DIGITALIZZAZIONE E CYBER RISK IN CRESCITA PARALLELA

A cura del Comitato Italiano Gas
in collaborazione con Emanuele Martinelli, Energia Media

Sono tempi di veloci cambiamenti con un progetto Paese che prosegue con autorevole convinzione da parte delle istituzioni, verso i punti chiave del piano Italia 2030: banda ultralarga per tutti entro il 2026, cloud computing, PA interoperabile, digitale inclusivo, cyber security e innovazione *human centered*. Sono i pilastri della strategia digitale italiana tracciata dal ministro alla Transizione digitale Vittorio Colao che ben si inserisce nel quadro tracciato dall'Unione europea con il Digital Compass.

Un Paese il nostro che vuol raggiungere almeno l'80% dei servizi pubblici erogati online già nel 2026 e coprire le aree grigie con reti ad altissima velocità, con la realizzazione di infrastrutture su cui implementare servizi di pubblica utilità sempre più evoluti, per famiglie e imprese, erogati da utility ed energy company in versione digital anche con l'obiettivo di definire un diverso rapporto tra cittadino e amministrazione.

Su questo impianto assai prossimo si inserisce un allineamento in termini d'innovazione e digitalizzazione quanto mai auspicabile tra i settori energetici e della gestione del servizio idrico in particolare, ambiti che non hanno subito sostanziali variazioni fino a qualche anno fa e che oggi hanno tutti gli strumenti per rendere gli asset sempre più controllati, i consumi sempre meglio misurati, a vantaggio sia dei gestori che dei cittadini stessi.

Processi che peraltro cambieranno profondamente per esempio il mondo della distribuzione gas, grazie soprattutto al binomio digitalizzazione e "plurigenerazione" multigas, attraverso l'immissione in rete di idrogeno, biometano, gas di sintesi e così via.

Un momento storico di grande fascino e accelerazioni, pensiamo per esempio a smart meter, protocolli di comunicazione dati, telecontrollo e IoT, utilizzo dell'Intelligenza Artificiale e lo sviluppo di data management sofisticato.

Innovazione spinta alto livello di fragilità di sistema

Processi e tecnologie sempre più patrimonio degli operatori che al tempo stesso devono però fare i conti con evidenti fragilità da un punto di vista della sicurezza cibernetica.

Transizione ecologica, energetica e digitale vanno gestite con la massima sicurezza, dove la cyber security nazionale a protezione delle persone e delle infrastrutture diventa parte essenziale di un piano geostrategico che dovrà porre l'Italia - insieme alle nazioni europee più rappresentative - al centro di un quadro di sicurezza internazionale.

Comitato Italiano Gas – antonella.palmieri@cig.it – tel. 335 791 7978 (Antonella Palmieri)

Il contesto dal punto di vista della cyber security sta velocemente mutando.
È sempre più elevata l'attenzione di hacker in direzione delle campagne con finalità di spionaggio.

Pur permanendo marginali sul piano quantitativo (2,5%), queste forme di aggressione, definite Advancend Persistent Threat (APT) e caratterizzate dalla difficile individuazione per la natura volutamente occulta dell'azione ostile, si rivelano estremamente insidiose per il Sistema Paese perché in grado di causare perdita di operatività e competitività, nonché dispendio di risorse economiche per la loro mitigazione.

In quest'ambito, sono parse di assoluto rilievo le campagne indirizzate verso Ministeri e primari fornitori nazionali di servizi di comunicazione elettronica, condotte attraverso azioni digitali altamente strutturate e con l'impiego di tecniche e strumenti sofisticati.

Estremamente significativo l'impegno profuso dall'Intelligence nel contrasto di eventi che hanno interessato operatori di servizi essenziali del settore energetico, come dimostrato in occasione dell'attacco digitale emerso in dicembre ai danni della società texana SolarWinds, per il potenziale impatto su reti e sistemi nazionali.

Rapporto Clusit: nel 2020, 1871 attacchi di dominio pubblico

Il Rapporto Clusit (Associazione italiana per la sicurezza informatica) di recente pubblicazione evidenza che nel 2020 a livello globale si sono verificati 1871 attacchi gravi di dominio pubblico, con un impatto sistemico su ogni ambito della società, della politica, dell'economia e della geopolitica.

"Si è registrato un +12% di attacchi rispetto al 2019 con un trend di crescita pressoché costante, facendo segnare però un aumento di attacchi gravi del 66% rispetto al 2017; i servizi online sono stati colpiti dal 10% degli attacchi complessivi, sono cresciuti gli attacchi verso Banking & Finance (8%), verso i produttori di tecnologie hardware e software (5%), e verso le infrastrutture critiche (4%), nelle quali sono comprese quelle del settore energia.

Con l'evoluzione di città sostenibili, digitalizzazione e tecnologie che impattano su efficienza energetica (con l'introduzione per esempio di Smart Meter), energie rinnovabili e redesign del mercato all'insegna di flessibilità del mix energetico e sicurezza dell'approvvigionamento, gli operatori di sistema sono fortemente coinvolti con investimenti che non possono esser messi a rischio da problemi di cyber security.

Per questo si tratta di un tema sempre più all'attenzione degli amministratori delegati almeno quanto dei tecnici, dato che impatta fortemente sul patrimonio stesso di un'azienda.

Se un tempo dunque si parlava di sicurezza energetica con riferimento quasi esclusivamente agli approvvigionamenti, oggi è vero che le procedure di autorizzazione richiedono miglioramenti per lo sviluppo delle risorse necessarie a raggiungere gli obiettivi di decarbonizzazione dell'UE per il 2030 e il 2050; in questo contesto le città giocano un ruolo crescente nello sviluppo economico, infrastrutturale e sociale del paese e la sfida resta nell'identificazione di una nuova resilienza attraverso strumenti in grado di convertire efficacemente le aree urbane esistenti, così come le infrastrutture, gli edifici e le reti di trasporto attraverso sistemi più intelligenti e sostenibili.

Per questo il rapporto tra innovazione e sicurezza informatica si fa ogni giorno più complesso, soprattutto quando, come nel caso di Smart City e Smart Land, i nodi di connessione aumentano con governance di sistemi da integrare.

In riferimento a questo contesto ricordiamo che il 2020 è stato l'anno peggiore di sempre in termini di evoluzione e crescita delle minacce cyber e dei relativi impatti, evidenziando un trend persistente di aumento degli attacchi, della loro gravità e dei danni conseguenti.

"Se tre anni fa - si legge nel rapporto Clusit - si era registrato un "salto quantico" nei livelli di cyber-insicurezza globali, e nel 2018 si era ormai giunti a "due minuti dalla mezzanotte", nel 2019 era stata utilizzata l'espressione degli antichi cartografi "hic sunt leones", a significare di essere ormai giunti su un altro pianeta, in una terra incognita e pericolosa, popolata da mostri."

Una rotta che va invertita quanto prima. Se 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, 2015-2017, era stata "solo" dell'11% (da 873 a 1.127). Si sono moltiplicati i danni, con un cambiamento epocale nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi stessi.

Siamo di fronte a fenomeni che per natura e dimensione ormai travalicano costantemente i confini dell'IT e della stessa cyber security, con impatti profondi, duraturi e sistemici su ogni aspetto della società. Citando sempre il rapporto Clusit, "per fare un esempio eclatante della mutazione sostanziale dello spettro delle minacce cyber avvenuta negli ultimi 3 anni, il Cybercrime è paradossalmente diventato un rischio secondario, nel senso che ormai ci troviamo a fronteggiare quotidianamente minacce ben peggiori (in particolare Espionage e Information Warfare), nei confronti delle quali le contromisure disponibili sono particolarmente inefficaci.

Dai tempi del "salto quantico" (nel 2017) gli attacchi gravi rilevati sono aumentati del 66% (in 4 anni) e i danni globali causati dalle minacce cibernetiche rappresentano ormai una cifra enorme, pari se non superiore al PIL italiano (a seconda degli elementi considerati e di come vengono calcolati)."

In base al recente report McAfee a fronte di 945 miliardi di dollari di danni generati dal solo cybercrime nel 2020 (erano 600 miliardi nel 2018), nello stesso anno la spesa globale in ICT security è stata di 145 miliardi di dollari (di cui 1,5 miliardi in Italia); questo vuol dire che per ogni dollaro investito in sicurezza dai difensori gli attaccanti hanno causato (considerando solo gli attacchi realizzati con finalità cybercriminali) 7 dollari di perdite.

Una situazione grave che potrebbe mettere in discussione i benefici economici della rivoluzione tecnologica e organizzativa in atto; a cui si può rispondere aumentando sensibilmente gli investimenti in ICT Security (da una media del 2,5% del budget ICT ad almeno il 10% nel prossimo quadriennio) e introducendo rapidamente tutte le agevolazioni e gli incentivi necessari perché questo possa accadere, trattandosi di un importante rischio per la sicurezza dei Paesi.

In base al NIS Investment Report dell'ENISA di dicembre 2020, il gap di investimento in funzione della spesa ICT tra realtà europee e americane è in media del 41%. L'Italia investe in media il 50% in meno degli USA in ICT Security, in proporzione alla spesa ICT.

Utility ed energy company, si alza il grado di attenzione

Ricordiamo che il 27 ottobre 2020 una primaria S.p.A distributrice di energia è stata colpita da un attacco ransomware con esfiltrazione di circa 5 TB di dati; il giorno dopo un'altra multiutility italiana ha registrato lo stesso problema.

Ricordando sempre che i principali mercati di riferimento per la funzionalità ICS/SCADA protection riguardano i segmenti Energy & Utilities (che include Oil/Gas e Water/Wastewater); sistemi oggi monitorati per la loro estrema diffusione che mette al tempo stesso a rischio una serie di servizi fondamentali.

Il dato emergente dalle attività del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPIC, evidenzia come sia gli attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali (approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, comunicazione, trasporti, finanza sistemica), che gli attacchi apparentemente isolati, diretti a singoli enti, imprese o cittadini, manifestino una dimensione criminale organizzata, essendo ascrivibili all'operato di sodalizi ben strutturati, spesso operanti a livello transnazionale.

"Le tipologie di eventi cyber che hanno maggiormente impegnato gli operatori del Centro sono rappresentate dagli attacchi a mezzo malware, soprattutto di tipo ransomware, attacchi DDoS con finalità estorsiva, accessi abusivi con l'intento di carpire dati sensibili, campagne di phishing e, in ultimo, campagne APT (Advanced Persistent Threats), particolarmente insidiosi perché ricollegabili ad attori malevoli dotati di notevole expertise tecnico e rilevanti risorse."

Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici protocolli a tutela delle infrastrutture critiche nazionali.

Se dunque all'inizio del nostro contributo abbiamo parlato di accelerazione dei processi d'innovazione che toccano infrastrutture e utility, il rischio di rallentamento dei processi di crescita di una società digitale oggi esiste; sarà fondamentale evitare di innescare dinamiche negative (a livello micro e macro) rispetto allo sviluppo del digitale e alla distribuzione dei suoi benefici.

Gestione del rischio. Un approccio olistico

Intervenuto durante il Security Summit organizzato da Clusit nel marzo scorso Antonio Ieranò - IT e Cybersecurity Advisor - ha approfondito una serie di tematiche a partire dal rapporto tra gestione del rischio e sicurezza informatica.

"È necessario partire dall'assunto che il rischio zero non esiste. Negli ultimi tempi gli attaccanti cyber hanno modificato in modo significativo le modalità di attacco, cambiamenti non recepiti con la stessa rapidità dai responsabili delle security aziendali. Le motivazioni a proposito sono varie.

In primis, la diffusione del cloud e delle infrastrutture di dialogo con gli utenti che lavorano da remoto rende il passaggio più complicato; inoltre, un perimetro di rischio che sicuramente oggi va considerato è l'interazione con la supply chain, con le terze parti, con i clienti, e così via.

Questo threat landscape è chiaro a chi è dedito al cyber crime ma non a chi ha a che fare con la difesa; ancora oggi si tende ad idealizzare la security informatica e i suoi addetti, ma non è ancora chiaro che concetti come cyber crime e malware dovrebbero entrare nel lessico quotidiano e divenire patrimonio comune. Infatti, le piattaforme colpite dal ransomware sono innumerevoli, un tipo di attacco che nella maggior parte dei casi inizia via e-mail. In ordine seguono le connessioni RDP Remote Desktop Protocol e VPN Virtual Private Network, legate all'ambiente di chi lavora da remoto, il primo canale di comunicazione, l'interfaccia con le risorse e gli strumenti con cui pensiamo di rendere sicuri i nostri software.

Al di la del numero complessivo di attacchi, l'elemento fondamentale per comprendere a pieno l'importanza del cyber crime è la quantità di denaro che genera: il 51% delle revenue è ottenuto da attacchi di tipo BEC (Business Email Compromise), il 49% da attacchi di altro genere.

Questo tipo di azioni è definito *social engineering* verso esseri umani e sono quelle che hanno una resa economica più alta. Il cyber crime è un grande business ed è quindi necessaria un'ottimizzazione delle risorse rispetto ai risultati.

Attaccare oggi esseri umani è più efficiente ed efficace di qualsiasi altra azione, prendere di mira le persone monitorandone i comportamenti; fare OSINT Open Source INTelligence è possibile da chiunque, anche senza particolari competenze informatiche; è sufficiente infatti fare brevi ricerche su piattaforme social come ad esempio Linkedin, che fornisce un numero di informazioni tali da rendere manifesto uno specifico attacco per un singolo utente. Il problema principale attorno al quale ruota il tutto è quindi la gestione e il calcolo del rischio."

Per avere un indice di rischio affidabile calcolando gravità per probabilità, quest'ultima dev'essere relazionata al tipo di minaccia e vulnerabilità, intesa come capacità della minaccia di ottenere l'effetto desiderato. Riportando questo discorso sugli esseri umani l'indice di rischio va calcolato attraverso il rapporto tra gravità, minaccia e vulnerabilità".

Come si traduce questo nella gestione di una popolazione di utenti che lavorano e accedono a sistemi informatici? Ponendo come presupposto il rischio calcolato secondo i tre fattori sopra citati, si aprono tre diverse dimensioni:

- **Minaccia:** considerare quanti e quali attacchi vengono indirizzati verso un utente o gruppi di utenti; quindi il numero, da chi vengono elaborati, che tipo di attacchi sono, quale è la pericolosità intrinseca. Significa avere una comprensione precisa e puntuale di cosa sia realmente la minaccia da affrontare.
- **Vulnerabilità:** quanto sono attaccabili i miei utenti; questo dipende dalla loro capacità reattiva e dalla loro esposizione oggettiva al rischio. Quindi avere la consapevolezza di usare certe risorse in rete, di essere esposti pubblicamente o avere comportamenti a rischio.
- **Privilegio:** a quali risorse gli utenti possono accedere, che tipo di informazioni posseggono, quali azioni possono svolgere in autonomia, quali risorse gestiscono e quali diritti amministrativi hanno. Questi tre domini entrano nel campo dell'esperienza dell'uso normale degli utenti.
-

Se consideriamo queste dimensioni come facenti riferimento a persone che condividono diversi ambiti, possiamo dividere in aree i nostri utenti in termini di rischio che emerge dalla sovrapposizione di questi tre domini. Da queste intersezioni derivano tre diversi target:

- **Imminent Target:** un utente è vulnerabile e ha privilegi elevati. Uno degli utenti considerato dall'attaccante veicolo principe per sviluppare l'attacco.
- **Major Target:** non è così vulnerabile ma necessita comunque di attenzione.
- **Soft Target:** non ha grandi privilegi ma è facile da attaccare. Quest'ultimo è spesso utilizzato come veicolo per fare un movimento laterale verso altri target.

A seconda di dove si viene collocati sono necessarie diverse considerazioni. L'idea di base è poter definire il rischio associato agli utenti calcolato su vulnerabilità, attacchi e privilegi.

"Quando sono consapevole del rischio, lo gestisco e quindi posso fare security - spiega Ieranò; nel momento in cui non sono a conoscenza della mia esposizione mi limito a un acquisto di tecnologia fine a sé stessa.

Conoscere l'indice di rischio mi permette di sapere chi è a rischio, perché lo è, qual è la natura delle minacce e quali sono le azioni di protezione da eseguire. L'approccio quindi, è di analisi matematica legata al rischio.

È fondamentale che ci siano sistemi che lo facciano in maniera consistente e continua perché il rischio è multidimensionale, quindi siamo obbligati a tener conto di situazioni complesse che si intersecano. Il pericolo non è univoco ma può provenire da sorgenti correlate, inoltre dipende dal tempo e dal contesto.

È necessario per questo un monitoraggio costante e un aggiornamento quasi quotidiano, su cui è necessario investire; a maggior ragione quando ci si occupa di asset strategici come quelli legati alle infrastrutture.

I tre valori -minaccia, vulnerabilità e privilegi- non sono dunque fra loro impossibili da correlare, si può trasformare la questione in una funzione che leghi i tre elementi; e la funzione dipende dal dominio di sicurezza che si analizza.

Estendendo la gestione al rischio, questi nel tempo dipende dalla sommatoria delle funzioni che si calcolano nel momento temporale; l'uso per esempio di piattaforme dedicate rende meno complesso questo tipo di gestione.

Con questo approccio per ogni gruppo di utenze è possibile individuare i rischi a cui sono esposti, gli attacchi e la vulnerabilità. Permette quindi di identificare i security control che devono essere implementati per diminuire il livello di rischio stesso; security control diversi in base ai tre elementi che compongono la matrice di rischio, che come detto sopra, non è più quindi bidimensionale ma multidimensionale.

"Tutto questo è fondamentale - conclude Ieranò. Per capire qual è la nostra posizione nei confronti dei pericoli che arrivano dall'esterno e dall'interno dobbiamo poter monitorare in modo costante e coerente, in ottica di risk rating, quello che accade; solo così abbiamo la possibilità di intervenire opportunamente per gestire l'esposizione e ridurre i rischi.

Questo è un approccio diverso dal solo dotarsi di alert di sistema che mi fornisce qualche informazione sull'evento specifico ma nulla su come si modifica la mia posizione di rischio nei confronti di questo tipo di attività o attacco.

Avere un approccio olistico rende dunque la gestione più coerente con i rischi che andiamo a incontrare e per questo diventa fondamentale un monitoraggio costante dei sistemi di gestione che quotidianamente utilizziamo."

Aggiornamenti sugli sviluppi del programma saranno forniti nelle prossime newsletter.

A chi interessa

- *Aziende di Trasporto, Distribuzione e vendita gas, elettricità, acqua*
- *Aziende del settore ICT e Telecomunicazioni*
- *Fabbricanti di apparecchi utilizzatori, accessori, componenti e strumenti*
- *Aziende costruttrici di impianti*
- *Progettisti, consulenti aziendali*
- *Istituzioni ed Enti di Ricerca*

Forum UNI CIG 2021 i temi trattati:

10 giugno: La sicurezza negli usi finali dei gas combustibili

23 settembre: Digitalizzazione degli asset e dei processi. Dallo smart meter alla Cyber Security: il ruolo decisivo delle nuove tecnologie.

11 novembre: Innovazione e ricerca nel settore multi-gas per una transizione energetica resiliente

Comitato Italiano Gas – antonella.palmieri@cig.it – tel. 335 791 7978 (Antonella Palmieri)