Kybernetické útoky

Kybernetický útok

- Prováděn pomocí počítače.

- Počítač slouží jako prostředek pro útok.
  Může ale sloužit i jako cíl útoku.

Typy útoků #1

1. **Únik informace** - vyzrazení informací neautorizovanému subjektu

2. **Narušení integrity** - poškození, změna, vymazání dat

3. **Potlačení služby** - úmyslné bránení v přístupu k informacím, aplikacím, či systému.

4. **Nelegitimní použití** - použití informací neautorizovaným subjektem či neoprávněným způsobem.

Typy útoků #2

- Malware
- Phishing
- (D)DoS
- Password Attack
- Internet of Things (IoT) Attacks
- Key logger
- Deepfakes

Malware

- Škodlivé aplikace nebo kódy, které poškozují zařízení koncových bodů nebo narušují jejich normální provoz.
- Když se zařízení infikuje malwarem, může dojít k neoprávněnému přístupu, ohrožení dat nebo zablokování zařízení, dokud nezaplatíte výkupné.
- Malware funguje tak, že pomocí triků znemožňuje normální provoz zařízení. Kyberzločinec získá přístup k vašemu zařízení prostřednictvím jedné nebo několika různých technik – phishingový e-mail, nakažený soubor, zneužití chyby v zabezpečení systému nebo softwaru, nakažený USB flash disk nebo škodlivý web.
- Útočník zneužije tuto situaci ke spouštění dalších útoků, získání přihlašovacích údajů k účtu, shromažďování osobních údajů ke zpeněžení, prodeji přístupu k výpočetním prostředkům nebo vylákání plateb od obětí.

Phishing

- Phishing je typ kybernetického útoku pomocí technik sociálního inženýrství, kdy se útočník snaží získat důvěrná data oběti nebo spustit na zařízení oběti škodlivý kód.
- Nejčastěji probíhá phishingový útok pomocí podvodného e-mailu s žádostí o informace k naší platební kartě nebo přihlašovací údaje do našeho internetového bankovnictví.
- Výjimkou ale není ani v chatovacích aplikacích a na sociálních sítích.

- https://www.eset.com/cz/phishing/

DoS – Denial of Service

- Typ útoku, který dokáže zahltit konkrétní informační kanál (web, IP adresy – servery, služby - porty pro FTP, …)
- Informační kanál se jeví jako nedostupný
- Posílá se velký počet požadavků na konkrétní port.
- Podtypem je **DDoS – Distributed Denial of Service**

Password Attack

- Snaží se zjistit heslo pro přístup k informacím.
- Existuje mnoho metod - nejjednodušší je tipování správného hesla.
- Tipování hesla využívá i metoda **brute-force –** skript systematický zkouší všechna možná hesla (A, AA, AAA, B, BB, AB, AAB, …)

Keylogger

- Keylogger (někdy také Keystroke Logger) je software, který snímá stisky jednotlivých kláves.
- Antivirem bývá považován za virus. V případě software se jedná o určitou formu spyware, ale existují i hardwarové keyloggery.
- Keylogger neohrožuje přímo počítač, ale slouží ke zjišťování hesel jiných lidí.
- Některé z nich bývají v operačním systému Microsoft Windows proti svému zničení chráněny pomocí Archivace a Skrytí souborů, takže je není možné pomocí Průzkumníku najít (je nutné použít vyhledávání).

https://www.eset.com/cz/keylogger/

Deepfakes

- Obecně můžeme za deepfakes označit realisticky upravené fotografie, videa nebo zvukové záznamy, které se tváří jako skutečné, že je téměř nemožné to poznat. Více informací a praktické ukázky najdete v článku.

- S masovým rozšiřováním umělé inteligence tak bohužel ještě roste význam "tradičních" metod ověřování informací, při kterých si můžeme pouze vypomoci různými nástroji typu deepware.ai. Hlavní práce ale zůstává na nás.
- Jedno je jisté: při ověřování bychom se měli zdržet rychlých soudů a zbrklého přejímání informací.

Ochrana

- Nepřistupovat k důležitým osobním datům na veřejných WIFI (banka, email, …)
- Pozorně sledujte, která oprávnění po vás weby a aplikace chtějí (GPS, kontakty, přístup k fotkám, …)
- Používejte dvoufázové ověřování tam, kde je to možné.
- Buďte skeptiční vůči odkazům a přílohám v mailech a chatu.
- Buď si jistý, že jsou tvá data v bezpečí, pokud ztratíš telefon.

Zdroje

- kybernetické_utoky.pdf (cesnet.cz)
- Hacker – Wikipedie (wikipedia.org)
- Kybernetický útok – Wikipedie (wikipedia.org)
- Hackerský útok – Wikipedie (wikipedia.org)
- Anonymous via twitter.com
- log4j – Wikipedie (wikipedia.org)
- Cracking – Wikipedie (wikipedia.org)
- (In)Famous Hacking Groups - United States Cybersecurity Magazine (uscybersecurity.net)