Praktiskā sociālā inženierija

Agris Krusts, SIA IT Centrs

Kas ir sociālā inženierija?

Sociālā inženierija

Tradicionāla definīcija

Manipulēšana ar cilvēku, lai tas izpaustu klasificētu informāciju vai veiktu kādas noteiktas, uzbrucējam vēlamas darbības

Kā tā izpaužas mūsu darbā

Darbības, kurās mēs iesaistam klienta darbiniekus pašiem to nezinot

Ko pārbauda sociālās inženierijas testos

Darbinieku zināšanas IS drošībā

Vienkāršākais no testiem

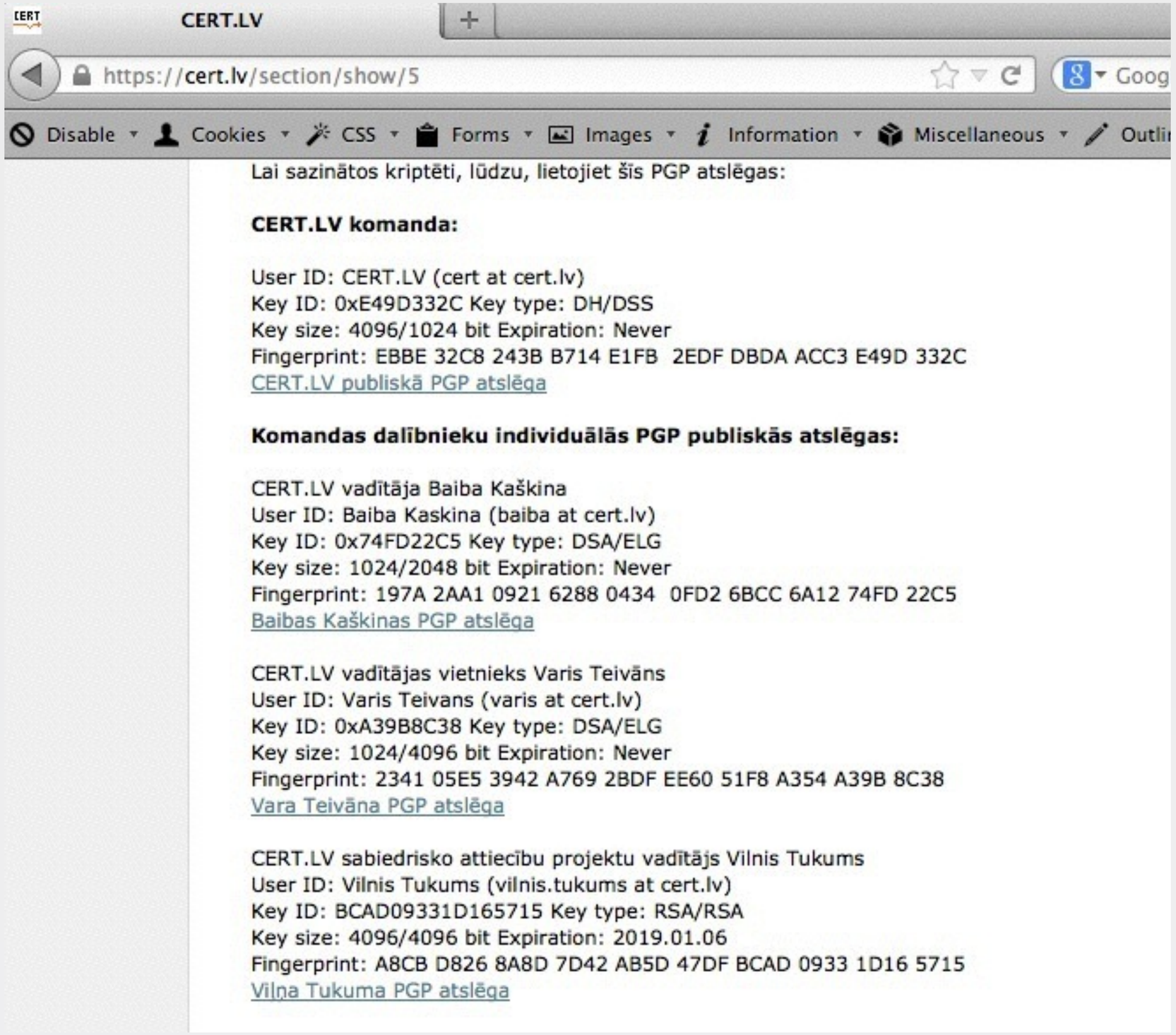
Parasti izsūta vēstules un apkopo statistiku par to ko darbinieki darījuši

Apvienot ar apmācību par IS drošību

Rezultāti atkarīgi no darbinieku zināšanām un testētāju pieredzes un ieguldītā darba

IS perimetra aizsardzība

- Sākotnējā izpēte
  - Kam sūtīt, no kā sūtīt, ko sūtīt
  - Mājaslapa, Google, LinkedIn, Facebook (Graph Search), Uzņēmumu reģistrs
  - Kādi antivīrusi tiek izmantoti, kāda ir tīkla arhitektūra
- Uzbrukums
  - Visbiežāk tiek sūtīti e-pasti
  - Var tikt izmantotas arī citas metodes


CERT.LV
https://cert.lv/section/show/5
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Lai sazinātos kriptēti, lūdzu, lietojiet šīs PGP atslēgas:
CERT.LV komanda:
User ID: CERT.LV (cert at cert.lv)
Key ID: 0xE49D332C Key type: DH/DSS
Key size: 4096/1024 bit Expiration: Never
Fingerprint: EBBE 32C8 243B B714 E1FB 2EDF DBDA ACC3 E49D 332C
CERT.LV publiskā PGP atslēga
Komandas dalībnieku individuālās PGP publiskās atslēgas:
CERT.LV vadītāja Baiba Kaškina
User ID: Baiba Kaskina (baiba at cert.lv)
Key ID: 0x74FD22C5 Key type: DSA/ELG
Key size: 1024/2048 bit Expiration: Never
Fingerprint: 197A 2AA1 0921 6288 0434 0FD2 6BCC 6A12 74FD 22C5
Baibas Kaškinas PGP atslēga
CERT.LV vadītājas vietnieks Varis Teivāns
User ID: Varis Teivans (varis at cert.lv)
Key ID: 0xA39B8C38 Key type: DSA/ELG
Key size: 1024/4096 bit Expiration: Never
Fingerprint: 2341 05E5 3942 A769 2BDF EE60 51F8 A354 A39B 8C38
Vara Teivāna PGP atslēga
CERT.LV sabiedrisko attiecību projektu vadītājs Vilnis Tukums
User ID: Vilnis Tukums (vilnis.tukums at cert.lv)
Key ID: BCAD09331D165715 Key type: RSA/RSA
Key size: 4096/4096 bit Expiration: 2019.01.06
Fingerprint: A8CB D826 8A8D 7D42 AB5D 47DF BCAD 0933 1D16 5715
Viļņa Tukuma PGP atslēga

Ko var uzzināt

Lielākajai daļai ir Facebook un LinkedIn profili, kur var redzēt intereses, ceļojumus utt:

ceļošana, foto, mūzika, auto, 4x4 u.c.

CERT.LV amatpersonas ir tikušas ārā no VID publiskojamās DB

Gandrīz visiem ir vēsture un bildes atrodama meklētājos

Atrodas vienā ēkā ar MII un Sigmanet bez atsevišķas apsardzes

Ko var uzzināt

Darbinieki cert.lv epastiem izmanto ārējās sistēmas, piemēram gmail.com:

- iespējams pārsūta cert.lv e-pastus uz privātiem e-pasta kontiem

E-pasta serveris izmanto ClamAV pretvīrusu programmatūru

Darbā izmanto Windows datorus

- daži ir paveci ar iespējams novecojušu programmatūru

Internetu nodrošina Sigmanet

```
Received: from rubenis.sigmanet.lv (rubenis.si
        by mx.google.com with ESMTP id be6si81
        for <agris.krusts@gmail.com>;
        Tue, 18 Mar 2014 05:30:05 -0700 (PDT)
Received-SPF: neutral (google.com: 92.240.66.6
Received: from localhost (localhost [127.0.0.1
        by rubenis.sigmanet.lv (Postfix) with
        for <agris.krusts@gmail.com>; Tue, 18
X-Virus-Scanned: Debian amavisd-new at rubenis
Received: from rubenis.sigmanet.lv ([127.0.0.1
        by localhost (rubenis.sigmanet.lv [127
        with ESMTP id cEGwHt4kljsy for <agris.
        Tue, 18 Mar 2014 14:30:02 +0200 (EET)
Received: from rubenis.sigmanet.lv (localhost
        by rubenis.sigmanet.lv (Postfix) with
        for <agris.krusts@gmail.com>; Tue, 18
Received: from [127.0.0.1] (unknown [85.254.19
        by rubenis.sigmanet.lv (Postfix) with
        for <agris.krusts@gmail.com>; Tue, 18
Message-ID: <53283BF8.5030802@cert.lv>
Date: Tue, 18 Mar 2014 14:28:40 +0200
From: [redacted]cert.lv
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:24
MIME-Version: 1.0
To: agris.krusts@gmail.com
Subject: =?UTF-8?B?U2VtaW7EgXJzIEVzaSBkcm/FoXM
X-Enigmail-Version: 1.6
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-AV-Checked: ClamAV
```

Ko var darīt?

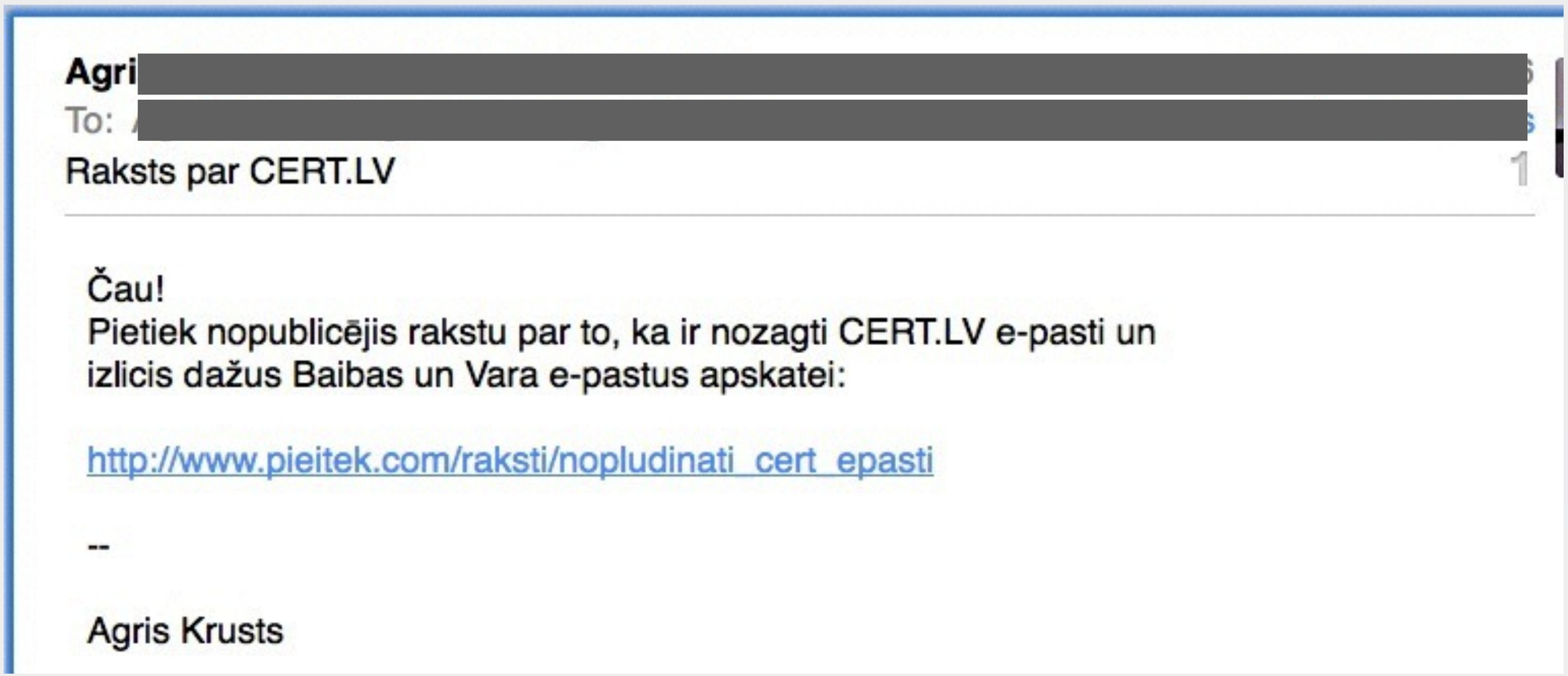
Maza organizācija - grūti izlikties par kolēģi

Iespējams veca un neatbalstīta programmatūra uz darbstacijām

Nav striktas robežas starp privāto un darba e-pastu

Iespējams uzbrukumiem var izmantot MII vai Sigmanet tīklu

E-pasta piemērs

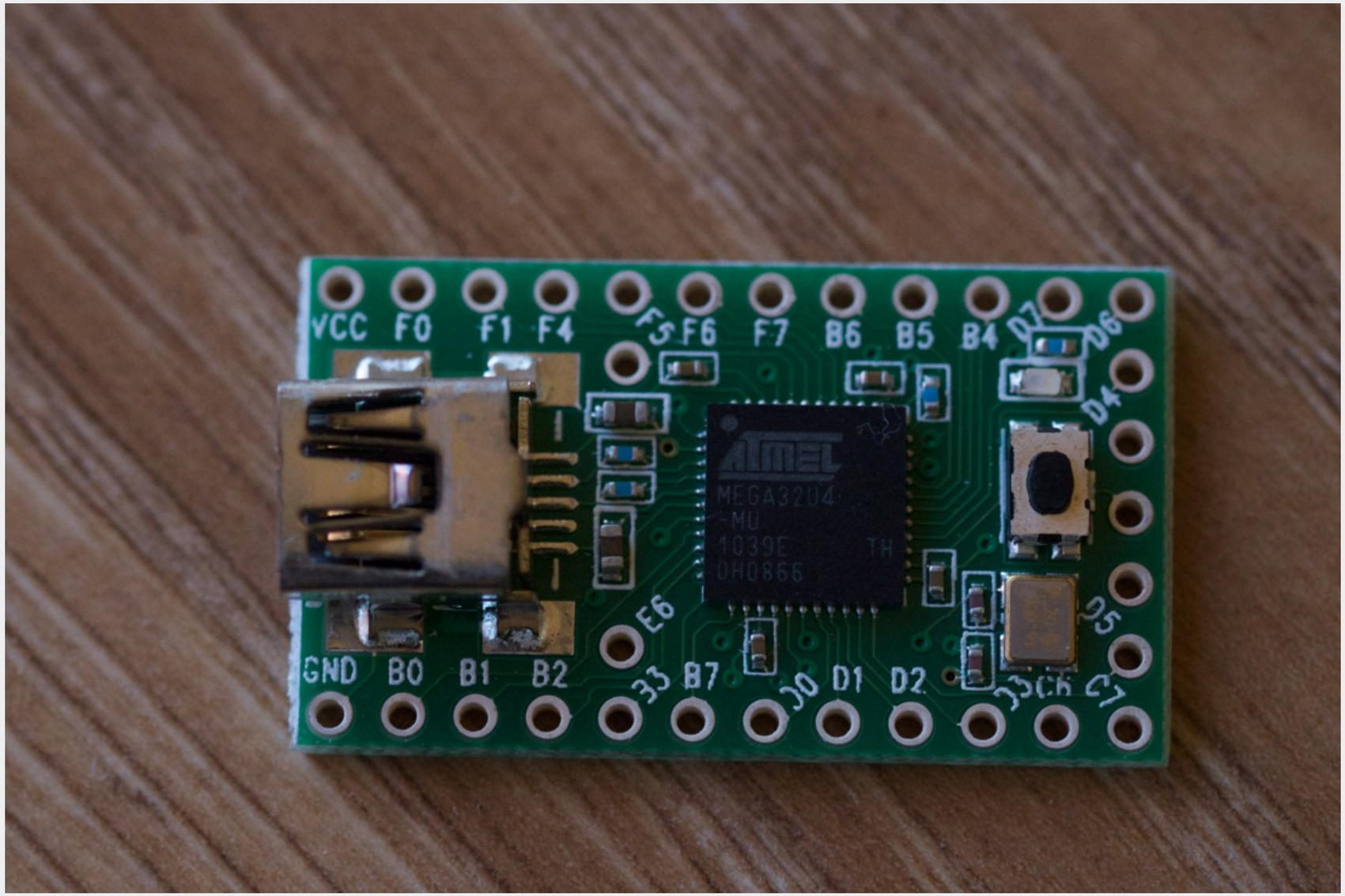


Tālrunis un IS palīdzības dienests

Ir maz lielu uzņēmumu, kur palīdzības dienestā strādā daudz darbinieku

Lietotāji ir pietiekami aizdomīgi un parasti šādi uzbrukumi tiek pamanīti vai nu uzreiz vai dažu stundu laikā

Ja nestrādā saites e-pastā



Para

B

File Edit View Bookmarks Settings Help

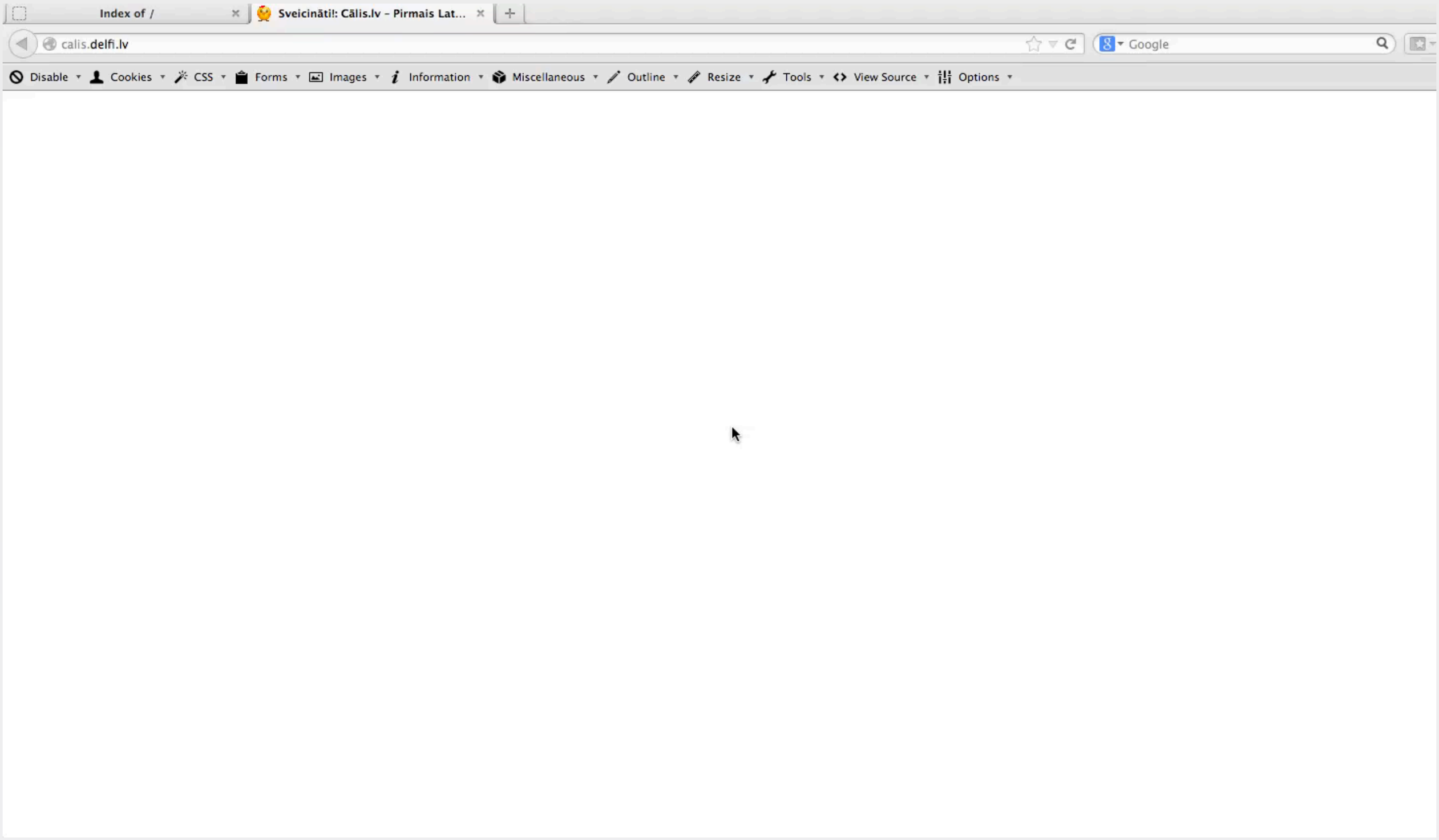
set : bash

File Edit View Bookmarks Settings Help

```
root@bt:~/ak/set#
```

Ne vienmēr vajag ļaunatūtru

Ja sociālās inženierijas uzbrukumu apvienu ar citām ievainojamībām, tad, piemēram, var pietikt uz brīdi lietotāju aizsūtīt uz kādu lapu


Index of /
Sveicināti!: Cālis.lv – Pirmais Lat...
calis.delfi.lv
Google
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options

Kur beidzas IS drošība un sākas fiziskā?

IS un fiziskā drošība

Jautājumi kurus mēģinam noskaidrot šādos testos

Vai varam iekļūt uzņēmuma telpās, serveru telpā, rezerves kopiju glabātuvē utt?

Vai varam pieslēgt savas iekārtas datortīklam?

Vai varam „iznest” informāciju?

Ne vienmēr tīklam jāpieslēdz dators

Pietiek uzdāvināt klaviatūru vai USB kafijas sildītāju

Informācijas ievākšana

Mājaslapa, Google, LinkedIn, Facebook, Uzņēmumu reģistrs

Kāda piekļuves sistēma tiek izmantota, vai var izgatavot atslēgu kopijas?

Kāds ir durvju kods?

Ja ir sargs, kāda ir iekļūšanas procedūra - vai to var apiet?

Kur atrodas tīkla pieslēgumi un informācija

Kam zvanīt, ja noķer apsardze

u.c.

Metodes kas noder

„Pretextinng”:

IS daļas inženieris no Rīgas risināt problēmu (var pašu radītu)

Lattelecom inženieris instalēt maršrutētāju tīkla problēmu risināšanai

Identifikācijas kartes attēli

Ienākšana telpās no rīta kopā ar visiem darbieniekiem

u.c.

Kādas ir tipiskākās problēmas klientiem?

- Informācijas sistēmas bieži ir vāji aizsrgātas pret uzbrukumiem ar sociālās inženierijas metodēm
- Tradicionāliem drošībniekiem bieži ir slikta izpratne par tehnoloģijām
- Darbinieki netiek apmācīti kā rīkoties aizdomīgās situācijās

Sociālā inženierija un pop-kultūra

Kevin Mitnick „Art of Deception”

TV šovi: The Mentalist, Tiger Team, Lie to Me

Paldies par uzmanību!

Agris Krusts

E-pasts: agris.krusts@itcentrs.lv

Skype: ak_t41

Twitter: @agris_krusts

www.itcentrs.lv