ACTIVE24-CSIRT

Ing. Tomáš Hála
ACTIVE 24, s.r.o.
www.active24.cz

ACTIVE24

- doménový registrátor
- webhosting
- email hosting
- serverová řešení
- člen projektu Fénix

ACTIVE24-CSIRT

- http://www.active24.cz/csirt/

- první oficiálně konstituovaný CSIRT tým z komerční sféry v ČR

- u Trusted Introducer registrován 9.2.2012 – status Listed

- navázal přímou spolupráci s ostatními týmy v ČR i po celém světě

Co tento tým řeší

- reakce na hlášené incidenty

Co tento tým řeší

- reakce na hlášené incidenty

- proaktivní vyhledávání incidentů

- analýza incidentů a bezpečnostní audity

- interní vývoj a implementace preventivních opatření

- edukace, školení – interní i externí

- sdílení informací a zkušeností s ostatními týmy, spolupráce

- účast na cvičeních kybernetické bezpečnosti

Stručná statistika

- cca 2000 hlášení/rok (často jeden incident nahlášen vícekrát resp. z různých zdrojů)

- zabýváme se každým přijatým podnětem!

- na základě těchto podnětů realizujeme cca 500 zásahů ročně

- převážně spam/phishing/malware, pokusy o neautorizované přístupy

- ale také DoS, DDoS, řídící centra botnetů, napadání web aplikací i závažnou trestnou činnost (hospodářská, dětská pornografie aj.)

- spotřeba cca 15% MD's technického oddělení

Příklady incidentů

- DoS březen 2013

Příklady incidentů

- DoS březen 2013, 2014, 2015..

Příklady incidentů

- DoS březen 2013, 2014, 2015..

- phishing na náš vlastní webmail

- BGP IP highjack z Ruské federace

- Drupal SQL Injection

- bruteforceing CMS administrace

- napadení stránek velvyslanectví

- ...

Některá opatření/projekty, které implementujeme

Projekt Fénix

- reakce na útoky z března 2013

- platforma sdružující důvěryhodné operátory

- plnění přísných technických i organizačních kritérií

- spolupráce, rychlé sdílení relevantních informací

- bezpečná VLAN

Poloautomatické řešení běžných incidentů

- sledování stížností

- admin jen ověří, že je stížnost oprávněná

- další akce se již dějí automaticky podle šablony:

  - vynucení opatření / blokace dílčí služby
  - oznámení zákazníkovi
  - odkaz na podrobné informace k dalšímu postupu
  - vyrozumění CSD
  - zalogování

Proaktivní vyhledávání malwaru v obsahu webů

- ClamAV, maldet, vlastní signatury

- deaktivace přidáním suffixu

- automatické oznámení zákazníkovi

Aplikace patche na zákaznické weby

- Drupal SQLi - závažná bezpečnostní chyba v oblíbeném CMS
- aplikace patche na zákaznické weby (rychlost)
- zásah do prezentace – kontroverzní
- pilotní případ
- žádné negativní reakce, naopak řada pozitivních
- úspora incidentů a tedy i času/práce/prostředků

Omezení přístupu na FTP

- pam_exec + GEOIP detekce

- default jen CZ/SK

- možnost volby vlastních zemí / IP / rozsahů

Proaktivní vyhledávání slabých hesel

- řeší se v prvé řadě pro SMTP službu

- po opakovaném oznámení vynucení změny hesla

- validační pravidla pro sílu hesla

- řeší se způsob oznamování zákazníkům pokusy o prolomení

Informace z GovCERT

- Botnet Feed - pravidelná data, zdrojem je MS

- po vyfiltrování zjevných false positives jsou data relevantní

- informace i o provozu, který neopustil naši sít!

(D)DoS

- projekt Fénix (BCP-38 aj.)
- levné útoky generovat, drahé se jim bránit
- předpřipravené konfigurace
- zavedené postupy
- kvalitní dokumentace
- rozšířený monitoring
- cvičení (CE2012,2014, CC2013 – NATO, CC2014 - GovCERT)
- simulace (testování HW spolu s CZ.NIC)
- komunikace s CSIRT.CZ, zákazníkem, médii
- nginx / ACL / FW dle typu packetů / RTBH
- scrubbing center?

Odkazy

- ACTIVE 24:
  www.active24.cz

- ACTIVE24-CSIRT:
  www.active24.cz/csirt

- Projekt Fénix:
  fe.nix.cz

- twitter.com/active24cz
  twitter.com/tomashala

Otázky?