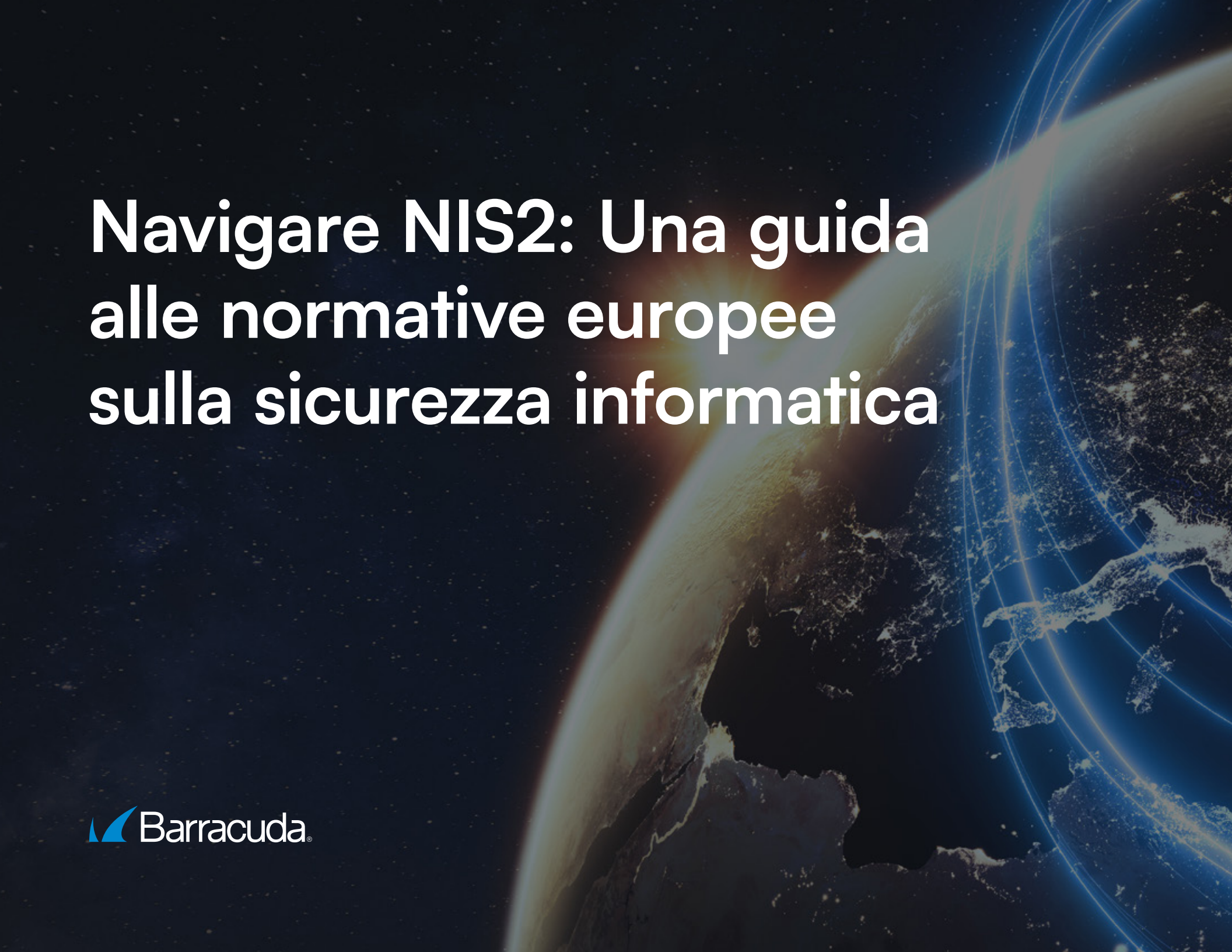
Navigare NIS2: Una guida alle normative europee sulla sicurezza informatica



Barracuda

L’evoluzione delle normative sulla sicurezza informatica in Europa

Il ruolo in costante evoluzione delle normative sulla sicurezza informatica in Europa riflette la crescente consapevolezza dell’aumento delle minacce che le violazioni e i criminali informatici rappresentano per le singole aziende e organizzazioni, nonché per la società in generale. Dato che la nostra società ora è composta da organizzazioni sempre più interconnesse, qualsiasi attacco può avere conseguenze inaspettate e di ampia portata.

Le recenti modifiche apportate alle normative dell’Unione Europea (UE), note come NIS2 (Direttiva sulla sicurezza delle reti e delle informazioni 2), menzionano anche l’impatto del COVID-19 sulle pratiche di lavoro. Con un numero sempre maggiore di persone che lavorano da casa dopo la pandemia, la superficie potenziale delle minacce aumenta, così come la nostra dipendenza dalle reti per portare a termine il lavoro, e il resto delle nostre vite.

Ma riflette anche la crescente maturità della regolamentazione della sicurezza informatica. Mentre le organizzazioni lavorano per rimanere sicure, si riconosce anche che abbiamo bisogno di leggi unificate e standard minimi per mantenerci tutti al sicuro.

Il primo passo in questo percorso è stato compiuto nel 2016, con la Direttiva sulla sicurezza delle reti e delle informazioni, o NIS1. Questa Direttiva ha stabilito gli standard di base della sicurezza informatica per le organizzazioni che operano in settori critici, tra cui il settore idrico, delle infrastrutture digitali, delle banche, della sanità e dei trasporti. La NIS2 amplia questi settori, abbracciando un insieme molto più ampio di settori.

Detto questo, va anche detto che la NIS2 è una direttiva e non una legge: deve essere quindi recepita nel diritto nazionale dagli Stati membri, cosa che alcuni Stati hanno già fatto. La NIS2 è ormai in vigore e diversi Paesi, tra cui Belgio, Croazia e Italia, l'hanno accolta nelle rispettive legislazioni locali, mentre altri sono in procinto di adottarla.

La NIS2 sta trasformando e informando la regolamentazione sia all'interno dell'UE sia oltre i suoi confini. Questo è un altro fattore trainante fondamentale nella legislazione sulla sicurezza informatica. Non opera in un singolo Stato-nazione. Le aziende che interagiscono con i cittadini o con altre imprese nell'UE devono seguire le stesse regole. Ci stiamo muovendo verso un mondo in cui gli standard di sicurezza informatica sono condivisi tra i paesi e le aziende saranno obbligate a conformarsi per fare affari e rassicurare i clienti che stanno attuando le normative.

Va anche notato che il governo del Regno Unito si è impegnato a non adottare la NIS2 nella legislazione nazionale, ma ad allineare la NIS1 alle altre normative, come il Cyber Security and Resilience Bill. Ma guardando a quello che viene effettivamente suggerito, sembra che il Regno Unito e l'UE si stiano muovendo nella stessa direzione con le modifiche apportate, anche se la legislazione britannica proposta promette di essere meno onerosa. Non è chiaro quando il governo del Regno Unito troverà il tempo in Parlamento per apportare queste modifiche. In realtà, la maggior parte delle organizzazioni che lavorano o commerciano con l'UE probabilmente sceglierà un insieme di regole da rispettare anziché due.

Le basi di NIS2

Chi:

Si applica in tutta l'UE, ma anche le imprese di tutto il mondo che intrattengono rapporti commerciali o forniscono servizi a imprese o organizzazioni all'interno dell'UE dovranno seguire le pratiche della NIS2.

Estende le regole dalle grandi organizzazioni che si occupano di infrastrutture critiche alle aziende più piccole e a quelle definite dall'UE come fondamentali.

Regole estese alle aziende con più di 50 dipendenti in determinati settori.

Energia, trasporti, banche, sanità, infrastrutture digitali, fornitori di cloud computing, fornitori di servizi di sicurezza gestiti, gestione dei rifiuti, produttori alimentari, gran parte dell'industria manifatturiera, motori di ricerca ed enti di ricerca sono tutti inclusi.

Cosa:

Stabilisce regole affinché i Paesi siano preparati in caso di incidenti di sicurezza informatica e incoraggia la cooperazione transfrontaliera.

Gli Stati membri avrebbero dovuto recepire la direttiva nel proprio diritto nazionale entro ottobre 2024. Molti Stati lo hanno fatto, mentre altri sono in varie fasi di adozione. Controlla lo stato attuale della trasposizione.

Notifica obbligatoria degli incidenti.

Come:

La sicurezza informatica è una chiara responsabilità dei dirigenti senior, e la NIS2 lo fa rendendoli personalmente responsabili dei fallimenti.

La direttiva, e i relativi equivalenti di diritto nazionale, coprono una selezione più ampia di società e organizzazioni, non solo infrastrutture vitali, ma anche quelle definite dall'UE come fondamentali.

Definisce l'obbligo di avvisare tempestivamente in caso di incidenti entro 24 ore, fornire una notifica più dettagliata entro 72 ore e un rapporto dettagliato entro un mese. Questo mira a creare due effetti vantaggiosi. In primo luogo, per incoraggiare la conformità sotto la minaccia di una pubblicità sgradita e, in secondo luogo, per fornire spunti d'azione ad altre organizzazioni che potrebbero essere bersaglio di attacchi simili.

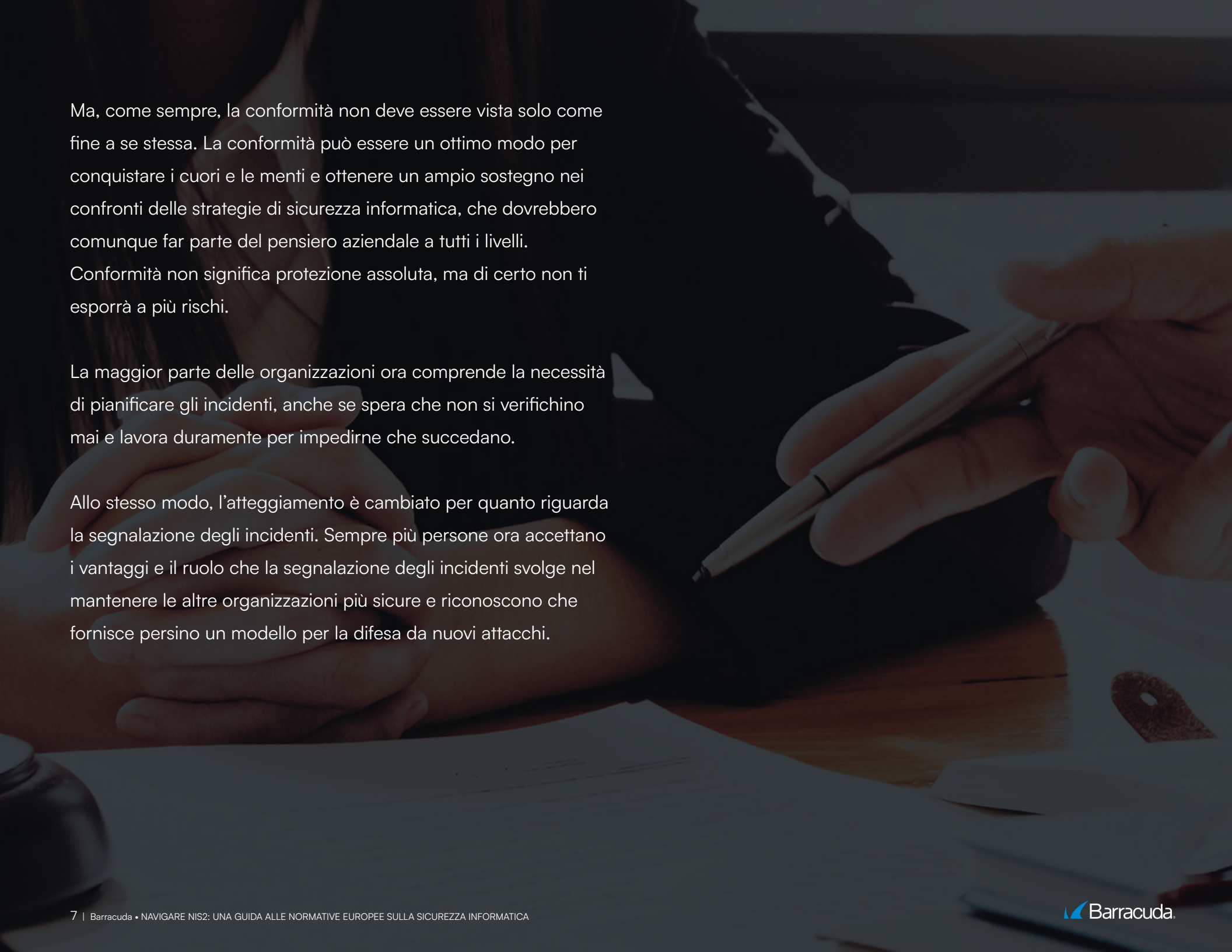
Nozioni di base sulla NIS2: Cosa devi fare per garantire la conformità

Va detto che la NIS2 assomiglia molto a qualsiasi manuale di "best practice" per una buona igiene generale della sicurezza informatica, anche se prevede severe sanzioni finanziarie in caso di mancato rispetto. Le sanzioni previste dalla NIS2 sono severe, con multe che possono raggiungere i 10 milioni di euro o il 2% del fatturato globale annuo, a seconda di qual è l'importo più alto.

La conformità alla direttiva e la protezione per l'azienda significano determinare quello che è necessario per proteggere i dispositivi, gli asset e i dati. Questo significa sicurezza fisica, sicurezza informatica e personale formato per operare in tutta sicurezza. Oltre ad implementare tali misure, le organizzazioni devono anche dimostrare di disporre di un'efficace strategia di gestione del rischio. Questo include la dimostrazione di ciò che hai fatto: aver valutato lo stato delle tue reti, dei tuoi sistemi IT e delle tue competenze umane e di aver agito ove appropriato.

Devi dimostrare di avere un piano in atto per la gestione degli incidenti se dovesse succedere il peggio. Dovrai dimostrare di aver valutato la sicurezza della supply chain, la gestione delle vulnerabilità e la divulgazione, e di aver implementato una strategia per l'uso della crittografia e, ove appropriato, della cifratura.

La NIS2 riconosce le certificazioni di sicurezza informatica dell'UE per prodotti e soluzioni per contribuire ad alleggerire l'onere della conformità per le aziende. Se la tua organizzazione è già conforme alla norma ISO 27001, sei già sulla buona strada per soddisfare la NIS2.



Ma, come sempre, la conformità non deve essere vista solo come fine a se stessa. La conformità può essere un ottimo modo per conquistare i cuori e le menti e ottenere un ampio sostegno nei confronti delle strategie di sicurezza informatica, che dovrebbero comunque far parte del pensiero aziendale a tutti i livelli. Conformità non significa protezione assoluta, ma di certo non ti esporrà a più rischi.

La maggior parte delle organizzazioni ora comprende la necessità di pianificare gli incidenti, anche se spera che non si verifichino mai e lavora duramente per impedirne che succedano.

Allo stesso modo, l'atteggiamento è cambiato per quanto riguarda la segnalazione degli incidenti. Sempre più persone ora accettano i vantaggi e il ruolo che la segnalazione degli incidenti svolge nel mantenere le altre organizzazioni più sicure e riconoscono che fornisce persino un modello per la difesa da nuovi attacchi.

Best practice per la conformità e la sicurezza: Capire la differenza

I professionisti della sicurezza informatica devono comprendere la differenza tra il raggiungimento della conformità e il raggiungimento della migliore protezione possibile. E non è la stessa cosa. Le organizzazioni devono dimostrare la conformità: devi essere in grado di dimostrare, concretamente, a una terza parte che quello che è stato fatto è il più sicuro possibile. È come mostrare alla tua compagnia di assicurazioni che hai installato le serrature e gli allarmi giusti per proteggere il tuo magazzino. Tutto questo è necessario, ma non basta per essere veramente al sicuro.

Ecco 13 elementi da prendere in considerazione nel tuo percorso verso la conformità NIS2:

Politica di sicurezza della rete: Stabilisci una politica sulla sicurezza della rete e dei sistemi informativi che definisca i ruoli e le responsabilità dei vari reparti aziendali, con un processo per monitorare la conformità.

Valutazione del rischio: Stabilisci e implementa una politica di gestione degli incidenti che stabilisca ruoli, responsabilità e procedure per rilevare, analizzare, contenere o rispondere, riprendersi, documentare e segnalare gli incidenti in modo tempestivo.

Continuità aziendale e gestione delle crisi: Sviluppa e mantieni un piano di continuità aziendale, gestione delle crisi e ripristino di emergenza da applicare in caso di incidenti di sicurezza informatica e altre crisi che includa piani di backup per le risorse critiche, compreso il personale. Forma il personale interessato su questi documenti e conduci regolarmente crisi simulate per assicurarti che tutti conoscano e possano svolgere i propri ruoli.

Politica di sicurezza della supply chain: Crea e implementa una politica di sicurezza della supply chain che includa una valutazione delle pratiche di sicurezza dei potenziali fornitori come parte del processo di contrattazione.

Comprendere l'uso dei fornitori di tecnologie dell'informazione e della comunicazione (ICT): Mappa i fornitori ICT, cosa fanno, quali sono quelli critici per le operazioni e gli standard di sicurezza che devono soddisfare. Mantieni un elenco di fornitori critici, comprese le informazioni di contatto. Sviluppa un processo per valutare la conformità dei fornitori agli standard di sicurezza.

Valutazione del processo di rischio informatico: Crea un processo in cui puoi valutare l'efficacia delle tue procedure relative al rischio informatico ed conduci tale valutazione periodicamente.

Formazione sulla sicurezza: Assicura la formazione sulla sicurezza informatica e promuovi pratiche di igiene informatica di base tra i dipendenti per favorire una cultura della sicurezza e consapevolezza.

Crittografia: Sviluppa e applica l'uso corretto della crittografia e della cifratura per garantire la riservatezza e l'integrità dei dati sensibili.

Sicurezza delle risorse umane: Implementa politiche e procedure che regolino il comportamento dei dipendenti per quanto riguarda l'igiene della sicurezza informatica. Utilizza procedure di screening appropriate in background in conformità con la legge applicabile quando assumi del personale. Crea una procedura standard per revocare tutti gli accessi alle risorse informatiche e alle informazioni aziendali quando i dipendenti lasciano l'azienda.

Controllo degli accessi: Implementa procedure di sicurezza per i dipendenti con accesso a dati riservati. Utilizza l'autenticazione a più fattori (MFA) e la valutazione Zero Trust continua e, se necessario, crittografa le comunicazioni di emergenza interne per migliorare le misure di sicurezza.

Classificazione delle risorse aziendali: Configura un sistema per classificare le informazioni aziendali, come le informazioni aziendali riservate e le informazioni sensibili (ad esempio, informazioni sanitarie, numeri di documento d'identità governativi, carte di credito, ecc.).

Sicurezza ambientale e fisica: Valuta le infrastrutture critiche di supporto per i siti aziendali, come i sistemi di comunicazione e l'alimentazione e, ove possibile, implementa processi di backup. Proteggi le posizioni fisiche dalle minacce esterne, inclusi i controlli degli accessi fisici.

Prima le persone e i processi, poi la tecnologia

Spesso i fornitori sono accusati di vendere prima le soluzioni. Ma in realtà è necessario iniziare mettendo in atto i processi, le procedure e le persone giuste, e poi pensare alla tecnologia per supportare e rafforzare queste capacità. I team di sicurezza spesso considerano l'uomo l'anello più debole e non la prima linea di difesa.

Formare il personale e migliorare le loro competenze in ambito di sicurezza è un passo fondamentale, riconosciuto anche nella direttiva NIS2.

Ogni cambiamento normativo è una valida opportunità per rivedere le basi e valutare quello che si sta facendo bene e dove c'è spazio per miglioramenti.

Sono necessari controlli di accesso e gestione delle identità efficaci. Hai bisogno di protezione dell'e-mail, che rappresenta ancora il vettore e il punto di partenza più comune per un attacco. Sono anche necessari un firewall e la protezione della rete.

Ma hai anche bisogno di sistemi di sicurezza più intelligenti che lavorino per te. Analizzare il comportamento della rete e delle applicazioni è sempre più importante in un mondo in cui identificare il "perimetro" di qualsiasi rete diventa ogni giorno più difficile. Questo può anche aiutarti a proteggerti dagli attacchi alla supply chain.

Barracuda può aiutarti a soddisfare i requisiti NIS2 e a migliorare il tuo livello di sicurezza complessiva con la protezione delle applicazioni, la protezione della rete e la protezione dell'e-mail. Possiamo persino fornire un XDR gestito per supervisionare il tutto.

Informazioni su Barracuda

Barracuda è un'azienda leader globale nel settore della sicurezza informatica che offre una protezione completa contro le minacce complesse per aziende di tutte le dimensioni. La nostra piattaforma BarracudaONE basata sull'IA protegge e-mail, dati, applicazioni e reti con soluzioni innovative, XDR gestito e una dashboard centralizzata per massimizzare la protezione e rafforzare la resilienza informatica. Scelta da centinaia di migliaia di professionisti IT e provider di servizi gestiti in tutto il mondo, Barracuda offre difese potenti e facili da acquistare, implementare e utilizzare. Per ulteriori informazioni, visita it.barracuda.com.

Barracuda