Swascan
TINEXTA GROUP

SWASCAN

The CYBER SECURITY PARTNER

The Threat Intelligence Platform

Cyber Security **Competence Services**

The First Cyber Security Testing Platform

Cyber Risk Indicators

L'Osservatorio Cyber Swascan

info@swascan.com
swascan.com

In collaboration with **CISCO**

L'osservatorio cyber di **Swascan**:

Misura

L'esposizione al Rischio Cyber delle Aziende. Identifica l'indicatore di rischio cyber relativo ad un campione di aziende in modalità aggregata e anonimizzata.

Comunica

I risultati dell'Osservatorio Cyber in **un evento** al fine di **sensibilizzare e formare** il Management sui cyber risk aziendali e impatti sulla Business Continuity.

Verifica

L'esposizione al Rischio Cyber delle singola aziende attraverso un **servizio gratuito** messo a disposizione delle aziende grazie alla sottoscrizione di una convenzione.

L’osservatorio cyber di **Swascan**:

MISURA

L’esposizione al Rischio Cyber delle Aziende. Identifica l’indicatore di rischio cyber relativo ad un campione di aziende in modalità aggregata e anonimizzata.

Osservatorio Cyber Security: **MISURA**

Perché

Permette di rispondere al bisogno delle aziende di **affrontare le nuove minacce cyber** che possono impattare in termini di:

- Compliance Legislativa.
- Brand Reputation.
- Business Continuity.

I Benefici

- **Identificare** l'esposizione del Rischio Cyber del settore di Mercato.
- **Rilevare** ed identificare la potenziale esposizione del rischio cyber delle singole Aziende.
- **Diffondere** la consapevolezza dei nuovi rischi digitali.

L'osservatorio

L'osservatorio Cyber Security di Swascan è basato solo ed unicamente su dati oggettivi.

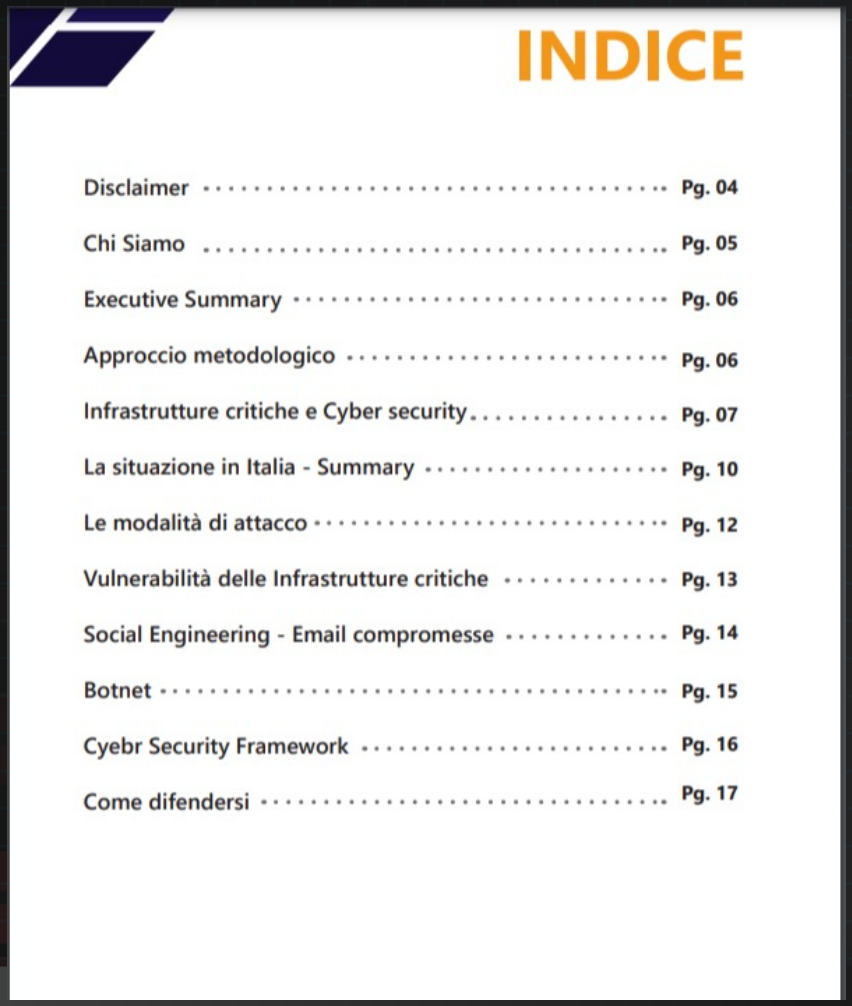
I dati analizzati e clusterizzati sono basati su informazioni pubbliche disponibili a livello web, darkweb e deepweb:

- **OSINT**
- **CLOSINT**

Osservatorio Cyber Security: **MISURA**

Esempio

https://www.swascan.com/it/cyber-risk-indicators-infrastrutture-critiche-italia/



Osservatorio Cyber Security di Swascan

- ✓ L'osservatorio di Cyber Security di Swascan opera attraverso l'attività di **Domain Threat Intelligence.**
- ✓ Raccoglie, analizza e clusterizza le informazioni legate a **domini, subdomini ed email compromesse** per determinare l'esposizione al rischio cyber delle aziende.
- ✓ Distinguere possibili minacce e vulnerabilità informatiche a livello tecnico.
- ✓ L'attività di **Domain Threat Intelligence** ha l'obiettivo di individuare le informazioni pubbliche disponibili a livello di **OSINT e CLOSINT** collegate ad un obiettivo determinato.

Potential Vulnerability
19

Low Vulnerability
5

Medium Vulnerability
7

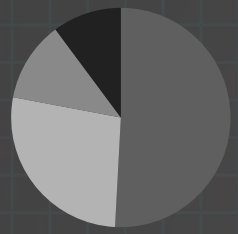
High Vulnerability
7

98
EMAILS
Compromised

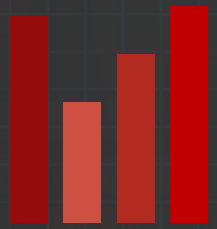
15
IP
found

19
Subdomains
found

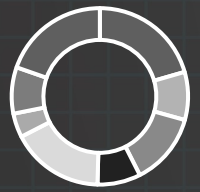
Average Potential Vulnerability
For Subdomains



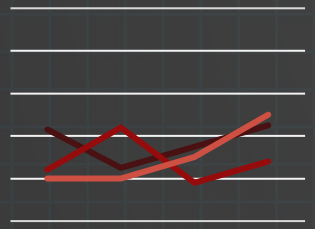
Potential Vulnerability
By risk (%)



GDPR
impact



Historical
Diagram



GDPR Potential Vulnerability impact (%)

L'osservatorio cyber di **Swascan**: **COMUNICA**

Comunica

I risultati dell'Osservatorio Cyber in **un evento** al fine di **sensibilizzare e formare** il Management sui cyber risk aziendali e impatti sulla Business Continuity.

Osservatorio Cyber Security: **COMUNICA**

Perché

- **Sensibilizza** gli Imprenditori e Manager sui rischi concreti relativi agli attacchi cyber.
- **Diffonde** la consapevolezza dei nuovi rischi digitali.
- **Dimostra** gli impatti diretti e indiretti sul Business.

I Benefici

- **Identifica** le best practise da implementare.
- **Illustra** tecniche e modalità degli attacchi informatici.
- **Fornisce** strumenti, metodologie e approccio alla corretta gestione del rischio cyber.

L’osservatorio cyber di **Swascan**: **VERIFICA**

Verifica

L’esposizione al Rischio Cyber delle singola aziende attraverso un **servizio gratuito** messo a disposizione delle aziende grazie alla sottoscrizione di una convenzione.

Osservatorio Cyber Security: **VERIFICA**

Perché

- **Misura** l'esposizione del rischio cyber aziendale.
- **Identifica** l'esposizione del rischio attacco ransomware.
- **Determina** il rischio di subire attacchi di phishing.

I Benefici

- **Determina** le criticità cyber aziendali.
- **Fornisce** un piano di remediation.
- **Supporta** le aziende alla compliance legislativa.

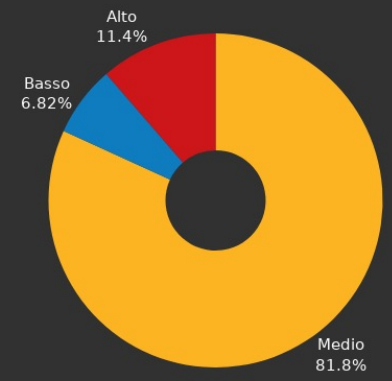
IL RISCHIO CYBER di xxxxxx.xx

Esempio

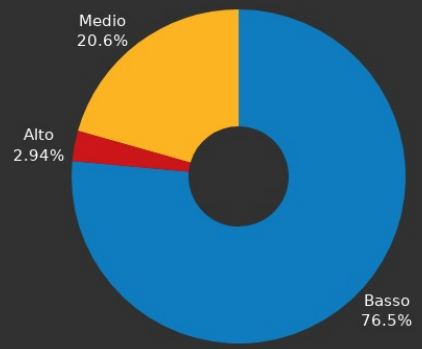
Vulnerabilità potenziali totali	Alta Severità	Media Severità	Bassa Severità
88	10	72	6

IP Totali trovati	Sottodomini Totali trovati	Emails compromesse	Fonti delle Breach
77	158	1175	34

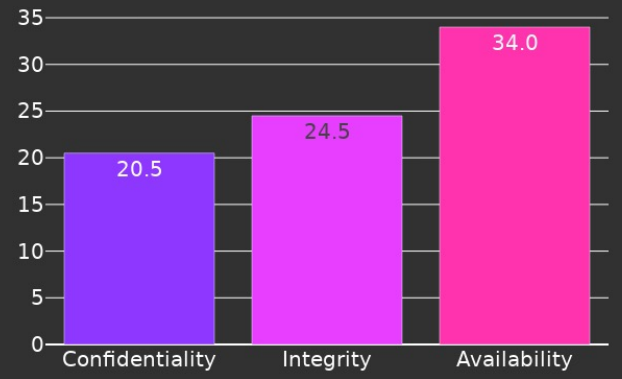
Rischio Tecnologico (Potenziali vulnerabilità per rischio)



Human Risk (Breaches per rischio)



GDPR Risk (Impatto su Confidentiality, Availability e Integrity)



Ransomware Risk: Technology Risk

Esempio

Vulnerabilità potenziali totali	Alta Severità	Media Severità	Bassa Severità
88	10	72	6

Terze parti hanno indicato pubblicamente la presenza di **88 potenziali vulnerabilità** presenti sul perimetro esposto su internet a livello di dominio e sottodominio. Vulnerabilità che, se sfruttate e sfruttabili potrebbero compromettere i servizi e permettere a terzi di accedere direttamente all'interno dell'infrastruttura aziendale per:

- Un attacco ransomware
- Esfiltrare i dati
- Interrompere l'operabilità dei sistemi

ACTION PLAN

- Attività di Penetration Test a livello infrastrutturale del perimetro esposto
- Attività di Penetration Test degli applicativi esposti su Internet
- Attività di Network Scan della rete interna
- Attività di Active Directory Assessment
- ISO27001 Assessment
- Technology Monitoring

Ransomware Risk: Social Engineering

Esempio

Sono state identificate 1175 e-mail compromesse. Parliamo di e-mail e password che i dipendenti hanno usato per registrarsi su siti terzi, siti che hanno subito un data breach e di conseguenza le credenziali (e-mail/password) sono diventate pubbliche.

I rischi sono:

- **Phishing e Spear Phishing**: le mail possono essere usate per campagne mirate di Phishing. Campagne customizzate utilizzando anche dalle ulteriori informazioni rilasciate sui siti terzi (data di nascita, cellulari, indirizzi fisici…).
- **Account Take Over:** furto dell'identità, in particolare gli account social. In questo modo è possibile inviare messaggi con link malevoli ai propri contatti.
- **Credential Stuffing**: utilizzo delle credenziali per accedere ai servizi esposti su internet (VPN, webmail, gestionali…).

E-mail compromesse

1175

ACTION PLAN

- Attività di Phishing Simulation
- Attività di Formazione e Awareness dei dipendenti
- GDPR Assessment

Ransomware Risk: Superficie di Attacco

Esempio

L'attività di Domain Threat Intelligence ha evidenziato che terze parti hanno identificato e mappato:

- 77 IP assegnati all'azienda
- 158 domini e sottodomini aziendali

L'attività di Information Gathering permette di determinare la superficie di attacco e rappresenta il primo step del Ransomware Cyber Kill Chain.

IP totali trovati

77

Sottodomini totali

158

ACTION PLAN

- Domain Threat Intelligence
- Threat Intelligence
- Early warning Giornaliero

Swascan
TINEXTA GROUP

SWASCAN

The CYBER SECURITY PARTNER

The Threat Intelligence
Platform

Cyber Security
Competence Services

The First Cyber Security
Testing Platform

Osservatorio
Cyber Security

info@swascan.com
swascan.com
In collaboration with
CISCO