Namirial

GO Passwordless

Multi-factor authentication made easy

fido ALLIANCE

fido CERTIFIED

Un po’ di rassegna stampa

Presunto attacco informatico al comune di Padova. Credenziali in vendita nelle underground

Redazione RHC - 26/10/2022

Sicuramente tutto questo ci riporta indietro di qualche mese fa all’attacco alla ULSS6 Euganea di Padova, ma questa a quanto pare è un’altra storia. Pare

Sono in arrivo gli Amazon delle credenziali aziendali compromesse!

Redazione RHC - 27/12/2022

Gli analisti di KELA riferiscono che ci sono almeno 225.000 account di posta elettronica in vendita sul dark web. Allo stesso tempo, puoi acquistare l’accesso alla posta aziendale

1.137.893 di account di Libero nelle underground. Abilitate la Multi Factor Authentication!

Redazione RHC - 31/01/2023

Il disservizio che ha coinvolto Libero e Virgilio negli ultimi giorni, ci ha portato all’attenzione quanto siano fragili le autenticazioni con utenza e password e

DarkTracer: credenziali di 140 istituzioni italiane in una colossale collection di 49.000 istituzioni.

Redazione RHC - 08/03/2022

Darktracer, una nota azienda di intelligence delle minacce, riporta sul suo profilo twitter un post che descrive una violazione colossale di 1,753,658 credenziali, relative a

Attacco informatico ad Exprivia. Engineering scrive a RHC fornendo la versione dei fatti

Redazione RHC - 08/03/2023

A seguito della diffusione della notizia riportata in precedenza, sull’attacco in supply-chain ad Exprivia, ci ha contattato prontamente Engineering riportando la propria versione dei fatti.

Fonte: https://www.redhotcyber.com/

Il problema delle Password

La **Password** rappresentano oggigiorno ancora il sistema più diffuso per l'autenticazione a postazioni e agli applicativi (web e desktop), anche se vulnerabili a **tecniche di hacking**: **sniffing, brute force, keylogger, ecc.**

CONTESTO

- Passaggio da lavoro full-site (in cui si da rilevanza alla sicurezza dell'edifico) a **flessibilità** e **smart working** (spostando il focus sulla sicurezza del singolo utente)
- Tutela dei **dati sensibili** in possesso delle aziende, con personale geograficamente distribuito.
- Presenza di **postazioni condivise** (es. strutture ospedaliere e universitarie).
- La sicurezza informatica è principalmente un argomento dell'IT, è qualcosa legato ai valori fondamentali e al marchio dell'azienda.

PROBLEMI

BASSA SICUREZZA

- **Password semplici**
  ⇨ deboli contro brute force
- Password complesse, ma scritte su **post-it** o su note
  ⇨ semplici da leggere
- Stessa password utilizzata **su più applicazioni**
  ⇨ compromesse tutte le applicazioni
- Postazioni **condivise**
  ⇨ deboli contro keylogger.

SOVRACCARICO DEL REPARTO IT

- All'aumentare della complessità delle password aumenta anche la probabilità che queste vengano **dimenticate**
  ⇨ **sovraccarico** delle attività del reparto IT per lo sblocco delle postazioni e degli applicativi

COMPLIANCE NORMATIVA

- Direttiva europea NIS2 sulla **tracciabilità degli accessi** ai dati sottoposti alla protezione della privacy.

OBIETTIVO

Risolvere tutti i problemi legati agli accessi con un sistema semplice, intuitivo, economico e soprattutto **FACILMENTE INTEGRABILE**

- Gli utenti non rischiano di subire il furto di dati presenti nelle workstation o nelle applicazioni, lavorando **in sicurezza dovunque**
- E' possibile identificare con **MAGGIORE CERTEZZA** chi fa uso di una credenziale.
- Si riducono le attività e lo stress dei reparti IT

Autenticazione Multifattoriale

Una autenticazione **MULTIFATTORIALE** consiste nell'utilizzo di credenziali semplici come username e password con l'aggiunta di un ulteriore metodo di autenticazione fisico. La sicurezza è infatti fornita dall'unione dei due fattori: qualcosa che sai e qualcosa che hai.

Per utilizzare l'autenticazione **MULTIFATTORIALE** è sufficiente dotarsi di dispositivi a **crittografia asimmetrica**, che sono gli unici a garantire il massimo livello di sicurezza.

Token

Un dispositivo portatile per archiviare in modo sicuro le informazioni crittografiche, che l'utente può facilmente portare sempre con sé.

Smartcard /Badge

Un pratico dispositivo con le dimensioni di una carta di credito, che usa un piccolo microchip per archiviare e processare dati.

SMS/TOTP

Uno strumento versatile e sempre a portata di mano per accedere con codici temporanei tramite l'utilizzo di smartphone.

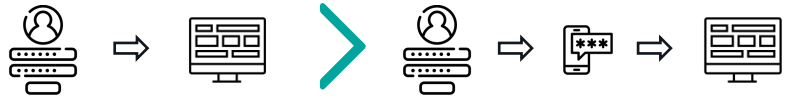
Mobile App

Una soluzione che permette agli utenti di autenticarsi con lo smartphone, grazie a funzioni biometriche come impronta digitale, riconoscimento facciale, etc.

fido™ device

Un dispositivo certificato FIDO (smartcard o token), già in possesso dell'utente per suo uso personale oppure fornito dall'amministratore IT.

L'utente non vedrà uno sconvolgimento del flusso di autenticazione; l'access agli applicativi avviene con i meccanismi finora adottati, con l'unica differenza che vedrà uno step relativo al secondo fattore di autenticazione



- L'utente inserisce username e password
- ***New*** L'utente deve eseguire un'azione:
  - inserire il codice SMS
  - inserire il codice di un Authenticator
  - accettare la notifica push
  - ...
- L'utente entra nel sistema

PROTEZIONE PER

CUSTOMER

Garantire facilità di adozione e implementazione delle soluzioni SafeAccess per tutti i tuoi clienti

SCA (Strong Customer Authentication)

IDP / SSO (Single Sign-On)

Integrazione semplice grazie all'utilizzo delle API

WORKFORCE

Proteggi la tua organizzazione adottando meccanismi di protezione sui sistemi utilizzati dai tuoi utenti, dalle singole macchine alle applicazioni

Autenticazione della WORKSTATION

Autenticazione degli APPLICATIVI

Credential Lifecycle Management

LOG collector

SIEM

Workforce CMS Centralizzato

Registrazione MFA da parte dell'Admin (IT administrator / HR)

NamirialSafeAccess

Workforce CMS Self-enroller

Registrazione MFA da parte dell'utente in autonomia

NamirialSafeAccess

Workforce Login automatizzato (Enterprise-SSO)

Accesso agli applicativi con un click e senza inserimento manuale delle credenziali

NamirialSafeAccess

Workforce RDP authentication

Accesso al Desktop Remoto con autenticazione multifattoriale

NamirialSafeAccess

Customer SSO authentication

Accesso agli applicativi in Single Sign-On con FIDO

NamirialSafeAccess

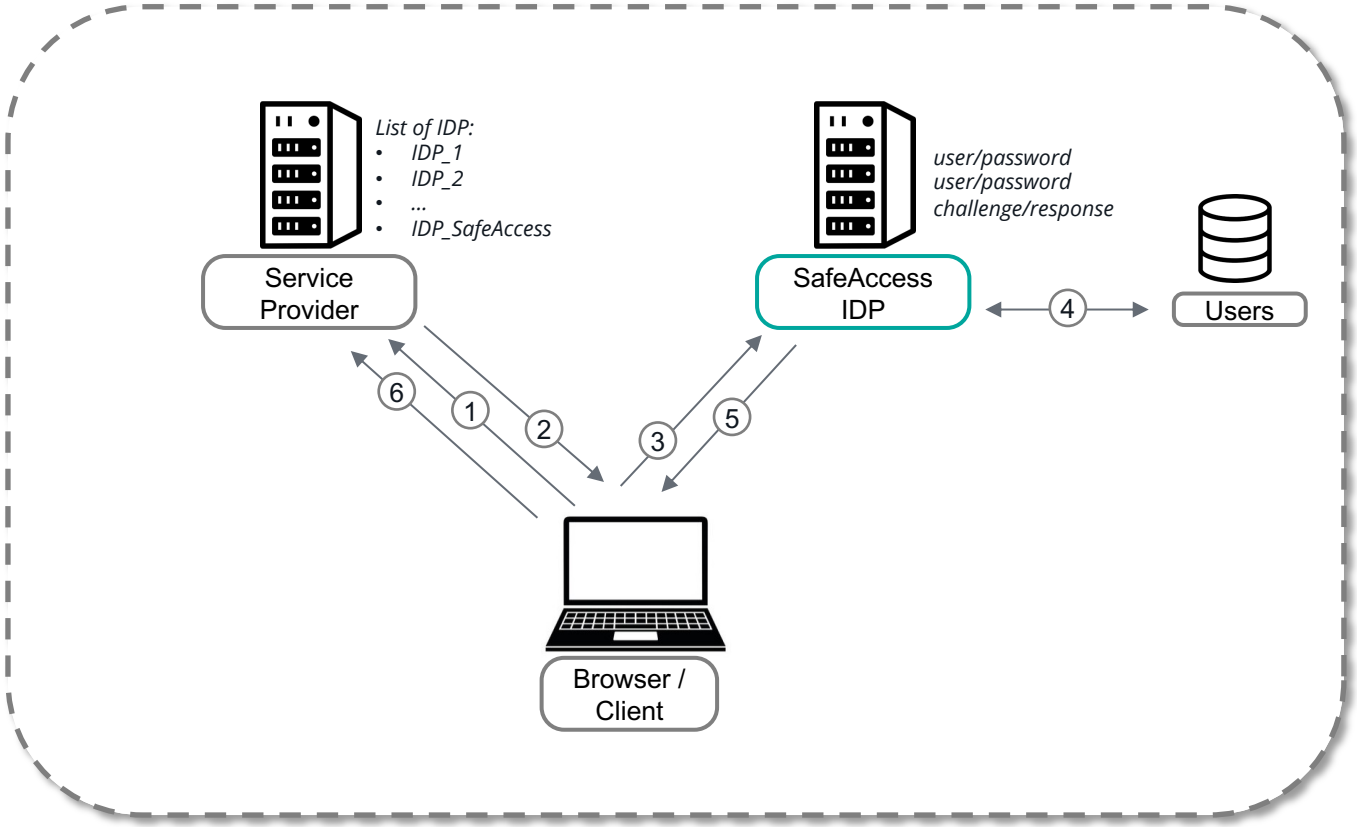
Architecture: Customer (IDP) components

- **Identity Provider (IDP)**
  is the component responsible of authenticate the user, based on its own database, giving the access to all the customer applications (service providers) through standard communication protocols (SAML, OIDC).

The customer has the possibility to integrate all the existing services to the IDP through:

- **Service Provider**
  the customer shows the list of IDPs that are responsible of authenticating the users

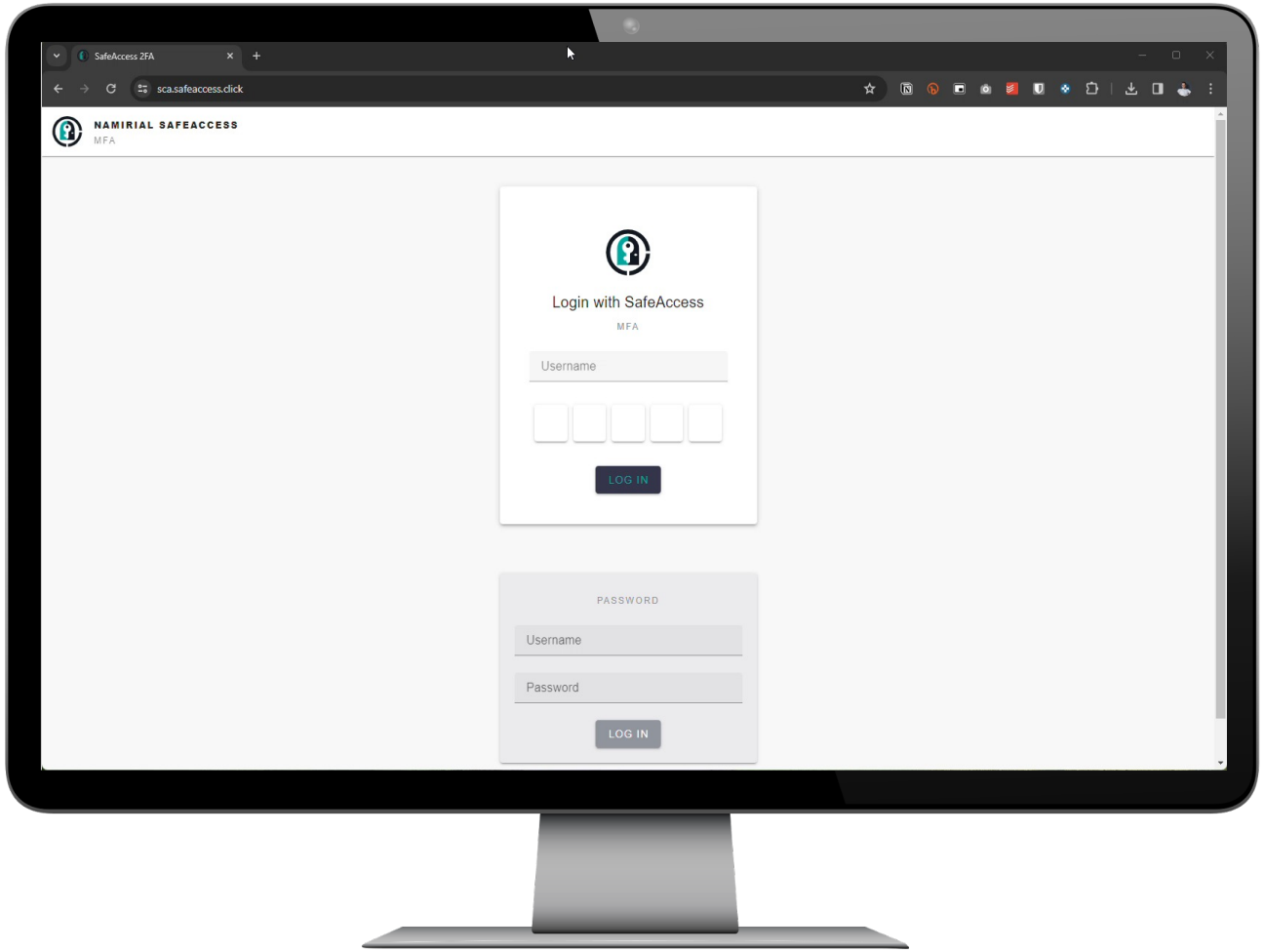
- **Client**
  the application that uses the exposed services



1. The Browser/Client wants to access to the Service and select the IDP for authentication
2. The Service Provider redirects to the IDP using SAML/OIDC
3. The Browser/Client executes the authentication on the IDP with one of the allowed methods
4. The IDP check if the user exists and perform all the verification steps
5. The IDP return the authentication token to the Browser/Client
6. The Browser/Client shares the token with the Service Provider, that allows the access

Customer: Biometric SCA Authentication

Something the user has (the phone) and is (the biometric data)



NamirialSafeAccess

Use case

Health sector| **Hospital agency “Papa Giovanni XXIII”**

- **Postazioni di lavoro condivise**

L'Azienda Ospedaliera “Papa Giovanni XXIII” di Bergamo aveva bisogno di una soluzione per risolvere i problemi legati ai frequenti cambi di password e all'accesso sicuro alle postazioni di lavoro. Lavorando su turni, il personale sanitario è tenuto a cambiare costantemente le password per motivi di sicurezza. Inoltre, molti operatori lavorano su postazioni condivise, per cui più utenti devono accedere allo stesso PC, ognuno con la propria area di lavoro.

- **Utilizzo degli stessi badge già in uso**

Con SafeAccess, Namirial ha permesso agli operatori sanitari di utilizzare una smartcard con firma digitale (rilasciata dalla Regione Lombardia) e il proprio badge identificativo (rilasciato dall'ente stesso) come dispositivo unico per accedere a tutti i servizi e le postazioni di lavoro: i dipendenti possono ora utilizzare lo stesso badge per accedere al parcheggio, alla mensa, ai PC e alle oltre 50 applicazioni in uso nella struttura nella massima sicurezza e nel pieno rispetto della privacy.

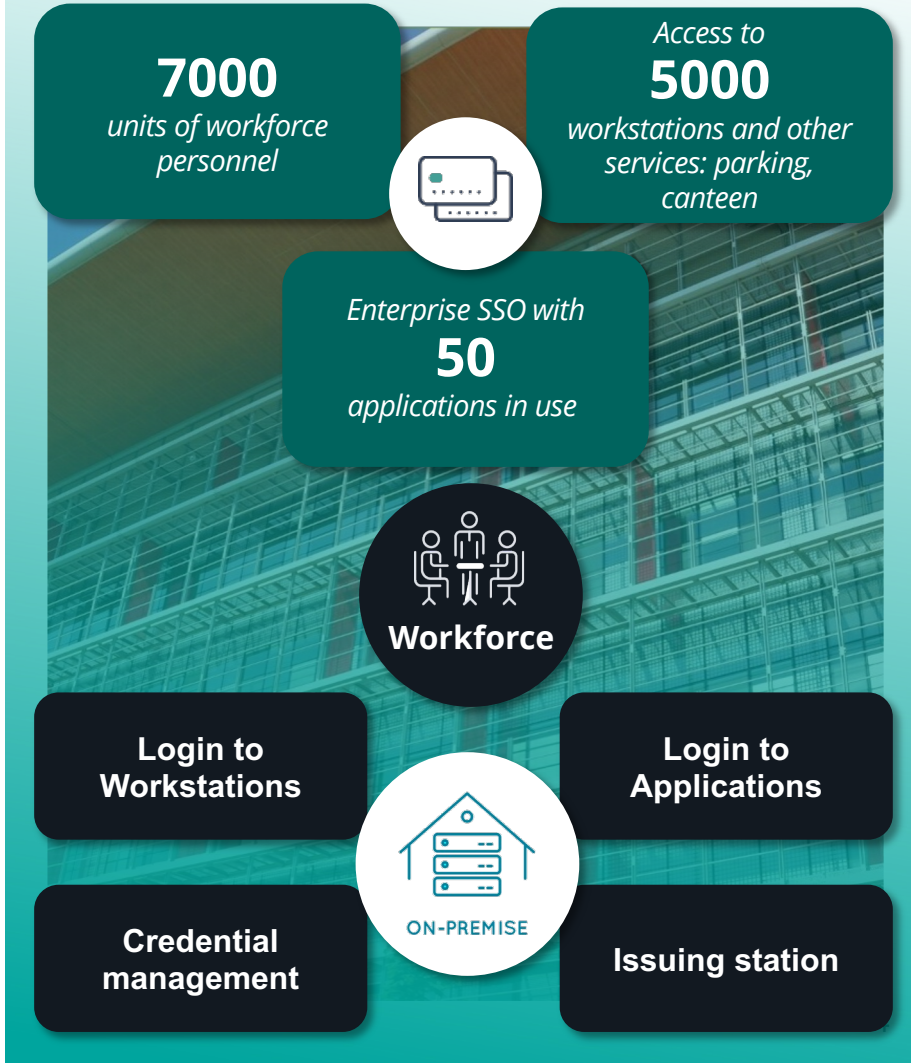
- **Metodi di fallback per garantire la continuità**

SafeAccess ha permesso all'ospedale di eliminare per sempre i costi legati alla gestione del reset delle password e ha garantito una soluzione in caso di eventi imprevisti: ad esempio, se i dipendenti perdono il badge, hanno a disposizione una postazione di riferimento per l'emissione di un badge temporaneo che permette la continuità lavorativa in ospedale.

- **Conformità alle normative vigenti in materia di privacy**

SafeAccess di Namirial ha aiutato gli “Ospedali Riuniti di Bergamo” a diventare un fiore all'occhiello nel campo della sicurezza degli accessi e dell'efficienza nella gestione delle risorse umane, garantendo un accesso sicuro, facile e veloce alle postazioni di lavoro..

Azienda Ospedaliera
Papa Giovanni XXIII
Bergamo



- **Autenticazione federata ai servizi per i cittadini**

La Regione Veneto ha deciso di ampliare il proprio portafoglio di servizi e ha quindi richiesto una serie di soluzioni in grado di garantire l'interazione con essi e la facilità d'uso per gli utenti. Il primo componente richiesto è un IDP SAML federato all'interno delle ASL della Regione Veneto per l'accesso dei cittadini e degli operatori ai portali sanitari locali.

- **Autenticazione centralizzata allo IAP per medici e operatori**

La soluzione è composta anche da una IAP con un duplice scopo. Una è la connessione di medici e operatori ai servizi sanitari, utilizzando un'autenticazione federata che verifica l'autorizzazione sui LDAP dell'AULSS, consentendo l'accesso con un'unica credenziale.

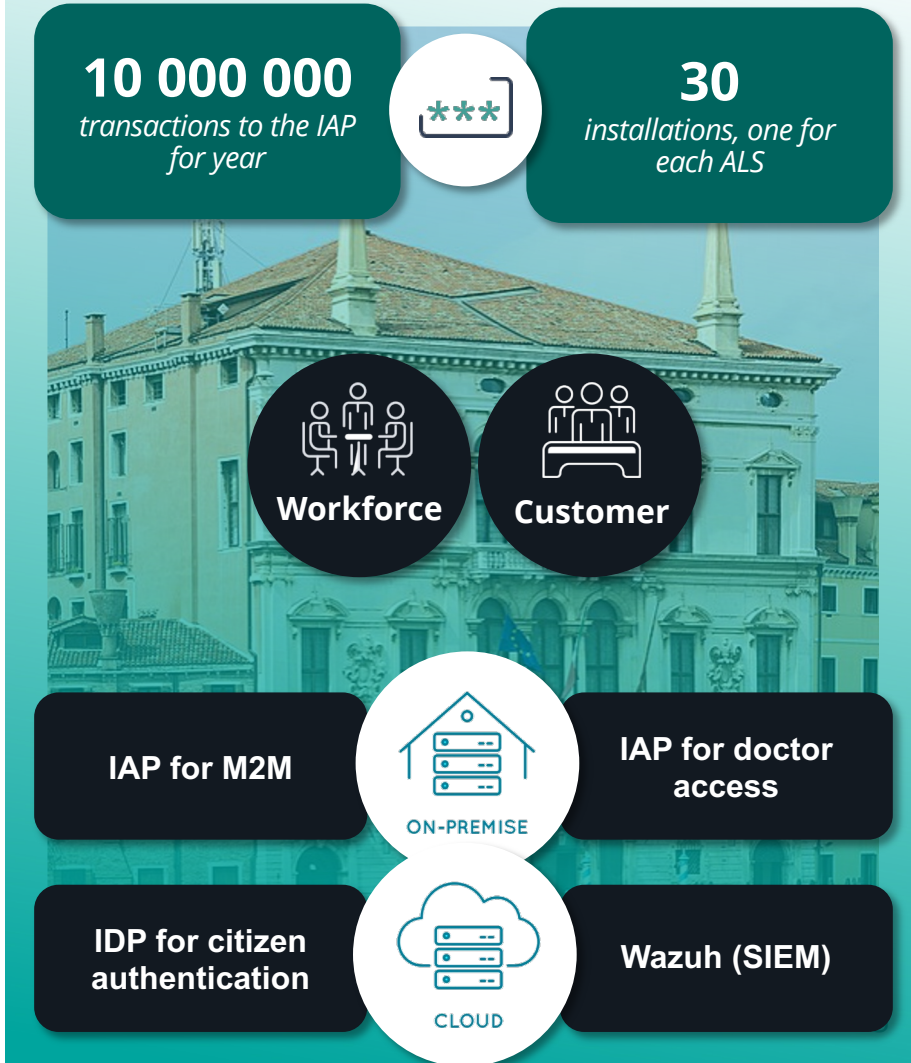
- **Autenticazione machine-to-machine per i server**

Un altro scopo importante è quello di consentire l'autenticazione Machine-To-Machine (M2M) tra i servizi dell'AULSS e il server IAP che verifica l'accesso e fornisce l'accesso ai dati sanitari centralizzati disponibili su un server regionale (utilizzato per i batch periodici o le interrogazioni tra i sistemi). La soluzione è stata fornita on-premise e installata nel centro dati distribuito per la regione.

- **Un portale “to rule them all”**

Il SIO (Sistema Informativo Ospedaliero) è il portale, federato con le modalità sopra descritte, dove tutti possono accedere alle informazioni sanitarie personali grazie alle soluzioni fornite.

REGIONE DEL VENETO



Prepararsi alla NIS2

Perché l'Identity Trust è la chiave per prepararsi alle nuove sfide normative

Che cos'è la NIS2

Nel gennaio 2023 la direttiva europea 2022/2555, nota come ***NIS2*** (acronimo di *Network and Information Systems*), è entrata in vigore a tutti gli effetti, aggiornando la precedente direttiva 2016/1148.
La direttiva ha come obiettivo principale raggiungere un livello comune elevato in materia di sicurezza delle reti e dei sistemi informativi in tutta l'UE, aumentando la resilienza degli stessi ma soprattutto creando un quadro comune per la notifica degli incidenti informatici e la **salvaguardia dei dati personali di terzi**.
Gli Stati membri avranno tempo fino al **ottobre 2024** per trasporre la Direttiva NIS2 nell'ordinamento nazionale.

La NIS2 estende i settori coperti dalla prima direttiva NIS individuando un numero di settori **essenziali** ed **importanti** per la continuità di business e per l'erogazione di servizi ai cittadini UE.

Settori coperti dalla prima direttiva NIS	Settori **aggiuntivi** coperti dalla NIS2
• Sanità • Infrastruttura digitale • Trasporti • Approvvigionamento idrico • Provider di servizi digitali • Settore bancario • Infrastruttura del mercato finanziario • Energia *Nero = Entità Essenziali* *Verde = Entità importanti*	• Provider di reti o servizi di comunicazione elettronica pubblica • Acque reflue • Prodotti chimici • Salute (farmaci, R&S, dispositivi medici critici) • Produttori, aziende di trattamento e distributori di prodotti alimentari • Fabbricazione di prodotti critici (dispositivi medici, computer, elettronica, veicoli a motore) • **Provider di servizi digitali essenziali alla continuità di business** • Spaziale • Servizi postali e corrieri espresso • Amministrazione pubblica

A differenza della prima direttiva NIS, i requisiti di sicurezza informatica individuate nella NIS2 si applicano non solo alle organizzazioni impattate, **ma anche ai subappaltatori e ai fornitori di servizi di queste**.

Namirial | © Namirial – All rights reserved

Che cosa prevede la NIS2

L'**articolo 21** della direttiva NIS2 impone agli stati membri di garantire che le entità **essenziali** e **importanti** gestiscano il rischio di attacchi informatici mediante l'attuazione di sistemi, politiche e *best practice* che coprano un'ampia gamma di misure e discipline di sicurezza informatica, tra cui:

- Politiche di analisi dei rischi e sicurezza dei sistemi informativi
- Gestione e segnalazione degli incidenti
- Continuità operativa, come la gestione del backup e il ripristino di emergenza
- Gestione della crisi
- Sicurezza della *supply chain*
- Acquisizione, sviluppo e manutenzione dei sistemi di sicurezza
- Pratiche di base di c.d. *cyber hygiene* (vedere box di seguito) e formazione sulla sicurezza informatica
- Crittografia e tecnologie di crittografia
- Sicurezza delle risorse umane, **politiche di controllo degli accessi e gestione degli asset**
- **Accesso Zero Trust (autenticazione multi-fattore, autenticazione continua)**

La direttiva NIS2 introduce **obblighi più stringenti di segnalazione** degli incidenti informatici. Le entità critiche devono ora:

- Fornire notifica di un incidente di sicurezza significativo entro 24 ore dal rilevamento.
- Fornire una valutazione iniziale dell'incidente entro 72 ore dal rilevamento.
- Presentare un rapporto finale dettagliato entro un mese dal rilevamento.

La direttiva NIS2 **impone sanzioni** fino a 10 milioni di euro o al 2% del fatturato annuo per determinate violazioni o **esposizione di dati di terzi**. Inoltre, gli organi amministrativi possono essere ritenuti personalmente responsabili delle infrazioni.

Cyber Hygiene

Le politiche di *cyber hygiene* forniscono le basi per proteggere le infrastrutture di rete e dei sistemi informativi, l'hardware, il software e i dati aziendali o degli utenti finali su cui. Le politiche comprendono *best practice*, inclusi aggiornamenti software e hardware, modifiche delle password.

Namirial | © Namirial – All rights reserved

Perché l'Identity Trust è centrale nella NIS2

L'**autenticazione** è il processo attraverso cui persone, applicazioni o macchine accedono ai servizi, alle infrastrutture e ai **dati** di un'organizzazione. L'**Identity Trust** è l'adozione di tecnologie informatiche che permettono di collegare in maniera forte una credenziale ad un'entità ben precisa, riducendo i rischi di attacchi informatici.

L'**Identity Trust** è fondamentale per difendere le infrastrutture critiche da attacchi diretti, ransomware e altre minacce, e contemporaneamente adempiere ai requisiti chiave dell'**articolo 21** della NIS2, relativi alla gestione e alla segnalazione degli incidenti, alla sicurezza della *supply chain*, crittografia e tecnologie di cifratura, politiche di controllo degli accessi e sicurezza *Zero Trust*.

Una strategia completa di **Identity Trust** include:

- Gestione basata su policy delle credenziali amministrative e non.
- Accesso just-in-time per limitare i rischi posti dal furto di credenziali.
- Sicurezza dei privilegi degli endpoint per applicare il principio del privilegio minimo e difendersi dai ransomware e attacchi dannosi.
- Autenticazione multi-fattore (MFA) senza password e gestione centralizzata tramite l'autenticazione basata su certificati digitali.

Con le soluzioni di **Identity Trust Namirial** è possibile:

- Autenticare e autorizzare continuamente gli utenti interni ed esterni in conformità con i principi *Zero Trust*.
- Utilizzare il fattore di autenticazione più idoneo per il singolo utente (badge aziendale, token, APP, SMS/OTP)
- Controllare rigorosamente l'accesso alle risorse locali e basate su cloud.
- Monitorare e verificare attivamente l'attività degli utenti e fornire prova di conformità (*audit log*).

Namirial | © Namirial – All rights reserved


Namirial