

Kybernetické útoky – cíle a metody útočníků

Obsah

- 1 / Kybernetická rizika**
- 2 / Druhy rizik**
- 3 / Malware**
- 4 / Kybertest**

1 / Kybernetická rizika

Druhy kybernetických rizik je velmi důležité znát, abychom jim mohli předcházet. Tato forma útoku zahrnuje různé metody, mezi které patří útoky na online účty, phishing a distribuce malwaru.

2 / Druhy rizik

- Skimming
 - Zařízení, které během použití bankomatu získá informace o kartě uživatele.
- Phishing
 - Útočník vytváří falešné webové stránky, které napodobují legitimní instituce.
 - Cílem je nalákat oběti k poskytnutí svých citlivých údajů.
- Bruce force útoky
 - Útočníci provádějí opakované pokusy o uhodnutí PIN kódu kreditní karty.



2 / Malware

- Virus
 - Infikují soubory a šíří se po síti.
 - Může poškodit nebo smazat soubory, nebo je použit pro šíření dalšího malware.
- Červ
 - Mají schopnost se sami replikovat a šířit po síti.
 - Mohou způsobovat přetížení sítě a snižují výkon počítačů.

2 / Malware

- Spyware
 - Sleduje uživatele a shromažďuje jeho osobní údaje.
 - Tyto údaje mohou být použity k phishing útokům nebo k cílení reklamy.
- Adware
 - Zobrazuje reklamy bez souhlasu uživatele.
 - Může také shromažďovat osobní údaje uživatele.

2 / Malware

- Ransomware
 - Zablokuje přístup k počítači a požaduje výkupné.
 - To může být ve formě peněz, kryptoměny nebo poskytnutí citlivých informací.

|

KYBERTEST

3 / Kybertest

- kybertest.cz

Pracovní list 2