La cybersecurity nella logistica: lo stato dell'arte e la gestione dei rischi

Paola Girdinio

Presidente Start4.0

Stato dell’arte

- Le ***aziende nel settore dei trasporti, dello stoccaggio e della consegna*** sono state tra i primi tre obiettivi colpiti più duramente dagli attacchi informatici durante il 2021.
- Il ***settore dei trasporti è un obiettivo “popolare”*** in cui gli attori delle minacce cyber, spesso sponsorizzati da uno Stato, cercano di interrompere la capacità logistica e di fornitura dei concorrenti.
- Durante la prima metà del 2021 ***quattro organizzazioni su cinque hanno subito una minaccia di Cyber Security*** che ha sfruttato una vulnerabilità nel proprio ecosistema di fornitori terzi.
- Il ***costo medio di una violazione dei dati*** è salito a circa ***3,56 milioni di dollari***, mentre il ***pagamento medio di un riscatto*** del ***ransomware*** ha subito un’impennata del 33%, ***superando i 100.000 dollari***.

Stato dell’arte

- Logistica sempre più caratterizzata da ***IoT***, ***Intelligenza Artificiale, machine learning*** e ***robot*** di ogni tipo
- Nasce la ***Supply Chain 4.0***.
- La caratteristica più importante della ***Supply Chain 4.0***, e della ***logistica 4.0*** in generale, è quella di ***essere sempre connessa in rete***.
- Da un lato in grado di fornire continuamente dati, aumento ***efficienza logistica***, dall’altro
    - esposizione l’intera filiera a ***rischi legati alla cybersecurity*** e altre vulnerabilità.
    - necessità di iper-specializzazione nei servizi indispensabili
    - ***aziende sempre più dipendenti da fornitori esterni***.

- ***Sferrando attacchi alla supply chain*** dei Service Provider Gestiti (Managed Service Provider), gli hacker ottengono ***l’accesso sia all’attività degli MSP che a quella di tutti i loro clienti.***
- Es: violazione subita da SolarWinds (ha colpito direttamente i database dei clienti, oltre 33.000 in tutto il mondo, tra cui la Difesa degli Stati Uniti e Microsoft);lo scorso anno e attacco ai danni di Kaseya VSA all’inizio del 2021.

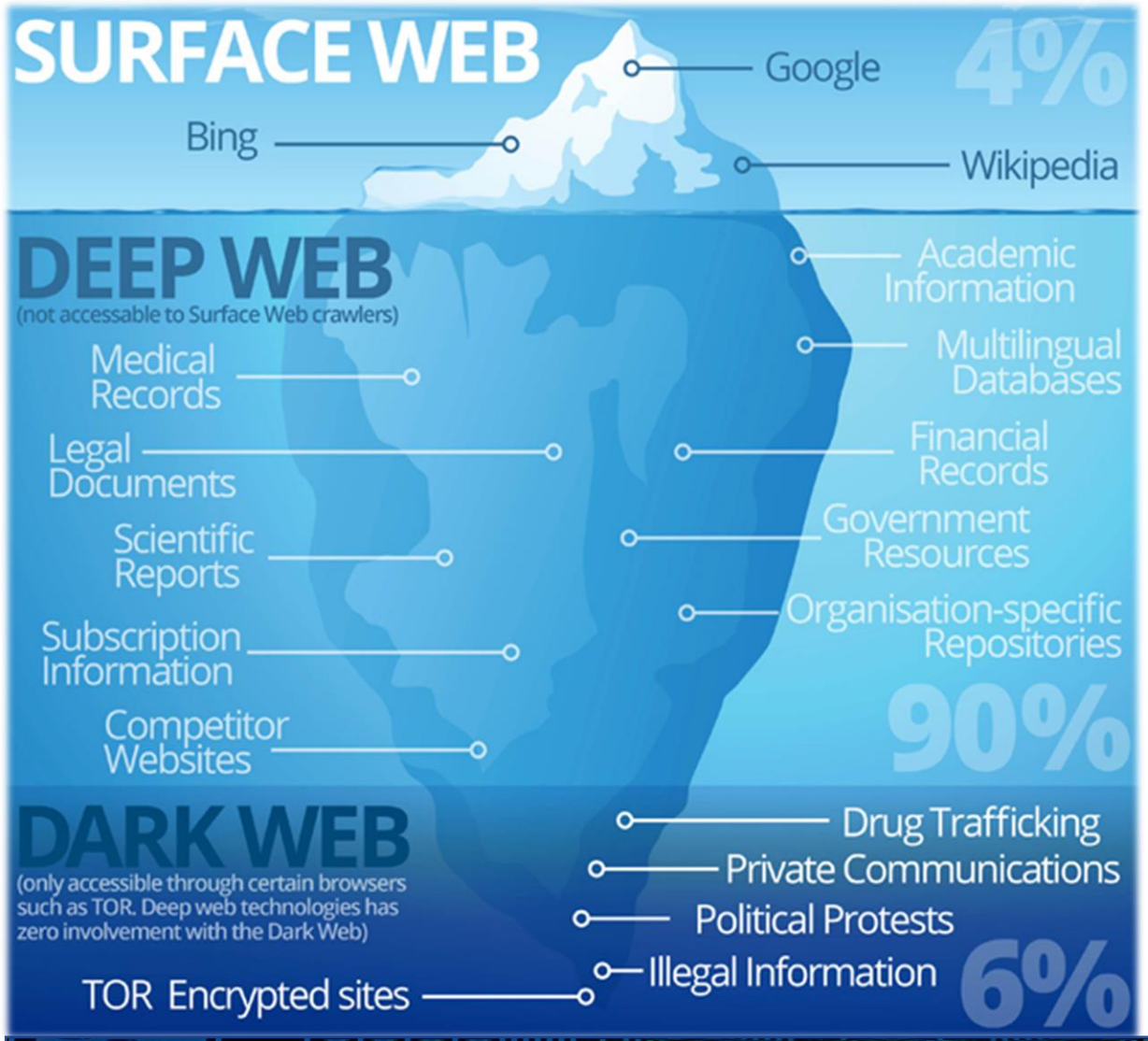
Stato dell’arte

- A dilagare gli ***attacchi di phishing***: le e-mail di phishing sono aumentate del 62% tra il primo e il secondo trimestre del 2021. Questo picco è particolarmente preoccupante poiché il 94% del malware viene introdotto tramite le e-mail.
- Aumentano ***i casi di esfiltrazione dei dati***. Nel 2021, più di 1.300 vittime di ***ransomware*** hanno visto i loro dati divulgati pubblicamente dopo l’attacco subito, poiché gli hacker cercano di ottimizzare il tornaconto economico che possono ottenere da attacchi messi a segno.
- Durante la prima metà del ***2021***, sono state rilevate oltre 1.100 fughe di dati, con un ***incremento del 70% alla fine dell’anno***.
- ***Per difendersi da tali minacce, le organizzazioni devono adottare un approccio “pervasivo” alla sicurezza della posta elettronica, integrando strumenti di sicurezza che consentano una maggiore visibilità all’interno e oltre il perimetro*.**

Stato dell’arte

- Nella logistica 4.0 i fronti su cui possono svilupparsi le ***minacce di cybersecurity*** sono fondamentalmente due:
- La prima potenziale minaccia proviene dagli ***scambi*** che avvengono ***tra fornitori e clienti aziendali***;

- La seconda minaccia consiste in un ***attacco frontale alla catena logistica*** tramite ***malware.***
  - Un esempio di questo tipo di attacco è quello successo recentemente ***all’oleodotto statunitense Colonial Pipeline***, un attacco talmente potente che ha causato per quasi una settimana il blocco della produzione giornaliera, pari a 2,5 milioni di barili di greggio. In questo caso l’attacco informatico è stato possibile grazie all’utilizzo di un ***ransomware di ultima generazione***.

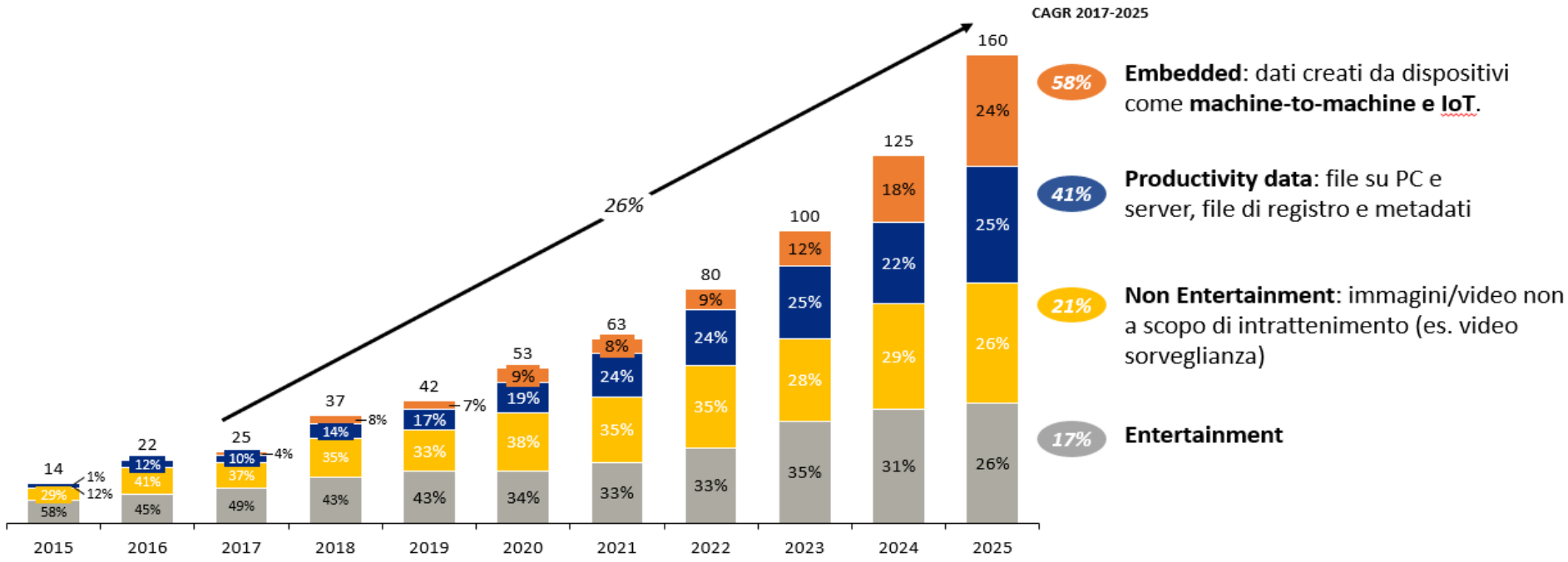


Al giorno d'oggi, un utente malintenzionato non ha bisogno di essere un abile hacker.

Può facilmente acquistare hacking capabilities *'As a Service'* sul dark web.

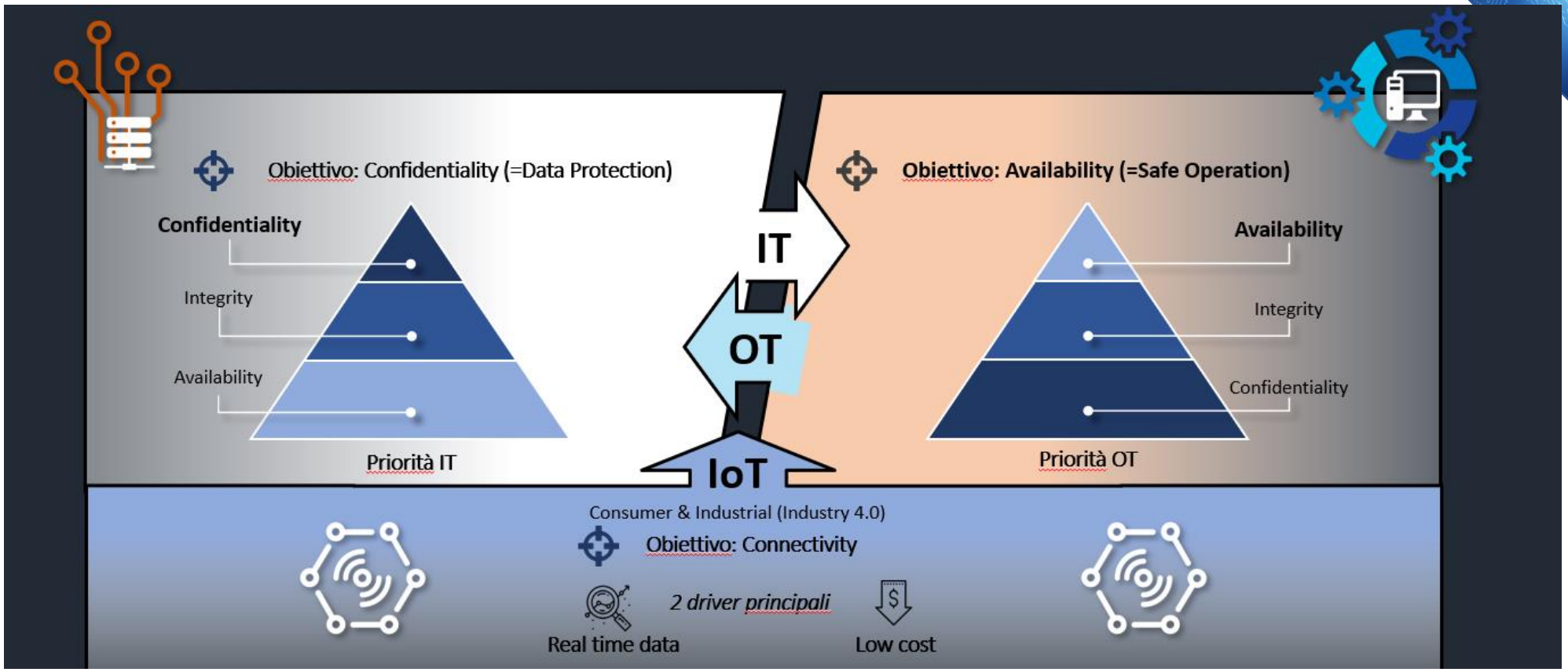
I dati generati stanno crescendo in maniera esponenziale, guidati da M2M, IoT e productivity data

Generazione dati per tipologia (ZB, 2015-25; CAGR, 2017-25)



Nel 2025 si prevedono oltre 75 Mld di dispositivi connessi

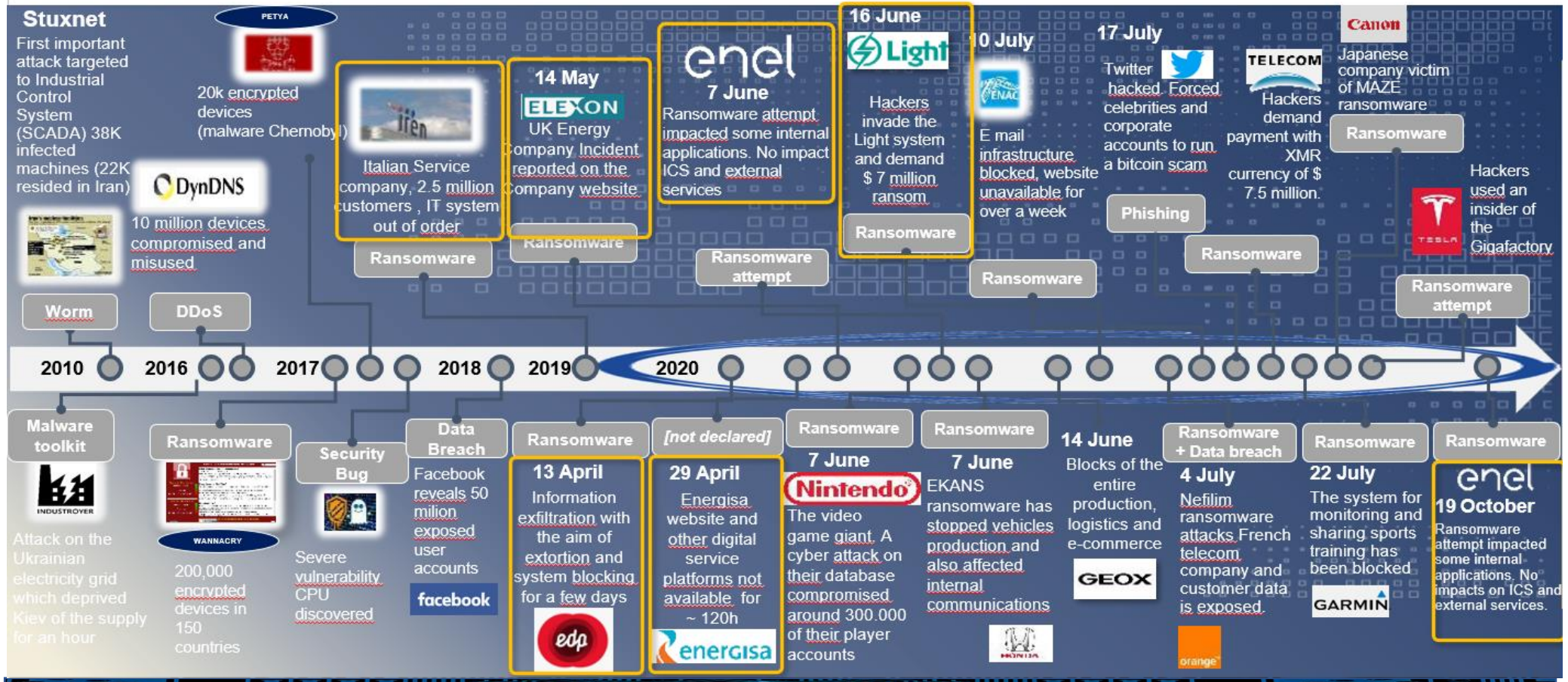
La convergenza IT / OT / IoT offre opportunità ma aumenta anche i rischi cyber



Attacks to Energy Companies

Supply Chain Attacks

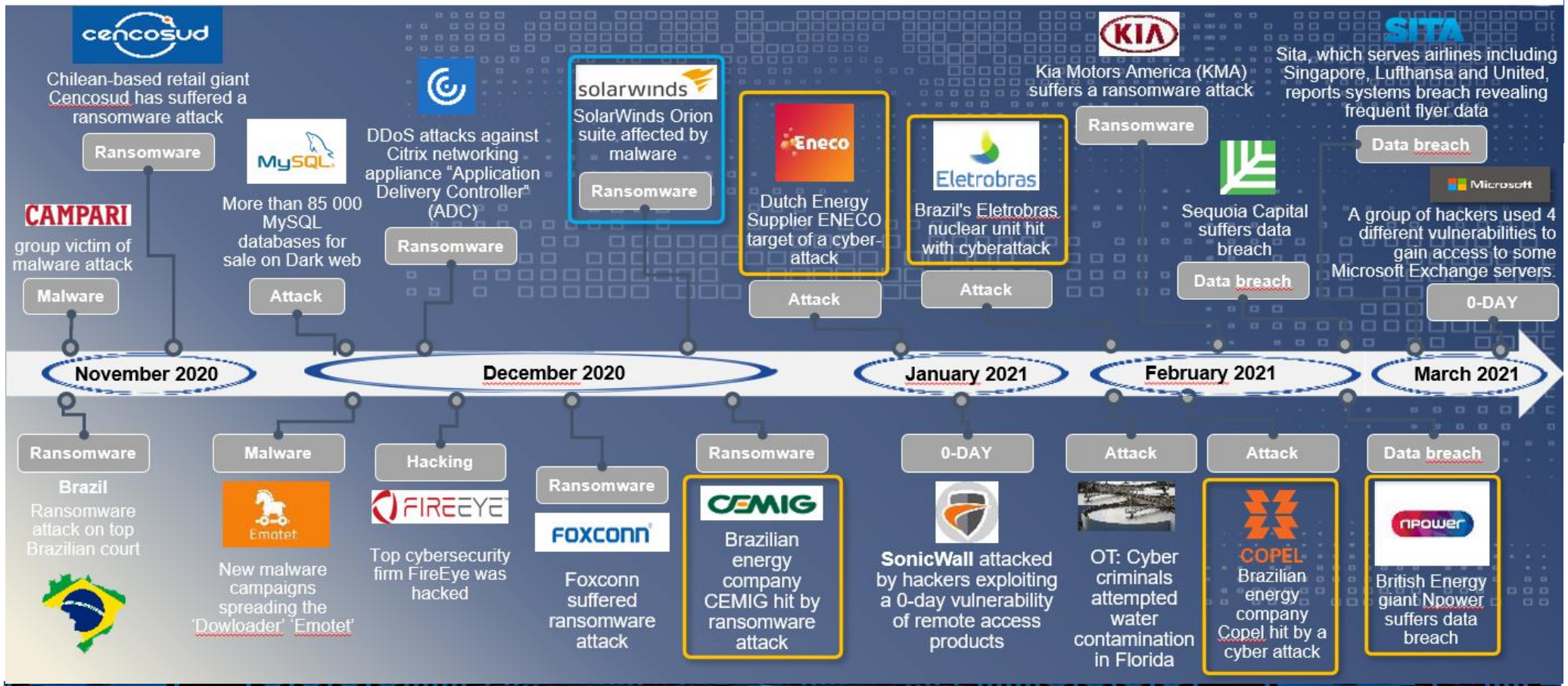
Cyber attacks crescono esponenzialmente



Attacks to Energy Companies

Supply Chain Attacks

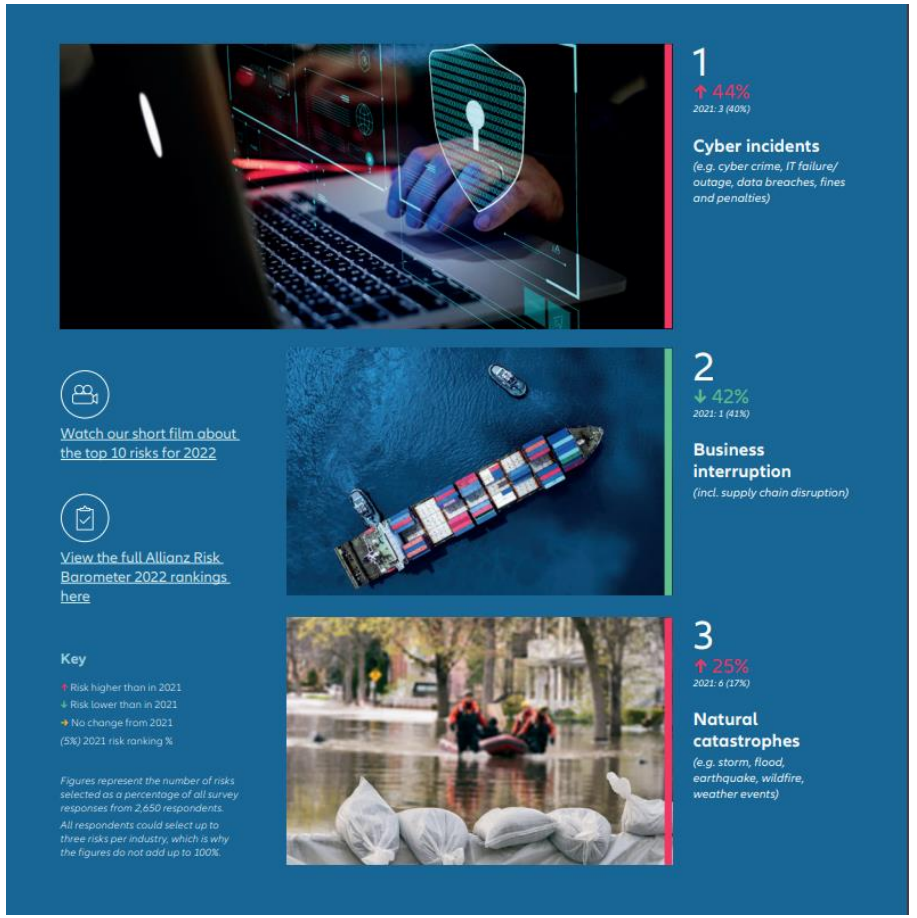
Cyber attacks crescono esponenzialmente



La percezione degli attacchi cyber sta crescendo nel settore assicurativo

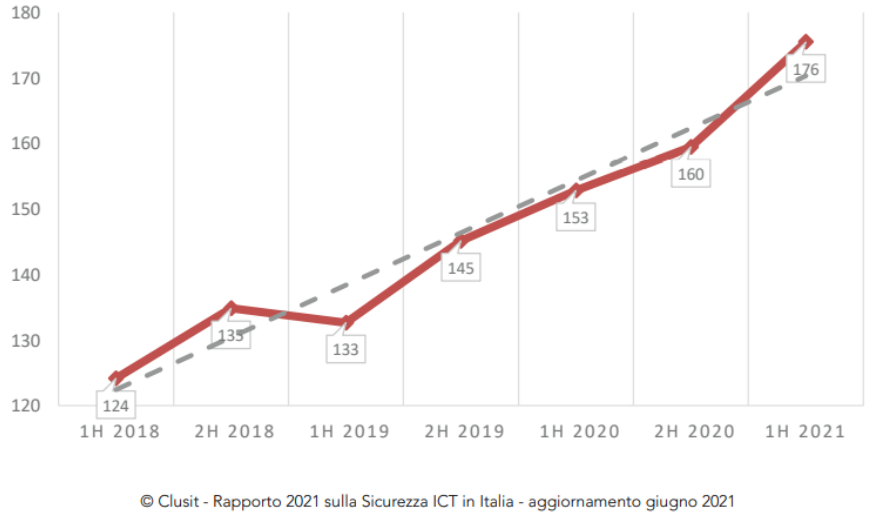
- **Allianz Risk Barometer 2022 (gennaio 2022):** il rischio informatico è il primo rischio percepito dalle aziende a livello mondiale

- Nel frattempo, incombe la minaccia di ***interruzione dell'attività***, dovuta ad attacchi ***ransomware***, guasti tecnici o da attacchi alla catena di approvvigionamento, sempre più gravi le conseguenze delle violazioni dei dati e rischi derivanti dall'accelerazione della digitalizzazione post-Covid-19.



Clusit rapporto 2021 su sicurezza ICT (novembre 2021)

Ancora l'anno peggiore di sempre, sul fronte cyber security. Il trend delle minacce, dopo la crescita degli ultimi anni, è ulteriormente in aumento, con danni dall'impatto economico che supera ***il 6% del PIL mondiale***



Media mensile attacchi per semestre (2018-1H 2021)

Distribuzione delle vittime per tipologia (2018-1H 2021)

(Clusit rapporto 2021 su sicurezza ICT)

- Nel mese di ***dicembre 2021*** si contano ***138 vittime di attacchi ransomware nel mondo***. Per un totale di ***26,3 milioni di dollari*** di richieste di riscatto.
- Per l'anno 2021, in testa a questa triste classifica troviamo il ***gruppo criminale Conti*** con 477 vittime e a seguire ***Lockbit2.0*** con 457 attacchi portati a compimento.

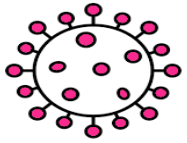
VITTIME PER CATEGORIA	2018	2019	2020	2H 2020	1H 2021	1H 21 su 2H 20	TREND
Government, Military, Law Enforcement	220	233	224	120	167	39.2%	↑
Healthcare	161	186	210	117	139	18.8%	↑
Multiple Targets	326	406	401	158	121	-23.4%	↓
Information Communication Technology	191	233	269	149	113	-24.2%	↓
Education	106	140	174	103	100	-2.9%	↗
Financial, Insurance	162	107	122	66	60	-9.1%	↗
Professional, Scientific, Technical	18	19	59	27	50	85.2%	↑
Wholesale, Retail	33	45	54	31	50	61.3%	↑
Transportation, Storage	35	20	44	23	48	108.7%	↑
Manufacturing	32	32	61	32	47	46.9%	↑
News, Multimedia	70	69	43	23	38	65.2%	↑
Organizations	40	35	46	29	30	3.4%	↗
Arts, Entertainment	68	55	40	19	26	36.8%	↑
Energy, Utilities	24	25	39	13	19	46.2%	↑
Hospitability	44	27	22	12	17	41.7%	↑
Other Services	9	14	21	13	13	0.0%	-
Telecommunications	13	19	32	16	9	-43.8%	↓
Construction	1	2	7	4	3	-25.0%	↗
Agriculture, Forestry, Fishing	0	0	5	2	3	50.0%	↑
hMining, Quarrying	1	0	1	0	0	0.0%	-
TOTALE	1.554	1.667	1.874	957	1.053		

Qualche caso

SCENARIO REALE

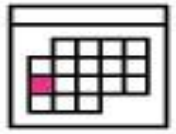
Attacco ransomware per €1.000.000

L'aggressore ha registrato un dominio falso molto simile a quello di proprietà del cliente



L'aggressore ha iniziato a inviare dal dominio falso comunicazioni sul COVID-19 per conto delle risorse umane dell'azienda

I dipendenti hanno aperto l'allegato, quindi l'aggressore ha ottenuto il controllo sulla rete del cliente ed è rimasto in attesa



10 giorni dopo il cliente ha trovato tutti i server crittografati, inclusi tutti i backup, e una richiesta di riscatto in bitcoin pari all'1,7% dei ricavi annuali dell'azienda

Qualche caso

- Nel giugno del 2017, ***quasi 80 porti e terminal in tutto il mondo si sono fermati o hanno subito ritardi*** significativi, tra cui il porto di New York e del New Jersey, il porto di Los Angeles, il porto di Rotterdam (il più grande d'Europa) e il porto vicino a Mumbai, il più grande porto container dell'India; la causa
  - ***Attacco ransomware alla compagnia di spedizioni A.P. Moller-Maersk***, costato alla compagnia 300 milioni di dollari. Senza possibilità di pulire i sistemi informatici infetti, Maersk ha dovuto ricostruire una parte significativa della sua infrastruttura IT, installando oltre 50.000 nuovi PC, server e applicazioni in due settimane.
- ***Il 31 gennaio 2020 il gruppo australiano Toll ha subito un attacco informatico da parte di un virus ransomware***, che rende inutilizzabili i dati (generalmente tramite il loro criptaggio) e li "libera" solo dopo il pagamento di una somma.
  - In una nota diffusa il 4 febbraio, la multinazionale precisa che l'attacco è stato "mirato" e ha portato alla decisione di ***isolare e disattivare immediatamente alcuni sistemi informatici per evitare la diffusione del virus informatico***.
  - Nel frattempo la società opera attraverso una combinazione di processi manuali e automatizzati in tutte le operazioni globali, anche se alcune procedure stanno subendo ritardi o interruzioni. Toll assicura l'intero processo di trasporto delle spedizioni, mentre le prenotazioni avvengono per telefono.

Qualche caso

- La ***Hellmann Worldwide Logistics*** è stata colpita da un attacco informatico che ha bloccato le operazioni quotidiane: si è trattato di un ***ransomware***.
  - Le indagini sono ancora in corso per accertare le cause dell'incidente di sicurezza, ma intanto la ***gang criminale RansomExx*** ha diffuso i dati con un leak di 70 GB sul proprio sito nel Dark Web, raggiungibile sotto rete Tor, ne rivendica l'attacco pubblicamente dal 15 dicembre 2021.
  - Dei file che destano maggiore curiosità si rileva un Excel in formato XLS contenete un grande numero di codici utente e password memorizzati in chiaro, ognuno del corrispettivo sito web per il quale la società era cliente/fornitore.
  - ***Problematica gestione delle password all'interno dei luoghi di lavoro***.

Threat landscape for supply chain attacks

ENISA (European Union Agency for Cybersecurity)

- ***Enisa*** definisce la ***supply chain*** o catena di approvvigionamento come "***la combinazione dell'ecosistema di risorse necessarie per progettare, produrre e distribuire un prodotto. Nella sicurezza informatica, una catena di approvvigionamento include hardware e software, cloud o meccanismi di archiviazione e distribuzione locali".***
- Il documento riporta nella sua analisi una ***carrellata di 24 incidenti che hanno interessato la supply chain nel periodo tra gennaio 2020 ed inizio luglio 2021***.
- Numericamente la casistica dimostra facilmente come ***nel 2020***, ***in un intero anno*** di osservazione ***sono stati presi in esame 8 casi di incidenti*** di cui sono emerse informazioni. ***Nel 2021, in soli 6 mesi, sono stati segnalati 16 incidenti***.
- La sicurezza aziendale passa sempre più dalla ***cybersecurity***, ma questo non deve far dimenticare che il fattore umano è l'elemento più importante in ogni azienda: ***formare il personale*** in modo da rispondere al meglio alle difficoltà è la chiave per affrontare ogni tipo di crisi.