cesnet

TO NEJ Z AGENDY CESNET-CERTS

Daniel Studený
CESNET-CERTS

6. února 2024
Seminář o bezpečnosti sítí a služeb 2024

cesnet

...ANEB VESELÉ HISTORKY ZE ZPRACOVÁVÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

- **Testovací servery**
  - nikdo je neupgraduje, zapomenuté stále běží, ačkoliv měly být dávno vypnuté
- **Starý systém**
  - na novém by aplikace neběžela a nemá ji kdo přepsat
- **Externí firma**
  - systém spravuje někdo cizí a zcela nepružný v servisních zásazích
- **„Hloupá“ zařízení bez vlastní ochrany**
  - měla by být za firewallem, ale mají veřejnou IP adresu a otevřené služby
  - příklad skutečného následku: klimatizace provedla DoS útok

- **Nezkontrolovaná konfigurace**
  - po reinstalaci se nespustily orchestrační skripty nastavující zabezpečení
  - po změně konfigurace či výměně síťového prvku se nenastavila původní ACL
  - na IPv6 chyběla ACL, která byla na IPv4
  - po přepnutí na záložní linku chyběla ACL primární linky
- **Hlad**
  - správce spustil skript s **nmap**em a odešel na oběd; během něj skript provedl DoS
  - správce nainstaloval zařízení s tím, že ho dokonfiguruje po obědě, a než se vrátil, nakonfiguroval mu ho někdo jiný
- **Náruživý divák**
  - notebook používaný pro práci i zábavu měl nevypnutý Torrent a nabízel licencovaný obsah i po připojení do NREN

NAT A SÍTĚ PRO HOSTY

- **Incident v kolejní síti**
  - uživatele nelze vystopovat, chybí informace (flow, logy)
- **Odpojený hotel**
  - na konferenci hrál uživatel kybernetickou hru, způsobil incident vyhodnocený jako útok a odpojil tím celý hotel, který byl přes NAT za jedinou veřejnou adresou
- **Síť pro hosty**
  - do WiFi sítě se sdíleným heslem se připojil uživatel s malwarem, který otrávil keš od DNS proxy; ta pak uživatele směrovala na phishingovou stránku

Nevinné ťukání

- správce si (prý nevinně) hrál s **knockd** a způsobil incident
- správce testoval schopnosti **nmap**u, ty se mu však vymkly z rukou
- student hádal SSH hesla, prý to ale bylo v rámci diplomové práce, takže jsme vlastně narazili na falešné pozitivum ;-)
- správce se z domova periodicky hlásil na pracovní stanici SSHčkem a odsud zpětně skenem ověřoval zabezpečení domácího routeru
- student z cizí koleje přes eduroam zkoušel připojení na výukový server své školy, který byl pro přístup z venku uzavřen; dohledáním své identity a vysvětlením incidentu zaměstnal pět lidí
- CS:GO server běžící v Dockeru a komunikující s privátními adresami „utekl“ mimo univerzitu díky chybějícímu firewallu a způsobil incident

Malware na nečekaném místě

- na jednu naši univerzitu přišel phishingový mail, správci mu podhodili identitu z honeypotu
- přihlásil se jim nakažený stroj z jiné naší univerzity

IGNORACE

- **Neohlášené PEN testy**
  - teď budeme testovat a nikomu to neřekneme
- **Nefunkční abuse@**
  - je nám líto, nepřijímáme
  - přijímáme, ale kdo to má čas číst
  - bereme na vědomí, možná i vyřešíme, ale bavit se s vámi fakt nebudeme
- **Špatná vnitřní komunikace a dokumentace**
  - zranitelné či útočící zařízení má neznámého správce
  - když je nalezen, nemůže najít, kde je ono zařízení fyzicky umístěné
  - proces od nahlášení do vyřešení trvá často měsíc i déle

CO ZLEPŠIT?

- **Abuse kontakty**
  - mějte funkční
  - čtěte poštu
  - kontrolujte i spam
- **Zranitelnosti**
  - neberte na lehkou váhu
  - řešte preventivně
  - čtěte CSIRT-FORUM
  - dokumentujte síť, nastavte si pravidla součinnosti s dalšími správci

CO ZLEPŠIT?

- **Síť**
  - vyzkoušejte si nestandardní situace
  - nechte se otestovat
    - PEN testy vždy hlaste dopředu
  - dělejte si inventury serverů, likvidujte včas „šrot“
  - nezapomeňte na zařízení, která nelze zabezpečit přímo (kamery, klimatizace, tiskárny, aj.)
  - i po IPv6 může přijít útok
  - NAT zajistěte sběrem flow či logováním, ještě lépe zrušte a nahraďte IPv6

- **Od rozdělané konfigurace a spuštěných skenů neodcházejte**
  - na oběd
  - domů
  - na dovolenou
  - do penze
  - na věčnost

cesnet

DĚKUJI ZA POZORNOST!