CSIRT-MU

Soňa Príborská

CSIRT: Bezpečnostní tým MU

- https://security.ics.muni.cz
- Computer Security Incident Response Team of Masaryk University
- řešení a detekce bezpečnostních incidentů v univerzitní počítačové síti
- osvěta uživatelů v oblasti PC bezpečnosti

Z cílů a kompetencí CSIRT:

- Asistence fakultám a lokálním správcům při zvyšování úrovně zabezpečení síťové infrastruktury MU
- Zvyšování povědomí o základních principech IT bezpečnosti mezi univerzitní veřejností

security.ics.muni.cz

- zvýšení povědomí v oblasti elementární IT bezpečnosti u studentů a zaměstnanců
- zvýšení odbornosti univerzitních správců IT systémů
- vývoj a použití nových metodik v oblasti vedení běžných uživatelů a zvyšování jejich gramotnosti v rámci IT bezpečnosti

V praxi:

- Sekce veřejnost, univerzita, správci
- Veřejnost bez přihlášení
- Univerzita, správci po přihlášení přes Poskytovatele identit MU (UČO+ sekundární heslo)

Veřejnost

- Postaveno na vyprávění "uživatelských" příběhů
- Hlavní postavou příběhů běžný uživatel pan Bohumil - "Bob"
- Témata: zejména phishing (6 příběhů), dále bezpečnost a síla hesel, malware

Veřejnost - phishing

- Články obsahují důkladně popsané různé metody a postupy phishingu
- Díky interaktivním prvkům má návštěvník webu možnost rozhodovat se o správném postupu v příběhu
- Vysvětlení průběhu a důsledků úspěšně provedeného phishingu
- Poučení na závěr - jak se v dané situaci správně zachovat

Veřejnost - hesla

- Bezpečnost a síla hesel - vysvětlení potřeby dobrého hesla, možné útoky na hesla, jak by (ne)mělo dobré heslo vypadat
- Doporučení pro tvorbu hesel
- Možnost ověřit sílu hesla ve vlastní aplikaci s následným rozborem

Veřejnost - malware

- opět příbeh s Bobem
- příklad konkrétního vyděračského malware
- rozbor případu, typické prvky
- poučení uživatele jak zareagovat

Sekce univerzita

- Pouze výklad směrnice rektora o správě a užívání počítačové sítě
- V r. 2011 pro osoby s aktivním účtem v IS akce “Phishing na vlastní kůži”

Phishing na vlastní kůži

- Uživatelé se mohli zúčastnit akce, kdy jim byly bez předchozího upozornění zasílány typicky phishingové zprávy
- ve skutečnosti samozřejmě ne nebezpečné
- Cílem vyzkoušet si, zda je uživatel dovede rozeznat a adekvátně (ne)reagovat

Phishing na vlastní kůži

- Vyhodnocení s celkovou statistikou, zhodnocením osobní úspěšnosti a vysvětlením daného případu + jak se zachovat
- Zúčastnilo se 263 osob

Sekce Správci

- Whitelist a blacklist IP adres v rozsahu sítě MU a mimo ni
- Doporučení pro zabezpečení - síťově dostupných zařízení, webových serverů

Zhodnocení zdroje:

- Ve veřejné sekci profesionální a podrobné informace z oblasti informační bezpečnosti
- Bohužel málo aktualizované - pouze několik příspěvků, mezi některými i roční rozestup
- Jako zdroj informací o phishingu velmi podrobný a užitečný, ostatní témata upozaděna
- Poslední příspěvek 17. 12. 2012