EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ODZIVANJE IN OBNOVITEV-VAJA

VSEBINA

Omejitev, zajezitev in odstranitev grožnje.

Obnova delovanja sistemov in storitev.

Poročanje in komuniciranje.

Sodelovanje in odločanje.

POTEK VAJE

Vaja je osredotočena na omejitev napada, odstranitev grožnje in obnovitev sistemov in storitev.

Udeleženci zdaj nastopate kot krizna ekipa za odziv na incident, ki mora ukrepati hitro in usklajeno.

Vaja pokriva prvih nekaj ur in dni po incidentu ter aktivnosti do zaključka incidenta, vključno s pripravo poročil za SI-CERT in SIGOV-CERT (72 ur) in končnega poročila (1 mesec)

POVZETEK INCIDENTA IZ PREJŠNJE VAJE

Email sporočilo z okuženo priponko

Email sporočilo s strani Finančne uprave RS, en uporabnik odpre priponko in s tem sproži sosledje zlonamernih akcij.

Iznos podatkov

Z dvigom privilegijev uporabniškega računa in zlonamernim programom napadalec izvede iznos podatkov.

Sprožitev ransomware

V zadnjem koraku napadalec sproži ransomware kodo in zašifrira podatke na strežnikih in delovnih postajah.

IMAMO INCIDENT, KAJ ZDAJ ?

Imamo plan, sledimo mu!

Če smo naredili domačo nalogo, vnaprej premislili scenarije in jih tudi dokumentirali, nam bo veliko lažje.

Velik incident je velik stres v vsakem primeru.

Sicer pa smiselno sledimo tem korakom

- Zajezimo širitev škodljivega delovanja, napadalcu prekinimo dostop, izoliramo, izključimo sisteme, ocenimo resnost.
- Onemogočimo, odstranimo zlonamerne programe in nastavitve.
- Obnovimo sisteme, podatke in storitve, brez plačila napadalcem.
- V vseh fazah primerno komuniciramo z vsemi deležniki, notranjimi in zunanjimi.
- Poročamo skladno z obveznostmi.
- V vseh fazah analiziramo dogodke in artefakte, hranimo forenzične podatke.
- Ko se prah poleže izvedemo temeljito analizo in potegnemo nauke.

ZAJEZITEV ŠIRJENJA

Aktivacija ekipe

Gre za hud incident, sistemi in storitve ne delujejo.

Kdo se prvi aktivira, kdo vodi, kdo sodeluje, kako poteka informiranje in odločanje?

Prvi ukrepi

Kako ugotoviti žarišče in razširjenost ? Kaj storiti prvo ? Kako daleč iti s prvimi ukrepi ?

Sodelovanje analitikov in IT skrbnikov.

Zaustavili smo širjenje

Prekinili smo internet dostop, izolirali smo okužene naprave, stabilizirali smo stanje. Čas za prvo kavo, analizo stanja, prvo oceno škode in odločitve za nadaljnje korake.

ODSTRANITEV ZLONAMERNIH PROGRAMOV

Analiza vdora

Kje se nahajajo zlonamerni programi in nastavitve in kaj počnejo? Smo zagotovo našli vse?
Vemo vstopno točko in pot napada (TTP)?
Če smo res tako prepričani lahko odstranimo samo artefakte.
Ali so ti artefakti mogoče tudi v varnostnih kopijah?

Forenzična preiskava

Ali rabimo forenzične slike in revizijske sledi tudi za kasnejše analize?
Jih bo zahteval regulator ali policija?

OBNAVLJANJE

Podatki

Vsi podatki v bazah šo šifrirani. Ali so podatki iz varnostnih kopij na voljo ? So res vsi in so uporabni? Od kdaj so? Koliko časa bo trajala obnovitev ?

Strežniki

Ali je potrebno strežnike ponovno namestiti, ali je virtualizacija nedotaknjena, imamo slike virtualnih strežnikov? Ali je Microsoft AD sistem kompromitiran?

Storitve

Celoten sistem, ki podpira storitve je treba ponovno „sinhronizirati“ in testirati.

Takojšnji ukrepi utrjevanja

Kritične ranljivosti in pomanjkljivosti se odpravi že v fazi obnove.

Uporabnikom se omogoči dostop po menjavi gesla, vključi se MFA, odstrani se nepotrebne račune, zniža se privilegije,…

DOKUMENTIRANJE

Vodenje dnevnika dejavnosti

- Ali se bomo čez mesec dni še spomnili v vseh podrobnosti?
- Izvedene aktivnosti se sproti beležijo.
- Shranjujejo se artefakti, forenzične slike, dokazila, morebitna komunikacija z napadalci, CTI informacije v zvezi z incidentom.

Vse to koristi pri pripravi poročil, kasnejši analizi, pravnih postopkih, zavarovalniških postopkih itd.

KOMUNICIRANJE

Pomembno! Pomembno! Pomembno!

- Kdo bo komuniciral s kom, s kakšnim namenom, kaj bo sporočal, kako pogosto, prek kakšnih kanalov?
- Ali email sploh dela? Imate račun organizacije na socialnih omrežjih?
- Kako boste komunicirali z zaposlenimi ?
- Strankami, partnerji?
- Kako se boste odzivali na medijske objave, na socialnih omrežjih (tudi zlonamerne)?

POROČANJE

Poročanje je obveznost.

Prvo obvestilo SI-CERT in SIGOV-CERT	24 ur
Priglasitev incidenta SI-CERT ali SIGOV-CERT	72 ur
Prijava kršitve OP	72 ur
Končno poročilo	1 mesec, če traja dlje, po zaključku

Navodilo:
https://www.cert.si/prijava-incidenta/

Obrazec:
https://www.cert.si/wp-content/uploads/2024/04/PRILOGA-E_OBRAZEC-ZA-POROCANJE-ZAVEZANCA-O-KIBERNETSKEM-INCIDENTU.docx

SPOZNANJA IN IZBOLJŠAVE

Kaj smo se iz incidenta naučili

Ali se znamo organizirati, razdeliti naloge, usklajeno in učinkovito delovati?

Ali imamo potrebna znanja in vire, katere od njih potrebujemo dodatno angažirati izven organizacije?

Ali je naš načrt odzivanja, če ga imamo, ustrezen?

Ali je komuniciranje ustrezno, preveč, premalo, smo koga zanemarili, kako smo se odzivali na objave?

Smo poročali skladno z obveznostmi?

Samo dali celo več koristnih informacij, ki pomagajo drugim organizacijam?

Smo odkrili nove ranljivosti, pomanjkljivosti v procesih, politikah, dokumentacijah?

Vsaka kriza je priložnost za učenje

Namesto da bi incident pometli pod preprogo, smo ga analizirali do potankosti in iz njega potegnili pomembne izboljšave.

To je kultura, ki jo spodbuja ZInfV-1 – stalno izboljševanje kibernetske odpornosti.

HVALA

+111 123 456 789

info@enisa.europa.eu