CYBER RISK INDICATORS
DEL SUD ITALIA

AGOSTO 2021

Swascan
TINEXTA GROUP

Indice

Executive Summary

Il servizio **Cyber Risk Indicators** determina e misura il potenziale rischio cyber del settore merceologico o geografico oggetto di analisi L'analisi condotta è riferita al mese di Agosto 2021.

Gli indicatori sono stati determinati con il servizio di Domain Threat Intelligence (DTI)

(https://security.swascan.com)

Per maggiori informazioni sull'approccio metodologico visita:

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

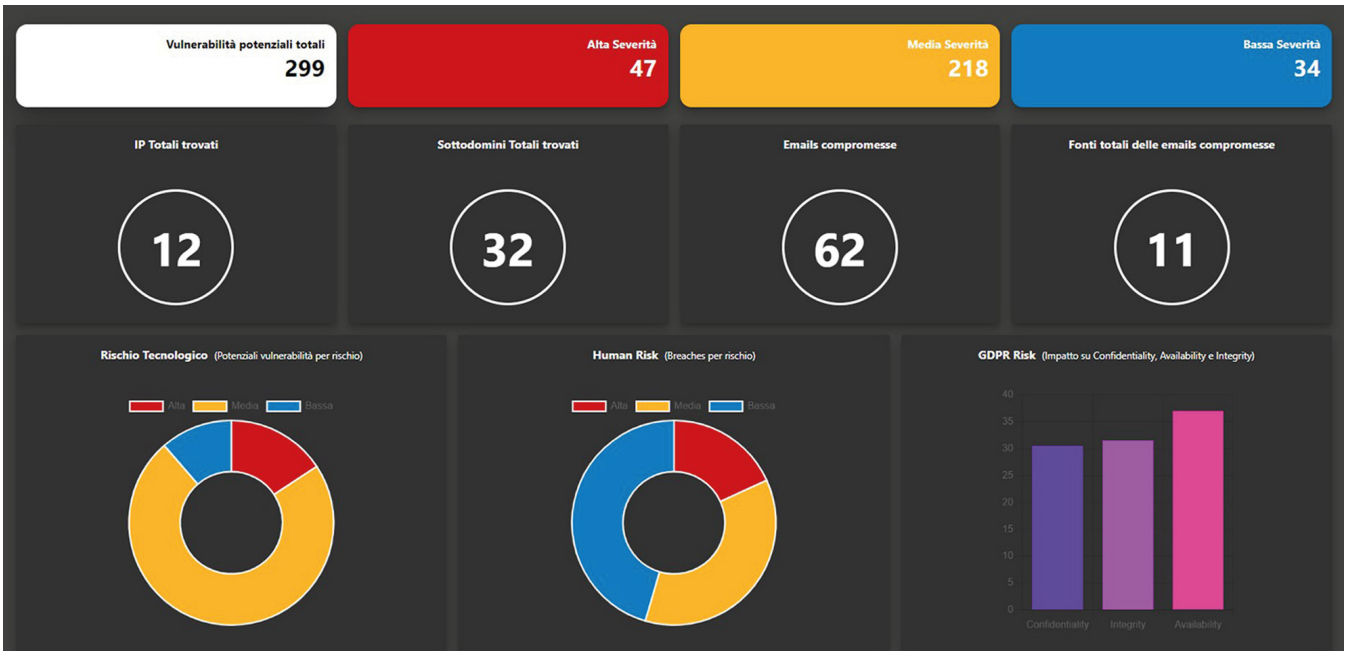
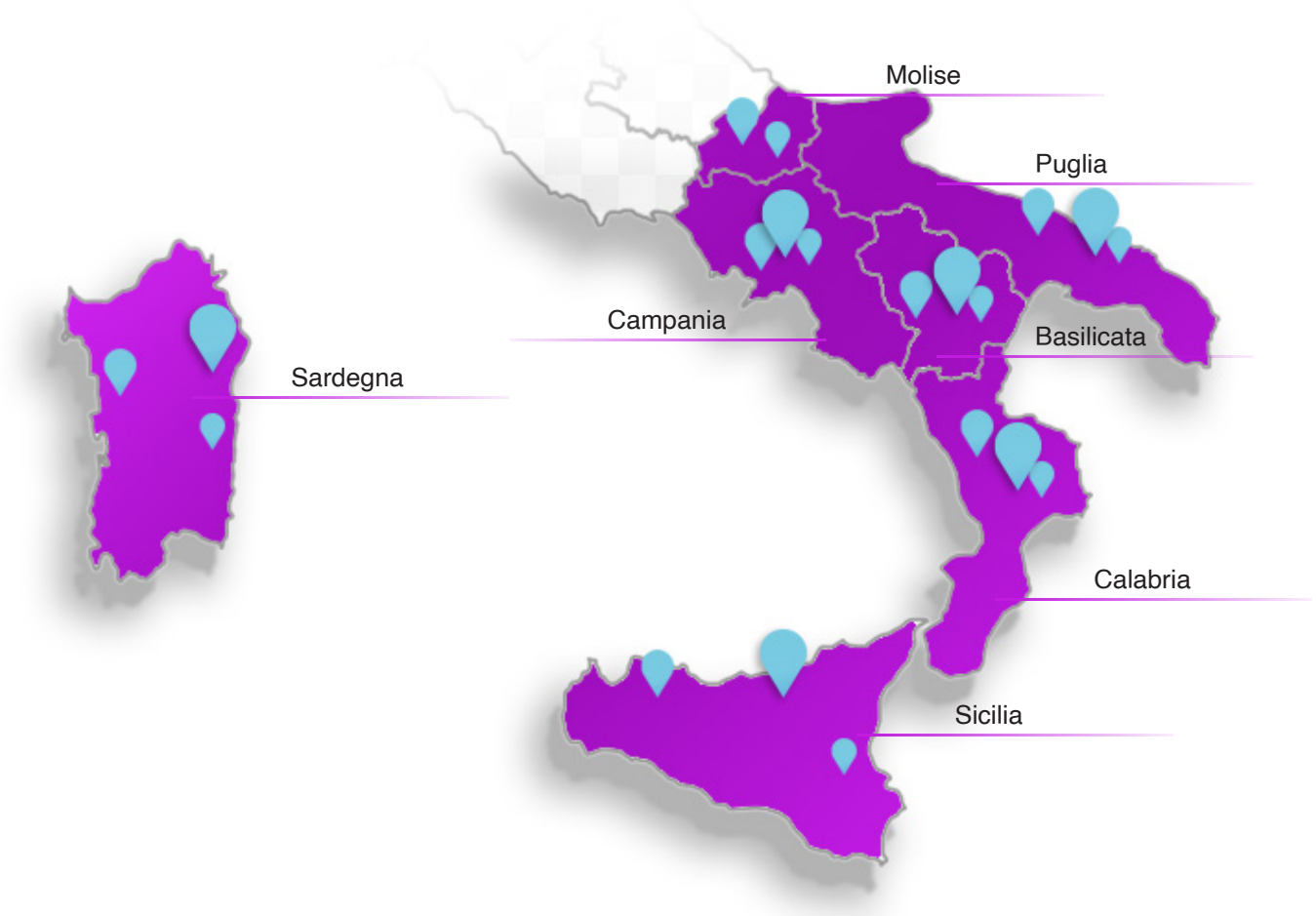


Figura 1 Esempio Dashboard Domain Threat Intelligence – https://security.swascan.com

Executive Summary

L'analisi è stata condotta analizzando 20 aziende del **SUD ITALIA**.
L'area geografica analizzata è riferita alle regioni rappresentate nella mappa.
Le aziende selezionate per ciascuna regione sono tra le prime 100 per fatturato.



Per le prime **6 regioni** (Puglia, Campania, Basilicata, Calabria, Sicilia, Sardegna)
sono state analizzate 3 Aziende ciascuna mentre solo 2 aziende per il Molise.

Executive Summary

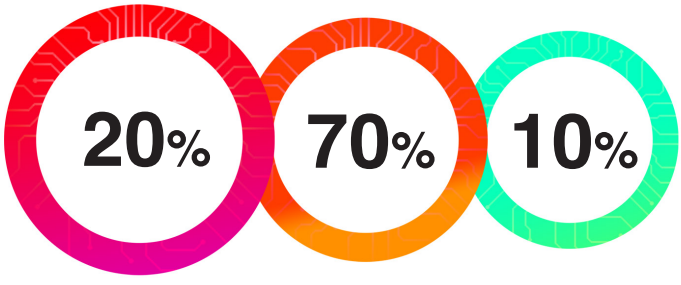
Il **Soc Team di Swascan** ha rilevato un rischio concreto di subire un cyber attack per le aziende campione analizzate. Nello specifico, operando solo su informazioni pubbliche e semipubbliche - disponibili nel web, dark web e deep web - è venuto a conoscenza che le aziende del territorio del campione in esame presentano diversi rischi:

VULNERABILITÀ IN TOTALE

E-MAIL COMPROMESSE

IP ESPOSTI SU INTERNET

SERVIZI ESPOSTI SU INTERNET



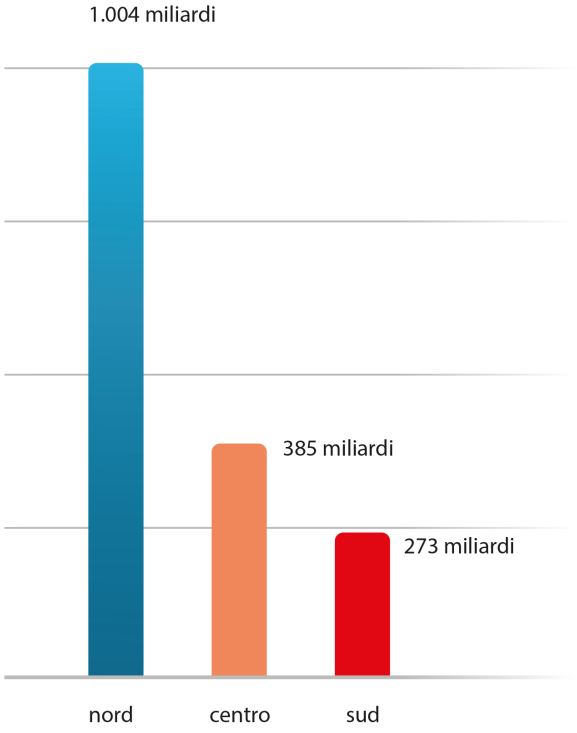
VULNERABILITÀ ALTE ***VULNERABILITÀ MEDIE*** ***VULNERABILITÀ BASSE***

E-MAIL COMPROMESSE IN MEDIA PER DOMINIO

Il SUD ITALIA e il PIL Italiano

I dati Eurostat sul Pil:

Il Prodotto interno lordo del Mezzogiorno è pari a **274 miliardi di euro**, un quarto di quello del nord. Nel dettaglio: nel 2019 il Pil nazionale valeva 1.789 miliardi di euro, così ripartiti: 1.004 miliardi al Nord (591 miliardi nel nord-ovest e 413 miliardi nel nord-est), 385 miliardi al Centro, 273 miliardi al Sud e 620 milioni nelle isole maggiori.



Calabria e Sicilia sono le regioni col più basso reddito pro-capite, ma nel Mezzogiorno le regioni con la minore ricchezza risultano Molise e Basilicata. La Campania invece si afferma come motore economico del Mezzogiorno: dei **274 miliardi** di euro di PIL dell'intero sud Italia, quasi la metà (109,6 miliardi) sono appannaggio proprio della regione intorno a Napoli.

Ovviamente il diverso grado di ricchezza delle diverse aree geografiche si riflette anche nel diverso grado di benessere, con i cittadini del Sud e delle Isole al di sotto delle media per PIL pro-capite. Se in Italia questo indicatore è pari a **29.700 euro** a persona, nelle regioni meridionali peninsulari il valore si riduce a **19.600 euro,** per assottigliarsi ulteriormente a **18.800 euro** per quanto concerne le due regioni insulari.

Il GAP della Digitalizzazione del SUD ITALIA

Lo scenario di rischio Cyber che emerge da questa panoramica realizzata dal Soc Swascan potrebbe essere anche collegato al gap della digitalizzazione - in termini di mancanza di tecnologie/ competenze/processi -.
Come si evince dal **DESI** (Digital Economy and Society Index) regionale 2020, su dati 2019, le regioni del mezzogiorno sono il fanalino di coda.

Il collegamento tra queste deficienze sistemiche e la significativa esposizione registrata, quindi, non è del tutto casuale.

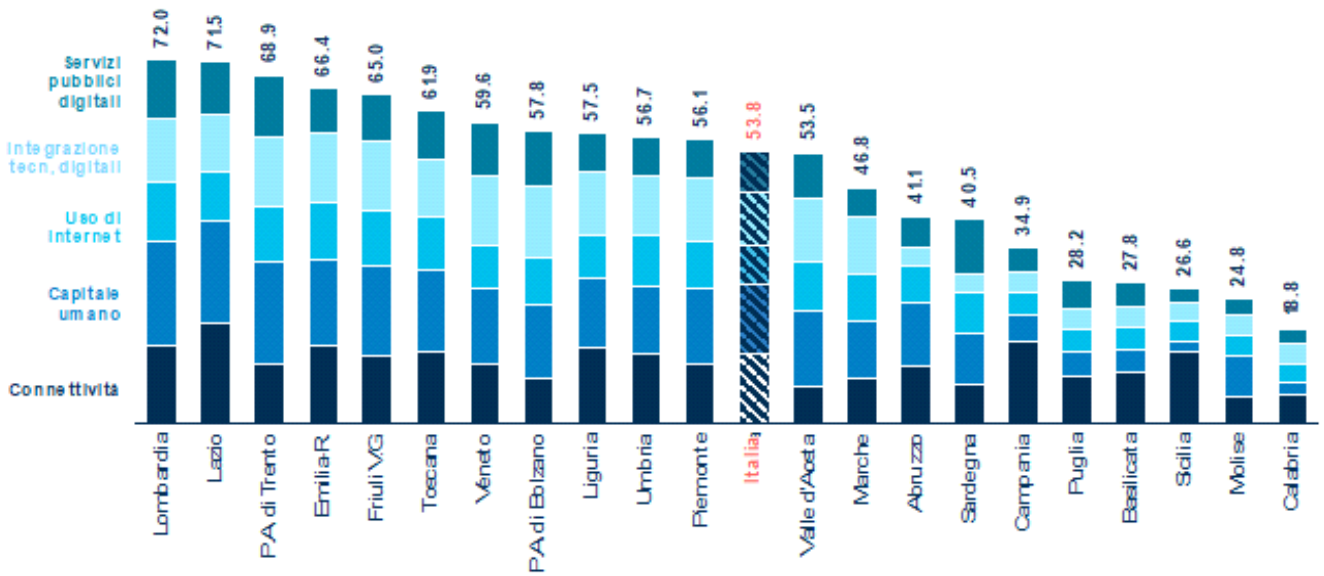


Figura 2: fonte: Osservatorio Agenda Digitale del Politecnico di Milano

Il PNRR una opportunità anche per la Cyber Security

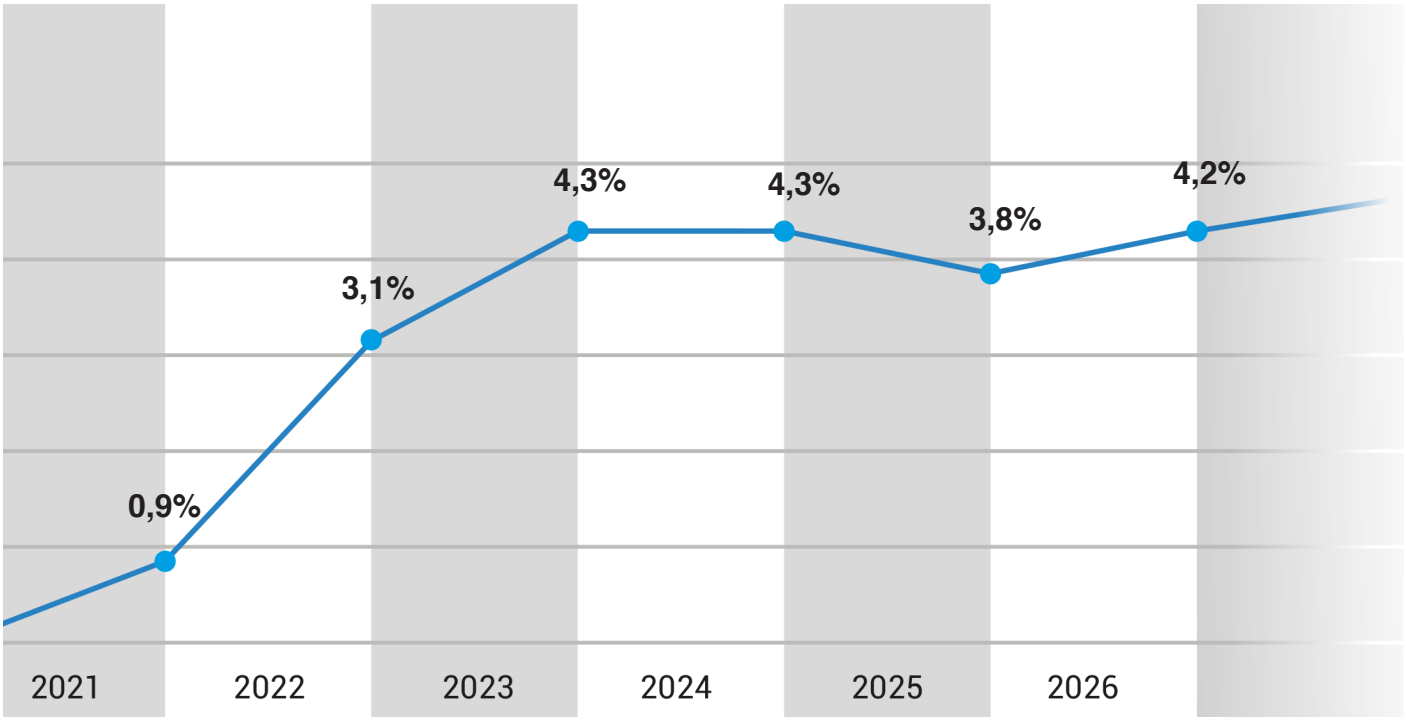
Nonostante le storiche difficoltà economiche del Sud Italia e il divario presente con il Nord, il Piano nazionale di ripresa e resilienza, come riporta il Ministero del Sud, promette di avere un impatto promettente sul Pil della zona grazie ai **221 miliardi** di euro messi a disposizione tramite il recovery fund.

Le stime parlano di una crescita – nel quinquennio 2021-2026 – del **22,4%**, rispetto ai valori registrati nel 2020.

Come riporta lo stesso Ministero in una nota: "L'impatto del **PNRR** sulla crescita del Pil nazionale nell'arco dei cinque anni sarebbe del 15,3% (per il Centro-Nord sarebbe del 13,2%).

Oggi il Pil del Mezzogiorno rappresenta il 22,7% di quello nazionale; nel 2026, se le misure del Piano saranno pienamente applicate, il Pil del Mezzogiorno costituirà il 24,1% del Pil nazionale".

Questo l'impatto sul Pil del Mezzogiorno:



Naturalmente questa crescita prevista a livello economico passa gioco-forza per grandi investimenti in strutture digitali: una grande opportunità per il mezzogiorno di fare un importante passo in avanti nella digitalizzazione e al contempo aumentare la resilienza cyber del proprio perimetro.

Le regioni a rischio attacco informatico

L'analisi condotta attraverso il servizio di Cyber Risk Indicators utilizzando i servizi di Threat Intelligence di Swascan ha permesso di identificare, sulla base del campione analizzato, le regioni maggiormente esposte a possibili attacchi informatici di cybercrime.

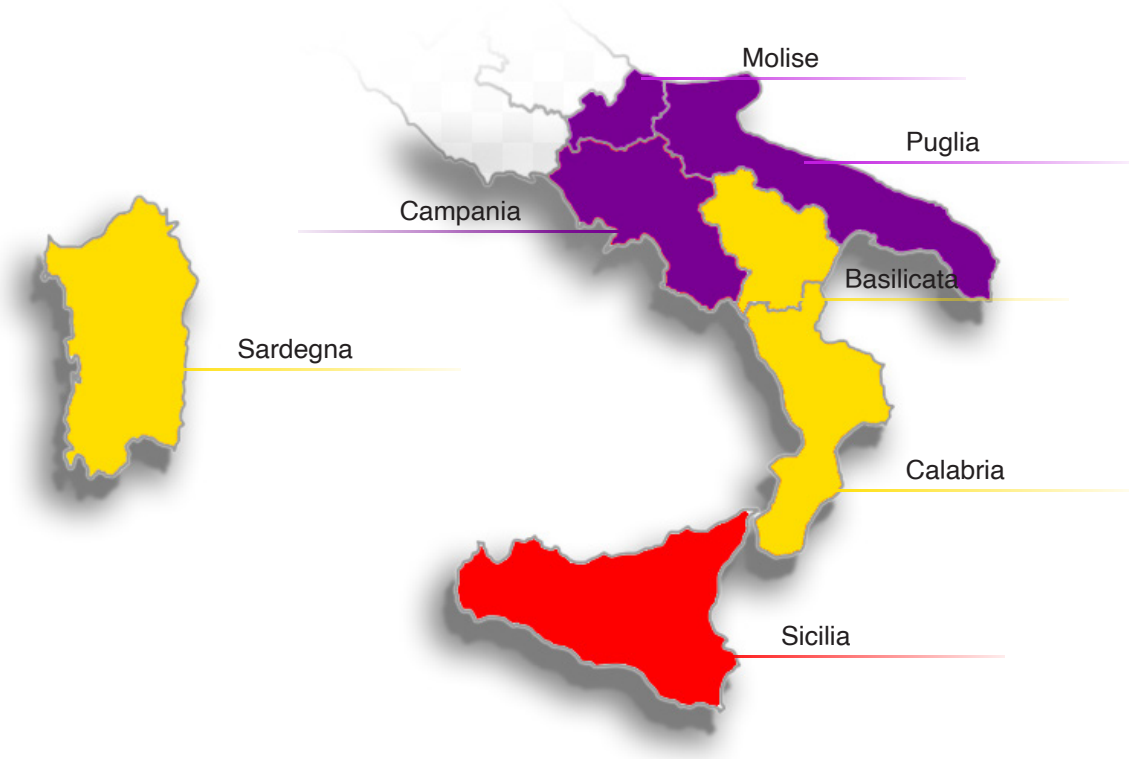
Nello specifico, le regioni esposte a livello Critico - con una media di oltre 50 vulnerabilità già disponibili pubblicamente - sono:

Campania
Puglia
Molise

Segue la Sicilia con una media di vulnerabilità tra 26 e 50 e con un'elevata esposizione al rischio Cyber.

Infine, Basilicata, Calabria e Sardegna hanno una esposizione ai cyber risk di tipo medio essendo stato possibile identificare una media tra **1-25 vulnerabilità.**

DISTRIBUZIONE VULNERABILITÀ PER REGIONE



Un’esposizione così elevata rende vulnerabile il perimetro del sud Italia ad una serie di possibili attacchi da parte di Criminal Hacker. In particolare, il rischio principale è collegato al Ransomware, la minaccia per eccellenza nel panorama del cyber crime.

Più è debole il perimetro, maggiore sarà la probabilità che vengano lanciati attacchi ransomware. Un sistema con un alto numero di vulnerabilità, infatti, rappresenta – a livello di costo/beneficio – per i Criminal Hacker un target molto più appetibile di uno ben difeso.

D’altronde agli aggressori non mancano le “armi” per lanciare i loro attacchi.

Vulnerabilità: exploit e kit di exploit

Quando parliamo di exploit facciamo riferimento ad una parte di codice maligno compilato per sfruttare una vulnerabilità.
I kit, invece, sono un insieme di exploit multipli disponibili sul dark web. Questi permettono ai criminali non necessariamente qualificati di automatizzare gli attacchi sulle vulnerabilità conosciute.

Social engineering

Il social engineering è usato per ingannare e manipolare le vittime, per ottenere informazioni o ottenere l’accesso ai loro computer. Si tratta di una serie di tecniche che vanno a colpire il “fattore umano”: ovvero sfruttano la disattenzione delle persone per invogliarle a cliccare su link malevoli, fornire informazioni personali...
Una delle tecniche più note, il phishing, per esempio, sfrutta le mail per ingannare le persone a divulgare informazioni sensibili o riservate. Non sempre facile da distinguere dai messaggi, perché costruite a regola d’arte per imitare mittenti legittimi, queste truffe possono infliggere enormi danni alle organizzazioni.

Botnet

Le botnet sono grandi reti di computer compromessi, la cui potenza di elaborazione viene utilizzata all’insaputa dell’utente per svolgere attività criminali. Questo può includere la distribuzione di spam o email di phishing o l’esecuzione di attacchi DDoS, ma anche il furto di credenziali.

La portata della minaccia Ransomware per il Sud Italia

Non a caso abbiamo parlato immediatamente di ransomware come minaccia principale per le aziende. Questo tipo di attacco – secondo le stime di Cybersecurity Ventures entro il 2031 supererà 265 miliardi di dollari a livello globale.

Gli attacchi di ransomware sono quindi la minaccia principale soprattutto per le aziende del Sud

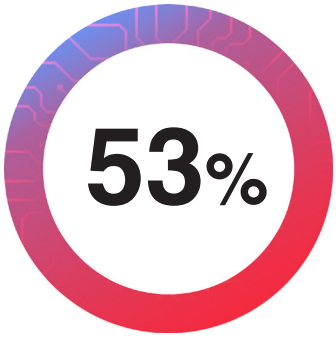
D'altronde il profitto che è in grado di fruttare ai Criminal Hacker è in costante aumento. Schiere di aggressori si sono "convertiti" a questo modello di business, anche quando non possiedono le abilità necessarie a portare avanti gli attacchi. Questo grazie al Ransomware-as-a-Service che, come suggerisce il nome, permette loro di disporre di strumenti e assistenza utili a perpetrare gli attacchi.

YOUR FILE ARE ENCRYPTED

Il **ransomware** è un problema enorme non solo sotto l'aspetto finanziario ma soprattutto per quanto concerne la business continuity. Nel momento in cui il ransomware si attiva in un sistema vulnerabile, i file vengono prima copiati poi crittografati. La prima conseguenza più grave è che gli utenti non possono più lavorare. Inoltre i dati rischiano di essere pubblicati o messi in vendita sul dark web, con potenziali gravi danni alla reputazione. La vittima, quindi, rischia sanzioni e danni d'immagine, oltre a essere sottoposta a riscatto per poter ripristinare la funzionalità dei sistemi. Secondo quanto riporta Cyberreason l'80% delle aziende che cedono ad un riscatto finiscono per subire un secondo attacco (spesso per mano dello stesso gruppo di attori). A questo si aggiunge il fatto che il 46% delle aziende colpite non riesce abitualmente a recuperare la totalità dei dati compromessi. Se in passato questo tipo di attacco era sporadico, adesso è una minaccia costante per qualsiasi organizzazione, come conseguenza della rapidissima evoluzione delle tecniche di attacco.

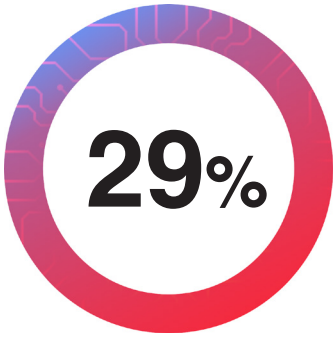
IL DANNO ECONOMICO REALE

Quantifichiamo quali sono le ricadute reali di un attacco ransomware. In primo luogo, si può verificare una riduzione del fatturato aziendale: il 66% delle organizzazioni ha riportato una significativa perdita di entrate a seguito di un attacco ransomware (abbiamo la fonte? Se no attribuite la fonte a Swascan dicendo anche quanti incidenti avete gestito). Inoltre, le richieste di riscatto aumentano: il 35% delle aziende hanno pagato un riscatto tra i 350.000 e 1,4 milioni di dollari, mentre il 7% importi superiori a 1,4 milioni $.



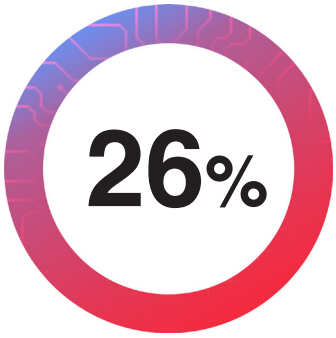
DANNI AL MARCHIO E ALLA REPUTAZIONE:

il 53% delle organizzazioni ha indicato che il proprio marchio e la propria reputazione sono stati danneggiati a seguito di un attacco



LICENZIAMENTI DEI DIPENDENTI:

il 29% ha riferito di aver dovuto licenziare dipendenti a causa di pressioni finanziarie a seguito di un attacco ransomware;

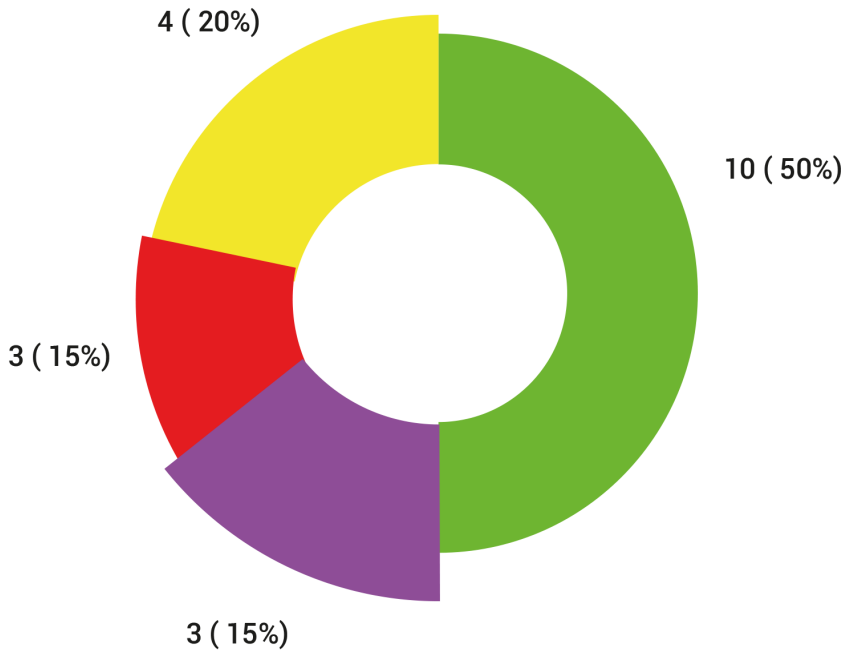


CHIUSURE DI ATTIVITÀ:

un sorprendente 26% delle organizzazioni ha riferito che un ransomware ha costretto l'azienda a chiudere completamente le operazioni.

Sud Italia: i Cyber Risk Indicators

Il numero totale delle potenziali vulnerabilità riscontrate per il settore oggetto di analisi è 489, così distribuite: **10 aziende** (50% del campione) hanno **0 potenziali vulnerabilità**, **4 aziende** (20% del campione) hanno tra **1 e 25 potenziali vulnerabilità**, **3 aziende** (15% del campione) hanno tra **26 e 50 potenziali vulnerabilità** e **3 aziende** (15% del campione) hanno più di **50 potenziali vulnerabilità**.
20 aziende sulle 100 top performer del sud Italia.
La media delle potenziali vulnerabilità è 24, ma è presente 1 azienda che espone circa 200 potenziali vulnerabilità:
escludendola dal calcolo della media, il numero medio di potenziali vulnerabilità per azienda si abbassa da 24 a 15.



TECHNOLOGY RISK INDICATOR

TOTALE DELLE POTENZIALI VULNERABILITÀ

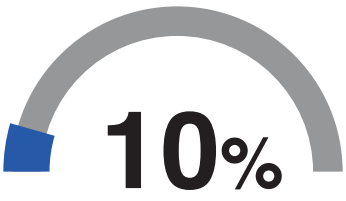
NUMERO MEDIO DELLE POTENZIALI VULNERABILITÀ

Il **Technology Risk Indicator** è determinato dal numero medio delle vulnerabilità potenziali presenti sul campione delle aziende del territorio in analisi seguito dal trend percentuale rispetto al mese precedente. In questo caso sono state identificate **489 vulnerabilità potenziali**; 24 in media per azienda parte del campione.

È stata quindi data indicazione sul valore percentuale medio di ogni livello di severità per le vulnerabilità del settore.

MEDIUM

HIGH



LOW

Le potenziali vulnerabilità identificate fanno principalmente riferimento a:

- ***Sistemi non aggiornati***
- ***Sistemi non patchati***
- ***Sistemi di Remote desktop Protocol vulnerabili***

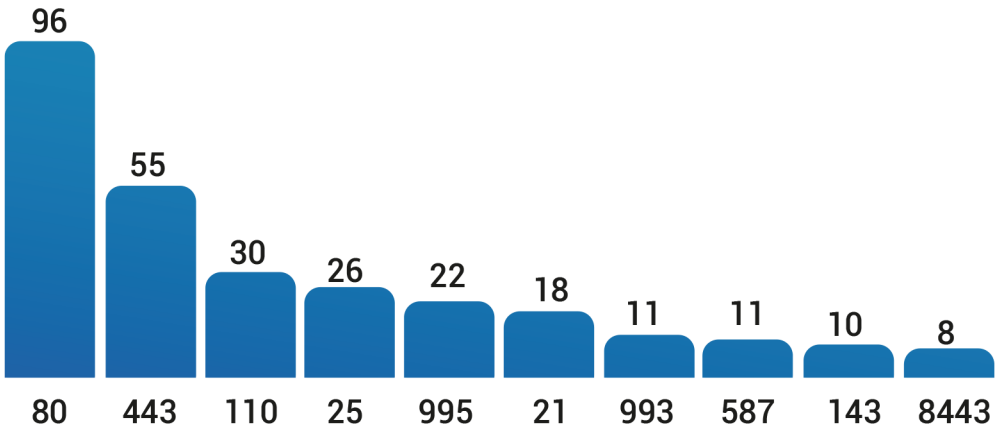
Il **Technology Risk Indicator** quantifica l'esposizione al rischio di un attacco informatico attraverso lo sfruttamento di vulnerabilità tecnologiche con l'esecuzione di exploit.

Tutti i dati contenuti nella ricerca fanno riferimento a informazioni disponibili pubblicamente e semi-pubblicamente. Ogni asset digitale esposto su Internet è costantemente vittima di attacchi informatici. I dati ottenuti attraverso gli attacchi vengono spesso pubblicati e condivisi nelle community del Web, Dark Web e Deep Web.

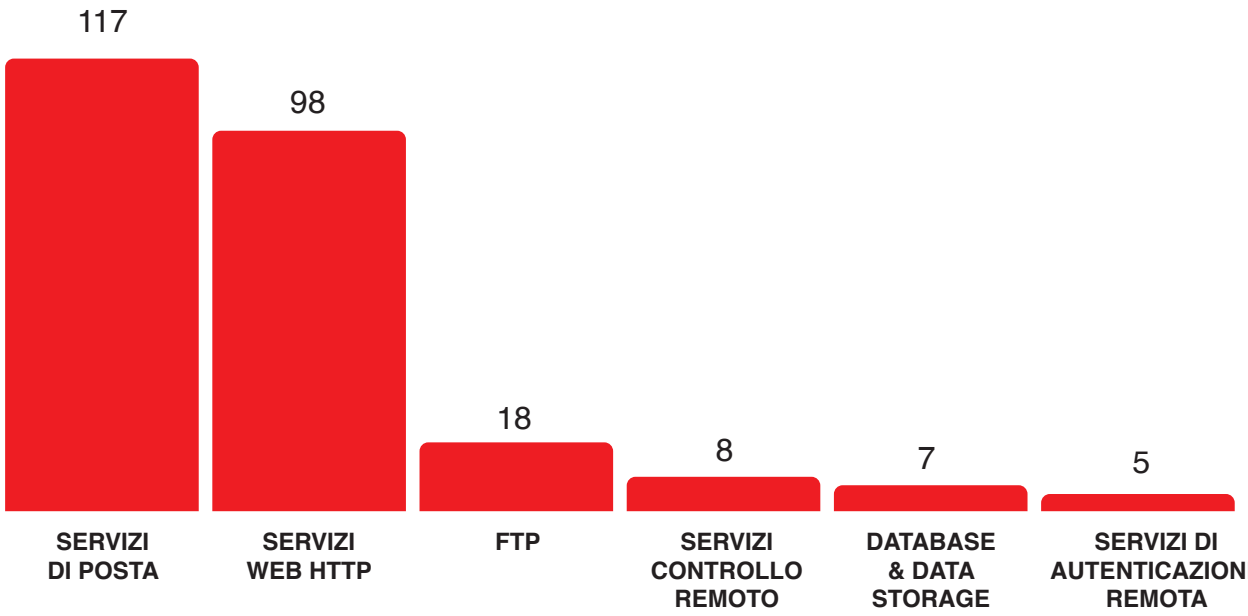
L'analisi è frutto del servizio Swascan di Domain Threat Intelligence (DTI), che ricerca le informazioni relative alle potenziali vulnerabilità dei domini, sottodomini ed email compromesse. Il servizio non effettua alcun test sul target ma raccoglie, analizza e clusterizza le informazioni disponibili a livello **OSINT** (Open Source Intelligence) e **CLOSINT** (Close Source Intelligence) presenti su database, forum, chat e newsgroup.

Come evidenziato, delle 20 aziende analizzate la metà non ha presentato vulnerabilità.
A seguito della raccolta ed analisi delle informazioni, è anche emerso che su un totale di **123 indirizzi IP** appartenenti alle **20 aziende** oggetto di analisi, vi sono **346** porte esposte con i seguenti servizi potenzialmente vulnerabili:

346
TOTALE PORTE ESPOSTE



Dei 346 potenziali servizi esposti, è possibile considerare a rischio i seguenti servizi:



SERVIZI DI POSTA esporre apertamente un servizio di posta non adeguatamente aggiornato, potrebbe potenzialmente portante alla compromissione dei sistemi e all'utilizzo di questi come ulteriore vettore d'attacco

SERVIZI WEB HTTP l'utilizzo di un protocollo non ciftato può comportare un rischio elevato della confidenzialità delle informazioni che transitano tra client e server

FTP l'utilizzo di un protocollo non cifrato, nel caso di un'intercettazione dell'username e della password da parte di un attaccante, comporterebbe un rischio per l'integrità, per la confidenzialità e per la disponiblilità del dato

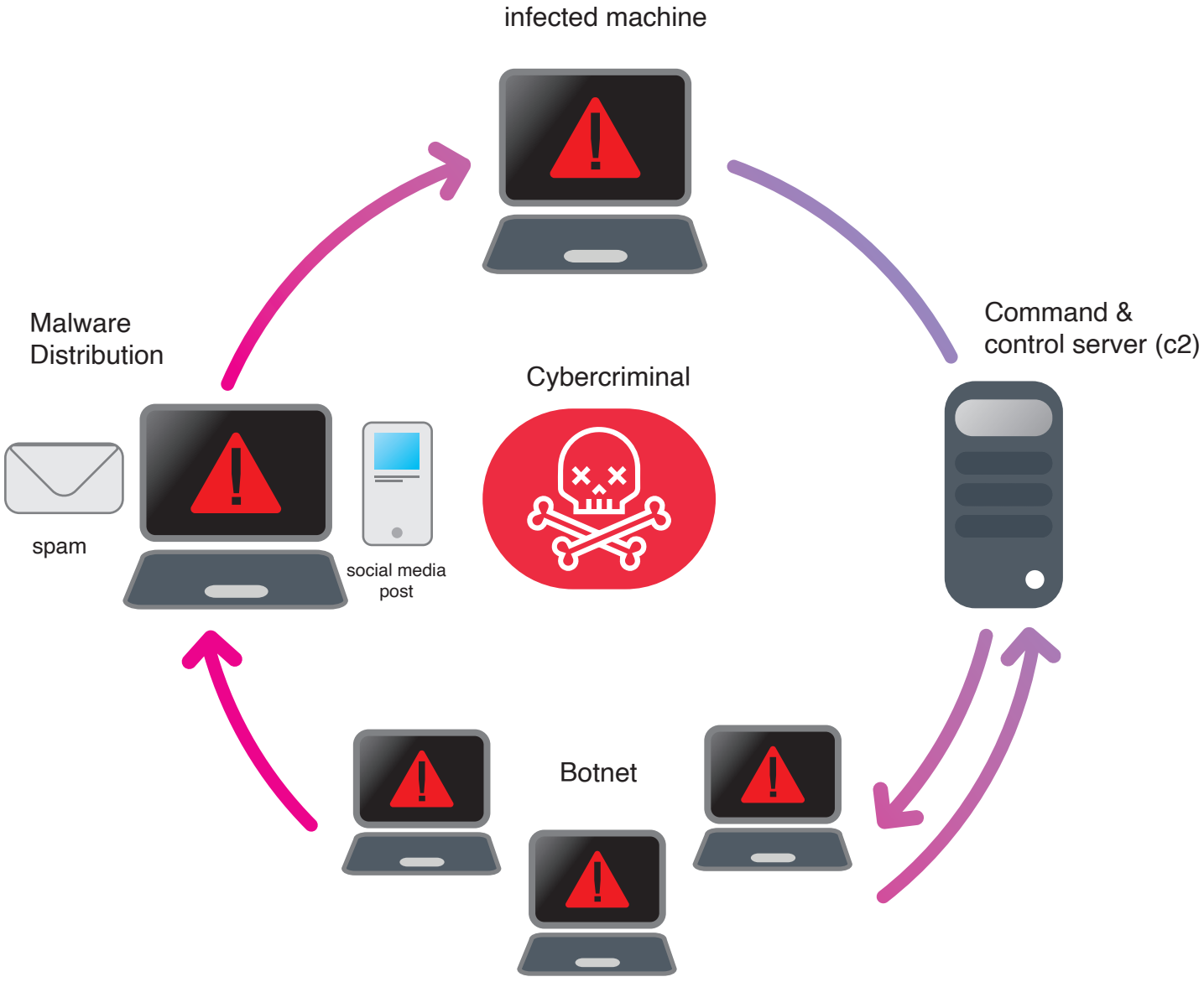
SERVIZI CONTROLLO REMOTO permettere connessioni in ingresso in grado di garantire il controllo remoto spesso protette da un solo fattore di autenticazione, espone le aziende al rischio di bruteforcing da parte degli attaccanti che, nel caso avessero successo, comporterebbero la compromissione dei sistemi e di parte dell'infrastruttura delle aziende

DATABASE & DATA STORAGE l'esposizione di database direttamente su Internet può comportare, qualora non debitamente protetti, l'esecuzione da parte di criminali di attacchi volti ad ottenere un accesso non autorizzato ai dati

SERVIZI DI AUTENTICAZIONE REMOTA eventuali attacchi potrebbero lanciare attacchi di tipo DoS (Denial Of Service) sull'azienda che espone il servizio oppure sfruttare i servizi esposti per rilanciare attacchi DDoS (Distributed Denial Of Service) verso altre infrastrutture, con conseguenze immaginabili

Le criticità identificate potrebbero permettere:

- la fase di exploiting della Cyber Kill Chain. L'exploiting consiste nell'esecuzione di uno script (exploit), che sfruttando un errore di configurazione o una vulnerabilità del sistema target, permette l'accesso al sistema senza autorizzazioni.
- Lo sfruttamento di credenziali di accesso compromesse da botnet presenti sui dispositivi di dipendenti, clienti o fornitori (vedi attacco alla Regione Lazio). Nello specifico da attenzionare sono i servizi di controllo remoto e ftp.



L'attività di **Cyber Risk Indicator** effettuata attraverso il servizio web di Domain Threat Intelligence ha permesso di enumerare (non classificare o trattare) il numero delle e-mail/password compromesse:

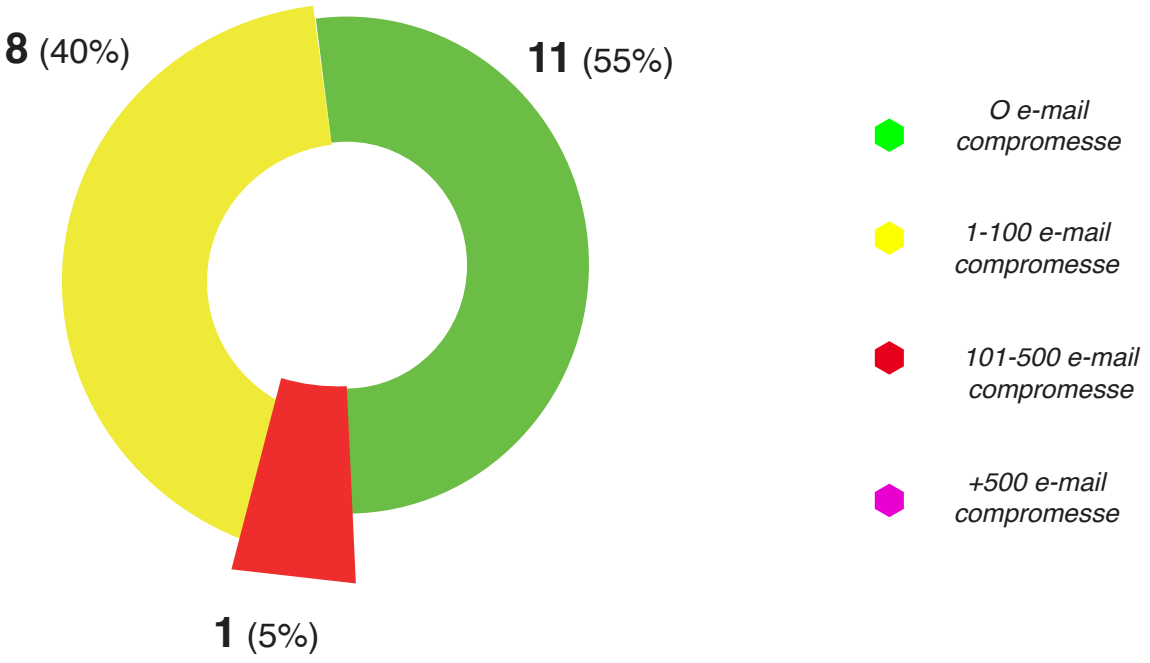
536
E-MAIL COMPROMESSE

27
MEDIA PER DOMINIO

92
TYPOSQUATTING

5
MEDIA PER DOMINIO

Il numero totale delle e-mail compromesse riscontrate per il territorio oggetto di analisi è 536 (pubblicate in 85 data breach) e così distribuite: **11 aziende** (55% del campione) ha **0 e-mail compromesse**, **8 aziende** (40% del campione) hanno tra **1 e 100 e-mail compromesse** e **1 azienda** ha tra **101 e 500 e-mail compromesse**. La media delle e-mail compromesse è 27, ma è presente **1 azienda** che ha oltre **220 e-mail compromesse**: escludendola dal calcolo della media, il numero medio di e-mail compromesse per azienda si abbassa da 27 a 16.



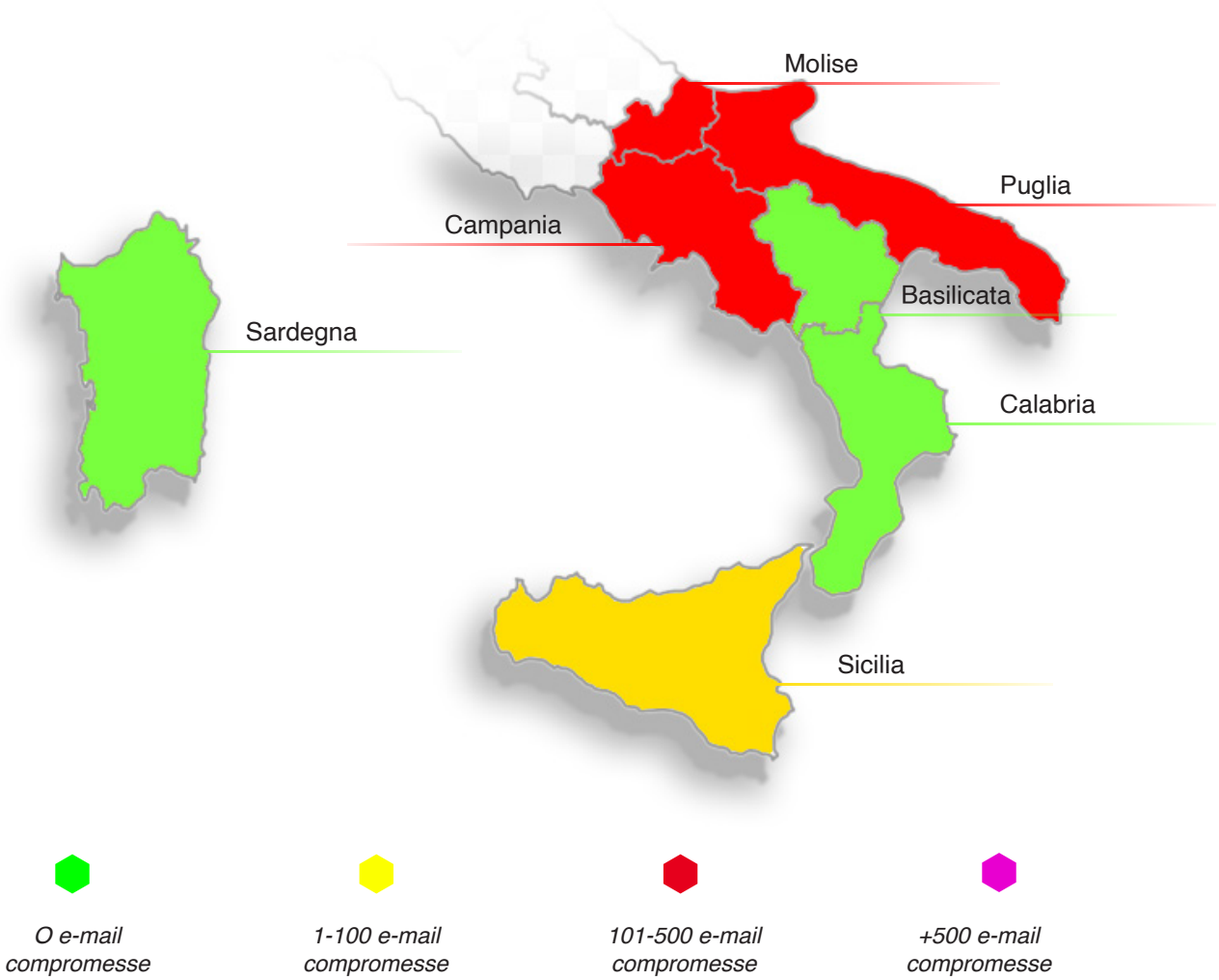
Le regioni a rischio attacco di Social Engineering

L'analisi condotta attraverso il servizio di **Cyber Risk Indicators** utilizzando i servizi di Threat Intelligence di Swascan ha permesso di identificare, sulla base del campione analizzato, le regioni maggiormente esposte a possibili attacchi informatici di social engineering.

Nello specifico le regioni esposte a livello Critico con una media di oltre 101 e-mail/password compromesse e disponibili pubblicamente ci sono:

Puglia
Campania
Molise

DISTRIBUZIONE E-MAIL COMPROMESSE PER REGIONE

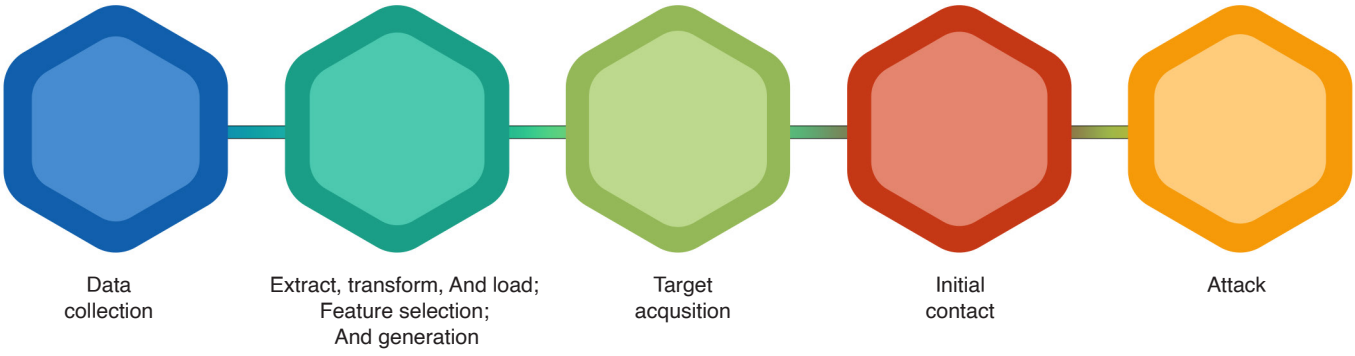


Segue la Sicilia con una media di email/password compromesse tra 1 e 100

Social Engineering Attack

La presenza delle e-mail compromesse unitamente alle informazioni associate a ciascun utente di fatto espongono le aziende a possibili attacchi di:

- **Phishing e Spamming**
- **Spear Phishing**
- **Smishing e Spoofing**
- **Credential Stuffing**
- **Account Take Over**

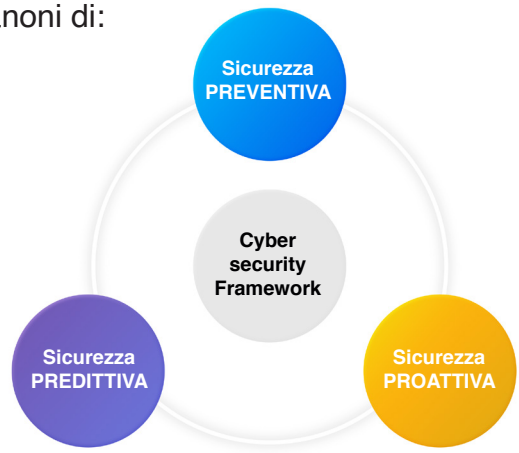


AUMENTARE LA RESILIENZA DEL PERIMETRO

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna.

Per questo motivo vanno consolidati e rispettati i tre canoni di:

- **Sicurezza Predittiva**
- **Sicurezza Preventiva**
- **Sicurezza Proattiva**



Cyber Security Framework

Sicurezza Preventiva

1. Verifica e misura il Rischio Cyber
2. Definisce i piani di remediation
3. Indica il Rischio esposto al Layer di Sicurezza Proattiva
4. Fornisce le aree di Investigazione alla Sicurezza Predittiva

Sicurezza Predittiva

1. Identifica le minacce fuori dal perimetro aziendale operando a livello di web, dark web e deep web
2. Ricerca eventuali minacce emergenti
3. Effettua attività di Early Warning
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di attenzione alla Sicurezza Proattiva

Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale
2. Contrasta e blocca gli attacchi informatici
3. Gestisce i Cyber Incident
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di investigazione alla Sicurezza Predittiva

Domain Threat Intelligence: la Domain Threat Intelligence ricerca le informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed e-mail compromesse. Il servizio non effettua alcun test sul target ma opera unicamente sulle informazioni disponibili sul web, dark web e deep web e raccoglie, analizza e clusterizza le informazioni disponibili a livello OSINT (Open Source Intelligence) e CLOSINT (Close Source Intelligence) presenti su database, forum, chat, newsgroup.

- Potenziali Vulnerabilità
- Dettagli delle Vulnerabilità in termini di CVE, impatti e severity
- Impatti GDPR (CIA)
- Numero dei Sottodomini
- Numero Potenziali e-mail compromesse (vengono solo conteggiate e non raccolte o trattate)
- Numero delle Source delle e-mail compromesse
- Typosquatting

Cyber Threat Intelligence: è il servizio evoluto di Threat Intelligence di Swascan. Effettua una attività di ricerca, analisi e raccolta delle informazioni presenti a livello web, Darkweb e deep web relativamente al dominio/target di analisi. Nello specifico:

- Rileva la presenza di credenziali/source/data all'interno di Data Leaks
- Identifica le informazioni mediante analisi di post pubblicati nei Forum
- Botnet relative a dispositive di Clienti, Fornitori e dipendenti
- Botnet con credenziali e relative url di login page
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Early Warning Threat Intelligence: è il servizio di Early Warning che segnala giornalmente le evidenze che vengono identificate e raccolte nel dark web e nel deep web relativamente al target di analisi.

- Data Leaks
- Scraping data
- Phishing data
- Botnet

Rischio Tecnologico

Vulnerability Assessment: esegue la scansione di siti e applicazioni web per identificare e analizzare in modo proattivo le vulnerabilità di sicurezza.

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

Rischio Umano

Phishing/Smishing attack Simulation: permette alle aziende di prevenire i danni dovuti ad attacchi di phishing/smishing attraverso vere e proprie simulazioni di attacco. È infatti possibile, grazie ad un'interfaccia web, inviare vere e proprie campagne di phishing/ smishing simulate che generano delle insostituibili occasioni di apprendimento per i dipendenti. Questi ultimi, infatti, grazie ad attacchi simulati di questo tipo, riusciranno in futuro ad individuare una vera e-mail di phishing o un messaggio di smishing e ad evitarla. Una attenta attività di formazione e consapevolezza dei propri dipendenti, tramite vere e proprie simulazioni di attacco phishing/ smishing, può contribuire a ridurre la nostra esposizione alla compromissione.

Awareness: corsi di formazione dedicati di Cybersecurity in aula o tramite Webinar. Attività di consapevolezza ed informazione per il personale tecnico, per i dipendenti e per i Top Manager.

Processo - Compliance

ISO27001: ISO/IEC 27001:2013 (ISO 27001) è lo standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano).
Dal momento che l'informazione è un bene che aggiunge valore all'organizzazione, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

ICT Security Assessment: l'ICT Security Assessment è una metodologia proprietaria di Swascan che permette alle aziende di verificare e misurare il proprio livello di rischio cyber e di valutare l'efficacia delle misure di sicurezza adottate.
Il servizio fornisce le indicazioni e le azioni correttive da adottare a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo.

SOCaaS: la progettazione, la messa in esercizio e il mantenimento di un Security Operation Center può essere costoso e complesso. Il servizio SOC as a Service Swascan è la soluzione più efficace, efficiente, coerente e sostenibile per i contesti aziendali. Il Soc as a service con il suo servizio di Monitoring & Early Warning permette di identificare, rilevare, analizzare e segnalare gli attacchi informatici cyber prima che possano trasformarsi in una minaccia concreta per l'azienda. Un team dedicato nell'attività di Monitoring & Early Warning reattivo delle minacce informatiche sulle reti locali, ambienti cloud, applicazioni ed endpoint aziendali. Il nostro team di Security Analyst monitora i dati e le risorse ovunque risiedano all'interno dell'azienda. Indipendentemente dal fatto che le risorse siano archiviate nel cloud, in locale o in entrambi. L'attività di monitoring e segnalazione permette di agire solo quando viene identificata una minaccia reale.

Incident Response Management: è un insieme di risorse e procedure organizzate e strutturate per garantire la corretta reaction e gestione degli attacchi informatici. In caso di incidente informatico, Data Breach, DDoS, attacco Ransomware e/o relativo Data Recovery è necessario affrontare e rispondere con un approccio strutturato, predisposto e organizzato per affrontare in maniera efficace ed efficiente la violazione della sicurezza e per ridurre gli impatti a livello di Business Continuity aziendale. L'obiettivo dell'Incident Response è quello di:

- **Gestire l'incidente**
- **Limitare i danni diretti e indiretti**
- **Ridurre tempi e costi di ripristino**

About us

Swascan

È una Cyber Security Company innovativa nata da un'idea di Pierguido Iezzi e Raoul Chiesa La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security testing e di 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: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Technical Contributors:

Pierguido Iezzi
Fabrizio Rendina
Andrea D'Angelo
Dario Buonocore
Riccardo Michetti
Riccardo D'Ambrosio
Matteo Biagini
Mario Cambria
Daniele Scozia
Andrea Melignano
David Brunetti
Soc Swascan Team

Editing & Graphics:

Federico Giberti
Antonio Contrastato

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI

Disclaimer

La ricerca svolta da Swascan si è basata su siti contenenti dati e numeriche fonti di ricerche OSINT e CLOSINT tramite Threat Intelligence.

Questa pubblicazione non rappresenta necessariamente lo stato dell'arte – data la natura transitoria delle fonti – e Swascan si riserva la prerogativa di aggiornamento periodico.

Fonti di terze parti sono citate a seconda dei casi. Swascan non è responsabile del contenuto delle fonti esterne, compresi i siti web esterni a cui si fa riferimento in questa pubblicazione.

La presente pubblicazione ha uno scopo puramente informativo. Essa deve essere accessibile gratuitamente.

Né Swascan né alcuna persona che agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.