TECHNOLOGICAL

COLLANA "MACRO TREND" | SETTORE ASSICURATIVO | 2024

INTERNET OF EVERYTHING

OSSERVATORIO

REPUTATIONAL & EMERGING RISK

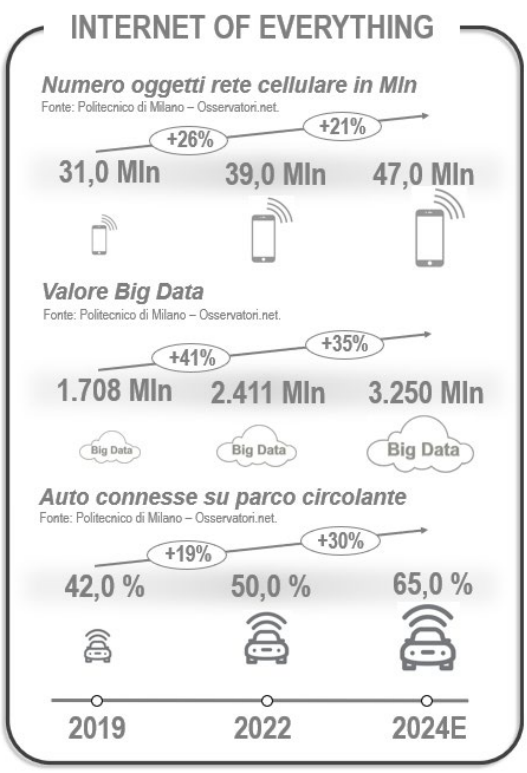
Gruppo Unipol

TECHNOLOGICAL

INTERNET OF EVERYTHING

Sono sempre più diffusi i device dotati di sensori che dialogano con altre apparecchiature elettroniche. La diffusione del 5G, dell'AI e dell'Edge Computing consentirà di rilevare sempre più dati, molti di questi sensibili come quelli sulla salute. E i rischi per la sicurezza saranno molti e da monitorare con attenzione.

I Macro Trend in sintesi Mappa Interconnessioni



Nel 2024 saranno oltre 207 miliardi i dispositivi connessi alla rete mondiale di strumenti, giocattoli, dispositivi ed elettrodomestici che compongono l'Internet delle cose (IoT). Un numero sempre crescente di essi non sarà computer o smartphone, poiché di tutto, dagli spazzolini da denti ai macchinari industriali pesanti, potrà essere connesso. Si tratterà sempre più di dispositivi intelligenti dotati di intelligenza artificiale. Numeri decisamente importanti per un settore che vede un trend rialzista senza sosta. Il segmento IoT sta ancora affrontando una serie di sfide: catena di approvvigionamento vincolata, inflazione, nuovi ceppi del virus e crisi geopolitica. Tuttavia, le condizioni di forte domanda continuano a supportare la redditività della maggior parte dei player con esposizione all'IoT. Le implementazioni tecnologiche che si osservano in relazione ad altri Macro Trend come, ad esempio, il Metaverso o l'Intelligenza artificiale e Robotica, si riflettono anche nell'IoT. Gli utenti si stanno allontanando dal 2G/3G per indirizzarsi pressoché completamente verso 4G/5G. Le connessioni IoT 4G sono cresciute del 24% grazie alla maggiore adozione di chipset, ma a riguardo della carenza di chip la tendenza non è particolarmente favorevole e le catene di approvvigionamento sono ancora in affanno. Oltre a queste problematiche, si aggiunga il fatto che è in atto una guerra per l'accaparramento di talenti digitali. Molte aziende stanno affrontando un'enorme sfida per trovare manodopera qualificata per andare avanti a pieno regime con la trasformazione digitale, l'IA, l'IoT e i progetti cloud. L'edge computing sarà una tendenza chiave dell'IoT poiché i produttori inseriranno funzionalità di analisi integrate nelle loro apparecchiature, spostando essenzialmente l'elaborazione dei dati il più vicino possibile alla fonte di origine. Invece di dotare le macchine di ciò che Forbes chiama sensori "stupidi", come microfoni o fotocamere di base, i dispositivi edge sono invece dotati di sensori intelligenti. Ciò include microfoni con capacità di elaborazione del linguaggio, sensori di umidità e pressione o telecamere dotate di visione artificiale. L'edge computing può combinarsi con questi sensori intelligenti e i calcoli possono essere eseguiti più rapidamente, mentre meno dati vengono trasmessi da e verso il cloud per alleviare la congestione della rete e ridurre la latenza sulla rete. L' edge computing ha il potenziale per rendere più pratiche le auto a guida autonoma, affrontando anche molti degli odierni problemi di larghezza di banda, sicurezza e affidabilità del cloud. Nonostante questi vantaggi, oggi è ancora una tecnologia di nicchia, ma le cose cambieranno con l'espansione dell'Internet delle

Cresce la consapevolezza di aziende, pubbliche amministrazioni e consumatori, sempre più interessati a gestire da remoto asset e dispositivi smart, attivando servizi e funzionalità avanzate.

Osservatori.net – Politecnico di Milano

cose. Un altro elemento fortemente sotto attenzione è la sicurezza. Con l'aumento della popolarità dell'Internet delle cose, i suoi difetti di sicurezza diventano sempre più preoccupanti. La maggiore adozione di applicazioni e dispositivi intelligenti (tablet, smartphone, dispositivi indossabili) da parte dei consumatori rappresenta un rischio credibile per la privacy e la sicurezza delle persone. Poiché i dati vengono raccolti sul loro movimento, posizione, salute e stato mentale, ciò li espone a rischi di violazione dei dati e privacy. In una rete complessa di dispositivi connessi, se un dispositivo è compromesso, ogni altro dispositivo con cui comunica deve affrontare una potenziale vulnerabilità. Inoltre, le "cose" fisiche che compongono l'IoT possono essere perse o rubate, richiedendo un altro livello di sicurezza per la protezione da violazioni e attacchi. IoT World Today evidenzia come nell'ultimo anno gli attacchi verso gli IoT siano aumentati del 400%. L'Internet delle cose ha inaugurato una nuova era di connettività e comodità, ma ha anche portato con sé nuove sfide sotto forma di attacchi informatici. Essere consapevoli dei tipi di minacce che i dispositivi IoT devono affrontare e adottare misure proattive per proteggerli è essenziale per proteggere la privacy personale, i dati sensibili e le infrastrutture critiche. Poiché il panorama dell'IoT continua ad evolversi, altrettanto devono fare i nostri sforzi in materia di sicurezza informatica per garantire un futuro sicuro e connesso.

FOCUS ON...

► La sicurezza come priorità

I device IoT non sono esenti da problematiche di cybersicurezza

I tradizionali framework di sicurezza informatica sono probabilmente inadeguati per l'IoT di oggi. I dispositivi IoT continuano a moltiplicarsi, e alcuni hardware e software già in uso, spesso creati prima delle maggiori innovazioni IoT attuali, non sono in grado di stare al passo con questa evoluzione tecnologica molto rapida. Nuove categorie di IoT vengono introdotte e ampliate man mano che gli innovatori perseguono una più recente "killer app" in uno specifico settore: medico, automobilistico, consumer, ecc. Le violazioni e gli attacchi che vanno dal malware agli attacchi DdoS (Distributed Denial of Service) passando per il semplice errore umano continuano ad aumentare parallelamente alla proliferazione di dispositivi intelligenti vulnerabili come telefoni cellulari, tablet, dispositivi indossabili, smartwatch, fitness tracker, veicoli, elettrodomestici, e altro ancora. Molti di questi attacchi non provengono dalla debolezza dei singoli dispositivi, ma dai servizi centralizzati che si connettono a questi dispositivi. In alcuni casi, una nuova innovazione IoT può essere così convincente che l'aspetto "Internet" dell'IoT passa inosservato e i rischi per la sicurezza associati vengono ignorati. Le statistiche e le previsioni sulle violazioni della sicurezza IoT forniscono numeri importanti. Anche una semplice stampante per ufficio può aprire la porta alla perdita di dati. Se poi i dispositivi sono quelli che consentono il monitoraggio della nostra salute, l'interfaccia con il veicolo che stiamo guidando, la gestione della domotica della nostra abitazione, allora il fenomeno diventa ancora più pericoloso. Per sviluppare un framework di governance della sicurezza informatica, l'obiettivo è integrare la progettazione e i controlli durante lo sviluppo dei prodotti e dei servizi. Questo approccio "secure by design" integra le funzioni di cyber assurance all'interno dello stack tecnologico e durante tutto il ciclo di vita dello sviluppo del prodotto/servizio. La sicurezza informatica non può essere applicata al dispositivo IoT una volta sviluppato.

Macro trend in a glance • INTERNET OF EVERYTHING

I DRIVER DEL CAMBIAMENTO

- Diffusione del 5G e sviluppo del 6G (ma non prima del 2030)
- Progressiva evoluzione verso l'internet of nano things
- Evoluzione e diffusione dei sensori intelligenti
- Integrazioni con protocolli di intelligenza artificiale
- Diffusione anche nei confronti di generazioni più anziane
- Utilizzo confermato e consolidto in diversi ambiti emergenti e non
- Sviluppo nel percorso di governo e analisi dei Big Data

GLI IMPATTI SUL SETTORE ASSICURATIVO

Sul Sistema

- Apertura verso nuovi modelli di business nel settore assicurativo
- Miglioramento della gestione dei reclami attraverso la raccolta di dati in tempo reale sugli incidenti e sulla posizione geografica
- Sempre più focus sul servizio rispetto al prezzo
- Apertura verso un contesto di ecosistema gestito mediante le partnership
- Incremento dell'ottica della prevenzione

Sui Clienti

- Incentivo verso comportamenti virtuosi
- Polizze a misura con tariffe personalizzate
- Focus sulla prevenzione intesa come elemento di salvaguardia da applicare in contesti assicurativi trasversali
- Possibile limitazione della privacy in ottica di utilizzo e diffusione dei dati, da compensare con operazioni di "reward" intese come proposte di servizi aggiuntivi o di scontistica

OPPORTUNITA'

- Sviluppo di nuovi prodotti
- Prevenzione degli incidenti
- Pricing sempre più personalizzato, predittivo e dinamico
- Miglioramento dell'esperienza cliente
- Maggiori "touch-point" e maggiore percezione di rilevanza nella vita quotidiana del cliente anche attraverso l'associazione di un elemento "tangibile" alla polizza
- Riduzione dei costi operativi, soprattutto con l'adozione di sistemi di prevenzione
- Evoluzione del ruolo dell'assicurazione da "Payer" a "Partner and Preventer"
- Ottimizzazione della gestione sinistri e contrasto delle frodi
- Ampliamento delle opportunità di servizio al cliente
- Iniziative di creazione di valore condiviso con cliente e con collettività

RISCHI

- Rischio perdita presidio proprietà dati e proprietà cliente
- Nuove sfide normative e di conformità, specialmente in relazione alla protezione dei dati personali e alla gestione dei rischi
- Perdita di quote di mercato e/o rischio di antiselezione a seguito di una mancata evoluzione dei modelli di pricing e di inadeguato sviluppo di analytics
- Crescente potere dei costruttori di auto e dei player tecnologici in grado di intermediare la relazione con il cliente e l'accesso a informazioni privilegiate
- Difficoltà di attrazione e ritenzione risorse specializzate per l'analisi e gestione di Big Data (Trend New Skills)
- Crescente vulnerabilità a cyber risk con potenziali rischi catastrofali
- L'utilizzo estensivo di dispositivi IoT potrebbe esporre le compagnie assicurative a nuovi tipi di rischi, come la responsabilità per danni causati da dispositivi difettosi o la dipendenza da fornitori di tecnologia terze parti.

Hanno partecipato alla predisposizione del presente Quaderno:

Liliana Cavatorta
Capo Progetto - Responsabile Emerging and Reputational Risk

Gianluca Rosso
Emerging and Reputational Risk

Davide Iaciofano
Emerging and Reputational Risk

Elena Borovina
Emerging and Reputational Risk

Prof. Egeria Di Nallo
già Direttore del Dipartimento di Sociologia dell'Università di Bologna

Il Gruppo di lavoro si è avvalso del supporto del Tavolo Tecnico dell'Osservatorio R&ER e della sponsorship della funzione Risk Management nella persona di Gian Luca De Marchi.

unipol.it

Unipol Gruppo S.p.A.
Sede Legale
Via Stalingrado, 45
40128 Bologna