

Sadržaj

1.	UVOD.....	4
2.	RAČUNARSKE MREŽE.....	5
2.1	TIPOVI RAČUNARSKIH MREŽA	5
2.1.1	LOKALNE MREŽE (LAN).....	5
2.1.2	ŠIROKOPOJASNE MREŽE (WAN)	5
2.1.3	MREŽE PREDUZEĆA (Engl. ENTERPRISE).....	6
2.1.4	MREŽE DOBAVLJAČA USLUGE (Engl. ISP).....	6
2.2	OSI MODEL.....	6
2.2.1	FIZIČKI SLOJ.....	7
2.2.2	SLOJ VEZE PODATAKA (ENGL. DATA LINK LAYER, DLL.)	7
2.2.3	MREŽNI SLOJ (ENGL. NETWORK LAYER.).....	8
2.2.4	TRANSPORTNI SLOJ (ENGL. TRANSPORT LAYER.)	9
2.2.5	SLOJ SESIJE (ENGL. SESSION LAYER.).....	9
2.2.6	SLOJ PREZENTACIJE (ENGL. PRESENTATION LAYER.)	9
2.2.7	SLOJ APLIKACIJE (ENGL. APPLICATION LAYER.)	9
2.3	TCP/IP MODEL	10
2.3.1	SLOJ ZA VEZU PODATAKA (ENGL. DATA LINK LAYER.).....	12
2.3.2	SLOJ INTERNET.....	12
2.3.2	TRANSPORTNI SLOJ.....	12
2.3.2	SLOJ APLIKACIJE.....	12
2.4	KLJUČNE RAZLIKE IZMEĐU OSI I TCP/IP MODELA	12
3.	SAJBER PRIJETNJE	13
4.	KLASIČNI TIPOVI NAPADA.....	14
4.1	PRIJETNJE U TRANZITU.....	14
4.2	OTMICA TCP SESIJE	15
4.3	MAN IN THE MIDDLE NAPAD.....	17
4.4	SMURF NAPAD	18
4.5	NAPAD PREUSMJERAVANJA SAOBRAĆAJA.....	18
4.6	NAPADI NA USLUGU NAZIVA DOMENA (DNS)	19
4.7	NAPADI DISTRIBUIRANOG ODBIJANJA USLUGE (DDOS)	20
4.8	SYN FLOOD NAPAD	20
5.	MODERNI TIPOVI NAPADA.....	20
5.1	ZLONAMJERNI SOFTVER (ENGL. MALWARE)	20
5.1.1	RAČUNARSKI VIRUSI.....	22
5.1.2	CRVI (ENGL. WORMS)	22

5.1.3 TROJANSKI KONJI (ENGL. TROJANS)	22
5.1.4 ZLONAMJERNI SOFTVER BEZ TRAGA DATOTEKA (ENGL. FILE-LESS MALWARE)	24
5.1.5 POLIMORFNI ZLONAMJERNI SOFTVER (ENGL. POLYMORPHIC MALWARE)	24
5.2 ŠPIJUNSKI SOFTVER (ENGL. SPYWARE)	26
5.3 UCJENIVAČKI SOFTVER (ENGL. RANSOMWARE)	27
5.4 ADWARE	29
5.5 ROOTKIT	29
5.6 ŠPIJUNIRANJE UNOSA SA TASTATURE (Engl. Keyloggers).....	29
5.7 ZLONAMJERNO RUDARENJE KRIPTO VALUTA (ENGL. CRYPTOJACKING). 30	
5.8 ROGUE SOFTWARE	30
5.9 ZAŠTRAŠUJUĆI SOFTVER (ENGL. SCAREWARE)	30
5.10 NAPADI KOMANDOVANJA I KONTROLE (C2).....	31
5.11 NAPREDNA ISTRAJNA PRIJETNJA (ENGL. ADVANCED PERSISTENT THREAT)	32
5.12 LAŽNO PREDSTAVLJANJE (ENGL. PHISHING).....	34
5.13 NAPADI NA WEB APLIKACIJE	35
5.13.1 CROSS-SITE SCRIPTING (XSS).....	35
5.13.2 FUZZING (FUZZ TESTIRANJE)	37
5.13.3 STRUCTURED QUERY LANGUAGE (SQL) INJECTION.....	37
5.14 NAPADI NA BEŽIČNE MREŽE.....	38
6. SAJBER ZAŠTITA.....	39
7. ŠTA JE MREŽNA BEZBJEDNOST?	40
8. METODE ZAŠTITE I ODBRANE RAČUNARSKIH MREŽA I SISTEMA.....	41
8.1 ŠIFROVANJE PODATAKA (ENGL. DATA ENCRYPTION)	41
8.1.1 ŠIFROVANJE VEZE ILI ŠIFROVANJE S KRAJA NA KRAJ (ENGL. LINK ENCRYPTION AND END-TO-END ENCRYPTION).....	42
8.1.2 VIRTUELNE PRIVATNE MREŽE (ENGL. VPN)	42
8.2 ZAŠTITNI ZID (ENGL. FIREWALL).....	43
8.2.1 PAKETNI FILTERI.....	44
8.2.2 LIČNI ZAŠTITNI ZID.....	44
8.2.3 APPLICATION PROXY FIREWALL.....	44
8.2.4 STATEFUL INSPECTION FIREWALL	45
8.2.5 ZAŠTITNI ZID SLJEDEĆE GENERACIJE (Engl. NEXT GEN FIREWALL).....	45
8.3 SISTEM ZA OTKRIVANJE UPADA (Engl. Intrusion Detection Systems).....	46
8.4 SKENIRANJE SADRŽAJA I DUBOKA INSPEKCIJA PAKETA (Engl. Content Filtering and Deep Packet Inspection).....	47

8.4.1 SPRJEČAVANJE GUBITKA PODATAKA (Engl. DATA LOSS PREVENTION).....	48
8.4.2 HTTP/S INSPEKCIJE PROKSI SISTEM (Engl. HTTP/S EXPLICIT INSPECTION PROXY SYSTEM).....	49
8.5 UPRAVLJANJE I KONTROLA MOBILNIH UREĐAJA U PREDUZEĆU (ENGL. MOBILE DEVICE MANAGEMENT)	50
8.6 ANTI-MALWARE SOFTVER.....	51
8.7 ZAŠTITA KRAJNJE TAČKE (Engl. Endpoint Security).....	51
8.8 SIGURNOST KAO SERVIS.....	52
9. PREPORUKE ZA IZGLED I FUNKCIONISANJA SISTEMA ZA ZAŠTITU PREDUZEĆA.....	53
10. ZAKLJUČAK	55
11. LITERATURA.....	56
12. POPIS SLIKA	57