REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

KONFERENCA ZInfV-1
ZAKON ZA KIBERNETSKO VARNO PRIHODNOST SLOVENIJE

URSIV

13. oktober 2025
Brdo pri Kranju

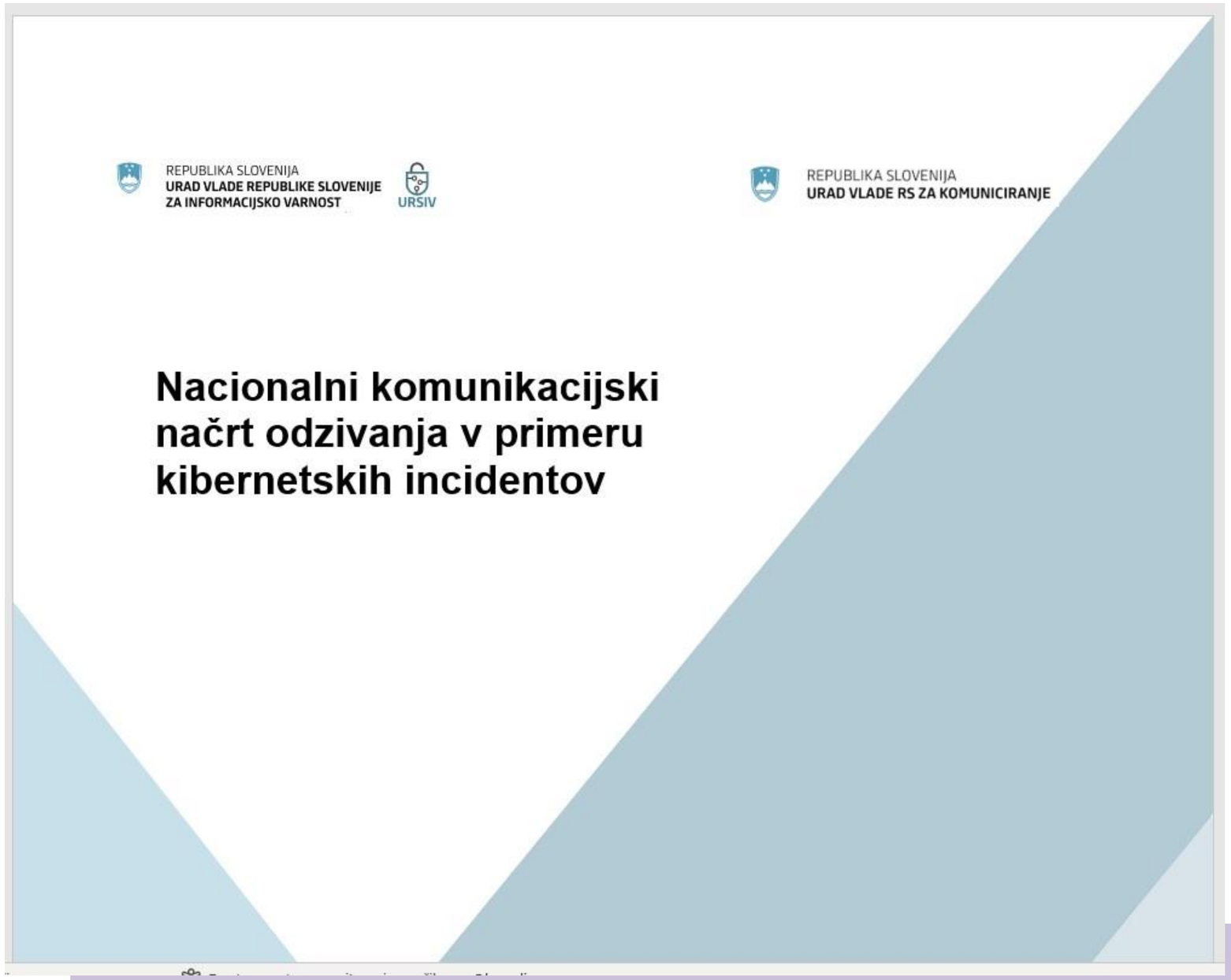
KOMUNICIRANJE Z JAVNOSTJO V PRIMERU KIBERNETSKIH INCIDENTOV

Sektor za mednarodne zadeve in odnose z javnostmi
pr.uiv@gov.si

pr.uiv@gov.si

T: 01 478 86 52

URSIV



z domačo in tujo javnostjo v primeru kibernetskih incidentov.

:://www.gov.si/assets/vladne-sluzbe/URSIV/PR/Nacionalni-komunikacijski-nacrt-odzivanja-v-primeru-kibernetskih-incidentov_URSIV_UKOM.pdf

ZInfV-1

10. člen (pristojni nacionalni organ):

(2) Pristojni nacionalni organ izvaja naslednje naloge:

13. strokovne in svetovalne naloge in naloge koordinatorja na področju odnosov z javnostmi, ki zajemajo komunikacijo z zunanjimi in notranjimi javnostmi ter **krizno komuniciranje v primeru incidenta**.

14. v sodelovanju s službo vlade, pristojno za komuniciranje z javnostmi, izdela in vzdržuje **nacionalni načrt komuniciranja v primeru incidentov.**

URSIV

12. člen (organ za obvladovanje kibernetskih kriz):

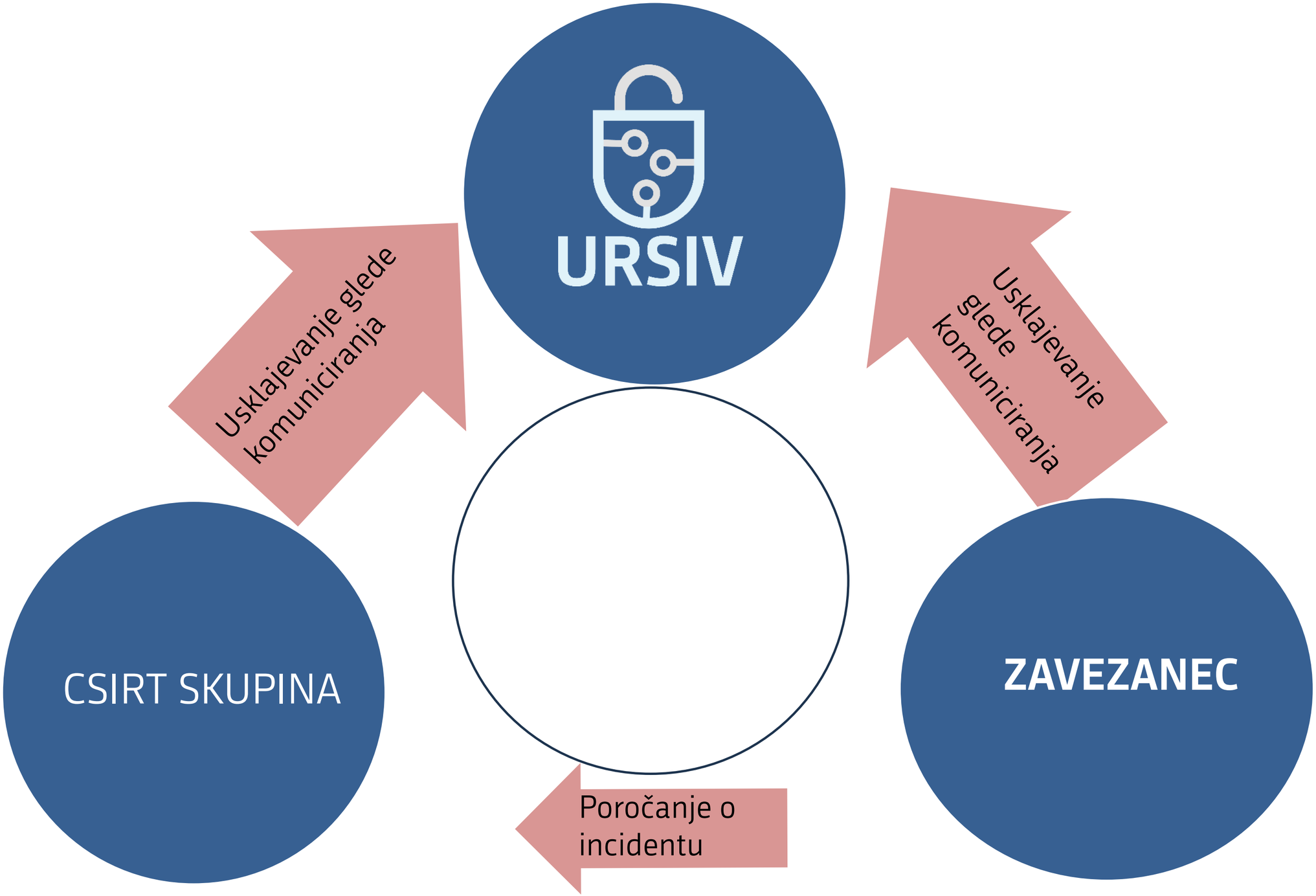
(7) Če je treba v zvezi z izvajanjem tega člena obvestiti tudi javnost, pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, **pripravi sporočilo za javno objavo, ki ga smejo mediji objaviti le v nespremenjeni obliki.**

URSIV

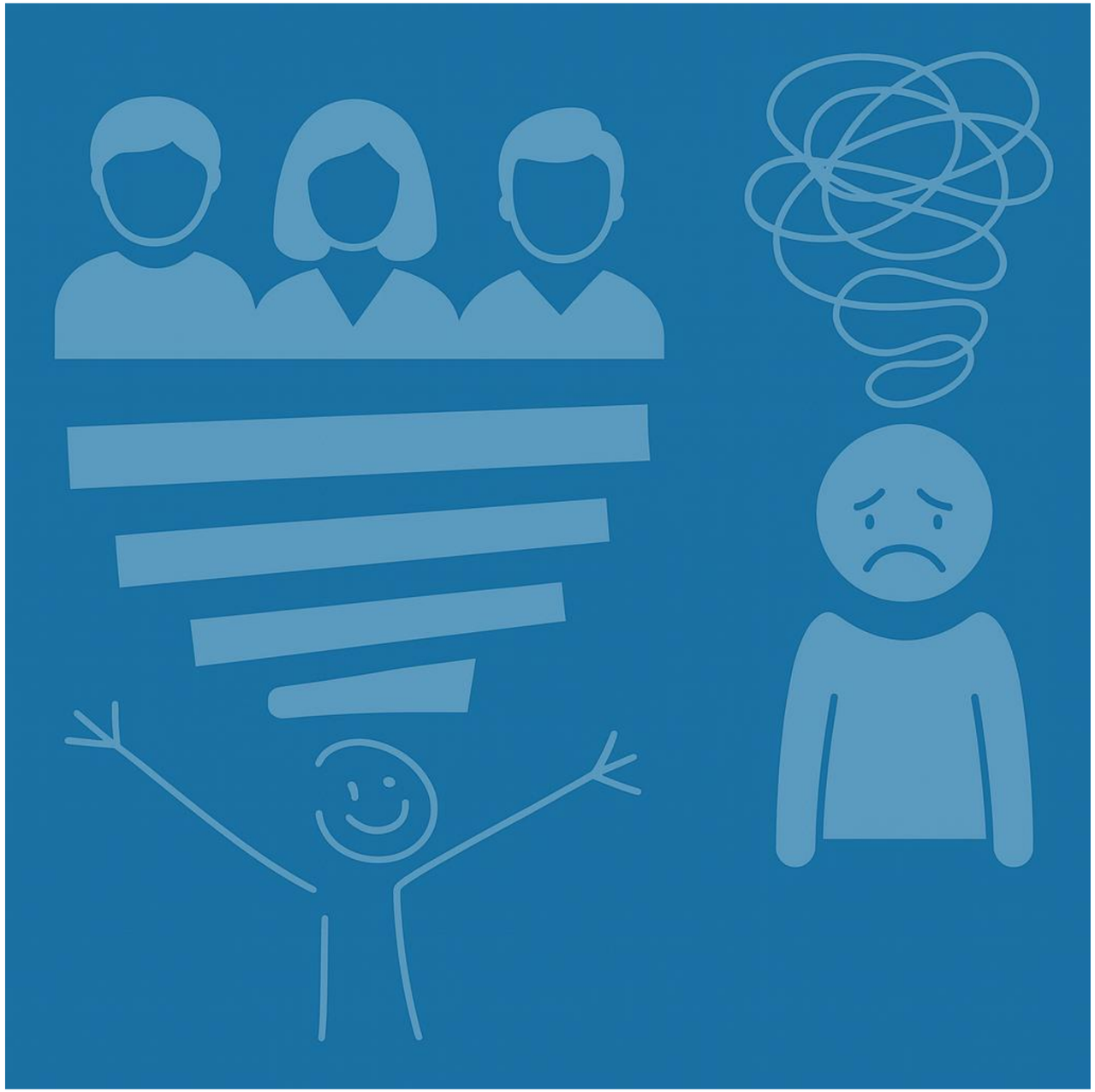
30. člen (postopek priglasitve pomembnih incidentov):

(6) Kadar je ozaveščenost javnosti potrebna za preprečitev pomembnega incidenta ali obravnavo pomembnega incidenta, ki še poteka, ali kadar je razkritje pomembnega incidenta kako drugače v javnem interesu, **pristojni nacionalni organ po posvetovanju z zadevnim zavezancem obvesti javnost o pomembnem incidentu ali zahteva, da to stori zavezanec**. Predlog za takšno obveščanje lahko pristojnemu nacionalnemu organu poda tudi pristojna skupina CSIRT.

URSIV


URSIV
Usklajevanje glede komuniciranja
Usklajevanje glede komuniciranja
CSIRT SKUPINA
ZAVEZANEC
Poročanje o incidentu

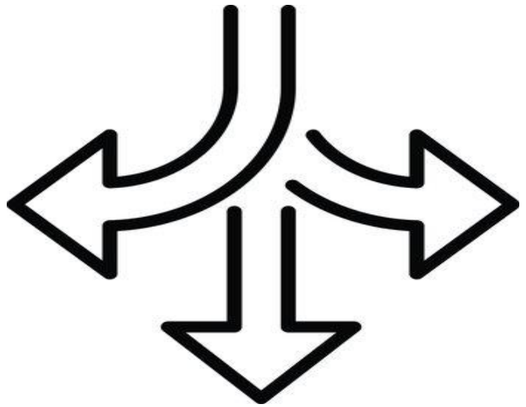
ZAKAJ JE POMEMBNO USKLAJENO KOMUNICIRANJE?



URSIV

Javnost mora biti o kibernetskem incidentu obveščena
pravočasno, **celovito** in **objektivno**,
na način, ki je dostopen in razumljiv vsem.

Podajanje konteksta!



OZAVEŠČANJE IN OPOZARJANJE NA PRETEKLE INCIDENTE

Seznanjanje javnosti s preteklimi izkušnjami, nevarnostmi in ukrepi za preprečevanje nastanka novih kibernetskih incidentov.

PREPREČEVANJE STOPNJEVANJA INCIDENTA

Obveščanje javnosti o trenutnem kibernetskem incidentu, ki se že upravlja in zanj obstaja nevarnost, da preide v višjo stopnjo, kot je trenutno, na kar lahko vplivajo tudi aktivnosti javnosti v kibernetskem prostoru.

NEVARNOST NOVIH ENAKIH ALI PODOBNIH DOGODKOV

Obveščanje javnosti o kibernetskem incidentu, ki se trenutno upravlja, je ustavljen oziroma je v zaključnih fazah upravljanja in zanj obstaja nevarnost, da bi se zaradi aktivnosti javnosti razširil ali ponovil še pri katerem od zavezancev.

URSIV

VSI KLJUČNI AKTERJI MORAJO GOVORITI Z ENIM GLASOM

- Načela preprečevanja škodovanja dobremu imenu zavezanca, ki ga je kibernetski incident prizadel
- Varovanje podatkov o preiskavi incidenta
- Zagotavljanje varnosti
- Potrebe po ozaveščanju in varovanju osebnih podatkov prebivalstva

OBSEG IN NAČIN OBVEŠČANJA JAVNOSTI

URSIV

KAJ LAHKO POVEMO?

„Potrdimo lahko, da je do incidenta prišlo.“

„Zaradi interesa preiskave v tem trenutku dodatnih informacij ne moremo posredovati.“

SEZNAM MOŽNIH VPRAŠANJ:

Kako resna je grožnja?

Ste prejeli zahtevo za odkupnino?

Ali je incident nacionalen ali mednaroden?

Kako se je to zgodilo?

Kolikšni so ocenjeni stroški?

Kje lahko ljudje poiščejo pomoč?

Kdo je odgovoren za nastalo situacijo?

Je prišlo do kraje podatkov?

Kakšno škodo lahko incident povzroči?

Kateri sistemi so ranljivi, prizadeti in trenutno ne delujejo?

Kako lahko preprečite, da se to ne bi ponovilo?

Ali veste kdo stoji za napadom?

URSIV

- Preprost in razumljiv jezik
- Doslednost – vsi predstavniki uporabljajo enako terminologijo in podatke
- Prvo sporočilo hitro – tudi če še niso znani vsi podatki (“preiskava še poteka”).
- Preprečevanje panike / dezinformacij v javnosti
- Redne posodobitve informacij
- Zagotavljanje uradnih virov informacij
- Empatija in odgovornost za prizadete deležnike
- Konsistentnost
- Koordinacija med organi
- Ena uradna govorna oseba – zagotavlja enoten ton in izogiba se kontradiktornim izjavah
- Podprto z dokazi – vsako sporočilo temelji na preverjenih informacijah
- Popravljanje napak – če pride do napačne izjave, se jo hitro in odkrito popravi
- Dokumentiranje komunikacije – vse izjave in objave se hranijo za naknadno analizo.
- Povratne informacije in izboljšave
- Spremljanje odziva javnosti – analiza medijskega odziva in družbenih omrežij

URSIV

ELEMENTI KOMUNIKACIJSKEGA NAČRTA

- Vnaprej določen postopek – kdo odloča in kdo komunicira
- Skupina za krizno komuniciranje– vzpostavljeni varni kanali za komuniciranje
- Identifikacija ciljnih občinstev (notranji zaposleni, uporabniki, partnerji, regulatorji, mediji, širša javnost)
- Usmerjanje zaposlenih: kaj lahko in česa ne smejo komunicirati
- Vnaprej vzpostavljeni kanali – krizne telefonske linije, medijski kontakti, družbena omrežja
- Priprava uradnih izjav
- Obveščanje partnerjev, strank, regulatorjev
- Scenariji možnih kriznih situacij
- OFFLINE BACKUP pomembnih dokumentov in kontaktov!

URSIV

PRIPISOVANJE ODGOVORNOSTI

Pri obvladovanju kriznih situacij bodite hitri z dejstvi in počasni z obtožbami.

— Leonard Saffir, izvršni direktor za odnose z javnostmi

Na nacionalni ravni je določen medresorski postopek za pripisovanje odgovornosti v primeru kibernetskih incidentov, nobena entiteta ne sme odgovornosti pripisovati sama.

URSIV

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

HVALA ZA POZORNOST

URSIV
KIBERNETSKO VARNI