ARTICOLO DI ELEARNINGNEWS

Year 8 - number 298 Wednesday 17 July 2024

Normativa NIS2: come mettersi in regola entro ottobre 2024

La NIS2 è la normativa europea aggiornata sulla cyber security, entrata in vigore a gennaio 2023, che sostituisce la precedente NIS1.

Nel panorama digitale odierno, la **sicurezza informatica** non è più un'opzione, ma una necessità imprescindibile. Con l'aumento delle minacce cibernetiche sempre più sofisticate, la protezione dei dati e delle infrastrutture è diventata una priorità per aziende e organizzazioni di ogni settore. Per questo motivo, l'Unione Europea ha introdotto la **Direttiva NIS2**, un'evoluzione significativa della precedente NIS1 che mira a rafforzare la resilienza dell'Europa di fronte alle cyber-minacce.

NIS1: un solido punto di partenza

La Direttiva NIS1, entrata in vigore nel 2016, ha rappresentato un passo avanti importante nel panorama europeo della cyber security. Ha introdotto misure di sicurezza per i settori critici come l'**energia**, i **trasporti** e le **infrastrutture finanziarie**. Tuttavia, con il progresso della digitalizzazione e l'aumento delle minacce informatiche, è emersa la necessità di istituire un quadro normativo più robusto e completo.

NIS2: nuove misure di sicurezza per l'era digitale

La NIS2, entrata in vigore il **17 gennaio 2023**, risponde a questa esigenza in modo deciso e concreto. Introduce nuove e più stringenti misure di sicurezza per un'ampia gamma di settori, tra cui quelli **sanitari**, **postali** e delle **acque reflue**.

Cosa introduce la NIS 2?

Ecco alcuni dei punti chiave della NIS 2:

- **Un campo di applicazione più ampio**. La nuova normativa si applica a un numero maggiore di settori e attività, per garantire una protezione più completa e uniforme.
- **Nuove categorie di operatori**. Vengono introdotte due nuove categorie: gli Operatori di Servizi Essenziali (OSE) e i fornitori di servizi digitali (DSP). I primi sono enti pubblici o privati che forniscono servizi critici per la società come energia, trasporti, sanità e acque. I secondi sono enti che forniscono servizi digitali a un numero significativo di utenti nell'UE come piattaforme online, servizi cloud e comunicazioni elettroniche.
- **Obblighi più rigidi per la gestione del rischio**. La NIS 2 richiede alle organizzazioni di implementare misure di gestione del rischio più rigorose e strutturate, come la pianificazione della sicurezza informatica, la gestione e la notifica degli incidenti.
- **Maggiori obblighi di segnalazione**. La normativa impone alle organizzazioni, in maniera ancora più imperativa, di segnalare immediatamente alle autorità competenti i gravi incidenti di sicurezza informatica.
- **Sanzioni più severe**. La NIS2 introduce sanzioni più severe per le organizzazioni che non ottemperano ai suoi obblighi, incentivando il rispetto della normativa e la tutela della sicurezza informatica.

NIS2: quali sono le aziende interessate?

La NIS2 si applica a un'ampia gamma di aziende e organizzazioni, tra cui:

- **Operatori di settori critici**: energia, trasporti, sanità, finanza, acque reflue, settore pubblico.
- **Fornitori di servizi digitali**: posta elettronica, motori di ricerca, cloud computing.
- **Piattaforme online**: marketplace, social media.

L'Agenda Digitale, importante testata online di riferimento per tematiche riguardanti il Digitale e la Pubblica Amministrazione, ha stilato una **categorizzazione chiara e completa di tutti i soggetti coinvolti**, invitando le aziende appartenenti a uno o più dei settori o sottosettori menzionati ad attivarsi, se non lo hanno già fatto.

NIS 2: entro quando è necessario adeguarsi?

La scadenza per adeguarsi alla NIS 2 è il 18 ottobre 2024. Le aziende interessate devono quindi movimentarsi tempestivamente per implementare le misure di sicurezza necessarie e conformarsi alla nuova normativa.

Come prepararsi alla NIS 2

Per prepararsi alla NIS 2, le aziende devono seguire alcuni semplici passi fondamentali:

1. **Valutare la propria situazione**. E' necessario identificare i settori in cui opera l'azienda, i dati sensibili che gestisce e i potenziali rischi a cui è soggetta.
2. **Effettuare una valutazione del rischio**. Un'analisi approfondita delle **minacce** e delle vulnerabilità a cui l'azienda è esposta è fondamentale per definire le misure di sicurezza adeguate.
3. **Implementare le misure di sicurezza**. E' importante adottare le misure tecniche e organizzative necessarie per mitigare i rischi individuati, basandosi su standard e best practice del settore.
4. **Testare e monitorare**. Le misure di sicurezza implementate devono essere regolarmente testate per verificarne l'efficacia e monitorate costantemente per adattarle all'evolversi delle minacce.

Oltre a questi passi fondamentali, ecco alcuni suggerimenti extra per le aziende:

- **Nominare un responsabile per la sicurezza informatica**. Questa figura avrà la responsabilità di supervisionare l'implementazione e il mantenimento delle misure di sicurezza.
- **Formare il personale sulla sicurezza informatica**. Tutti i dipendenti dovrebbero essere consapevoli delle minacce informatiche e sapere come proteggere i dati e le infrastrutture aziendali.
- **Utilizzare soluzioni di sicurezza affidabili**. Investire in soluzioni di sicurezza informatica di ultima generazione per proteggere efficacemente le infrastrutture e i dati aziendali dalle minacce informatiche in continua evoluzione.

Soluzioni di cyber security avanzate

Ecco alcuni esempi pratici di come le **tecnologie di sicurezza informatica** di ultima generazione possono aiutare le aziende a conformarsi alla NIS 2:

- **Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS**). Questi sistemi monitorano il traffico di rete e identificano attività sospette che potrebbero indicare un attacco in corso.
- **Firewall di nuova generazione (NGFW).** Offrono una protezione più avanzata rispetto ai firewall tradizionali, filtrando il traffico in base a criteri più granulari e proteggendo dalle minacce più recenti.
- **Soluzioni di crittografia**. Permette di proteggere i dati sensibili sia in fase di archiviazione che durante la trasmissione, rendendoli inaccessibili agli hacker.
- **Soluzioni di gestione delle identità e degli accessi (IAM)**. Queste soluzioni controllano chi può accedere alle risorse aziendali e cosa può fare, garantendo che solo gli utenti autorizzati abbiano accesso ai dati e ai sistemi.
- **Soluzioni di backup e ripristino**. In caso di attacco informatico, è fondamentale avere a disposizione backup completi e aggiornati dei dati aziendali per poterli ripristinare rapidamente.

(Fonte: https://bitcorp.it/it/article/219)

NIS 2: un'opportunità per le aziende

Oltre all'investimento in soluzioni tecnologiche, è importante anche investire nella **formazione del personale sulla cyber security**. I dipendenti sono spesso l'anello debole della sicurezza informatica, quindi è fondamentale renderli consapevoli delle minacce informatiche e di come proteggersi.

In definitiva, l'adeguamento alla NIS 2 non rappresenta solo un obbligo normativo, ma anche un investimento significativo per le aziende: può essere **un'opportunità per migliorare la propria sicurezza informatica**, **aumentare la fiducia dei clienti e rafforzare la propria competitività**.

Vuoi formare i tuoi dipendenti e offrire loro strumenti per prevenire le minacce informatiche? Consulta il **catalogo di corsi online sulla cyber security di Mega Italia Media**.