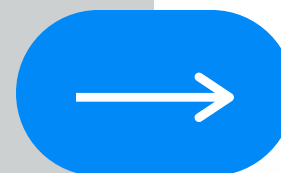




MKD-CIRT

Early warning

Free service to inform organizations of **cyber threats in their networks** as soon as possible



Background

MKD-CIRT is subscribed to multiple commercial and free threat intelligence vendors that provide feeds for network traffic on the territory of the Republic of North Macedonia.





The threat intelligence feeds contain information about:

- IP addresses based in North Macedonia that were **source** of cyber attacks
- IP addresses based in North Macedonia that were **destination** of cyber attacks
- Type of cyber attack related to the affected IP address: DDoS, Brute Force, Malware etc.

Example 1

Company A owns a server that is infected by a malicious bot **is not aware** that its server is used as a bot within a botnet “army” to cause DDoS attacks to another server.



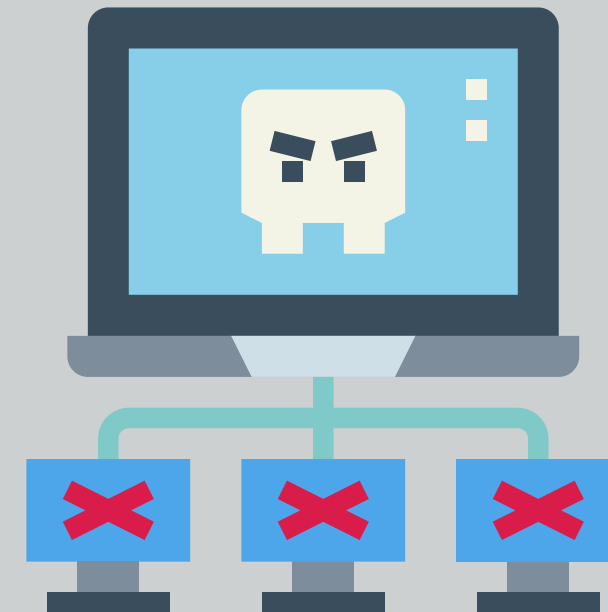
Company A is a source of
attack

Example 2

Company A owns an ecommerce store that is subject to attack that disrupts its operations and increases the cloud computing costs



Company A is a destination of attack



So while we had the data,
we were not sure how to best utilize it.

We were inspired by use-cases built by the
British and German Cyber Security authorities.

earlywarning.service.ncsc.gov.uk
reports.cert-bund.de



National Cyber
Security Centre



The result of this effort is a new
Early Warning Service
coming in North Macedonia



[Најави се](#) | [Регистрирај се](#) | [Извештаи](#)

Рано предупредување за сајбер закани

Национален центар за одговор на компјутерски инциденти (MKD-CIRT) овозможува бесплатен сервис наменет за информирање за потенцијални сајбер закани наменет за организации од јавниот и приватниот сектор.

Што претставува овој сервис?

Системот за рано предупредување процесира фидови од различни извори, вклучително и од комерцијални провајдери, кои се однесуваат на сајбер инциденти кои инволвираат IP адреси од Република Северна Македонија. При тоа, доколку некој од системите на вашата организација е вклучен во сајбер инцидент кој е детектиран од страна на некој од фидовите кои ги процесира сервисот, вашата организација ќе биде веднаш информирана за истото.

Како функционира сервисот?

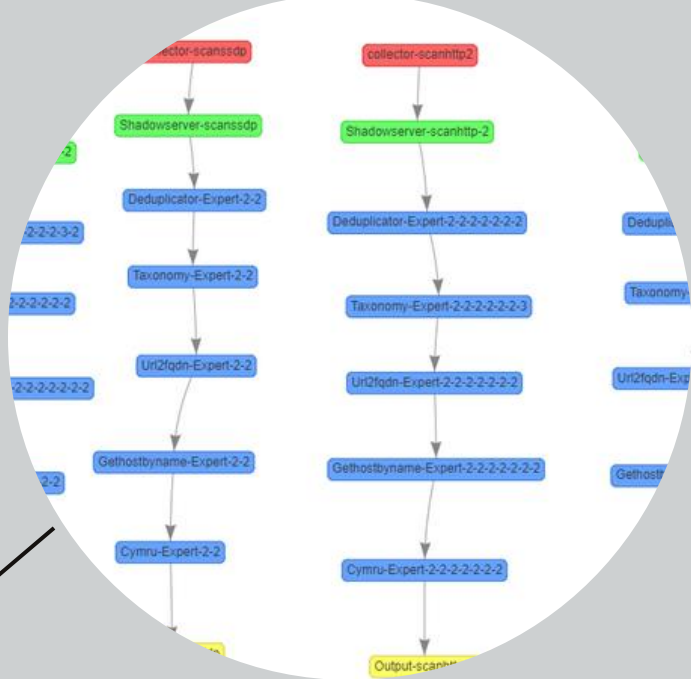
Најпрво, потребно е да креирате организациски профил. При тоа, во рамки на организацискиот профил внесувате податоци за IP адреси кои ги користи вашата организација. На пример, виртуелни машини, сервери и слично. Во рамки на сервисот можете да внесете повеќе адреси – истиот нема ограничување на бројот на IP адреси, но истите мора да се исклучиво користени од ваша страна. Нашите колеги ќе ги верификуваат податоците и ќе го активираат организацискиот профил.

Во случај на сајбер инцидент поврзан со некој од системите кои ги имате внесено во организацискиот профил, сервисот ќе испрати нотификација преку е-пошта од типот на:

- **Известување за инцидент** – Активност која укажува на ваш компромитиран систем.
На пример, вашата IP адреса е вклучена во DDoS Напад.
- **Инцидент на мрежно ниво** – Некој во вашата мрежа е дел од Ботнет.
- **Алерт за потенцијална ранливост** – Детектирана е отворена порта во вашата мрежа која може се искористи за сајбер напад.

How does it work?

Data is enriched in IntelMQ



REGISTER

Organization registers for the service

ENTER IP ADDRESS/RANGE

Enters static IP address it owns

APPROVED



e-mail notification

dashboard with data overview of all feeds where the IP of the organization is detected

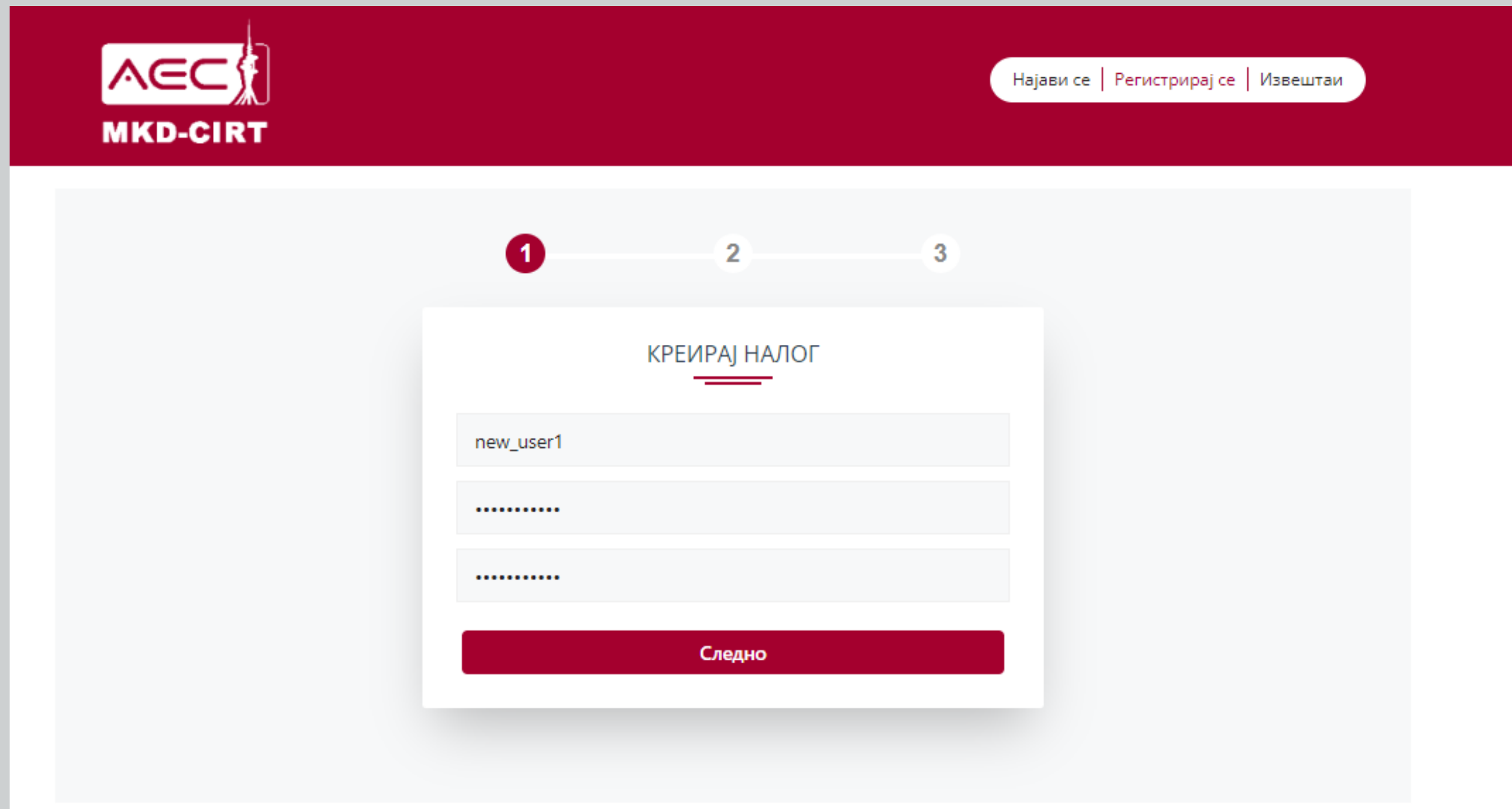


Live
Demo

Slide
s

Step 1

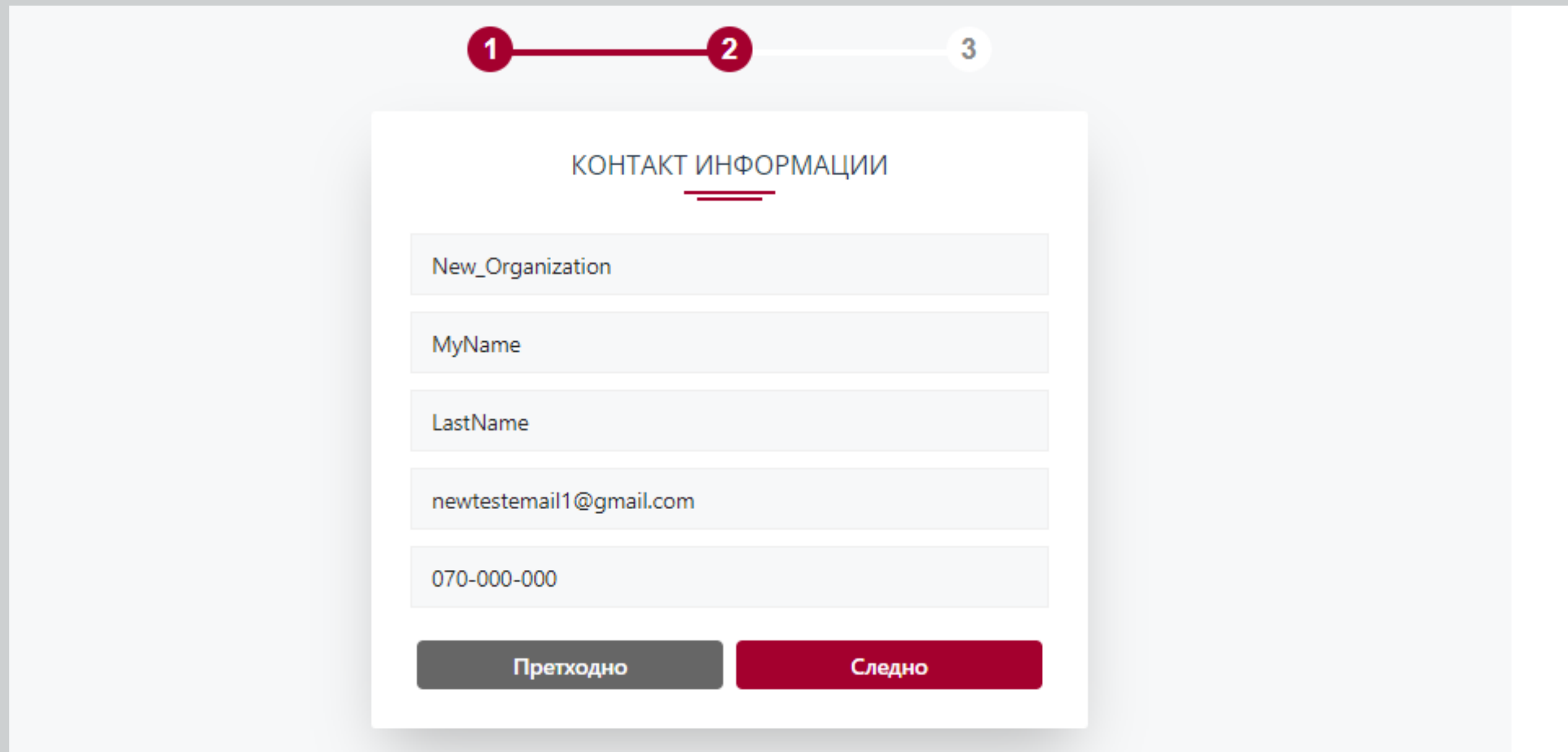
The organization registers a new account.



The screenshot displays the registration interface for AEC MKD-CIRT. At the top left is the logo with the text "AEC MKD-CIRT". At the top right, there are navigation links: "Најави се | Регистрирај се | Извештаи". Below the header is a progress indicator with three steps: "1" (highlighted in red), "2", and "3". The main content area is titled "КРЕИРАЈ НАЛОГ" (Create Account) and contains three input fields: the first contains "new_user1", the second and third are masked with dots. A red "Следно" (Next) button is positioned at the bottom of the form.

Step 2

Fill out organizational information. АЕК, MKD-CIRT at a later stage validates the information.



1 — 2 — 3

КОНТАКТ ИНФОРМАЦИИ

New_Organization

MyName

LastName

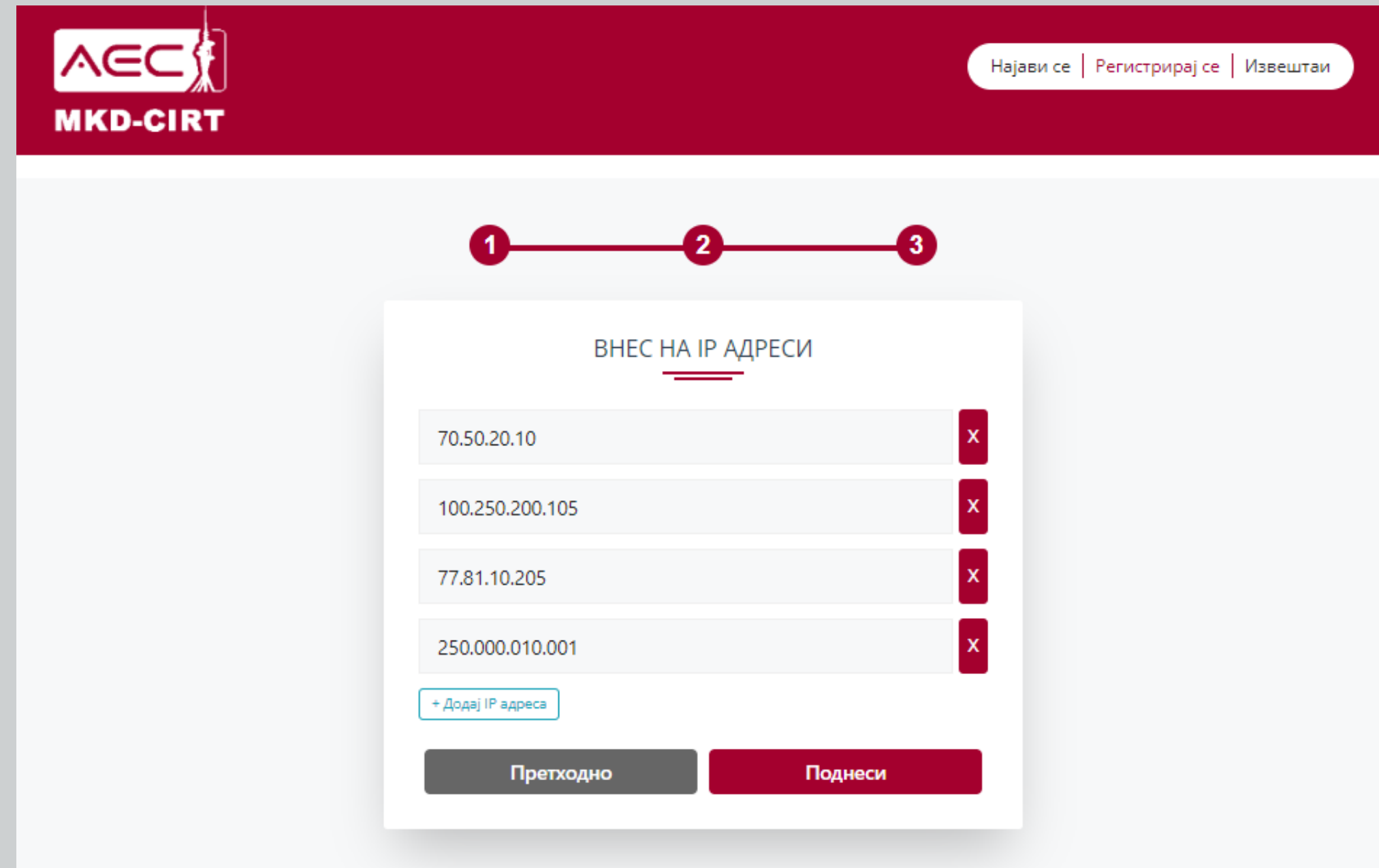
newtestemail1@gmail.com

070-000-000

Претходно Следно

Step 3

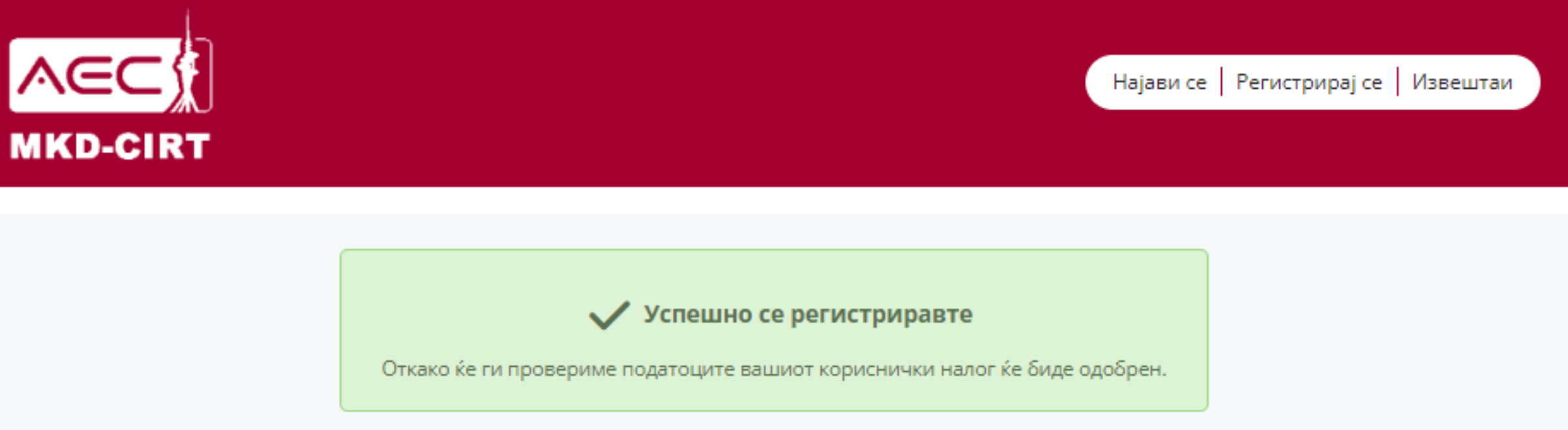
The organization fills in the IP addresses it owns (web applications, servers, mail servers etc).



The screenshot shows the AEC MKD-CIRT website interface. At the top left is the logo for AEC MKD-CIRT. At the top right are links for 'Најави се' (Log in), 'Регистрирај се' (Register), and 'Извештаи' (Reports). Below the header is a progress indicator with three steps, where step 3 is currently active. The main content area is titled 'ВНЕС НА IP АДРЕСИ' (IP Address Entry). It features a list of IP addresses, each with a delete button (X):

70.50.20.10	X
100.250.200.105	X
77.81.10.205	X
250.000.010.001	X

Below the list is a button '+ Додај IP адреса' (Add IP address). At the bottom of the form are two buttons: 'Претходно' (Previous) and 'Поднеси' (Submit).



MKD-CIRT needs to approve the account. And it's all set.

What does the user get?

In case one of the IP addresses provided by the organization / user gets detected with the threat feeds that MKD-CIRT retrieves daily, the user will be notified by **1) e-mail (left side)** and will get access to the data details through an **2) application (right side)**

Alert: Suspicious Activity Detected

PI Thu, 21 Sep 2023 12:21:27 PM +0200

To

Tags

Security TLS Learn more

Subject: Alert: Suspicious Activity Detected from IP Address 146.255.83.90

Dear

We are reaching out to notify you about suspicious activity detected from the IP address 146.255.83.90. Our security systems have flagged this activity as a potential threat to the security of your account or network. Please review the details below:

Description: Our monitoring systems detected unauthorized access attempts or suspicious behavior originating from the mentioned IP address.

Additional Information:
([{"feed.url": "file://localhost/tmp/shadowserver/latest/device_id/2023-09-17-device_id-macedonia-geo.csv", "extra.tag": "ftp", "feed.name": "File", "source.ip": "146.255.83.90", "source.asn": 34547, "source.port": 21, "time.source": "2023-09-17T13:43:31+00:00", "feed.accuracy": 100.0, "feed.provider": "shadowserver", "source.as_name": "TELESMART-AS, MK", "source.network": "146.255.80.0/22", "source.registry": "RIPE", "source.allocated": "2011-07-19T00:00:00+00:00", "time.observation": "2023-09-19T07:47:16+00:00", "extra.device_type": "web-panel", "protocol.transport": "tcp", "classification.type": "undetermined", "extra.device_vendor": "BT", "source.geolocation.cc": "MK", "classification.taxonomy": "other", "source.geolocation.city": "SKOPJE", "classification.identifier": "device-id", "source.geolocation.region": "CENTAR"}]);

Best regards,

AEC MKD-CIRT Кориснички профил | Одјави се | Извештаи

IP извештај | Кориснички податоци | Опис на извештаи

Пребарај...

Source IP: 46.217.249.126 | Destination IP: 195.123.208.126 | Server: Shadowserver

Бр.	Параметар	Вредност
1	feed.name	Honey-pot-Brute-Force-Events
2	source.ip	46.217.249.126
3	source.asn	41557
4	source.port	50472
5	time.source	2023-09-18T02:11:42+00:00
6	malware.name	telnet-brute-force
7	feed.accuracy	100
8	feed.provider	shadowserver
9	destination.ip	195.123.208.126
10	extra.end_time	2023-09-18T02:11:57.158824+00:00
11	source.as_name	TELEKABEL-AS, MK
12	source.network	46.217.248.0/22
13	destination.asn	50979
14	source.registry	RIPE

Benefits for the registered organizations

1

The organization can prevent infected devices within its own network

2

The organization indirectly prevents the threats to spread to other organizations

Benefits for the country

1

Data collected gives us an opportunity for automated statistical analysis of the threats we are facing

2

Better cyber defense and improved cyber security awareness

**Thank you for the time and
attention!**



Sevdali Selmani

Head of MKD-CIRT

sevdali.selmani@aec.mk

+389 (72) 220-625