Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

INFORMACINIS BIULETENIS
APSAUGA NUO PASLAUGŲ TRIKDYMO KIBERNETINIŲ ATAKŲ (ANGL. DDoS)

2021 m. lapkričio 5 d.
Vilnius

Siekiant užtikrinti įstaigos teikiamų ir naudojamų paslaugų (internetinės svetainės, el. pašto, administracinio tinklo interneto ryšiui ir kt.) pasiekiamumą, veiklos tęstinumą, turėtų būti įgyvendinti organizaciniai ir techniniai kibernetinio saugumo reikalavimai, taip pat kitos gerosios praktinės kibernetinio bei informacijos saugumo praktikos.[1] NKSC teikia esmines kibernetinio saugumo rekomendacijas organizacijoms apsaugai nuo paskirstytų paslaugos trikdymo atakų (toliau – DDoS).

1. Siekiant valdyti DDoS kibernetinių incidentų rizikas, pvz., organizacijų paslaugų nepasiekiamumą, svarbu iš anksto identifikuoti svarbiausius alternatyvius komunikacijos kanalus: el. paštas, organizacijos socialinių tinklų paskyros, atsarginiai interneto ryšio kanalai. Sudarant sutartis su trečiosiomis šalimis dėl veiklos tęstinumo mechanizmu svarbu įtraukti nuostatą dėl kibernetinių incidentų įrodymų (angl. *forensic data*) išsaugojimo.
2. Užtikrinkite, kad visų tinklo įrenginių aparatinė ir programinė įranga, serverių programinė įranga, aplikacijų platformos, būtų savalaikiai atnaujinamos siekiant išvengti techninių pažeidžiamumų, dėl kurių sėkmingai DDoS atakai įvykdyti užtektų mažiau resursų.
3. Įvertinkite galimybę naudoti dedikuotų debesų kompiuterijos paslaugas, suteikiančias kelių lygių saugumą. Dedikuotų debesų kompiuterijos paslaugų (pvz., *Cloudflare, Apptrana, Imperva*) naudojimas leidžia vienu metu aktyvuoti kelių lygių saugumo sprendimus, t. y. apsisaugoti nuo *HTTP DDoS* atakų (*HTTP floods*, *amplification HTTP*, *reflection HTTP* ir pan.), *SSL/TLS DDoS* atakų (*SSL exhaustion flood, SLL negotiation* ir pan.), tinklo lygio DDoS atakų (*ACK floods*, *SYN-ACK aplification*, *UDP*, *ICMP* atakų iš žinomų *botnetų*, pvz., Mirai).
4. Tinklo perimetre naudokite ugniasienes su giliojo paketų tikrinimo (angl. *deep packet inspection*, DPI) arba tiksliąja tinklo srauto analizės funkcija (angl. *accurate network traffic analysis*)[2];

4.1. Apsvarstykite galimybę blokuoti UDP paketus, kurių dydis viršija 468 bitus ir kurie atkeliauja iš prievadų (angl. *ports*), naudojamų stiprinimo atakoms vykdyti (pvz. 1-1023, 1194, 1434, 1900, 3074, 3283, 3702, 5683, 11211, 17185, 20800, 27015, 30718, 33848, 37810, 47808). Turėkite omenyje, kad paketų dydžio ribojimas gali daryti įtaką tinklo funkcionavimui;

4.2. Siekiant sustabdyti DDoS atakas, reikalingos automatinės tinklo priemonės, galinčios išanalizuoti tinklo srautą, siekiant surasti įtartiną veiklą – aptikti ataką ir užblokuoti atakos šaltinio IP adresą.

5. Rinkitės interneto, debesų kompiuterijos, svetainių prieglobos paslaugas, kurių teikėjas suteikia apsaugą nuo DDoS atakų, draudžia *IP spoofing* atakas.
6. Apribokite atvirus prievadus (DDoS atakos šaltinius) DNS, NTP, SNMP, SSDP (UPnP), *Memcached* arba apribokite prieigą prie jų, išjunkite ICMP atsaką.

[1] https://www.nksc.lt/doc/NKSC%20plakatas%20(20cc)_1.pdf
[2] https://owasp.org/www-project-dpd/

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

7. DDoS atakos įvykdymui gali būti pasitelktos paslaugos, veikiančios atvirais prievadais (prieiga prie jų nėra apribojama), taip fiktyviai padidinant duomenų srautą serviso atsakos metu, pvz., DNS serviso atsakymas ~50 kartų didesnis nei užklausa, NTP -~58 kartus, *Memcached* - ~10 000 kartų ir t.t. Atsako srautą nukreipus į atakuojamą objektą, išnaudojami jo infrastruktūros resursai fiktyvioms sesijoms sudaryti ir palaikyti, taip neleidžiama teisėtiems vartotojams pasiekti servisų.

8. Resursų paskirstymas padidina slenkstį (angl. *threshold*), kurį reikia įveikti sėkmingai DDoS atakai. Interneto ir el. pašto svetainių architektūroje:

8.1 *Anycast* tinklo resursų naudojimas:

- Turinio pristatymo tinklai (angl. CDN) paskirsto interneto, el. pašto svetainei tenkantį srautą įvairiose vietose esantiems serveriams, taip subalansuojant šį srautą, neapkraunant pagrindinio interneto svetainės pateiktį vykdančio serverio resursų;
- *Anycast* domenų vardų sistema (angl. DNS). *Anycast* paskirsto DDOS atakos srautą skirtą DNS keliems duomenų centrams, neleidžiant vienai lokacijai būti perpildytai užklausomis. Jei *Anycast* tinklo pajėgumas yra didesnis, nei atakos srautas, ataka veiksmingai užkardinama.

8.2 HTTP konversijai į HTTPS naudokite HSTS (sąlyga – ištekliai pasiekiami HTTPS):

- Įprastai HTTP konversija į HTTPS vykdoma pagrindinio interneto, el. pašto svetainės pateiktį vykdančio serverio žiniatinklio serviso pagalba (t. y. kai žiniatinklio servisas gauna HTTP užklausą, siunčia HTTP 301/302/303/307/308 atsakymą klientui ir peradresuoja HTTP į HTTPS, tam panaudojami ir apkraunami serverio resursai);
- HSTS (RFC6797) – mechanizmas, padedantis apsaugoti interneto ir el. pašto svetaines nuo MITM (angl. *Man in the Middle*) atakos, panaudojant protokolo žeminimo ataką (angl. *protocol downgrade attack*) ir slapukų pagrobimą (angl. *cookie hijacking*). Žiniatinklio serveriai deklaruodami, kad žiniatinklio naršyklės (arba kitos vartotojo priemonės[3]) turėtų naudoti tik HTTPS ryšius, kurie užtikrina transporto sluoksnio saugumą (TLS). Šis apsaugos mechanizmas įjungiamas, kai vartotojas apsilankė interneto ar el. pašto svetainėje bent kartą, tuomet kitus kartus (nuo pirmo karto nepraėjus daugiau kaip vieneriems metams, t.y. rekomenduojama 'Strict-Transport-Security: max-age=31536000' atraštė[4]), vartotojui naršyklėje įvedus HTTP, automatiškai atnaujinama į HTTPS naršyklės pagalba, nepateikiant HTTP užklausos, nenaudojant, neapkraunant serverio resursų.

8.3 HTTPS funkciją perkelkite į dedikuotą aparatinę įrangą:

- HTTPS šifruoto ryšio kanalo sudarymo funkciją perkelkite į tinklo įrenginį (pvz., ugniasienę), kurio dedikuota aparatinė įranga gali vienu metu palaikyti daugiau šifruoto ryšio kanalo sudarymo užklausų, nei turimas interneto, el. pašto svetainės pateiktį vykdantis serveris.

8.4 naudokite atvirkštinę įgaliotąją stotį (angl. *reverse proxy*):

- Atvirkštinis tarpinis serveris iš vieno ar daugiau serverių surenka užklausoje prašomą informaciją ir ją pateikia paslėpdamas tikruosius išteklius (IP adresus, naudojamas žiniatinklio serviso versijas, apsunkina galimybę identifikuoti techninius pažeidžiamumus ir kt.), taip pat sudaroma galimybė aktyvuoti apsaugos mechanizmus (pvz., ModSecurity WAF) su iš anksto aprašytomis taisyklėmis, kurių pažeidimai traktuojami kaip įsilaužimas ir vykdomas blokavimas.

8.5 HTTPS peradresavimas apkrovos balansavimui (angl. *HTTPS redirect for load balancing*):

- Paskirsčius užklausas tenkančias interneto, el. pašto svetainėms tarp serverių telkinio (angl. *pool*) elementų, minimizuojant įprastai vienam elementui tenkančią apkrovą.

8.6 Padidinkite interneto greitaveiką (administraciniam ir tarnybinių stočių tinklui):

- Didesnio pralaidumo interneto kanalas nėra vienintelis sprendimas apsaugai nuo DDoS, bet tai pakelia kartelę, kurią užpuolikai turi įveikti, kad galėtų įvykdyti sėkmingą DDoS ataką.

[3] https://caniuse.com/stricttransportsecurity
[4] https://hstspreload.org