G L /X Q H G u O X J O L R

Sommario Rassegna Stampa

Pagina	Testata	Data	Titolo	Pag.
Rubrica	**Sicurezza**			
7	Italia Oggi Sette	10/07/2023	*Cyber crimini, sanita' nel mirino (A.Longo)*	3
Rubrica	**Ambiente**			
1	Italia Oggi Sette	10/07/2023	*Il 40% delle aziende europee non ha alcuna familiarita' con i criteri Esg (T.Cerne)*	5
Rubrica	**Innovazione e Ricerca**			
1	Italia Oggi Sette	10/07/2023	*L'AI act boccia ChatGPT (M.Rizzi)*	8
6	Italia Oggi Sette	10/07/2023	*Crescono gli investimenti in Ict (A.Longo)*	10
Rubrica	**Energia**			
1	Il Sole 24 Ore	10/07/2023	*Fotovoltaico, 780 progetti in lista d'attesa (D.Aquaro)*	12
1	Il Sole 24 Ore	10/07/2023	*Idrogeno verde, ecco le regole per produzione e stoccaggi. E ora serve una strategia (I.Cimmarusti)*	15
Rubrica	**Mobilità e Trasporti**			
28/29	Affari&Finanza (La Repubblica)	10/07/2023	*Int. a H.Poupart-lafarge: "Il treno all'idrogeno e' la risposta green" (F.Santelli)*	17
Rubrica	**Pubblica Amministrazione**			
23	Il Sole 24 Ore	10/07/2023	*Gli Ordini ritornano nel conto annuale Pa (T.Grandelli/M.Zamberlan)*	20
Rubrica	**Normative e Giustizia**			
1	Il Sole 24 Ore	10/07/2023	*Con il doppio taglia leggi addio a 9mila atti inutili (E.Bruno)*	21

ItaliaOggi Sette

Settimanale Data 10-07-2023
Pagina 7
Foglio 1 / 2

SICUREZZA INFORMATICA

I dati contenuti nel rapporto Clusit presentato in occasione dell'Healthcare security summit

Cyber crimini, sanità nel mirino

Negli ultimi quattro anni triplicati gli attacchi informatici

Pagina a cura
DI ANTONIO LONGO

In Italia gli attacchi informatici alle strutture sanitarie sono triplicati negli ultimi quattro anni. E il trend non accenna a diminuire considerato che, a livello globale, nel 2022 il settore della salute è risultato il più attaccato dai cyber criminali e che nei primi tre mesi del 2023 gli attacchi alle organizzazioni che operano in tale comparto sono stati il 17% del totale, contro il 12% dello scorso anno, con il 71% di essi che ha avuto un impatto critico. Sono i dati che emergono dal focus "Healthcare" del rapporto stilato da Clusit, l'associazione italiana per la sicurezza informatica, relativo al primo trimestre 2023 sulla sicurezza informatica in Italia, presentato dai ricercatori del comitato direttivo nel corso di Healthcare security summit "Investire in formazione, non ci sono più scuse" promosso per analizzare lo stato dell'arte della cybersecurity nel settore sanitario e farmaceutico.

L'obiettivo degli attacchi. In base ai dati contenuti nel report emerge che l'obiettivo della criminalità informatica nel settore della sanità continua ad essere la monetizzazione, piuttosto che azioni dimostrative o di spionaggio. Gli attacchi nei primi tre mesi dell'anno sono stati, infatti, quasi tutti riferibili al cybercrime, in linea con la tendenza dello scorso anno, eccetto per una minima percentuale (3%) riferibile ad episodi di attivismo. Peraltro, nel primo trimestre di quest'anno sono stati rilevati oltre un terzo degli attacchi registrati nel corso di tutto lo scorso anno. «Questa tendenza esprime la difficoltà a proteggere i sistemi informativi da parte di un settore costretto, come tanti, ad una rapida digitalizzazione e particolarmente sotto pressione dagli anni di pandemia, ma anche di un settore che è indubbiamente arrivato meno preparato di altri a questa sfida», commenta Alessandro Vallega, componente del comitato scientifico di Clusit.

La gravità dell'impatto. La gravità dell'impatto degli incidenti nel settore healthcare è stata complessivamente per i primi tre mesi dell'anno più bassa rispetto alla media, con il 71% di incidenti classificati come "grave" o "critico" rispetto a una media dell'80%. In particolare, il 46% degli attacchi ha avuto impatti gravi mentre il 25% molto gravi sulle strutture sanitarie colpite. Soltanto un 29% degli incidenti è considerato con impatti medi. Tuttavia, trattandosi del settore più colpito, l'impatto globale risulta comunque estremamente alto e le conseguenze sociali dell'interruzione di servizi in questo ambito o la diffusione di informazioni sullo stato di salute dei cittadini sono particolarmente rilevanti. Il trend degli ultimi quattro anni mostra come nell'ultimo anno siano aumentati proprio gli attacchi critici.

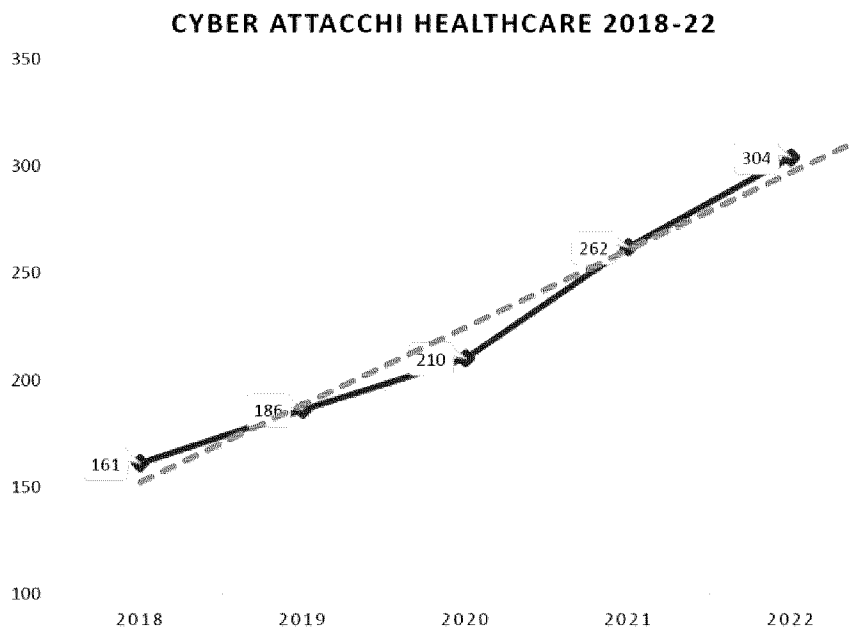
Dal punto di vista della distribuzione geografica, in testa si trova l'America, con un 84% dei target colpiti. A seguire l'Europa con un 11% degli incidenti informatici, l'Asia e l'Oceania (2%). Rispetto agli anni precedenti, i numeri americani, di Asia e Oceania restano sostanzialmente costanti mentre quelli europei diminuiscono percentualmente rispetto allo scorso anno (erano il 14%), ma sono di 3 punti percentuali più alti rispetto a 4 anni fa quando erano l'8% del totale. Le strutture sanitarie italiane nel primo trimestre dell'anno sono state per lo più colpite attraverso tecniche sconosciute e, in un terzo circa dei casi, da malware (ossia software malevoli).

L'utilizzo di vulnerabilità come punto di ingresso per violare sistemi ha rappresentato, invece, nel periodo il 16% dei casi. Di rilievo, secondo i ricercatori di Clusit, anche il 9% di attacchi basati su furti di identità e violazione di account, decisamente più alto della media.

Puntare sulla formazione. Per garantire la sicurezza dell'intero sistema sanitario è necessario che ciascun operatore sia consapevole circa l'utilizzo degli strumenti, conosca i rischi informatici e le contromisure.

«Si tratta di minacce per le quali le organizzazioni sanitarie dovrebbero certamente attrezzarsi meglio, anche con costanti verifiche delle vulnerabilità dei sistemi, poiché le conseguenze di questi attacchi non sono solo economiche e organizzative, a rischio ci sono i cittadini e la società» aggiunge Vallega. Al cospetto di tale grave scenario fotografato dai ricercatori, è il mix tra formazione, organizzazione e tecnologia che può rendere possibile l'accelerazione necessaria per colmare il divario in materia di sicurezza. Come hanno evidenziato i ricercatori di Clusit, al contrario di quanto spesso si crede, non sono solo gli utenti con posizioni intermedie all'interno delle aziende sanitarie e farmaceutiche a necessitare di formazione, infatti frequentemente accade che anche i vertici delle organizzazioni con competenze specifiche e di elevato livello non abbiano consapevolezza in ambito di cybersecurity. Come rileva il report, il Pnrr prevede finanziamenti pari a 2,5 miliardi di euro circa per il potenziamento degli strumenti digitali, dell'infrastruttura e del fascicolo sanitario ma non sono inclusi investimenti per la formazione specifica del personale sanitario. È quindi fondamentale che le singole organizzazioni investano in programmi di sensibilizzazione e formazione per il personale.

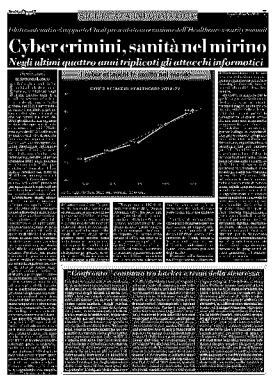
I cyber attacchi in sanità nel mondo



Fonte: rapporto Clusit 2023 sulla sicurezza Ict in Italia

"Confronto" continuo tra hacker e team della sicurezza

I malware, ossia software malevoli, attualmente conosciuti sono più di un miliardo, 94 milioni dei quali comparsi negli ultimi 12 mesi. Nel 2009 tale cifra complessiva ammontava a 25 milioni. In materia di sicurezza informatica, negli ultimi vent'anni hacker e team di sicurezza si sono continuamente adattati a uno scenario mutevole, imparando anche gli uni dagli altri, ed entrambe le parti hanno sia guidato sia subito il cambiamento. Nei prossimi anni la trasformazione proseguirà e diventerà ancor più rapida, emergeranno nuove vulnerabilità e nuove minacce che convivranno con tattiche e debolezze vecchie di decenni. A delineare scenari presenti e futuri sono gli analisti di Barracuda, fornitore di soluzioni di sicurezza, che hanno analizzato anche l'evoluzione degli attacchi e della sicurezza It con uno sguardo al passato. L'origine delle minacce e della cybersicurezza in risposta ad esse risale alla seconda metà degli anni Ottanta, poi nel 2003 le cyber minacce hanno iniziato a diversificarsi e moltiplicarsi ma gli attacchi erano ancora in gran parte frammentati, dirompenti e spesso opportunistici. Virus e altri malware traevano vantaggio dall'ascesa di internet tra le aziende ma non venivano propriamente implementati all'interno di campagne di cybercrimine organizzato. Gli attacchi prendevano di mira dispositivi laptop e desktop, cercando di intercettare le falle in un perimetro d'accesso definito e controllato. Dal 2003 al 2009 i dispositivi, i servizi e i software mobile conquistano il panorama aziendale, quindi il perimetro di sicurezza si allarga ulteriormente e gli hacker si organizzano. Dal 2009 al 2012 inizia, quindi, l'era del ransomware moderno. Gli attacchi basati sul web e sul social engineering si diffondono a macchia d'olio e aumentano gli attacchi da parte di gruppi sostenuti da stati e attivisti. Con l'avanzare del decennio, gli attacchi informatici diventano sempre più prolifici e distruttivi, si diffondono i sistemi Internet of Things connessi, offrendo una più ampia superficie d'attacco. Ai giorni nostri, come evidenziano gli esperti, l'integrazione e la visibilità in termini di sicurezza faticano a tenere il passo e questo causa delle falle che i criminali sanno rapidamente prendere di mira e sfruttare. L'intelligenza artificiale e il machine learning vengono utilizzati sia per colpire sia per difendersi. Secondo gli analisti di Barracuda, si proseguirà nell'adozione diffusa proprio dell'intelligenza artificiale che avrà significative ricadute sulle aziende, sulla società e sulla stabilità geopolitica.


Cyber crimini, sanità nel mirino
Negli ultimi quattro anni triplicati gli attacchi informatici

ItaliaOggi Sette

Settimanale Data 10-07-2023
Pagina 1
Foglio 1 / 3

SOSTENIBILITÀ

Il 40% delle aziende europee non ha alcuna familiarità con i criteri Esg

Cerne da pag. 2

TRANSIZIONE GREEN

Dati Giuffrè Francis Lefevbre: il 40% delle aziende non ha alcuna familiarità con i criteri Esg

Reporting di sostenibilità, le imprese Ue restano indietro

Pagine a cura
DI TANCREDI CERNE

Imprese europee sostenibili ma non troppo. Nonostante l'approssimarsi della scadenza per ottemperare alle regole imposte dalla direttiva sul reporting di sostenibilità delle imprese ("Csrd", acronimo di corporate sustainability reporting directive), il 45% delle aziende del Vecchio continente non ha intrapreso alcuna azione per anticipare l'imminente entrata in vigore della normativa e il il 43% non possiede nessun punto di riferimento designato per i criteri Esg (environmental, social and governance).

Cosa ancora più grave, il 40% delle aziende europee non sembra avere ancora la minima familiarità con i criteri di sostenibilità ambientale, sociale o di governance. L'allarme è stato lanciato da Giuffrè Francis Lefevbre che ha preso in esame 744 aziende europee di varie dimensioni e diversi settori di attività, puntandone a misurare il grado di consapevolezza riguardo alle tematiche Esg e di corporate social responsability. I risultati sono stati estremamente deludenti in modo trasversale. «Non abbiamo evidenziato particolari disparità tra i paesi europei, piuttosto una carenza di consapevolezza collettiva che solleva questioni importanti in un momento in cui le aspettative dell'Ue stanno diventando più chiare», hanno spiegato gli esperti di Giuffrè Francis Lefevbre che hanno realizzato lo studio. Entro il 2024, infatti, le aziende con più di 500 dipendenti o con un fatturato superiore a 40 milioni di euro dovranno segnalare il loro impatto ambientale, sociale e di governance, in linea con la direttiva europea Csrd. L'ambito di applicazione sarà gradualmente esteso ogni anno: nel 2025 riguarderà le aziende con più di 250 dipendenti, nel 2026 le pmi quotate, nel 2028 le filiali di gruppi non europei, e così via. «Troppe aziende sottovalutano il ruolo futuro della direttiva Csrd, così come le questioni ambientali, sociali ed economiche che questa solleva», ha spiegato Camille Sztejnhorn, Esg impacts director di Lefebvre Sarrut. «Se opportunamente compresi, i criteri Esg possono rappresentare un valore aggiunto. Dall'altro lato, ignorandoli si corre il rischio di compromettere la sostenibilità a lungo termine dell'azienda».

Ma quali sono i settori più attivi e quelli invece meno in linea con le disposizioni di Bruxelles? Secondo l'analisi di Giuffrè Francis Lefevbre, nonostante vengano spesso criticate, le aziende del settore industriale (automobilistico, manifatturiero, chimico) hanno spiccato per la loro maggiore maturità quando si tratta di criteri Esg, con l'implementazione di politiche volte a controllare e ridurre il loro impatto sociale e ambientale. Al contrario, i settori dei servizi e della consulenza hanno mostrato una grande immaturità e carenza di consapevolezza delle aspettative nei loro confronti e dell'imminente applicazione della direttiva Csrd. «Il livello di maturità delle aziende europee, riguardo ai criteri Esg, è inferiore alle aspettative dell'Unione europea», hanno continuato gli esperti. «Anche se non ci sono differenze sostanziali tra i Paesi, quasi metà delle aziende europee non possiede una politica o un manager dedicati a Esg o Csr. In questo panorama, l'industria manifatturiera ha mostrato una grande maturità nei confronti di questi argomenti, mentre il settore dei servizi è apparso particolarmente indietro». Una situazione di disparità che può essere spiegata dalla precoce esposizione dei settori industriali ai criteri ambientali, fattore che ha permesso alle aziende coinvolte di acquisire una solida esperienza nell'identificazione e nella reazione alle normative e nella creazione di politiche di sostenibilità. Sul fronte opposto, le aziende di servizi e consulenza, che finora sono state esenti da normative severe, dovranno essere spinte a rivedere il loro impatto Esg.

«Le normative europee in materia di Esg e Csr pongono sfide rilevanti sia per le aziende, che dovranno progressivamente adeguarsi ai nuovi obblighi, sia per i professionisti che in veste di consulenti saranno chiamati, non solo a dare loro supporto concreto nei vari settori di pertinenza, ma anche a prospettare le grandi opportunità di crescita del business che derivano da una corretta applicazione dei criteri csr », ha aggiunto Stefano Garisto, amministratore delegato di Giuffrè Francis Lefebvre.

ItaliaOggi Sette

Settimanale Data 10-07-2023
Pagina 1
Foglio 2 / 3

TRANSIZIONE GREEN

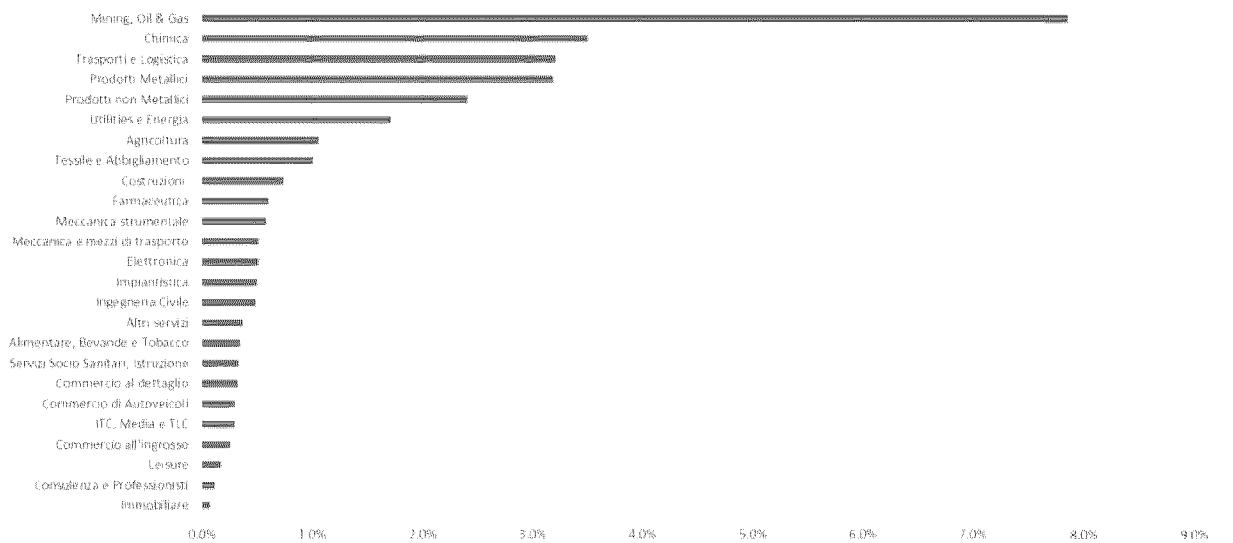
L'outlook di Crif sulle pmi dello Stivale: il 30% è ad uno stadio di adeguamento avanzato

Esg, italiane promosse a metà

Italiani promossi a metà in materia di Esg. Se è vero che solo l'8% delle piccole e medie aziende della Penisola non ha ancora avviato un percorso di transizione sostenibile, è altrettanto vero che quasi il 60% ha mosso i primi passi con un livello medio e basso di adeguatezza ai criteri di sostenibilità, mentre appena il 30% ha raggiunto uno stadio di adeguamento già avanzato. A certificare lo stato di salute del sistema imprenditoriale italiano in materia di sostenibilità aziendale è stato l'Esg outlook realizzato dal Crif che, grazie alle risposte fornite da 150.000 aziende, ha fotografato in modo inequivocabile lo stato dell'arte sulle tematiche di environmental, social e governance delle aziende italiane. Per fare questo, gli esperti del Crif hanno utilizzato lo score Esg, uno strumento di valutazione che, attraverso 150 indicatori relativi alle componenti environmental (E), social (S) e di governance (G) è arrivato a sintetizzare il livello di adeguatezza verso la sostenibilità di ciascuna azienda, tenendo in considerazione il settore di appartenenza e l'area geografica in cui è localizzata. Dall'analisi è emerso che quasi il 60% delle aziende italiane si attesta ancora a livelli medio-bassi di adeguatezza Esg, mentre oltre il 30% si trova a uno stadio avanzato. In particolare, le aziende con un fatturato superiore ai 10 milioni di euro risultano più avanti nel percorso di transizione verso un'economia più sostenibile. Infine, le pmi che non raggiungono i 10 milioni di euro di giro d'affari sono risultate essere il segmento più bisognoso di supporto verso la transizione sostenibile. «Tra i principali fattori Esg analizzati che contribuiscono alla valutazione complessiva delle pmi verso la sostenibilità c'è quello ambientale su cui, a oggi, c'è maggiore attenzione anche da parte delle autorità di vigilanza», hanno sottolineato gli esperti del Crif. «La nostra analisi ha evidenziato una notevole eterogeneità tra le piccole e medie imprese (pmi) italiane nelle regioni e nei diversi settori. Lombardia e Piemonte sono risultate le aree migliori secondo lo score ambientale, con oltre il 60% delle aziende che ha raggiunto un alto livello di adeguatezza. Mentre tra i settori più performanti si sono imposti l'immobiliare e le attività leisure».

Un altro fattore significativo analizzato dall'Esg outlook di Crif è relativo all'impatto da rischio fisico, che misura il potenziale impatto economico e finanziario dovuto al cambiamento climatico e al degrado ambientale. Due le macrocategorie di riferimento: rischi cronici, ovvero quelli legati ai cambiamenti climatici in atto, e rischi acuti, come i disastri naturali improvvisi. In questo ambito solamente il 5,9% delle piccole e medie imprese si è mostrato essere a rischio fisico acuto alto o molto alto a fronte, tuttavia, di oltre il 78% del totale che non sembra essere soggetto a questo genere di timori. Per quanto riguarda i rischi fisici cronici, invece, le imprese molto esposte (livello alto o molto alto) hanno raggiunto il 16% a fronte di un 57% che non viene toccato da questa problematica. L'Esg outlook sviluppato da Crif è andato oltre arrivando a valutare gli impatti finanziari di lungo termine per le piccole e medie imprese determinati dalla transizione verso la sostenibilità. Un indicatore che tiene conto dei costi, dei ricavi e degli investimenti, arrivando a fornire una visione chiara dei possibili scenari futuri. «I risultati mostrano una significativa variabilità dei costi della transizione verso un'economia sostenibile tra i diversi settori», hanno fatto sapere gli esperti del Crif. «I costi derivanti dalla transizione (costi diretti per la carbon tax e investimenti), espressi come percentuale del fatturato, variano ampiamente con una forte correlazione tra il livello attuale di intensità delle emissioni e l'impatto della transizione. In particolare, i settori ad alta intensità energetica come l'estrazione mineraria, i trasporti, la chimica e la lavorazione dei prodotti metallici hanno mostrato impatti significativi, con una percentuale prevista che varia tra il 3 e l'8% annuo di costi sul fatturato». Impatti moderati, ma comunque importanti, invece, nei settori della lavorazione di prodotti non metallici, della produzione e distribuzione di elettricità e gas, con una percentuale di circa il 2-3% annuo di costi sul fatturato. Mentre i settori legati ai servizi, alle attività immobiliari e al commercio hanno mostrato un impatto marginale, inferiore allo 0,5% annuo. «Dal nostro Esg outlook si evince che solo una impresa su tre può dire di essere a un livello avanzato del proprio percorso verso un'economia sostenibile», ha ammesso Marco Macellari, Director - Head of Risk Management di Crif. «Questo conferma il ruolo fondamentale della finanza green nell'abilitare prima e accelerare poi questo percorso virtuoso».

Costi di transizione (incidenza % media annua su fatturato, 2021-2050)



Fonte: ESG Outlook di CRIF, giugno 2023