DNS klientu drošībai

Gints Mālkalnietis

24.11.2022

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Identitāes problēma

lvdpd.shop
lvdpdsafe.xyz ...

Īsts vai viltots?

R: Jauns pasūtījums / preces pieprasījums_V79607

AS [redacted]-SIA "VIA" <info@axz1.xyz>

Kam [redacted]

SIA VIA_P.O_V79607-Doc.zip
146 KB

Labrīt,

Es rakstu, lai pieprasītu cenu par pievienotajiem pasūtītajiem produktiem.

Nosūtiet mums cenas un katalogu, ja tas ir pieejams, lai mēs varētu izvēlēties paši.

Lūdzu, šis pasūtījums ir steidzams.

Mums ir vajadzīgi šie materiāli, lai pabeigtu klienta projekta darbu.

Gaida savlaicīgu atbildi.

Ar laba vēlējumiem,

Ar cieņu / Best regards,

SIA "VIA" akmens apstrādes vadītāja

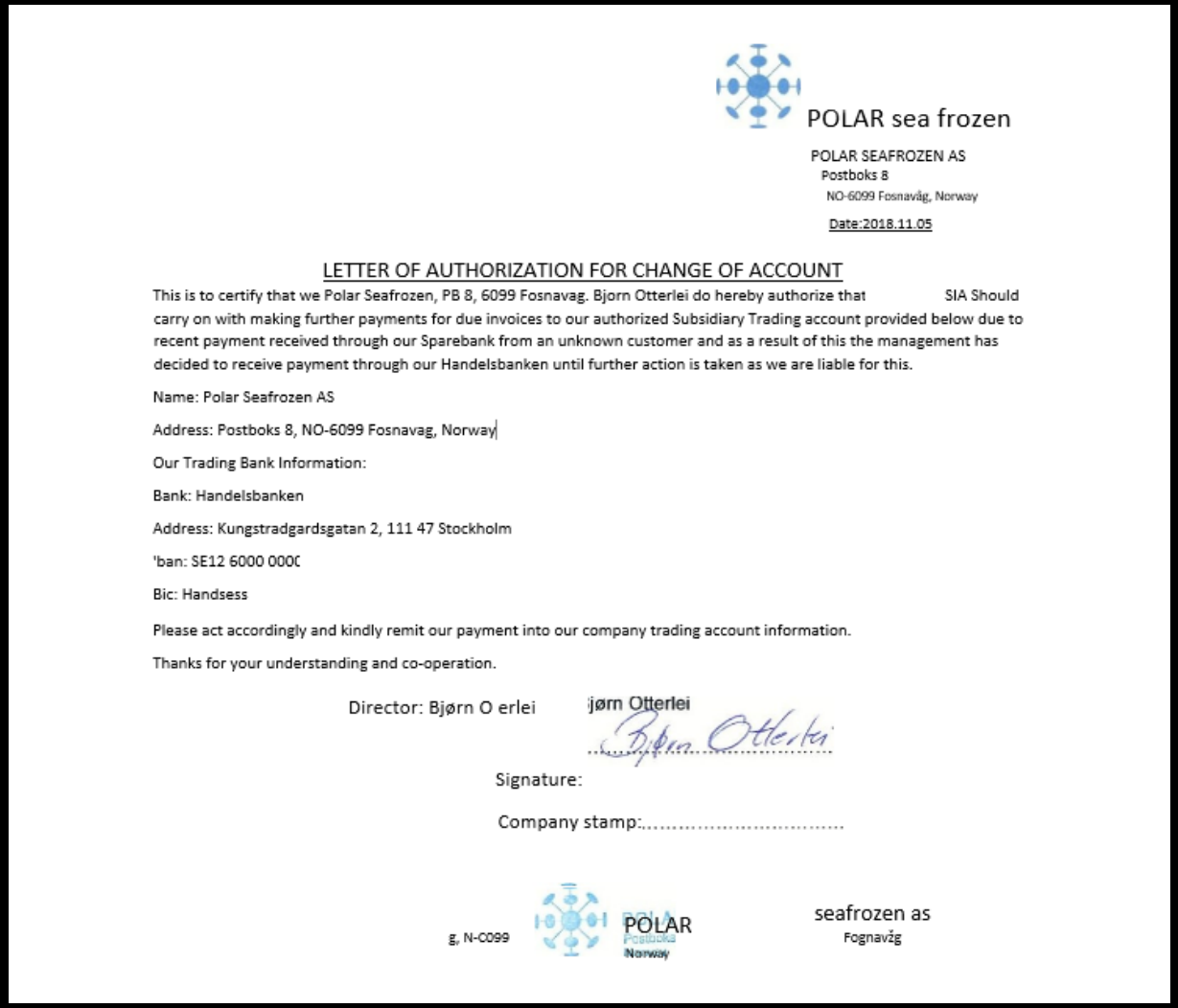
[redacted]

Starta iela 5, Rīga, LV-1026

Mob.: +371 29265380

ww.akmens-virsmas.lv
www.via.com.lv
www.facebook.com/Via.com.lv

Viltoti rēķini



POLAR sea frozen

POLAR SEAFROZEN AS
Postboks 8
NO-6099 Fosnavåg, Norway

Date:2018.11.05

LETTER OF AUTHORIZATION FOR CHANGE OF ACCOUNT

This is to certify that we Polar Seafrozen, PB 8, 6099 Fosnavag. Bjorn Otterlei do hereby authorize that SIA Should carry on with making further payments for due invoices to our authorized Subsidiary Trading account provided below due to recent payment received through our Sparebank from an unknown customer and as a result of this the management has decided to receive payment through our Handelsbanken until further action is taken as we are liable for this.

Name: Polar Seafrozen AS

Address: Postboks 8, NO-6099 Fosnavag, Norway

Our Trading Bank Information:

Bank: Handelsbanken

Address: Kungstradgardsgatan 2, 111 47 Stockholm

'ban: SE12 6000 000(

Bic: Handsess

Please act accordingly and kindly remit our payment into our company trading account information.

Thanks for your understanding and co-operation.

Director: Bjørn O erlei jørn Otterlei

Signature:

Company stamp:.....

g, N-C099 POLAR Norway seafrozen as Fognavåg

Zaudējumi

Latvijā ir gan veiksmīgi izkrāptas ar 6 cipariem rakstāmas summas, gan savlaicīgi apturētas tik pat lielas transakcijas
Dominē gadījumi no 10 – 100 tūkstoši EUR
Garākais CERT.LV zināmais reakcijas laiks – 11 mēneši

- ✓ Jo ātrāk izdodas atklāt krāpšanu – jo labākas iespējas atgūt naudu
- ✓ Krāpniekiem ir vienalga, kura darījumu partnera e-pastā ielauzties
- ✓ Cilvēcīgais faktors – vēl arvien labākais veids, kā atklāt krāpšanu ir apmācīti un gana aizdomīgi darbinieki!

Aizsardzība pret e-pastu viltošanu

- E-pasts pamati ir noteikti RFC 821 , 1982. gada protokolu kurā NAV aizsardzības pret e-pastu viltošanu
- Saskaroties ar e-pasta viltošanas problēmu, ieviestas dažādas papildus tehnoloģijas:
- SPF – 2006. gads
- DKIM – 2007. gads
- DMARC- 2015. gads

Aizsardzība pret e-pastu viltošanu -SPF

SPF – vecākais, populārākais un visvienkāršākais, nepieciešams tikai viens DNS ieraksts!

Tipiskākās kļūdas to ieviešot:

1) Vairāk kā viens SPF ieraksts katram domēnam
2) Pārbaudot SPF ierakstu, tiek pārsniegts 10 DNS pieprasījumu limits (10 pieprasījumos jāiekļaujas pārbaudot arī iekļautos apakšierakstus)
3) Ierakstam jābūt īsākam par 255 zīmēm (var apiet izmantojot «include»)
4) Ieraksts satur neeksistējošus DNS vārdus
5) Ierakstā norādīti MX (ienākošie) serveri, nevis izejošie SMTP serveri

Aizsardzība pret e-pastu viltošanu -SPF

6) Ierakstā iekļauti serveri, kas netiek izmantoti e-pastu izsūtīšanai (visi domēna MX un A ieraksti)
7) SPF ir ierakstīts, pareizs, bet netiek reāli izmantots – ieraksts pabeigts ar nosacījumu +all
8) Tāpat bieži bezjēdzīgs ir nosacījums ~all, jo viltotie e-pasti tāpat veiksmīgi sasniedz adresātu (tiem jātiek marķētiem, bet katra e-pasta servera konfigurācijā to var definēt dažādi, vai ignorēt)

Aizsardzība pret e-pastu viltošanu -DKIM

- Sarežģītāks ieviešot par SPF
- DKIM parakstam jābūt pievienotam katrā no izsūtīšanai izmantotajām sistēmām (jāsūta caur vienu izejošo serveri, vai katrai sistēmai jāveido sava DKIM atslēga)
- Izmantojot `l=` tegu paraksts tiek veidots izmantojot tikai daļu no vēstules, iespējams pievienot tekstu esošai vēstulei un tā DKIM paraksts vēl arvien būs valīds

MK noteikumi 442

15.15. sistēmās, kas nodrošina elektroniskā pasta saņemšanu no ārējiem resursiem, ienākošo saziņu apstrādā vismaz atbilstoši e-pastu autentifikācijas protokola (DMARC) prasībām, ieviešot e-pasta apstrādi atbilstoši sūtītāja domēna vārda DMARC politikai, atskaites ģenerēšanu un nosūtīšanu DMARC konfigurācijā norādītajam kontaktam;
15.16. institūcija, kas ir elektroniskā pasta domēna īpašnieks, publicē DMARC atbilstošu ierakstu savā domēna vārdu sistēmā (DNS), norādot striktu atteikuma politiku (p=reject), ievieš procedūru DMARC ziņojumu saņemšanai un to analīzei;

DMARC ieviešana

- Ieviešana jāsāk ar SPF vai DKIM tehnoloģijām, jo DMARC pieprasa, ka katrs leģitīmi izsūtītais epasts ir aizsargāts vismaz ar vienu no tām.
- Ir ieteicams izmantot DKIM + DMARC vai SPF + DKIM + DMARC kombināciju, jo SPF + DMARC (bez DKIM) var sagādāt piegādes traucējumus vairākos scenārijos (visbiežākie - epastu pārsūtīšana un meilinglistes).
- Lai gan DKIM + DMARC konfigurācija no drošības perspektīvas ir tikpat droša kā SPF + DKIM + DMARC (un dažreiz pat drošāka dēļ tā, ka SPF ierakstos nākas iekļaut mazāk uzticamus serverus), praksē bieži vien nav iespējams izvairīties no SPF.

DMARC ieviešana

- Izmantojot SPF + DKIM + DMARC konfigurāciju, tik un tā jārēķinās ar to, ka daļa sūtītāju būs spējīgi validēt tikai SPF.:
- Saņēmēji, kas neatbalsta DMARC, validēs SPF pēc tā oriģinālās specifikācijas, neizmantojot DMARC ieviesto papildus prasību par Envelope Sender' un Originator (parasti 'From' header'is) alignment.
- Ja visi uzņēmuma e-pasti tiek korekti pasargāti ar DKIM, tad daļa no tiem varētu arī noteiktos apstākļos nākt no serveriem, kas nav iekļauti SPF ierakstā. Tas var notikt kļūdas pēc vai arī uzsākot e-pastu izsūtīšanu no jaunas vietas (kas ir pasargāta ar DKIM, bet serveri netika ievietoti SPF ierakstā). Šajā gadījumā saņēmēji, kas spēj validēt DMARC, turpinās saņemt visus e-pastus, bet tie saņēmēji, kas spēj validēt tikai pliku SPF, daļu e-pastu var nesaņemt. Šādi piegādes traucējumi var nebūt pamanīti uzreiz un tad, kad tas ir pamanīts, to cēloni var būt visai grūti izskaidrot.

Domēna vārdi kas netiek izmantoti e-pastam

Ieteicams domēna vārdiem, kurus neizmanto e-pasta sarakstei, izveidot šādus ierakstus:

DMARC: 'v=DMARC1; p=reject'
SPF: 'v=spf1 -all'

DNSSEC

Visi izmantotie e-pasta aizsardzības mehānismi, paļaujas uz to, ka klienta saņemtā DNS servera atbilde ir korekta, bet eksistē uzbrukumi kā:

- DNS cache poisoning
- Dažāda veida DNS spoofing

kuri var pārveidot korekto DNS servera atbildi

DNSSEC izmanto kriptogrāfiski parakstītas DNS atbildes, lai apstiprinātu zonas servera autentiskumu un aizsargātu tās pret izmaiņām transporta laikā

Dnsmuris.lv


https://dnsmuris.lv
Par DNS ugunsmūri
Instrukcijas
Nē karam Ukrainā!
#StandWithUkraine
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija
NIC
DNS
ugunsmūris
JUMS IR AKTĪVS

Dnsmuris.lv

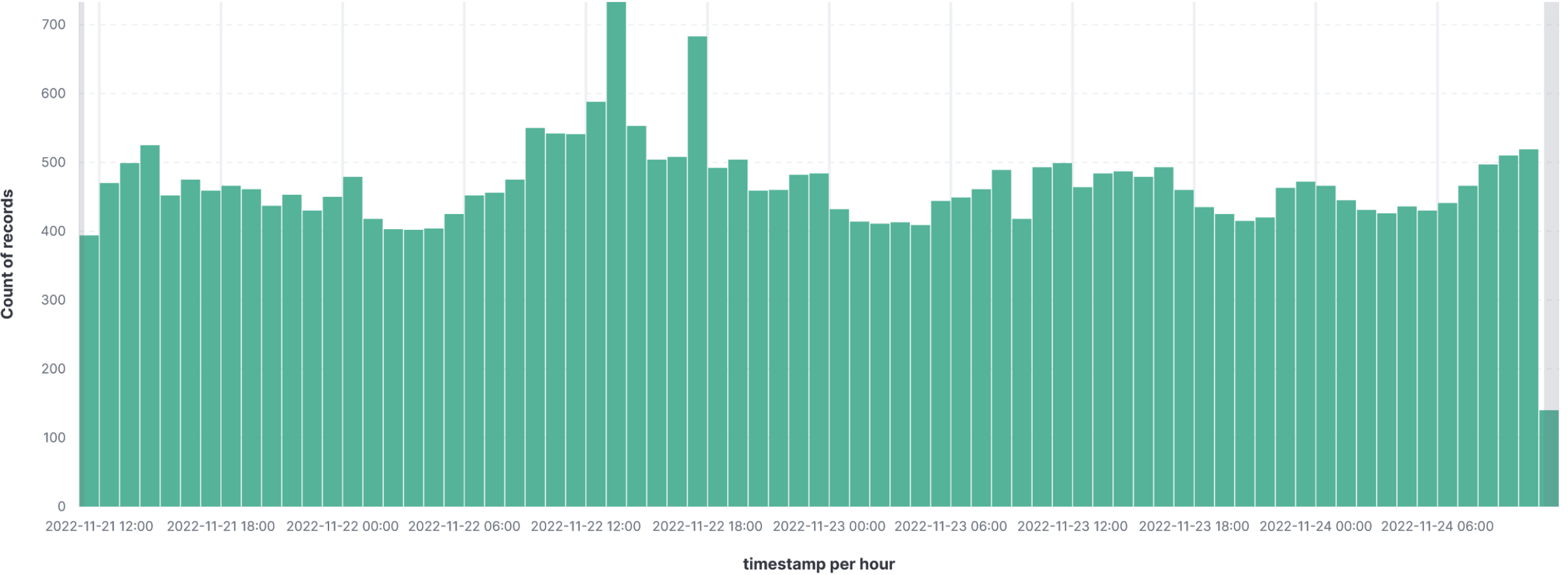
- DNS RPZ serviss
- Tiek regulāri un ātri ievietoti Latvijas kibertelpā identificētie apdraudējumi:

✓ Pikšķerēšanas vietnes
✓ Krāpnieciskas vietnes
✓ Datorvīrusu izplatīšanā iesaistīti resursi

- Lietotāji no piekļuves kaitīgajam saturam tiek pasargāti uzreiz, nav jāgaida uz mitinātāja atbildi
- Pirms pievienošanas dnsmuris.lv vietnes tiek pārbaudītas, netiek pievienoti vispārzināmu pakalpojumu sniedzēju domēna vārdi, vietnes ar kuru uzturētājiem iespējams nekavējoties sazināties.

CERT.LV

Dnsmuris.lv



Dnsmuris.lv

- Ir iespējams preventīvi identificēt krāpniecībā izmantotos resursus un tos bloķēt (DGA veidotie domēna vārdi, datorvīrusu konfigurācijā iekļautie domēna vārdi, pikšķerēšanas kampaņās izmantotie)
- Aktīvu pikšķerēšanas kampaņu gadījumā bloķēto pieprasījumu skaits var sasniegt vairākus simtus stundā, katram domēnam.
- Domēna vārdi dnsmuris.lv tiek ievietoti uz noteiktu laiku, jo aktīva ļaunatūras izplatīšana un citas darbības, visbiežāk, ir neilga

Paldies!

https://www.cert.lv
gints@cert.lv
Gints Mālkalnietis