IT•NEWS

N. 19 MAG./GIU. 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**

Direttiva NIS2: cybersicurezza a livello comunitario

La Direttiva NIS2 (Network and Information System Security), approvata dal Parlamento dell'Unione Europea, introduce nuove norme per le aziende che forniscono servizi essenziali o critici per la società.

La scadenza per mettersi in regola è il 18 ottobre 2024 e non manca molto. Cosa cambia rispetto alla Direttiva NIS originale e quali sono i requisiti minimi di sicurezza dei dati, reti e sistemi?

Cosa prevede la Direttiva NIS2

La Direttiva NIS2 rappresenta il primo tentativo di rafforzare il livello globale di "cyber sicurezza" tra i 27 Stati membri dell'Unione Europea. Si concentra principalmente sugli **Operatori dei Servizi Essenziali** (OSE), ovvero aziende che forniscono servizi essenziali la cui interruzione avrebbe un impatto significativo sull'economia o sulla società.

La Direttiva NIS2 stabilisce una norma comune di difesa contro le minacce informatiche all'interno dell'UE.

A chi è rivolta la Direttiva NIS2?

La **Direttiva NIS2** si applica a **organizzazioni pubbliche e private** che gestiscono **servizi essenziali per la società**, ad esempio:

- società di produzione e distribuzione energia
- servizi sanitari
- trasporti
- infrastrutture di comunicazione elettronica
- servizi bancari e finanziari.

Inoltre, coinvolge anche i **fornitori di servizi digitali** che includono le piattaforme online di:

- e-commerce
- motori di ricerca
- cloud computing
- gestione dei servizi ICT e della pubblica amministrazione

Le principali novità della Direttiva NIS2

1. **Ampliamento delle responsabilità:** la NIS2 impone maggiori responsabilità alle aziende che forniscono servizi essenziali o critici. Questi soggetti devono adottare misure adeguate per proteggere i loro sistemi e reti da minacce informatiche.
2. **Requisiti minimi:** la NIS2 definisce norme minime comuni per la sicurezza dei dati, delle reti e dei sistemi. Questi requisiti includono la notifica di incidenti di sicurezza, la gestione dei rischi e la collaborazione tra gli Stati membri.

Quali sono gli obblighi per le diverse categorie di soggetti coinvolti?

1. **Operatori dei Servizi Essenziali (OSE):**
   - Identificazione e notifica degli incidenti: devono identificare e notificare gli incidenti di sicurezza informatica alle autorità competenti.
   - Adozione di misure di sicurezza: devono implementare misure adeguate per proteggere i loro sistemi e reti da minacce informatiche.
   - Collaborazione con gli Stati membri: devono collaborare con gli Stati membri e con altri OSE per affrontare le minacce informatiche.
2. **Fornitori di servizi digitali (DSP):**
   - Gestione dei rischi: devono valutare e gestire i rischi per la sicurezza dei loro servizi digitali.
   - Notifica degli incidenti: devono notificare gli incidenti di sicurezza alle autorità competenti.
   - Adozione di misure di sicurezza: devono implementare misure di sicurezza adeguate per proteggere i loro servizi digitali.

Le sanzioni in caso di mancato adeguamento

Gli **operatori essenziali** potranno essere sottoposti a sanzioni pari a un massimo di **10 mln** di euro o il **2% del totale del fatturato** mondiale globale.

Gli **operatori importanti**, invece, potranno essere soggetti a sanzioni pari a un massimo di **7 mln** di euro o a fino ad un massimo del **1,4 % del totale del fatturato** mondiale globale.

Sarà obbligatorio per tutte le organizzazioni pubblicare sui propri canali la violazione subita.

Abbiamo tempo fino al 18 ottobre 2024!

A cura di
Marco Cecchi

METTIAMOCI AVANTI CON LE FERIE!

8 consigli per migliorare la sicurezza informatica

Le ferie sono un momento di meritato riposo per i dipendenti, ma non dovrebbero essere un periodo di pausa per la sicurezza informatica.

Durante questo periodo, infatti, le imprese possono persino essere più vulnerabili agli attacchi hacker, poiché i criminali informatici approfittano della ridotta sorveglianza e delle pratiche di sicurezza meno rigorose.

È essenziale che le imprese adottino misure preventive per garantire la protezione dei propri dati e delle reti informatiche anche durante il periodo di chiusura estiva.

Ecco alcuni consigli per andare in ferie senza più dover pensare alla cybersicurezza!

Aggiornamenti di sicurezza e patch 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.

Backup dei dati Prima di partire, esegui un backup completo di tutti i dati critici dell'azienda. Assicurati che i backup siano completi, aggiornati e archiviati in un luogo sicuro. In caso di incidente o attacco, i backup sono essenziali per ripristinare rapidamente i dati e ridurre l'impatto sulle operazioni aziendali. Naturalmente, a meno che non abbiate attivato un backup automatico con I-Team.

Protezione antivirus e antimalware Assicurati che tutti i dispositivi aziendali siano dotati di software antivirus e antimalware aggiornati. Queste soluzioni proteggono da malware, phishing e altri attacchi informatici. Verifica che i software siano configurati per eseguire scansioni automatiche e aggiornamenti regolari anche durante le ferie.

Gestione delle password Rivedi e rafforza le password di accesso a tutti i sistemi aziendali. Incoraggia l'utilizzo di password complesse e uniche per ciascun account. È consigliabile anche abilitare l'autenticazione a due fattori (2FA) per aggiungere un ulteriore strato di sicurezza.

Limita l'accesso ai dati sensibili Prima di andare in ferie, valuta e riduci i privilegi di accesso ai dati sensibili. Limita l'accesso solo al personale strettamente necessario e revoca temporaneamente i permessi di accesso per gli utenti che non ne hanno bisogno durante il periodo di ferie.

Monitoraggio continuo della sicurezza Se possibile, attiva sistemi di monitoraggio continuo della sicurezza per rilevare attività sospette o anomalie durante il periodo di chiusura aziendale. Questo può aiutare a individuare tempestivamente eventuali attacchi e adottare misure correttive immediate.

Consapevolezza dei dipendenti Educa i dipendenti sulle buone pratiche di sicurezza informatica e sui rischi associati alle minacce online. Incoraggia la prudenza nell'aprire allegati o cliccare su link sospetti e ricorda loro di non condividere informazioni aziendali riservate con terze parti non autorizzate.

Monitoraggio delle comunicazioni aziendali Assicurati che le comunicazioni aziendali, come email o messaggi di lavoro, siano monitorate anche durante le ferie. Questo garantisce una risposta tempestiva a eventuali problemi o richieste urgenti.

Anticipa e prendi le giuste precauzioni per proteggere la sicurezza informatica della tua impresa e se hai qualche dubbio o perplessità, consulta subito I-TEAM.

Ricordati che la sicurezza informatica è una responsabilità continua e richiede attenzione anche quando si è in vacanza.

A cura di
Federico Melucci

Centralino in cloud Digikoll:
adesso integrato anche con WhatsApp

Scopri tutte le novità del centralino multicanale!
Vuoi portare l'esperienza di comunicazione ad un livello superiore di praticità e semplicità? Ad esempio, integrando la messaggistica di WhatsApp fra i canali di comunicazione del tuo centralino. Con Digikoll, l'innovativo centralino digitale, è infatti possibile gestire tutte le comunicazioni dei principali canali di messaggistica direttamente attraverso la piattaforma online; con l'aggiunta della messaggistica WhatsApp, le aziende possono comunicare con i propri clienti attraverso una grande varietà di canali, gestendo tutte le interazioni da una piattaforma unica.

Un centralino unico per tutti i canali di comunicazione

Digikoll supera i confini delle tradizionali chiamate vocali e video, offrendo una soluzione omnicanale che include WhatsApp ed è comunque in costante evoluzione, pronto per accogliere ulteriori canali che si andranno ad affermare. Le imprese possono ricevere e gestire le conversazioni dei clienti attraverso un'unica piattaforma, semplificando la gestione delle comunicazioni, con tutti i canali che convergeranno in un unico luogo, eliminando la necessità di passare da un'app all'altra.

Quali sono le caratteristiche di Digikoll

1. Accesso a tutti i principali canali di comunicazione: con Digikoll, le aziende possono interagire con i clienti tramite chiamate vocali, videochiamate, SMS e WhatsApp. Questa diversificazione dei canali di comunicazione consente di offrire ai clienti più opzioni per mettersi in contatto con l'azienda.

2. Interfaccia unificata per la gestione delle chat: Digikoll fornisce un'interfaccia unificata in cui è possibile gestire tutte le chat dei clienti, indipendentemente dal canale utilizzato. Questo elimina la confusione e semplifica il processo di gestione delle interazioni dei clienti.

3. Registro centrale di tutte le conversazioni: tutte le conversazioni dei clienti sono conservate in un unico archivio. Ciò consente alle aziende di mantenere un registro completo di tutte le interazioni e di accedervi in qualsiasi momento, facilitando la risoluzione delle richieste dei clienti e migliorando la qualità del servizio.

4. Esperienza utente senza soluzione di continuità: Digikoll è accessibile da qualsiasi dispositivo, che sia un browser web, un'app mobile o un'app desktop. Ciò consente di gestire la messaggistica omnicanale ovunque ci si trovi, garantendo un'esperienza utente fluida e senza interruzioni.

A cura di
Paolo Vannini

Web Hosting come strumento di successo per un'azienda

Il Web Hosting è un servizio che consente ai siti web di essere presenti e accessibili su Internet; si basa sull'allocazione degli elementi costitutivi di un sito web, come file, immagini, script e altri contenuti, all'interno di un sistema di memorizzazione fisica, come HDD o SSD, che si trova in una struttura di hosting, come una web farm o un data center. La velocità di accesso ad un sito web è un fattore cruciale per migliorare e rendere gratificante l'esperienza online dell'utente. Un elemento fondamentale che influisce su questi aspetti è l'hosting.

Quali sono le tipologie di Hosting e cosa comportano

Hosting condiviso:

- Ideale per i siti web con traffico limitato e budget ridotto
- I server sono condivisi tra più siti, riducendo i costi ma potenzialmente influenzando le prestazioni
- Consigliato per siti web personali, blog o piccoli siti aziendali

Hosting dedicato:

- Offre un server riservato esclusivamente al vostro sito web
- Massime prestazioni, maggiore controllo e personalizzazione
- Adatto per siti web ad alto traffico, applicazioni web complesse od e-commerce

Hosting semidedicato:

- Una soluzione intermedia tra l'hosting condiviso e l'hosting dedicato
- Alcune risorse sono condivise, mentre altre sono assegnate in esclusiva
- Fornisce maggiore flessibilità e prestazioni rispetto all'hosting condiviso

Virtual Private Server (VPS):

- Utilizza un server virtuale che condivide lo stesso hardware fisico con altri server virtuali
- Offre maggiore separazione delle risorse e controllo rispetto all'hosting condiviso
- Adatto per siti di medie dimensioni che richiedono scalabilità e flessibilità

Cloud hosting:

- Utilizza una rete di server virtuali interconnessi per ospitare un sito web
- Offre alta affidabilità, scalabilità e flessibilità
- Ideale per siti web con picchi di traffico imprevedibili o che richiedono risorse flessibili

Perché l'hosting web è così importante?

1) Velocità del sito web:

La velocità di caricamento di un sito web è cruciale per coinvolgere gli utenti e ridurre i tassi di abbandono. L'hosting gioca un ruolo fondamentale nel determinare la velocità complessiva del sito. Un hosting di bassa qualità o sovraccaricato può causare tempi di risposta lenti e un'esperienza utente negativa. Ciò può avere un impatto negativo sulla reputazione del vostro sito e sulle conversioni.

2) Valutazione dei motori di ricerca:

I motori di ricerca, come Google, attribuiscono grande importanza alla velocità del sito web nella valutazione della qualità delle pagine. Un sito web veloce è considerato più affidabile e offre un'esperienza utente migliore e, di conseguenza, i motori di ricerca possono posizionare il vostro sito web più in alto nei risultati di ricerca, aumentando la visibilità e il traffico.

Investire in un hosting di qualità può fare la differenza nella velocità del sito web aziendale e nel successo complessivo della presenza della vostra azienda online.

I-TEAM è un provider di hosting web affidabile e supporta le aziende nel valutare attentamente le proprie esigenze, le caratteristiche specifiche del sito web e le opzioni disponibili, con soluzioni scalabili per adattarsi alle esigenze future del sito web, e un supporto tecnico tempestivo.

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