USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT

NOO | NAČRT ZA OKREVANJE IN ODPORNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI

Financira Evropska unija
NextGenerationEU

Kibernetska varnost

Ransomware: Kibernetska Grožnja

Razumevanje, preprečevanje in odzivanje

Predavatelj: dr. Miha Dvojmoč
Naročnik: GRIFFIN d.o.o.
Izvajalec: MD svetovanje d.o.o.
Datum: 9. 1. 2025

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Ransomware: Izsiljevalska programska oprema

Ransomware je oblika zlonamerne programske opreme, ki uporabniku ali organizaciji onemogoči dostop do podatkov, sistemov ali naprav. Napadalci nato zahtevajo odkupnino, običajno v zameno za obljubo, da bodo dostop obnovili.

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Kaj je ransomware?

Ransomware je zlonamerna programska oprema, ki zaklene ali šifrira podatke. Napadalci običajno zahtevajo plačilo odkupnine, pogosto v kriptovalutah, in grozijo z objavo ukradenih podatkov. Ni zgolj tehnični problem, ampak tudi poslovno in organizacijsko tveganje.

Zakaj je ransomware nevaren?

- Izguba dostopa do podatkov
- Ustavitev poslovnih procesov
- Velika finančna škoda
- Pravne posledice in izguba ugleda
- Motnje pri izvajanju storitev
- Popolna prekinitev delovanja organizacije

Kako ransomware deluje?

Tipičen potek napada

Faza 1

Napadalec pridobi dostop

Faza 2

Zlonamerna programska oprema se namesti

Faza 3

Ransomware se razširi po sistemu

Faza 4

Podatki se šifrirajo

Faza 5

Uporabnik prejme obvestilo o odkupnini

Faza 6

Napadalec zahteva plačilo

Faza 1

Napadalec pridobi dostop

Faza 2

Zlonamerna programska oprema se namesti

Faza 3

Ransomware se razširi po sistemu

Faza 4

Podatki se šifrirajo

Faza 5

Uporabnik prejme obvestilo o odkupnini

Faza 6

Napadalec zahteva plačilo

Kako ransomware deluje?

Tipičen potek napada

Faza 1

Napadalec pridobi dostop

Faza 2

Zlonamerna programska oprema se namesti

Faza 3

Ransomware se razširi po sistemu

Faza 4

Podatki se šifrirajo

Faza 5

Uporabnik prejme obvestilo o odkupnini

Faza 6

Napadalec zahteva plačilo

Najpogostejši načini okužbe

- Zlonamerne e-poštne priponke in lažne povezave
- Okužene spletne strani
- Šibka gesla in nezaščiten oddaljen dostop
- Ranljivosti v programski opremi
- Okuženi USB-ključi
- Napadalci izkoriščajo nepazljivost uporabnikov

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

E-pošta kot vstopna točka

- Lažni računi in obvestila dostavnih služb
- Ponarejena sporočila bank
- Navidezno nujna obvestila
- Okužene priponke in povezave do lažnih strani
- Phishing in spear phishing napadi
- Vsaka nepričakovana priponka ali povezava je varnostno tveganje

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Socialni inženiring

- Manipulacija ljudi, da izvedejo dejanje v korist napadalca.
- Izkoriščanje strahu in nujnosti.
- Zloraba radovednosti ali zaupanja.
- Uporaba lažne avtoritete ali identitete.
- Pogosto preko lažnih e-poštnih sporočil z nujnimi navodili.
- Ransomware napadi pogosto ciljajo na človeški faktor.

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Šifriranje podatkov

- Datotek ni več mogoče odpreti
- Dokumenti postanejo neuporabni
- Baze podatkov so lahko nedostopne
- Poslovni sistemi lahko prenehajo delovati
- Šifriranje se iz varnostnega mehanizma spremeni v orodje napadalca

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Odkupnina

- Koliko in kam mora žrtev plačati (običajno kriptovalute)
- Do kdaj mora biti plačilo izvedeno
- Kaj se zgodi, če žrtev ne plača
- Navodila za stik z napadalci
- Plačilo ne zagotavlja obnove podatkov ali preprečitve zlorabe

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Dvojno izsiljevanje

- Poleg šifriranja napadalci podatke tudi ukradejo
- Grožnje z objavo ukradenih podatkov
- Grožnje s prodajo podatkov ali obveščanjem strank
- Dodatni pritiski na organizacijo
- Dobra varnostna kopija ne odpravi vseh posledic napada

Trojno izsiljevanje

- Napadalci pritisk razširijo še na stranke in poslovne partnerje
- Vključuje zaposlene, javnost in regulatorje
- Namen je povečati pritisk za plačilo
- Ransomware se razvija v širšo obliko pritiska
- Povečana škoda za ugled in zaupanje

Kdo so tarče napadov?

- Podjetja vseh velikosti
- Javne ustanove in občine
- Bolnišnice in šole
- Banke in proizvodna podjetja
- Posamezniki in manjše organizacije
- Tarče so, kjer bi nedostopnost podatkov povzročila veliko škodo

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Ransomware v podjetjih

- Prizadetost proizvodnje, prodaje in dobavnih verig
- Motnje v računovodstvu in kadrovskih evidencah
- Izguba baz strank in ključne dokumentacije
- Prekinitev interne in eksterne komunikacije
- Ransomware lahko hitro preraste v poslovno krizo
- Resne finančne in operativne posledice

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Ransomware v javnem sektorju

- Vpliv na delovanje občin in upravne postopke
- Motnje v zdravstvu in izobraževanju
- Nedostopnost evidenc in podatkov
- Prekinitev komunikacije z državljani
- Onemogočanje izvajanja javnih storitev
- Posledice prizadenejo tudi uporabnike javnih storitev

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Ransomware v zdravstvu

- Nedostopnost zdravstvenih podatkov pacientov
- Težave pri naročanju in diagnostični opremi
- Motnje v komunikaciji med oddelki
- Prekinitev obravnave in oskrbe pacientov
- Ransomware vpliva tudi na varnost ljudi
- Posebej občutljivo področje z resnimi posledicami

Posledice za organizacijo

- Finančna izguba in stroški obnove
- Trajna izguba podatkov
- Dolgoročne motnje v poslovanju
- Pravni postopki in globe
- Izguba zaupanja in ugleda
- Posledice lahko trajajo mesece ali celo leta

Varnostne kopije

- Redne in preverjene varnostne kopije podatkov
- Ločene od glavnega sistema
- Zaščitene pred spreminjanjem
- Dostopne ob incidentu
- Redno testiranje obnovitvenih procesov
- Varnostna kopija je koristna le, če jo lahko ob napadu resnično uporabimo

Pravilo 3-2-1

- **3 kopije** podatkov (original + dve kopiji)
- **2 različna medija** (npr. disk in oblak)
- **1 kopija izven lokacije** ali izven glavnega sistema
- Namen: da podatki niso izgubljeni, tudi če napadalec prizadene glavni sistem ali eno od kopij.

Posodabljanje sistemov

- Posodabljanje operacijskih sistemov in aplikacij
- Posodobitve protivirusnih programov in varnostnih sistemov
- Posodobitve strežnikov, brskalnikov in vdelane programske opreme
- Redno odpravljanje znanih ranljivosti
- Neposodobljeni sistemi imajo ranljivosti, ki jih napadalci lahko izkoristijo

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Močna gesla in večfaktorska avtentikacija

- Uporaba močnih in edinstvenih gesel
- Neuporaba istega gesla povsod
- Redna menjava ogroženih gesel
- Uporaba upravljalnika gesel
- Večfaktorska avtentikacija (MFA) močno zmanjša nepooblaščen dostop

Omejevanje dostopov

- Dodelitev najmanjših potrebnih pravic (princip najmanjših privilegijev)
- Redno preverjanje uporabniških računov in njihovih pravic
- Odstranjevanje neaktivnih in starih računov
- Omejevanje administratorskih pravic
- Ločevanje običajnih in privilegiranih uporabnikov

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Izobraževanje zaposlenih

- Prepoznavanje lažnih e-sporočil (phishing)
- Varna uporaba priponk in preverjanje povezav
- Pravilno ravnanje z gesli
- Prijavljanje sumljivih dogodkov
- Ravnanje z občutljivimi podatki
- Varnostno zavedanje ljudi je ključnega pomena

Tehnični varnostni ukrepi

- Robustna protivirusna in proti-zlonamerna zaščita
- Sistemi za zaznavanje in preprečevanje vdorov (IDS/IPS)
- Požarne pregrade (firewall)
- Filtriranje e-pošte in spletnih vsebin
- Segmentacija omrežja in nadzor dostopov
- Beleženje dogodkov in varnostno spremljanje (SIEM)

Segmentacija omrežja

- Razdelitev omrežja na ločene dele
- Napadalec se težje širi po sistemu
- Občutljivi sistemi so bolje zaščiteni
- Incident je lažje omejiti
- Posledice napada so lahko manjše

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Kaj storiti ob sumu na ransomware?

- Takoj odklopiti okuženo napravo iz omrežja
- Ne izklapljati vsega brez premisleka
- Obvestiti odgovorne osebe in IT službo
- Ne brisati dokazov, zabeležiti dogodke
- Ne odpirati dodatnih datotek
- Vključiti strokovnjake za kibernetsko varnost

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Načrt incidentnega odziva

- Opredelitev odgovornih oseb in vlog
- Jasni postopki obveščanja in eskalacije
- Tehnični in pravni postopki ukrepanja
- Načrt komunikacije z vsemi deležniki
- Načrt obnove sistemov in podatkov
- Poročanje pristojnim organom

Komunikacija med napadom

- Z vodstvom, IT službo in pravno službo
- S strankami in poslovnimi partnerji
- S pristojnimi organi in po potrebi z javnostjo
- Transparentnost in točnost informacij
- Izogibanje paniki in širjenju nepreverjenih informacij
- Slaba komunikacija lahko poveča škodo in izgubo zaupanja

Ali plačati odkupnino?

- Ni zagotovila za obnovitev podatkov
- Tveganje, da napadalci zahtevajo dodatna plačila
- Podatki so lahko že ukradeni in objavljeni
- Plačilo spodbuja kriminalno dejavnost
- Odločitev mora vključevati pravne, poslovne in varnostne strokovnjake

Ključni preventivni ukrepi

- Redne in preverjene varnostne kopije.
- Redno posodabljanje sistemov in programske opreme.
- Večfaktorska avtentikacija (MFA).
- Omejevanje dostopov in privilegijev.
- Izobraževanje in ozaveščanje zaposlenih.
- Segmentacija omrežja.

Zaključek

- Ransomware je ena najresnejših kibernetskih groženj sodobnega časa.
- Lahko povzroči izgubo podatkov, prekinitev poslovanja in finančno škodo.
- Prinaša tudi pravne posledice in dolgoročno škodo za ugled in zaupanje.
- Zaščita zahteva celovit pristop, ki vključuje tehnologijo, organizacijo in ljudi.
- To ni enkraten ukrep, ampak stalni proces prilagajanja in izboljšav.
- Pripravljenost in hiter odziv sta ključna za zmanjšanje morebitne škode.

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT

NOO | NAČRT ZA OKREVANJE IN ODPORNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI

Financira Evropska unija
NextGenerationEU

Kibernetska varnost

Ransomware: Kibernetska Grožnja

Razumevanje, preprečevanje in odzivanje

Predavatelj: dr. Miha Dvojmoč
Naročnik: GRIFFIN d.o.o.
Izvajalec: MD svetovanje d.o.o.
Datum: 9. 1. 2025