**E-Mail – Hardening Guide**

**Oggetto:** Rafforzate la sicurezza della vostra rete con 2N Hardening Guide

**Preheader:** Scarica

Gentile [Nome del destinatario],

nell'attuale panorama della cybersecurity in rapida evoluzione, **garantire la sicurezza dei dispositivi basati su IP non è più facoltativo, è essenziale.** Con minacce informatiche sempre più sofisticate, la necessità di salvaguardare i sistemi non è mai stata così urgente.

Per aiutarvi a essere all'avanguardia vi offriamo la 2N Hardening Guide, una risorsa completa che illustra le best practice fondamentali per migliorare la sicurezza dei dispositivi di rete 2N.

Sia che si tratti di gestire dispositivi in un ambiente ad alta sicurezza come quello sanitario o governativo, sia che si voglia semplicemente proteggere un edificio residenziale o multifunzionale, queste raccomandazioni sono pensate per ridurre al minimo le vulnerabilità e rafforzare le difese.

**Cosa imparerete**

* **Impostazione di password forti:** Stabilire credenziali solide per impedire l'accesso non autorizzato.
* **Aggiornamenti regolari del firmware:** Aggiornare le vulnerabilità conosciute per essere sempre al passo con le minacce.
* **Protocolli di comunicazione sicuri**: Garantire una comunicazione sicura tra i dispositivi.
* **Abilitazione della crittografia:** Proteggere i dati sensibili durante la trasmissione.
* **Disabilitare i servizi non necessari:** Ridurre al minimo le superfici di attacco potenziali.
* **Limitare l'accesso alla rete:** Ridurre l'esposizione limitando l'accesso agli utenti fidati.
* **Segmentazione della rete**: Isolare i dispositivi critici dal traffico di rete più ampio per migliorare la sicurezza.

Non aspettate che si verifichi una violazione. Informatevi e proteggete subito il vostro sistema. La 2N Hardening Guide è una risorsa essenziale per mantenere una rete solida e sicura.

[Scarica]

Cordiali saluti,

**Banner - articolo di tendenza**

La visione di 2N sulla direttiva NIS2

Ricevete sempre più domande sull'imminente direttiva NIS2 dell'UE e sul suo impatto sulle aziende? Scoprite cosa significa, quali sono i suoi effetti e come 2N, fornitore leader di sistemi di controllo degli accessi, si sta preparando ad affrontarla in questo articolo di approfondimento.

>>Continua a leggere

**NIS2 – Trend Article**

**La strada verso la sicurezza digitale: uno sguardo alla direttiva NIS2 dell'UE**

**Le minacce informatiche e la risposta europea**

La crescente digitalizzazione non porta solo progresso. Comporta anche un rischio crescente: gli attacchi informatici. Per affrontare questo problema, nel 2016 l'Unione europea ha introdotto la direttiva NIS (Network and Information Security). L'obiettivo era quello di rafforzare la sicurezza informatica in settori strategici ed essenziali: in particolare energia, trasporti, banche, mercati finanziari, sanità, acqua e infrastrutture digitali.

Da allora, tuttavia, si sono verificati cambiamenti fondamentali nella società, in particolare dopo la COVID. La diffusione massiccia di strumenti di videoconferenza (come MS Teams, Zoom o Google Meet) e l'aumento della domanda di e-commerce e di servizi di consegna hanno intensificato la transizione verso il mondo digitale. Secondo McKinsey, infatti, la pandemia ha accelerato la digitalizzazione di 3-4 anni. Questi sviluppi hanno comportato nuove sfide per la sicurezza informatica e l'UE ha dovuto aggiornare la propria direttiva.

**NIS2: regole più severe per un mondo più sicuro**

L'UE ha adottato la nuova direttiva NIS2 nel novembre 2022. Questa direttiva amplia in modo significativo l'ambito di applicazione della legislazione originale e rende più severe le misure di sicurezza. Oltre ai sette settori originari, la NIS2 copre ora nuove aree come la produzione, i servizi postali e di corriere, la scienza, la ricerca e l'istruzione.

La NIS2 richiede alle aziende e alle organizzazioni di tutti questi settori di identificare e gestire i rischi informatici, di proteggere i sistemi informatici e di formare regolarmente il personale. Uno dei nuovi regolamenti prevede addirittura l'obbligo di segnalare gli incidenti di sicurezza gravi entro 24 ore dalla scoperta, con una relazione dettagliata entro 72 ore e una relazione finale entro 30 giorni.

La direttiva divide inoltre le organizzazioni in due categorie: entità “essenziali” e “critiche”, con obblighi specifici per ciascuna categoria. Le sanzioni per la mancata osservanza delle norme possono essere molto severe. Le entità essenziali rischiano multe fino a 10 milioni di euro o al 2% del fatturato mondiale annuo, se superiore. Le entità principali possono essere multate fino a 7 milioni di euro o all'1,4% del fatturato.

Il NIS2 svolge quindi un ruolo fondamentale nel garantire la sicurezza informatica in tutta l'UE. L'organizzazione si impegna a introdurre nuove misure e a rispettare regole rigorose per proteggere le infrastrutture critiche come le reti energetiche, l'acqua e la sanità. Ciò garantisce che i servizi essenziali su cui i cittadini fanno affidamento rimangano funzionanti e sicuri in caso di attacco informatico.

**Come si sta preparando 2N per il NIS2?**

2N deve essere conforme al NIS2: si qualifica come soggetto obbligato (oltre 250 dipendenti e un fatturato annuo superiore a 10 milioni di euro) e rientra in diversi settori regolamentati come “Fabbricazione di dispositivi e apparecchiature elettroniche”, “Fornitura di servizi di comunicazione elettronica accessibili al pubblico” e anche “Fornitore di servizi di cloud computing”.

L'azienda è da tempo attiva sul tema della cybersecurity e possiede la certificazione ISO 27001, che mantiene regolarmente negli audit di sorveglianza e ricertificazione. Quest'anno, 2N ha ottenuto anche la certificazione di sicurezza IEC 62443-4-1, che si applica ai suoi prodotti per ascensori.

Ma qual è il prossimo passo? 2N deve rispettare le rigide norme NIS2 e rivedere in modo approfondito e regolare le misure di sicurezza esistenti. Per questo motivo, sta conducendo un'analisi delle lacune per determinare quali obblighi NIS2 siano già soddisfatti (grazie alla certificazione ISO 27001) e quali debbano ancora essere implementati. Essendo la sicurezza informatica una delle principali priorità di 2N, l'azienda si aspetta che la conformità ai restanti requisiti avvenga senza problemi ed entro i termini previsti dalla legge. Potete essere certi che scegliendo 2N non rischiate la non conformità alle direttive UE.

**Conoscenza, fiducia e trasparenza: valori chiave**

2N si avvale da tempo della vasta conoscenza ed esperienza in materia di cybersecurity della sua società madre AXIS. Gli esperti di entrambe le aziende sono in contatto quotidiano e condividono le migliori pratiche e idee per uno sviluppo sicuro.

Uno degli strumenti chiave adottati da 2N è l'Axis Security Development Model (ASDM), che delinea 13 processi e pratiche di sicurezza incentrati sull'implementazione (e la successiva verifica) delle misure di sicurezza in ogni fase di sviluppo. Questo approccio riduce al minimo il rischio di incidenti di sicurezza e rafforza la fiducia e la soddisfazione dei clienti.

La fiducia e la trasparenza tra l'azienda e i suoi clienti sono valori fondamentali per 2N. L'azienda pubblica tutti i materiali e le informazioni relative alla sicurezza informatica sul proprio sito web, il che non solo garantisce la sicurezza dei suoi prodotti e servizi, ma rafforza anche la vostra fiducia nella loro affidabilità.