Pārdomas par sociālās inženierijas riskiem

Agris Krusts

Agris Krusts, IT drošības konsultants

Ikdienas darbs: sistēmu drošības testēšana

- www.itcentrs.lv
- e-pasts: Agris.Krusts@itcentrs.lv
- Twitter: @agris_krusts
- Linked-in: http://lv.linkedin.com/in/agriskrusts

Kas ir “Sociālā inženierija”

Tradicionāla definīcija

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

Daudz informācijas ir pieejams popkultūtrā:

- Kevin Mitnick „Art of Deception”
- Soacial Engineering: The Art of Human Hacking, Christopher Hadnagy
- TV šovi: Tiger Team, Lie to Me, Mr. Robot

Ikdienas piemēri


Jūsu datora faili ir nošifrēti ar CTB-Locker.
Jūsu datora faili ir nošifrēti ar CTB-Locker.
Jūsu dokumenti, bildes, datubāzes un citi svarigi faili tika nošifrēti ar neuzlaužamu šifrēšanas algoritmu un atslēgu ģenerētu šim datoram.
Privātā atslēga failu atšifrēšanai ir noglabāta slēptā interneta serveri un nevienam nav iespējas atšifrēt jūsu failus tikmēr, kamēr jūs nesamaksāsiet prasito summu lai saņemtu privāto atslēgu.
Jums ir tikai 96 stundas laika, lai nosūtītu maksājumu. Ja jūs nevelcat maksājumu norāditajā laika, visi jūsu faili paliks neatgriezeniski nošifrēti un neviens nevarēs tos atšifrēt.
Nospiežat 'Apskatīt' lai apskatitu sarakstu ar failiem kas tika nošifrēti.
Nospiežat 'Turpināt' lai turpinātu uz nākošo lapu.
UZMANĪBU! NEMĒGINIET IZDZĒST PROGRAMMU PAŠI. JEBKĀDAS DARBĪBAS LAI DZĒSTU PROGRAMMU IZRAISĪS ATŠIFRĒŠANAS ATSLĒGAS IZNĪCINĀŠANU. JŪS NEATGRIEZENISKI PAZAUDĒSIET SAVUS FAILUS. VIENĪGAIS VEIDS, KĀ SAGLABĀT SAVUS FAILUS IR SEKOT INSTRUKCIJĀM.
Apskatīt
95:59:21
Turpināt >>

FBI recommends paying ransom for infected computer

TECH

The FBI says you may need to pay up if hackers infect your computer with ransomware

Tess Danielson 13h 5,096 4

CERT.LV valsts iestāžu darbinieku apmācība

To [redacted]

From CERT Informācija <info@cret.lv> Cc Bcc

CERT.LV valsts iestāžu darbinieku apmācība

Labdien!

Saistībā ar Latvijas prezidentūru Eiropas Savienības Padomē tiek veikta vasts iestāžu darbinieku apmācība informācijas drošības jomā.

Sarežģītu un tajā pašā laikā viegli iegaumējamu paroļu izvēlēšanās ir viens no informācijas drošības pamatprincipiem. CERT.LV ir izstrādājis rekomendācijas drošu paroļu veidošanā, kuras tiek rekomendēts ņemt vērā veidojot lietotāju paroles valsts informāciju sistēmu resursos:
http://www.cret.lv/paroles/301

Ar cieņu,
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

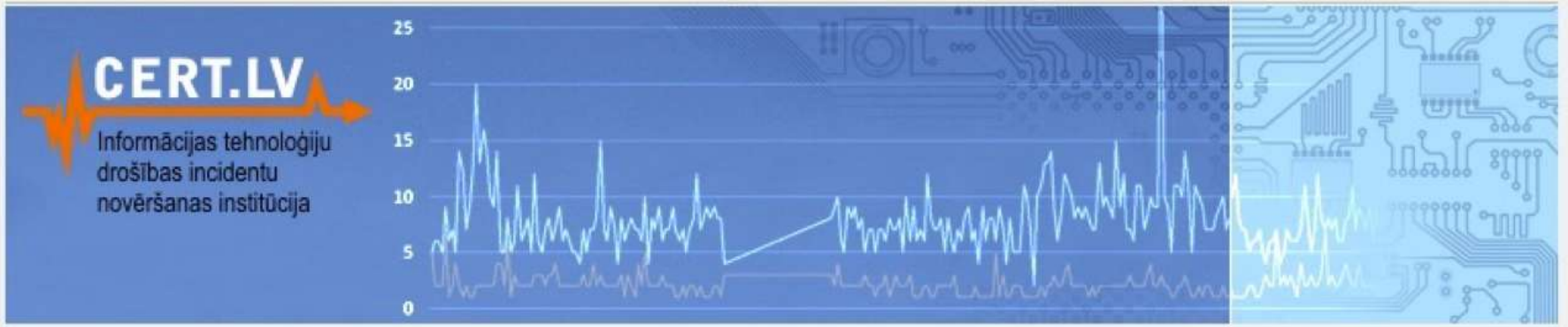
2014-10-28 9:23 GMT+02:00 [redacted]
> Labdien!
>
> Kā jau vienojāmies, pielikumā nosūtu sarakstu ar darbinieku epasta adresēm. Lūdzu, informējiet
> par rezultātiem.
>
> Ar cieņu,
> [redacted]
> Datorsistēmu un datortīklu administrators
> Tel. 67078412
>
> 2014-10-28 9:19 GMT+02:00 CERT.LV <info@cert.lv>:
> > Labdien!

Sans Serif | B I U A | sts iestāžu darbinieku apmācība informācijas drošības jomā. Lūdzam atsūtīt

Send

CERT.LV - Paroļu pārbaude

www.cret.lv/paroles/1



Bezmaksas paroļu stiprības pārbaudes rīks

Lietotāja vārds

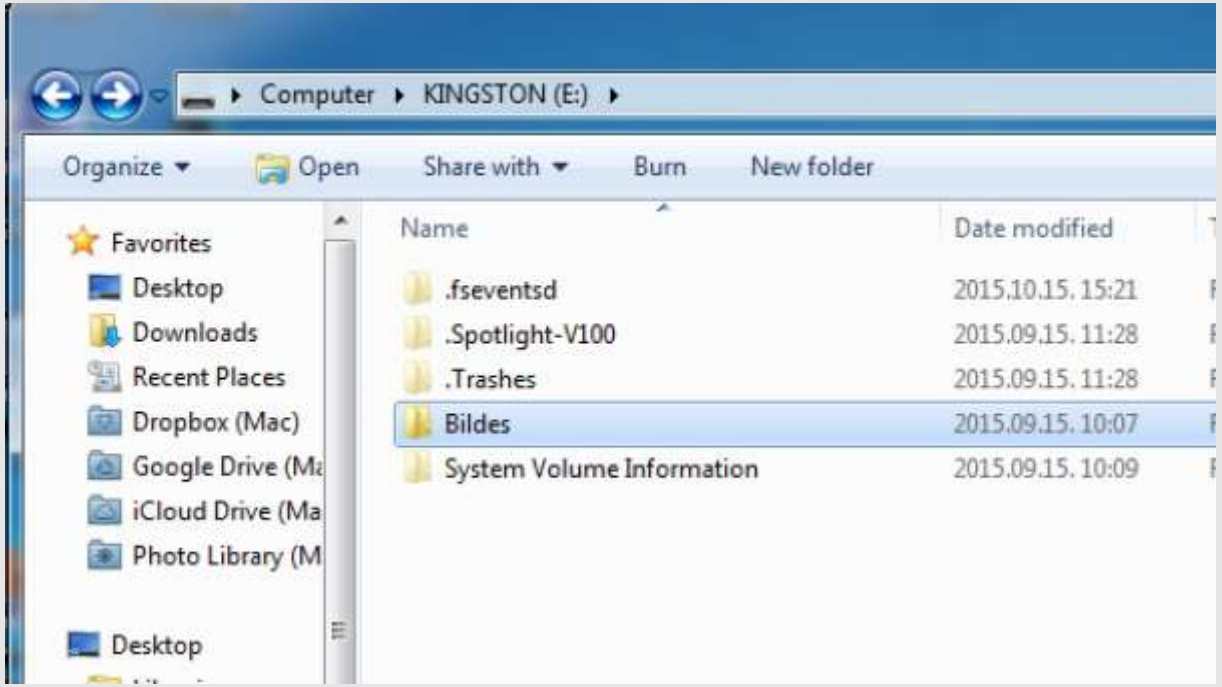
Parole

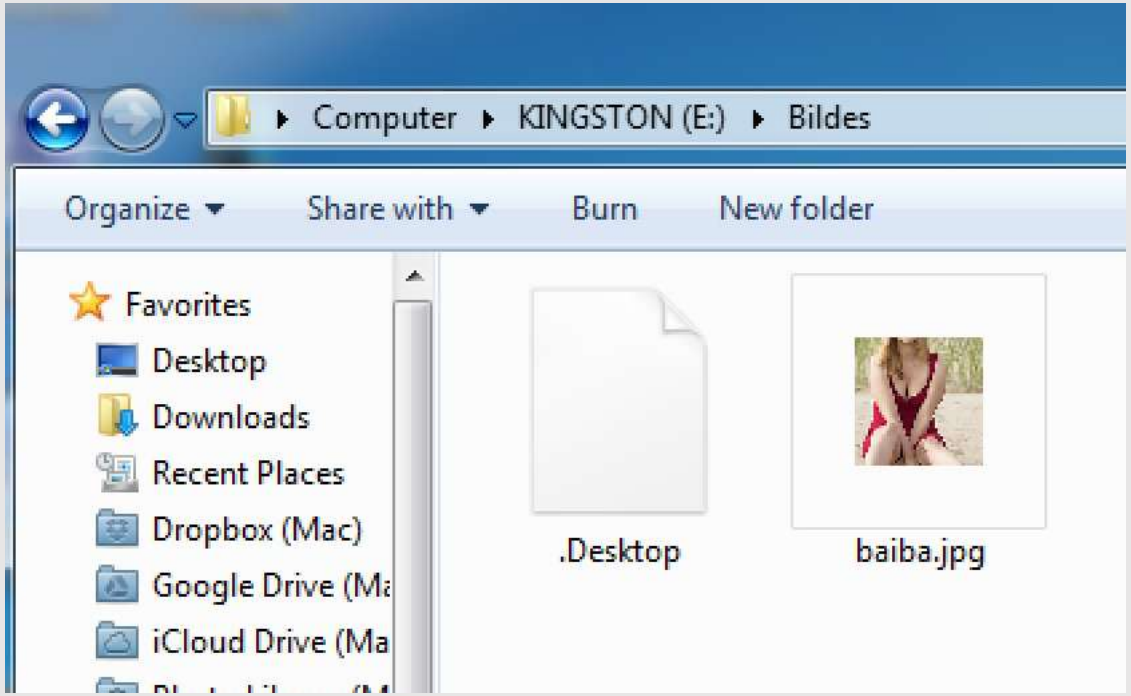
Pārbaudīt paroli

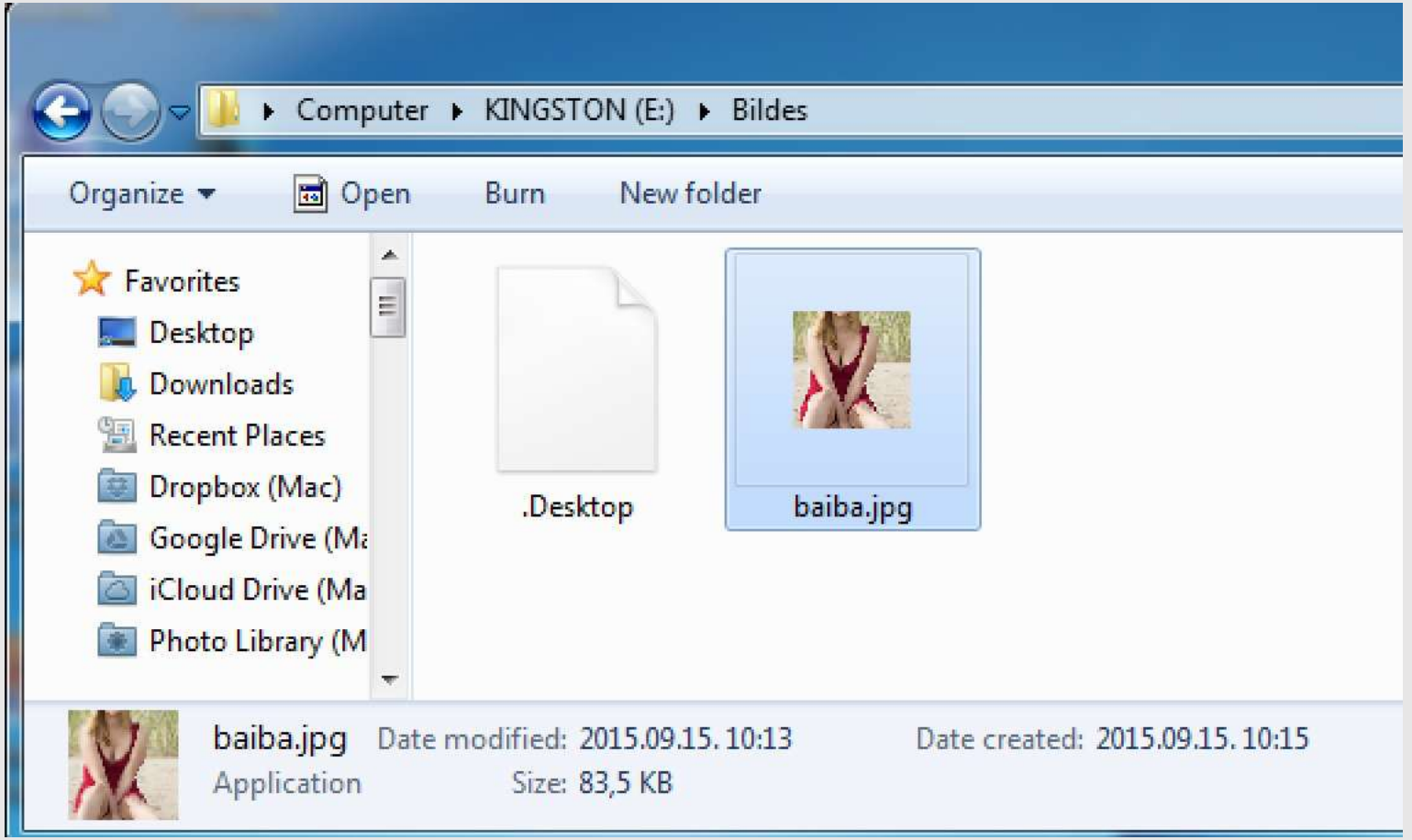
- Par mums
- Jaunumi
- Pasākumi
- Tīkli
- Kontaktinformācija

Latvijas Republikas Aizsardzības ministrija


win32_remote
X-CTU
Mozilla Firefox
eParakstītājs 3.0
desktop
VMware vSphe...
McAfee Security Sc...
desktop
akmens
Skype
Kingo ROOT
Browser Choice
ak
SEB Telebanka
iTunes
Atmel Studio 6.0
Tools
Parallels Share...
Immunity Debugger
Adobe Reader XI
FPRAS project
NetBeans IDE 8.0.2
Google Chrome
Recycle Bin
14:39
2015.10.13.


Computer ▸ KINGSTON (E:) ▸
Organize
Open
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Dropbox (Mac)
Google Drive (Ma
iCloud Drive (Ma
Photo Library (M
Desktop
Name
Date modified
.fseventsd
2015.10.15. 15:21
.Spotlight-V100
2015.09.15. 11:28
.Trashes
2015.09.15. 11:28
Bildes
2015.09.15. 10:07
System Volume Information
2015.09.15. 10:09


Computer ▸ KINGSTON (E:) ▸ Bildes
Organize
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Dropbox (Mac)
Google Drive (Ma
iCloud Drive (Ma
.Desktop
baiba.jpg

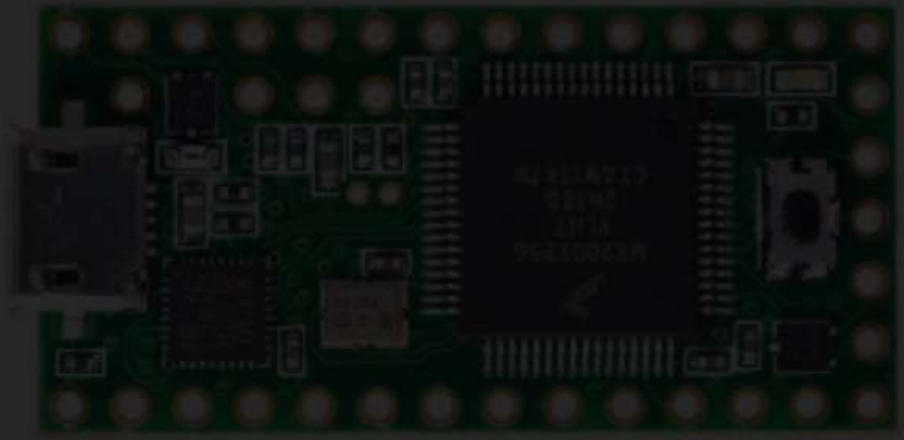

Computer
KINGSTON (E:)
Bildes
Organize
Open
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Dropbox (Mac)
Google Drive (Ma
iCloud Drive (Ma
Photo Library (M
.Desktop
baiba.jpg
baiba.jpg
Date modified: 2015.09.15. 10:13
Date created: 2015.09.15. 10:15
Application
Size: 83,5 KB

C&C servera dati

```
root@kali-birojs:/var/www_output# cat 20151013-1444736365-1354585055.txt
==========START 2015-10-13 14:10:25 195.122.22.44 0:1C:42:B8:EB:D3
Win32_Processor instance
-----------------------

Architecture : 9
Caption : x64 Family 6 Model 70 Stepping 1
Family : 198
ProcessorId : BFEBFBFF00040661
NumberOfCores : 1
SystemName : AKRUSTS-PC
UniqueId :
MaxClockSpeed : 2194
MAC : 00:1C:42:B8:EB:D3
User : akrusts-PC\akrusts

==========END
root@kali-birojs:/var/www_output#
```



Darbinieki – organizācijas reklāma

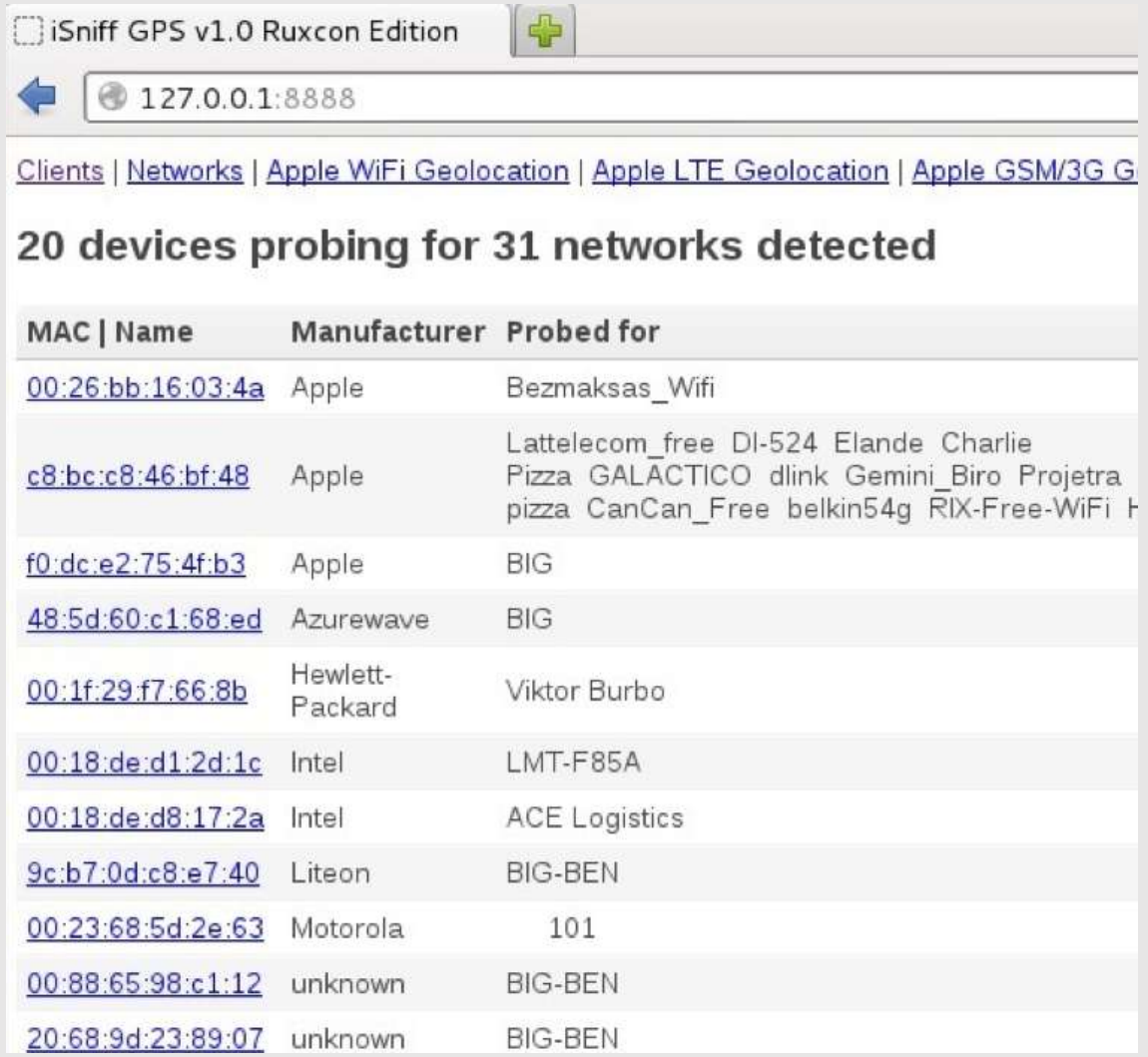
Jo svarīgāks darbinieks, jo tam vairāk vai dārgāki “gadžeti”

- Dators: PC ierindas darbiniekam, Apple – vadītājam
- Mobilie tālruņi un planšetdatori: Android vs Apple

Bezvadu tehnoloģijas

Ceļošanas vēsture

Viedtālruņi ar ieslēgtu bezvadu tīklu nepārtraukti mēģina pieslēgties sev zināmiem bezvadu tīkliem un pastāstīt kur bijuši



“Bezmaksas” piekļuves punkti – informācijas iegūšana

“Bezmaksas” piekļuve Internetam, kur daudz cilvēku

- Zināmiem piekļuves punktiem slēdzas bez jautāšanas
- Ja nelieto šifrēšanu un drošus sertifikātus var pārtvert informāciju
- Bez skanēšanas var noteikt organizācijas ārējo resursu adreses

Uzbrukumi WPA Enterprise

Izmanto viltotu piekļuves punktu, kurš nodrošina tādu pašu autorizāciju, kā organizācijas

Izmanto modificētu Radius serveri, kurš vienmēr autentificē lietotāju

Ja organizācija neizmanto drošu sertifikātu Radius serverim un klienti nevieic tā pārbaudi, ir iespējams:

- Iegūt lietotāja vārdu, kuru viņš izmanto autentifikācijai tīklā
- Liekt lietotājam izmantot uzbrucēja bezvadu tīklu


mschapv2: Mon Mar 2 10:02:05 2015
username: aivars
challenge: f7:91:4d:f5:3c:b8:89:90
response: :31:7f:ed:b1:9f:a7:98:1a:c0:6e:d3:9d:3b:bc:c6
jtr NETNTLM: aivars:$NETNTLM$f7
7fedb19fa7981ac06ed39d
3bbcc6
mschapv2: Mon Mar 2 10:02:30 2015
username: uldi
challenge: bc:08:fc:02:63:88:97:98
response: e6:14:5e:25:62:24:b8:fc:e4
:f1:6d
jtr NETNTLM: uldi :$NETNTLM$bc08fc026
ed59b108145
554f16d

Vai var cilvēks “no ielas” iekļūt ministru kabinetā G7 premjera vizītes laikā vienā telpā ar viņu?

Un ja var, kā to izdarīt?


DEMOTIX.COM

Noteikumus un likumus ievērot nav obligāti, jo neviens tā nedara

Problēmas

Mūsdienu tehnoloģijas ir nojaukušas robežu starp ārējo un iekšējo infrastruktūru

Lielākais risks informācijas sistēmu drošībai ir cilvēks

- Attiecas ne tikai uz informācijas sistēmām

Risinājumi?

Infrastruktūras aizsardzība ņemot vērā, ka būs veiksmīgi sociālās inženierijas uzbrukumi

“Security awarness” apmācība darbiniekiem

Paldies par uzmanību!

Jautājumi un diskusija

Agris Krusts, IT drošības konsultants

- www.itcentrs.lv
- e-pasts: Agris.Krusts@itcentrs.lv
- Twitter: @agris_krusts
- Linked-in: http://lv.linkedin.com/in/agriskrusts