HPE aruba networking

Una rete basata sull'AI security-first per la compliance a NIS2

Accelerare la compliance a NIS2 con HPE Aruba Networking

HPE GreenLake

Indice del contenuto

NIS2: un livello comune elevato di cybersicurezza nella UE

La Direttiva NIS2 (Network and Information Security) è una legislazione completa e punto di riferimento per l'intera Unione Europea (UE) in materia di cybersicurezza, concepita per migliorare il livello generale di sicurezza informatica nella UE[1]. Basata sulla Direttiva NIS del 2018, la prima legislazione sulla cybersicurezza a livello di UE[2], la Direttiva NIS2 è stata adottata a dicembre 2022 in risposta a una maggiore digitalizzazione e alle crescenti minacce derivanti dalla pandemia da COVID-19 e dal conflitto russo-ucraino. Le normative NIS2 ampliano l'ambito delle organizzazioni soggette ai requisiti di cybersicurezza della UE.

Secondo le previsioni, saranno oltre 100.000 le organizzazioni interessate dagli standard di cybersicurezza NIS2 che gli stati membri della UE dovranno implementare entro il 17 ottobre 2024[3].

Qualsiasi organizzazione (1) con più di 250 dipendenti o 50 milioni di euro di fatturato annuo che fornisca servizi all'interno della UE (2) e in un settore classificato come "entità essenziali e importanti" deve conformarsi alla Direttiva NIS2[4]. I settori non soggetti alla compliance a NIS2 includono la pubblica amministrazione e gli enti locali, la produzione, la lavorazione e la distribuzione di alimenti, i servizi postali e dei corrieri e i provider di servizi digitali e di produzione[5]. Le organizzazioni che operano in settori soggetti ai requisiti della precedente Direttiva NIS devono conformarsi anche agli obblighi della Direttiva NIS2. Tali settori includono l'assistenza finanziaria, i servizi bancari e finanziari e i trasporti. Nota: questo elenco non è esaustivo. Per ulteriori informazioni, consulta gli allegati 1 e 2 della Direttiva NIS2[6].

Problematiche della compliance a NIS2

Rispettare la compliance può risultare problematico sia per le organizzazioni che implementano tecnologie e pratiche conformi per la prima volta sia per quelle che aggiungono funzionalità per soddisfare requisiti superiori.

Requisiti tra più domini: i framework di compliance come NIS2 coprono in genere più domini della tecnologia all'interno di un'organizzazione, influendo su pratiche e infrastruttura dall'edge al cloud.

Funzionalità frammentate: le funzionalità richieste per conformarsi a NIS2 spesso riguardano più soluzioni tecnologiche, il che può comportare l'adozione frammentaria dei prodotti in questione. Oltre ad aumentare la complessità a livello di architettura e operazioni, con il tempo questo approccio confuso espone anche l'organizzazione a falle di sicurezza, incoerenze nelle policy e nella relativa applicazione e potenziali rischi per la cybersicurezza.

Collaborazione tra team: per introdurre efficacemente innovazioni che soddisfino i requisiti di compliance, è spesso che i team di rete e sicurezza collaborino per perseguire finalità e obiettivi comuni, fornendo competenze specialistiche mentre proteggono l'organizzazione da attacchi sempre più sofisticati e diffusi.

Per le entità essenziali, le penali per la mancata compliance possono raggiungere almeno 10 milioni di dollari o il 2% del fatturato globale annuo[7].

[1] The NIS2 Directive: A high common level of cybersecurity in the EU. Parlamento europeo. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[2] The NIS2 Directive: A high common level of cybersecurity in the EU. Parlamento europeo. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[3] Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. Int. Cybersecur. Law Rev. 2, 223–231 (2021). https://doi.org/10.1365/s43439-021-00033-8 (#Fn19)

[4] NIS2 si applica alle organizzazioni dell'allegato I e dell'allegato II non classificate come microimprese o piccole imprese. Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN. Definizione di microimprese e piccole imprese in base alla Raccomandazione della Commissione del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese. http://data.europa.eu/eli/reco/2003/361/oj

[5] Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148. Unione Europea.

[6] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2). http://data.europa.eu/eli/dir/2022/2555/oj. Dicembre 2022

[7] Direttiva sulle misure per un livello comune elevato di cibersicurezza in tutta l'Unione (direttiva NIS2) - FAQ. Commissione europea. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs. Giugno 2023.

Una rete basata sull'AI security-first per la compliance a NIS2

Accelera il percorso verso la compliance a NIS2 con una rete basata sull'AI security-first di HPE Aruba Networking. Basate sui principi zero trust, le soluzioni di rete basate sull'AI security-first di HPE Aruba Networking forniscono ai team di rete e sicurezza un fondamento comune per offrire esperienze uniche e risultati di business innovativi, senza penalizzare la protezione della cybersicurezza.

La rete basata sull'AI security-first di HPE Aruba Networking semplifica la compliance a standard e normative in materia di cybersicurezza consentendo alle organizzazioni di utilizzare la rete come soluzione di sicurezza. Oggi la rete può fornire visibilità più avanzata, informazioni, gestione centralizzata delle policy, protezione dei dati, difesa dalle minacce e controllo degli accessi, il tutto in una singola piattaforma. Grazie a queste funzionalità integrate di sicurezza zero trust, la rete stessa diventa una linea di difesa critica, che può aiutare a soddisfare i requisiti NIS2 senza aumentare la complessità derivante da più tool disparati e senza richiedere una sostituzione integrale dell'infrastruttura esistente con i costi e le interruzioni che comporta.

Una rete basata sull'AI consente anche di moltiplicare il potenziale umano dell'organizzazione, un aspetto cruciale a fronte dell'espansione del quadro normativo, di una carenza di talenti sempre più grave e dell'aumento delle minacce informatiche. Con la rete basata sull'AI security-first di HPE Aruba Networking, i team possono sfruttare l'automazione intelligente per ridurre gli interventi manuali, migliorare la visibilità e il rilevamento delle anomalie, oltre a ottimizzare le procedure di monitoraggio e diagnostica. Tutte cose che, insieme, evitano di esporre l'azienda a una serie di rischi inutili.

Rispettare i principali requisiti NIS2 con HPE Aruba Networking

Le linee guida NIS2 riguardano un'ampia varietà di funzionalità e requisiti volti ad aumentare la cybersicurezza, a livello locale e organizzativo, e la resilienza aziendale. Includono requisiti per il rilevamento e la risposta agli incidenti, la strategia e la governance per la cybersicurezza e la protezione di applicazioni e infrastruttura.

Pratiche di base per l'igiene informatica

Il preambolo 89 della Direttiva NIS2 definisce una serie di requisiti dell'igiene informatica di base, ovvero le pratiche essenziali per ottimizzare la postura di cybersicurezza e proteggere l'organizzazione da minacce e vulnerabilità[8].

Le soluzioni di HPE Aruba Networking contribuiscono a soddisfare questi requisiti con:

- principi di sicurezza zero trust
- gestione di identità e accessi o responsabilizzazione degli utenti
- segmentazione della rete
- integrazione di tecnologie per ottimizzare la cybersicurezza, come AI e ML
- aggiornamenti software
- configurazione di dispositivi

Sicurezza zero trust

Anche se nessun singolo fornitore o soluzione è in grado di offrire tutta la protezione informatica che serve a un'organizzazione, iniziare con una rete in grado di fornire una base integrata per la sicurezza zero trust può contribuire a ridurre il numero di tool disparati necessari a soddisfare i requisiti NIS2, aggiungendo protezione nei punti di accesso digitali critici.

HPE Aruba Networking Edge Services Platform (ESP) è una piattaforma basata sui principi di sicurezza zero trust dall'edge al cloud, ottimizzando la protezione e semplificando al contempo le operazioni. HPE Aruba Networking offre le funzionalità zero trust chiave di visibilità completa, autenticazione, autorizzazione, controlli degli accessi con privilegi minimi, oltre a monitoraggio continuo e applicazione di policy, in collaborazione con l'ecosistema di sicurezza più ampio, sia all'interno che all'esterno della rete aziendale.

[8] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2). Unione Europea.

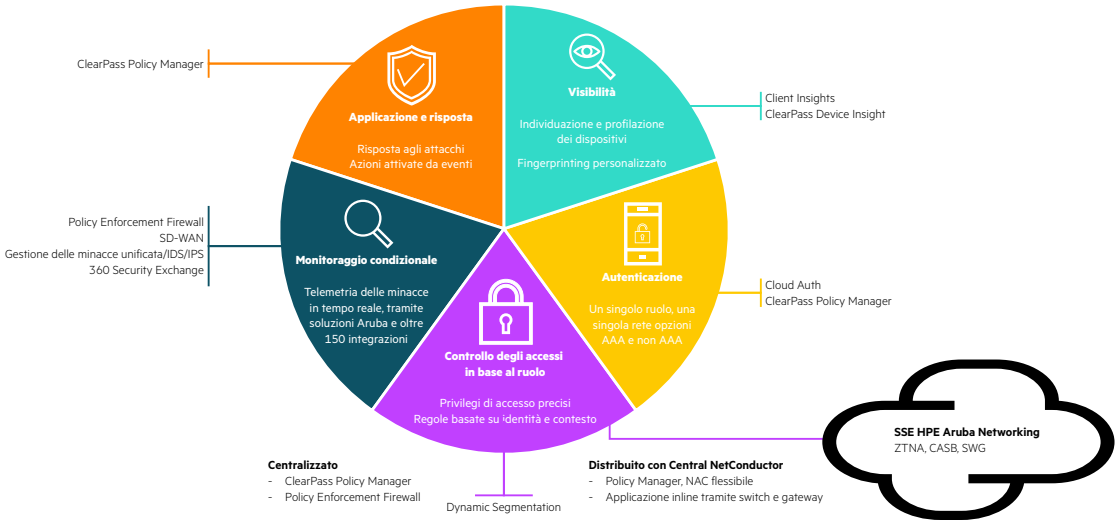

Figura 1. Base per la sicurezza zero trust di HPE Aruba Networking

Gestione di accessi e identità

La sicurezza zero trust inizia dalla visibilità degli utenti e dei dispositivi connessi. La soluzione per la gestione della rete basata su cloud **HPE Aruba Networking Central** include funzionalità di visibilità e profilazione basate sull'AI con **Client Insights**. Client Insights analizza i dati di telemetria nativi dell'infrastruttura direttamente da access point, switch, gateway e client, senza richiedere l'installazione di agenti né strumenti di raccolta fisici. Sfruttando le tecnologie AI/ML, Client Insights fornisce una profilazione dei dispositivi accurata fino al 99% per i client noti, con una percentuale di incertezza inferiore al 5% per quelli sconosciuti, per una vasta gamma di endpoint connessi alla rete, che comprendono una serie diversificata di dispositivi IoT distribuiti in tutta l'infrastruttura cablata e wireless[9]. Per gli ambienti non gestiti dal servizio HPE Aruba Networking Central basato su cloud o che utilizzano dispositivi di rete di terzi, **HPE Aruba Networking ClearPass Device Insight** fornisce un servizio di identificazione e profilazione dei client basato su ML.

Profilazione accurata fino al 99% per i dispositivi connessi alla rete, inclusi quelli IoT

Una volta identificato e profilato un utente o un dispositivo, il passo successivo prevede l'autenticazione della relativa identità ogni volta che si connette alla rete. Con **HPE Aruba Networking ClearPass**, gli utenti e i dispositivi possono essere autenticati rispetto a un'ampia varietà di provider di identità, come Active Directory. Grazie a un avanzato motore di gestione delle policy, che supporta i privilegi di accesso di precisione, ClearPass controlla gli utenti e i dispositivi autorizzati ad accedere alle varie risorse. Le policy seguono utenti e dispositivi in modo trasparente tra reti cablate, wireless e WAN, anche in ambienti multivendor.

Per le reti gestite da HPE Aruba Networking Central, la soluzione di controllo accesso di rete (NAC) cloud-native **Cloud Auth** consente l'onboarding senza attriti di utenti finali e dispositivi client tramite l'autenticazione basata su indirizzo MAC o tramite integrazioni con archivi di identità cloud comuni come Google Workspace™ o Azure Active Directory per assegnare automaticamente il giusto livello di accesso alla rete.

Per gli utenti che lavorano in modalità ibrida o da remoto, così come per i collaboratori esterni e i lavoratori temporanei e qualsiasi altra terza parte, la funzionalità **SSE HPE Aruba Networking Zero Trust Network Access (ZTNA)** si avvale di un broker di trust per limitare l'accesso solo alle specifiche applicazioni o ai microsegmenti approvati per l'utente in questione, come definito tramite una singola interfaccia globale per le policy. Il monitoraggio continuo garantisce che le policy si adattino automaticamente in base ai cambiamenti di identità, posizione e integrità dei dispositivi rendendo più facile garantire la sicurezza zero trust per ogni evento di accesso.

[9] Aruba Helps Network Teams Overcome Scarce Staff Resources with First AIOps Solution that Combines Network and Security Insights for Improved IT Efficiency. https://www.businesswire.com/news/home/20220726005426/en/Aruba-Helps-Network-Teams-Overcome-Scarce-Staff-Resources-with-First-AIOps-Solution-that-Combines-Network-and-Security-Insights-for-Improved-IT-Efficiency; AI-powered Network Infrastructure: The answer to IT Efficiency. https://www.arubanetworks.com/resource/ai-powered-network-infrastructure-the-answer-to-it-efficiency/

Segmentazione della rete

La soluzione **Dynamic Segmentation** di HPE Aruba Networking separa il traffico di rete in base alle identità e alle autorizzazioni di accesso associate, applicando il principio dei privilegi minimi per l'accesso a dati e applicazioni dall'edge al cloud. Dynamic Segmentation supporta due modelli di applicazione, centralizzata e distribuita, consentendo al personale IT di utilizzarne uno o entrambi in base alle esigenze dell'ambiente. L'applicazione centralizzata è garantita dal **Policy Enforcement Firewall**, un firewall applicativo completo incorporato nell'infrastruttura di rete HPE Aruba Networking.

Per l'applicazione distribuita inline all'interno dell'infrastruttura di gateway e switching, **HPE Aruba Networking Central NetConductor** di basa su una tecnologia ampiamente adottata, come EVPN/VXLAN, per produrre un overlay di rete distribuito. Questa soluzione full-stack comprende servizi di sicurezza cloud-native per la gestione globale di policy e la configurazione di rete con una semplice interfaccia basata su logica di business e flussi di lavoro intuitivi che i team di rete e sicurezza possono utilizzare per ottimizzare le prestazioni di rete definendo e applicando al contempo le policy di sicurezza granulari che rappresentano la base delle architetture zero trust.

Le organizzazioni possono inoltre utilizzare la piattaforma **SD-WAN HPE Aruba Networking EdgeConnect** per applicare policy di sicurezza coerenti a tutte le reti WAN e LAN, sfruttando le funzionalità NGFW end-to-end integrate, come IDS/IPS, la protezione dagli attacchi DDoS e la microsegmentazione a livello dell'intera azienda. I servizi NGFW integrati consentono di consolidare le reti e le funzioni di sicurezza delle filiali, eliminando i firewall e i router legacy in tali sedi.

All'interno del data center, **HPE Aruba Networking Fabric Composer** agevola l'implementazione della sicurezza zero trust, semplificando e automatizzando il processo di microsegmentazione tramite un'interfaccia utente grafica estremamente intuitiva. Lo **switch HPE Aruba Networking CX 10000** offre servizi inline di microsegmentazione distribuita, funzionalità di firewall est-ovest, crittografia e telemetria su ogni singola porta, in una posizione più vicina alle applicazioni enterprise critiche, evitando il ricorso a firewall aggiuntivi.

Il monitoraggio continuo di utenti e dispositivi sulla rete è un'altra best practice di sicurezza zero trust. Le soluzioni HPE Aruba Networking si integrano con oltre 150 soluzioni di sicurezza migliori della categoria all'interno di **Aruba 360 Security Exchange**, per fornire dati di telemetria provenienti da più origini consentendo di intervenire in tempo reale sulle minacce. Con la comunicazione bidirezionale tra la rete e l'ecosistema di sicurezza più ampio, le organizzazioni possono sfruttare i dati di rete non solo per acquisire visibilità e controllo sull'attività di utenti e dispositivi, ma anche per incrementare il valore dei loro investimenti.

Aggiornamenti software e configurazioni dei dispositivi

HPE Aruba Networking Central semplifica il flusso di lavoro di configurazione per i dispositivi gestiti consentendo agli amministratori di combinare una serie di dispositivi in gruppi. Con i gruppi, gli amministratori possono gestire i dispositivi in modo efficiente utilizzando un flusso di lavoro di configurazione basato su interfaccia utente o un modello di configurazione basato su interfaccia della riga di comando.

HPE Aruba Networking rende disponibili aggiornamenti sulla sicurezza e sulle prestazioni del software tramite il pluripremiato **portale di assistenza**.

Premio TSIA STAR Award 2023 per l'innovazione dei portali per clienti che migliorano la customer experience digitale

Gestione dei rischi

L'articolo 21 della Direttiva NIS2 stabilisce i requisiti delle misure di carattere tecnico, operativo e organizzativo per la gestione dei rischi posti alla cybersicurezza di sistemi informatici e di rete, oltre che per prevenire o ridurre al minimo l'impatto di incidenti di sicurezza[10].

Le soluzioni HPE Aruba Networking soddisfano i requisiti dell'articolo 21 riguardanti le misure di gestione dei rischi per la cybersicurezza con:

- sviluppo software sicuro
- sicurezza della supply chain
- crittografia e decrittografia
- sicurezza nell'acquisizione di sistemi informatici e di rete
- uso dell'autenticazione continua
- gestione degli incidenti
- continuità operativa
- generazione di report e risoluzione di vulnerabilità

Sviluppo software sicuro

HPE Aruba Networking adotta processi di sviluppo sicuri per ridurre le vulnerabilità, ottimizzando al contempo i costi e la disponibilità delle soluzioni. Lo sviluppo di prodotti in base a **Software Development Lifecycle e alle best practice del framework di sviluppo software sicuro** contribuisce a proteggere le organizzazioni da un'esposizione evitabile ai rischi.

- **Analisi dei requisiti:** analizza i rischi di sicurezza e imposta requisiti di alto livello.
- **Definizione:** esegui processi di modellazione e analisi delle minacce alla sicurezza.
- **Progettazione:** progetta con l'obiettivo di mitigare i rischi di sicurezza in base ai requisiti. Individua i componenti open source e di terze parti.
- **Scrittura di codice:** riutilizza componenti protetti. Implementa pratiche sicure di scrittura di codice. Esamina il codice e utilizza tool di analisi statica.
- **Test:** testa le funzionalità di sicurezza eseguendo scansioni, convalida degli input e test di penetrazione per ottenere una configurazione sicura.
- **Distribuzione:** firma in formato digitale il software (firma del codice) per verificare l'integrità del codice. Esegui scansioni per verificare l'eventuale presenza di malware e analizza il codice open source. Fornisci distinte base del software (SBOM).
- **Manutenzione:** pubblica i tuoi messaggi sul portale di assistenza HPE Aruba Networking. Applica le patch ed effettua la manutenzione delle versioni in base alle esigenze.

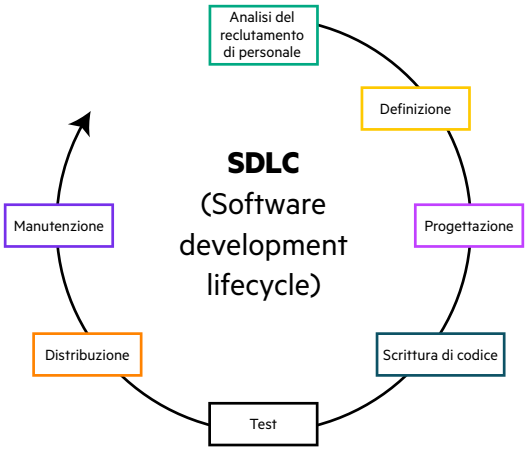

Figura 2. Software Development Lifecycle (SDLC)

[10] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2). Unione Europea.

Sicurezza della supply chain

HPE è l'azienda leader nel settore ICT per la cybersicurezza della supply chain. Le soluzioni HPE Aruba Networking vengono realizzate solo con SKU certificati per la **compliance a TAA**, riducendo la probabilità che i componenti hardware e software del prodotto siano stati manipolati da qualcuno in un Paese ostile.

Ai fini della compliance a TAA, i prodotti devono essere realizzati o trasformati in modo sostanziale negli Stati Uniti o in un Paese designato da TAA.[11])

Le soluzioni vengono fornite con una **distinta base del software** per la gestione del rischio dei componenti software. Con l'evoluzione delle minacce alla cybersicurezza, HPE Aruba Networking continua a identificare e mitigare i rischi all'interno della propria supply chain e a fornire prodotti sicuri alle organizzazioni in modo che possano concentrarsi sui loro obiettivi di business.

Sviluppo di una base sicura

Le soluzioni HPE Aruba Networking sono state certificate e/o convalidate con i rigorosi standard del governo degli Stati Uniti, a dimostrazione di caratteristiche di **crittografia controllata** e resistenza agli attacchi. Le soluzioni HPE Aruba Networking sono state valutate e autorizzate per l'uso in compliance agli obblighi di cybersicurezza degli Stati Uniti e a programmi come Common Criteria, FIPS-140, DoDIN-APL e USGv6, confermando che soddisfano requisiti di sicurezza rigorosi.

L'infrastruttura HPE Aruba Networking è stata scelta per reti classificate e non classificate all'interno del Pentagono, quartier generale del Dipartimento della Difesa USA, supportando decine di migliaia di dispositivi ogni giorno. Il Pentagono sta inoltre estendendo la distribuzione di ClearPass Policy Manager per il controllo accesso di rete sicuro[12].

Per la protezione da codice di avvio dannoso e attacchi con impersonificazione di dispositivi, le soluzioni di rete cablate e wireless di HPE Aruba Networking utilizzano la **tecnologia TPM (Trusted Platform Module)**, uno standard internazionale per un crittoprocessore sicuro e resistente alle manomissioni progettato per proteggere l'hardware integrando chiavi crittografiche nei dispositivi. Installata durante la produzione, la tecnologia dei chip TPM può fornire una root of trust sicura a cui aggiungere ulteriori livelli di sicurezza zero trust e SASE (Secure Access Service Edge).

Per impedire agli AP rogue di acquisire l'accesso backdoor alla rete e intercettare i dati degli utenti, HPE Aruba Networking Central offre funzionalità avanzate di **prevenzione delle intrusioni wireless**. I team di rete e sicurezza possono impostare regole personalizzate per il rilevamento di AP rogue in base a specifiche soglie di rischio.

Generazione di report e risoluzione di vulnerabilità

HPE Aruba Networking Threat Labs gestisce e mitiga le vulnerabilità della sicurezza all'interno dei prodotti HPE Aruba Networking. Le vulnerabilità possono essere riferite da ricercatori indipendenti di sicurezza, clienti o anche dipendenti di HPE Aruba Networking. HPE Aruba Networking gestisce anche un programma di ricerca di bug per scoprire più rapidamente le vulnerabilità.

[11] Federal Acquisition Regulation: 52.225-5 Trade Agreements. Governo degli Stati Uniti. https://www.acquisition.gov/far/52.225-5.

[12] The Pentagon Modernizes Wired and Wireless Connectivity, Across All Classification Levels, with Aruba Infrastructure. https://www.businesswire.com/news/home/20201026005079/en/The-Pentagon-Modernizes-Wired-and-Wireless-Connectivity-Across-All-Classification-Levels-with-Aruba-Infrastructure. Ottobre 2020.

Continuità operativa

Le piattaforme di rete e gestione di HPE Aruba Networking offrono un'ampia gamma di funzionalità di resilienza progettate per supportare operazioni con interruzioni minime, un maggiore uptime di rete, tra cui failover hitless, upgrade del software durante l'esecuzione, upgrade del software ottimizzati per VSF, upgrade live e architettura a disponibilità elevata.

Integra le soluzioni HPE Aruba Networking con HPE GreenLake Disaster Recovery and Backup as-a-service, un prodotto per proteggere carichi di lavoro on-premise e cloud-native da attacchi di ransomware con backup crittografati, e HPE Services, che ti aiuta a configurare policy per la gestione di sicurezza e rischi dei sistemi informatici su misura per la tua organizzazione.

Conclusioni

Senza un approccio strategico alla semplificazione e alla collaborazione, può essere difficile adempiere agli obblighi di compliance a NIS2. Con la rete basata sull'AI security-first di HPE Aruba Networking, la rete può diventare un asset per l'organizzazione che aiuta i team a realizzare obiettivi condivisi per la sicurezza, la privacy e la compliance.

Ulteriori informazioni alla pagina https://www.arubanetworks.com/products/security/

Risorse aggiuntive

HPE supply chain security innovation: Enhancing trust and resilience from edge to cloud

Politica di risposta agli incidenti di sicurezza dei prodotti | HPE Aruba Networking

Formazione e certificazione sulla sicurezza informatica | HPE Services - Education

Prendi la decisione d'acquisto giusta.
Contatta i nostri specialisti della prevendita.

Contattaci

Visita **ArubaNetworks.com**

BWP_NIS2Compliance_RVK_020224 a00137587ite

Hewlett Packard Enterprise