Swascan
TINEXTA GROUP

Cyber Risk Indicators

Infrastrutture Critiche Italia

Febbraio 2022

INDICE

"La Russia è il Paese più attrezzato al mondo per la guerra cibernetica, dobbiamo quindi alzare il livello di guardia, anche attraverso una migliore e più puntuale informazione per estendere le resilienza del Paese, come fa questo rapporto che identifica le principali vulnerabilità in settori strategici del Paese**"**

Adolfo Urso

Senatore della Repubblica e
Presidente del Comitato parlamentare per
la sicurezza della Repubblica (COPASIR)

Disclaimer

La ricerca svolta da Swascan è basata su dati OSINT e CLOSINT ottenuti 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.

Chi Siamo

Swascan S.r.l.

Swascan è una **Cyber Security** Company italiana 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 **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 Group), 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.

Tinexta Cyber S.p.A.

Tinexta Cyber Tinexta Group, è il polo italiano della **Cyber Security** con forti competenze verticali e soluzioni custom proprietarie per la mitigazione e la governance dei rischi legati alla sicurezza digitale. Con servizi basati in Italia e nel rispetto della compliance EU in ambito di data residency, data protection e GDPR, la società assiste i clienti con attività specializzate di assessment e advisory e si occupa del design, development ed integration delle soluzioni, curandone anche il monitoring e management.

Tinexta Group

Tinexta, quotata al segmento STAR della Borsa di Milano, ha riportato i seguenti Risultati consolidati al 31 dicembre 2021: Ricavi pari a Euro 375,4 milioni, EBITDA pari a Euro 93,0 milioni e Utile netto pari a Euro 39,6 milioni. Tinexta Group è tra gli operatori leader in Italia nelle quattro aree di business: Digital Trust, Cybersecurity, Credit Information & Management, Innovation & Marketing Services. La Business Unit Digital Trust eroga, attraverso le società InfoCert S.p.A., Visura S.p.A., Sixtema S.p.A. e la società spagnola Camerfirma S.A., prodotti e soluzioni per la digitalizzazione: firma digitale, identità digitale, onboarding di clientela, fatturazione elettronica e posta elettronica certificata (PEC) per grandi aziende, banche, società di assicurazione e finanziarie, PMI, associazioni e professionisti. Al 31 dicembre 2021 il personale del Gruppo ammontava a 2.393 dipendenti.

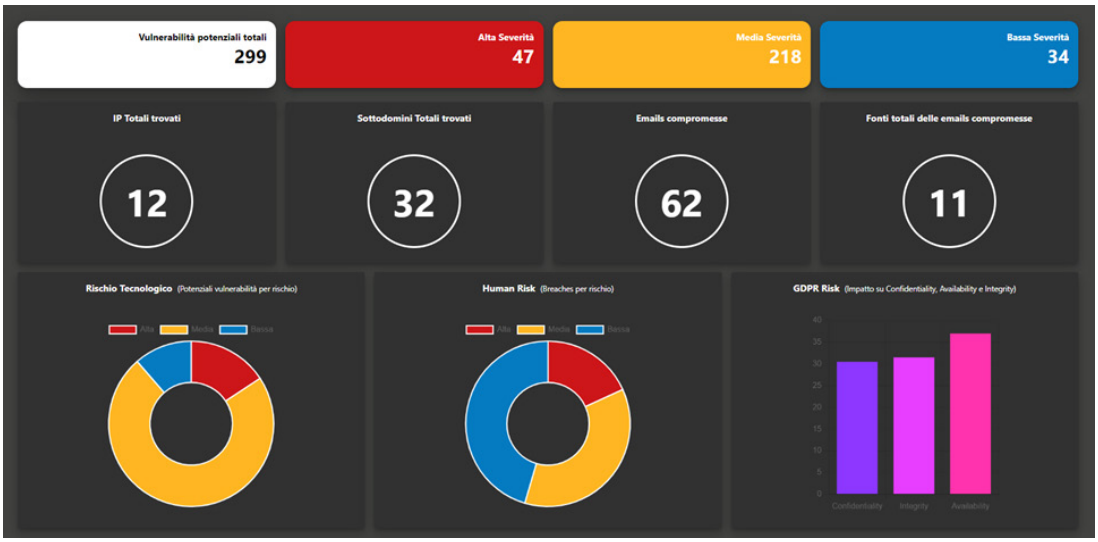
Executive Summary

Il servizio Cyber Risk Indicators determina e misura il potenziale rischio cyber del settore preso in esame.
Per questo focus, l'analisi condotta - riferita ai dati raccolti nel mese di febbraio 2022 - ha esaminato il livello di resilienza cyber di 20 infrastrutture critiche italiane presenti in questi quattro settori:

- Energia
- Trasporti
- Pubblica Amministrazione Centrale
- Sanità

Approccio metodologico

Gli indicatori sono stati identificati 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/



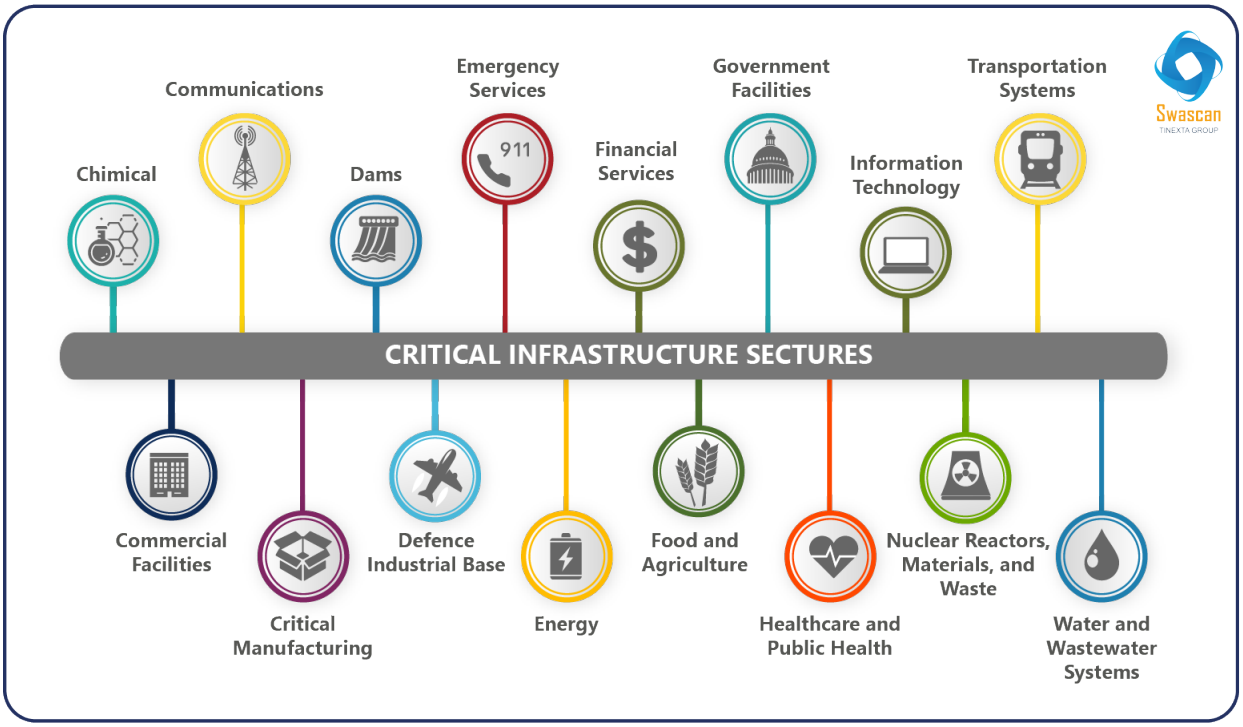
Un Esempio di output di Domain Threat Intelligence – https://security.swascan.com

Infrastrutture critiche e Cyber security

La situazione di conflitto scoppiata alla fine del febbraio 2022, che ha visto coinvolti Russia e Ucraina ha acceso ancora di più i riflettori sulla potenziale esposizione ad attacchi cyber delle infrastrutture critiche.
In quella che è stata definita guerra ibrida – o dottrina Gerasimov – infatti, uno dei principali dogmi è quello di utilizzare le competenze cyber per attaccare e disabilitare le infrastrutture avversarie.

In Ucraina è successo nei giorni precedenti all'invasione, ma questo scenario è tutt'altro che un caso limite legato alle peculiarità dello scontro Kiev – Mosca, potrebbe ben presto riproporsi in qualsiasi altro Paese.
Naturalmente, maggiore sarà la digitalizzazione dei Paesi coinvolti in scenari di scontro – non necessariamente armato, ricordiamo – maggiore sarà il rischio che un attacco cyber risulti catastrofico.

Le infrastrutture critiche, come la produzione e la distribuzione di energia, i trasporti, la sanità o anche la Pubblica Amministrazione, d'altronde, stanno diventando sempre più complesse e dipendenti da reti di dispositivi collegati. Solo decenni fa, le reti elettriche e altre infrastrutture critiche funzionavano in modo isolato. Ora sono molto più interconnesse, sia in termini geografici che tra i settori.



I cyberattacchi alle infrastrutture critiche possono causare impatti economici e sociali di massa.
Non esistono strategie migliori dei cyber attacchi per causare ansia e instabilità, soprattutto quando a essere presi di mira sono i sistemi e le reti che consentono le nostre attività quotidiane.
I cyberattacchi perpetrati contro le infrastrutture critiche, quindi, sono diventati un'altra potentissima arma di interruzione di massa.

D'altronde, un'interruzione dei servizi essenziali, anche se breve, può occupare significative risorse civili e militari in una regione o in un intero paese.
La marcia verso un mondo più interconnesso e in rete, aumenta la probabilità che i cyberattacchi contro le infrastrutture critiche possano essere usati come nuove armi di distruzione di massa. In questo nuovo ambiente, di minacce, più che mai abbiamo bisogno di aumentare e sfruttare le partnership tra governo e settore privato per mitigare e neutralizzare queste minacce informatiche.
Non si tratta, sfortunatamente, di congetture, ma di una realtà a cui è necessario prepararsi.

Campaign	Starting year	Attribution	Countries Affected	Targets
Stuxnet	2010	US and Israel	Iran	Uranium enrichment plants
Dragonfly 2.0	2015	Russia	Switzerland, US, Turkey and Ukraine	Electricity, nuclear, water supply and aviation sector
Shamoon	2016	Iran	Saudi Arabia	Aramco and Saipem S.P.A
BlackEnergy	2017	Russia	Ukraine	Electricity distribution network
NotPetya	2017	Russia	Ukraine, but with global effects	Finance, transportation, energy, and healthcare
Industroyer	2017	Non- attributed (Russia)	Ukraine	Electrical substations
Triton/Trisis	2017	Russia	Saudi Arabia	Oil companies

Figura 1 Alcuni esempi di Cyber attacchi contro infrastrutture critiche. Source: Izycki and Vianna

Oltre a compromettere le risorse fisiche, gli attacchi informatici ai servizi fondamentali di una società funzionano anche come armi psicologiche e strategiche. Le interruzioni causate alle infrastrutture critiche possono minare la fiducia nello stato.

Tali attacchi possono servire come minacce esistenziali a regimi instabili. Come armi strategiche, i cyberattacchi alle infrastrutture critiche che causano interruzioni di massa hanno il potenziale di impegnare significative risorse militari ed economiche nello stesso momento in cui la nazione affronta una minaccia militare.

Tali attacchi hanno il potenziale di occupare completamente il tempo e l'attenzione dei decisori e dei comandanti sul campo, facendoli mancare o ignorare altre minacce in sospeso.
Gli attacchi possono avvenire inosservati, con i "cattivi" che rimangono dormienti all'interno dei sistemi per un lungo periodo di tempo.

La natura di un attacco può cambiare nel tempo, nel senso che un'intrusione può progredire in un'operazione di raccolta di informazioni e furto di dati, prima di degenerare in un attacco denial-of-service o ransomware. La progressione di un attacco può cambiare a seconda della natura dell'attore. L'obiettivo degli attori non statali o criminali nel condurre attacchi informatici può essere guidato dal profitto o incentrato sul causare danni economici, mentre gli attori statali possono favorire la raccolta di informazioni e la creazione di opzioni strategiche o risultati.

Nel caso della Corea del Nord, per esempio, gli obiettivi possono essere sia finanziari che di raccolta di informazioni, in quanto raccolgono conoscenze tecniche e i mezzi finanziari per acquistare i materiali e le attrezzature necessarie.
L'ubiquità dei sistemi in rete e l'ampia disponibilità di strumenti di intrusione informatica non lasciano immune nessun paese o settore di infrastrutture critiche.

La situazione in Italia - Summary

Tenendo in mente questi presupposti, Swascan ha deciso di effettuare un'analisi campionaria delle infrastrutture critiche nel nostro Paese – per sondare il loro livello di resilienza.
Utilizzando la metodologia dei Cyber Risk Indicators, questi sono i risultati restituiti dall'analisi:

SOCIAL ENGINEERING RISK

Swascan
TINEXTA GROUP

EMAIL COMPROMESSE

Totale	Media
52555	2628

FONTI EMAIL COMPROMESSE

Totale	Media
424	21

DOMINI TYPOSQUATTING

Totale	Media
353	18

CYBER THREAT INTELLIGENCE

Swascan
TINEXTA GROUP

Botnet

Totale	Media
52985	2649

Le modalità di attacco

Le principali modalità di attacco che potrebbero essere messe in campo contro le infrastrutture critiche sono le seguenti:

1) **DDoS:** Un attacco DDoS (distributed denial-of-service) è una tecnica di cyber attack utilizzata al fine di interrompere il normale funzionamento di server, servizi o reti tramite un flusso di traffico internet anomalo e oltre la capacità del target;

2) **Sfruttamento Vulnerabilità:** In cybersecurity, una vulnerabilità è una criticità che può essere sfruttata dai Criminal Hacker per ottenere un accesso non autorizzato a un sistema informatico. Dopo aver sfruttato una vulnerabilità, un criminale informatico può eseguire codice dannoso, installare malware e persino rubare dati sensibili;

3) **Social Engineering:** Nel contesto della sicurezza informatica, il social engineering è l'uso dell'inganno per manipolare le persone nel divulgare informazioni riservate o personali che possono essere utilizzate a fini fraudolenti. In altre parole, le persone possono essere ingannate nel condividere informazioni che altrimenti non divulgherebbero. La variante più comune è il Phishing, mail costruite ad hoc per ingannare il destinatario e costringerlo a rivelare dati o informazioni sensibili;

4) **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 e-mail di phishing, così come l'esecuzione di attacchi DDoS, ma anche il furto di credenziali di accesso a servizi aziendali e non solo;

5) **Supply Chain attack:** ogni azienda o infrastruttura non è più oramai monolitica, ma si appoggia su una lunga e complessa supply chain digitale. I Criminal Hacker possono colpire il proprio target proprio andando a compromettere un fornitore a monte;

6) **0 – Day:** Questa è l'insidia maggiore per ogni organizzazione, gli zero-day sono così noti perché lasciano appunto – zero giorni di tempo – agli sviluppatori per correggere una vulnerabilità prima che venga sfruttata. In essenza sono criticità che vengono scoperte solo nel momento in cui un attacco è già in corso.

Vulnerabilità delle Infrastrutture critiche

In dettaglio, è stato rilevato come la maggior parte delle vulnerabilità potenziali rilevate sia di tipo medium (77%) che denota comunque un significativo rischio di possibile sfruttamento.

Quando si parla di vulnerabilità rilevate, specifichiamo che non è stato effettuato alcun test di sicurezza sul target, ma il SOC Swascan ha operato unicamente sulle informazioni raccolte a livello OSINT e CLOSINT e disponibili sul Dark Web

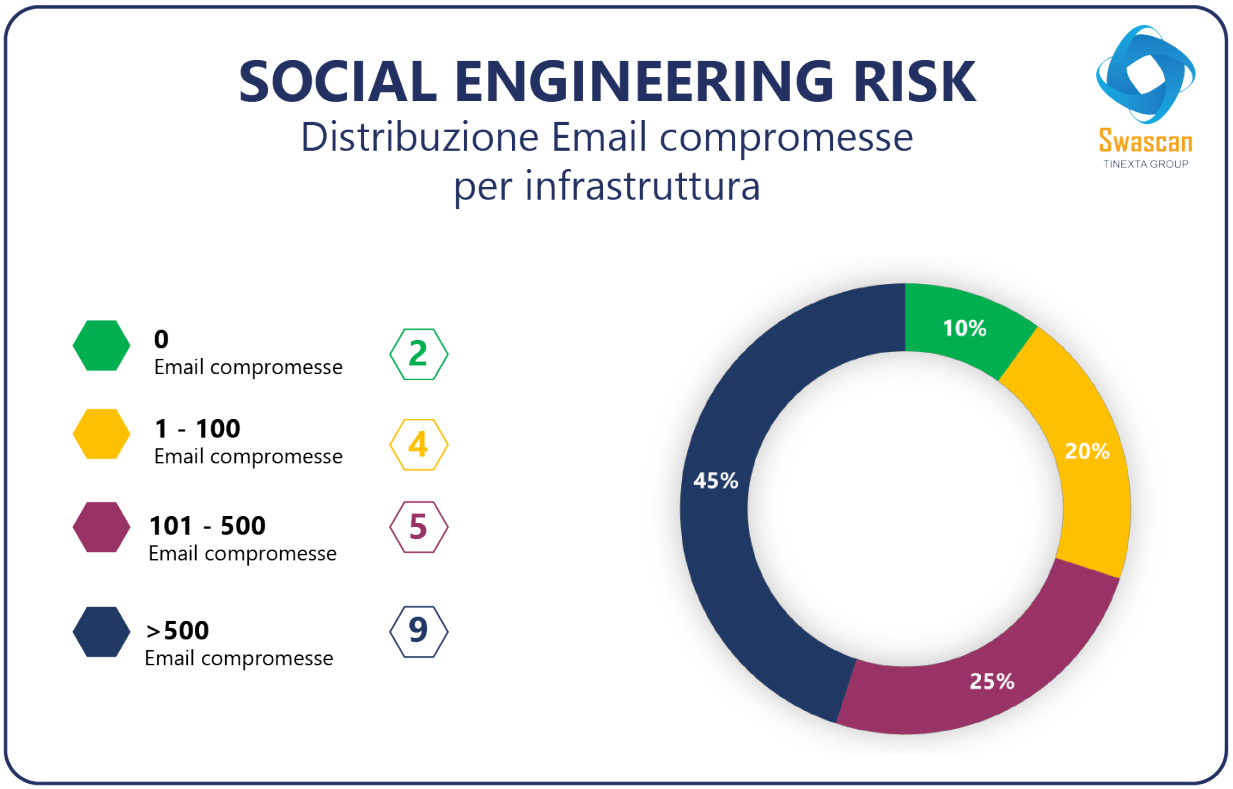
Social Engineering - Email compromesse

L'analisi Social Engineering ha permesso di individuare un totale di **52555 mail compromesse**, con una **media di 2628** mail per dominio analizzato.

Le e-mail potenzialmente compromesse riportate all'interno del report fanno riferimento all'uso delle stesse su siti terzi compromessi e/o all'interno di Data Breach Database.

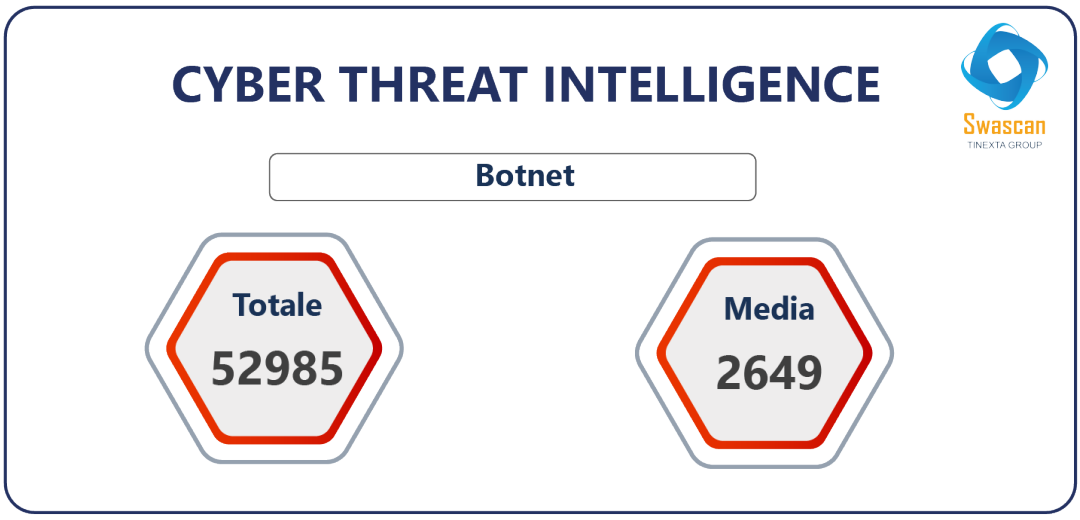
Una mail compromessa è un'arma potente delle mani di un Criminal Hacker esperto, questa può essere utilizzata per prendere il controllo degli account; mandare altre mail a fornitori o colleghi o semplicemente per diffondere ancora più velocemente un malware all'interno di un'organizzazione.

Delle 20 aziende campione, 18 avevano almeno un indirizzo email compromesso, come si evince dalla tabella di seguito:



Botnet

Le botnet sono grandi reti di computer compromessi (chiamati BOT), la cui potenza di elaborazione viene utilizzata all'insaputa dell'utente per svolgere attività criminali. Questo può includere la distribuzione di spam o e-mail di phishing, così come l'esecuzione di attacchi DDoS, ma anche il furto di credenziali di accesso a servizi aziendali e non solo.



All'interno dei **20** casi esempio sono presenti **52985** Bot; una media di **2649** Bot per azienda.

Si specifica che i Bot rilevati non sono presenti all'interno della struttura, ma fanno riferimento a dispositivi che dall'esterno hanno interagito con gli asset dei target analizzati.
Questi potrebbero essere device di ogni genere, impiegati da dipendenti, fornitori o utenti che in un lasso di tempo di non oltre 4 anni hanno in qualche modo interagito con il target per portare a termine le loro attività.
Particolare attenzione va posta sul possibile rischio derivante da questa interazione se fosse proprio proveniente dai device di dipendenti o fornitori.

Cyber Security Framework

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno solidificati e rispettati i tre canoni di:

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

Sicurezza Predittiva

1. Domain Threat Intelligence
2. Cyber Threat Intelligence
3. Early Warning Threath Intelligence
4. Technology Monitoring
5. Social Threat Intelligence
6. Supply Chain Cyber Risk

Sicurezza Preventiva

1. Vulnerability Assessment
2. Network Scan
3. Penetration Test
4. Code Review
5. Phishing Attack
6. Smishing Attack
7. Security Management
8. GRC Assessment
9. Cyber Academy
10. DevSecOps
11. Cyber Security Framework Checkup
12. Ransomware Attack Simulation
13. SOC Performance Simulation
14. Zero Day Attack Simulation
15. CISO as a Service
16. Competence Center as a Service

Sicurezza Proattiva

1. Security Operation Center
2. Incident Response Team

Come Difendersi

Sicurezza Predittiva

1. Identifica le minacce aziendali fuori dal perimetro aziendale operando a livello di Web, Darkweb e Deepweb;
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 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 Proattiva

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

Sicurezza Predittiva

Domain Threat Intelligence: La Domain Threat Intelligence ricerca le informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed email compromesse. Il servizio non effettua alcun test sul target. Opera unicamente sulle informazioni disponibili sul web, Darkweb e deepweb. Raccoglie, analizza e clusterizza le informazioni disponibili a livello OSINT (Open Source Intelligence) e Closint (Close Source Intelligence) presenti su database, forum, chat, newsgroup.
Nello specifico, in base al dominio-target di analisi, identifica:

- 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 Deepweb relativamente al dominio/target di analisi.
Nello specifico:

- Data Leaks: credenziali/source/data
- Identifica Forum/Chat ...
- 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 Darkweb e deep web relativamente al target di analisi.
Nello specifico:

- Data Leaks
- Scraping data
- Phishing data
- Botnet

Sicurezza Preventiva

Tecnologico

Vulnerability Assessment: Esegue la scansione di siti e applicazioni web per identificare e analizzare i 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.

Human Risk

Phishing/Smishing attack Simulation: Permette alle aziende di prevenire i danni dovuti ad attacchi di phishing/smishing attraverso delle vere e proprie simulazioni di attacco. È infatti possibile, attraverso un'interfaccia web inviare vere e proprie campagne di phishing/ smishing simulate che generano delle insostituibili occasioni di apprendimento per i dipendenti. I dipendenti, infatti, grazie a questi attacchi simulati riusciranno, in futuro, ad individuare una vera e-mail di phishing o un messaggio di smishing e ad evitarla. Un'insostituibile attività di formazione e awareness dei tuoi dipendenti tramite vere e proprie simulazioni di attacco phishing/smishing .

Awareness: 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.

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.

Sicurezza Proattiva

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 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 incidenti 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.

Technical Contributors:

Pierguido Iezzi
Fabrizio Rendina
Matteo Biagini
Riccardo Bracale
David Brunetti
Dario Buonocore
Mario Cambria
Daniele Capponi
Riccardo D'Ambrosio
Andrea D'Angelo
Alessandro Di Liberto
Alessandra Garau
Riccardo Michetti
Fabio Pensa
Gianmarco Daniele
Soc Swascan Team.

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

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