In One Security e li utilizza in contemporanea per garantire la cattura di tutti i file compromessi. Esistono molti software e tutti hanno punti di forza e punti deboli, dato che i tool per WordPress sono infiniti; per questo, ne utilizziamo diversi: proprio per non far scappare niente.

2) Provvedere alla prevenzione. I-TEAM ti aiuta ad aggiornare regolarmente i plugin e il tema, ad utilizzare password complesse e ti consigliamo come restare ad occhi aperti in caso di movimenti strani sul proprio sito.

Gli hackeraggi WordPress sono interventi all'ordine del giorno e i nostri esperti hanno appreso, nel corso degli anni, una specifica esperienza: sappiamo gestire e risolvere diverse problematiche e siamo in grado di rimettere in piedi il vostro sito con una certa celerità. Naturalmente, sappiamo anche aiutarvi a proteggevi preventivamente.

AVETE QUALCHE DUBBIO? DIFFICOLTÀ? VOGLIA DI SICUREZZA?
Scrivete a info@i-team.tech

I·TEAM

Cinque società che si sono unite per dare forma a un grande progetto:
aiutare le imprese a crescere nella digitalizzazione
e nella rivoluzione digitale, per avere performance
sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti
dell'economia e della società contemporanea.

Allyou.srl

ego communication

GlobalNet
Servizi di Telecomunicazioni per la tua Azienda

OMEGA SISTEMI
Soluzioni Informatiche Professionali

NETWORK PRIVACY

PANTAREI INFORMATICA
La tecnologia resa semplice

WWW.I-TEAM.TECH

Via Benedetto Dei 64 · 50127 FIRENZE · Numero Verde 800-199760 · info@i-team.tech