VPS drošības kontrolsaraksts

Sākuma pārbaude kontrolētai piekļuvei, mazākai ekspozīcijai un atjaunošanai

1 Kontrolēta piekļuve

- [ ] Fiksēt un pārbaudīt pakalpojuma sniedzēja konsoli vai atjaunošanas piekļuvi.
- [ ] Izveidot vārdā nosauktus administratorus un ikdienā neizmantot root.
- [ ] Pārbaudīt SSH publiskās atslēgas no otras sesijas.
- [ ] Ierobežot administratīvās tiesības un aizsargāt privātās atslēgas.
- [ ] Sinhronizēt laiku un dokumentēt īpašnieku, mērķi, OS un atbalsta periodu.

2 Atjaunināšana un publiski pieejamo pakalpojumu samazināšana

- [ ] Uzstādīt atbalstītos OS un pakotņu atjauninājumus.
- [ ] Iestatīt automātiskos drošības atjauninājumus un restartēšanas kārtību.
- [ ] Apkopot portus un servisus un dzēst nevajadzīgos.
- [ ] Izmantot ienākošā ugunsmūra noklusējuma aizliegumu ar skaidriem izņēmumiem.
- [ ] Datubāzes un iekšējos servisus nepiesaistīt publiskām adresēm bez vajadzības.

3 Lietotņu un datu aizsardzība

- [ ] Publiskai tīmekļa datplūsmai izmantot aktuālu TLS.
- [ ] Noslēpumus neglabāt publiskās mapēs, repozitorijos vai komandu vēsturē.
- [ ] Servisus darbināt ar atsevišķiem nepriviliģētiem lietotājiem.
- [ ] Veidot ārpus servera glabātas kopijas un pārbaudīt atjaunošanu.
- [ ] Dokumentēt atkarības, sertifikātus, DNS, darbus un atjaunošanas secību.

4 Uzraudzība un uzturēšana

- [ ] Apkopot autentifikācijas, ugunsmūra, sistēmas un lietotņu žurnālus.
- [ ] Uzraudzīt pieejamību, resursus, sertifikātus, kopijas un pieteikšanos.
- [ ] Regulāri pārskatīt kontus, atslēgas, ugunsmūri, pakotnes un portus.
- [ ] Sagatavot incidenta kontaktus un izolēšanas veidu.
- [ ] Atkārtot pārbaudi pēc būtiskām lietotnes, tīkla vai piekļuves izmaiņām.

Primārie avoti

Tīmekļa versijā ir aktuālās saites un papildu skaidrojumi.

1 Ubuntu Server documentation: Firewalls
https://documentation.ubuntu.com/server/how-to/security/firewalls/

2 Ubuntu Server documentation: OpenSSH server
https://documentation.ubuntu.com/server/how-to/security/openssh-server/

3 Ubuntu Server documentation: Automatic updates
https://documentation.ubuntu.com/server/how-to/software/automatic-updates/

4 CISA: Cybersecurity Performance Goals
https://www.cisa.gov/resources-tools/resources/cybersecurity-performance-goals