WEBINAR

Proteggi la tua infrastruttura

Strategie efficaci per una sicurezza completa

28 GENNAIO
2025

EDU TIPS
CYBERSECURITY

EDU TIPS | smeup

Sicurezza informatica, il percorso formativo per rafforzare la tua sicurezza aziendale.

Le minacce digitali sono in continua evoluzione e affrontarle con consapevolezza è fondamentale.

Smeup ti invita a seguire un **percorso formativo gratuito** composto da **10 webinar di 30 minuti** , pensati per guidarti con soluzioni pratiche e strategie concrete nella **sicurezza aziendale** .

EDU TIPS Cybersecurity

10 webinar TIPS - 30 minuti al mese
su tematiche specifiche di Cybersecurity

DATA	DESCRIZIONE
28/1	**Mese 1: Sicurezza dell'infrastruttura**
13/2	Mese 2: **Cyber Security Awareness**
13/3	Mese 3: **Data Protection**
10/4	Mese 4: **Identità e accesso**
13/5	Mese 5: **Cloud security**
12/6	Mese 6: **Incident response**
8/7	Mese 7: **Sicurezza delle applicazioni**
11/9	Mese 8: **Analisi delle minacce e vulnerability assessment**
10/10	Mese 9: **Sicurezza delle reti industriali (OT)**
11/11	Mese 10: **Sicurezza in ambito A.I.**

👉 SCOPRI DI PIÙ

EDU TIPS
CYBERSECURITY

SIMONE
ZABBERONI

Security Specialist *- smeup ICS*

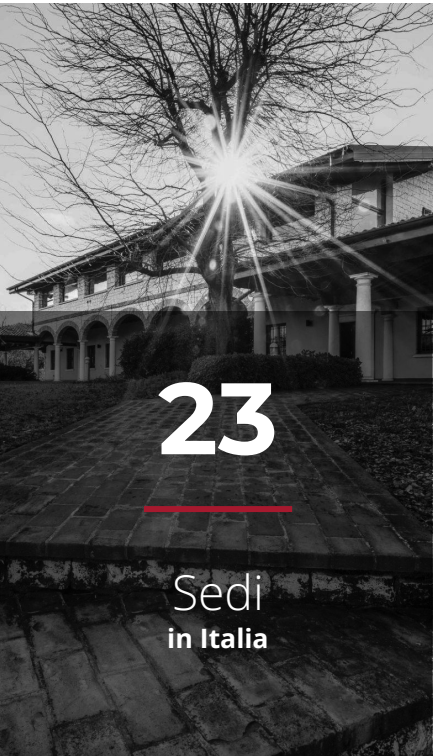
simone.zabberoni@smeup.com

COMPANY OVERVIEW

smeup in breve.

COMPANY **OVERVIEW**

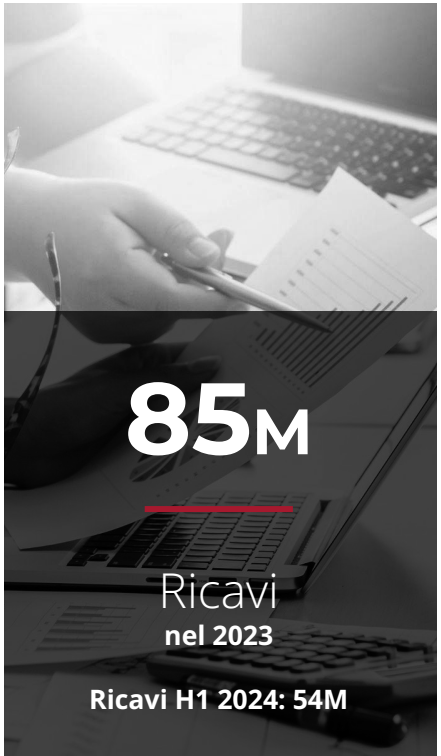
smeup in Numeri



23

Sedi

in Italia



85M

Ricavi

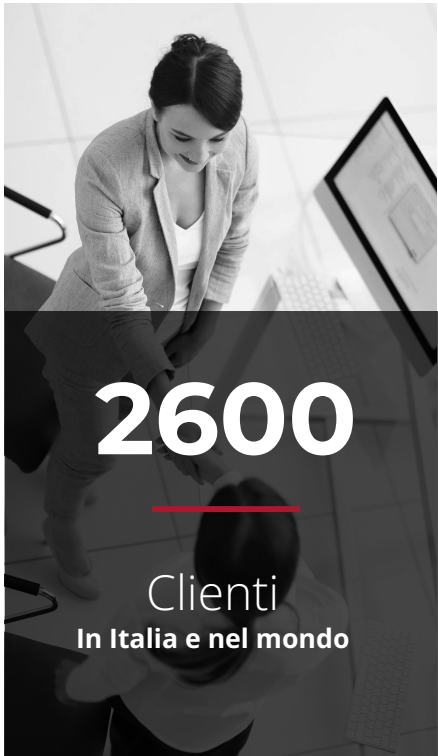
nel 2023

Ricavi H1 2024: 54M

610

Collaboratori

nelle nostre aziende



2600

Clienti

In Italia e nel mondo

BUSINESS SECTOR

BUSINESS SOFTWARE APPLICATION

Soluzioni **Software** per **PMI** e **grandi industrie.**

Ogni azienda è unica. smeup lo sa!
Usare la digitalizzazione per sviluppare il business e generare valore, ***insieme***.

- e GESTIONALI ERP
- r RETAIL
- b BUSINESS ANALYTICS
- d DOCUMENTALE
- w WEB & MOBILE APPLICATION
- h RISORSE UMANE
- p PROGETTAZIONE
- f IOT E INTEGRAZIONE INDUSTRIALE
- l LOGISTICA E TRASPORTI

BUSINESS SECTOR

INFRASTRUCTURE, CLOUD & SECURITY

Soluzioni per **Architetture IT** e **servizi gestiti.**

Innovazione e **sicurezza** per rispondere ai bisogni delle aziende.

- i INFRASTRUTTURA
- c CLOUD
- cs CYBER SECURITY
- ps IBM POWER SYSTEMS

INDICE

CYBERSECURITY

EDU TIPS

EDU TIPS
CYBERSECURITY

01. Network security e difesa perimetrale

28 GENNAIO
2025

SEPARARE GLI **AMBITI**

Firewall e segmentazione.

Le reti aziendali comprendono dispositivi diversi per provenienza, sistema operativo e sicurezza

Le vulnerabilità di uno possono diventare un rischio per tutti: un PC compromesso può innescare un attacco su tutta la rete.

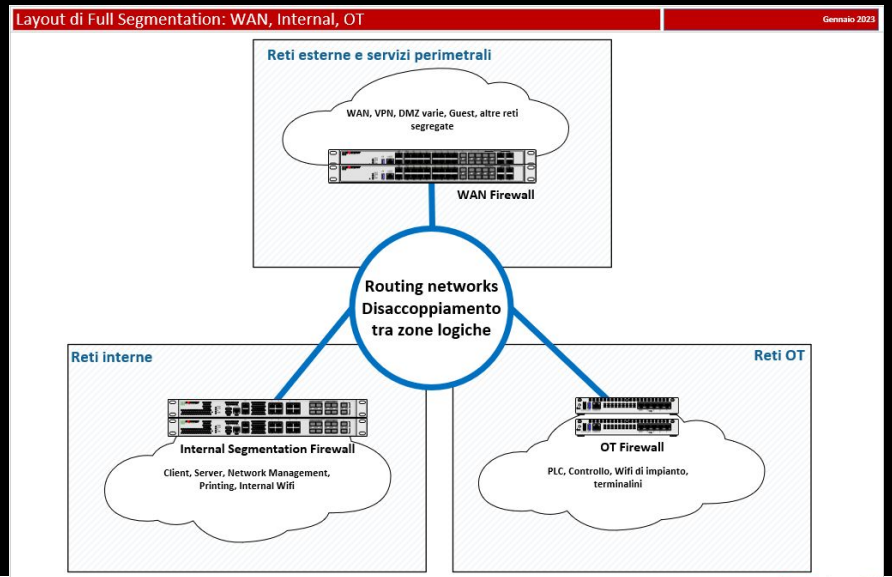
RIORGANIZZARE E RAZIONALIZZARE

→ Separiamo le cose: *PC, server, telecamere, controllo accessi, apparati smart ecc.*

→ Chi parla con chi?

→ Il pericolo del movimento laterale.

→ Attenzione agli accessi A internet e DA internet



PERICOLI **ESTERNI**

Protezione perimetrale: Firewall e Web Application Firewall

Proteggere l’erogazione dei servizi pubblicati.

Qualsiasi servizio pubblicato può attirare l'interesse dei malintenzionati di tutto il mondo.

Ogni servizio esposto rappresenta un potenziale punto di accesso ai dati che contiene o all'intera rete.

PROTEZIONE MULTILIVELLO

→ Rilevamento e blocco dei tentativi di intrusione.

→ Strato di sicurezza dedicato alle applicazioni web.

→ Attenzione alle scansioni remote.

→ Rilevazione e blocco degli attacchi a forza bruta

2025/01/07 15:14:47	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 15:09:04	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 15:03:36	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:58:11	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:52:19	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:46:57	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:41:32	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:36:01	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:30:16	Administrator admin login failed from https(92.255.57.48) because of invalid password
2025/01/07 14:24:39	Administrator admin login failed from https(92.255.57.48) because of invalid password

02

Protezione dei dispositivi

28 GENNAIO
2025

SICUREZZA DEI **DISPOSITIVI UTENTE**

Antivirus, EDR, XDR, MDR.

- Vari nomi e sigle per i diversi strati di protezione per PC e dispositivi mobili.
- Gestione del perimetro esteso.

> *No, l’antivirus da solo non basta più!*

PROTEZIONE DALLE MINACCE NOTE

VERIFICA “COMPORTAMENTALE”

CORRELAZIONE DEGLI EVENTI

RISPOSTA AGLI INCIDENTS

EDU TIPS
CYBERSECURITY

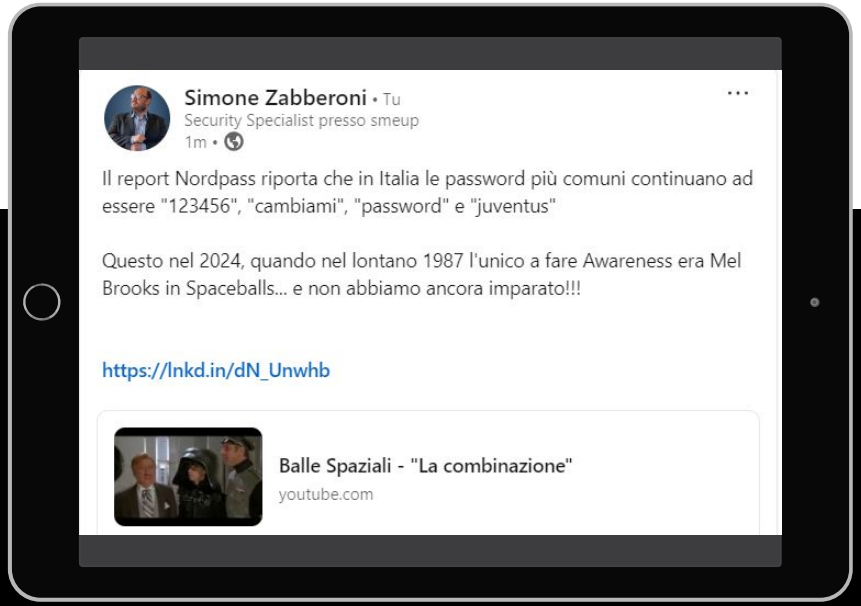
03

Gestione dell’identità.

28 GENNAIO
2025

UTENTI, PASSWORD E **MULTIFACTOR**

Sei veramente chi dici di essere?



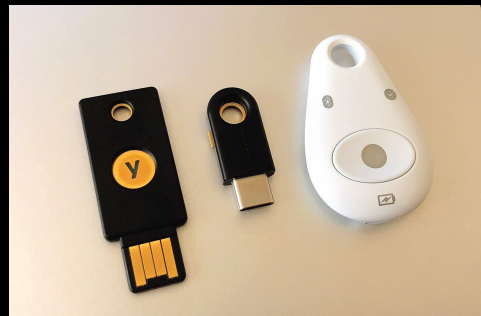
Le password da sole non bastano più a proteggerci… e non siamo tanto bravi a usarle:

Molto spesso basta una password compromessa per “entrare” in azienda.

Nel dark web le password compromesse sono merce di scambio, vendute “a peso” in base al livello di accesso, alla dimensione potenziale del cliente.

Più è grande → più riscatto si può chiedere → la password costa di più!

- Password complesse vs passphrase: meglio **“c44ds£THc_!”** o **“Ma!Che!Bel!Castello”** ?
- Password policy
- Rotazione delle password
- Password Manager
- Multifactor Authentication
- Biometrica
- Token Mobile
- Token fisici



EDU TIPS
CYBERSECURITY

04

Gestione degli accessi remoti e perimetro esteso.

28 GENNAIO
20**25**

PERIMETRO **ESTESO**

I dati non sono più tutti in azienda. Gli utenti nemmeno.

SERVIZI CLOUD

Personalmente ed aziendalmente non ne possiamo più fare a meno, ma non dobbiamo dimenticarci che la sicurezza è sempre in capo a noi!

VPN

Modalità di accesso “classico” per i remote workers
Funziona ancora (se gestita bene!) ma inizia a presentare alcuni limiti.

SASE

Evoluzione sicura della gestione del “Service Edge”.

EDU TIPS
CYBERSECURITY

05

SOC e monitoraggio H24.

28 GENNAIO
20**25**

I malviventi lavorano h24, 7su7 e spesso attaccano dal venerdì alle 22:00!

SOTTO **ATTACCO**

Non si tratta di *“se”* ma di *“quando”*.

01 **SICUREZZA PROATTIVA**
Implementazione di tutti gli strati di sicurezza possibili e proporzionati all’azienda.

02 **MONITORAGGIO**
Sta succedendo qualcosa sui nostri sistemi? Qualcuno parla di noi sul dark web?

03 **REAZIONE ISTANTANEA**
Se viene rilevato un “incident”, bisogna reagire prima che diventi un vero e proprio danno (ransomware, furto dati, defacement).

EDU TIPS
CYBERSECURITY

06

NIS2 e altre.

28 GENNAIO
20**25**

OBBLIGHI NORMATIVI DELLA **NIS2**

A quali soggetti si applica?

Soggetti **ESSENZIALI**
(essential entities)

Soggetti **IMPORTANTI**
(important entities)

- La **differenza** pratica riguarda i **controlli** e le **sanzioni**.
  Ulteriori soggetti potrebbero essere aggiunti dalla normativa nazionale.
- Le entità dovranno riconoscersi come soggetti a cui è applicabile la NIS2, non è più l'autorità che le designa come tali.
- Entro il **17 aprile 2025** gli Stati membri **definiranno** un **elenco dei soggetti.**

OBBLIGHI NORMATIVI DELLA **NIS2**

Approccio «multirischio»

1. Politiche di **analisi dei rischi** e della sicurezza
2. Sistemi di gestione degli **incidenti**
3. Soluzioni di **business continuity**
4. Misure di sicurezza dell'intera **supply chain**
5. Sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi e delle reti informatiche, compresa la gestione e la divulgazione delle **vulnerabilità**
6. Strategie e procedure per valutare l'**efficacia delle misure** di gestione dei rischi di cybersecurity
7. Pratiche di **igiene informatica** basilari e **formazione** in materia di sicurezza informatica
8. Uso della **crittografia**
9. Sicurezza delle **risorse umane** e **politiche di controllo** degli accessi (log management) e gestione degli asset
10. Uso di **soluzioni di autenticazione** a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti all'interno dell'entità, ove opportuno.

OBBLIGHI NORMATIVI DELLA **NIS2**

Adeguate misure di sicurezza.

Si suggerisce di rifarsi a uno standard noto a livello internazionale come la **ISO/IEC 27001.**

NIS2 stabilisce **requisiti di sicurezza più rigorosi e dettagliati**, con l'obiettivo di aumentare la resilienza complessiva delle reti e dei sistemi informativi. Questo include l'implementazione di politiche di sicurezza più avanzate e la gestione proattiva dei rischi di sicurezza informatica. **Non occorre più progettare la sicurezza in modo virtuale, ma occorre renderla operativa ed efficace.**

01 VALUTARE IL RISCHIO

02 TRATTARE IL RISCHIO E SCEGLIERE DELLE ADEGUATE MISURE DI SICUREZZA

03 GESTIRE GLI INCIDENTI

04 MIGLIORAMENTO CONTINUO

05 CONTINUITÀ OPERATIVA

NON SOLO **NIS**

Altri standard e framework

ISO, TISAX, PCIDSS, IEC62443, NIST... e tanti altri!

Facciamo chiarezza: NIS2, ISO e framework

- **NIS2** → Non è una certificazione, **è una norma da rispettare**.
- **ISO** (es. 27001) → Standard certificabile per strutturare i processi aziendali.
- **Framework** (es. NIST) → Strumenti per analizzare, contestualizzare e gestire i rischi.

ATTENZIONE: NON BASTA L'ISO 27001!

- La certificazione **non copre tutto** ciò che serve per la conformità NIS2.
- **Punto positivo**: Adottando ISO 27001, buona parte dei requisiti tecnologici sono già coperti, facilitando l'adeguamento.

Webinar **Edu Tips - Cybersecurity**

Thank you!

SIMONE **ZABBERONI**

Security Specialist - smeup ICS

simone.zabberoni@smeup.com