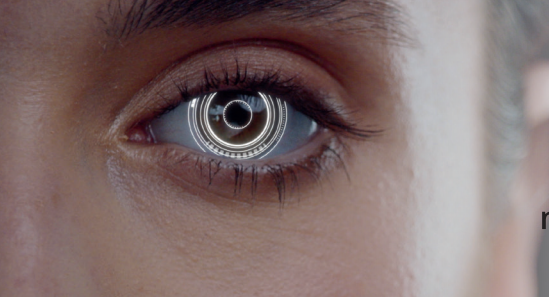

SafeAccess

La chiave per prepararsi alle nuove sfide normative della NIS2

Namirial

Le sfide: i 10 punti di intervento della NIS2

La NIS2 è la **nuova direttiva europea sulla cybersecurity** che punta a rafforzare la sicurezza informatica nell'UE. Entrata in vigore il 17 gennaio 2023, la direttiva **dovrà essere recepita** dai singoli Stati membri **entro il 17 ottobre 2024.**

1) RISK MANAGEMENT
Adottare misure per identificare, valutare e gestire i rischi legati alla sicurezza delle informazioni e delle infrastrutture digitali.

2) GESTIONE E SEGNALAZIONE INCIDENTI
Adottare misure per prevenire, rilevare e rispondere agli incidenti di sicurezza informatica, attraverso sistemi di monitoraggio continuo delle reti e piani di risposta agli incidenti.

3) CONTINUITÀ DI BUSINESS
Sviluppare piani di continuità operativa e di ripristino in caso di incidenti. Garantire la resilienza dei sistemi informativi per ridurre al minimo le interruzioni e assicurare un rapido recupero.

4) SUPPLY CHAIN
Garantire che i fornitori e i partner adottino misure di sicurezza adeguate. Le relazioni contrattuali devono prevedere obblighi specifici per la gestione dei rischi legati alla sicurezza informatica.

5) SICUREZZA DEI SISTEMI
Mettere in sicurezza tutti gli asset informatici in dotazione all'azienda, anche se forniti da terze parti, in ogni fase, dallo sviluppo all'utilizzo in campo.

6) GOVERNANCE E RESPONSABILITÀ AZIENDALE
Aumentare il coinvolgimento del top management nelle decisioni sulla sicurezza informatica. Il personale dirigente ha la responsabilità legale di garantire che siano adottate le misure necessarie per la conformità alla direttiva.

7) FORMAZIONE DEL PERSONALE
Realizzare programmi di formazione continua per il personale, al fine di aumentare la consapevolezza sui rischi di sicurezza informatica e di riconoscere tentativi di phishing, truffe e altri attacchi informatici.

8) USO DELLA CRITTOGRAFIA
Fare ricorso all'utilizzo di crittografia informatica per l'accesso ai sistemi e alla cifratura di dati per garantire la sicurezza delle reti e dei sistemi informativi.

9) SICUREZZA DEL PERSONALE
Implementare politiche di controllo accessi ai sistemi informatici, basato su autenticazione forte e uso di certificati digitali, seguendo il principio del minimo previlegio, l'accesso basato su ruoli e l'auditing degli accessi.

10) AUTENTICAZIONE MULTI-FATTORIALE
Fare uso di soluzioni di autenticazione a più fattori, o di autenticazione continua, non solo per l'accesso ai sistemi interni delle organizzazioni ma anche per i servizi agli utenti finali, in particolare nei settori essenziali edimportanti che trattano informazioni sensibili di terzi.

Date importanti

7 AGOSTO 2024
DECRETO DI RECEPIMENTO

FEBBRAIO DI OGNI ANNO
ISCRIZIONI IN PIATTAFORMA

18 OTTOBRE 2024
ENTRATA IN VIGORE DELLA NIS2

APRILE DI OGNI ANNO
DEFINIZIONE ELENCO NAZIONALE

Sanzioni Economiche

€10M o il 2% del fatturato consolidato globale, se superiore, per i soggetti essenziali.

€7M o l'1,4% del del fatturato consolidato globale, se superiore, per i soggetti importanti.

Da **€10K a €125k per le Pubbliche Amministrazioni**

Sanzioni Amministrative

Sospensione temporanea di attività o servizi

Revoca di autorizzazioni o licenze per alcuni settori

Responsabilità della governance aziendale: sospensione o il **divieto temporaneo** a qualsiasi persona che svolga funzioni dirigenziali di svolgere le suddette funzioni in quel soggetto.

SafeAccess è la suite completa per l'autenticazione senza password che permette di risponde ai requisiti della **NIS2**. E' la soluzione più efficiente per superare i problemi di sicurezza, ridurre i tempi e i costi della manutenzione IT.

WORKFORCE

Proteggi il personale della tua organizzazione adottando meccanismi di protezione sui sistemi, dalle singole macchine alle applicazioni

- Possibilità di installazione on Premises per un'integrazione completa e perfetta con MS Active Directory
  (*Disponibile anche per versioni cloud come Azure AD)*
- Protezione delle postazioni di lavoro grazie al Credential Provider
- Proteggi l'accesso alle applicazioni con Enterprise SSO per applicazioni Web, desktop e legacy senza sviluppi applicativi

CUSTOMER

Garantire facilità di adozione e implementazione delle soluzioni di Autenticazione Multi-Fattoriale per tutti i tuoi clienti

- Full Cloud così che il cliente non debba preoccuparsi della gestione del server
- Integrazione semplice grazie all'utilizzo delle API
- Ampio portafoglio di metodi di autenticazione a più fattori

Autenticazione Multi-Fattoriale per ogni caso d'uso

TOKEN

Un dispositivo portatile per archiviare in sicurezza informazioni crittografiche, facile da portare con sé.

SMARTCARD/BADGE

Un dispositivo pratico, grande come una carta di credito, con microchip per archiviare e processare dati.

SMS/OTP

Strumento versatile a portata di mano per l'accesso con codici temporanei via smartphone.

MOBILE APP

Soluzione di autenticazione tramite smartphone con biometria (impronta digitale, riconoscimento facciale.

FIDO DEVICE

Dispositivo certificato FIDO (smartcard o token), in possesso dell'utente o fornito dall'amministratore IT.

Namirial S.p.A. | Via Caduti sul Lavoro n. 4 | 60019 Senigallia (AN) | Italia | www.namirial.com