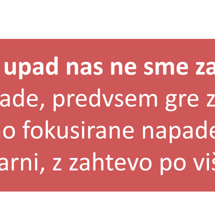
RANSOMWARE

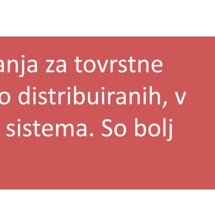
Izsiljevalski virusi v 2020*

Kaj se zgodi, ko nas ransomware napad doleti?

Kar polovica organizacij je že bila žrtev ransomware napada



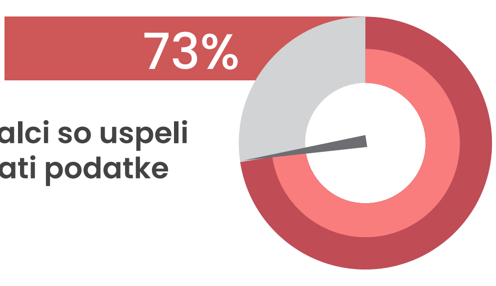
2017
54 % podjetji je bilo žrtev ransomware napada



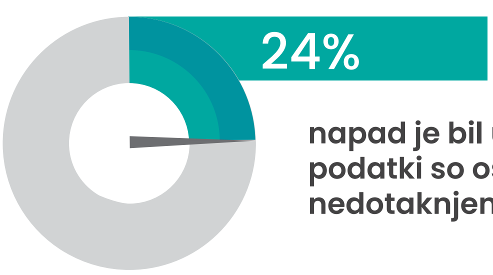
2020
51 % podjetji je bilo že žrtev ransomware napada

3 % upad nas ne sme zavesti - to ni posledica zmanjšanja zanimanja za tovrstne napade, predvsem gre za spreminjanje taktik napada. Iz masovno distribuiranih, v ciljno fokusirane napade, ki izkoriščajo točno določeno ranljivost sistema. So bolj nevarni, z zahtevo po višji odkupnini.

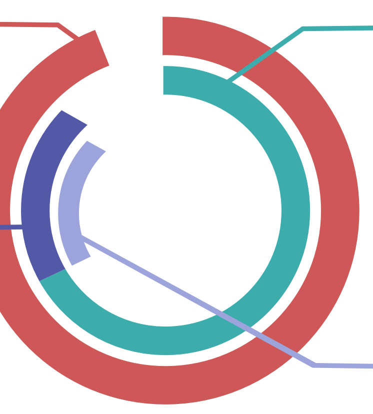
Stopnja uspešnosti ransomware napada



napadalci so uspeli zašifrirati podatke



napad je bil ustavljen, podatki so ostali nedotaknjeni



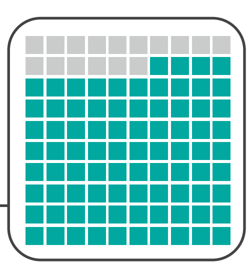
94%
organizacij je zašifrirane podatke dobilo nazaj

56%
s pomočjo varnostnih kopij

26%
s plačilom odkupnine

94%
s plačilom odkupnine, ki ga je krilo zavarovanje

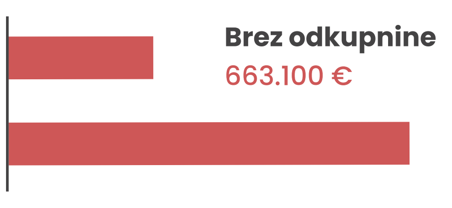
84%
podjetji že ima zavarovanja v primeru kibernetskega napada, v povprečju 64 % teh ima zavarovalno polico, ki krije ransomware napade



Večinoma vse žrtve napadov povrnejo svoje podatke, a ne za isto ceno

Plačilo odkupnine v povprečju podvoji stroške, saj ne zagotovi takojšnjega zagona delovnih procesov, potrebno je še veliko dela in sredstev za povrnitev v prvotno stanje.

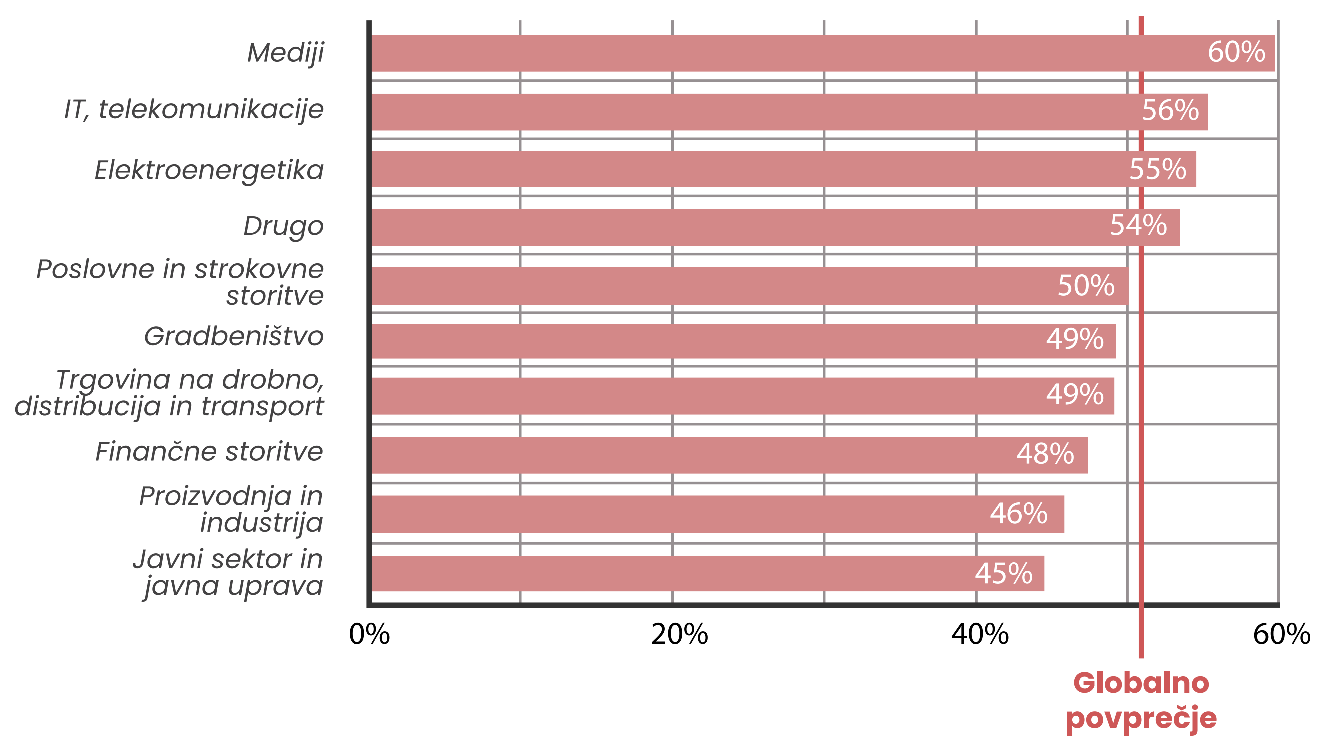
Povprečni stroški napada
(čas izpada, čas zaposlenih, stroški naprav, stroški omrežja, izguba dogodkov, odkupnina...)



Brez odkupnine
663.100 €

Z odkupnino
1.261.950 €

Pogostost napadov glede na gospodarsko dejavnost



Med zašifriranimi podatki prevladujejo podatki v javnem oblaku

59%
uspešnih napadov je na podatke v javnem oblaku

Nobeni podatki niso varni, zato morate poskrbeti za varno hranjenje in kopiranje, tako podatkov pri sebi kot tistih v oblaku.

TEHNIKE NAPADA

Kako virus pride v sistem žrtve?

Napadalec prodira v sistem na najrazličnejše načine (z uporabo širokega nabora tehnik) dokler ne najde šibke točke v obrambi, ki jo izkoristi.

29% prenos zlonamerne datoteke iz spleta preko lažne povezave

21% oddaljeni napadi na ciljne strežnike

16% e-mail z zlonamerno kodo

9% napačna konfiguracija oblačnih instanc

9% preko protokola za oddaljeno namizje

9% preko zunanjih izvajalcev

7% preko USB in druge zunanje naprave

- Napadi se spreminjajo – iz eksplozivne distribucije so se prelevili v nekaj napadov na dan, iz masovnih so prešli na usmerjene, ciljane napade. Iz takih, ki so se izvršili znotraj par tednov, do takih, ki ostanejo skriti tudi po več let. To so t. i. napredne trajne grožnje (APT-Advanced Persistent Threat).
- Temeljijo na konkretni izbiri in študiji tarče in delujejo po principu 'land + expand', kar pomeni da napadalec poskuša dobiti kontrolo nad čim širšim delom omrežja. Širitev okužbe po omrežju je vztrajna, tiha in vodljiva.
- Napadalec navadno svojo pozornost in čas usmeri na specifično napravo, najpogosteje je to končni strežnik, s ciljem pridobiti odkupnino v zameno za povrnitev podatkov v prvotno stanje.

7 VARNOSTNIH PRIPOROČIL
Da se izognete izsiljevalskim virusom

1 Ransomware napadi so v današnjem svetu povsem realna in vse skozi prisotna grožnja. Pred napadom se lahko zaščitite zgolj tako, da ga poskušate preprečiti.

2 Z investicijo v “anti-ransomware” tehnologijo lahko ustavite nepooblaščeno šifriranje datotek.

3 Kot zelo dobro vemo, ampak občasno na to pozabimo: varnostno kopiranje zelo pomaga.

4 Zavarujte podatke, kjer jih hranite - v javnem, zasebnem oblaku ali na lokaciji. Javni oblak še vedno predstavlja določen delež tveganja, zato sprejmite priporočilne ukrepe.

5 Zavarujte se za primer kibernetskega napada oz. se prepričajte, da obstoječe zavarovanje krije škodo v primeru ransomware napada.

6 Implementirajte večnivojsko zaščito, s tem se boste zaščitili proti različnim vektorjem napada.

7 Ozaveščajte uporabnike o možnih nevarnostih, ki nanje pretijo na Internetu, ter s tem zmanjšajte tveganja t. i. človeškega faktorja.

---

*Vir: Povzeto po neodvisni raziskavi “The state of ransomware 2020”, v kateri je sodelovalo 5.000 IT managerjev iz 26 držav. Sophos, maj 2020.

30 SMART COM

Že več kot 30 let delujemo na področju IKT in smo eden izmed vodilnih sistemskih integratorjev v Jugovzhodni Evropi. Z ekipo več kot 70 strokovnjakov in specialistov vzpostavljamo sodobna in zanesljiva komunikacijska omrežja in varnostne rešitve za zaščito pred naprednimi kibernetskimi grožnjami. Z vpeljavo tehnoloških rešitev, ki temeljijo na strojnem učenju in umetni inteligenci ter avtomatizacijo in orkestracijo skrbimo za zaščito IK infrastrukture.

Smart Com d.o.o., Brnčičeva 45, 1231 Črnuče - Ljubljana

www.smart-com.si