PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4802 di Lunedì 26 ottobre 2020

Una lettura obbligata per tutti i responsabili della sicurezza informatica

En Isa, l'agenzia dell'unione europea per la sicurezza informatica, ha pubblicato l'ultima rassegna sugli attacchi informatici in Europa. Sono evidenti segni di una evoluzione delle tecnologie di attacco e tutti i responsabili della sicurezza informatica.

Ogni anno la ENISA pubblica un rapporto sugli scenari di criminalità informatica, avvenuti nell'anno precedente in Europa, con l'obiettivo di aiutare tutti i soggetti coinvolti nella sicurezza informatica a definire strategie atte a difendere i cittadini, le aziende e lo spazio informatico. Il contenuto di questo rapporto è raccolto sia da documenti pubblici, come ad esempio articoli, opinioni di esperti e simili, sia da rapporti sulla sicurezza informatica e da interviste con prestigiosi esponenti della comunità informatica.

Sulla base delle informazioni raccolte, ENISA produce il proprio documento, il cui pregio particolare sta nel presentare l'elenco annuale del di 15 maggiori rischi informatici. Quest'anno la pubblicazione è offerta in allegato a questo articolo ed è composta da uno strumento di sensibilizzazione di massa ed uno strumento tecnico più approfondito. In particolare, anche ENISA conferma che durante la pandemia i criminali informatici hanno migliorato le loro capacità di attacco, prendendo di mira con maggiore efficienza le categorie a rischio. Il rapporto conferma che vi è ancora un lungo cammino da fare, per raggiungere un ambiente informatico più sicuro. In particolare, il lavoro a domicilio ha contribuito indubbiamente una diminuzione del livello di affidabilità delle difese in atto.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

Il documento è articolato in una serie di rapporti, che analizzano vari aspetti della sicurezza informatica. Le aree che presentano i rischi maggiori, e cui il rapporto dedica più spazio, riguardano la rete 5G, l'intelligenza artificiale e le auto intelligenti.

Di particolare interesse è l'elenco dei 15 rischi maggiori, che viene aggiornato ogni anno e che è approvato dai massimi specialisti del settore. Riporto di seguito l'elenco completo:

1. Web-based Attacks
2. Malware
3. Phishing
4. Web Application Attacks
5. SPAM
6. Distributed Denial of Service (DDoS)
7. Identity Theft
8. Data Breach
9. Insider Threat
10. Botnets
11. Physical Manipulation, Damage, Theft and Loss
12. Information Leakage

13. Ransomware
14. Cyber Espionage
15. Cryptojacking

Non ho tradotto ogni singola voce perché penso che i lettori comprendano forse meglio le espressioni originali anglosassoni, che sono certamente più diffuse nell'ambiente.

In particolare, il numero di siti Web on-line fraudolenti è aumentato in maniera straordinaria, sia imitando nomi ben noti, sia creando nuovi nomi. La frode più diffusa è quella di incassare l'importo della vendita e non consegnare la merce. L'esperienza della pandemia ha messo in evidenza come occorra migliorare l'affidabilità del commercio on-line. Sono anche cresciuti gli incidenti legati a estorsioni, spesso di origine sessuale, soprattutto perché i giovani sono assai più esposti a questo tipo di attacco.

Ancora una volta, il rapporto mette in evidenza come gli aspetti economici siano alla base della gran parte degli attacchi, mentre attacchi con risvolti politici o di altra natura sono assai meno significativi.

Il furto di credenziali, che successivamente vengono usate in modo fraudolente, è pure in continuo aumento. Inutile dire che il ransomware risulta sempre essere presente nel mondo della criminalità informatica, con costose conseguenze per molte organizzazioni europee. Anche il crescente uso di processi automatici di elaborazione porta all'aumento degli scenari, che possono essere attaccati da malviventi.

Faccio presente lettori che ho allegato il testo in inglese, che ritengo sia quello più facilmente comprensibile, ma ENISA mette a disposizione anche il testo in francese e tedesco.

Il poster allegato può essere affisso al muro dell'ufficio del responsabile informatico, per mantenere alta la guardia su questi critici tv.

Il rapporto (pdf)

Il poster (pdf)

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it