ACTIVE24-CSIRT - řešení bezpečnostních incidentů v praxi

Ing. Tomáš Hála

ACTIVE 24, s.r.o.

www.active24.cz

CSIRT/CERT

- Computer Security Incident Response Team resp.
  Computer Emergency Response Team

- hierarchický koncept bezpečnostních týmů, které spolupracují při řešení bezpečnostních incidentů na síti

- obvykle jsou to týmy v rámci společností jako ISP, poskytovatelé obsahu, banky, univerzity apod. a nad nimi týmy národní

- národní týmy fungují ve většině civilizovaných zemí světa, ale jsou různě organizovány resp. spadají pod různé instituce
  (last resort, koordinace a případně i vynucení reakce)

Co tyto týmy řeší?

- v prvé řadě všechny nahlášené bezpečnostní incidenty

- spolupráce, výměna informací a zkušeností s ostatními týmy

- koordinace postupu v případě rozsáhlých útoků

- vlastní proaktivní sledování citlivých míst, hlášení incidentů pocházejících z jiných sítí a nasazování preventivních opatření

- případně i osvěta (např. mezi svými zákazníky nebo pro veřejnost)

Jak takový tým založit?

- určit rozsah zodpovědností

- určit funkční a přímé kontaktní údaje (a udržovat je aktuální!)

- uvést pracovní dobu týmu

- vygenerovat PGP klíč

- vše zveřejnit na stránkách

- vyplnit formulář u Trusted Introducer

- zajistit si podporu minimálně dvou akreditovaných týmů

Jaká je situace v ČR

- CSIRT.CZ - Národní CSIRT tým České republiky

- ACTIVE24-CSIRT - bezpečnostní tým společnosti ACTIVE24, s.r.o.

- CZ.NIC-CSIRT - bezpečností tým pro dohled nad sítí provozovanou sdružením CZ.NIC

- CESNET-CERTS - bezpečnostní tým pro dohled nad sítí národního výzkumu a vzdělávání, kterou provozuje CESNET

- CSIRT-MU - bezpečnostní tým Masarykovy univerzity v Brně

ACTIVE24-CSIRT

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

- první oficiálně registrovaný CSIRT tým z komerční sféry v ČR

- u Trusted Introducer registrován 9.2.2012 – status Listed

- bez registrace fungoval již řadu let přes abuse@active24.cz

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

ACTIVE24-CSIRT

- cca 1200 hlášení/rok (často jeden incident nahlášen vícekrát resp. z různých zdrojů)

- zabýváme se každým přijatým podnětem!

- na základě těchto podnětů realizujeme cca 120 zásahů ročně

- řešíme převážně spam/phishing/malware případně copyright

- ale také DoS, DDoS, řídící centra botnetů, napadání web aplikací i závažnou trestnou činnost včetně šíření dětské pornografie

ACTIVE24-CSIRT – jak postupujeme

U rutinních případů jako spam/phishing/malware:

- odstranění závadného obsahu

- dohledání zneužitého slabého místa (php script/odcizené heslo apod.)

- nastavení protiopatření (selektivní vypnutí php, změna hesla apod.) (prevence – karanténa/SMTP kvóta/GeoIP FTP autentizace apod.)

- vyrozumění zákazníka spolu s informacemi, jak dále postupovat a žádostí o sjednání nápravy (upgrade CMS, nasazení captcha, hromadnou korespondenci upravit dle platné legislativy apod.)

- princip 2x a dost (přichází ke slovu VOP)

ACTIVE24-CSIRT – příklady nedávných incidentů

- předvánoční DDoS – RC modely

- napadení stránek syrského velvyslanectví

- hrozby od Anonymous

- řídící centra botnetu

Vyplatí se ustavení CSIRT týmu?

- získáte přístup k cenným informacím a kontaktům

- řešení incidentů se vyplácí, protože zabráníte jejich opakování, a tak zásadním způsobem snížíte jejich negativní dopady

- získané zkušenosti výrazně pomohou zvýšit zabezpečení vaší sítě

- sami nepochybně uvítáte, že budete mít s kým řešit incidenty, které přicházejí z venčí do vaší sítě

Vyplatí se ustavení CSIRT týmu?

- dáváte světu najevo vaši ochotu se bezpečnostními incidenty zabývat

- podpoříte tím seriózност vaší organizace, zvyšujete si kredibilitu

- pomůžete vybudovat funkční infrastrukturu bezpečnostních týmů v ČR (je potřeba mít na paměti, jaká je alternativa..)

- ustavení týmu je jednoduché a nic nestojí

Užitečné odkazy

- Národní CSIRT tým České republiky: WWW.CSIRT.CZ (provozuje CZ.NIC)

- Registrace nového týmu: http://www.trusted-introducer.nl/ti_process/list.html

- Celosvětový seznam registrovaných týmů: https://www.trusted-introducer.org/teams/country_LICSA.html

- Sdružení TERENA a evropské fórum TF-CSIRT: www.terena.org a www.terena.org/activities/tf-csirt/

- FIRST - světové fórum týmů CSIRT: www.first.org

Prostor pro Vaše dotazy