Swascan
TINEXTA CYBER

Cyber Risk Indicators

Sanità Italiana

2022 e 2021 a confronto

swascan.com
info@swascan.com

SOMMARIO

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.

I Cyber Risk Indicators:

- Cyber Risk Indicators: Blue Economy (Giugno 2021)
- Cyber Risk Indicators: Energy (Giugno 2021)
- Cyber Risk Indicators: Sanità (Agosto 2021)
- Cyber Risk Indicators: Sud Italia (Settembre 2021)
- Cyber Risk Indicators: Pubblica Amministrazione e Capoluoghi Italiani (Ottobre 2021)
- Cyber Risk Indicators: European Healthcare
- Cyber Risk Indicators: Infrastrutture Critiche Italia (Febbraio 2022)

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 **Aprile 2022** - ha esaminato il livello di resilienza cyber di 30 strutture sanitarie - pubbliche e private, distribuite uniformemente sul territorio della penisola .

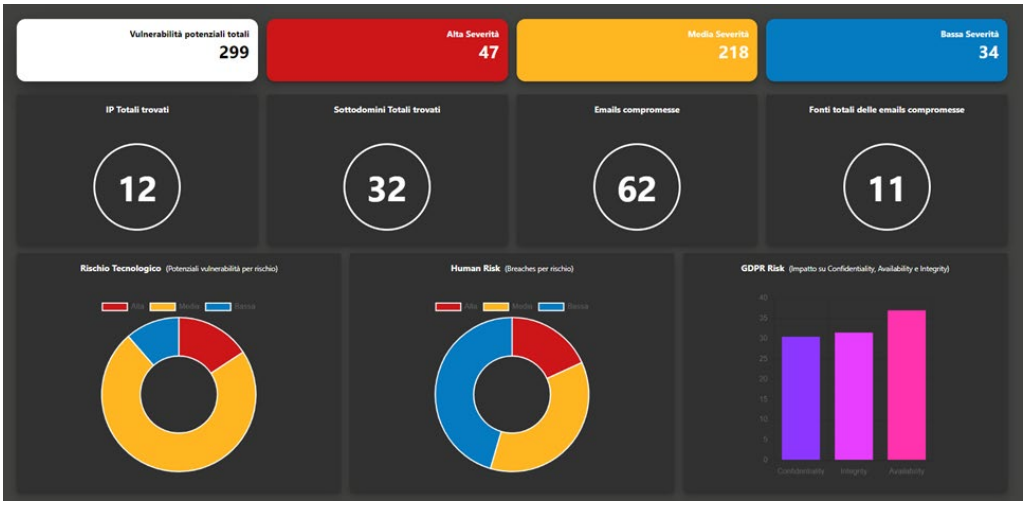
Approccio Metodologico

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

La Sanità Sempre Nel Mirino

Nel mese di agosto 2021, **Swascan** aveva esaminato per la prima volta il livello di esposizione al rischio cyber del comparto sanità italiano.
Per comprendere come sia evoluto lo stato dell'arte della sicurezza informatica all'interno del settore Healtcare a quasi un anno di distanza, il **Team SoC** ha deciso di analizzare nuovamente un campione di aziende e strutture – pubbliche e private – alla ricerca di vulnerabilità potenziali e/o email compromesse.
Ma per capire come mai questa categoria di infrastrutture critiche facciano così "gola" ai Criminal Hacker dobbiamo fare un passo indietro.
Il settore Healtcare, infatti, è da lungo tempo oggetto delle mire dei Criminal Hacker. Il dato, in qualsiasi sua forma, è la vera merce di scambio nel mondo dei criminali informatici, ma non tutte le informazioni sono uguali.

Nell'ultimo decennio il settore sanitario si è trasformato radicalmente grazie alle tecnologie digitali. La pandemia ha solamente accelerato dati e processi operativi, imponendo anche al mondo della sanità di cambiare.
A causa della natura dei dati medici, la sicurezza informatica nel settore sanitario è diventata una sfida critica. Per esempio, è possibile bloccare una carta di credito rubata e ottenerne una nuova. Ma se trapelano informazioni su esami di laboratorio o malattie, è impossibile "cancellarle". Non solo, le falle nei sistemi elettronici clinici possono mettere in pericolo la salute e potenzialmente anche la vita di un paziente.

Ma non è solo l'alto valore dei dati ad attirare i Criminal Hacker. Strutture come ospedali e cliniche raramente possono permettersi periodi di disservizio e downtime causati da un Cyber attacco, per ovvi motivi.
I criminali informatici, forti di questa nozione, ne approfittano per cercare di usare l'importanza vitale di queste strutture come leva per forzare il pagamento di un ricatto (questo è il caso di attacchi come il ransomware, in particolare).

Tutto questo scenario è sicuramente stato amplificato dall'arrivo dell'IoT, ma anche dell'eterogeneità di sistemi e strumenti digitali impiegati nelle strutture.
Più device vengono introdotti, maggiore sarà la possibilità per un attaccante di trovare una vulnerabilità e lanciare un attacco.
Fatta questa premessa, diamo uno sguardo ai dati estrapolati per questo 2022 dal team **SoC Swascan.**

I Dati 2022

Tenendo in mente questi presupposti, utilizzando la metodologia dei Cyber Risk Indicators, questi sono i risultati restituiti dall'analisi:

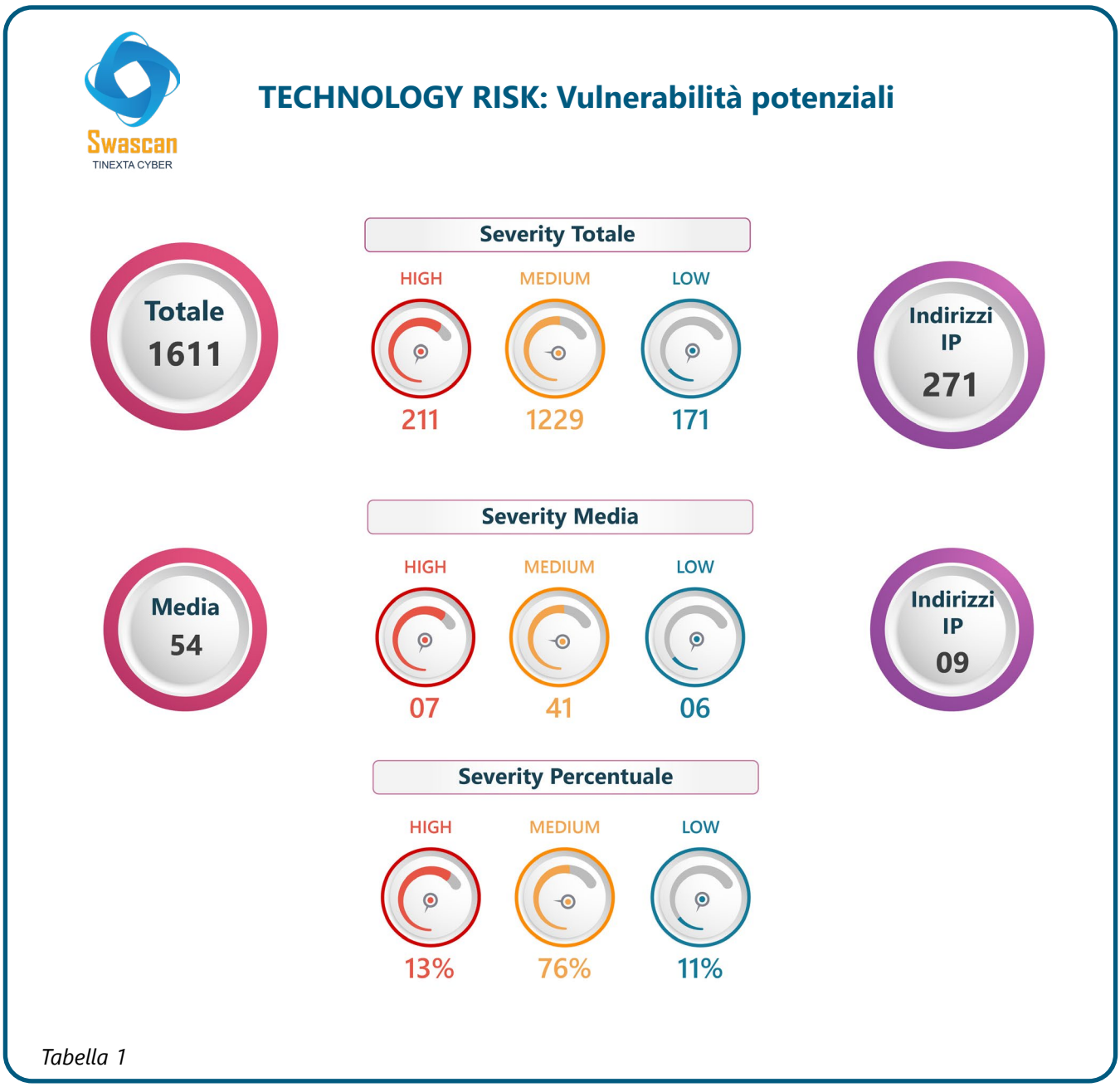


Tabella 1

Come si evince da questa prima macro tabella (Tabella 1), il maggior numero di potenziali vulnerabilità è ascrivibile alla categoria medium con 1229 riscontri analizzati e restituiti dalla tecnologia di Threat Intelligence Swascan. Non è comunque da sottovalutare la presenza di oltre il 10% di vulnerabilità potenziali di tipo High. Questo, come suggerisce il nome sono le più pericolose in quanto richiedono un minor sforzo da parte dei Criminal Hacker per ottenere un Exploit di successo.

Swascan
TINEXTA CYBER

SOCIAL ENGINEERING RISK

EMAIL COMPROMESSE	
Totale	Media
7286	243

FONTI EMAIL COMPROMESSE	
Totale	Media
283	09

DOMINI TYPOSQUATTING	
Totale	Media
158	05

Tabella 2

Nella seconda macro tabella (*Tabella 2*), sono invece raccolti gli indicatori che denotano un possibile rischio di attacco tramite social engineering. In particolare la presenza di email potenzialmente compromesse.

D'altronde, ogni infrastruttura è sicura quanto le persone che la compongono. Per questo motivo il social engineering rimane anche una delle tecniche preferite dai Criminal Hacker per portare a termine un attacco.
Come si evince dal grafico, sono state rilevate un totale di **7286 email compromesse**; una **media di 243** per dominio analizzato.

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.

I Dati A Confronto Con Il 2021

Il sample di dati analizzato permette di tracciare un confronto diretto con quanto emerso durante la prima analisi del settore Healthcare.

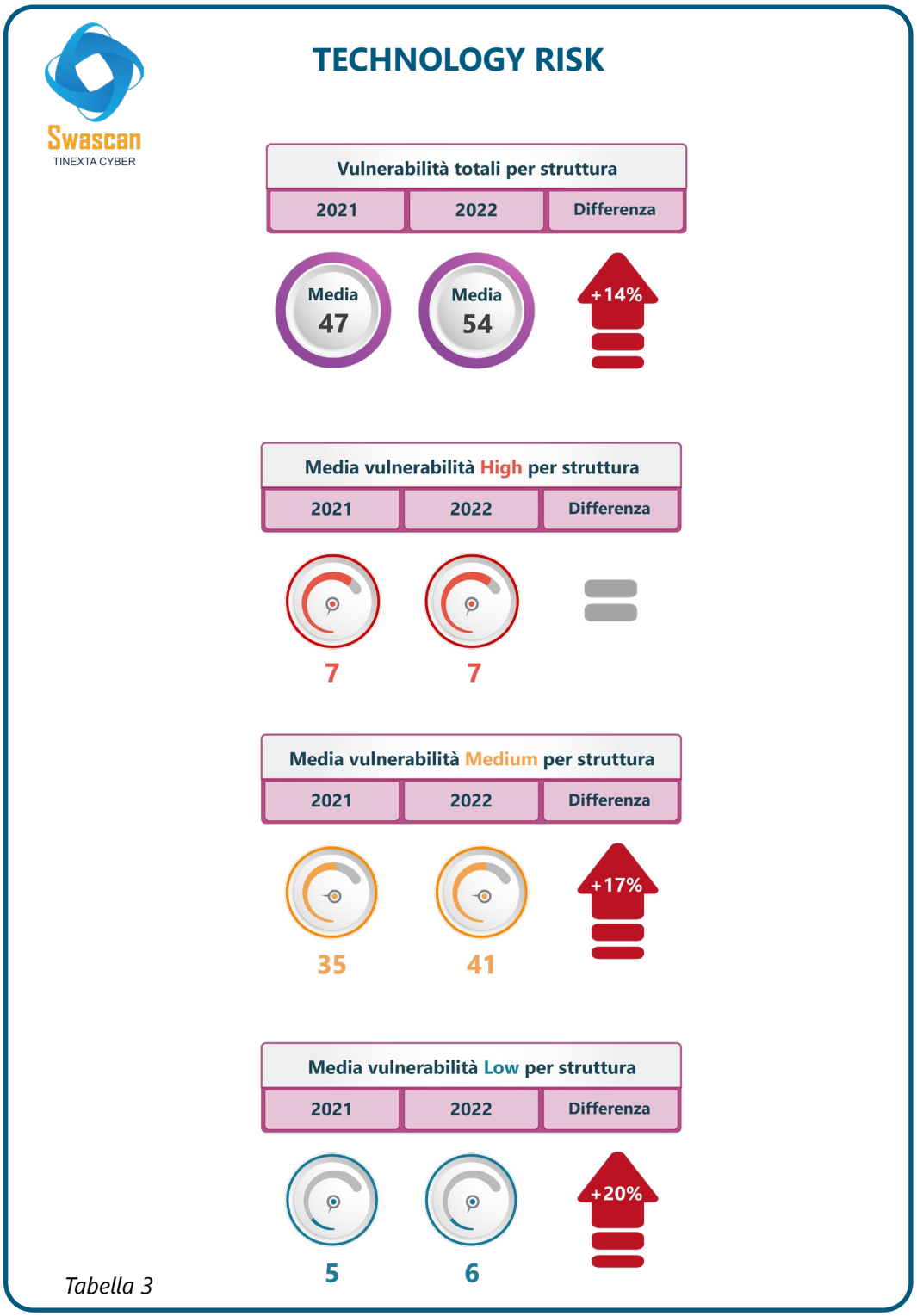


Tabella 3

Come si può vedere dal grafico precedente (Tabella 3) non ci sono stati significativi cambiamenti per quanto riguarda le vulnerabilità HIGH, ma questa è l'unica notizia positiva.

Infatti, sul campione analizzato, è possibile osservare come in media ci sia stato un **incremento** di **vulnerabilità potenziali totali del 14%**, un incremento di **vulnerabilità potenziali Medium del 17%** e delle vulnerabilità **potenziali Low del 20%**.

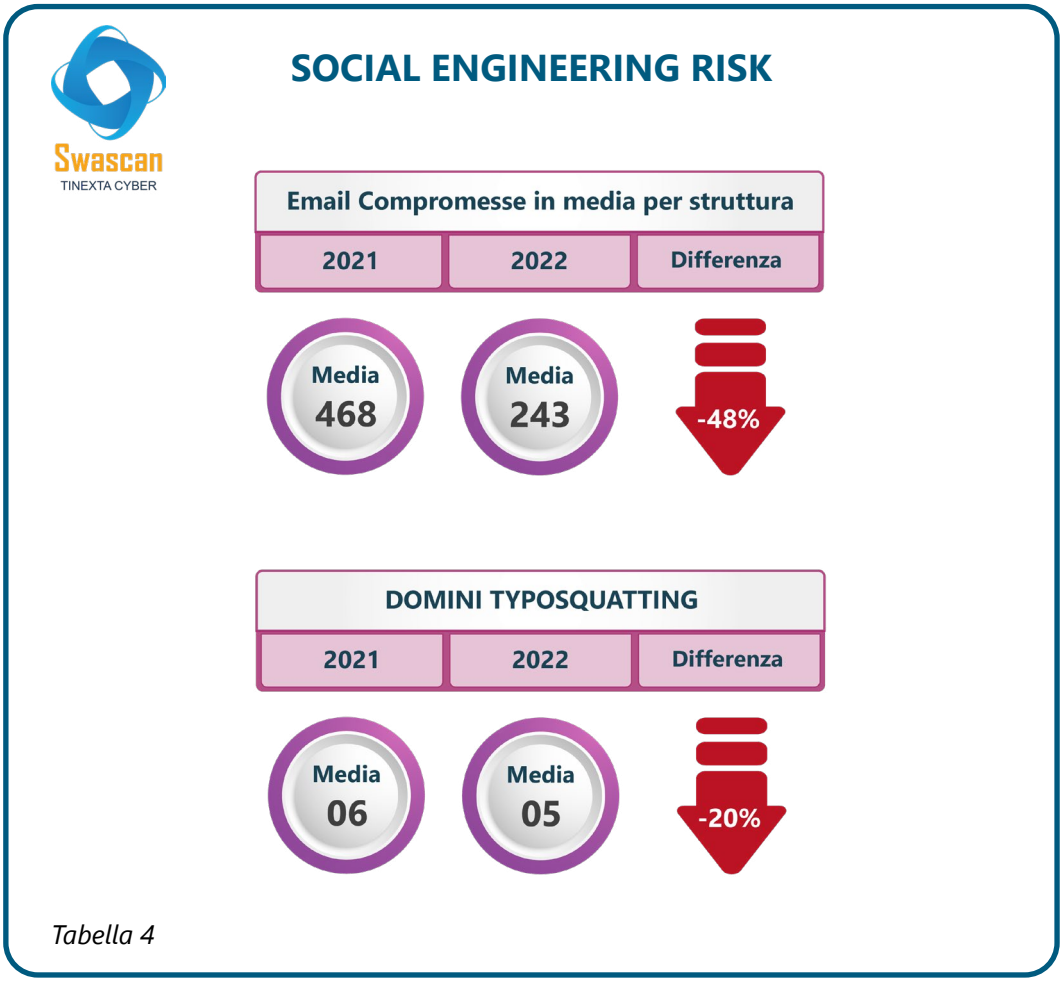


Tabella 4

Notizie decisamente più positive le troviamo sul fronte social engineering (Tabella 4), dove il numero di **email compromesse** rilevate **scende di quasi il 50%**; così come quello dei **domini di typosquatting** che **cala del 20%.**

Come si evince chiaramente dal confronto a distanza di quasi un anno, **il rischio tecnologico** è lievemente **aumentato (+%14)**, mentre è diminuito quello legato al social engineering. I numeri rilevati in questo secondo ambito, però, anche se diminuiti, lasciano comunque pochi dubbi sulla pericolosità e sul possibile rischio ancora presente su questo fronte. Non dobbiamo dimenticarci che basta un singolo anello debole e la catena della cyber defense rischia di spezzarsi.

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.

Technology Risk: Servizi E Porte Esposte

Tabella 5

What is: a cosa corrispondono queste vulnerabilità

SERVIZI WEB http: l'utilizzo di un protocollo non cifrato può comportare un rischio elevato della confidenzialità delle informazioni che transitano tra client e server.

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

SERVIZI TRASFERIMENTO FILE: 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 disponibilità del dato.

SERVIZI DI 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 attaccanti 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.

SERVIZI SCADA, ICS E IOT: l'esposizione di protocolli per l'Internet of Things (IoT) privi di autenticazione e crittografia può causare attacchi di Spoofing, di Man In The Middle e DDoS (Distributed Denial Of Service).

SIP / VoIP: l'esposizione di servizi utili ad effettuare comunicazioni, ad esempio VoIP, potrebbe comportare disservizi dovuti ad attacchi di tipo DoS (Denial Of Service) .

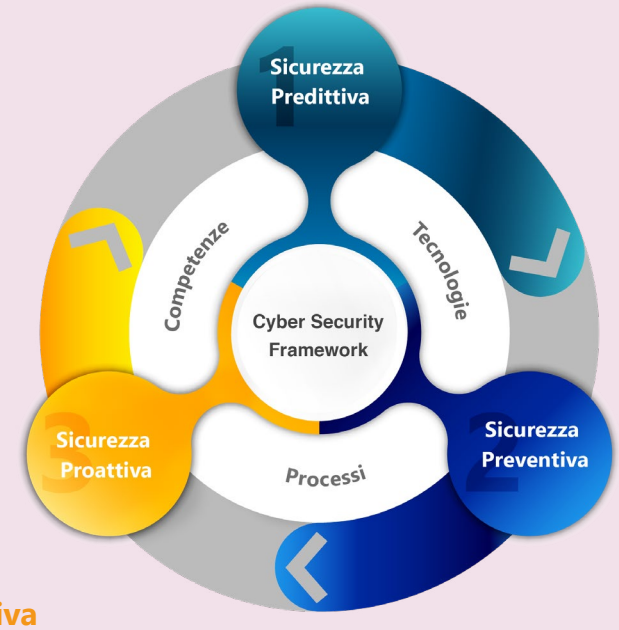
Cyber Security Framework

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
Martina Fonzo
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