INTESA SANPAOLO

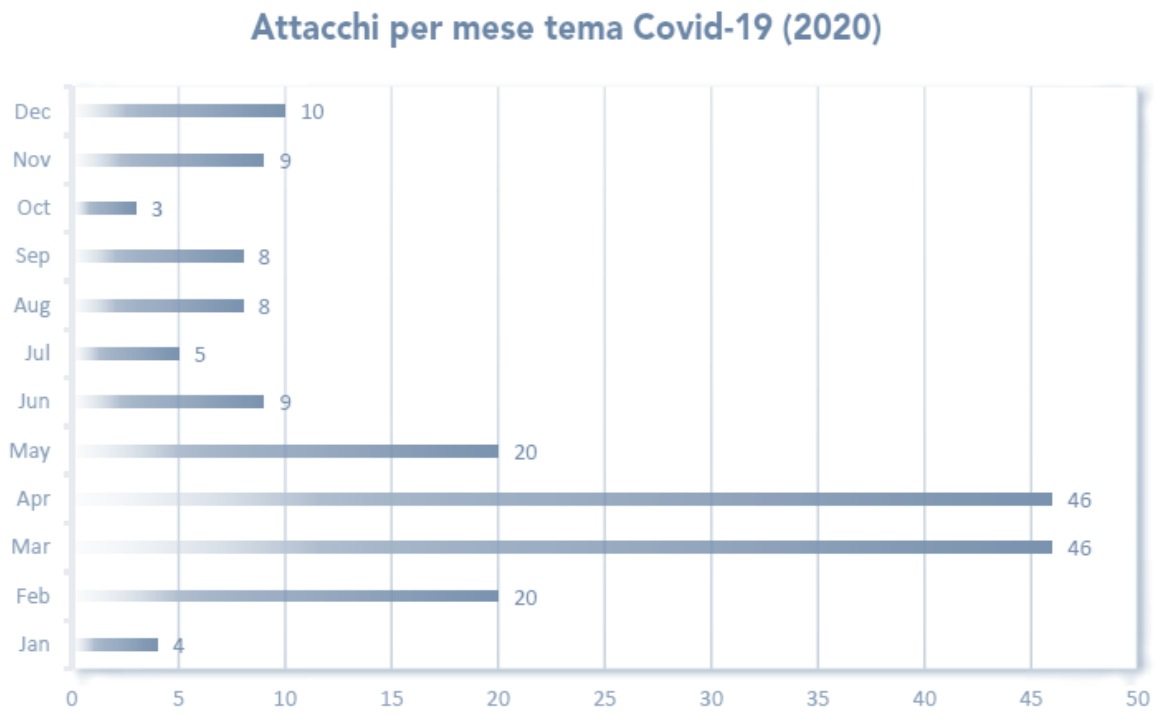
Scenari di rischio Cyber Security

Alberto Crippa
Intesa Sanpaolo - Head of Cyber Security Architecture, Cloud Integration & Innovation

I rischi **Cyber**

L'evoluzione della minaccia

L'evoluzione della minaccia Cyber è un fenomeno in continua crescita in termini numerici, di complessità ma soprattutto di impatto. Dal punto di vista qualitativo lo studio di diverse migliaia di attacchi degli ultimi 3 anni (5.093, quasi metà del totale del campione di 11.959 attacchi analizzati dal 2011) ci fa comprendere che si è prodotto un *cambiamento epocale* nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi.

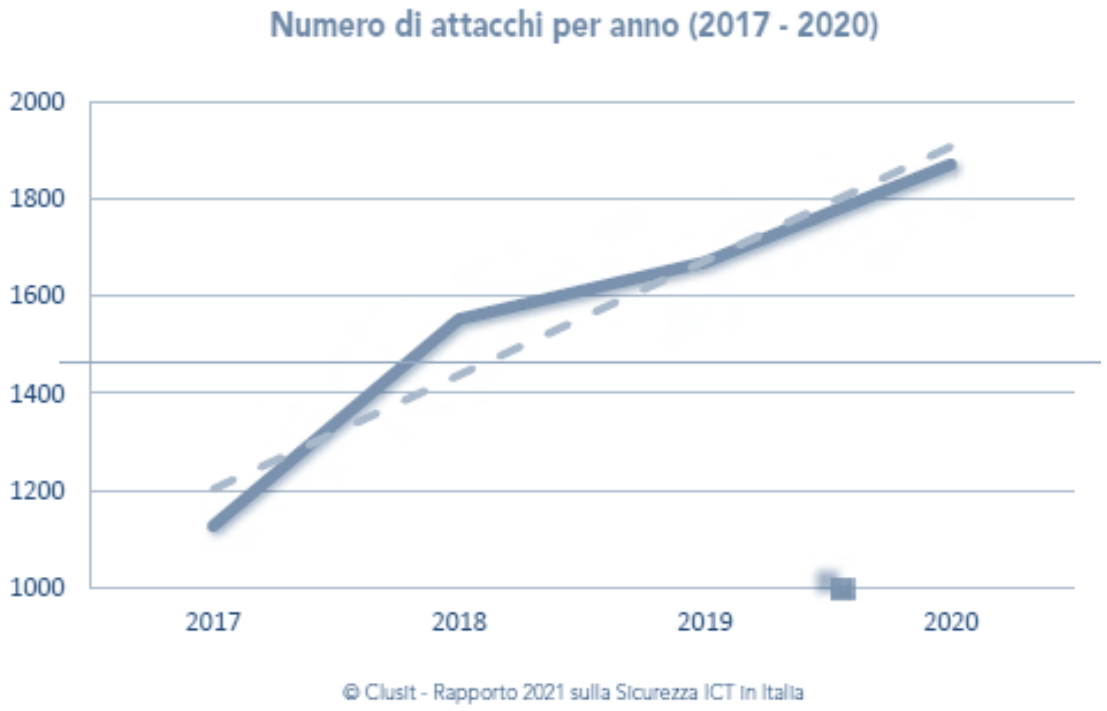


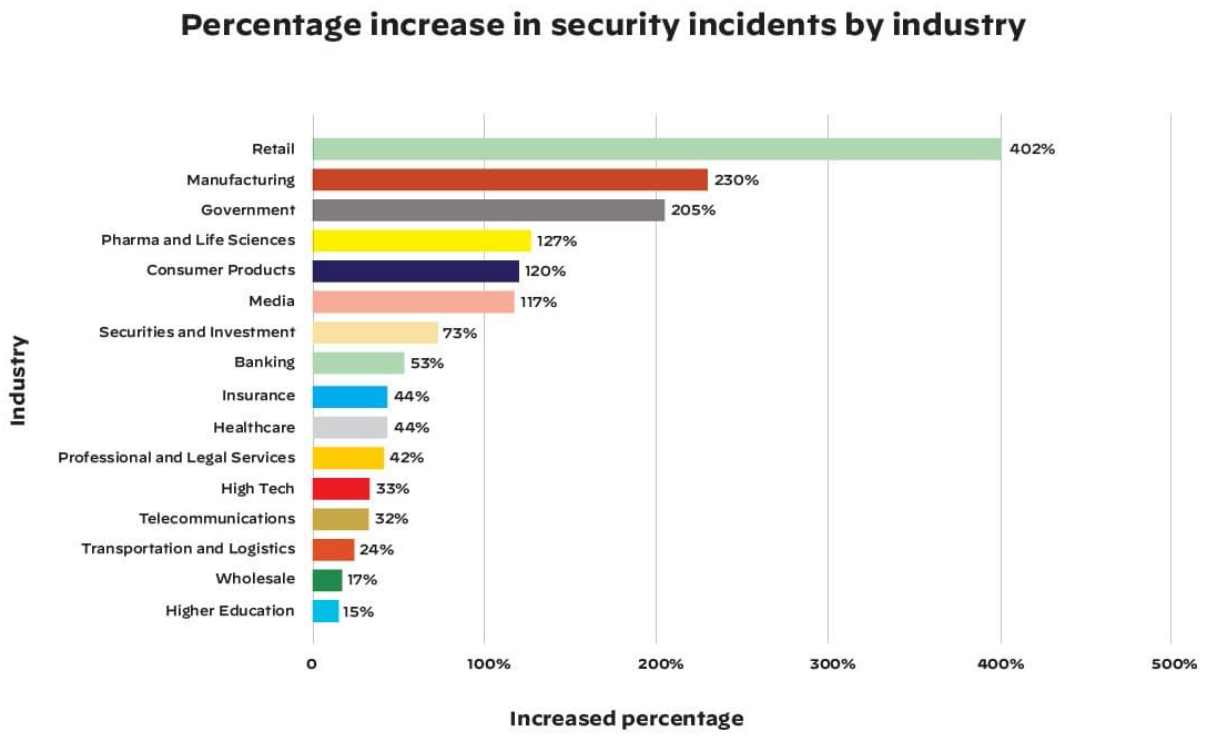
Un esempio è quello della **pandemia Covid-19 che ha costretto le aziende a ripensare** profondamente le proprie **abitudini** e i **propri processi organizzativi**, e a modificarli in corsa passando ad un modello di accesso ibrido. Questa situazione ha causato un allargamento della superficie di attacco che è stata inevitabilmente sfruttata da attori ostili. Si è verificato un significativo incremento del numero degli attacchi Cyber verso società organizzazioni attraverso le postazioni in «home office».

Questo a dimostrazione **dell'estrema pragmaticità** degli attaccanti, che **reagiscono con estrema rapidità** e non perdono alcuna opportunità per massimizzare i loro risultati, senza preoccuparsi delle possibili ricadute, dirette ed indirette.

L'evoluzione della minaccia – la numerosità

Osservando la situazione dal punto di vista quantitativo, la crescita degli attacchi gravi di pubblico dominio nel triennio 2018- 2020 è stata del **20%** (da 1.552 a 1.871). Nel triennio precedente la crescita era stata dell' **11%.**





INTESA SANPAOLO

L'evoluzione della minaccia – vettori di attacco

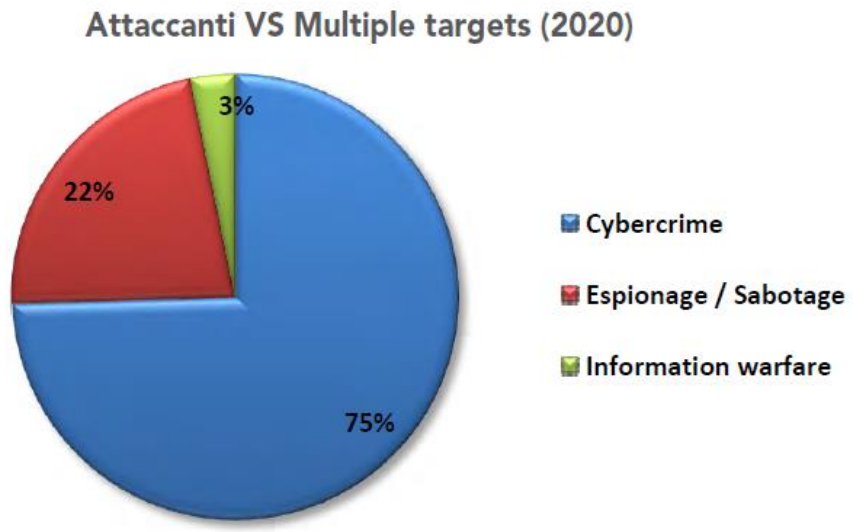
Ransomware	Il Ransomware è un tipo attacco malevolo che prevede la cifratura dei dati di un'organizzazione e la richiesta di un pagamento per ripristinarne l'accesso. Negli ultimi anni gli attacchi Ransomware sono stati la minaccia principale, sia a livello internazionale che italiano con diverse società e organizzazioni governative colpite e con un alto impatto operativo, mediatico e reputazionale
Furto di informazioni	Questa categoria include i data breaches e la divulgazione involontaria di informazioni. Un data breach o data leak si presenta a seguito di una fuoriuscita di informazioni sensibili, personali, confidenziali o protette senza autorizzazioni e senza le necessarie misure di sicurezza.
I Malware sono dei software o firmware sviluppati per eseguire processi non autorizzati che possono avere un impatto sulla disponibilità, sull'integrità e sulla confidenzialità di informazioni o sistemi	**Malware**
La disponibilità e l'integrità sono obiettivi di un elevato numero di attacchi fra cui i Denial of Service (DoS). Strettamente mirati a piattaforme web-based, gli attacchi DDoS rappresentano una delle minacce più critiche per i sistemi IT mirando alla indisponibilità degli stessi attraverso l'esaurimento delle risorse e causando perdite di dati e impatti sulle performance, fino all'indisponibilità dei sistemi stessi	**Minacce sulla disponibilità e integrità dei servizi**
Crypto Jacking	I Cryptojacking o hidden cryptomining è un tipo di cybercrime dove un attaccante sfrutta di nascosto la capacità computazionale della vittima per generare cryptovalute
Minacce non correlate ad attacchi diretti	In questa categoria sono incluse le minacce non correlate ad attacchi malevoli. Questi sono principalmente causati da errori umani o misconfigurazioni sui sistemi ma possono anche includere eventi o disastri naturali che impattano le infrastrutture IT di un'azienda.
Gli attacchi alle E-mail molto spesso non mirano a vulnerabilità tecniche sulle infrastrutture ma cercano di sfruttare debolezze dei comportamenti umani nella gestione delle attività quotidiane. Interessante notare che nonostante le attività di sensibilizzazione, questi tipi di attacchi continuano ad avere successi e a rappresentare uno dei principali vettori per il furto di credenziali, di informazioni e per la distribuzione di malware e ransomware.	**Minacce che sfruttano il canale Email**
Fanno parte di questa tipologia gli attacchi che non cercano di sfruttare direttamente vulnerabilità presenti sull'infrastruttura target. Per riuscire nel loro scopo, gli attaccanti cercano di penetrare nei sistemi di società partner o di fornitori al fine di entrare in possesso di informazioni o per avere un punto di accesso privilegiato all'infrastruttura target	**Attacchi che sfruttano la Supply-chain**

L'evoluzione della minaccia – attaccanti e obiettivi

Le istituzioni governative hanno innalzato il loro livello di attenzione sia a livello nazionale che internazionale. **E' stato rilevato un impegno maggiore** nel combattere e perseguire legalmente gli attacchi informatici, in particolare quelli supportati da stati stranieri

I Cybercriminali sono sempre più motivati dalla **monetizzazione dei loro attacchi** es. ransomware.

Gli attacchi di Cybercrime sono sempre più mirati a **colpire infrastrutture critiche**



Distribuzione delle vittime per tipologia

VITTIME PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Institutions: Gov - Mil - LEAs - Intelligence	179	252	247	258	4.5%	↗
Multiple targets	222	304	395	374	-5.3%	↗
Health	80	159	203	215	5.9%	↗
Banking / Finance	117	157	100	97	-3.0%	↗
Online Services / Cloud	95	129	186	177	-4.8%	↗
Research - Education	71	109	141	207	46.8%	↑
Software / Hardware Vendor	68	109	70	113	61.4%	↑
Entertainment / News	115	102	83	69	-16.9%	↓
Critical Infrastructures	40	57	50	70	40.0%	↑
Hospitability	34	45	27	22	-18.5%	↓
GDO / Retail	24	39	37	35	-5.4%	↗
Others	40	30	53	140	164.2%	↑
Org / ONG	8	18	17	26	52.9%	↑
Gov. Contractors / Consulting	6	14	11	16	45.5%	↑
Telco	13	11	18	25	38.9%	↑
Automotive	4	9	10	8	-20.0%	↓
Security Industry	11	4	17	12	-29.4%	↓
Religion	0	3	2	5	150.0%	↑
Chemical / Medical	0	1	3	2	-33.3%	↓
TOTALE	1127	1552	1670	1871	+12%	

L'evoluzione della minaccia – trend

- Crescono i numeri degli **attacchi Ransomware** che utilizzano attacchi Phishing alle email o ai servizi RDP (Remote Desktop Services) come vettori principali di compromissione
- Cresce il numero degli **attacchi sofisticati** che sfruttano compromissioni nella **supply chain**
- Cresce ancora il numero degli attacchi mirati legati alle **nuove modalità operative introdotte dalla pandemia**
- Numerosi data breaches accaduti negli ultimi 12 mesi sono causati da **errori umani o misconfigurazioni di sistema.** Nel 2020 c'è stato un picco in incidenti di sicurezza non legati ad attacchi malevoli
- Gli **attacchi alle caselle di posta aziendali** - Business E-mail Compromise (BEC) – sono cresciuti in numero, in complessità e sono sempre più **personalizzati per raggiungere uno specifico bersaglio**
- **L'industrializzazione degli attacchi**: Ransomware as a Service (RaaS), Phishing as a Service (PhaaS)
- I nuovi malware mirano agli ambienti a **Container** evolvendo in nuove varianti file-less
- Le attività di CryptoJacking hanno raggiunto **nuovi record** sfruttando nuove tipologie di attacco
- La nuova frontiera degli attacchi DDoS è il **Ransom Denial of Service (RDoS**) e sempre più spesso si basano su compromissioni di dispositivi IoT (Internet of Things)

Nuove superfici di attacco

Nuove superfici di attacco

- Cloud
- Third parties
- DEVOPS
- Internet of Thing (IoT)
- Hybrid workplace
- Mobile

Le contromisure

Le contromisure – Da dove iniziare

1. Sapere cosa proteggere
2. Conoscere da cosa proteggersi
3. Conoscenza del perimetro
4. Adeguata percezione del rischio
5. Formazione sulla Sicurezza
6. Adeguata preparazione del personale

Le contromisure – Tecnologie e processi

Data Security	Application Security	Endpoint Security	Network Security	Perimetral Security	Cloud Security
• Data Classification • Data Encryption • Database Activity Monitoring • Data Masking • Enterprise Right Management (ERM) • Data Retention • Data Loss Prevention (DLP)	• Web Application Firewall (WAF) • Static Code Review • DEV SEC OPS • Dynamic App Testing • API Protection	• Antimalware • Endpoint Detect & Response (EDR) • Personal Firewall • OS Hardening • Patch Management • Disk Encryption • DLP Agent • Enterprise Mobile Management	• Network Segregation • IDS/IPS • Network Access Control (NAC) • Web Proxy • Sock Proxy • Reverse Proxy • Mail Security • Wireless security • Deception • IoT Security	• Secure DMZ • Firewall Perimetrali • IDS/IPS • Anti DDoS • Mail Security • DNS Protection	• Cloud Access Security Broker (CASB) • Cloud Security Posture Management • Cloud Workload Protection

Identity & Access Mgmt	• Centralized Access Management • Privileged Access Management (PAM) • Federated Access Management	• Physical Access Management • Multifactor Authentication • Password Vaulting
Security Governance	• Security Policies & Compliance • Security Awareness • Third Party Governance	• Business Continuity & Disaster Recovery • Security by Design • Risk Management
Security Operation	• Security Operation Center (SOC) • Vulnerability Assessment / Penetration Test • Threat Detection & Hunting	• SIEM, SOAR, UEBA & Log Management • Threat Exposure Management • Threat Intelligence

Le contromisure - Peculiari

Ogni attività o area di business potrebbe avere la necessità di avere un presidio di sicurezza verticale relativo alle attività svolte

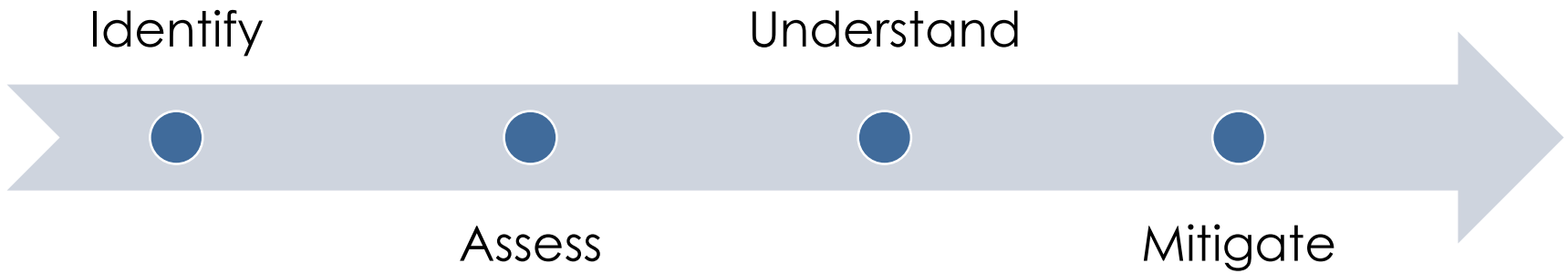
- **Anti Frode finanziaria**
- **Protezione dei dati personali**
- **Protezione delle comunicazioni**
- **Protezione dei segreti aziendali**
- **Anti pirateria del diritto d'autore**
- **Continuità di servizio**

Costi della Cyber Security

È il giusto mezzo che bisogna scegliere, e non l'eccesso né il difetto, poiché il giusto mezzo è come la retta ragione dice - Aristotele

Costi della Cyber Security – Approccio risk based

Per garantire un livello di protezione adeguato sono necessari diversi processi, soluzioni e tecnologie. Quando la disponibilità del budget non permette l'implementazione di tutto quanto previsto, è necessario applicare un approccio Risk Based, partendo dall'analisi degli use cases da cui ci si vuole proteggere e scegliere il processo o la tecnologia che meglio serve allo scopo.



Non dovrebbe essere la tecnologia a guidare. La tecnologia è lo strumento che può aiutare nella mitigazione di un rischio

Automazione dei controlli

Automazione dei controlli

Security as a code

Sinergie

Artificial Intelligence

Machine Learning

Riferimenti

- Rapporto **Clusit** sulla Sicurezza ICT in Italia 2021
- **ENISA** Threat Landscape report 2021
- **Unit42** Cloud Threat report H1 2021