PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5433 di Lunedì 17 luglio 2023

Se siete interessati alla sicurezza informatica, occorre guardare lontano

L'agenzia europea per la sicurezza informatica, ENISA, ha recentemente pubblicato un documento, che cerca di mettere in evidenza i rischi informatici che potranno manifestarsi o accrescersi da oggi all'anno 2030.

In allegato a questa notizia, i lettori trovano una infografica, che permette loro di guardare lontano, in modo da prepararsi per tempo all'evoluzione dei rischi informatici dei sistemi, affidate alle loro cure. Ecco i 10 principali rischi che la agenzia europea per la sicurezza delle reti ha già individuato.

1-Compromissione della catena logistica di aggiornamento del software

I componenti ed i servizi sempre più integrati, che coinvolgono soggetti terzi, possono portare a nuove impreviste vulnerabilità, che possono compromettere la sicurezza informatica sia dal lato del fornitore, sia dal lato del cliente.

2-Campagne di disinformazione

Gli attacchi di tipo deepfake possono manipolare l'atteggiamento di intere comunità, per orientarle verso atteggiamenti geopolitici, che poco possono avere a che fare con la realtà.

3-Aumento incontrollato delle tecniche di sorveglianza digitale e perdita di privacy

Il riconoscimento facciale, la sorveglianza digitale e il monitoraggio delle piattaforme Internet o di archiviazione di dati potrebbero diventare un attraente bersaglio per gruppi criminali.

4-Gli errori umani e le debolezze di sistemi informatici non aggiornati

La rapida adozione di IoT, l'esigenza di aggiornare sistemi informatici antiquati e una progressiva diminuzione di competenze tecniche disponibili potrebbero portare ad una mancanza di conoscenze, addestramento e comprensione del sistema informatico, sia a livello fisico, sia a livello di software, con evidenti conseguenze legate alla sicurezza informatica.

5-Attacchi mirati potenziati da smart devices

Attraverso Internet è possibile ottenere un gran numero di dati, disponibili a smart devices, che gli attaccanti possono utilizzare per accedere a informazioni specifiche o per perpetrare attacchi più sofisticati.

6-Insufficiente analisi e controllo di infrastrutture basate su strutture spaziali

La continua intersezione fra le infrastrutture private e pubbliche, nello spazio che circonda la terra, fa sì che la sicurezza di queste nuove infrastrutture e tecnologie dovrebbe essere approfondita, perché una insufficiente conoscenza dei rischi connessi potrebbe portare a vulnerabilità di questa porzione della rete informatica di comunicazione

7-Crescita delle minacce ibride di tipo avanzato

Gli attacchi fisici o off line continuano a crescere e talvolta vengono abbinati con attacchi informatici, grazie all'aumento di dispositivi intelligenti, all'uso del cloud, all'identità on-line e alle piattaforme sociali.

8-Insufficienza di risorse specializzate

La mancanza di risorse specializzate e di specifiche competenze nel settore della sicurezza informatica può consentire a gruppi di criminali informatici di prendere a bersaglio le organizzazioni, che non dispongono di sufficienti competenze tecniche.

9-I fornitori di servizi informatici distribuiti in vari paesi

Il settore ITC, che permette collegamento tra servizi critici, come ad esempio i trasporti, le reti elettriche e le reti industriali, offre servizi che superano molte frontiere e possono quindi diventare oggetto di attacchi provenienti da paesi, in cui queste strutture non hanno raggiunto un livello soddisfacente di protezione da attacchi informatici criminali.

10-L'abuso dell'intelligenza artificiale

La manipolazione degli algoritmi di intelligenza artificiale e la cattura incontrollata di dati può creare situazioni pericolose, legate a disinformazione e diffusione di notizie false, che possono portare a conseguenze oltremodo gravi, sia a livello civile, sia a livello militare, per inquinamento dei dati.

clicca sull'immagine per vederla ingrandita

Adalberto Biasiotti

---

www.puntosicuro.it