Unione
CONFCOMMERCIO
IMPRESE PER L'ITALIA
MILANO · LODI · MONZA E BRIANZA
Area Innovazione Digitale

edi
ECOSISTEMA
DIGITALE
PER L'INNOVAZIONE

CONFCOMMERCIO
IMPRESE PER L'ITALIA

spin

CYBER CHECK-UP

Gratuito

Grazie per l'invito. Mi presento

Pier Carlo Pozzati
Head of Digital Innovation Office - Responsabile SPortello INnovazione at Confcommercio Milano
Milan, Lombardy, Italy · Contact info
500+ connections

Confcommercio Milano
MIP-Politecnico Di Milano

Aggiungetemi su LinkedIn:
https://www.linkedin.com/in/piercarlopozzati/

ECOSISTEMA
DIGITALE
PER L'INNOVAZIONE

EDI è il soggetto Confcommercio
riconosciuto e accreditato
dal Piano Nazionale Impresa 4.0

EDI è la risposta Confcommercio
alla crescente esigenza
di supportare i processi
di innovazione e trasformazione
digitale delle imprese

EDI supporta le imprese di:
Commercio, Turismo, Servizi,
Trasporti, Professioni, Logistica,
Terziario avanzato.

Gli SPIN offrono alle aziende, di qualsiasi categoria e in qualsiasi settore, un supporto concreto nel processo di Trasformazione Digitale, attraverso consulenze e supporto gratuiti, servizi a valore aggiunto, soluzioni digitali di alto profilo, aiuto per l'accesso a bandi e finanziamenti sul digitale.

SPIN Milano

- Fa parte dell'Area Innovazione Digitale di Confcomnmercio Milano

- Assiste ogni anno piu di 400 imprese sui temi legati al Digitale
  - Consulenza Diretta
  - CheckUp Digitali di varia natura
  - Ricerca Partner e Fornitori per soluzioni digitali di ogni genere

Premessa

- Oggi avere una presenza online comporta dei rischi di natura sia tecnologica, sia umana e di processo.
  La **protezione dei sistemi digitali** non è solo importante per il tuo patrimonio di dati e di informazioni, ma è anche un **obbligo di legge**.
- I criminali informatici prendono di mira chiunque. Nel loro mirino troviamo **aziende di qualunque dimensione.**
- Sito internet, social, portali o business email, sono tutti possibili **bersagli di un attacco informatico** in grado di impattare significativamente il business.

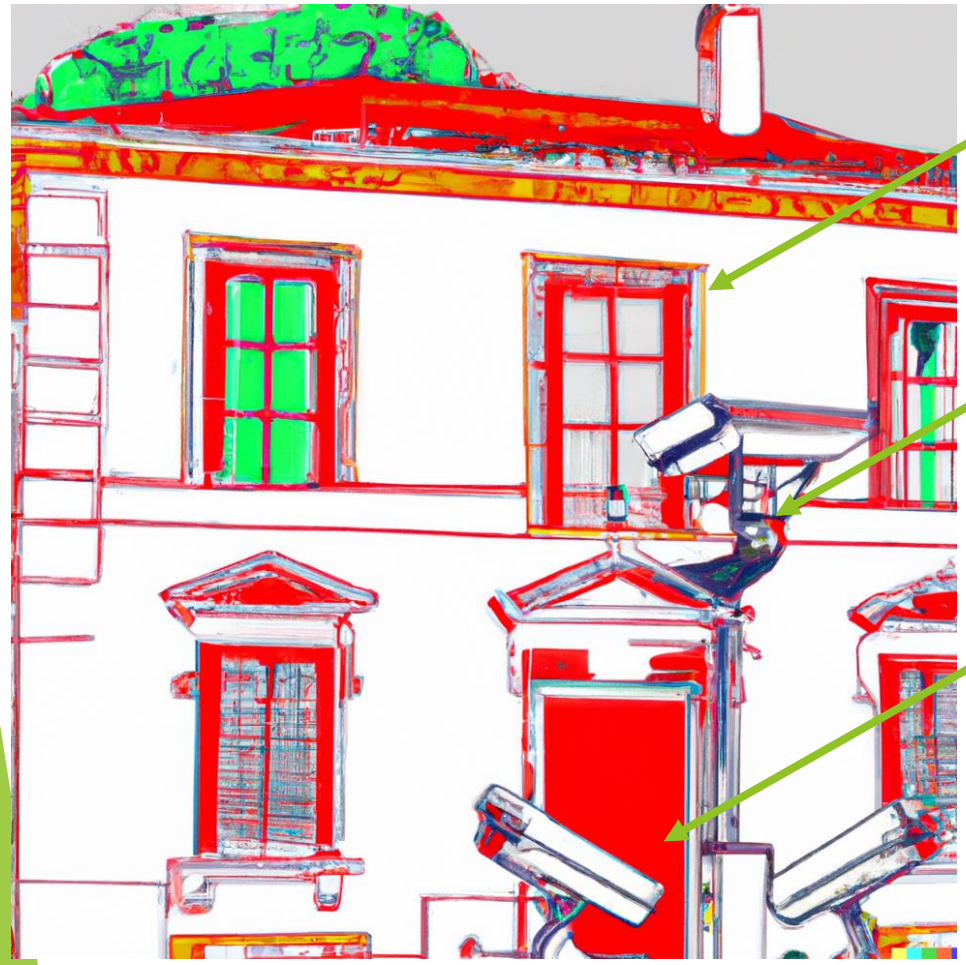
Nasce il CyberCheckUp Gratuito (per i Soci Confcommercio)

SOCIO ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

Swascan

Swascan è una Cyber Security Company, associata ad Assintel. La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security Testing e Threat Intelligence, oltre ad un centro di eccellenza di Cyber Security Research; centro premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo. Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security

Una METAFORA: la vostra villa videosorvegliata dotata di vari sistemi di sicurezza



Sensori alle finestre e porte

Telecamere di sorveglianza

Porte blindate

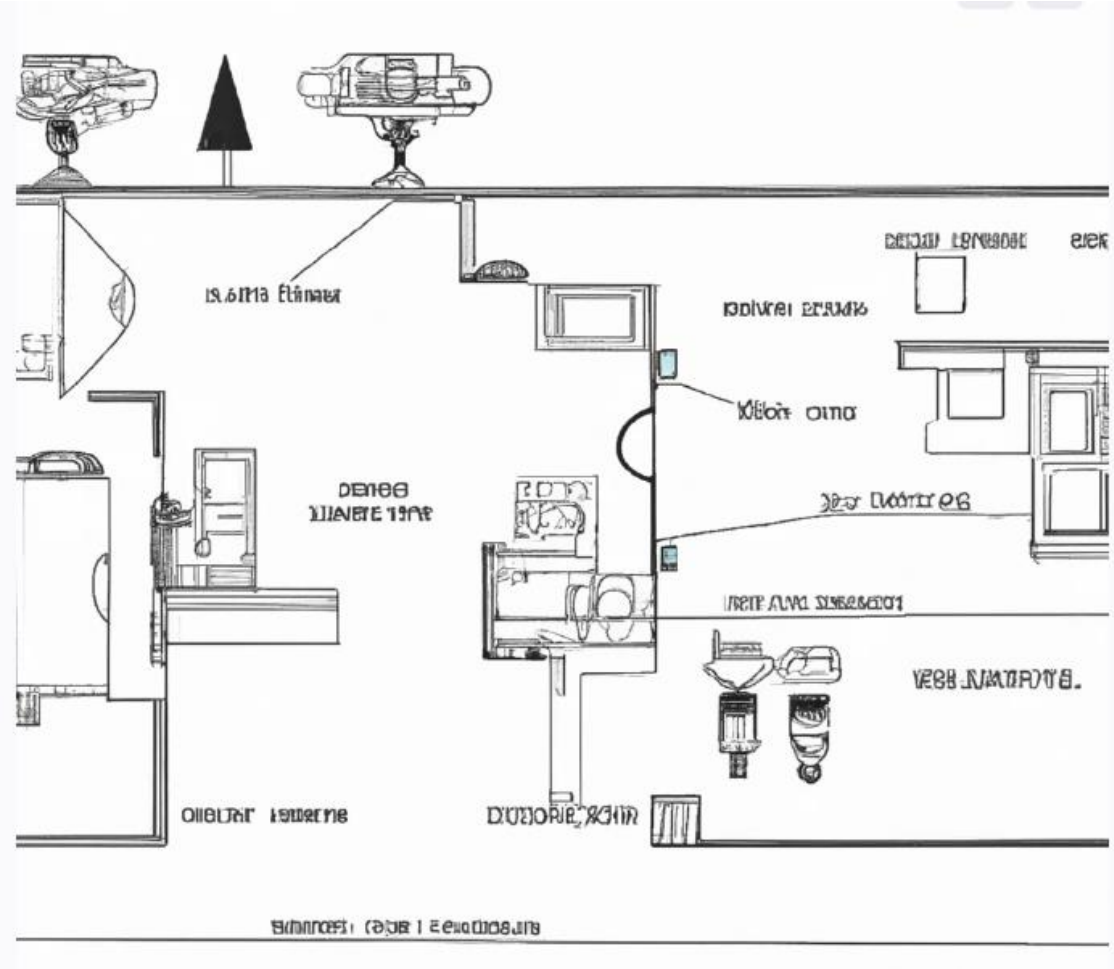
Siamo discretamente tranquilli….

Intanto nel

«Bar della Malavita»

SI PARLA DI VOI… a vostra insaputa

La mappa della villa…



- **Mappa**: tutte le porte/finestre esposte
- **Vulnerabilità** (due sensori delle finestre OVEST non funzionano)
- **Chiavi rubate**

Ma un «uomo misterioso» sta ascoltando tutto e prende nota….

Usciamo dalla METAFORA. Cosa fa il Cyber ChekUp?

Senza effettuare alcun test diretto sul perimetro dell'azienda, il Cyber Check-up restituisce informazioni cruciali – ottenute analizzando web/deep web e dark web – su:

•Numero e-mail compromesse, **cioè mail esposte pubblicamente da utenti che si sono registrati su siti che hanno subito un data breach. (un po' come farsi rubare le chiavi)**

•Potenziali vulnerabilità (SW installati che hanno dei punti di attacco sfruttabili) (il sensore che non funziona)

•Superfice d'attacco (la mappa)

Al completamento dell'analisi verrà fornito un action plan completo con tutti gli step e le misure correttive/migliorative per rendere la tua impresa sicura e a norma.

Rischio di Social Engineering Attack

Rischio di Ransomware Attack

Rischio di Cyber Attack

Come funziona

Si tratta di un servizio di **“security intelligence”** che effettua una ricerca delle informazioni **pubbliche** e **semipubbliche** relative alle vulnerabilità del dominio, sottodomini ed e-mail compromesse. Il servizio non effettua alcun test diretto sul target, opera unicamente sulle informazioni disponibili a livello OSINT e CLOSINT.

La **Open Source INTelligence**, acronimo **OSINT** (in italiano: "Intelligence su fonti aperte"), è quella disciplina dell'intelligence che si occupa della ricerca, raccolta ed analisi di dati e di notizie d'interesse pubblico tratte da fonti aperte. OSINT è stata introdotta durante la seconda guerra mondiale dalle agenzie di sicurezza di alcune nazioni.

fonti «chiuse» (o riservate)

Cyber CheckUp

- La prima fase del test è erogata direttamente da

- Vengono fornite informazioni e un action plan

- La seconda fase (di approfondimento) è supervisionata da SPIN ma erogata da SWASCAN (tramite un consulente)

IL REPORT CHE VIENE EROGATO

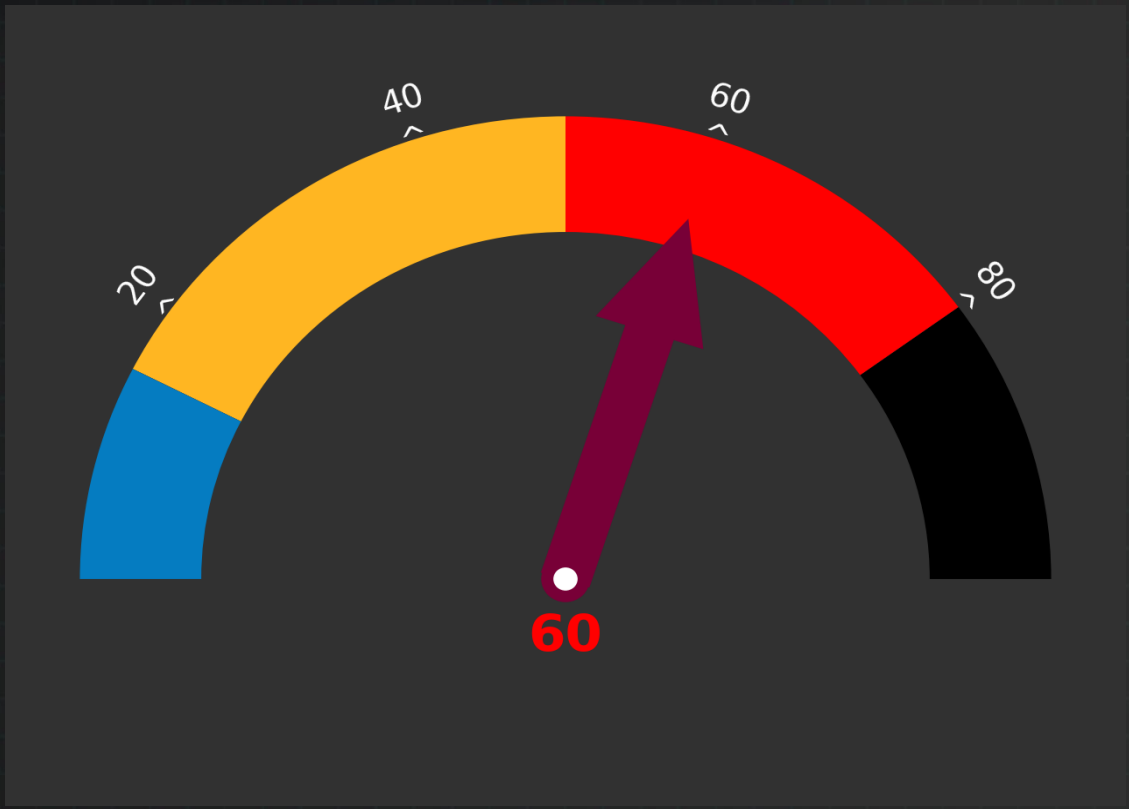
Ransomware Attack Index

Il Ransomware Attack Index indica il livello di rischio di attacco Ransomware in considerazione dei valori e dati raccolti e analizzati negli ultimi 30gg relativamente al dominio aziendale.

Tale indice si basa su:

1. Analisi del numero di servizi esposti;
2. Analisi dei data leak, quali email aziendali e password sottratte ai dipendenti;
3. Analisi delle potenziali vulnerabilità sfruttabili dall'attaccante.

Queste tre dimensioni riassumono la possibile superficie di attacco sfruttabile da parte dei cybercriminali.



MISURA Il tuo RISCHIO CYBER!

Il servizio di **Ransomware Risk Index** permette di valutare ed identificare il rischio di **CYBER ATTACK e RANSOMWARE ATTACK** di una azienda in base alle informazioni che sono già disponibili nel Web, Dark Web e Deep Web. Informazioni che terzi hanno pubblicato e di conseguenza accessibili e disponibili a tutti.

Si tratta di un servizio di "security intelligence" che effettua una ricerca delle informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed e-mail compromesse. Il servizio non effettua alcun test diretto sul target, opera unicamente sulle informazioni disponibili a livello OSINT e CLOSINT.

L'attività di Threat Intelligence viene effettuata su target e identificavi digitali relativi agli asset ed alle e-mail compromesse. L'attività è condotta attraverso la ricerca, individuazione e selezione delle informazioni disponibili pubblicamente relative al dominio, sottodomini ed e-mail compromesse.

Il servizio non effettua alcun test di sicurezza sul target, opera unicamente sulle informazioni raccolte a livello OSINT e CLOSINT e disponibili sul Dark Web.

OSINT: acronimo di Open Source Intelligence, si fa riferimento al processo di raccolta d'informazioni attraverso la consultazione di fonti di pubblico dominio definite anche «fonti aperte» impatti.

CLOSINT: Close Source Intelligence, processo di raccolta d'informazioni attraverso consultazione di «fonti chiuse», non accessibili al pubblico o aree «riservate».

Swascan
TINEXTA GROUP

Lo stato dell’arte del RISCHIO CYBER

France

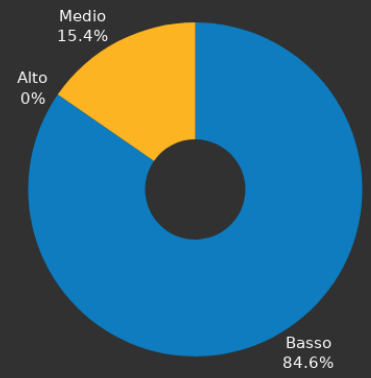
IL RISCHIO CYBER di france.fr

Vulnerabilità potenziali totali	Alta Severità	Media Severità	Bassa Severità
0	0	0	0

IP Totali trovati	Sottodomini Totali trovati	Emails compromesse	Fonti delle Breach
19	242	471	39

Rischio Tecnologico (Potenziali vulnerabilità per rischio)

Human Risk (Breaches per rischio)



GDPR Risk (Impatto su Confidentiality, Availability e Integrity)

Ransomware Risk: Technology Risk

Vulnerabilità potenziali totali	Alta Severità	Media Severità	Bassa Severità
0	0	0	0

Terze parti hanno indicato pubblicamente la presenza di **0 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

Anche se l'analisi non ha evidenziato criticità, è opportuno valutare le seguenti azioni:

- 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

E-mail compromesse

471

Sono state identificate 471 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,…)

ACTION PLAN

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

Ransomware Risk: Superficie di Attacco

IP totali trovati

19

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

- 19 IP assegnati all'azienda
- 242 domini e sottodomini aziendali

Sottodomini totali

242

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

ACTION PLAN

- Domain Threat Intelligence
- Cyber Threat Intelligence
- Early warning Giornaliero

Swascan
TINEXTA GROUP

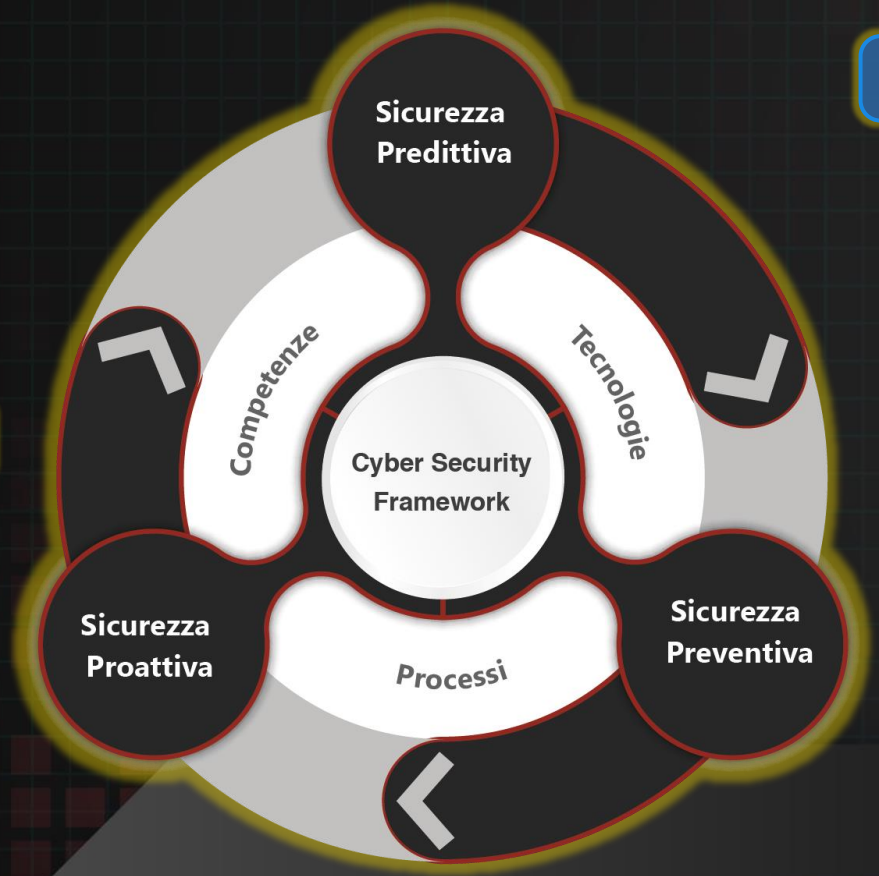
Proposta Progettuale

Cyber Risk Framework

Proposta Progettuale

Sicurezza Predittiva

- Domain Threat Intelligence
- Cyber Threat Intelligence
- Early warning Giornaliero



Sicurezza Preventiva

Rischio Tecnologico

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

Human Risk

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

Organizational Risk

- GDPR Assessment
- ISO27001 Assessment

Sicurezza Proattiva

- SOC as a Service
- Incident Response Team

Grazie dell'attenzione

SPIN MILANO e tutti gli SPIN in Italia sono a disposizione dei soci Confcommercio per Ascoltare, Assistere ed Affiancare nella ricerca di soluzioni digitali

https://www.ediconfcommercio.it/

Pier Carlo Pozzati

Responsabile SPIN Milano

spin@unione.milano.it

02-7750401