5G e intelligenza artificiale i rischi cyber del 2030. Il report

Nel 2030, la connettività avrà un impatto su ogni aspetto della vita quotidiana, sia a livello fisico che psicologico. I cybercriminali si evolveranno per utilizzare e approfittarsi delle innovazioni tecnologiche, come da loro abitudine.

Lo rivela Trend Micro in "Project 2030: Scenari per il futuro della cybersecurity", uno studio a cui è legata una webserie che mostrano come potrebbe essere il mondo all'inizio del prossimo decennio, in modo particolare nel merito delle nuove minacce alla sicurezza informatica.

Tra queste, il gruppo annovera i prossimi standard di connettività 5G e 6G, che renderanno i tentativi di intromissione più precisi e sofisticati.

Poi gli strumenti di intelligenza artificiale, che potranno dare anche ad hacker senza competenze tecniche l'opportunità di compiere attacchi cybercriminali, su scale di ampiezza più grandi, facilitati da software automatici.

Ecco quello che potrebbe succedere nel 2030

- Gli strumenti di intelligenza artificiale permettono anche agli individui senza competenze tecniche di compiere attacchi cybercriminali, su una scala di grandezza mai vista prima
- Gli attacchi causano il caos nelle supply chain delle industrie e danni fisici agli esseri umani che utilizzano impianti cyber

- L’ingegneria sociale e la disinformazione diventano più radicate e difficili da ignorare, a causa dell’utilizzo di massa degli Heads Up Display (HUD)
- Gli ambienti caratterizzati da un utilizzo massivo di IoT (Massive IoT environments – MioT) attraggono azioni di sabotaggio ed estorsione, soprattutto nei settori manifatturiero, della logistica, dei trasporti, della sanità, dell’istruzione, della vendita al dettaglio e domestico
- Le tecniche di occultamento attraverso l’intelligenza artificiale rendono impossibile l’attribuzione delle identità, ponendo problematiche circa l’incident response e la gestione degli accessi
- Il 5G e il 6G rendono gli attacchi più precisi e sofisticati
- L’ “Everything as a Service” trasforma i cloud provider in ricchi obiettivi per i cyber criminali
- Il tecno-nazionalismo diventa uno strumento geostrategico chiave per alcune delle nazioni più potenti del mondo e questo allarga ulteriormente il divario con gli altri Paesi

Secondo il report le tecniche di occultamento attraverso l’intelligenza artificiale rendono impossibile l’attribuzione delle identità, ponendo problematiche sull’effettivo riconoscimento dei criminali e dei loro accessi non autorizzati ai sistemi violati. Spunto interessante è quello del “tecno-nazionalismo”. Con tale termine, gli specialisti indicano uno scenario in cui la tecnologia avanzata diviene “uno strumento geostrategico chiave per alcune delle nazioni più potenti del mondo e questo allargherà ulteriormente il divario con gli altri Paesi”. Project 2030 è stato costruito sulla base di ricerche open source, sullo studio di rapporti sul panorama delle minacce a firma di aziende e scienziati, sul monitoraggio di brevetti e con il supporto di un sondaggio online solo su invito e un altro rivolto ai CISO.

Scarica il report

https://www.key4biz.it/5g-e-intelligenza-artificiale-i-rischi-cyber-del-2030-il-report/386918/