KRAŠTO APSAUGOS MINISTERIJA

KIBERNETINIS SAUGUMAS

Rimgaudas Gamulis
Krašto apsaugos ministerija

Kylančios grėsmės: esama situacija

- 2017 m. Lietuva patyrė 50 tūkst. kibernetinių incidentų, 10% daugiau nei pernai;
- Visoje ES 2017 m. kasdien buvo užfiksuojama 4 tūkst. kibernetinių incidentų;
- Neatrėmus grėsmių ES ekonomika gali patirti 640 milijardų eurų;
- Vienas globalaus masto kibernetinis incidentas gali sukelti tiek nuostolių, kiek kainavo uraganas Katrina, 120 milijardų JAV dolerių.

Saugos konsolidacija

Laiko juosta

Pradžia

VĮ Infostruktūra
2017 / 06
Perėjimas į KAM

KAM pertvarka
2017 / 08
ITT
Naujas NKSC

VRM el. sauga
2017 / 11
Perėjimas į KAM

RRT CERT.LT
2017 / 11
Perėjimas į KAM

Nauja KAM struktūra
2018 / 01
KSITD
ITT
Naujas NKSC

Direktyva ir strategija
2018 / 08 / 12
NIS direktyvos įgyvendinimas
Kibernetinio saugumo strategija

Valstybinis tinklas
2019
Valstybės institucijų kertinis tinklas

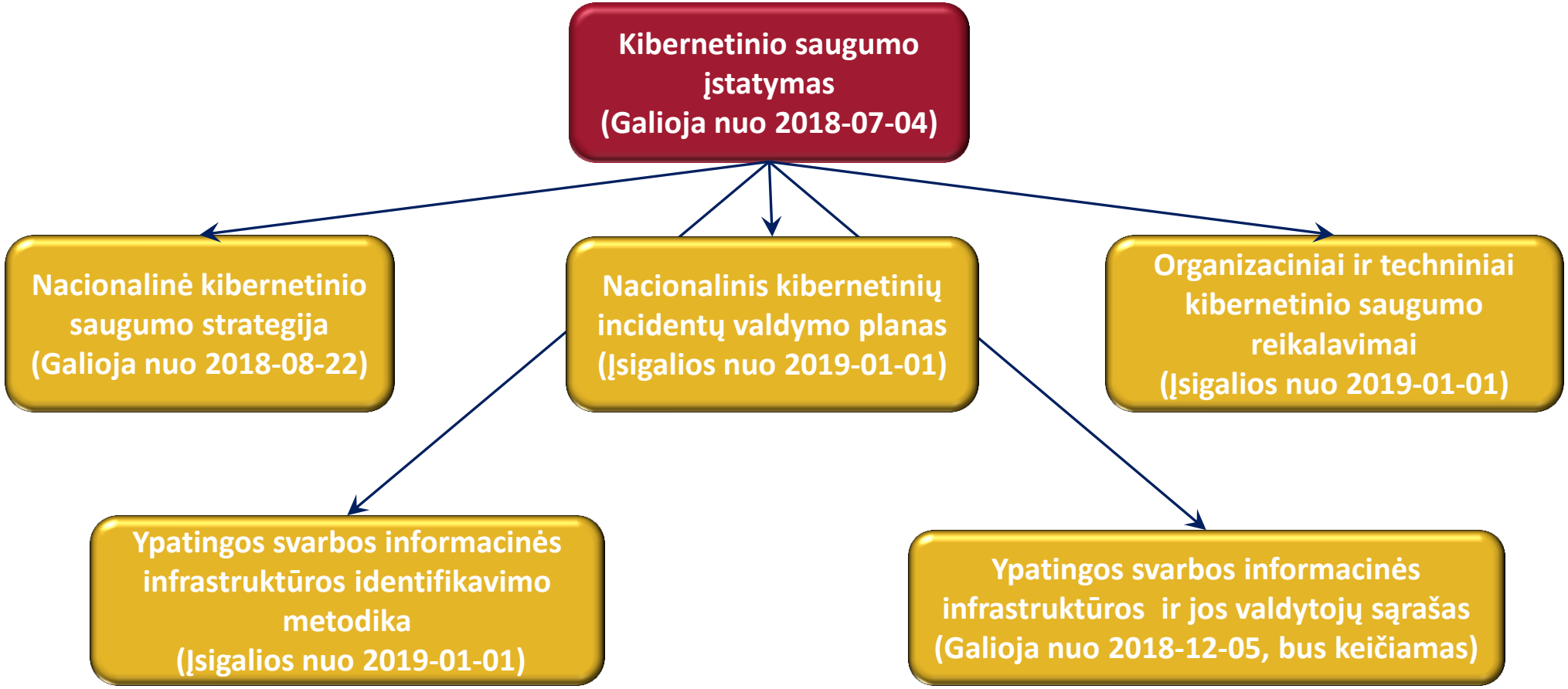
Siekiamas rezultatas

NKSC
Stiprus Nacionalinis kibernetinio saugumo centras

Vieningi saugos reikalavimai
Įvairių saugos sričių reikalavimų suvienijimas

Valstybinis tinklas
Patikima valstybės institucijų ryšių platforma

Teisinė sistema



Kibernetinio saugumo įstatymas – https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c

Kibernetinio saugumo įstatymą įgyvendinantys teisės aktai – https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/4c9d3ce0f85211e895b0d54d3db20123?jfwid=-7x1bdzfye

Nacionalinė kibernetinio saugumo strategija

Kova su nusikaltimais kibernetinėje erdvėje

Kibernetinio saugumo kultūra ir inovacijų plėtra

Valstybės kibernetinis atsparumas
ir kibernetinės gynybos pajėgumų plėtra

Privataus ir viešojo sektorių bendradarbiavimas

Tarptautinis bendradarbiavimas ir
tarptautinių įsipareigojimų vykdymas

Ypatingos svarbos infrastruktūra

Ypatingos svarbos informacinės infrastruktūros (YSII) sąrašo sudarymas ir tvirtinimas

Ypatingos svarbos informacinės infrastruktūros (YSII) nustatymas

Ypatingos svarbos infrastruktūros (YSI) objektų nustatymas

Pirminis Ypatingos svarbos infrastruktūros (YSI) objektų sąrašas

YSII

YSII sąrašas

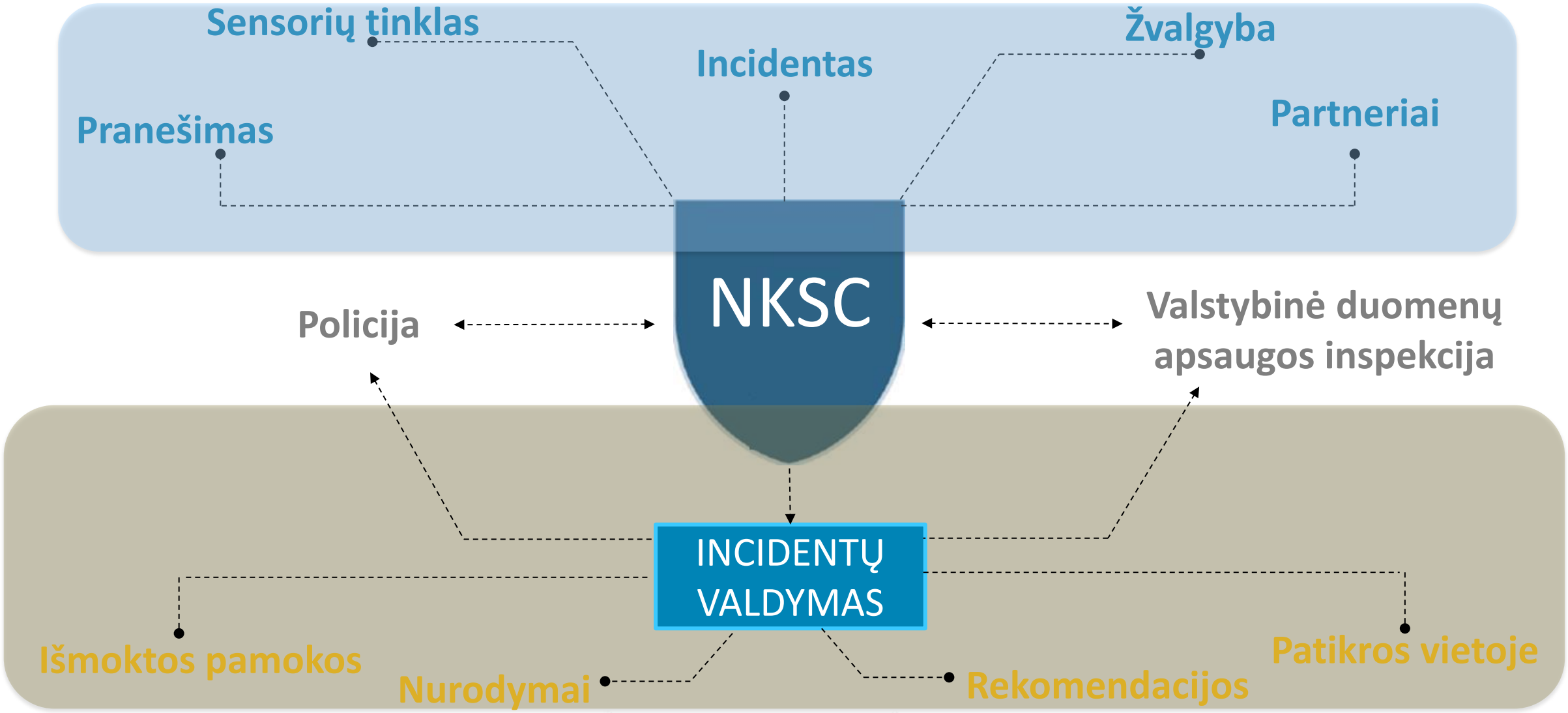
YSI sąrašas

Pirminis YSI sąrašas

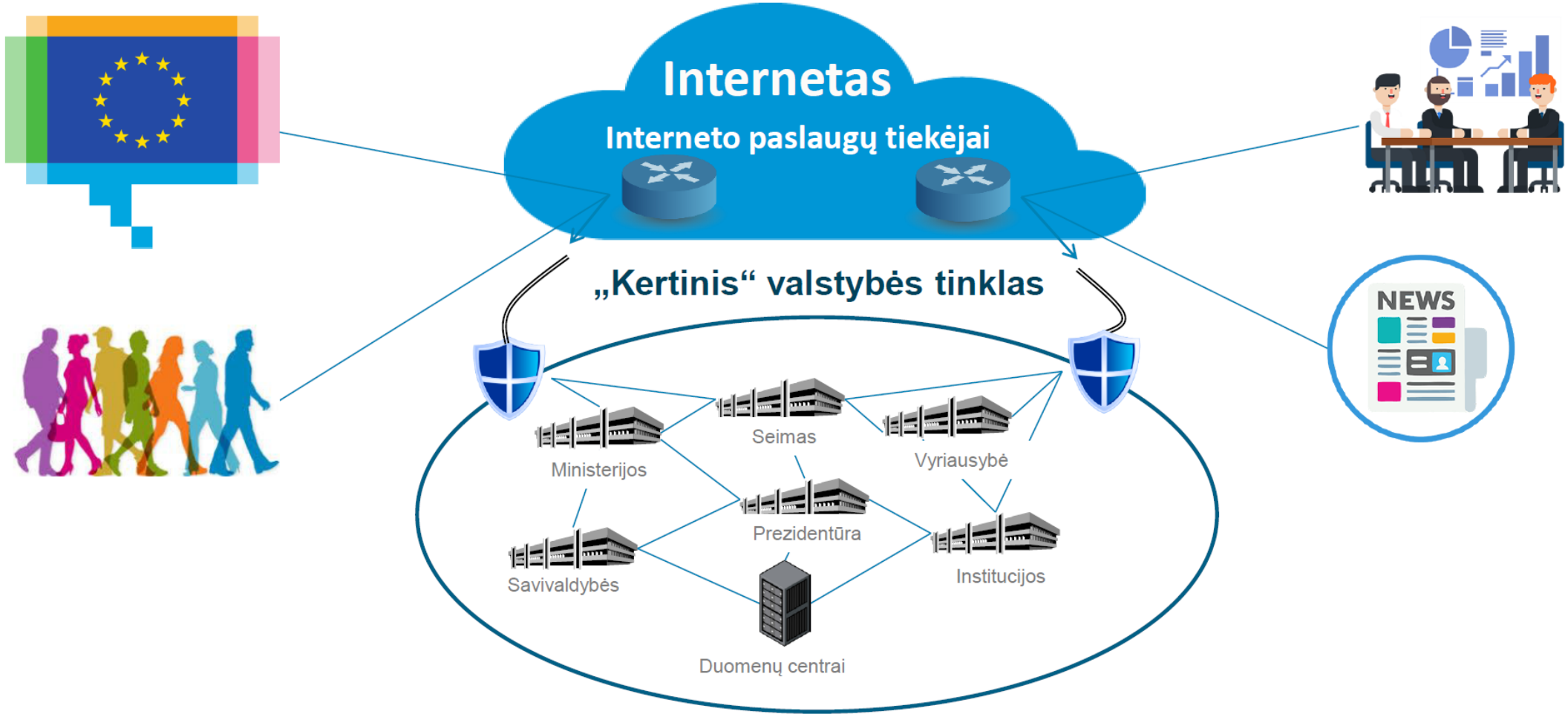
Ypatingos svarbos informacinė infrastruktūra

Savivaldybių administracijoms nustatyti visus jų veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas **energetikos, transporto ir pašto, sveikatos priežiūros, geriamojo vandens tiekimo, paskirstymo ir tvarkymo, valstybės valdymo sektoriuose,** užpildyti Metodikos 2 priede pateiktą klausimyną, jį pateikti Metodikos 1 priede nurodytai institucijai (institucijoms) ir Metodikos nustatyta tvarka vykdyti Atsakingo valdytojo funkcijas.

Incidentų valdymo schema



Valstybinis tinklas



Valstybinio tinklo kriterijai

„Valstybės valdymas ir savivaldybių institucijų veikla“

„Ekonomikos ir civilinės infrastruktūros funkcionavimas“

„Gyventojų būtinųjų poreikių tenkinimas“

Gyvybiškai svarbių valstybės funkcijų sąrašas

(Vyriausybės 2012-05-29 nutarimas Nr. 631)

Gyvybiškai svarbios valstybės funkcijos

(Mobilizacijos ir priimančios šalies paramos įstatymas)

Valstybinės mobilizacinės užduotis valstybės ir savivaldybių institucijoms ir įstaigoms

(Vyriausybės 2013-03-27 nutarimas Nr. 256)

Europos valstybių veikla, užtikrinant šalies kibernetinį saugumą

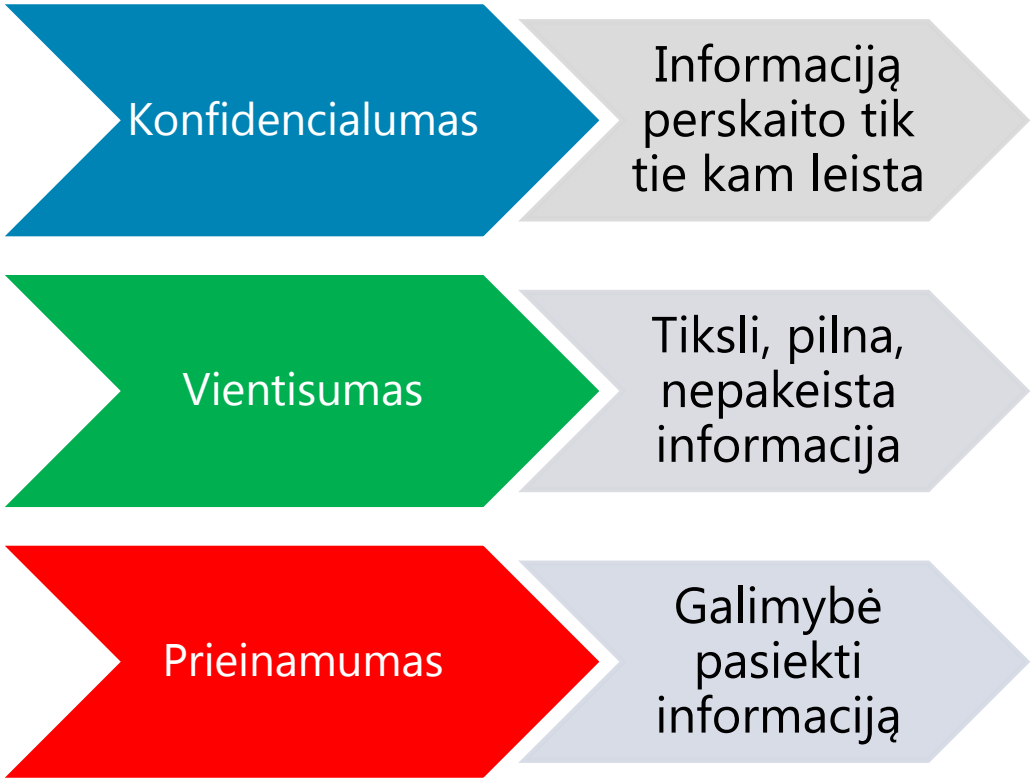
1. Lithuania 89.61 PDF

1st	National Cyber Security Index	Population	2.8 million
56th	Global Cybersecurity Index	Area (km²)	65.3 thousand
41st	ICT Development Index	GDP per capita ($)	34.1 thousand
29th	Networked Readiness Index		

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Lithuania	89.61	70.95	18.66
2.	Spain	89.61	73.24	16.37
3.	Estonia	88.31	79.27	9.04
4.	France	83.12	79.06	4.06
5.	Germany	83.12	81.95	1.17
6.	Slovakia	80.52	66.73	13.79
7.	Singapore	80.52	83.11	-2.59
8.	Finland	79.22	82.26	-3.04
9.	United Kingdom	75.32	83.96	-8.64
10.	Czech Republic	74.03	69.37	4.66
11.	Malaysia	72.73	66.90	5.83
12.	Latvia	72.73	70.59	2.14
13.	Switzerland	72.73	85.13	-12.40
14.	Poland	70.13	66.59	3.54
15.	Portugal	68.83	70.65	-1.82

DEFENDING CYBER FRONTLINE

Kas yra kibernetinis saugumas?



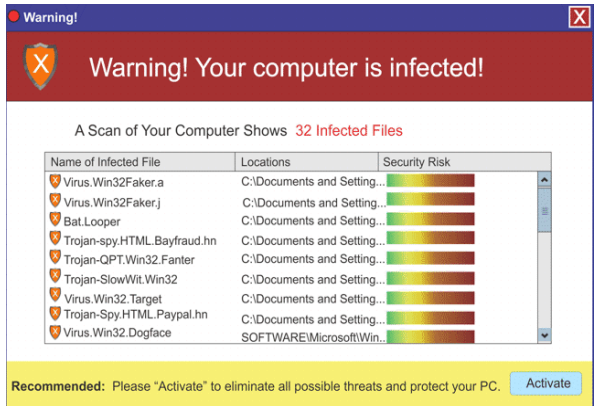
"...užtikrinama, kad tik naudotojai, kuriems leidžiama (konfidencialumas) turi prieigą prie tikslios ir pilnos informacijos (vientisumas) tuo metu, kai tam yra poreikis (prieinamumas)."

Pavojingumo lygis

Vertybės kompiuteryje

- e-bankininkystės **prisijungimo duomenys**, **piniginės lėšos**;
- Facebook, gmail, iCloud, twitter, Amazon, PayPal ir pan. **paskyros**, kurių pagalba galima pasiekti jautrią informaciją, ar išnaudoti jose esančius kontaktus;
- **Asmens duomenys**, kurių pakanka tapatybei pavogti (asmens kodas, dokumentų numeriai, soc. draudimo numeris);
- Programinės įrangos **licencijos**, prieigos **kodai**, tinklo žaidimų **paskyros**;
- Šantažavimas grasinant **informacijos užšifravimu** arba **paviešinimu**;
- Kompiuterio **resursų** išnaudojimas;

Socialinė inžinerija



From: arvyc[redacted]@gmail.com> Sent: Pn
To:
Cc:
Subject: žiūrėti sąrašą

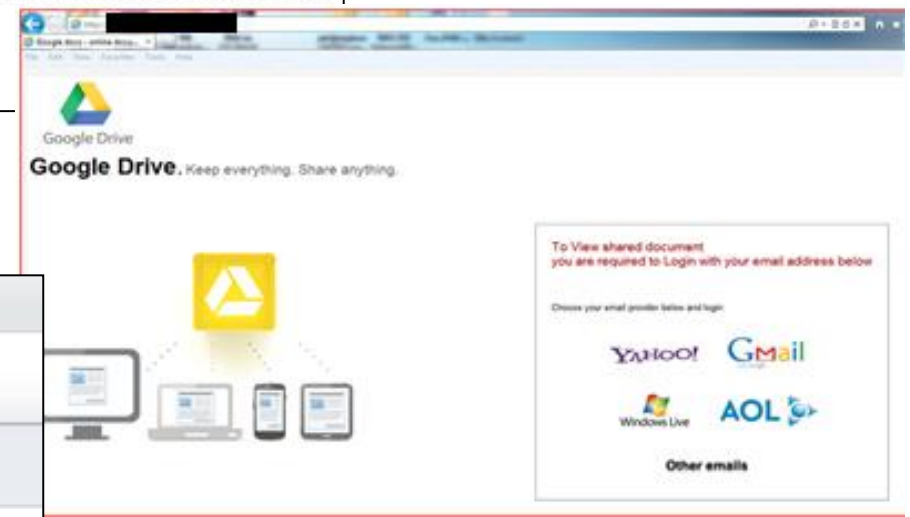
Sveiki,

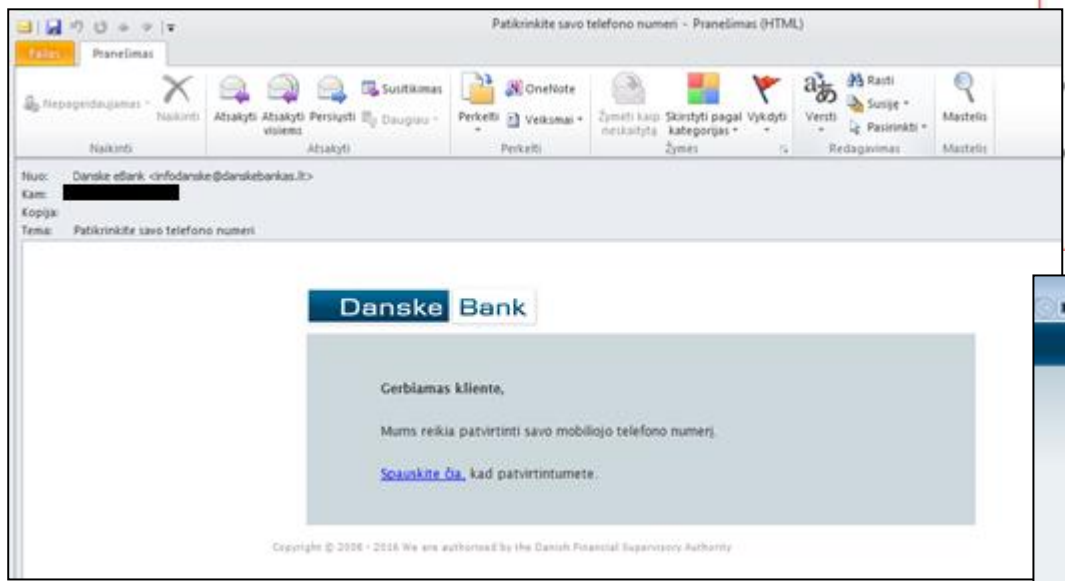
Prašome peržiūrėti Svarbi atsiųsta dokumentą aš noriu pamatyti. Tai ne areštas, jis uploaded su Google Dok.

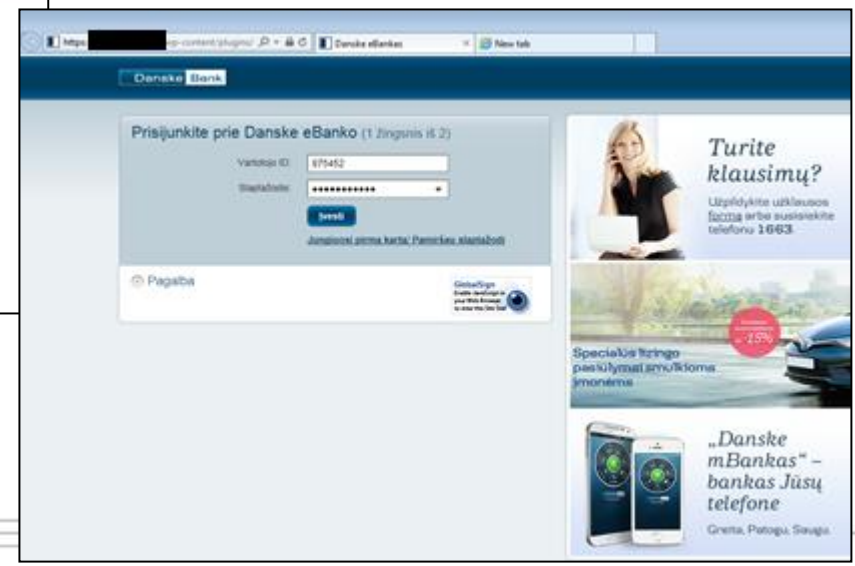
Norėdami peržiūrėti, spauskite ant http / / docs.google.com ir prisijungti su savo elektroninio pašto tiesiogiai susipažinti su nuomone.

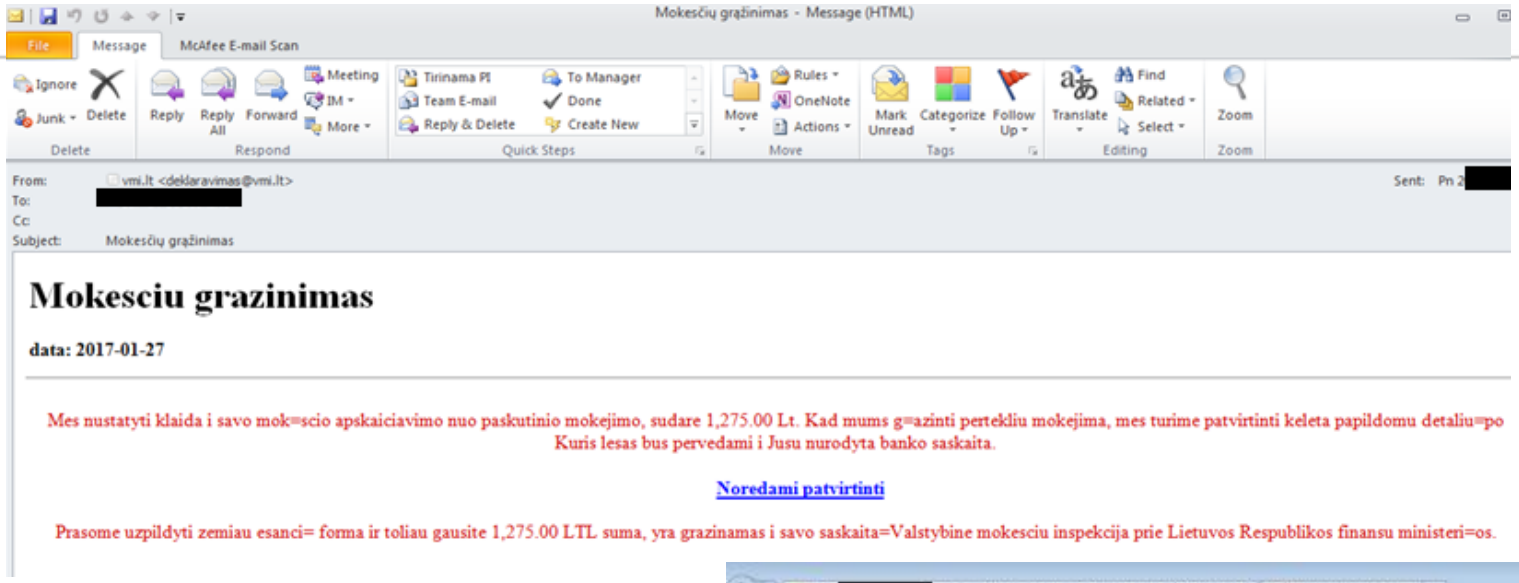
http:/[redacted]x.cl/m/index.html
Click to follow link

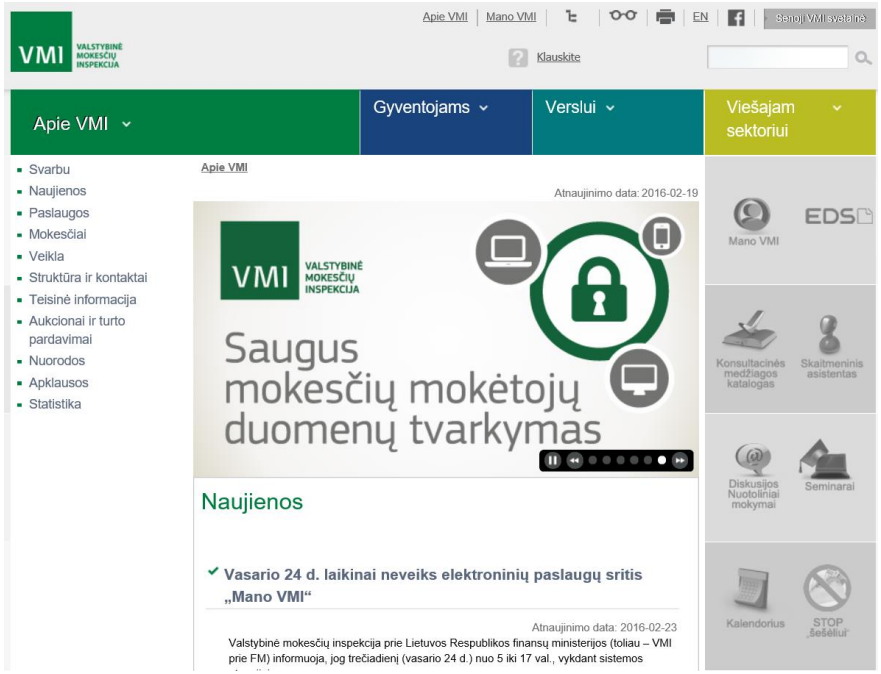
Kind regards.

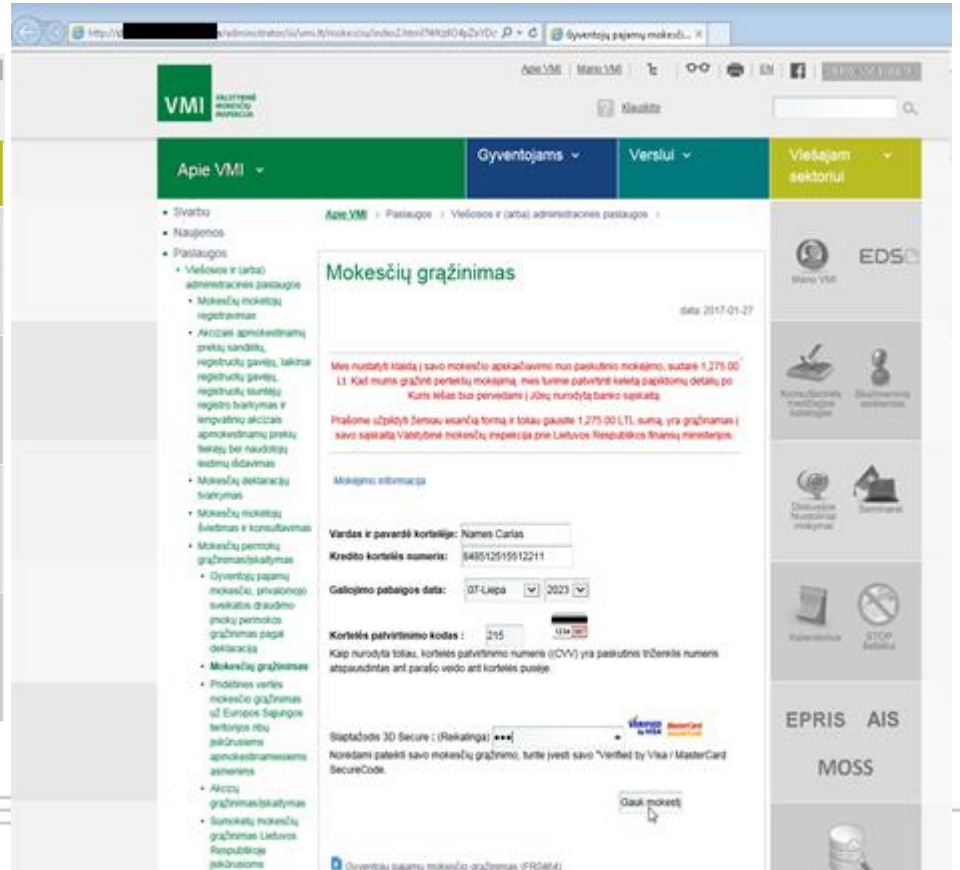







Mokesčių grąžinimas - Message (HTML)
File
Message
McAfee E-mail Scan
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
IM
More
Delete
Respond
Tirinama PI
Team E-mail
Reply & Delete
To Manager
Done
Create New
Quick Steps
Move
Rules
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
Zoom
From: vmi.lt <deklaravimas@vmi.lt>
To: [redacted]
Cc:
Subject: Mokesčių grąžinimas
Sent: Pn 2[redacted]
Mokesciu grazinimas
data: 2017-01-27
Mes nustatyti klaida i savo mok=scio apskaiciavimo nuo paskutinio mokejimo, sudare 1,275.00 Lt. Kad mums g=azinti pertekliu mokejima, mes turime patvirtinti keleta papildomu detaliu=po
Kuris lesas bus pervedami i Jusu nurodyta banko saskaita.
Noredami patvirtinti
Prasome uzpildyti zemiau esanci= forma ir toliau gausite 1,275.00 LTL suma, yra grazinamas i savo saskaita=Valstybine mokesciu inspekcija prie Lietuvos Respublikos finansu ministeri=os.


VMI
VALSTYBINĖ MOKESČIŲ INSPEKCIJA
Apie VMI
Mano VMI
EN
Senoji VMI svetainė
Klauskite
Apie VMI
Gyventojams
Verslui
Viešajam sektoriui
Svarbu
Naujienos
Paslaugos
Mokesčiai
Veikla
Struktūra ir kontaktai
Teisinė informacija
Aukcionai ir turto pardavimai
Nuorodos
Apklausos
Statistika
Apie VMI
Atnaujinimo data: 2016-02-19
Saugus mokesčių mokėtojų duomenų tvarkymas
Naujienos
Vasario 24 d. laikinai neveiks elektroninių paslaugų sritis „Mano VMI“
Atnaujinimo data: 2016-02-23
Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos (toliau – VMI prie FM) informuoja, jog trečiadienį (vasario 24 d.) nuo 5 iki 17 val., vykdant sistemos
Mano VMI
EDS
Konsultacinės medžiagos katalogas
Skaitmeninis asistentas
Diskusijos Nuotoliniai mokymai
Seminarai
Kalendorius
STOP „Šešėliui“


VMI
Apie VMI
Gyventojams
Verslui
Viešajam sektoriui
Mokesčių grąžinimas
Mokėjimo informacija
Vardas ir pavardė kortelėje:
Kredito kortelės numeris:
Galiojimo pabaigos data:
Kortelės patvirtinimo kodas :
Gauk mokestį
EDS
EPRIS
AIS
MOSS

Nuo: DHL Express <uzklausa@dhl.com>
Kam: undisclosed-recipients:
Kopija:
Tema: DHL Express Shipment Notification
Išsiųsta: Wed 9/20/2017 10:11 AM
Pranešimas RECEIPT_PDF.ace (351 KB)

ORDER: PI#545223
ARRIVAL PERIOD: Yesterday

Dear Customer,

Your parcel has arrived at the post office. Our courier was unable to deliver the parcel to you

Please click the attachment to DOWNLOAD AND PRINT RECIEPT

To receive your parcel, please go to the nearest office and show this receipt.

Best Regards, DHL Express Team.

Nuo: Dropbox <verify@dropbox.com>
Kam: [redacted]
Kopija:
Tema: Please verify your email address [redacted]t
Išsiųsta: Mon 9/11/2017

Hi an[redacted]

We just need to verify your email address before your sign up is complete!

Verify your email

Happy Dropboxing!

Nuo: Amazon.co.uk <auto-shipping@amazon.co.uk>
Kam: [redacted]
Kopija:
Tema: Your Amazon.co.uk order 464-8110362-9240461 has been dispatched
Išsiųsta: Tue 9/12/2017 12:56 PM

amazon.co.uk prime

Your Orders | Your Account | Amazon.co.uk

Dispatch Confirmation
Order #464-8110362-9240461

Hello,

We thought you'd like to know that we've dispatched your item(s). Your order is on the way, and can no longer be changed. If you need to return an item or manage other orders, please visit Your Orders on Amazon.co.uk.

Arriving:
Saturday, September 16

Track Your Package

Your item(s) is (are) being sent by Amazon Logistics. Your tracking number is H40056346323. Depending on the delivery method you chose, it's possible that the tracking information might not be visible immediately. Learn more about Tracking.

If you have a mobile device, you can use the free Amazon Mobile App to receive delivery notifications and track your parcel on the go.

Need to view or print your invoice? Go to Order Details.Learn more.
It's easy to return an item. Visit our Online Returns Centre.
If you need further assistance with your order, please visit Customer Service.

www.sanagustinturismo.co/Facebook/

facebook

Email
Stay logged in

Connect with your friends faster, wherever you are.

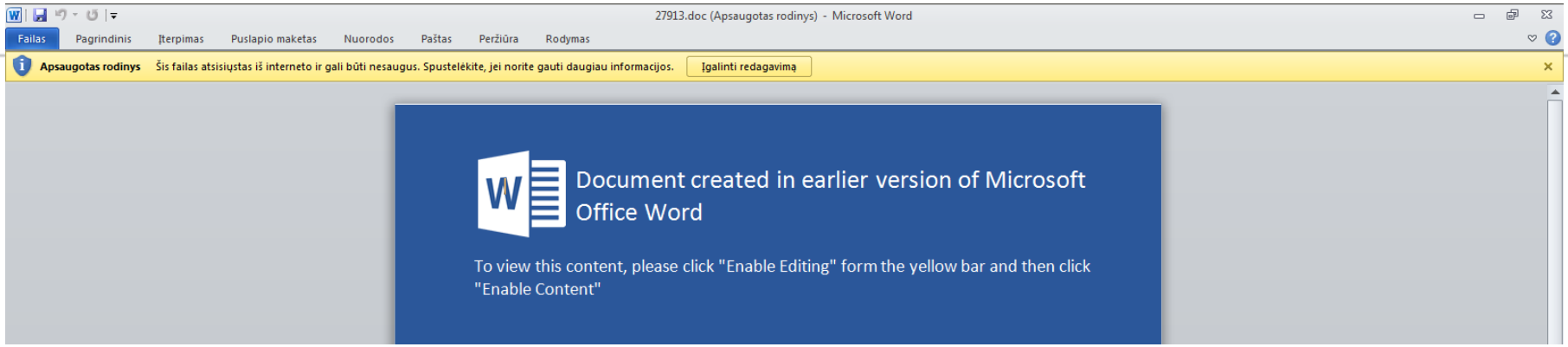
The Facebook application is available in more than 2,500 phones.

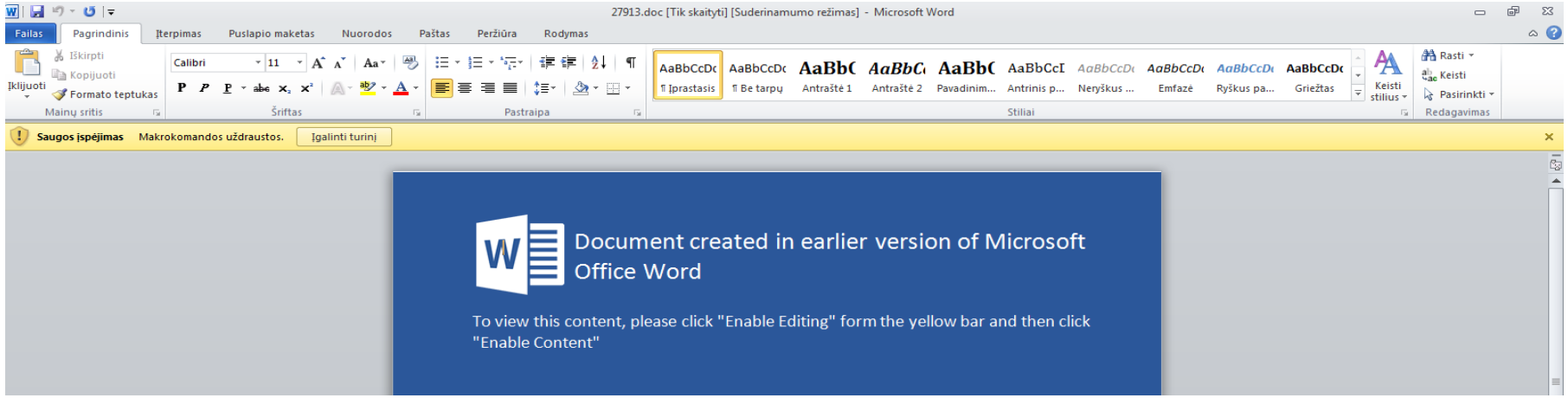
- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

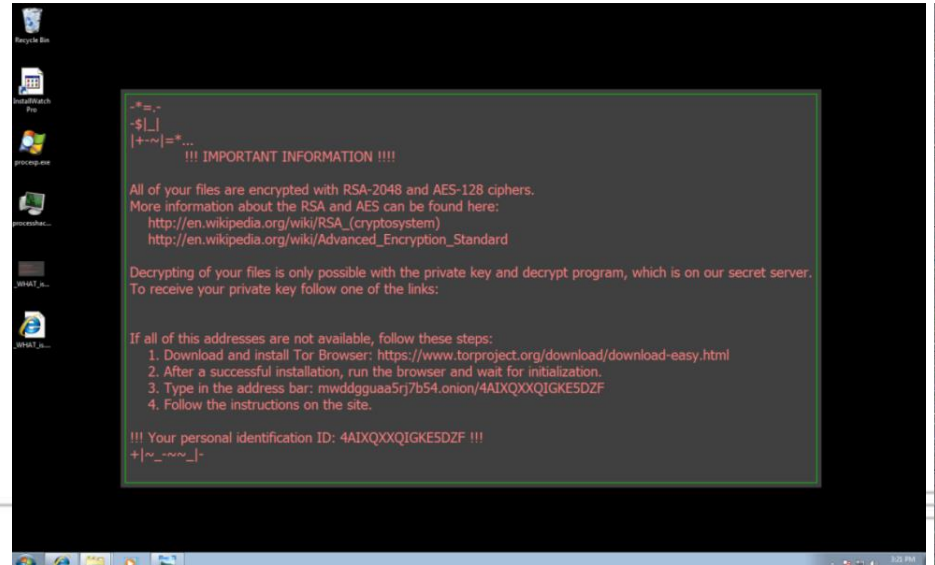
Discover Facebook Mobile

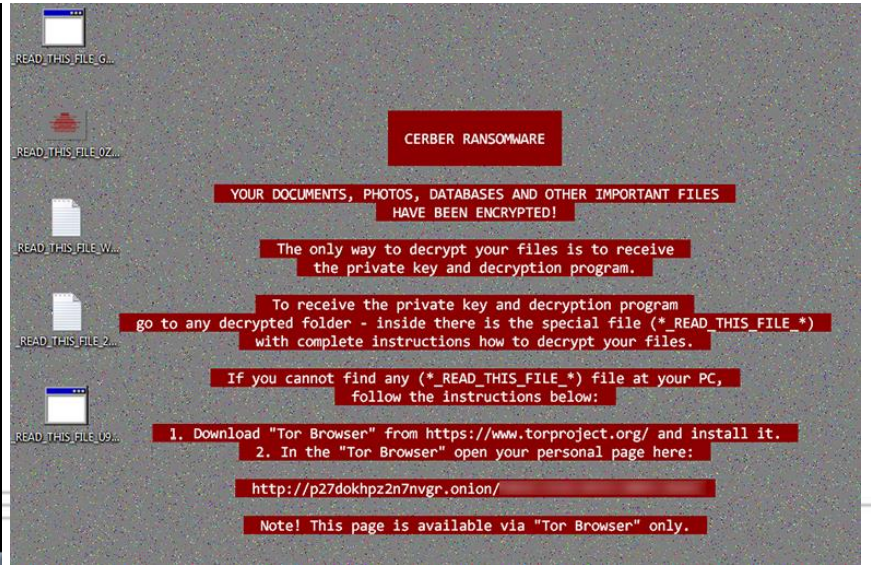
Sign up
It's free (and will remain).

Name:
Surname:
Your email:
Re-enter your email address:
Password:
Gender: Select sex:
Date of Birth: Day:
Why do I have to
Sign up


27913.doc (Apsaugotas rodinys) - Microsoft Word
Failas
Pagrindinis
Įterpimas
Puslapio maketas
Nuorodos
Paštas
Peržiūra
Rodymas
Apsaugotas rodinys
Šis failas atsisiųstas iš interneto ir gali būti nesaugus. Spustelėkite, jei norite gauti daugiau informacijos.
Įgalinti redagavimą
Document created in earlier version of Microsoft Office Word
To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"


27913.doc [Tik skaityti] [Suderinamumo režimas] - Microsoft Word
Failas
Pagrindinis
Įterpimas
Puslapio maketas
Nuorodos
Paštas
Peržiūra
Rodymas
Saugos įspėjimas
Makrokomandos uždraustos.
Įgalinti turinį
Document created in earlier version of Microsoft Office Word
To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"


-*=-
-$|_|
|+~~|=*...
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: mwddgguaa5rj7b54.onion/4AIXQXXQIGKE5DZF
4. Follow the instructions on the site.
!!! Your personal identification ID: 4AIXQXXQIGKE5DZF !!!
+|~_-~~_|-


CERBER RANSOMWARE
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt your files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*_READ_THIS_FILE_*) with complete instructions how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below:
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/
Note! This page is available via "Tor Browser" only.

Vandalizmas/terorizmas

- - Prasideda Ukrainoje 2017 birželio 27;
- - Per pusdienį išplinta per visą Maersk pasaulinį tinklą;
- - Per dvi valandas tinklas atjungiamas nuo pasaulinio Interneto;
- - Nuostoliai 300 mln dolerių;
- - 2 savaitės atstatyti sistemų veiklą;
- - Tikslas – išsibandyti kibernetinius ginklus.

THE COST OF NOTPETYA

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

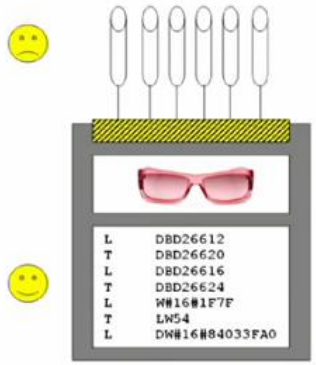
French construction company Saint-Gobain

$300,000,000

Danish shipping company Maersk

Advanced Persistent Threat

Coolest stuff in Stuxnet: A reality blocker for controllers



← 984 centrifuges (unhappy)

← Electrical IO

← Reality blocker

← Legitimate program (happy)

Compromised controller

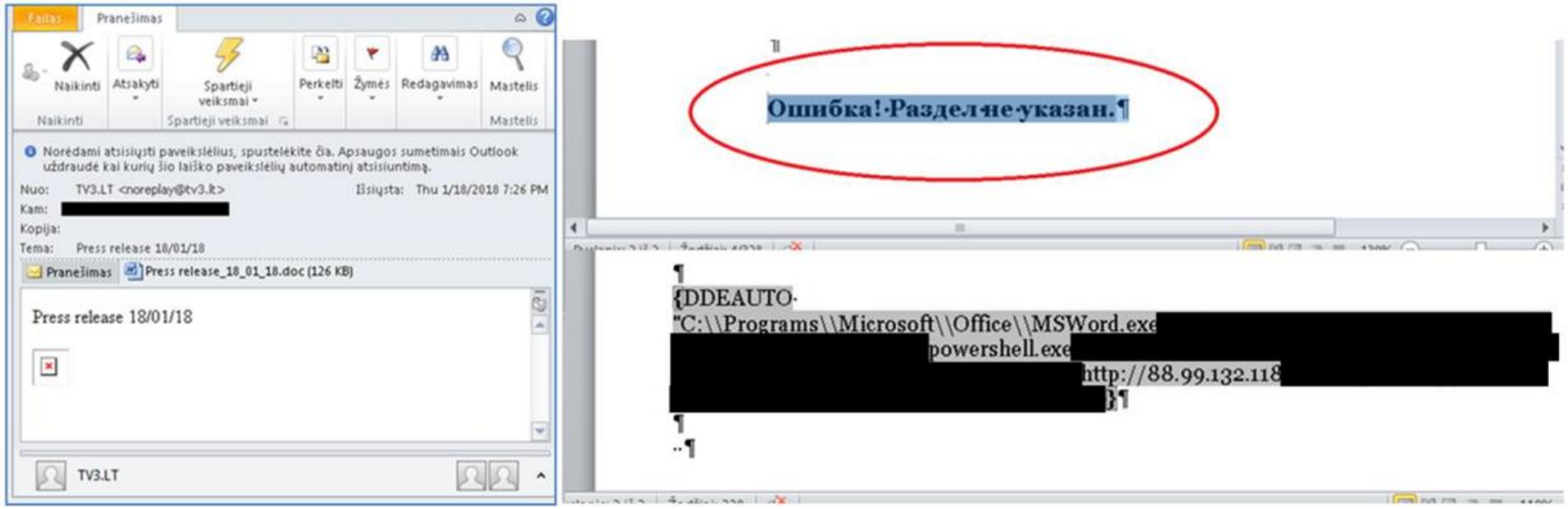
Malware dropper (on Windows PCs)

Payload (on controllers)

Target: Natanz FEP

Mission goal: Denial of nukes

Įsibrovimas į TV3 svetainę ir kenksmingo kodo platinimas



pats įsilaužimas. Taip pat pasinaudojant suklastota „sensacinga informacija“ tikslingai išplatinami laiškai su kenksmingu kodu, kuris, patekęs į sistemą, galėtų ją išnaudoti (pvz.: suteikti įsibrovėliams prieigą prie joje saugomų dokumentų, sudarytų sąlygas sekti naudotojų veiklą).

Atpažinkite potencialiai pavojingą laišką

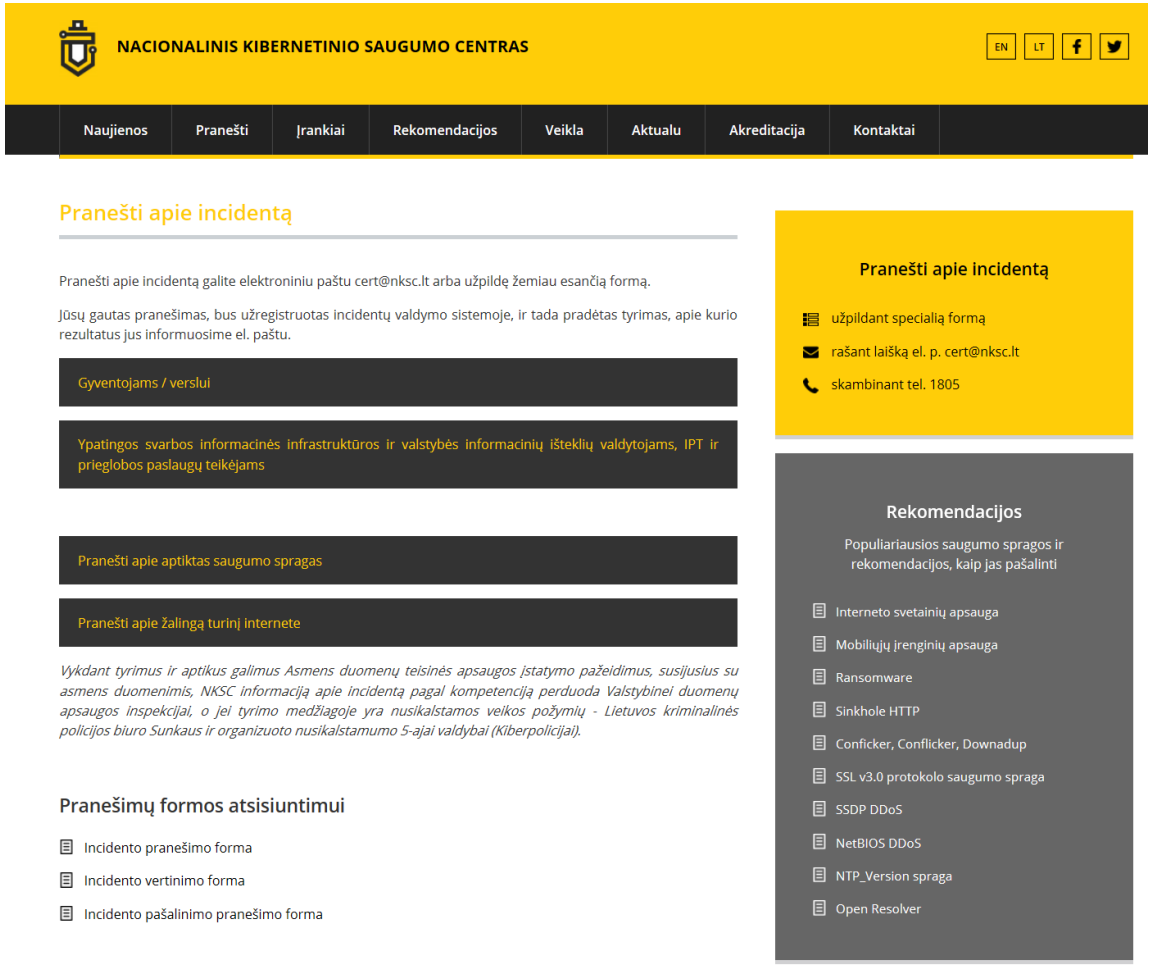
- Ar tokių laiškų laukiau? Ar tikrai pažįstu siuntėją ir žinau apie ką jis kalba? Slaptažodis pateikiamas kartu su siunčiamu failu?
- Siuntėjas Jums nėra žinomas, tačiau bando su Jumis „draugiškai“ bendrauti, siunčia Jums „prašytą“ dokumentą;
- Laiško antraštė (arba turinyje pateikiama nuoroda) siūlo Jums pamatyti sensacingą informaciją, bando vilioti arba gąsdinti (tarptautinės katastrofos, nukritę lėktuvai, nuogų garsenybių nuotraukos, teisėtvarkos atstovų grasinimai ar pateikiama informacija);
- Prašoma skubiai atidaryti „svarbų Jums“ dokumentą ar nuorodą;
- Viliojama negirdėtomis „akcijomis“, „nuolaidomis“ ar kitais „itin vertingais verslo pasiūlymais“;
- Laiško kalba keista (versta automatizuotų vertimo programų);
- Įspėja Jus apie pasibaigusį slaptažodžio galiojimo laiką ar saugumui iškilusį pavojų (siūlo paspausti nuorodą ir prisijungti prie svetainės pasitikrinti „ar viskas gerai“);
- Siūlo laisvalaikio pramogas, filmukus, nuotraukas ar žaidimus.

Kiti patarimai (1)

- Legalios programinės įrangos ir operacinės sistemos naudojimas
- Saugos programų naudojimas
- Savalaikis naudojamos programinės įrangos atnaujinimų diegimas
- Svarbių duomenų ir dokumentų kopijos turi būti saugomos atskirai nuo sistemos
- Sudėtingų slaptažodžių naudojimas ir jų periodiškas keitimas (nenaudokite tų pačių slaptažodžių skirtingose sistemose)
- Visada įvertinti informacijos jautrumą prieš jos siuntimą paštu ar įkėlimą į „debesėlį“
- Neteikite perteklinės asmeninės informacijos internete ar socialiniuose tinkluose
- Jei kolega staiga atsiuntė netikėtą prašymą ar prašo veiksmų, kurie gali būti lemtingi (pvz.: pervesti pinigų) – pasitikslinkite paklausdami jį telefonu
- Atsiminkite, kad išmanieji telefonai – maži kompiuteriai, jie „paveldi“ visas kompiuterių kibernetines grėsmes
- Naudotojai visada turėtų būti atsargūs ir truputį paranojiški (bet kuris gautas laiškas, dokumentas ar nuoroda gali būti kenksmingas).
- Niekada niekam neduokite savo slaptažodžių (administratoriai niekada to jūsų neklaus, nes jie turi aukštesnio lygmens teises)

Kaip pranešti?

- 1805
- cert@nksc.lt
- www.nksc.lt



Ačiū!

Klausimai?