La sicurezza delle Infrastrutture Critiche al tempo del COVID-19

Domenico Vecchiarino

In questo documento vengono analizzati gli impatti del COVID-19 sulle infrastrutture critiche con particolare riferimento all'aumento della vulnerabilità di queste durante tutto il periodo emergenziale. Nell'elaborato vengono presentate le risposte delle principali aziende fornitrici di servizi essenziali e le normative predisposte dal governo per garantire l'erogazione dei beni primari nella crisi tutt'ora in corso. Vengono poi esaminate le principali minacce fisiche e soprattutto informatiche alle infrastrutture critiche con un riferimento anche alle minacce ibride.

Con l'epidemia di COVID-19 l'Italia, come il resto dell'Europa, si è trovata per la prima volta in una situazione emergenziale mai verificatasi prima. Per tutta la durata dell'emergenza COVID-19 le aziende operatrici nel settore delle infrastrutture critiche, per poter svolgere il proprio lavoro, hanno dovuto prendere una serie di misure che hanno avuto il duplice compito di garantire l'erogazione dei servizi essenziali, e dall'altra assicurare la salute dei propri lavoratori. All'interno di ogni azienda, per la maggior parte dei lavoratori "amministrativi" la soluzione dello *smart working* ha, *de facto*, risolto il problema della sicurezza dei dipendenti sul posto di lavoro. Provvedimenti diversi sono stati adottati, invece, per i lavoratori "operativi", cioè i tecnici impiegati ad esempio all'interno delle sale operative o in quelle di controllo. Per alcuni di essi è stato adottato il criterio definito "di segregazione" a fronte del quale gli addetti del settore sono stati isolati in alcune aree aziendali scelte *ad hoc*, per altri è stato adottato il criterio definito "della turnazione delle squadre" a fronte del quale alcuni gruppi di operatori, in seguito alla pronta attivazione dei siti di *recovery*, si sono alternati ad altri, evitando così ogni forma di contatto. Queste regole, che a tutti gli effetti si sono trasformate in *best practices*, sono state enunciate nelle linee-guida contenute nei Principi Precauzionali per gli operatori di Infrastrutture Critiche emanate dall'Ufficio del Consigliere Militare della Presidenza del Consiglio dei Ministri nei

primi giorni dell'emergenza e che hanno rappresentato un primo punto di riferimento, grazie alle quali gli operatori del settore hanno potuto rispettare tutte le misure opportune per il contenimento ed il contrasto al SARS-CoV-2, assicurando allo stesso tempo la fornitura dei servizi erogati[1]. Successivamente, il legislatore è intervenuto nuovamente nella materia con l'art.211 bis del D.L. 19.05.2020, n. 34 (il così detto DL Rilancio) che impone agli operatori delle infrastrutture critiche, al fine di assicurare la continuità del servizio di interesse pubblico erogato e il funzionamento in sicurezza delle infrastrutture stesse, di adottare o aggiornare i propri piani di sicurezza con disposizioni recanti misure di gestione delle crisi derivanti da emergenza di natura sanitaria emanate dalle autorità competenti. Nel dettaglio il comma 3 prevede che, per l'aggiornamento dei piani di sicurezza, le aziende fornitrici di servizi essenziali tengano conto delle linee guida sulla gestione dell'emergenza medesima emanate dai Ministeri competenti e dei principi precauzionali emanati dalla Segreteria infrastrutture critiche[2].

Ma l'epidemia di COVID-19 ha evidenziato ancora di più i rischi e le minacce alle infrastrutture critiche, sottolineando la vulnerabilità di alcune di queste e inasprendo la competizione tecnologica e scientifica per altre. Su tutte, il primo problema è stata l'adozione dello *smart working* tramite collegamenti VPN (*Virtual Private Network*)[3], che ha allargato il perimetro informatico delle aziende e di conseguenza moltiplicato le aree di attacco da parte degli hacker. Con l'adozione del lavoro da casa, infatti, i network aziendali sono stati ampliati in aree che non hanno lo stesso livello di protezione della rete aziendale; si pensi alle reti domestiche attraverso le quali i dipendenti si collegano, che sono al di fuori del controllo dell'ICT e, pertanto, rappresentano potenziali falle per la sicurezza delle reti aziendali.

---

[1] Presidenza del Consiglio dei Ministri, Segreteria Infrastrutture Critiche, Principi Precauzionali per gli operatori di infrastrutture critiche ai fini della continuità in sicurezza del servizio di interesse pubblico, 26 marzo 2020.

[2] Art. 211 bis del D.L. 19.05.2020, n. 34.

[3] La VPN (Virtual Private Network) è una rete privata virtuale utilizzata per criptare il traffico Internet e, di conseguenza, proteggere la propria identità online. In ambito prettamente aziendale, una VPN può essere paragonata ad una estensione geografica della rete locale privata (LAN) e che, quindi, permette di collegare tra loro, in maniera sicura, i siti della stessa azienda dislocati sul territorio.

Questa vulnerabilità, come è stato riportato dalla Relazione sulla politica dell'informazione per la sicurezza del 2020, è stata utilizzata dagli hacker durante la pandemia per effettuare attacchi informatici alle infrastrutture critiche e alle organizzazioni strategiche in prima linea nella lotta contro il COVID-19, quali ospedali, aziende farmaceutiche e produttori di apparecchiature medicali. L'allarme dell'intelligence per il settore sanitario è arrivato dopo i numerosi cyber attacchi subiti dal comparto dove "è emerso come attori statuali abbiano tentato di sfruttare le debolezze connesse all'ondata pandemica per porre in atto attacchi sofisticati, miranti a esfiltrare informazioni sensibili su terapie e stato della ricerca"[4]. Sul *thread* va segnalato il cyber attacco che ha colpito nella scorsa primavera l'Ospedale Spallanzani di Roma, hackerato durante il periodo di maggior picco della diffusione del COVID-19, che è stato oggetto di una specifica riunione straordinaria del Nucleo Sicurezza Cibernetica, l'organismo collegiale a cui è affidato il compito di gestire gli incidenti informatici di alto impatto sulla sicurezza nazionale[5]. A fare da sponda a questi allarmi sono arrivati i recenti numeri sugli attacchi al settore della Sanità, pubblicati nel Rapporto Clusit 2021, secondo cui il 55% degli attacchi a tema COVID-19 è stato perpetrato a scopo di *cybercrime*, ovvero per estorcere denaro; con finalità di *Espionage* e di *Information Warfare* nel 45% dei casi[6].

I cyber attacchi hanno riguardato anche altre infrastrutture critiche, in particolare il settore energetico. L'azienda Dragos[7], nel recente report 2020 Ics Cybersecurity Year In Review, ha posto l'accento sullo stato della sicurezza dei sistemi di controllo industriale

[4] Presidenza del Consiglio dei Ministri, "Relazione sulla politica dell'informazione per la sicurezza", 2020.

[5] "Coronavirus, riunione straordinaria del Nucleo Sicurezza Cibernetica", Sicurezza Nazionale, 1 Aprile 2020, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/comunicato-stampa-coronavirus-riunione-straordinaria-del-nucleo-di-sicurezza-cibernetica.html.

[6] Rapporto Clusit 2021, reperibile al seguente link: https://clusit.it/rapporto-clusit/

[7] Dragos è un'azienda leader globale di cyber security per gli industrial controls systems (ICS)/operational technology (OT).

[8]. In particolare, gli analisti di Dragos hanno individuato quattro nuovi gruppi di hacker che hanno preso di mira i sistemi industriali delle infrastrutture critiche energetiche, tentando di infiltrarsi nelle reti sfruttando le vulnerabilità dello *smart working*. Lo scopo di queste intrusioni sarebbe quello di rubare informazioni crittografando sistemi con *ransomware* o effettuando operazioni di hacking atte a determinare potenziali interruzioni di servizi essenziali.

Dietro tutti questi attacchi informatici non vi sono solo cyber criminali, ma anche e soprattutto molti gruppi *state-sponsored,* attraverso i quali molte nazioni hanno celato la loro identità. Paesi come Russia, Cina e Iran negli ultimi anni hanno aumentato le loro capacità cyber per meglio proiettare il loro potere all'estero con azioni aggressive specie contro le infrastrutture critiche, com'è stato nei casi famosi di Ucraina, Georgia ed Estonia[9]. La pandemia ha evidenziato la dipendenza da internet e dalle tecnologie digitali, allo stesso tempo aumentando l'esposizione a cyber attacchi, rendendo le infrastrutture critiche il target principale, con l'aggravante delle ripercussioni di azioni malevole sulla società che già vive un momento emergenziale. Si pensi ad esempio all'impatto di un blackout generato da un cyber attacco al sistema sanitario già fortemente impattato dal COVID-19 e che dovrebbe reggere le ripercussioni sulle terapie intensive. Oppure quello che sarebbe potuto accadere in Florida con il cyber attacco, fermato poco dopo l'inizio, contro il sistema idrico della città di Oldsam durante il quale gli hackers hanno modificato il livello di idrossido di sodio dalle

---

[8] Report 2020 Ics Cybersecurity Year In Review, Dragos, reperibile al seguente link: https://www.dragos.com/year-in-review/

[9] L'Estonia nel 2007 è stata vittima di una prolungata e massiccia ondata di attacchi del tipo DDoS (attacco informatico che consiste nel tempestare di richieste un sito fino a mandarlo off-line e renderlo irraggiungibile) che hanno intasato di traffico IP di computer di banche, agenzie governative e media nazionali, generando una pesante interruzione di alcuni servizi al pubblico, tra cui il prelievo di contante dai bancomat. La Georgia nel 2008 è stata colpita da una serie di attacchi del tipo DDoS, in concomitanza con il conflitto armato con i separatisti appoggiati dalla Russia, che hanno paralizzato i principali siti di istituzioni, banche, servizi e soprattutto i sistemi di comando e controllo dell'esercito georgiano. L'Ucraina è stata attaccata due volte, con due cyber attacchi alla rete elettrica, uno nel 2015 con il malware BlackEnergy, e nel 2016 con il malware Industrioyer (detto anche Crashoverraide), che hanno causato estesi e lunghi blackout.

normali 100 parti per milione a 11.100, una quantità che avrebbe potuto avvelenare i cittadini se l'acqua avesse raggiunto le loro abitazioni.[10]

Insieme alla pandemia si è anche diffusa un'infodemia, ovvero l'enorme diffusione di *fake news*, presenti in modo massiccio specie sui social network[11]. Queste operazioni di influenza rientrano nel quadro delle minacce ibride (*hybrid threats*)[12] portate avanti su più fronti da molti soggetti stranieri e da alcuni Paesi terzi, in particolare Russia e Cina, con lo scopo di influenzare e modificare pesantemente gli equilibri socio-politici in Europa e Nord America[13]. In particolare, come riportato nella già citata Relazione sulla politica dell'informazione per la sicurezza 2020, questa minaccia ibrida "è stata caratterizzata da costanti tentativi di intossicazione del dibattito pubblico attraverso attività di disinformazione e/o di influenza, nel contesto di più ampie campagne ibride". Dello stesso parere anche l'Alto rappresentante UE Josep Borrell, il quale ha affermato che "la pandemia da covid-19 è stata un vero e proprio test di prova per le minacce ibride, con attori statali e non statali che hanno utilizzato questa crisi di salute globale per portare avanti i propri obiettivi economici e sociali, con campagna ibride che hanno attaccato i nostri valori democratici e anche le nostre infrastrutture critiche in un tentativo di indebolire le nostre società e democrazie"[14].

---

[10] Massimo Gacci, "Mistero hacker in Florida: un clic da remoto per avvelenare la rete idrica. Prove di cyberwar?", *Corriere della Sera*, 12 febbraio 2021, https://www.corriere.it/esteri/21_febbraio_12/mistero-hacker-florida-clic-remoto-avvelenare-rete-idrica-prove-cyberwar-79c52db0-6d10-11eb-9243-a33dd4e4072e.shtml.

[11] Il termine è stato usato dall'Organizzazione mondiale della sanità (OMS).

[12] Con il termine minaccia ibrida si riferisce ad azioni condotte da attori statali o non statali, il cui scopo è minare o danneggiare un obiettivo influenzando il suo processo decisionale a diversi livelli. Tali azioni mirano alle vulnerabilità degli stati e delle istituzioni e possono svolgersi, nei settori politico, economico, militare, civile o dell'informazione.

[13] Domenico Vecchiarino, "Infrastrutture Critiche: Sicurezza nazionale al tempo del virus", 7 agosto 2020, *ISPI,* https://www.ispionline.it/it/pubblicazione/infrastrutture-critiche-sicurezza-nazionale-al-tempo-del-virus-27101.

[14] Redazione ANSA, "Borrell, da Russia e Cina disinformazione per indebolirci", *ANSA*, 1 marzo 2021, https://www.ansa.it/europa/notizie/europarlamento/news/2021/03/01/borrell-da-russia-e-cina-disinformazione-per-indebolirci_1ebce019-c500-46bf-828a-b52b2a72ede7.html.

Tra le minacce alle infrastrutture critiche va infine segnalata quella legata all'anarco-insurrezionalismo, che risulta essere al momento l'unica concretizzatasi con attacchi fisici alle infrastrutture. Al centro della propaganda della galassia eversiva ci sono tralicci e ripetitori, specie quelli della tecnologia 5G, ma anche reti in fibra ottica, aziende specializzate in tecnologie digitali e infrastrutture energetiche. Si segnalano perlopiù atti vandalici e/o incendiari e sabotaggi, ai danni soprattutto d'infrastrutture delle telecomunicazioni, come l'incendio avvenuto il 29 aprile a Roma, dei cavi di un'antenna di una compagnia telefonica nazionale e il sabotaggio, tra il 14 e il 15 maggio 2020 a Rovereto (TN), di centraline della fibra ottica che ha provocato il temporaneo blocco della rete[15]. Altri eventi dolosi ai danni di infrastrutture telefoniche sono avvenuti nel corso dell'ultimo anno, in particolare nel mese di aprile 2021 ci sono stati due eventi a Roma e uno a Offanengo.

Infine, la crisi economica generata dalla pandemia ha prodotto delle forti ripercussioni nell'economia nazionale che hanno aumentato i rischi per il Sistema Paese. La crisi sanitaria ha evidenziato ancor più i pericoli di possibili scalate e acquisizioni ostili da parte di Stati esteri e grandi multinazionali su settori economici nazionali e sulle infrastrutture critiche. Il governo è pertanto intervenuto ampliando i poteri della *Golden Power* con delle modifiche introdotte dagli artt. 15 e 16 del D.L. 8 aprile 2020, n. 23 – convertito, con modificazioni, dalla Legge 5 giugno 2020, n. 40 (cd. Decreto "Liquidità") – che hanno ampliato gli strumenti a disposizione del decisore politico per contrastare il rischio di acquisizioni predatorie od opportunistiche di aziende e di asset strategici per il Paese da parte di investitori esteri[16].

DOMENICO VECCHIARINO è un ricercatore di geopolitica, intelligence e infrastrutture critiche. Dopo la laurea in Scienze Politiche e Relazioni Internazionali alla Lumsa ha conseguito numerosi master e corsi di formazioni approfondendo i temi dell'intelligence, della sicurezza, della geopolitica e delle infrastrutture critiche.

[15] Presidenza del Consiglio dei Ministri, Relazione sulla Politica dell'Informazione per la Sicurezza, 2020.

[16] Presidenza del Consiglio dei Ministri, Relazione sulla Politica dell'Informazione per la Sicurezza, 2020.

Attualmente lavora in una società energetica, e collabora con l'Università Lumsa e altri centri di ricerca e think tank.

Si precisa che le opinioni esposte nel presente elaborato, ricevuto e reso disponibile nell'ambito dell'iniziativa Call for Papers #CASD2021, sono attribuibili esclusivamente all'autore e non rispecchiano necessariamente il punto di vista del Centro Alti Studi per la Difesa.