|  | CICLE:  Sistemes Microinformàtics i Xarxes | CURS:  2n SMX |
| --- | --- | --- |
| **Mòdul M4: Sistemes Operatius en Xarxa**  **UF4: Compartició de recursos i entorns heterogenis** | | DATA:  20-03-23 |

| Nom i Cognoms: Òscar Rodríguez | Nota: |
| --- | --- |

**"Predicciones sobre ciberseguridad para 2023"**

https://www.datacenterdynamics.com/es/noticias/predicciones-sobre-ciberseguridad-para-20 23/

***1. Quines són les principals tendències que l'article prediu quant a ciberseguretat l'any 2023?***

L'augment de l'ús de la intel·ligència artificial i l'aprenentatge automàtic per part dels ciberdelinqüents. També es preveu un augment dels atacs a dispositius IoT, l'increment dels atacs de phishing i la utilització de tecnologies emergents com blockchain per millorar la seguretat.

***2. Com s'espera que la intel·ligència artificial canviï el panorama de la ciberseguretat en el futur proper?***

S'espera que la IA canviï el panorama mitjançant la detecció més precisa i ràpida de vulnerabilitats de seguretat, la millora dels sistemes de detecció d'intrusos i l’identificació de patrons d'activitat maliciosa.

***3. Quina és la importància de la col·laboració i l’intercanvi d'informació entre organitzacions per prevenir ciberatacs?***

És molt important per prevenir ciberatacs, ja que permet als professionals de la ciberseguretat compartir coneixements i recursos per detectar i respondre més eficaçment als atacs.

***4. Per què s'espera que els atacs dirigits a dispositius IoT s'intensifiquin els propers anys?***

S'espera q s'intensifiquin els propers anys a causa de l’augment d'aquests dispositius connectats a Internet i la manca de mesures de seguretat adequades per part dels fabricants.

***5. Quin paper juga la privadesa de les dades a la ciberseguretat i com s'espera que evolucioni en el futur?***

És clau en la ciberseguretat, ja que els atacs cibernètics solen buscar accedir i explotar informació confidencial. En el futur, s’espera q es desenvolupin tecnologies que permetin als usuaris protegir millor les seves dades i controlar la seva privadesa.

***6. Quins són els riscos de les contrasenyes i com s'espera que n'evolucioni l'ús en la ciberseguretat?***

Els riscos de les contrasenyes inclouen l'ús de contrasenyes febles i la reutilització de contrasenyes en diferents llocs, el qual facilita als atacants accedir a múlticomptes si es produeix una violació de seguretat. En el futur, s'espera que les solucions de gestió de contrasenyes millorin i que s'utilitzi més l'autenticació multifactorial per reduir aquests riscos.

***7. Com s'espera que el ransomware evolucioni els propers anys i quines són les mesures que es poden prendre per prevenir-lo?***

Es preveu que evolucioni els propers anys cap a atacs més sofisticats i dirigits a empreses i organitzacions crítiques, així com l'ús de criptomonedes per extorsionar diners. Les mesures per prevenir el ransomware inclouen l'educació als usuaris per evitar el phishing i altres atacs, així com l’implementació de mesures de seguretat com ara la realització de còpies de seguretat regulars.

***8. Quines implicacions tindrà la introducció de criptomonedes per part dels ciberdelinqüents al món de la ciberseguretat?***

L'ús de criptomonedes per part dels ciberdelinqüents pot complicar la detecció i seguiment dels atacs, augmentar el nombre d'atacs de ransomware, mineria de criptomonedes malicioses i posar en perill la seguretat/privacitat de les dades dels usuaris.