

# Lietotāja identitāte tiešsaistē

Riski un jaunās iespējas

ISACA konference 2013.gada 23.oktobris

Aigars Jaundālders  
DPA



# Dienas kārtība

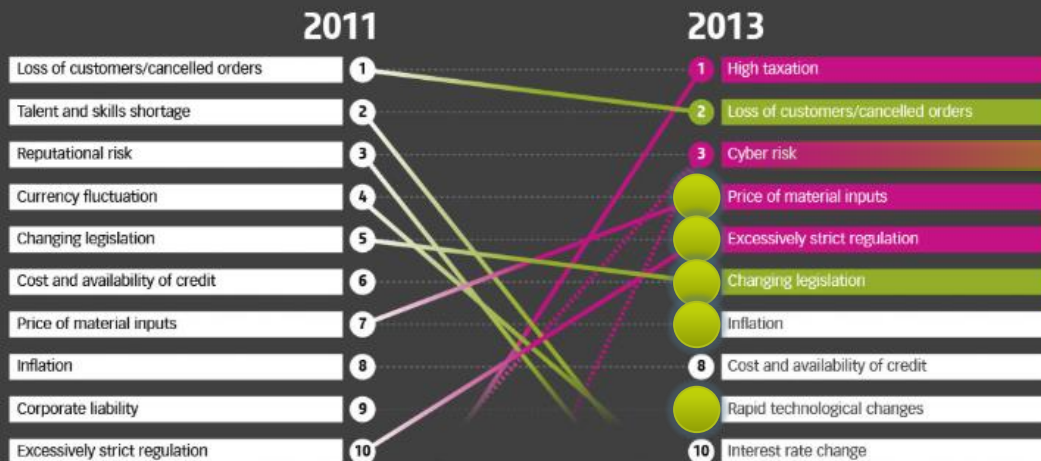


- Vai problēma ir aktuāla?
- Kas ir vājākais ķēdes posms šodien?
- Kādam būtu jāizskatās risinājumam?

# Vai IT drošība vispār ir svarīga?



## CHANGES IN RISK RANKING



20. gadsimtā...



Naftas un gāzes ieguve bija būtisks ekonomiskās un politiskās attīstības instruments...

Ar ko varēja nopelnīt naudu, varu... gan tad, kad to darīja pieejamu citiem, gan tad, kad atņēma?



10101. gadsimtā...



Informācija ir jaunā gadsimta  
nafta un zelts vienlaikus



if (user) then ...



Identitāte ir atslēga piekļuvei pie informācijas un tās izpratnei...

Daži mīti...



# # 1



- Es esmu vienkāršs pilsonis, mazs uzņēmējs utt., es nevienam neinteresēju...



small businesses are the path of least resistance for attackers...



Symantec Internet Threat Report 2013



## # 2



- Es visur lietoju labu antivīrusu. Pat uz mobilā telefona. Man nekas nevar kaitēt!



Like on desktop and server systems, private and corporate users should not rely on antivirus products for perfect protection of their Android devices.



On the Effectiveness of Malware Protection on Android, Fraunhofer AISEC, April 2013

# # 3



- Mēs esam liels uzņēmums ar labu IT un drošības komandu, mums ir vismodernākās tehnoloģijas. Mums nekas nevar kaitēt!

Jums neuzbruks... .. tomēr tiksiet “uzlauzti”

F-Secure Threat Report H1 2013

**Definition: Watering Hole attack**<sup>[1]</sup>  
The attacker wants to attack a particular group (organization, industry, or region). The attack consists of three phases

1. *Guess which websites the group often uses*
2. *Infect one or more of these websites with malware.*
3. *Eventually, some member of the targeted group will get infected.*

Relying on websites the group trusts makes this strategy efficient even with groups that are resistant to spear phishing and other forms of phishing.

Cik unikālas lietotājevārda / paroles kombinācijas izmanto Lietotājs Vidējais?

watering hole

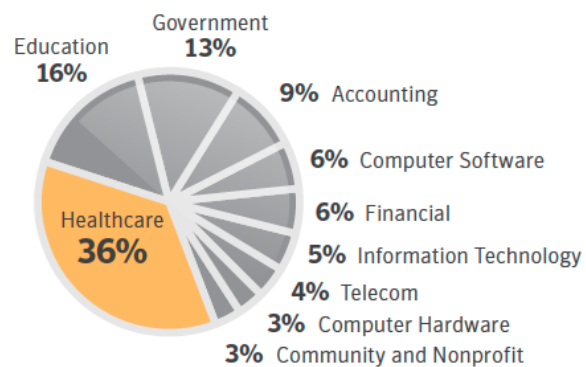
# # 4



➤ Mēs neesam banka, mūsu sistēmās nav ko zagt

**Data Breaches by Sector in 2012**

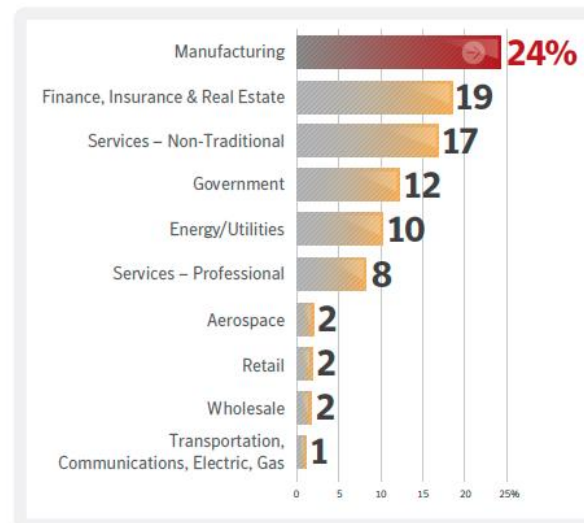
Source: Symantec



*At 36 percent, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industry.*

**Top 10 Industries Attacked in 2012**

Source: Symantec



Ja identitāte ir atslēga, kas ir vājākais posms?



Visu nosaka

**lietotājs**

tehnoloģijām gandrīz nav nozīmes

# Ko izmanto uzbrucēji šodien?

Kas ir šodienas autentifikācijas risinājumu galvenais trūkums?



Risinājumi ir tehnoloģiski droši

bet ...

**tie nav pielietojuma droši – neņem vērā lietotāju kontekstu**



# Kādam jābūt nākotnes risinājumam?



## user-proof

Lietotājs nevar sev apzināti vai neapzināti kaitēt

## ubiquitous

Aizsargā gan lietotājus, gan pakalpojumu sniedzējus, neierobežo kanālus utml.

## uninvolved

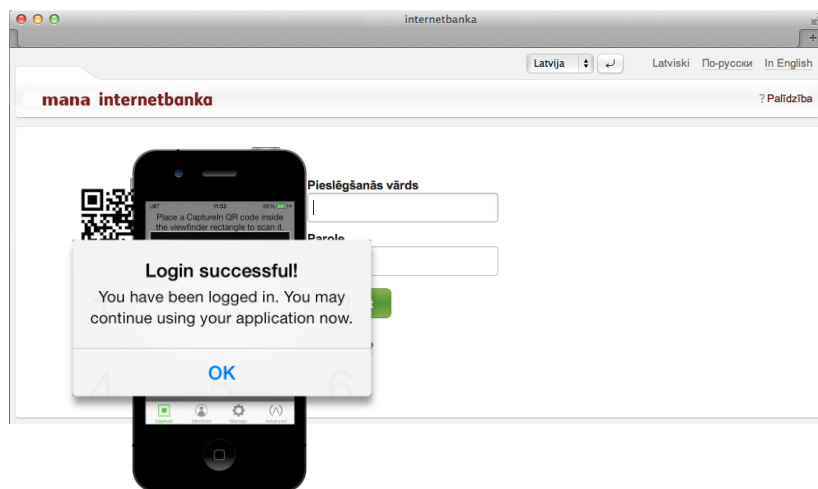
Neprasa lietotājam papildus darbības, zināšanas u.tml.  
Reflektori kontrolēta, dabiska daļa no ikdienas



# Piemēram...



## CaptureIn



### ➤ User – proof

Lietotājs nesaskaras ar jebkādu informāciju, ko ļaunprātis var attālināti izmantot pret to. Jebkāda ārpus ierīces pārsūtīta informācija nav atkārtoti izmantojama.

### ➤ Ubiquitous

Atbalsta darbu ar jebkādām tiešsaistes ierīcēm ar vizuālo displeju. Atbalsta darbu arīdzan no tā paša viedtālruņa, kur uzstādīts lietojums. Aizsargā gan gala lietotāju, gan pakalpojuma sniedzēju.

### ➤ Uninvolved

Lietotājam ir jāspēj vienīgi uzstādīt lietojumu un palaist to. Motorika jutīgo darbību kontrolei – lietotājs instinktīvi turpina kontrolēt situāciju. Jūtīgās darbības notiek vienīgi tad, ja lietotājs apzināti pavēš kameru pret CaptureIn QR kodu.



**Paldies!**

