



Haavatavad e-pood on ründajatele ahvatlevateks sihtmärkideks

Olukord

Möödunud aasta oktoobris tuvastas CERT-EE mõnisada e-poodi, mis olid haavatavad ühe konkreetse turvanõrkuse vastu. Kõik e-pood kasutasid aegunud versiooni Magento platvormist. CERT-EE saatis toona e-poodidele välja teavitused, et nad tarkvara uuendaksid. Olukord on tänaseks küll paranenud, kuid aegunud Magento tarkvara kasutavaid e-poode on Eestis jätkuvalt vähemalt ligi **sadakond**.

Sellised e-pood on ründajatele aga ahvatlevateks sihtmärkideks, sest nende kaudu on häkkeritel võimalik varastada näiteks e-poe klientide andmeid (sh pangakaartide andmeid) või teha muid pahaloomulisi tegevusi. Ohu reaalsust ilmestab tõsiasi, et hiljuti saime teada ühest mõjuga küberintsidendist, mis sellesse kategooriasse langeb.

Turvanõrkustega e-poodidest kirjutasime ka RIA 2023. aasta [aastaraamatus](#). Ründajad kuritarvitavad paljuski eelmisel aastal avaldatud haavatavusi, et e-poode kompromiteerida. Kui e-poele on ligipääs saadud, üritatakse sageli varastada selle klientide või teiste inimeste pangakaartide andmeid. Selleks paigaldatakse veebipoele vastav pahavara või lisatakse õngitsusleht, mille kaudu potentsiaalsetele ohvritelt andmed kokku korjatakse.

Kuna Eestis on endiselt suur hulk haavatavaid e-poode, mis kasutavad aegunud Magento tarkvara, jagab RIA järgnevalt Magento platvormi haldajatele soovitusi, kuidas enda e-poode paremini küberrünnakute eest kaitsta. Nende järgimine tuleb kasuks ka teiste e-poodide platvormide halduritele.

RIA soovitused Magento platvormi kasutajatele:

- Uuendage tarkvara (sh laiendusi) regulaarselt. Kõige värskemad Magento tarkvaraversioonid avaldati 22.05.2023 seisuga 14. märtsil (2.4.6, 2.4.5-p2 ja 2.4.4-p3). Ülevaate erinevatest Magento versioonidest ja nende avaldamiskuupäevadest leiate [siit](#).
- Veenduge, et teie e-poeiga seotud kontaktandmed oleks Eesti Interneti SA registris ajakohased. Nii jõuavad CERT-EE hoiatused kindlasti teieni. Rohkem infot leiate Eesti Interneti SA [kodulehelt](#).
- Piirake e-poe halduspaneelile ligipääs vajaduspõhiselt. Täpsemalt saate selle kohta lugeda [siit](#).
- Rakendage e-poe halduskontodele kaheastmeline autentimine. Õpetuse selle rakendamiseks leiate [siit](#).
- Võimalusel kasutage veebirakenduse tule müüri (WAF). See aitab kaitsta veebirakendusi, filtreerides ja jälgides HTTP-liiklust veebirakenduse ja Interneti vahel.
- Varundage regulaarselt veebiserveri ja andmebaasi sisu välisesse asukohta. Toimiva varukoopia abil on teil võimalik küberintsidendi (nt pahavara paigaldamise puhul) korral kiiremini veebiteenuse töö taastada.
- Testige enda veebilehti regulaarselt (eelisjärjekorras automaatsete tööriistadega), et neil poleks lihtsalt tuvastatavaid turvanõrkuseid.

¹ 1 KüTS'i paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.



Kui soovid olla kursis Eesti küberruumis toimuvaga, jälgi RIA [kuukokkuvõtteid](#), [kvartaliülevaateid](#) ja [blogi](#).

Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond koostöös CERT-EE-ga.