Riigi Infosüsteemi Amet

Küberturvalisus – kellele ja milleks?

Eesnimi Perenimi

15/10/2018

Millest räägime?

- Kübermaailma eripärad
- Mõju ning kriitilised teenused
- Trendid ja intsidentide liigid
- Näited ja soovitused

Kübermaailma eripärad

- Igapäevaelu sõltuvus IT-süsteemidest
- Haavatavus ja laiaulatuslik mõju
- Anonüümsus, väiksem ohutaju, kuna puuduvad käega katsutavad esemed (sh vestluspartner)
- Kurjategijaid on keerulisem tuvastada
- Õhuke spetsialistide ring

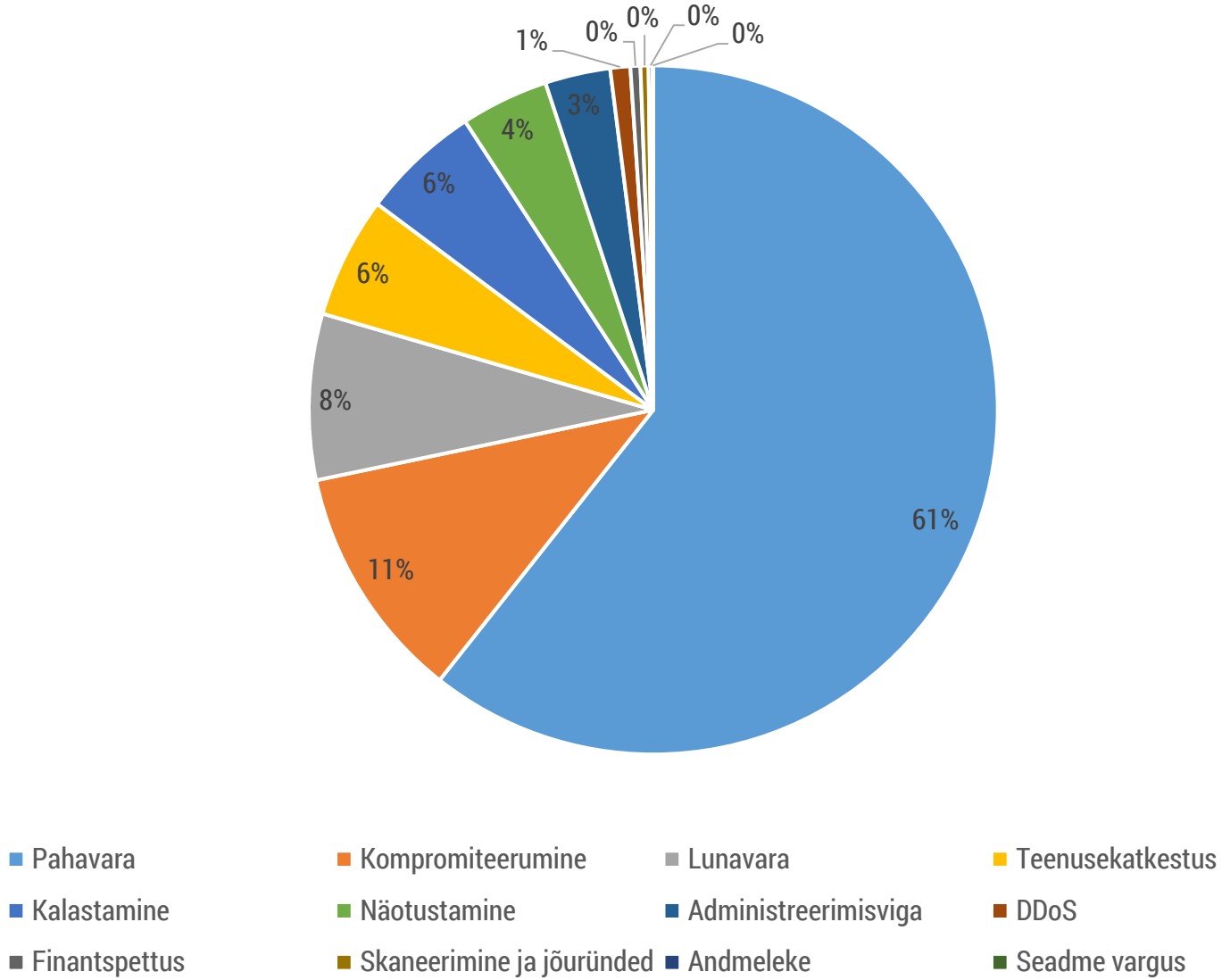
Sihtmärgid ning kriitilised teenused

- Meditsiin
- Energeetika
- Lennundus
- Finantssektor
- Telekommunikatsioon
- Riigiasutused

2017: RIA küberintsidentide lahendamise osakonna (CERT-EE) registreeritud juhtumid

- ~11 000 juhtumit – kolmandiku võrra rohkem kui 2016. aastal
- 3162 küberintsidenti, millest 122 olid kõrge prioriteediga ehk mõjutasid olulisi teenuseid
- 2500 küberrünnakut (pahatahtlik tegevus)
- 32 intsidenti raviasutustes, neist 10 juhul seiskus arstide või pereõdede töö

Intsidentide liigid



Pahavara – mõjutab ettevõtteid ja tavakasutajat

Eesmärk on kahjustada kasutaja seadet:

- andmete krüpteerimiseks ja raha välja pressimiseks
- info varastamiseks
- krüptoraha kaevandamiseks
- seadme liitmiseks robotvõrgustikuga

Levib e-kirjaga, nakatunud veebilehe või mälupulga jm välise seadme kaudu


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

FOTOD | Rahvusvahelise küberrünnaku tõttu on kõik Ehituse ABC poed suletud (131)

| Lisatud RIA kommentaar

Rivo Veski
Kasulik.ee peatoimetaja

Reet Pärgma
reporter

Foto: Argo Ingver

Ulatuslik rahvusvaheline küberrünnak, mis sai alguse nädala algul, on jõudnud otsapidi ka Eestisse: Ehituse ABC kõik poed on täna suletud, kuni küberrünnakust häiritud süsteemid taas tööle saadakse.

Perearstikeskus maksis lunaraha

25. aprill 2018 12:15

Riigi Infosüsteemi Amet avalikustas oma aastaraamatus, et möödunud aastal langes kaks Eesti perearstikeskust küberruumis esitatud lunavaranõude ohvriks.

.

Foto: commons.wikimedia.org

«Mõlemal juhul kasutati nakatamiseks kaugligipääsu perearstikeskuse infosüsteemile, mille kaudu paigaldatud lunavara krüpteeris patsientide terviseandmeid sisaldavad failid. Esimesel juhul arvati esiotsa olevat tegu serveriveaga. Tõde selgus paar päeva hiljem, kui pea 4000 krüpteeritud faili avamise

Krüpto-lunavara võttis FEB ehitusketi maha, poed üle Eesti on suletud

Täiendatud 16:00: lisatud RIA värske kommentaar

Hans Lõugas ja Marii Karell
23.08.2018 kell 10:33

FEBi kauplus Tallinnas Forelli tänaval. Foto: Siim Männik

Kaheksa FEB sanitaartehnikaketi kauplust üle Eesti on suletud, ettevõtte töö halvas lunavara.

Soovitused

- Uuenda seadmeid ja kasuta alati kõige uuemat ning ametlikelt lehtedelt alla laaditud tarkvara ja viirusetõrjet
- Ära ava tundmatuid kirju, linke ja manuseid (kahtluse korral küsi saatjalt üle!)
- Tee arvutis või muudes süsteemides olevatest andmetest regulaarselt varukoopiaid ja hoia neid eraldi süsteemides (sh eraldi võrgus)

- Küsi süsteemide hooldamiseks tuge professionaalidelt, osta vajadusel teenus sisse
- Ära maksa nõutud raha – see motiveerib kurjategijaid küsima rohkem ja otsima uusi ohvreid. Lunaraha maksmine ei garanteeri andmete muutmata kujul tagasi saamist
- Kui oled langenud ohvriks, küsi nõu: cert@cert.ee

Õngitsuslehed ja -kirjad

Eesmärk on varastada kasutaja isiklikke andmeid, sh finantsinfot ja kontoga seotud andmeid:

- kontode ülevõtmiseks
- finantspettuste tegemiseks
- uute õngitsuskirjade levitamiseks
- raha väljapressimiseks

Rõhk visuaalsel sarnasusel – kasutatakse tuntud ettevõtete logosid, isikute nimesid jms

Tegevjuhi petuskeem

- Üks levinumaid õngitsuskirju, mis on suunatud ettevõtete finantsjuhtidele
- Kasutatakse juhi nime ning sarnast meiliaadressi
- RIA-le teadaolevalt on 2018. aasta jooksul makstud petukirjade tõttu kümneid libaarveid
- Summad on ulatunud 5000 kuni 45 000 euroni

From: Taimar Peterkop <mingi_suvaline@domeen.com>
Reply to: mingiabsurdne@aadress.xyz
Date: 2018-03-22 9:23 GMT+02:00
Subject: Tasumata makse
To Tiia Uibooss

Kas me saame saata 9305,20 EUR täna?

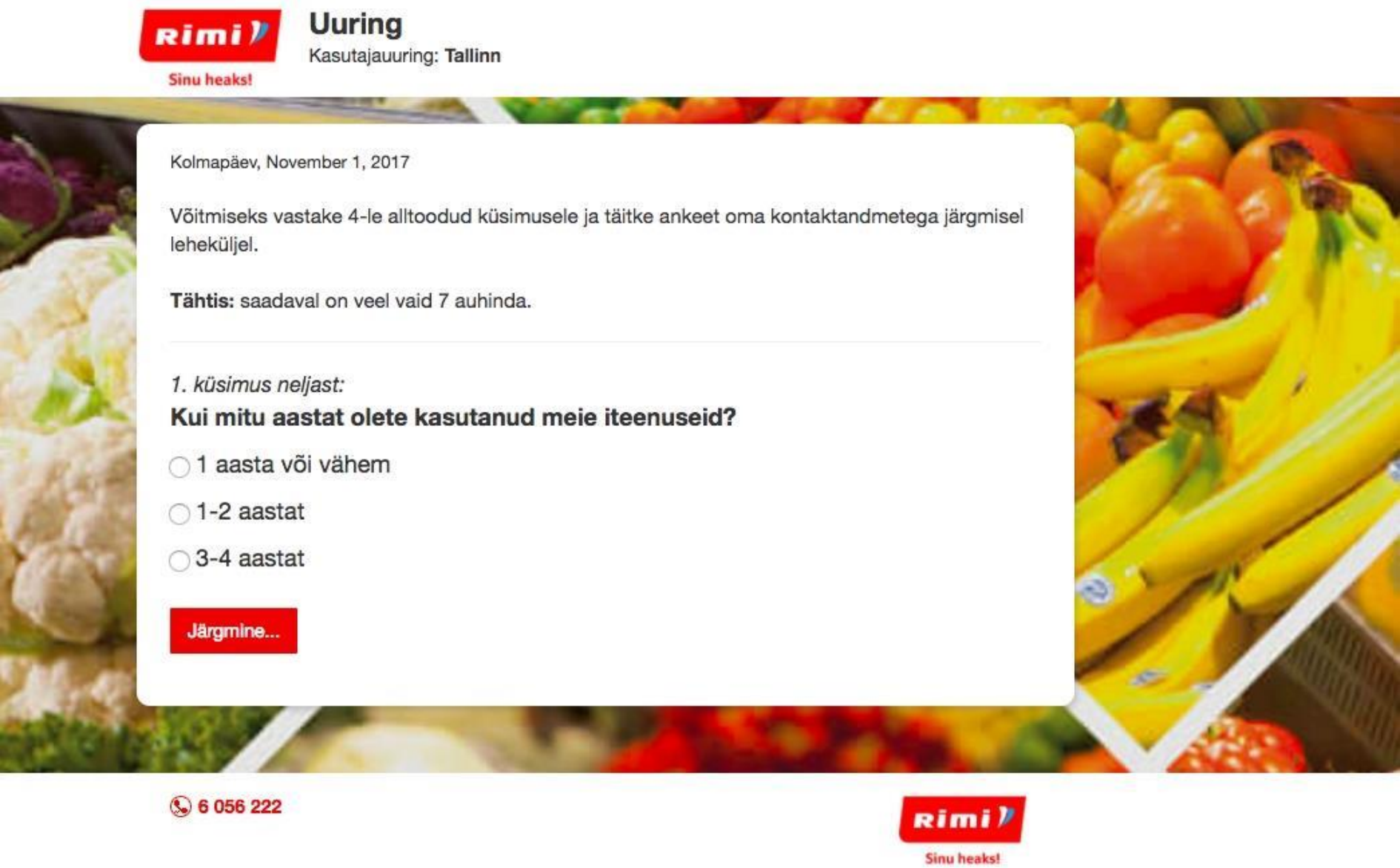
Kokku tasumata summa : 9305,20 Euro

Pangarekvisiidid:
Mingi Bank
kasusaaja : Miss A Nnao Ma Raha
IBAN : (riigikood)1234567890111213149876543210 1234
Kiirkood : S11n0NK00d
Saaja aadress : Puu 1, Oks 2, Mets, Riigis, 12345
transfeer tüüp: kiirmakse
viitekood : (Number)

Saada kinnitus makse Millal lõpetatud

Tervitades
Taimar Peterkop

Sotisaalmeedias levivad libaloosimised



Soovitused

- Veendu veebiaadressi õigsuses
- Vigane kirjaviis on ohumärk
- Enne tegutsemist kontrolli saatja infot, helista saatjale kinnituse saamiseks üle!
- Ära jaga enda paroole ja kasutajainfot

Paroolid ja kontod

- Eelista e-teenustes ID-kaarti, Smart- või M-ID-d
- Kasuta erinevates keskkondades erinevaid turvalisi paroole
- Kasuta kaheastmelist autentimist
- Ära jaga paroole ega kontoga seotud infot
- Kasuta paroolihaldurit, mis aitab iga veebilehe jaoks genereerida unikaalse parooli (nt LastPass ja 1Password)

Hea ja turvaline parool

- Võiks olla umbes 15 tähemärki pikk, sisaldada suuri ja väikeseid tähti, numbreid ja sümboleid
- Jääb kasutajale hästi meelde, kuid on võõrale keeruline ära arvata. Näiteks:
- K4ss1l,On!N3l1.J4lg4
- L3hm4d!On,L41gul1s3d

Halvad paroolide või salasõnade valikud

- Lühem kui 10 tähemärki
- Enda või pereliikme nime ja/või sünnikuupäeva sisaldav
- Levinumad sõnad või numbrijada. Näiteks:
- 12345
- Parool
- Marimaasikas123 jne

Halb paroolivalik

Need 20 ebaturvalist parooli on olnud laialt kasutuses just eestlase seas!

1. 123456	2. parool
3. qwerty	4. 123456789
5. lammas	6. 12345
7. minaise	8. maasikas
9. kallis	10. killer
11. armastus	12. lollakas
13. samsung	14. 123123
15. teretere	16. lilleke
17. martin	18. 12345678
19. kiisuke	20. kallike

Eestlaste sotsiaalmeedia paroolid murti lahti

Facebook
Foto: Veiko Tõkman

Äripäev
15. detsember 2017

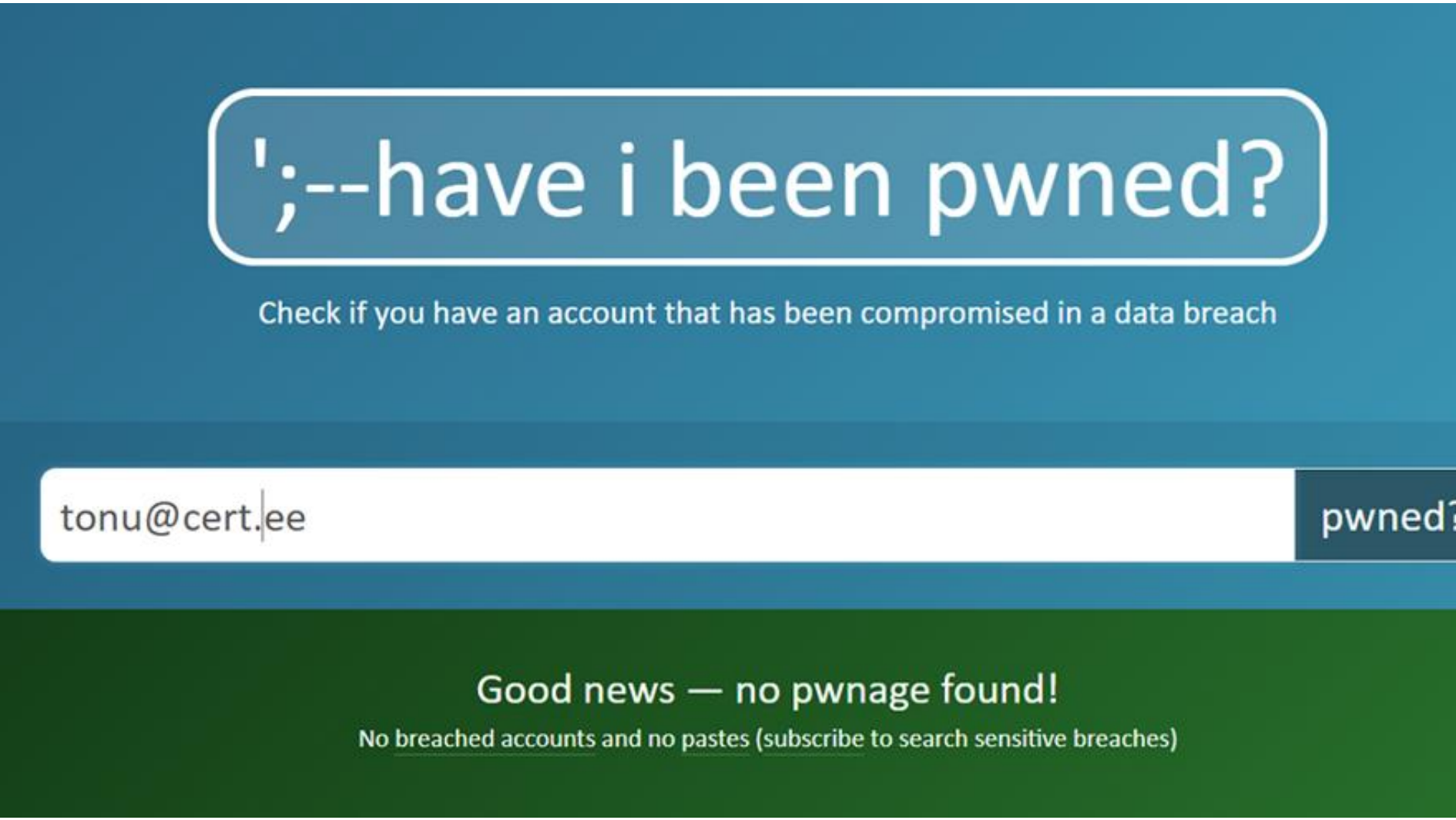
UUDISED

Riigi infosüsteemi ameti intsidentide lahendamise osakond (CERT) teavitas ligi 200 000 eestimaalast nende tööandja kaudu sotsiaalmeedia konto paroolide lekkimisest.

CERTi juht Klaid Mägi ütles ERRile, et kui varem oli teada, et paroolid lekkisid räsidena ehk krüpteeritud kujul, siis kolmapäeval sai riigi infosüsteemide amet teada, et paroolid on ka n-ö lahti murtud.

"Info, et paroolid on lekkinud, laekus aasta või poolteist tagasi ja toona teavitasime kõiki asutusi, et paroolide räsid on lekkinud ja peame valmis olema, et keegi paha inimene arvutab räsid lahti ja saab teada päris paroolid. Kutsusime üles kõiki inimesi, et minge muutke oma paroolid ära," meenutas Klaid.

Kas sinu parool on kunagi lekkinud?



Kokkuvõtteks

- Sõltuvus IT-süsteemidest eeldab teadlikku ja turvalist käitumist
- IT areneb kiiresti. Tänane turvaline lahendus vajab juba homme parandamist
- Süsteemidesse, teadlikkuse tõstmisse ja IT-personali tuleb investeerida
- Kontakt: cert@cert.ee; cybercrime@politsei.ee

Riigi Infosüsteemi Amet

Tänan!