Sicurezza e percezione del pericolo

Annuncio shock. La FIA durante una conferenza stampa nel weekend ha comunicato che dalla prossima stagione di Formula 1 non sarà più ammesso il pubblico alle gare. Tutti i sostenitori, anziché limitarsi al tifo dalle tribune, potranno recarsi presso i paddock durante i weekend di gara, ricevere una delle migliaia di monoposto che le scuderie metteranno a disposizione ed entrare in pista insieme ai piloti. Ogni partecipante potrà decidere se competere attivamente nella gara, limitarsi a un giro turistico oppure percorrere il circuito contromano per sperimentare nuove prospettive. Per girare in pista non sarà necessario possedere patenti di guida e, nel caso il tifoso sia talmente giovane da non raggiungere i pedali, le scuderie metteranno a disposizione anche delle comode prolunghe e cuscini per il sedile.

Questo annuncio è talmente inverosimile da risultare immediatamente falso, e così è. In uno scenario di questo tipo la pericolosità intrinseca è percepibile a chiunque. Eppure, traslando questo annuncio dai motori al mondo digitale, è esattamente quello che sta succedendo.

Pericolo non percepito

Nei prossimi anni la connettività diffusa sarà ancora più presente e pervasiva, e in termini anche numerici saranno molti di più i macchinari, gli impianti o i semplici elettrodomestici connessi rispetto a persone senzienti con uno smartphone in tasca. I rischi cyber che ne derivano non sono percepiti e sono anche difficilmente quantificabili proprio perché sono immensi. Sono rischi potenzialmente illimitati perché grazie a una connessione, chiunque, da qualunque parte del mondo, può fare qualsiasi azione su ogni dispositivo connesso. Questo avviene perché il mondo digitale è ancora largamente percepito come immateriale, come un non luogo dove è improbabile che succedano cose brutte. È l'esatto contrario, il mondo digitale è ormai una copia speculare del mondo fisico e in molti casi è la controparte digitale che governa quella fisica.

Come può essere limitato il pericolo

Partiamo dal presupposto che il pericolo non potrà mai essere eliminato del tutto perché insito nella tecnologia stessa. Il pericolo può essere contenuto tramite iniziative istituzionali o grazie a scelte di produttori e fornitori di tecnologia. Sfortunatamente, però, nessuno dei due approcci funzionerebbe. Analizziamo perché. Nel primo caso, un'iniziativa istituzionale, il pericolo potrebbe essere limitato impostando delle soglie di accesso alla tecnologia. Così come succede per il porto d'armi, un brevetto di volo o anche solo per la patente di guida, le istituzioni dovrebbero limitare l'accesso alla tecnologia, alla connettività e alla rete Internet solamente alle persone e alle aziende che possiedono determinati requisiti. In un mondo ideale i requisiti dovrebbero essere legati alla consapevolezza dei rischi che si corrono in rete, nel mondo reale sarebbe la creazione di un mercimonio in cui le credenziali di login per connettersi a Internet verrebbero scambiate al mercato nero. Nel secondo caso, ovvero le limitazioni imposte dai produttori stessi sarebbero impossibili perché in contrasto con il loro stesso business. Nessun vendor ridurrebbe la sua base clienti, conquistata a fatica, rendendo i propri prodotti tecnologici non accessibili a tutti, solo per aumentare la sicurezza dei propri utenti.

Una possibile soluzione potrebbe essere uno scenario definibile di 'digitalizzazione incrementale' in cui la governance istituzionale e l'implementazione tecnica delegata ai player tecnologici siano a loro volta vigilati da un garante. In maniera similare a quanto avvenuto per il Gdpr, si potrebbe iniziare a pensare a un Gsbr (General Security Behaviour Regulation) in cui, basandosi sul livello di preparazione dell'utente e sulla sua consapevolezza dei rischi informatici, può avere accesso a un numero maggiore o più 'rischioso' di servizi. Man mano che l'utente migliora la sua competenza sale di livello e si può muovere in sicurezza nella rete. Se non si ha nessuna competenza e consapevolezza, si potrà accedere alla rete in sola lettura, senza possibilità di caricare o condividere informazioni personali, in sostanza utilizzando Internet solo per leggere le notizie e controllare il meteo. Si conosce il ransomware e il suo funzionamento e, soprattutto, come evitarlo? Bene, allora si può ottenere una casella email da cui inviare e ricevere allegati. Si è consapevoli del metodo di classificazione dei dati e in grado di distinguere confidenzialità, integrità e disponibilità? Ottimo, allora è concessa l'scrizione ai social network. Può apparire un approccio intransigente, ma è l'unico con un elemento di proporzionalità utile a limitare i pericoli che si corrono in rete. I pericoli in rete sono ancora ampiamente sottovalutati ma basta spendere mezz'ora sul motore di ricerca Shodan o altri portali simili per rendersi conto di quante decine di migliaia di dispositivi siano connessi in rete senza nessuna protezione: hard disk contenenti dati privati o aziendali, webcam accese e puntate in ogni angolo della casa, router e access point con user e password di default ecc.

Approfondendo i pericoli che si corrono in rete, forse non fa più così paura gironzolare per un circuito di Formula 1 in contromano.

Simone Zanotti, sales & marketing director di E4 Computer Engineering (www.e4company.com)