UIL CREDITO ESATTORIE
E ASSICURAZIONI

VIA LOMBARDIA 30 - 00187 ROMA - TEL. 06.4203591 - FAX 06.484704

SEGRETERIA NAZIONALE
CENTRO STUDI UILCA ORIETTA GUERRA
Aderente a UNI Global Union

Comunicato stampa

Il Centro Studi Uilca Orietta Guerra: banche e finanza tra gli obiettivi del cybercrime

Fulvio Furlan: il Pnrr favorisca alfabetizzazione digitale e finanziaria

Roma, 5 febbraio 2022 – Nel 2021 banche e settore finanziario sono stati il quinto obiettivo dei *cyber attack* (8%). Primi gli obiettivi militari, governativi e di intelligence (14%); sanità (12%); ricerca e istruzione (11%) e i servizi on line (10%). Chiudono la classifica i produttori di *hardware* e *software* e le infrastrutture (rispettivamente con il 5% e il 4%). Questi i dati del rapporto *Clusit 2021*[1], analizzati dal **Centro Studi Uilca Orietta Guerra**, in occasione della giornata mondiale per la sicurezza in rete[2], martedì 8 febbraio. I danni economici di questi possibili attacchi a livello mondiale sono rilevanti e si stima che per il 2024 saranno pari a 3.000 miliardi di dollari, pari al Pil della Germania, con un costo medio mondiale di 500 dollari a persona. Per l'Italia si stima un danno pari a circa 20-25 miliardi di euro. Il *cyber risk* non va sottovalutato perché a oggi la spesa per la protezione, considerando solo il *cybercrime*, ed escludendo il *cyberespionage*, il *cybersabotage* e l'*hacktivism*[3], è circa 7 volte inferiore ai danni che ne derivano.

Sebbene in Italia (*Fig.1*) l'utilizzo dell'*internet banking* nell'ultimo decennio sia raddoppiato passando dal 18% al 39%, il Paese resta sotto la media europea del 58%. Per il **Centro Studi Uilca Orietta Guerra**, questo dato offre la possibilità al settore finanziario, nel breve periodo, di irrobustire le proprie difese contro il *cyber risk*. Il mercato assicurativo sta già investendo in questa nuova sfida digitale, sia in quanto utilizzatori di dati e dunque per proteggersi da eventuali attacchi, sia per offrire polizze che coprano questo rischio. Secondo l'*Osservatorio Cybersecurity & Data Protection* del Politecnico di Milano, in Italia la spesa in *cybersecurity* nel 2020 è stata di 1,37 miliardi[4].

La digitalizzazione della società ha aperto nuove occasioni di profitto al *cybercrime*, obbligando imprese e privati a investire in *software* e comportamenti che proteggano i dati, aziendali e personali, oggi nuovo *eldorado* dell'economia mondiale, contenuti nei vari *devices*.

Dal rapporto *Clusit 2021*, sono stati 1.871 gli attacchi mondiali di dominio pubblico nel 2020, dato in aumento del 66% rispetto al 2017, con una media mensile di 156 violazioni. Da non sottovalutare i *cyber attack* di natura *multiple targets,* pari al 20%, che colpiscono

[1] *Clusit – Associazione Italiana per la Sicurezza Informatica*
[2] *Safer Internet Day*
[3] *Clusit – Associazione Italiana per la Sicurezza Informatica*
[4] *L'Assicurazione italiana, 2020-2021 - Ania (pag. 200)*

Ufficio stampa Uilca
Lea Ricciardi
Mail: lea.ricciardi@uilca.it
Cell: +39 335 6672892

più obiettivi contemporaneamente, anche non correlati tra di loro. Gli allarmi contro i *cyber risk* sono presenti a livello mondiale: per l'*Allianz Risk Barometer 2021*[5] i *cyber incident* sono, dopo la *business interruption* (interruzione delle *global value chain*) e la *pandemic outbreak* (Covid-19), il terzo più importante elemento di rischio per l'economia mondiale.

"*In questo scenario, è necessario che il Piano Nazionale di Ripresa e Resilienza, tra le tante riforme che deve attuare, in particolare per quanto concerne il mondo del lavoro e l'occupazione, dia un impulso alle infrastrutture digitali, mirando al potenziamento dell'alfabetizzazione digitale e finanziaria, intervenendo sin dalle giovani generazioni*", dichiara il **segretario generale Uilca Fulvio Furlan**. Tale cultura è utile per individuare i bersagli di attacco più colpiti come credenziali compromesse, phishing, configurazione errata del cloud e compromissione delle mail aziendali[6].

La pandemia da Covid-19 ha favorito lo sviluppo dello *Smart Working*, che pur rispondendo alle necessità del momento, ha al contempo aumentato le possibilità di attacchi e intrusioni nelle reti aziendali. Alla luce di alcuni dati contenuti nel *Cost of data Breach Report 2021*, prodotto da Ibm[7], è utile una riflessione sullo sviluppo di tale modalità lavorativa. Nel rapporto si evince che per identificare e contenere una violazione di dati sono necessari 287 giorni, di cui 212 per identificare la violazione e 75 per correggerla. Questo tempo aumenta di 58 giorni quando più del 50% del personale lavora da remoto. Inoltre, le organizzazioni aziendali che utilizzano le intelligenze artificiali per prevenire gli attacchi informatici hanno costi dell'80% inferiori rispetto a chi non le utilizza.

Come riferisce il *Rapporto sulla stabilità finanziaria*[8] della Banca d'Italia anche le banche del Paese sono state oggetto di attacchi: nel 2020 sono stati registrati 15 gravi incidenti, in linea con quanto rilevato dalla Banca Centrale Europea per le banche significative dell'area euro. Gli attacchi hanno avuto conseguenze limitate e hanno provocato solo per un breve periodo di tempo l'interruzione dei servizi alla clientela. Per la Banca d'Italia il processo di esternalizzazione delle attività bancarie deve avvenire monitorando la sicurezza informatica, al fine di evitare che la stabilità finanziaria del settore venga compromessa.

Le porte da dove i cybercriminali possono attaccare il sistema informatico di un'azienda sono molteplici e lo sviluppo delle connessioni fra imprese e clienti, con un numero sempre crescente d'interfacce, obbliga ad alzare continuamente il livello di guardia, in attesa che le intelligenze artificiali diventino per tutti le guardie della nostra esistenza.

[5] *Allianz Risk Barometer 2021 - Allianz Global Corporate & Specialty*
[6] *Cost of data Breach Report 2021 - Ibm*
[7] *Cost of data Breach Report 2021 - Ibm*
[8] *Rapporto sulla stabilità finanziaria n. 2 - 2021 – Banca d'Italia*

Ufficio stampa Uilca
Lea Ricciardi
Mail: lea.ricciardi@uilca.it
Cell: +39 335 6672892

Fig. 1

% Fruitori internet banking tra i 16 e 74 anni												
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Delta 2010-2020
European Union - 27	34	36	38	40	42	44	46	49	51	55	58	71%
Belgium	51	54	56	58	61	62	64	67	69	71	75	47%
Bulgaria	2	3	4	5	5	5	4	5	7	9	13	550%
Czechia	23	30	35	41	46	48	51	57	62	68	70	204%
Denmark	71	75	79	82	84	85	88	90	89	91	94	32%
Germany	43	45	45	47	49	51	53	56	59	61	65	51%
Estonia	65	68	68	72	77	81	79	79	80	81	80	23%
Ireland	34	33	43	46	48	51	52	58	58	67	69	103%
Greece	6	9	9	11	13	14	19	25	27	31	37	517%
Spain	26	27	31	33	37	39	43	46	49	55	62	138%
France	50	51	54	58	58	58	59	62	63	66		32%
Croatia	20	20	21	23	19	33	38	33	41	46	50	150%
Italy	**18**	**20**	**21**	**22**	**26**	**28**	**29**	**31**	**34**	**36**	**39**	**117%**
Cyprus	17	20	21	23	24	20	28	28	33	41	52	206%
Latvia	47	53	47	55	57	64	62	61	66	72	76	62%
Lithuania	37	40	43	46	54	50	54	56	61	65	68	84%
Luxembourg	56	59	63	63	67	65	71	76	68	71	71	27%
Hungary	19	21	26	27	31	34	35	38	41	47	51	168%
Malta	38	42	41	43	45	47	47	50	51	54	60	58%
Netherlands	77	79	80	82	83	85	85	89	89	91	89	16%
Austria	38	44	45	49	48	51	53	57	58	63	66	74%
Poland	25	27	32	32	33	31	39	40	44	47	49	96%
Portugal	19	22	25	23	25	28	29	31	39	42	47	147%
Romania	3	4	3	4	4	5	5	7	7	8	12	300%
Slovenia	29	31	28	32	32	34	35	39	42	47	52	79%
Slovakia	33	34	40	39	41	37	45	51	50	55	58	76%
Finland	76	79	82	84	86	86	86	87	89	91	92	21%
Sweden	75	78	79	82	82	80	83	86	84	84	85	13%

Ufficio stampa Uilca
Lea Ricciardi
Mail: lea.ricciardi@uilca.it
Cell: +39 335 6672892