Cybersecurity e impresa: strumenti e prevenzione

CONFAPI BRESCIA

Relatore: Pierguido Iezzi – CEO Swascan

Pierguido Iezzi (CEO e co-founder di Swascan)

Ex Ufficiale di carriera presso l'Accademia Militare di Modena, laureato in Scienze dell'Informazione, con oltre 30 anni di esperienza nel mondo della Cyber Security. Ha alle spalle un'ampia gamma di attività operative relative a Tecnologia, Innovazione, Cyber Security e gestione aziendale. Autore di diverse pubblicazioni, collabora regolarmente a diversi giornali e pubblicazioni. Keynote speaker e testimonial presso università, eventi nazionali e internazionali.

p.iezzi@swascan.com

www.swascan.com

LinkedIn

1. La Piattaforma

The First **CyberSecurity** Testing **Platform**

CLOUD

Technology Risk

Vulnerability Assessment

Effettua analisi di siti web e applicazioni. Identifica le vulnerabilità, misura il livello di criticità, determina il piano di priorità e fornisce il piano di remediation.

Network Scan

Il Network Scanner identifica le vulnerabilità a livello network e device. Scopre le vulnerabilità, il livello di criticità, il piano di priorità e il relativo remediation plan.

Code Review

Effettua l'analisi del codice sorgente per identificare la presenza di vulnerabilità. Determina i livelli di criticità e priorità e fornisce le soluzioni e il piano di remediation.

Human Risk

Phishing Attack **Simulation**

Crea un'occasione unica di apprendimento per i tuoi dipendenti ed evita i sempre più frequenti attacchi di phishing

Smishing Attack **Simulation**

Attività di formazione e awareness dei tuoi dipendenti tramite vere e proprie simulazioni di attacchi smishing

Threat Intelligence

Domain threat Intelligence

Scopre vulnerabilità, criticità ed e-mail compromesse che sono pubbliche e semipubbliche disponibili a livello OSINT e CLOSINT relative al dominio aziendale.

Cyber Threat Intelligence

Analizza le informazioni del dominio aziendale presenti a livello Dark web e Deep web. Scopre la presenza di Botnet relative ai device di dipendenti, fornitori e clienti.

Risk Analysis

ICT Security Assessment

Permette di analizzare il proprio livello di rischio Cyber e valutare l'efficacia delle misure di sicurezza adottate

GDPR Assessment

Il Tool online che permette di valutare il livello di Compliance aziendale rispetto alla normativa privacy GDPR

2. Il Cyber Security Competence Center

Cyber Incident Response

Un Cyber team dedicato di pronto intervento Cyber per la gestione di Cyber Incident, attacchi DDOS, Data Breach e Attacchi Ransomware.

Incident Response e **Data Recovery**

SOC As a Service

Il servizio dedicato di Monitoring & Early Warning di Swascan per la corretta gestione della sicurezza proattiva e sicurezza preventiva.

SOC as a Service

Penetration test

Le attività di Penetration Test sono svolte da Penetration Tester certificati e in linea con gli standard internazionali OWASP, PTES e OSSTMM.

Penetration test

Cloud Security

Un Cyber Competence Center dedicato al mondo Cloud per le attività di governance, supporto e tutela dell' intero insieme di tecnologie, protocolli e best practice degli ambienti cloud computing.

Scopri di più

Security Management

Servizi di Security Advisory a livello consulenziale e a livello operativo per supportare i clienti nei piani di remediation, gestione della Cyber Security, Compliance Management e Risk Management.

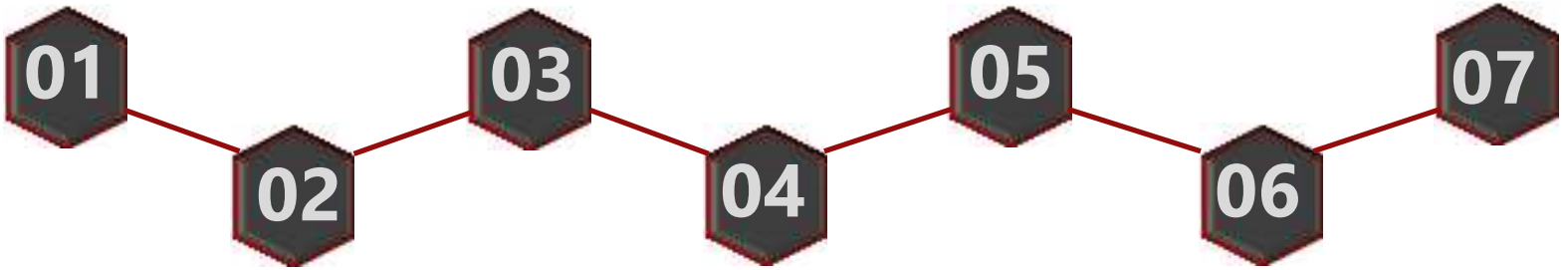
Security Management

Security Academy

Corsi di formazione dedicati di Cybersecurity in aula o tramite Webinar. Attività di Awareness per il personale tecnico, per i dipendenti e per i Top Manager.

Scopri di più

Cyber Kill Chain



Reconnaissance
Ricognizione dei target

Weaponization
Individuazione di uno strumento malevolo e delle vulnerabilità attraverso cui sfruttarlo

Delivery
Trasmissione dell'arma al target

Exploitation
Utilizzo di una vulnerabilità per entrare nei sistemi

Installation
Creazione di una via di accesso ai sistemi

Command & Control
Chiamata al Command & Control

Actions on objectives
Svolgimento di azioni mirate all'obiettivo dell'attacco

Tutti sono un target…

Gli attacchi informatici sono condotti by **opportunity.** L'opportunità è legata alla presenza di una vulnerabilità:

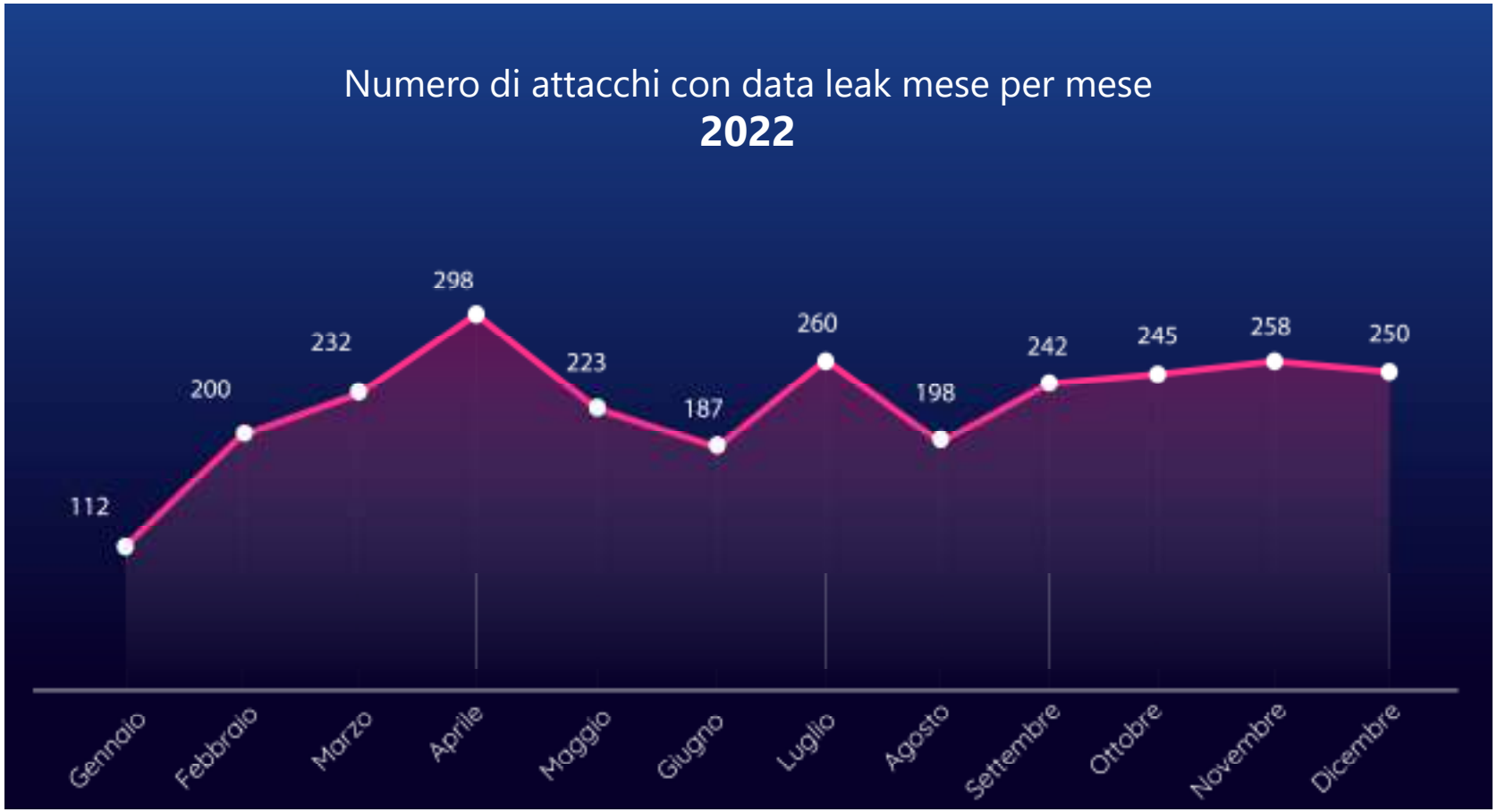
Tecnologica: un asset digitale esposto su internet che presenta una vulnerabilità che può essere sfruttata da un attaccante per accedere alla rete aziendale

Umana: la presenza di email compromesse permette all'attacante di sferrare un attacco di social engineering. Tecniche che hanno lo scopo e obiettivo di ingannare l'utente per sottrarre credenziali, infettare il dispositivo oppure per una frode (Phishing, Smishing,…)

Credenziali: la presenza di credenziali (compromesse) di accesso ai sistemi permettono agli attaccanti di poter accedere direttamente alla rete aziendale direttamente dalla «porta di ingresso» senza la necessità di avere competenze o capacità tecniche.

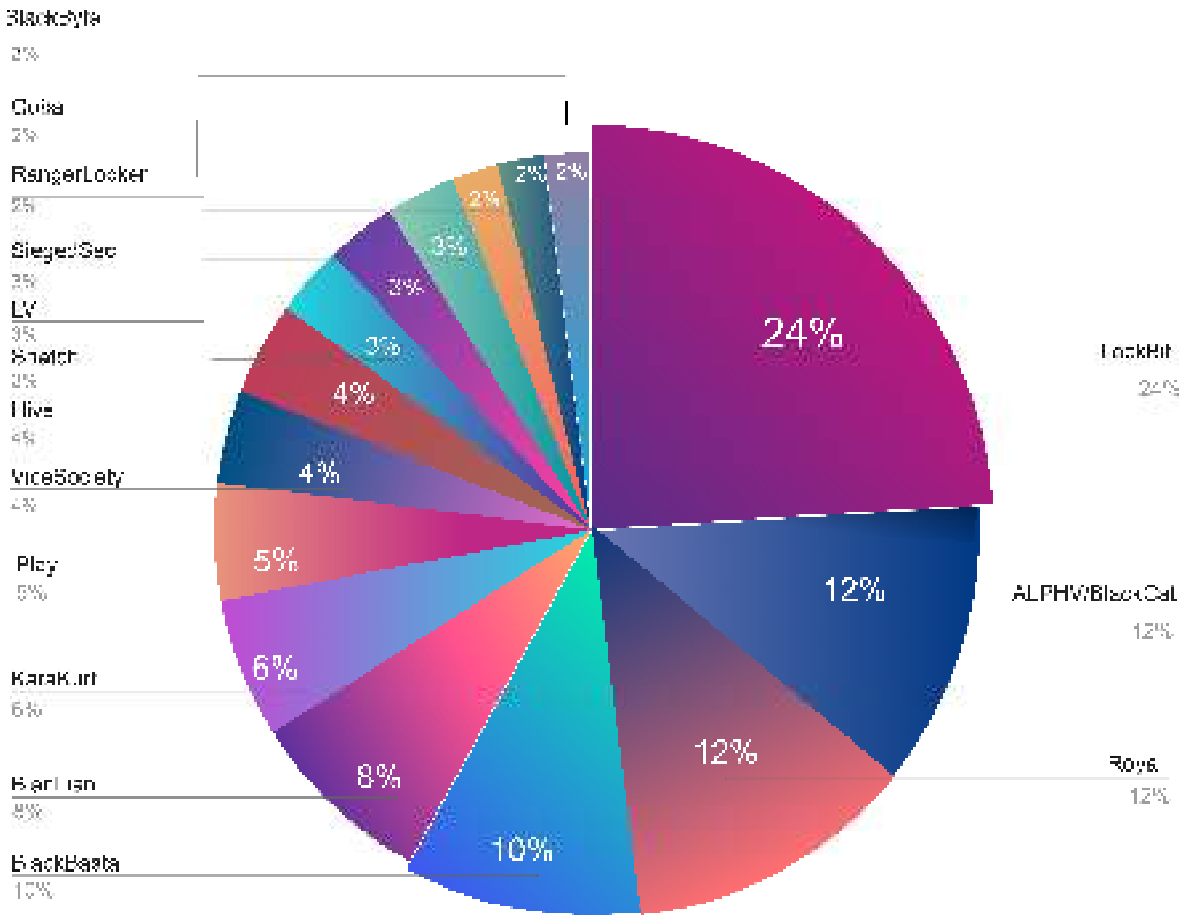
Supply Chain: fornitori e terze parti diventano inconsapevoli veicolo dell'attacco informatico. Attraverso la compromissione di un elemento della supply chain l'attaccante ottiene l'accesso alla rete aziendale. La supply chain diventa il «cavallo di troia» del criminal Hacker.

Un mondo cyber pericoloso....



Gli attacchi aumentano

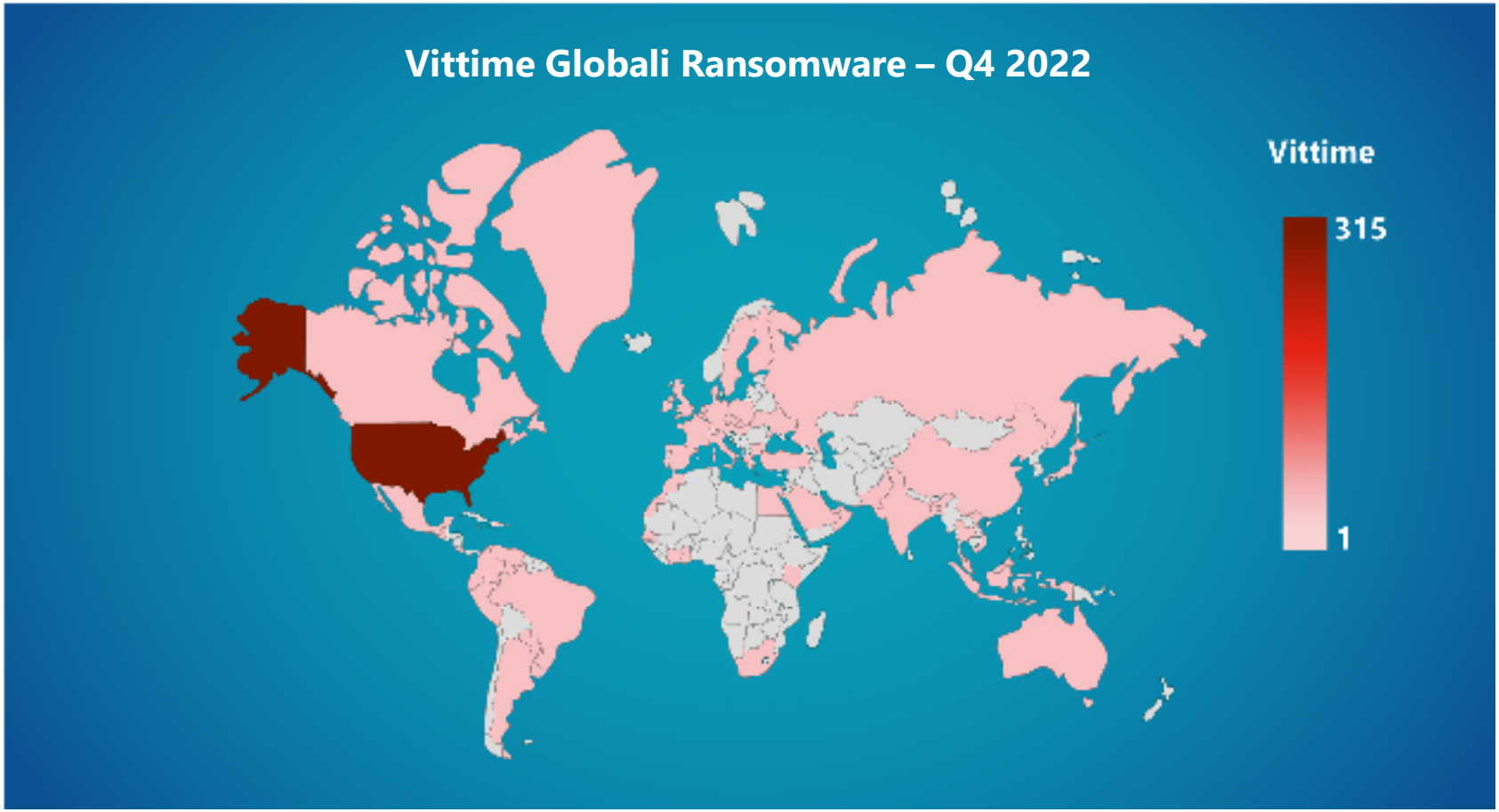
Numbers of victims – Q4 2022



Un mondo che cambia....

	Q3 2022	Q4 2022	Q4/Q3 (in %)	
Vittime di Data Leaks	700	753	+7.5%	↑
Gruppi di ransomware totali	36	41	+ 13%	↑
Vittime di LockBit con Data Leak	234	149	-36%	↓
Paese più colpito	United States	United States		
Totale Paesi colpiti	76	77	+ 1%	↑
I 5 paesi più colpiti	United States, France, Spain, United Kingdom, Germany	United States, United Kingdom, Canada, Germany, Brazil		
Settori più colpiti	Services	Services		
PMI colpite	82%	84%	+2%	↑

Come cambia sui valori assoluti?

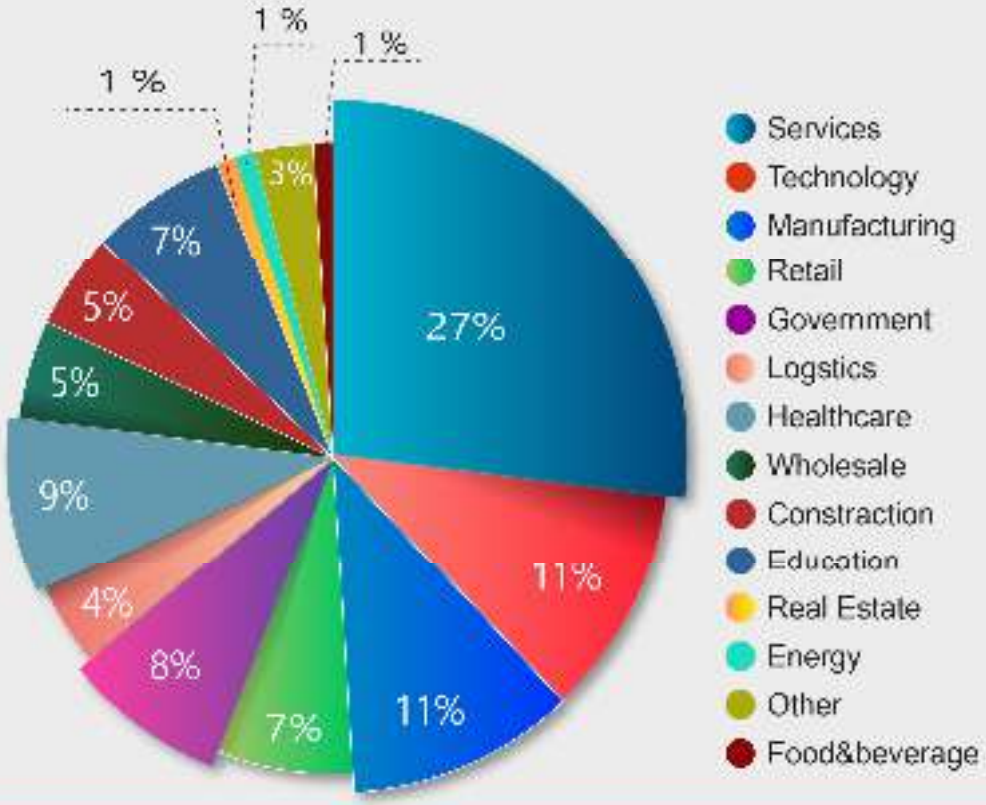


Come cambia sui valori assoluti?

Paese	Numero di aziende vittime di Ransomware con dati pubblicati – Q4 2022
United States	315
United Kingdom	42
Canada	40
Germany	29
Brazil	22
Australia	21
France	19
India	17

I settori di riferimento. Perchè ?

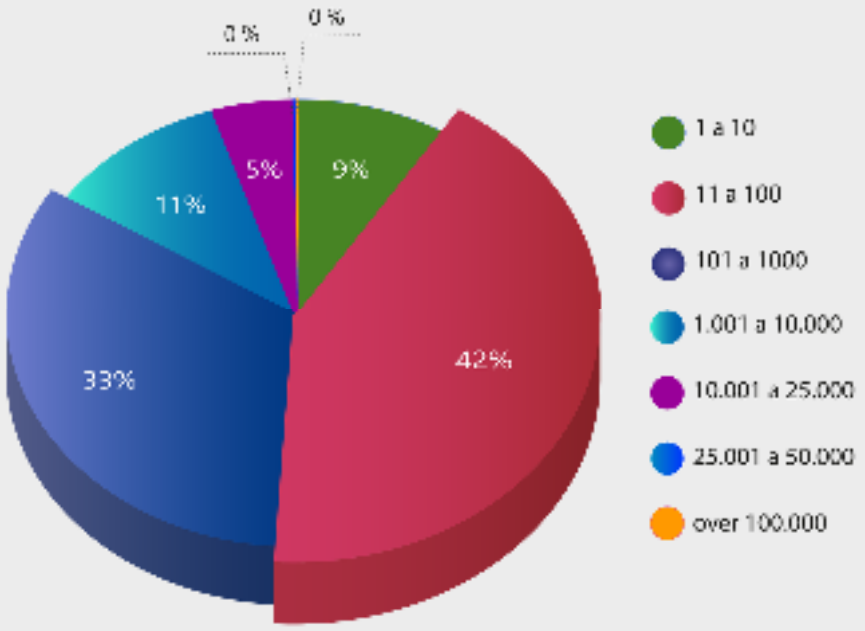
Attacchi per settore in percentuale- Q4 2022



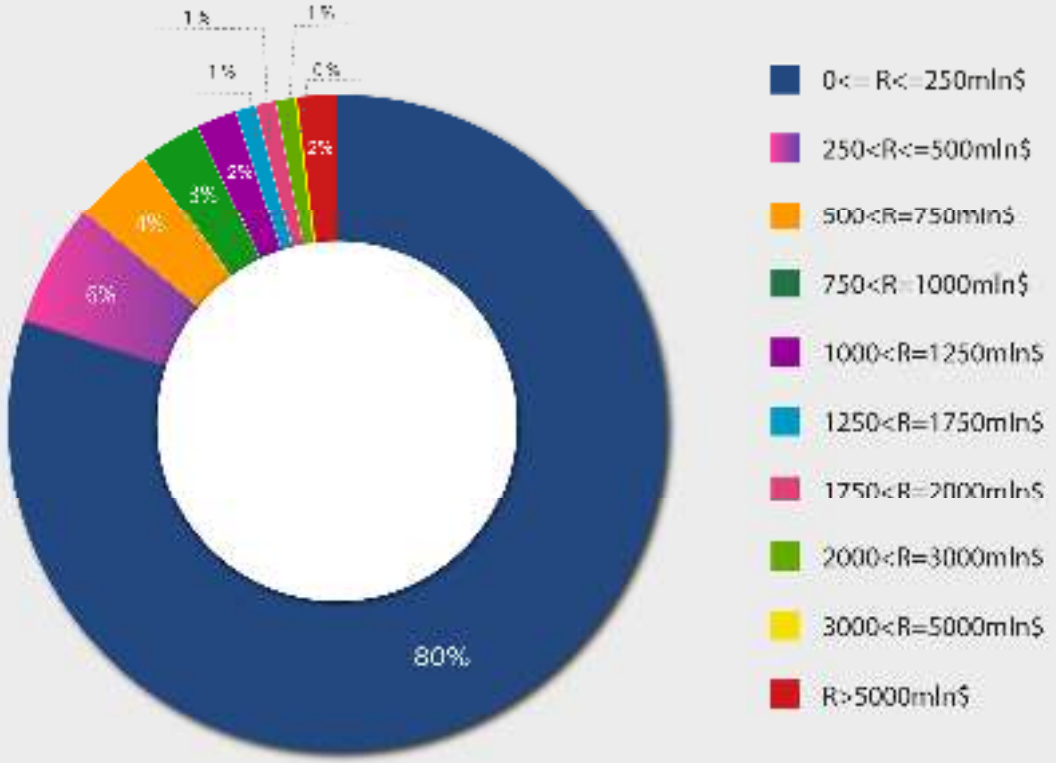
I Settori più Colpiti

Dipendenti e fatturato

Numero Dipendenti Aziende Colpite

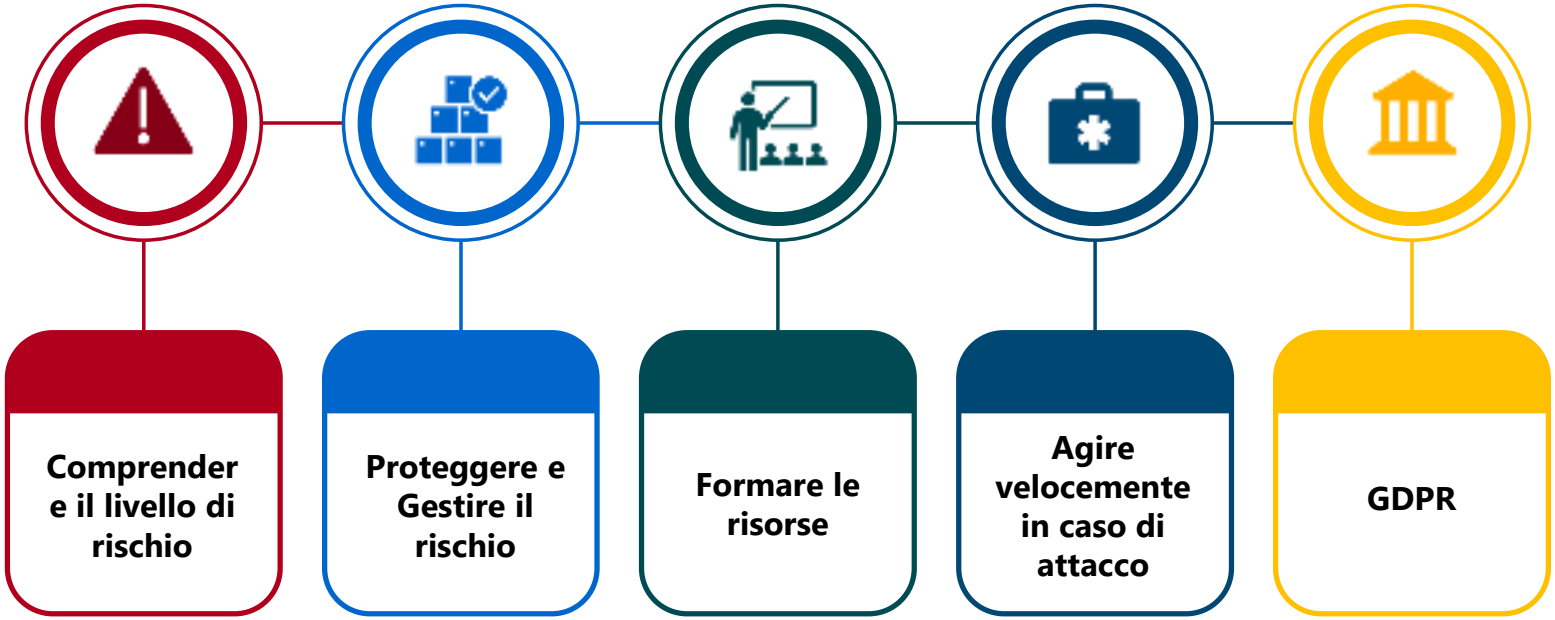


Spaccato Aziende Colpite In Base A Fatturato



Servizi Swascan a Pacchetti per Driver

- Per le Aziende da 1 a 25 dipendenti è stata strutturata una proposta a pacchetti in base al Driver di necessità:



Micro/Media Impresa: da 1 a 25 dipendenti

	Item	Descrizione	Driver
	Darkweb Mail Scan	**Darkweb Mail Scan:** licenza di utilizzo annuale che offre alle aziende la possibilità di scansionare indirizzi mail aziendali e il proprio dominio email per verificare se sono stati compromessi sul dark web. In caso di rilevamento di email compromesse, il servizio fornisce un report mensile dettagliato con informazioni su come e dove sono state violate le email e fornisce un piano d'azione per risolvere il problema. Protegge da Frodi e Phishing	N° 1 Dominio email
	Ransomware Attack Index	Licenza di utilizzo full usage della piattaforma **Ransomware Attack Index** che permette di misurare la probabilità di subire un attacco Ransomware in base alle informazioni e dati disponibili a livello pubblico e semipubblico (web, Darkweb e DeepWeb). Identifica i possibili vettori di attacco che potrebbero essere utilizzati dai criminal hacker	Azienda
	Check-up Sicurezza Light	Il **Check-up Sicurezza Light** Licenza di utilizzo full Usage del servizio che permette alle aziende di verificare e misurare il proprio livello di rischio cyber e di valutare l'efficacia delle misure di sicurezza adottate identificando due macro indicatori a livello Funzionale e Operativo. Il servizio fornisce un Report con le indicazioni e le azioni correttive da adottare a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo.	Azienda
	Network Vulnerability Scan	Il servizio di **Network Vulnerability Scan**. Il servizio online di Network scanner permette la scansione dell'infrastruttura esposta su internet per identificare le vulnerabilità e criticità di sicurezza. L' Analisi delle vulnerabilità ha lo scopo di quantificare i livelli di rischio e indicare le azioni correttive e di riposizionamento necessarie per il ripristino dei livelli di sicurezza. Servizio 12 mesi, scansione fino a 10 IP al mese. Il cliente riceve mensilmente un report delle criticità identificate	Azienda

Micro/Media Impresa: da 1 a 25 dipendenti

Item	Descrizione	Driver
Antiransomware	Il servizio «**Antiransomware**" è una soluzione di sicurezza progettata specificamente per le piccole aziende. Installando un agent sul dispositivo, RansomSafe fornisce protezione contro gli attacchi di ransomware, che sono una delle principali minacce per le piccole aziende. Protegge dagli attacchi Ransomware La soluzione include: • Rilevamento e prevenzione degli attacchi di ransomware in tempo reale • Backup automatizzato dei dati per garantire la possibilità di ripristinare i dati in caso di attacco • Protezione degli endpoint per prevenire la diffusione del malware all'interno della rete aziendale Il servizio è progettato per essere semplice da usare e gestire, per garantire che le piccole aziende possano proteggere efficacemente i loro dati senza dover investire in una grande quantità di risorse. Dispositivi supportati: Supporta tutti i sistemi Windows a partire dalla versione Windows 7 sp2 Installazione immediata con un semplice click tramite un agent	Per device
Cyber Formazione & Awareness	Il servizio **Cyber Eleraning Platform** consente al cliente l'accesso online a una vasta gamma di contenuti formativi sulla cybersecurity. Gli utenti hanno accesso a brevi pillole formative per imparare velocemente, corsi di approfondimento di 45-50 minuti con questionari di valutazione, webinar pre-registrati di 1 ora per approfondire gli argomenti, ed ebook su argomenti selezionati. La piattaforma viene aggiornata mensilmente con nuovi corsi inediti per garantire che gli utenti abbiano sempre accesso ai contenuti più recenti e aggiornati. Un servizio che risponde agli obblighi legislativi previsti dalla GDPR, ai requirement della ISO27001 e permette di ridurre il rischio di frodi e phishing.	utente

Micro/Media Impresa

Item	Descrizione	Driver
Security Log Management GDPR	Il nuovo servizio **Security Log Management GDPR** risponde agli obblighi legislativi GDPR per gli Amministratori di sistema e ai requisiti previsti nella ISO27001. E' la soluzione per la gestione dei registri di sistema che aiuta gli amministratori di sistema a conformarsi alle norme dell'UE per la protezione dei dati. Questo sistema raccoglie, archivia e analizza i registri di sistema, tra cui le informazioni sull'utilizzo del sistema, gli accessi e le modifiche apportate ai dati. Il sistema di Security Log Management GDPR consente agli amministratori di sistema di identificare e analizzare eventuali violazioni della sicurezza dei dati, come ad esempio tentativi di accesso non autorizzati o modifiche non autorizzate ai dati personali, in modo da poter prendere rapidamente misure per proteggere i dati. Inoltre, il sistema fornisce una cronologia completa degli eventi per supportare la tracciabilità e la conformità alle richieste dei regolatori. Inoltre, il sistema include anche la possibilità di generare report e analisi per supportare la valutazione del rischio e la gestione della sicurezza dei dati. ✓ Dispositivi: Server e Postazioni ✓ Dispositivi supportati: Supporta tutti i sistemi Windows a partire dalla versione Windows 7 sp2, MAC e Linux ✓ Installazione: Agent/API. ✓ Supporto: viene garantito un tutorial di installazione e 1gg di supporto.	Numero Dipendenti azienda
Pronto Intervento Cyber	**Pronto Intervento Cyber**: Licenza annuale del servizio di pronto intervento che nasce per supportare le attività di gestione di incidenti informatici che compromettono dati personali, sia a causa di una violazione esterna (data breach), sia a causa di vulnerabilità, errore umano o errati processi aziendali (data leak) o, ancora, nel caso in cui attacchi di virus Ransomware compromettano i dati aziendali. A tua disposizione - H24 ed entro 4 ore dalla segnalazione – 1h all'anno di un professionista cyber che ti fornirà le indicazioni e i passi da attuare al fine di ripristinare la Business Continuity aziendale. Il servizio comprende Assistenza H24, 1h di supporto all'anno.	Azienda
GDPR Assessment	**GDPR Assessment** è lo strumento online che permette alle Aziende di verificare e misurare il proprio livello di compliance alla disposizione legislativa privacy, il General Data Protection Regulation- Regolamento UE 2016/679. Il GDPR Swascan fornisce le indicazioni e azioni correttive da compiere a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo. Licenza Full Usage	Azienda

Cybersecurity e impresa: strumenti e prevenzione

CONFAPI BRESCIA

Relatore: Pierguido Iezzi – CEO Swascan